



Securing Cisco TelePresence Products, Release 1.7

August, 2011

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-18391-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

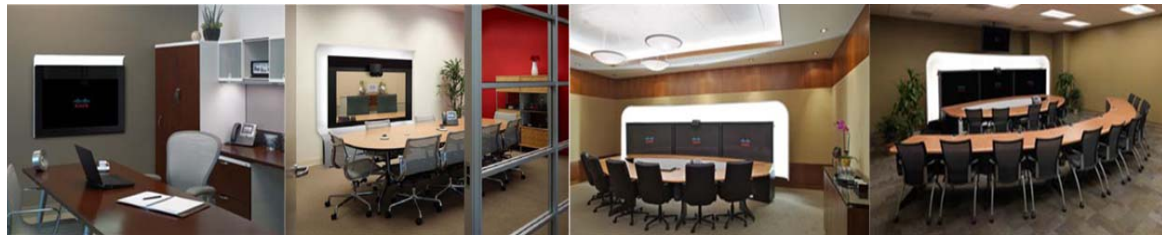
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Securing Cisco TelePresence Products, Release 1.7
© 2010-2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

What's in This Guide	vii
Contents	vii
Security Solutions Overview	vii
Ensuring Secure CTS Integration with the Cisco TelePresence Server	viii
Document Organization	viii
Related Documents	ix
Obtaining Technical Assistance	x
Cisco.com	x
Technical Assistance Center	x
Obtaining Documentation and Submitting a Service Request	xi
Activating the Certificate Authority Proxy Function Server	1-1
Contents	1-1
CAPF Server Activation Task Checklist	1-1
Activating the CAPF Server	1-2
Creating and Configuring an Application User	1-4
Creating a CAPF Profile for Cisco Unified CM	1-6
Downloading Certificates from Cisco Unified CM	1-9
Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates from the Phone	1-11
Finding Phones on Basis of LSC Status or Authentication String	1-12
Managing CAPF Settings in the Phone Configuration Window	1-13
Entering the CAPF Authentication String Using CLI	1-14
Where to Go Next	1-14
Configuring the Cisco CTL Client	2-1
Contents	2-1
Cisco CTL Client Overview	2-2
Important Installation Note for CTL Client 5.0 Plug-In	2-2
Important Installation Note for Windows 2000 Users	2-3
Configuration Tips for Cisco CTL Client Configuration	2-3
Cisco CTL Client Configuration Checklist	2-4
Activating the Cisco CTL Provider Service	2-5
Activating the Cisco CAPF Service	2-6

- Configuring Ports for the TLS Connection 2-6
- Installing the Cisco CTL Client 2-7
- Configuring the Cisco CTL Client 2-8
- Updating the CTL File 2-11
- Deleting a CTL File Entry 2-12
- Updating the Cisco Unified Communications Manager Security Mode 2-12
- Cisco CTL Client Configuration Settings 2-12
- Verifying the Cisco Unified Communications Manager Security Mode 2-15
- Setting the Smart Card Service to Started and Automatic 2-15
- Changing the Security Token Password (Etoken) 2-16
- Deleting the CTL File on the Cisco Unified IP Phone 2-16
- Determining the Cisco CTL Client Version 2-17
- Verifying or Uninstalling the Cisco CTL Client 2-17
- Where to Go Next 2-18

Configuring Security for the Cisco TelePresence Multipoint Switch 3-1

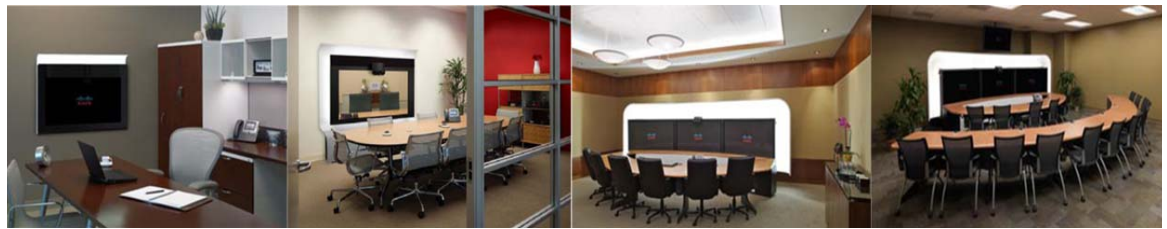
- Contents 3-1
- Cisco TelePresence Multipoint Switch Configuration Checklist 3-1
- Uploading Downloaded Security Certificates to CTMS 3-2
- Downloading LSCs on the CTMS 3-4
- Creating a SIP Trunk Security Profile 3-6
- Configuring the SIP Security Trunk 3-8
 - Configuring an Existing Trunk for SIP Security 3-9
 - Creating and Configuring a New Trunk for SIP Security 3-9
- Configuring the CTMS for SIP Security 3-11
- Removing Security from the Cisco TelePresence Multipoint Switch 3-12
- Understanding Encrypted Key Transport (EKT) and CTMS Secure Communications 3-13
 - Cisco TelePresence Multipoint Call Operation 3-14
- Where to Go Next 3-16

Configuring Security for the Cisco TelePresence Recording Server 4-1

- Contents 4-1
- Cisco TelePresence Recording Server Configuration Checklist 4-1
- Uploading the CAPF Root Certificate to the CTRS 4-2
- Downloading the Cisco Unified CM Root Certificate 4-3
- Uploading the Cisco Unified CM Root Certificate to the CTRS 4-4
- Downloading the LSC to the CTRS 4-4

Setting the Default Security Level	4-5
Configuring the SIP Security Trunk	4-6
Configuring an Existing Trunk for SIP Security	4-7
Creating and Configuring a New Trunk for SIP Security	4-7
Configuring the CTRS for SIP Security	4-9
Removing Security from the Cisco TelePresence Recording Server	4-10
Where to Go Next	4-11
Configuring Security for Cisco TelePresence Manager	5-1
Contents	5-1
Cisco TelePresence Manager Configuration Checklist	5-1
Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications	5-2
Uploading Downloaded Security Certificates to Cisco TelePresence Manager	5-4
Downloading LSCs to Cisco TelePresence Manager	5-5
Removing Security from Cisco TelePresence Manager	5-6
Where to Go Next	5-7
Configuring and Verifying Cisco TelePresence Security	6-1
Contents	6-1
Cisco TelePresence Security Configuration Checklist	6-1
Configuring Cisco TelePresence Phone Profile Security	6-2
Adding Authentication Information to the Cisco TelePresence System	6-3
Verifying Security Status	6-4
Verifying Security Status Between the Cisco TelePresence System and Cisco TelePresence Manager	6-4
Verifying Security Status Between the CTMS and Cisco TelePresence Manager	6-4
Where to Go Next	6-5
Troubleshooting Security Configuration on the Cisco TelePresence System	7-1
Contents	7-1
Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch	7-1
Resetting Administrator and Security Passwords	7-3
Where to Go Next	7-4
Contents	A-1
Overview	A-1
TCP and UDP Ports for Cisco TelePresence	A-2
Cisco TelePresence System (CTS) Primary Codec	A-3
Cisco Unified IP Phone 797X	A-5

Cisco TelePresence Manager (CTS-Manager) **A-7**
Cisco TelePresence Multipoint Switch (CTMS) **A-11**
Cisco TelePresence Recording Server (CTRS) **A-13**
Cisco IOS IP Service Level Agreements (IPSLA) **A-14**
Cisco Media Experience Engine (MXE) 5600 **A-15**



What's in This Guide

Revised: August 2011, OL-18391-01

Contents

- [Security Solutions Overview, page vii](#)
- [Ensuring Secure CTS Integration with the Cisco TelePresence Server, page viii](#)
- [Document Organization, page viii](#)
- [Related Documents, page ix](#)
- [Obtaining Technical Assistance, page x](#)
- [Obtaining Documentation and Submitting a Service Request, page xi](#)

Security Solutions Overview

Cisco TelePresence devices support secure communication between devices using Certificate Authority Proxy Function (CAPF). Cisco TelePresence is part of Cisco Unified Communications and shares security architecture using CAPF. This functionality is similar to Cisco Unified IP phone security architecture. Other key architectural elements that are used include the Certificate Trust List (CTL), Locally Significant Certificate (LSC), and Computer Telephony Integration (CTI).

The following is an overview of how CAPF is configured on Cisco TelePresence components:

1. CAPF service is started in Cisco Unified CM so that the Cisco Unified CM becomes the CAPF server.
2. The Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence Recording Server (CTRS), and Cisco TelePresence Manager (CTS-Manager) are configured as CAPF clients.
3. A common application user ID is configured for each CAPF client, and separate instance IDs are created for the CTMS, CTRS, and Cisco TelePresence Manager.
4. CAPF authenticates information between the Cisco TelePresence devices using a Locally Significant Certificate (LSC).

The LCS can be downloaded from the CAPF Server (same as the Cisco Unified CM host in most cases) using CTI secured connections over TLS. As part of the Cisco Unified Communications architecture, Cisco TelePresence endpoints follow the configuration on the Cisco Unified CM to

automatically download their LSC during initial setup. CTMS, CRTS, and CTS-Manager, on the other hand, do not register to the Cisco Unified CM and therefore require manual steps to obtain the LCS from the CAPF server.

To create secure services, you must activate and start CAPF service, create application users, create Cisco Unified CM root certificates for every Cisco Unified CM server associated with a Cisco TelePresence service, and create a CAPF root certificate. Then in the administration interface for each Cisco TelePresence device, you must upload the applicable Cisco Unified CM and CAPF root certificates and download the appropriate LSCs. When all certificates are in place and the LSC is downloaded, the Cisco TelePresence device reboots so that the security settings take effect.

See the [Cisco Unified Communications Manager Security Guide](#) for overall operational details.

Ensuring Secure CTS Integration with the Cisco TelePresence Server

To secure media on calls to a Cisco TelePresence Server, you will need to do the following:

1. Make the endpoint secure by using the configuration steps in this guide.
2. Add the encryption release key to the Cisco TelePresence Server. To obtain your encryption key, contact the Cisco Technical Assistance Center (TAC). See the [“Technical Assistance Center” section on page x](#) to choose a contact option.

See the following Cisco TelePresence Server support documentation on Cisco.com:

- [Cisco TelePresence Server home page](#)
- [Cisco TelePresence Management Suite](#)

Document Organization

See the following chapters to set up security on your system:

- [Chapter 1, “Activating the Certificate Authority Proxy Function Server”](#)
- [Chapter 2, “Configuring the Cisco CTL Client”](#)
- [Chapter 3, “Configuring Security for the Cisco TelePresence Multipoint Switch”](#)
- [Chapter 4, “Configuring Security for the Cisco TelePresence Recording Server”](#)
- [Chapter 5, “Configuring Security for Cisco TelePresence Manager”](#)
- [Chapter 6, “Configuring and Verifying Cisco TelePresence Security”](#)
- [Chapter 7, “Troubleshooting Security Configuration on the Cisco TelePresence System”](#)
- [Appendix A, “Cisco TelePresence Firewall and Access List Considerations”](#)

Related Documents

Related Topic	Document Title
How to navigate to Cisco TelePresence System (CTS) hardware and software documentation, including information about CTS devices.	<ul style="list-style-type: none"> • Cisco.com Products > TelePresence > Cisco TelePresence System > TelePresence System
Cisco Unified CM security operational details.	<ul style="list-style-type: none"> • Cisco Unified Communications Manager Security Guide
Configuration, maintenance, and monitoring tasks using Cisco TelePresence administration software.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software home page on Cisco.com
Cisco TelePresence administration software documentation and software download page.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software Download
Describes new features and open and closed hardware and software caveats for Cisco TelePresence System (CTS) software releases.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software Release Notes home page on Cisco.com
Cisco Unified CM installation with the Cisco TelePresence System.	<ul style="list-style-type: none"> • Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System
Cisco command-line interface (CLI) information for configuring the Cisco TelePresence System.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software Command References home page on Cisco.com
Guide to troubleshooting the Cisco TelePresence System, including Cisco Unified CM administration and CTS Cisco Unified IP phone issues.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software Troubleshooting Guide on Cisco.com
Cisco TelePresence User Guide and Quick Reference Card, including information about using the CTS Cisco Unified IP phone.	<ul style="list-style-type: none"> • Cisco TelePresence Administration Software End-User Guides on Cisco.com
Cisco TelePresence System system message information.	<ul style="list-style-type: none"> • Cisco TelePresence System Message Guide
Cisco TelePresence Manager documentation home page.	<ul style="list-style-type: none"> • Cisco TelePresence Manager home page on Cisco.com
Information about the Cisco TelePresence Multipoint Switch (CTMS).	<ul style="list-style-type: none"> • Cisco TelePresence Multipoint Switch home page on Cisco.com
Cisco TelePresence Recording Server information.	<ul style="list-style-type: none"> • Cisco TelePresence Recording Server home page on Cisco.com
Complete guide to the CTS software and hardware documentation.	<ul style="list-style-type: none"> • Cisco TelePresence System Documentation Roadmap
Cisco Unified CM documentation types and locations.	<ul style="list-style-type: none"> • Cisco Unified Communications Manager (CallManager) Documentation Roadmaps
Cisco Unified Communications Manager Support page.	<ul style="list-style-type: none"> • Cisco Unified Communications Manager Support
Cisco Validated Design Program. Systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments.	<ul style="list-style-type: none"> • Cisco TelePresence Network Systems 2.0 Design Guide

Information about Key Exchange via Encrypted Key Transport (EKT) and other Cisco TelePresence security solutions.	<ul style="list-style-type: none"> • Design Zone for Video: Cisco TelePresence Secure Communications and Signaling Guide
Information about the Cisco TelePresence Server.	<ul style="list-style-type: none"> • Cisco TelePresence Server home page
Information about managing your videoconferencing network.	<ul style="list-style-type: none"> • Cisco TelePresence Management Suite
Cisco Unified IP Phone firmware download instructions.	<ul style="list-style-type: none"> • Installation Notes section of the Cisco Unified IP Phone Release Notes for Firmware Release 8.5(3) (SCCP and SIP)

Obtaining Technical Assistance

When the recommended action of a syslog log message advises that you contact Cisco technical support, open a case with the Cisco Technical Assistance Center (TAC). Read the following methods to obtain additional information.

Cisco.com

Cisco.com is a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/en/US/customer/support/index.html>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<https://tools.cisco.com/RPF/register/register.do>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://tools.cisco.com/ServiceRequestTool/create/>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

P1 and P2 level problems are defined as follows:

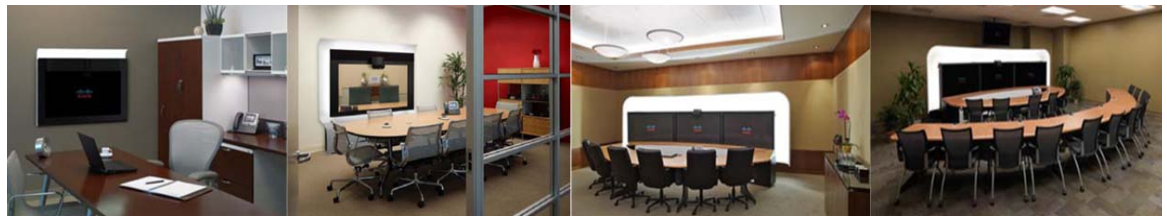
- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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.



CHAPTER 1

Activating the Certificate Authority Proxy Function Server

Revised: September, 2010, OL-18391-01



Tip

When performing the tasks in this chapter, it can be helpful to keep two browser sessions open, with one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Multipoint Switch (CTMS) administration interface.

Contents

This chapter describes how to activate the CAPF server and includes the following sections:

- [CAPF Server Activation Task Checklist, page 1-1](#)
- [Activating the CAPF Server, page 1-2](#)
- [Creating and Configuring an Application User, page 1-4](#)
- [Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates from the Phone, page 1-11](#)
- [Finding Phones on Basis of LSC Status or Authentication String, page 1-12](#)
- [Managing CAPF Settings in the Phone Configuration Window, page 1-13](#)
- [Entering the CAPF Authentication String Using CLI, page 1-14](#)
- [Where to Go Next, page 1-14](#)

CAPF Server Activation Task Checklist

[Table 1-1](#) provides a list of configuration tasks that you perform to activate CAPF Server for the first time.

Table 1-1 Cisco CAPF Server Activation Task Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Enable secure communications between Cisco Unified CM and Cisco TelePresence devices	Activating the CAPF Server, page 1-2.
Step 2	Create and configure an application user	Creating and Configuring an Application User, page 1-4
Step 3	Configure a CAPF profile on the server side and client side.	Creating a CAPF Profile for Cisco Unified CM, page 1-6
Step 4	Download the CAPF certificates from Cisco Unified CM	Downloading Certificates from Cisco Unified CM, page 1-9
Step 5	Enter the CAPF authentication string using command-line interface (CLI) to install the locally significant certificate (LSC).	Entering the CAPF Authentication String Using CLI, page 1-14

Activating the CAPF Server

Use the information in this section to enable secure communications between Cisco Unified CM and Cisco TelePresence devices. The CAPF Server is installed by default with Cisco Unified CM and runs as a service; after you activate and start the CAPF service, Cisco Unified CM is used as a CAPF server. You can then configure the CTMS, and Cisco TelePresence Manager (CTS-Manager) software as CAPF clients.



Note

To enable secure conference bridge registration, set the Cisco Unified CM cluster security mode to mixed mode: **Cluster Security Mode** field is set to **1**. Mixed mode allows authenticated, encrypted, and nonsecure Cisco Unified IP Phones to register with Cisco Unified Communications Manager. In this mode, Cisco Unified Communications Manager ensures that authenticated or encrypted devices use a secure port.

Cisco Unified Communications Manager disables auto-registration if you configure mixed mode.

To activate the CAPF server, follow these steps:

Step 1 Log in to Cisco Unified CM administration interface.



Note

If there are Cisco Unified CM subscribers in your cluster, perform this step for your Cisco Unified CM publisher. You configure the subscribers later in this chapter.

Step 2 From the Navigation drop-down list, choose **Cisco Unified Serviceability** and click **Go**.

Step 3 Choose **Tools > Service Activation**.

Step 4 Choose a server from the Server drop-down list and click **Go**.

Step 5 Scroll down to the Security Services area and check the **Cisco Certificate Authority Proxy Function** check box to activate the CAPF server, as shown in [Figure 1-1](#).

Figure 1-1 Activating the CAPF service in Cisco Unified CM

The screenshot shows the Cisco Unified CallManager Serviceability interface. The page title is "Service Activation" and the user is logged in as "ccmadministrator". The "Status" is "Ready". The "Select Server" dropdown is set to "vijendra-cm5".

CM Services		Activation Status
Service Name		
Performance and Monitoring Services		
Service Name		Activation Status
<input checked="" type="checkbox"/> Cisco Serviceability Reporter		Activated
<input checked="" type="checkbox"/> Cisco CallManager SNMP Service		Activated
Security Services		
Service Name		Activation Status
<input checked="" type="checkbox"/> Cisco CTL Provider		Activated
<input checked="" type="checkbox"/> Cisco Certificate Authority Proxy Function		Activated
Directory Services		
Service Name		Activation Status
<input type="checkbox"/> Cisco DirSync		Deactivated

Buttons: Save, Set to Default, Refresh

Info: *- indicates required item.

274402

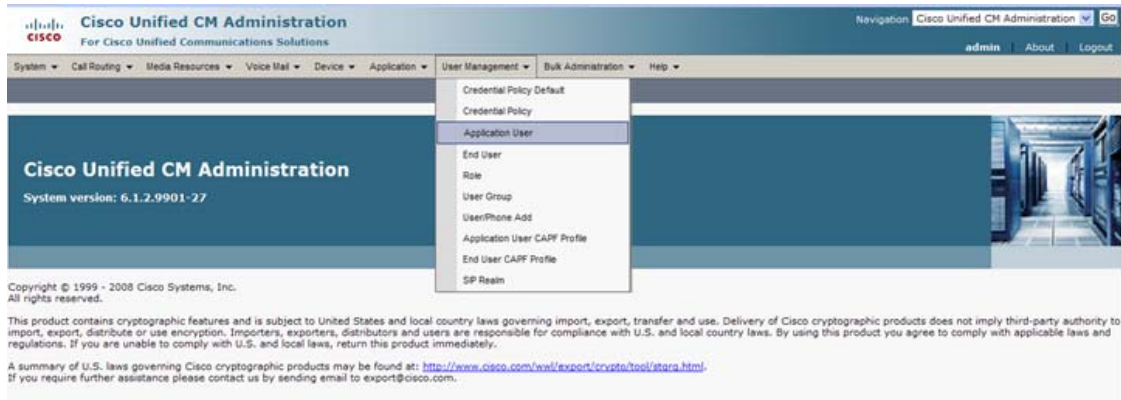
Step 6 Proceed to [Creating and Configuring an Application User](#).

Creating and Configuring an Application User

To create and configure an application user, or to modify the configuration of an existing user, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User**, as shown in [Figure 1-2](#).

Figure 1-2 Creating an Application User



- Step 2** Choose one of the following:

- To create a new CTMS application user, click the **Add New** button, and continue to [Step 3](#).



Note Cisco recommends that you create a new application user for each system component (CTMS, CTRS, and CTS-Manager.)

- To use an existing application user, click the **Find** button, locate the user ID, click the hypertext link to select that user, and continue to [Step 4](#).

Step 3 In the **Application User Information** area, enter a user ID and password, as shown in [Figure 1-3](#).



Note Make a note of the user ID that you create.

Figure 1-3 Adding Application User ID and Password

The screenshot shows the 'Application User Configuration' window. At the top, there are icons for Save, Delete, Copy, and Add New. Below this is a 'Status' section with an information icon and the text 'Status: Ready'. The main section is 'Application User Information', which contains the following fields:

- User ID***: A text box containing 'dhsr110'.
- Password**: A password field with masked characters.
- Confirm Password**: A password field with masked characters.
- Digest Credentials**: An empty text box.
- Confirm Digest Credentials**: An empty text box.
- Presence Group***: A dropdown menu showing 'Standard Presence group'.

A small number '274405' is visible in the bottom right corner of the screenshot.

Step 4 Add and verify the following groups and roles in the Permissions Information area:

- a. Click **Add to User Group**.
- b. Check the check box next to **Standard CTI Enabled** and **Standard CTI Secure Connection**.
- c. Click **Add Selected**.
Cisco Unified CM automatically adds the information that you choose in the Groups field to the Roles field.
- d. Verify that the following roles display in the Roles field:
 - Standard AXL API Access
 - Standard CCM Admin Users
 - Standard CTI Enabled
 - Standard CTI Secure Connection
- e. If the Standard AXL API Access and Standard CCM Admin Users roles do not appear in the Roles field, you can add them now.

Choosing this permission information enables the following security features in Cisco Unified CM:

- Transport Layer Security (TLS) support
- Certificate Tracking (in this case, the LSC)
- For Cisco Unified CM Version 7.0, Secure Real-Time Protocol (SRTP) support

Creating a CAPF Profile for Cisco Unified CM

A CAPF Server authenticates a CAPF Client based on a client profile pre-configured in the Cisco Unified CM database. This requires users to configure a CAPF Profile on the server side and client side. The CAPF Profile parameters need to be provided to authenticate each client. The CAPF Server configuration is performed from the Cisco Unified CM Administration web page which allows users to configure an Application or End-user CAPF Profile. This configuration record is stored in the server database to authenticate the client which is trying to download the certificate.

To create a CAPF profile, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User CAPF Profile**, as shown in [Figure 1-4](#).

Figure 1-4 Creating a CAPF Profile



- Step 2** Click the **Add New** button, as shown in [Figure 1-5](#).

Figure 1-5 Adding a New User



Step 3 Enter the following information using Figure 1-6 as a guide:

- **Application User**—Select the user you just created in the “Creating and Configuring an Application User” section on page 1-4.
- **Instance Id**—Enter an ID that is unique for this Cisco Unified CM cluster.



Note Make a note of the Instance ID that you create. You use this information later in this chapter when you download LSCs in the “Downloading LSCs on the CTMS” section on page 3-4.

- **Certificate Operation**—Choose **Install//Upgrade**.
- **Authentication Mode**—Choose **By Authentication String** (default).
- **Authentication String**—Click this text box and manually enter an authentication string. Optionally, you can click the **Generate String** button to create a randomly generated authentication string.



Note Make a note of the authentication string. You use this information later in this chapter.

- **Key size (bits)**—Choose **1024** (default).
- **Operation Completes By**—Leave the default value.



Note To avoid regenerating a new authentication string, complete the procedure in the “Downloading LSCs on the CTMS” section on page 3-4 before the date and time that is specified in the Operation Completes By field.

Figure 1-6 Configuring the CAPF Profile

Application User CAPF Profile Configuration

Save

Status

Status: Ready

Application User CAPF Profile

Application User* -- Not Selected --

Instance Id*

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* Install/Upgrade

Authentication Mode* By Authentication String

Authentication String Generate String

Key Size (bits)* 1024

Operation Completes By 2008 : 10 : 2 : 12 (MM:MM:DD:HH)

Certificate Operation Status: None

Save

* - indicates required item

Done

274409

- Step 4** Click **Save**. The Application User CAPF Profile Configuration window should look similar to the example in [Figure 1-7](#).

Figure 1-7 Application User CAPF Profile Configuration Window Example

Application User CAPF Profile Configuration

Save Delete Copy Add New

Status
 Status: Ready

Application User CAPF Profile

Application User* dh93-User
 Instance Id* 093

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* Install/Upgrade
 Authentication Mode* By Authentication String
 Authentication String 1410254971 **Generate String**
 Key Size (bits)* 1024
 Operation Completes By 2008 : 10 : 5 : 12 (YY:MM:DD:HH)
 Certificate Operation Status: Upgrade Success

Save Delete Copy Add New

274410

Downloading Certificates from Cisco Unified CM

Download the Certificates from Cisco Unified CM in preparation for uploading them to CTMS and Cisco TelePresence Manager. To download the certificate(s), follow these steps:

Step 1 Log in to Cisco Unified CM administration interface.

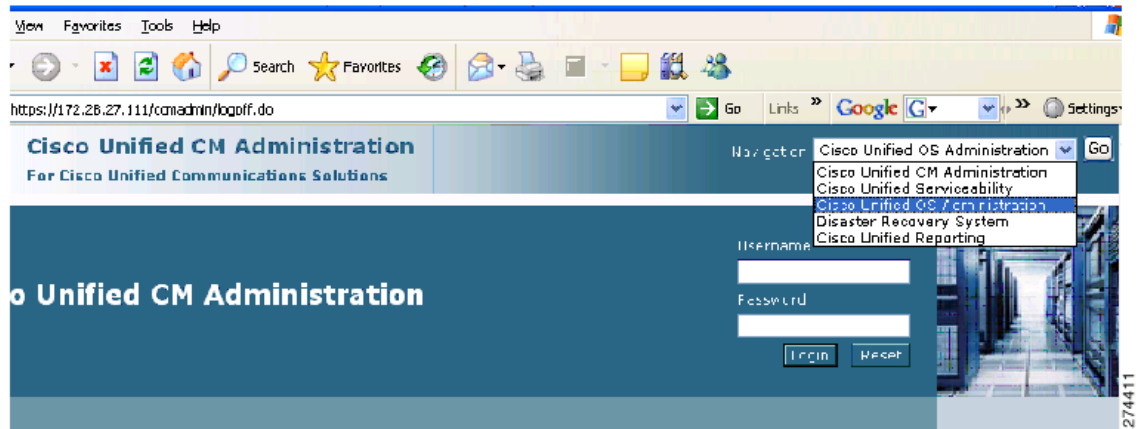


Note

If there are Cisco Unified CM subscribers in your cluster, perform this step for your Cisco Unified CM publisher. You configure the subscribers later in this procedure.

- Step 2** From the Navigation drop-down list, choose **Cisco Unified OS Administration** and click **Go**, as shown in [Figure 1-8](#).

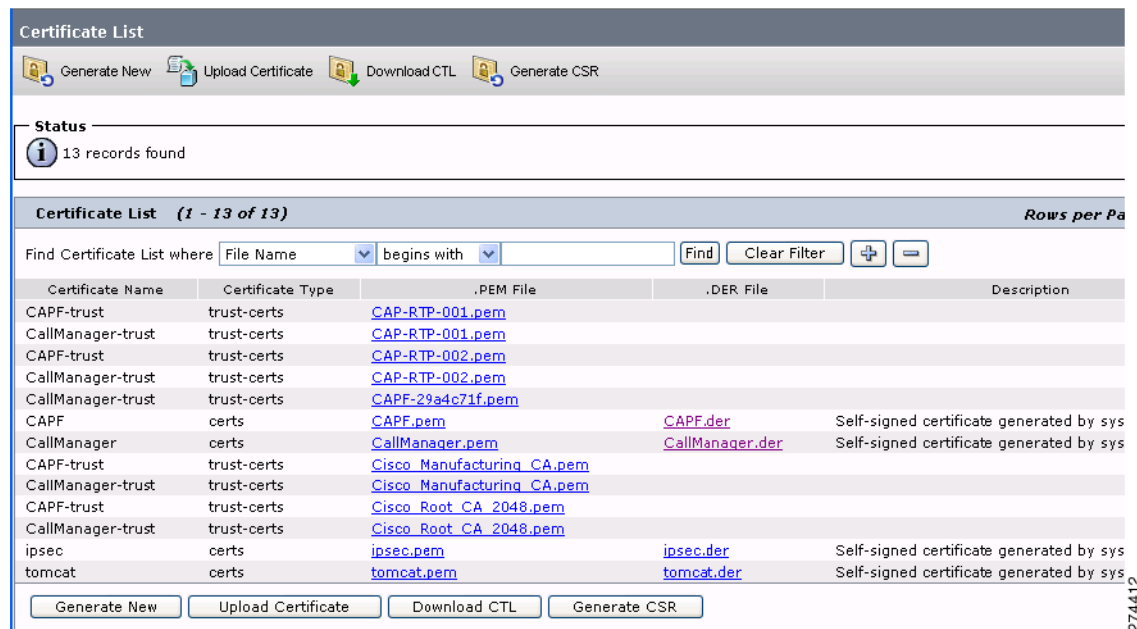
Figure 1-8 Navigating to the Cisco Unified OS Administration Page



- Step 3** Choose **Security > Certificate Management**. The Certificate List window appears, as shown in [Figure 1-9](#).

- Step 4** Click the **Find** button.

Figure 1-9 Location of CAPF.der File in Find Results



- Step 5** Locate the CAPF.der file and click the **CAPF.der** hypertext link. The Certificate Configuration window appears.

- Step 6** Click **Download**.

- Step 7** Download the file to your local machine, retaining the **CAPF.der** file name.

- Step 8** Return to the Certificate List window.
- Step 9** If you cannot locate the CallManager.der file, click the **Find** button.
- Step 10** Locate the CallManager.der file and click the **CallManager.der** hypertext link.
- Step 11** Click **Download**.
- Step 12** Download the file to your local machine. Rename the file to **CUCM0.der**.



Note Be sure to rename this file.

- Step 13** If there are any subscribers in your Cisco Unified CM cluster, do the following:
- Download the CallManager.der file from each subscriber to your local machine by performing [Step 1](#) through [Step 11](#).
 - For each subscriber, rename the CallManager.der file to **CUCM x .der**, where x is the number of the subscriber. For example:

Download the CallManager.der file from the first subscriber and rename that file **CUCM1.der**, download the CallManager.der file from the second subscriber and rename that file **CUCM2.der**, and so on.
-

Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates from the Phone

To use the Certificate Authority Proxy Function, follow these steps, using the information in [Table 1-2](#) as a reference:

-
- Step 1** Find the phone, as described in the *Cisco Unified Communications Manager Administration Guide*.
- Step 2** After the search results display, locate the phone where you want to install, upgrade, delete, or troubleshoot the certificate and click the **Device Name (Line)** link for that phone.
- Step 3** Enter the configuration settings, as described in [Table 1-2](#).
- Step 4** Click **Save**.
- Step 5** Click **Reset**.
-

Finding Phones on Basis of LSC Status or Authentication String

To find phones on the basis of certificate operation status or the authentication string, follow these steps:

Step 1 In Cisco Unified Communications Manager Administration, choose **Device > Phone**.

The Find and List window displays. Records from an active (prior) query may also display in the window.

Step 2 From the first drop-down list box, choose one of the following options:

- **LSC Status**—Choosing this option returns a list of phones that use CAPF to install, upgrade, delete, or troubleshoot locally significant certificates.
- **Authentication String**—Choosing this option returns a list of phones with an authentication string that is specified in the Authentication String field.

Step 3 From the second drop-down list box, choose a search pattern.

Step 4 Specify the appropriate search text, if applicable.



Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 5 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Step 6 From the list of records that display, click the link for the record that you want to view.



Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Managing CAPF Settings in the Phone Configuration Window

Table 1-2 describes the CAPF settings in the Phone Configuration window in Cisco Unified Communications Manager Administration.

Table 1-2 CAPF Configuration Settings

Setting	Description
Certificate Operation	<p>From the drop-down list box, choose one of the following options:</p> <ul style="list-style-type: none"> • No Pending Operation—Displays when no certificate operation is occurring. (default setting) • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture-installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified Communications Manager creates two trace files, one for each certificate type. <p>Tip By choosing the Troubleshoot option, you can verify that an LSC or MIC exists in the phone. The Delete and Troubleshoot options do not display if a certificate does not exist in the phone.</p>
Authentication String	<p>If you chose the By Authentication String option, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits.</p> <p>To install, upgrade, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string. See “Entering the CAPF Authentication String Using CLI” section on page 1-14 for more information.</p>
Generate String	<p>If you want CAPF to automatically generate an authentication string, click this button. The 4- to 10-digit authentication string displays in the Authentication String field.</p>
Operation Completes by	<p>This field, which supports all certificate operation options, specifies the date and time by which you must complete the operation.</p>
Operation Status	<p>This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot certificate operation options. You cannot change the information that displays in this field.</p>

Entering the CAPF Authentication String Using CLI

If you chose the By Authentication String mode and generated an authentication string, you must enter the authentication string using CTS command-line interface (CLI) to install the locally significant certificate (LSC).



Tip

The authentication string is for one-time use only.

Before You Begin

Before you enter the authentication string using CLI, verify that the following conditions are met:

- The CAPF certificate exists in the CTL file.
- You activated the Cisco Certificate Authority Proxy Function service, as described in [“Activating the CAPF Server” section on page 1-2](#).
- The Cisco Unified CM server is operational.

Procedure

To set the authentication string using CLI, follow these steps:

Step 1 Log into your SSH client.

Step 2 Enter the following command:

```
admin help set security authstring
```

```
authstring help:
```

```
This will set the CAPF authentication string.
```

```
syntax is: set security authstring numeric_string
```

```
numeric_string      mandatory      This is a numeric authorization
                                string that matches the CUCM device
                                setting
```

Note: The authentication string must be greater than four digits and numerical in value.

Example:

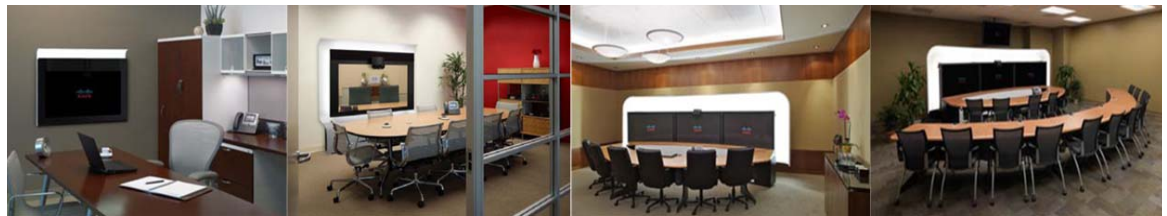
```
admin: set security authstring 123456
admin:
```

Related Information

See the [Cisco Unified Communications Manager Security Guide](#) for step-by-step instructions for configuring authentication and encryption for Cisco Unified Communications Manager and Cisco Unified IP Phones.

Where to Go Next

See [Chapter 2, “Configuring the Cisco CTL Client”](#) for information about the Certificate Trust List (CTL) file.



CHAPTER 2

Configuring the Cisco CTL Client

Revised: December, 2010, OL-18391-01

Contents

This chapter contains information on the following topics:

- [Cisco CTL Client Overview, page 2-2](#)
- [Configuration Tips for Cisco CTL Client Configuration, page 2-3](#)
- [Important Installation Note for CTL Client 5.0 Plug-In, page 2-2](#)
- [Important Installation Note for Windows 2000 Users, page 2-3](#)
- [Configuration Tips for Cisco CTL Client Configuration, page 2-3](#)
- [Cisco CTL Client Configuration Checklist, page 2-4](#)
- [Activating the Cisco CTL Provider Service, page 2-5](#)
- [Activating the Cisco CAPF Service, page 2-6](#)
- [Configuring Ports for the TLS Connection, page 2-6](#)
- [Installing the Cisco CTL Client, page 2-7](#)
- [Configuring the Cisco CTL Client, page 2-8](#)
- [Updating the CTL File, page 2-11](#)
- [Deleting a CTL File Entry, page 2-12](#)
- [Updating the Cisco Unified Communications Manager Security Mode, page 2-12](#)
- [Cisco CTL Client Configuration Settings, page 2-12](#)
- [Verifying the Cisco Unified Communications Manager Security Mode, page 2-15](#)
- [Setting the Smart Card Service to Started and Automatic, page 2-15](#)
- [Changing the Security Token Password \(Etoken\), page 2-16](#)
- [Deleting the CTL File on the Cisco Unified IP Phone, page 2-16](#)
- [Determining the Cisco CTL Client Version, page 2-17](#)
- [Verifying or Uninstalling the Cisco CTL Client, page 2-17](#)

Cisco CTL Client Overview

Device, file, and signaling authentication rely on the creation of the Certificate Trust List (CTL) file, which is created when you install and configure the Cisco Certificate Trust List Client on a single Windows workstation or server that has a USB port.

**Note**

Supported Windows versions for Cisco CTL Client include Windows 2000, Windows XP, and Windows Vista. Do not use Terminal Services to install the Cisco CTL Client. Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote troubleshooting and configuration tasks.

The CTL file contains entries for the following servers or security tokens:

- System Administrator Security Token (SAST)
- Cisco CallManager and Cisco TFTP services that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall

The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

After you create the CTL file, you must restart the Cisco Unified CM and Cisco TFTP services in on all nodes that run these services. The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in .sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

After the Cisco CTL Client adds a server certificate to the CTL file, you can display the certificate in the CTL Client GUI.

When you configure a firewall in the CTL file, you can secure a Cisco ASA Firewall as part of a secure Cisco Unified Communications Manager system. The Cisco CTL Client displays the firewall certificate as a “CCM” certificate.

Cisco Unified Communications Manager Administration uses an etoken to authenticate the TLS connection between the Cisco CTL Client and Cisco CTL Provider.

Important Installation Note for CTL Client 5.0 Plug-In

If you are upgrading to the CTL Client 5.0 or 5.2 plug-in, you first need to remove eToken Run Time Environment 3.00 by performing the following steps:

Step 1 Download Windows Installer Cleanup Utility at the following URL:

<http://support.microsoft.com/kb/290301>

Step 2 Install the utility on your PC.

Step 3 Run the utility.

Step 4 Find eToken rte3.0 in the list of programs and remove it.

Step 5 Proceed with CTL Client installation.

Important Installation Note for Windows 2000 Users

If you are running Windows 2000 on your workstation or server, you must download Windows Installer 3.0 updates to correctly install CTL Client plug-ins. You can obtain Windows Installer 3.0 at the following URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=5FBC5470-B259-4733-A914-A956122E08E8&displaylang=en>



Note

Windows 2000 comes with Windows Installer 2.0.

Windows Installer 3.0 requires validation. Follow the instructions to have your PC validated. Then, install Windows Installer 3.0, reboot your machine if necessary, and then proceed with CTL Client installation.

Configuration Tips for Cisco CTL Client Configuration

Consider the following information when you configure the Cisco CTL Client in Cisco Unified Communications Manager:

- The Cisco CTL Client limits the file size of a CTL file to 32 kilobytes because the phones cannot accept a larger CTL file. The following factors affect the size of a CTL file:
 - The number of nodes in the cluster. More nodes require more certificates in the CTL file.
 - The number of firewalls that are used for TLS Proxy
 - Firewalls with TLS Proxy feature, which are the same as nodes, therefore get included in the CTL file.
 - Whether an external certificate authority (CA) signs the CAPF and Cisco Unified CM certificates. Because certificates (CAPF/Cisco Unified CM) that are signed by an external CA are significantly larger than default self-signed certificates, this can limit the maximum number of certificates that can fit into the CTL file.

These factors directly limit the maximum number of certificates that you can fit in a 32-kilobyte CTL file, so they dictate the maximum number of nodes or firewalls that you can have in a secure Cisco Unified Communications Manager deployment.

- Ensure that the Cisco Unified Communications Manager node hostname or hostnames are resolvable on the remote PC where the Cisco CTL Client is installed, or the Cisco CTL Client will not function correctly.
- You must activate the Cisco CTL Provider service.
- After you create or update the CTL file, you must restart the Cisco Unified CM and Cisco TFTP services in Cisco Unified Serviceability.

The following information applies only to intercluster environments. Cisco does not support ICTs on Cisco Unified Communications Manager Business Edition systems.

When the Cisco CTL Client contains entries for off-cluster servers, such as alternate or centralized TFTP server, you must also run the Cisco CTL Provider service on these servers.

- The alternate TFTP server section of the Cisco CTL Client GUI designates a Cisco TFTP server that exists in a different cluster. Use the Alternate TFTP Server Tab settings to configure alternate and centralized TFTP servers in the Cisco CTL Client.

**Note**

See “Cisco TFTP” in the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System* for information about configuring off-cluster (alternate and centralized) TFTP servers with TFTP service parameters.

- For centralized TFTP configurations, all off-cluster TFTP servers that are operating in mixed mode (**Cluster Security Mode** field is set to **1**) must add the Master TFTP server or Master TFTP server IP address to the off-cluster CTL file. The master TFTP server serves configuration files from all alternate TFTP servers in the alternate file list that is configured for the master TFTP server. Clusters in a centralized TFTP configuration do not need to use the same security mode; each cluster can select its own mode.

Cisco CTL Client Configuration Checklist

Table 2-1 provides a list of configuration tasks that you perform to install and configure the Cisco CTL Client for the first time. See “Configuring the Cisco CTL Client” section on page 2-8 for more information about configuring the CTL file when you upgrade Cisco Unified Communications Manager.

Table 2-1 Cisco CTL Client Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Ensure that all the servers in the cluster are online and reachable from the PC on which the CTL Client will run. If a server is configured with a hostname, ping the hostname to verify reachability.	—
Step 2	Ensure that all of the hostnames of the cluster servers are defined in the DNS server that is configured on the publisher server.	—
Step 3	Activate the Cisco CTL Provider service in Cisco Unified Serviceability. Tip If you activated this service prior to a Cisco Unified Communications Manager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service, page 2-5
Step 4	Activate the Cisco Certificate Authority Proxy service in Cisco Unified Serviceability. Timesaver Performing this task before you install and configure the Cisco CTL Client ensures that you do not have to update the CTL file to use CAPF.	Chapter 1, “Activating the Certificate Authority Proxy Function Server”

Table 2-1 Cisco CTL Client Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	If you do not want to use the default settings, configure ports for the TLS connection. Tip If you configured these settings prior to a Cisco Unified Communications Manager upgrade, the settings migrate automatically.	Configuring Ports for the TLS Connection, page 2-6
Step 6	Obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL Client.	Configuring the Cisco CTL Client, page 2-8
Step 7	Install the Cisco CTL Client.	Installing the Cisco CTL Client, page 2-7
Step 8	Configure the Cisco CTL Client.	Configuring the Cisco CTL Client, page 2-8
Note	After you create or update the CTL file, you must restart the Cisco Unified CM and Cisco TFTP services in Cisco Unified Serviceability.	

Activating the Cisco CTL Provider Service

After you configure the Cisco CTL Client, the Cisco CTL Provider service changes the security mode from nonsecure to mixed mode (**Cluster Security Mode** field is set to **1**) and transports the server certificates to the CTL file. The service then transports the CTL file to all Cisco Unified Communications Manager and Cisco TFTP servers.

If you activate this service and then upgrade Cisco Unified Communications Manager, Cisco Unified Communications Manager automatically reactivates the service after the upgrade.

To activate the service, follow these steps:

-
- Step 1** In Cisco Unified Serviceability, choose **Tools > Service Activation**.
 - Step 2** In the Servers drop-down list box, choose a server where you have activated the Cisco CallManager or Cisco TFTP services.
 - Step 3** Click the **Cisco CTL Provider** service radio button.
 - Step 4** Click **Save**.



Note You can enter a CTL port before you activate the Cisco CTL Provider service. If you want to change the default port number, see the “[Configuring Ports for the TLS Connection](#)” section on [page 2-6](#).

- Step 5** Verify that the service runs on the server. In Cisco Unified Serviceability, choose **Tools > Control Center - Feature Services** to verify the state of the service.
-

Activating the Cisco CAPF Service

For information on activating this service, see the [Chapter 1, “Activating the Certificate Authority Proxy Function Server”](#).



Timesaver

Performing this task before you install and configure the Cisco CTL Client ensures that you do not have to update the CTL file to use CAPF.

Configuring Ports for the TLS Connection

You may have to configure a different TLS port number if the default port is currently being used or if you use a firewall and you cannot use the port within the firewall.

- The Cisco CTL Provider default port for the TLS connection equals 2444. The Cisco CTL Provider port monitors requests from the Cisco CTL Client. This port processes Cisco CTL Client requests, such as retrieving the CTL file, setting the cluster security mode, and saving the CTL file to the TFTP server.



Note

Cluster security mode configures the security capability for your standalone server or a cluster.

- The Ethernet Phone Port monitors registration requests from the phone that is running SCCP. In nonsecure mode, the phone connects through port 2000. In mixed mode (**Cluster Security Mode** field is set to **1**), the Cisco Unified Communications Manager port for TLS connection equals the value for the Cisco Unified Communications Manager port number added to (+) 443; therefore, the default TLS connection for Cisco Unified Communications Manager equals 2443. Update this setting only if the port number is in use or if you use a firewall and you cannot use the port within the firewall.
- The SIP Secure Port allows Cisco Unified Communications Manager to listen for SIP messages from phones that are running SIP. The default value equals 5061. If you change this port, you must restart the Cisco CallManager service in Cisco Unified Serviceability and reset the phones that are running SIP.



Tip

After you update the port(s), you must restart the Cisco CTL Provider service in Cisco Unified Serviceability.

You must open the CTL ports to the data VLAN from where the CTL Client runs. Phones that are running TLS for signaling back to Cisco Unified Communications Manager also use the ports that the CTL Client uses. Ensure that you open these ports to all VLANs where phones are configured for authenticated or encrypted status.

To change the default setting, follow these steps:

Step 1

Perform the following tasks, depending on the port that you want to change:

- To change the Port Number parameter for the Cisco CTL Provider service, perform [Step 2](#) through [Step 6](#).

- To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform [Step 7](#) through [Step 11](#).
- Step 2** To change the Cisco CTL Provider port, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration.
- Step 3** In the Server drop-down list box, choose a server where the Cisco CTL Provider service runs.
- Step 4** In the Service drop-down list box, choose **Cisco CTL Provider** service.



Tip For information on the service parameter, click the question mark or the link name.

- Step 5** To change the value for the Port Number parameter, enter the new port number in the Parameter Value field.
- Step 6** Click **Save**.
- Step 7** To change the Ethernet Phone Port or SIP Phone Secure Port settings, choose **System > Cisco Unified CM** in Cisco Unified Communications Manager Administration.
- Step 8** Find a server where the Cisco CallManager service runs, as described in the [Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System](#); after the results display, click the **Name** link for the server.
- Step 9** After the Cisco Unified Communications Manager Configuration window displays, enter the new port numbers in the Ethernet Phone Port or SIP Phone Secure Port fields.
- Step 10** Reset the phones and restart the Cisco CallManager service in Cisco Unified Serviceability.
- Step 11** Click **Save**.
-

Installing the Cisco CTL Client

You must use the client and update the CTL file when the following events occur:

- The first time that you set the cluster security mode
- The first time that you create the CTL file
- After the Cisco Unified Communications Manager installation
- After you restore a Cisco Unified Communications Manager server or Cisco Unified Communications Manager data
- After you change the IP address or hostname of the Cisco Unified Communications Manager server
- After you add or remove a security token
- After you add or remove a ASA firewall
- After you add or remove a TFTP server
- After you upload a third-party, CA-signed certificate to the platform



Tip

If the Smart Card service is not set to started and automatic on the server or workstation where you plan to install the client, the installation fails.

To install the Cisco CTL Client, follow these steps:

-
- Step 1** From the Windows workstation or server where you plan to install the client, browse to Cisco Unified Communications Manager Administration, as described in the Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System.
- Step 2** In Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
The Find and List Plugins window displays.
- Step 3** From the Plugin Type equals drop-down list box, choose **Installation** and click **Find**.
- Step 4** Locate the Cisco CTL Client.
- Step 5** To download the file, click **Download** on the left side of the window, directly opposite the Cisco CTL Client plug-in name.
- Step 6** Click **Save** and save the file to a location that you will remember.
- Step 7** To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file).



Note You can also click **Open** from the Download Complete box.

- Step 8** The version of the Cisco CTL Client displays; click **Continue**.
- Step 9** The installation wizard displays. Click **Next**.
- Step 10** Accept the license agreement and click **Next**.
- Step 11** Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.
- Step 12** To begin the installation, click **Next**.
- Step 13** After the installation completes, click **Finish**.
-

Configuring the Cisco CTL Client



Tip Configure the Cisco CTL Client during a scheduled maintenance window because you must restart the Cisco CallManager services and Cisco TFTP services on all servers that run these services in the cluster.

The Cisco CTL Client performs the following tasks:

- Sets the Cisco Unified Communications Manager cluster security mode.



Note Cluster security mode configures the security capability for a standalone server or a cluster.



Tip You cannot set the Cisco Unified Communications Manager cluster security parameter to mixed mode through the Enterprise Parameters window of Cisco Unified Communications Manager Administration. You must configure the Cisco CTL Client to set the cluster security mode. For more information, see the [“Cisco CTL Client Configuration Settings” section on page 2-12](#).

- Creates the Certificate Trust List (CTL), which is a file that contains certificate entries for security tokens, Cisco Unified Communications Manager, ASA firewall, and CAPF server.

The CTL file indicates the server(s) that support TLS for the phone connection. The client automatically detects the Cisco Unified Communications Manager, Cisco CAPF, and ASA firewall and adds certificate entries for these servers.

The security tokens that you insert during the configuration sign the CTL file.

Before You Begin

Before you configure the Cisco CTL Client, verify that you activated the Cisco CTL Provider service and the Cisco Certificate Authority Proxy Function service in Cisco Unified Serviceability. Obtain at least two security tokens; the Cisco certificate authority issues these security tokens. The security tokens must come from Cisco. You will insert the tokens one at a time into the USB port on the server/workstation. If you do not have a USB port on the server, you may use a USB PCI card.

Obtain the following passwords, hostnames/IP addresses, and port numbers:

- Administrative username and password for Cisco Unified Communications Manager



Tip

Ensure the administrative username is an application user, not an end user, and a member of a super user group with super user roles.

- Security token administrative password
- Administrative username and password for the ASA firewall

See [Table 2-2 on page 2-13](#) for a description of the preceding information.



Tip

Before you install the Cisco CTL Client, verify that you have network connectivity to the server. To ensure that you have network connectivity, issue a ping command, as described in the [Cisco Unified Communications Operating System Administration Guide](#).

If you installed multiple Cisco CTL Clients, Cisco Unified Communications Manager accepts CTL configuration information on only one client at a time, but you can perform configuration tasks on up to five Cisco CTL Clients simultaneously. While you perform configuration tasks on one client, Cisco Unified Communications Manager automatically stores the information that you entered on the other clients.

After you complete the Cisco CTL Client configuration, the CTL Client performs the following tasks:

- Writes the CTL file to the Cisco Unified Communications Manager server(s).
- Writes a CAPF capf.cer to Cisco Unified CM.
- Writes the file to all configured TFTP servers.
- Writes the file to all configured ASA firewalls.
- Signs the CTL file with the private key of the security token that exists in the USB port at the time you create the CTL file.

To configure the client, follow these steps:

- Step 1** Obtain at least two security tokens that you purchased.
- Step 2** Perform one of the following tasks:

- Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
 - Choose **Start > Programs > Cisco CTL Client**.
- Step 3** Enter the configuration settings for the Cisco Unified Communications Manager server, as described in [Table 2-2](#); click **Next**.
- Step 4** Click **Set Cisco Unified Communications Manager Cluster to Mixed Mode (Cluster Security Mode field is set to 1)**, as described in [Table 2-2](#); click **Next**.
- Step 5** Perform the following tasks, depending on what you want to accomplish:
- To add a security token, see [Step 6](#) through [Step 12](#).
 - To complete the Cisco CTL Client configuration, see [Step 17](#) through [Step 21](#).

**Caution**

You need a minimum of two security tokens the first time that you configure the client. Do not insert the tokens until the application prompts you to do so. If you have two USB ports on the workstation or server, do not insert two security tokens at the same time.

- Step 6** When the application prompts you to do so, insert one security token in an available USB port on the workstation or server where you are currently configuring the Cisco CTL Client; click **OK**.
- Step 7** The security token information displays for the token that you inserted; click **Add**.
- Step 8** The detected certificate entries display in the pane.
- Step 9** To add other security token(s) to the certificate trust list, click **Add Tokens**.
- Step 10** If you have not already done so, remove the token that you inserted into the server or workstation. When the application prompts you to do so, insert the next token and click **OK**.
- Step 11** The security token information for the second token displays; click **Add**.
- Step 12** For all security tokens, repeat [Step 9](#) through [Step 11](#).
- Step 13** The certificate entries display in the pane.
- Step 14** Enter the configuration settings, as described in [Table 2-2 on page 2-13](#).
- Step 15** Click **Next**.
- Step 16** Enter the configuration settings, as described in [Table 2-2](#); click **Next**.
- Step 17** When you have added all security tokens and servers, click **Finish**.
- Step 18** Enter the username password for the security token, as described in [Table 2-2](#); click **OK**.
- Step 19** After the client creates the CTL file, a window displays the server, file location, and status of the CTL file on each server. Click **Finish**.
- Step 20** Reset all devices for your standalone server or cluster.
- Step 21** In Cisco Unified Serviceability, restart the Cisco CallManager and Cisco TFTP services.
- Step 22** After you create the CTL file, you may remove the security token from the USB port. Store all security tokens in a safe place that you will remember.
-

Updating the CTL File

You must update the CTL file if the following scenarios occur:

- If you change the name or IP address of a Cisco Unified Communications Manager server
- If you change the IP address or hostname for any configured TFTP servers
- If you change the IP address or hostname for any configured ASA firewall
- If you enabled the Cisco Certificate Authority Function service in Cisco Unified Serviceability
- If you need to add or remove a security token
- If you need to add or remove a TFTP server
- If you need to add or remove an ASA firewall
- If you restore a Cisco Unified Communications Manager server or Cisco Unified Communications Manager data
- After you upload a third-party, CA-signed certificate to the platform



Tip

Cisco strongly recommends that you update the file when minimal call-processing interruptions will occur.

To update the information that exists in CTL file, follow these steps:

-
- Step 1** Obtain one security token that you inserted to configure the latest CTL file.
- Step 2** Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
- Step 3** Enter the configuration settings for the Cisco Unified Communications Manager server, as described in [Table 2-2](#); click **Next**.



Tip

You make updates in this window for the Cisco Unified Communications Manager server.

- Step 4** To update the CTL file, click **Update CTL File**, as described in [Table 2-2](#); click **Next**.



Caution

For all CTL file updates, you must insert one security token that already exists in the CTL file into the USB port. The client validates the signature of the CTL file through this token. You cannot add new tokens until the Cisco CTL Client validates the signature. If you have two USB ports on the workstation or server, do not insert both security tokens at the same time.

- Step 5** If you have not already inserted one security token in an available USB port on the workstation or server where you are currently updating the CTL file, insert one of the security tokens; click **OK**.
- Step 6** The security token information displays for the token that you inserted; click **Next**.
The detected certificate entries display in the pane.



Tip

You cannot update the Cisco Unified Communications Manager, Cisco TFTP, or ASA firewall entries from this pane. To update the Cisco Unified Communications Manager entry, click **Cancel** and perform [Step 2](#) through [Step 6](#) again.

- Step 7** To update existing Cisco CTL entries or to add or delete security tokens, consider the following information:
- To update servers settings or to add new security tokens, see [“Configuring the Cisco CTL Client” section on page 2-8](#).
 - To delete a security token, see the [“Deleting a CTL File Entry” section on page 2-12](#).
- Step 8** When you have finished updating the CTL file, restart the Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability.
-

Deleting a CTL File Entry

At any time, you can delete some CTL entries that display in the CTL Entries window of the Cisco CTL Client. After you open the client and follow the prompts to display the CTL Entries window, highlight the item to delete and click **Delete Selected** to delete the entry.

You cannot delete servers that run Cisco Unified Communications Manager, Cisco TFTP, ASA firewall, or Cisco CAPF from the CTL file.

Two security token entries must exist in the CTL file at all times. You cannot delete all security tokens from the file.

Updating the Cisco Unified Communications Manager Security Mode

You must use the Cisco CTL Client to configure the cluster security mode. You cannot change the Cisco Unified Communications Manager security mode from the Enterprise Parameters window in Cisco Unified Communications Manager Administration.

**Note**

Cluster security mode configures the security capability for a standalone server or a cluster.

To change the cluster security mode after the initial configuration of the Cisco CTL Client, you must update the CTL file. Navigate to the Cluster Security Mode window, change the mode setting, and click **Next**, then **Finish**, as described in the [“Updating the CTL File” section on page 2-11](#) and [Table 2-2](#).

If you change the cluster security mode from mixed to nonsecure mode, the CTL file still exists on the server(s), but the CTL file does not contain any certificates. Because no certificates exist in the CTL file, the phone requests an unsigned configuration file and registers as nonsecure with Cisco Unified Communications Manager.

Cisco CTL Client Configuration Settings

You can set the cluster security mode to nonsecure or mixed mode (**Cluster Security Mode** field is set to **1**), as described in [Table 2-2](#). Only mixed mode supports authentication, encrypted signaling, and encrypted media.

**Note**

Cluster security mode configures the security capability for a standalone server or a cluster.

Use the information in [Table 2-2](#) to configure the Cisco CTL Client for the first time, to update the CTL file, or to change the mode from mixed to nonsecure. For configuration tips, see the “[Configuration Tips for Cisco CTL Client Configuration](#)” section on page 2-3.

Table 2-2 Configuration Settings for CTL Client

Setting	Description
Cisco Unified Communications Manager Server	
Hostname or IP Address	Enter the hostname or IP address for the server.
Port	Enter the CTL port number for the Cisco CTL Provider service that runs on this Cisco Unified Communications Manager server. The default port number equals 2444.
Username and Password	Enter the application user username and password that has superuser administrative privileges.
Security Mode	
Set Cisco Unified Communications Manager Cluster to Mixed Mode	<p>Cluster Security Mode field is set to 1. Mixed mode allows authenticated, encrypted, and nonsecure Cisco Unified IP Phones to register with Cisco Unified Communications Manager. In this mode, Cisco Unified Communications Manager ensures that authenticated or encrypted devices use a secure port.</p> <p>Note Cisco Unified Communications Manager disables auto-registration if you configure mixed mode.</p>
Set Cisco Unified Communications Manager Cluster to Non-Secure Mode	<p>If you configure nonsecure mode, all devices register as unauthenticated, and Cisco Unified Communications Manager supports image authentication only.</p> <p>When you choose this mode, the Cisco CTL Client removes the certificates for all entries that are listed in the CTL file, but the CTL file still exists in the directory that you specified. The phone requests unsigned configuration files and registers as nonsecure with Cisco Unified Communications Manager.</p> <p>Tip To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Cisco Unified Communications Manager servers.</p> <p>You can use auto-registration in this mode.</p>
Update CTL File	After you have created the CTL file, you must choose this option to make any changes to the CTL file. Choosing this option ensures that the Cisco Unified Communications Manager security mode does not change.

Table 2-2 Configuration Settings for CTL Client (continued)

Setting	Description
CTL Entries	
Add Tokens	Click this button to add additional security token(s) to the certificate trust list. If you have not already done so, remove the token that you initially inserted into the server or workstation. When the application prompts you to do so, insert the next token and click OK . When the security token information for the additional token displays, click Add . For all security tokens, repeat these tasks.
Add TFTP Server	Click this button to add an Alternate TFTP server to the certificate trust list. For information on the settings, click the Help button after the Alternate TFTP Server tab settings display. After you enter the settings, click Next .
Add Firewall	Click this button to add an ASA firewall to the certificate trust list. For information on the settings, click the Help button after the Firewall tab settings display. After you enter the settings, click Next .
Alternate TFTP Server	
Hostname or IP Address	Enter the hostname or IP address for the TFTP server. Alternate TFTP server designates a Cisco TFTP server that exists in a different cluster. If you use two different clusters for the alternate TFTP server configuration, both clusters must use the same cluster security mode, which means that you must install and configure the Cisco CTL Client in both clusters. Likewise, both clusters must run the same version of Cisco Unified Communications Manager. Ensure that the path in the TFTP service parameter, FileLocation, is the same for all servers in the cluster. See “Configuration Tips for Cisco CTL Client Configuration” section on page 2-3 for more information.
Port	Not required with this release of Cisco Unified Communications Manager.
Username and Password	Not required with this release of Cisco Unified Communications Manager.
Firewall	
Hostname or IP Address	Enter the hostname or IP address for the firewall.
Port	Not configurable. The system uses the Cisco Unified Communications Manager port; the default port number equals 2444.
Username and Password	Not configurable. The system uses the administrator name and password that you configured during Cisco Unified Communications Manager installation.
Security Token	
User Password	The first time that you configure the Cisco CTL client, enter Cisco123 , the case-sensitive default password, to retrieve the private key of the certificate and ensure that the CTL file gets signed.

Verifying the Cisco Unified Communications Manager Security Mode

To verify the cluster security mode, follow these steps:

**Note**

Cluster security mode configures the security capability for a standalone server or a cluster.

- Step 1** In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
- Step 2** Locate the **Cluster Security Mode** field. If the value in the field displays as **1**, you correctly configured Cisco Unified Communications Manager for mixed mode. (Click the field name for more information.)

**Tip**

You cannot configure this value in Cisco Unified Communications Manager Administration. This value displays after you configure the Cisco CTL Client.

Setting the Smart Card Service to Started and Automatic

If the Cisco CTL Client installation detects that the Smart Card service is disabled, you must set the Smart Card service to automatic and started on the server or workstation where you are installing the Cisco CTL Client plug-in.

**Tip**

You cannot add the security tokens to the CTL file if the service is not set to started and automatic.

After you upgrade the operating system, apply service releases, upgrade Cisco Unified Communications Manager, and so on, verify that the Smart Card service is started and automatic.

To set the service to started and automatic, follow these steps:

- Step 1** On the server or workstation where you installed the Cisco CTL Client, choose **Start > Programs > Administrative Tools > Services** or **Start > Control Panel > Administrative Tools > Services**.
- Step 2** From the Services window, right-click the **Smart Card** service and choose **Properties**.
- Step 3** In the Properties window, verify that the **General** tab displays.
- Step 4** From the Startup type drop-down list box, choose **Automatic**.
- Step 5** Click **Apply**.
- Step 6** In the Service Status area, click **Start**.
- Step 7** Click **OK**.
- Step 8** Reboot the server or workstation and verify that the service is running.

Changing the Security Token Password (Etoken)

This administrative password retrieves the private key of the certificate and ensures that the CTL file gets signed. Each security token comes with a default password. You can change the security token password at any time. If the Cisco CTL Client prompts you to change the password, you must change the password before you can proceed with the configuration.

To review pertinent information on setting passwords, click the **Show Tips** button. If you cannot set the password for any reason, review the tips that display.

To change the security token password, follow these steps:

-
- Step 1** Verify that you have installed the Cisco CTL Client on a Windows server or workstation.
 - Step 2** If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL Client.
 - Step 3** Choose **Start > Programs > etoken > Etoken Properties**, right-click **etoken**, and choose **Change etoken password**.
 - Step 4** In the Current Password field, enter the password that you originally created for the token.
 - Step 5** Enter a new password.
 - Step 6** Enter the new password again to confirm it.
 - Step 7** Click **OK**.
-

Deleting the CTL File on the Cisco Unified IP Phone

**Caution**

Cisco recommends that you perform this task in a secure lab environment, especially if you do not plan to delete the CTL file from the Cisco Unified Communications Manager server(s).

Delete the CTL file on the Cisco Unified IP Phone for the following cases:

- You lose all security tokens that signed the CTL file.
- The security tokens that signed the CTL file appear compromised.
- You move a phone out of a secure environment; for example, to a storage area.
- You move a phone from an area with an unknown security policy to a secure Cisco Unified Communications Manager.
- You change the alternate TFTP server address to a server that does not exist in the CTL file.

To delete the CTL file on the Cisco Unified IP Phone, perform the tasks in [Table 2-3](#).

Table 2-3 *Deleting the CTL File on the Cisco Unified IP Phone*

Cisco Unified IP Phone Model	Tasks
Cisco Unified IP Phones 7960G and 7940G	Under the Security Configuration menu on the phone, press CTL file , unlock or **# , and erase .
Cisco Unified IP Phone 7970G and equivalent	Perform one of the following methods: <ul style="list-style-type: none"> • Unlock the Security Configuration menu, as described in <i>Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager</i>. Under the CTL option, press the Erase softkey. • Under the Settings menu, press the Erase softkey. <p>Note Pressing the Erase softkey under the Settings menu deletes other information besides the CTL file. For additional information, refer to the <i>Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager</i>.</p>

Determining the Cisco CTL Client Version

To determine which version of the Cisco CTL Client you are using, follow these steps:

-
- Step 1** Perform one of the following tasks:
- Double-click the **Cisco CTL Client** icon that exists on the desktop.
 - Choose **Start > Programs > Cisco CTL Client**.
- Step 2** In the Cisco CTL Client window, click the icon in the upper, left corner of the window.
- Step 3** Choose **About Cisco CTL Client**. The version of the client displays.
-

Verifying or Uninstalling the Cisco CTL Client

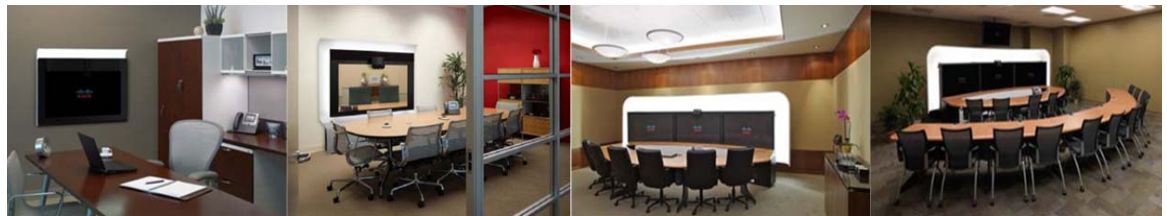
Uninstalling the Cisco CTL Client does not delete the CTL file. Likewise, the cluster security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the Cisco CTL Client, install the client on a different Windows workstation or server, and continue to use the same CTL file.

To verify that the Cisco CTL Client installed, follow these steps:

-
- Step 1** Choose **Start > Control Panel > Add Remove Programs**.
- Step 2** Double-click **Add Remove Programs**.
- Step 3** To verify that the client installed, locate **Cisco CTL Client**.
- Step 4** To uninstall the client, click **Remove**.
-

Where to Go Next

See [Chapter 3, “Configuring Security for the Cisco TelePresence Multipoint Switch”](#) to download your certificates and configure inter-device security on the CTMS.



CHAPTER 3

Configuring Security for the Cisco TelePresence Multipoint Switch

Revised: February, 2011, OL-18391-01



Tip

When performing the tasks in this chapter, it can be helpful to keep two browser sessions open, with one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Multipoint Switch (CTMS) administration interface.

Contents

This chapter describes how to configure inter-device security for the Cisco TelePresence Multipoint Switch and includes the following sections:

- [Cisco TelePresence Multipoint Switch Configuration Checklist, page 3-1](#)
- [Uploading Downloaded Security Certificates to CTMS, page 3-2](#)
- [Downloading LSCs on the CTMS, page 3-4](#)
- [Creating a SIP Trunk Security Profile, page 3-6](#)
- [Configuring the SIP Security Trunk, page 3-8](#)
- [Configuring the CTMS for SIP Security, page 3-11](#)
- [Removing Security from the Cisco TelePresence Multipoint Switch, page 3-12](#)
- [Understanding Encrypted Key Transport \(EKT\) and CTMS Secure Communications, page 3-13](#)
- [Where to Go Next, page 3-16](#)

Cisco TelePresence Multipoint Switch Configuration Checklist

CTMS supports secure communication between Cisco TelePresence devices using Certificate Authority Proxy Function (CAPF). Each Cisco TelePresence product downloads a Locally Significant Certificate (LSC) from a CAPF server; communication between devices is then authenticated using LSCs, Cisco Unified Communications Manager (Cisco Unified CM) Root Certificates, and a CAPF Root Certificate.

[Table 3-1](#) provides a list of configuration tasks that you perform to configure inter-device security for the CTMS for the first time.

Table 3-1 Cisco CTMS Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: <ul style="list-style-type: none"> • Activate the CAPF server. • Create the Certificate Trust List (CTL). 	<ul style="list-style-type: none"> • Chapter 1, “Activating the Certificate Authority Proxy Function Server” • Chapter 2, “Configuring the Cisco CTL Client”
Step 2	Upload the *.der certificate files to CTMS.	Uploading Downloaded Security Certificates to CTMS, page 3-2
Step 3	Download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the CTMS.	Downloading LSCs on the CTMS, page 3-4
Step 4	Create and configure the SIP security trunk	<ul style="list-style-type: none"> • Creating a SIP Trunk Security Profile, page 3-6 • Configuring the SIP Security Trunk, page 3-8
Step 5	Configure SIP security on the CTMS.	Configuring the CTMS for SIP Security, page 3-11
Step 6	(Optional) Remove the Standard CTI Secure Connection role from the default CTMS user.	Removing Security from the Cisco TelePresence Multipoint Switch, page 3-12

Uploading Downloaded Security Certificates to CTMS

To upload the *.der certificate files to CTMS, follow these steps.

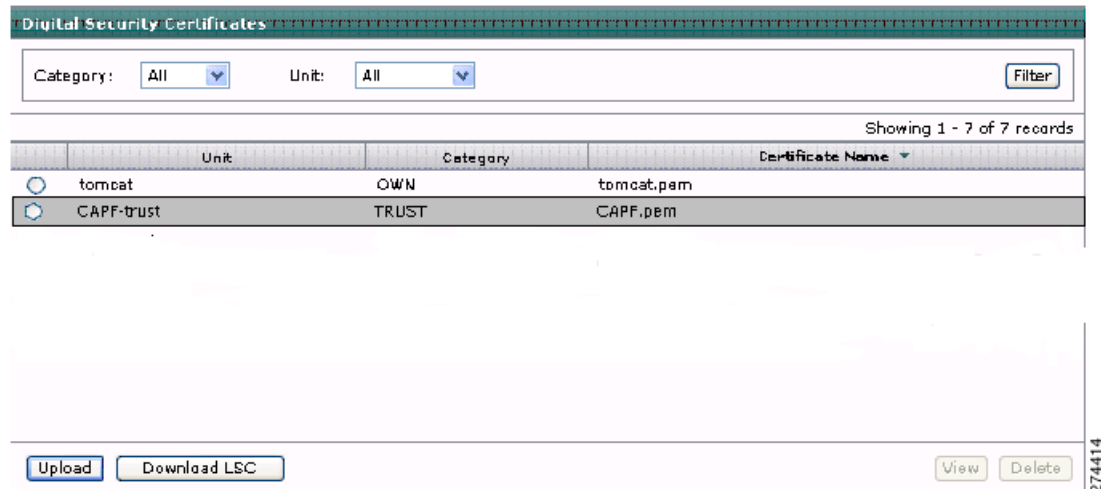
- Step 1** From the Cisco TelePresence Multipoint Switch administration interface, choose **System Configuration > Security Settings**.
- Step 2** Click **Upload**. The Certificate Upload window displays, as shown in [Figure 3-1](#).

Figure 3-1 Certificate Upload Window



- Step 3** Upload the CAPF.der file to CTMS by completing the following steps:
- From the Unit drop-down list, select **CAPF-trust**.
 - From the Category drop-down list, select **TRUST** (this is the default value).
 - Click the **Browse** button to upload a CAPF certificate.
 - Choose the CAPF.der that you downloaded to your local machine.
 - Click **Upload**. The CAPF.der file displays as a CAPF.pem file in the Digital Certificates Window, as shown in [Figure 3-2](#).

Figure 3-2 CAPF.pem (CAPF.der) File in Digital Certificates Window



- Step 4** Upload the CUCMx.der file from your local machine by completing the following steps:
- Return to the Security Settings window.
 - Click **Upload**.
 - After the Certificate Upload window displays, make sure that the following settings are present:
 - **CTM-TRUST** is selected in the Unit drop-down list
 - **TRUST** is selected in the Category drop-down list
 - Click the **Browse** button to upload the Cisco Unified CM root certificate.
 - Choose the CUCM0.der file that you downloaded to your local machine.
 - Click **Upload**. The CUCM0.der file displays as a CUCM0.pem file in the Digital Certificates Window.
 - If you have additional CUCMx.der files, upload each CUCMx.der file by completing Step a. through Step f.

After you complete the uploading of all *.der files, your window should look similar to the window in [Figure 3-3](#).

Figure 3-3 Digital Security Certificates Window Example

Digital Security Certificates

Category: All Unit: All Filter

Showing 1 - 7 of 7 records

	Unit	Category	Certificate Name
<input type="radio"/>	tomcat	OWN	tomcat.pem
<input type="radio"/>	CTM-trust	TRUST	CUCM2.pem
<input type="radio"/>	CTM-trust	TRUST	CUCM1.pem
<input type="radio"/>	CTM-trust	TRUST	CUCM0.pem
<input type="radio"/>	CAPF-trust	TRUST	CAPF.pem

274415

Downloading LSCs on the CTMS

Download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the CTMS. Use these LSCs to configure secure Session Initiation Protocol (SIP) trunks between Cisco Unified CM and the CTMS.

Before You Begin

You need the information that you created in previous steps in this section to download LSCs:

- CAPF Instance ID.
- CAPF authentication string.

In addition, you must have the following information:

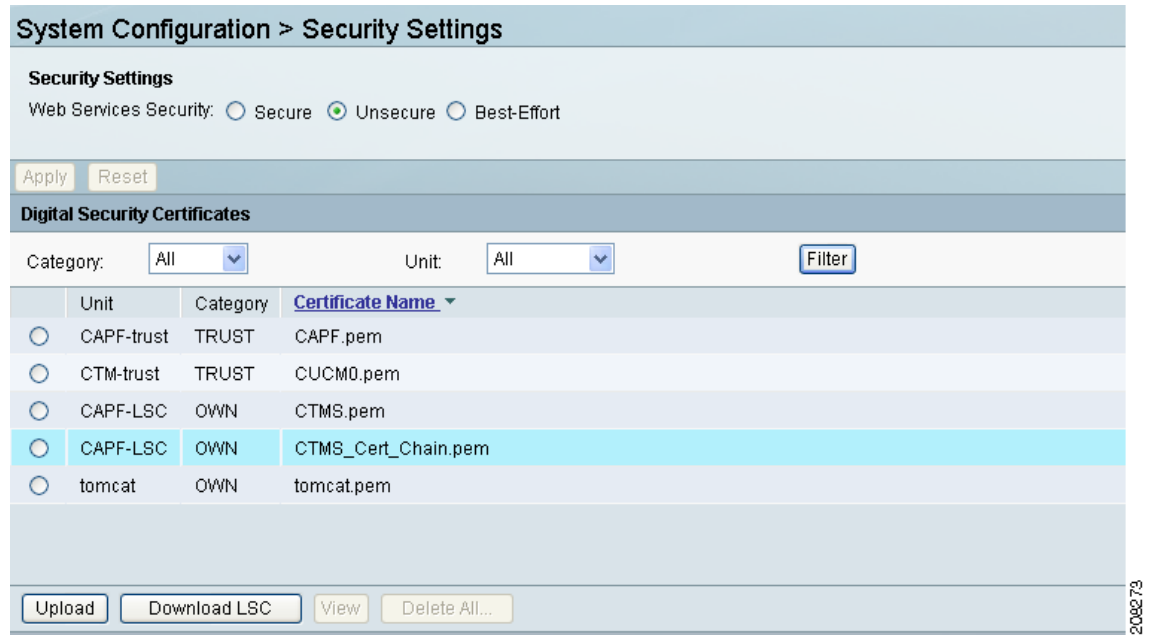
- The TFTP server IP address.
- The CAPF server IP address.

Procedure

To download LSCs, follow these steps:

-
- Step 1** From the Cisco TelePresence Multipoint Switch administration interface, choose **System Configuration > Security Settings**.
- Step 2** Click **Download LSC**. The Download CAPF LSC window appears, as shown in [Figure 3-3](#).

Figure 3-4 Download CAPF LSC Window



Step 3 Enter the following information in the fields:

- **CAPF Instance ID**—Enter the ID that you created in the [Chapter 1, “Creating a CAPF Profile for Cisco Unified CM”](#).
- **CAPF Auth. String**—Enter the string that you generated in the [“Creating a CAPF Profile for Cisco Unified CM”](#) section on page 1-6.
- **TFTP Server Host**—Enter the IP address of the TFTP server.



Note If your Cisco Unified CM Publisher is also configured as the TFTP server, use that IP address.

- **CAPF Server Port**—Leave the default value
- **CAPF Server Host**—Enter the IP address of the CAPF server



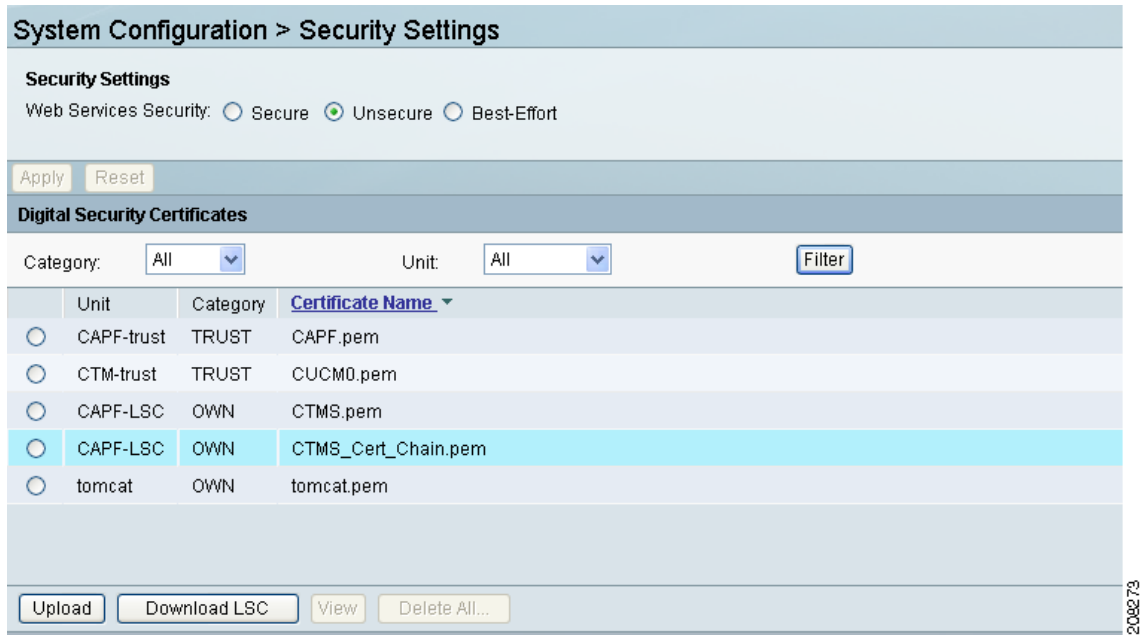
Note The CTMS automatically enters the IP address of the TFTP server in this field. If you use your Cisco Unified CM publisher as the TFTP server, use that default IP address.

Step 4 Click **Download LSC**.

Step 5 Click **OK** to confirm your choice. The CTMS creates the LSCs. The Digital Security Certificate window displays the LSC certificates that the CTMS created, as shown in [Figure 3-5](#):

- CTMS_Cert_Chain.pem
- CTMS.pem

Figure 3-5 Digital Security Certificate Window Displaying CTMS_Cert_Chain.pem and CTMS.pem Files



- Step 6** Obtain the SIP security trunk information by completing the following steps:
- Click the radio button for the CTMS.pem file.
 - Click the **View** button.
 - Note the information under Subject: in the file.

In the following example, you would note the subject name of **XXX-000**.

```
Version: V3
Subject: CN=XXX-000, O=cisco
Signature Algorithm: SHA1withRSA, OID = 0.0.000.000000.0.0.0
```

Creating a SIP Trunk Security Profile

To make the CTMS and Cisco Unified CM communication secure, create a secure SIP trunk. To create a SIP trunk security profile, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **System > Security Profile > SIP Trunk Security Profile**.
- Step 2** Click **Add New**. The SIP Trunk Security Profile Configuration window appears, as shown in [Figure 3-6](#).

Figure 3-6 Entering SIP Security Profile Information

SIP Trunk Security Profile Configuration

Save

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

Enable Application Level Authorization

Accept Presence Subscription

Accept Out-of-Dialog REFER

Accept Unsolicited Notification

Accept Replaces Header

Transmit Security Status

Done

274418

Step 3 Enter the following information in the fields:

- **Name**—Enter a unique name for the SIP trunk



Note Make a note of this name. You use it to configure the trunk in the [“Configuring the SIP Security Trunk”](#) section on page 3-8.

- **Description**—Enter a unique description for this SIP trunk
- **Device Security Mode**—Choose one of the following values:
 - For a secure connection, choose **Encrypted**.
 - Or
 - For a non secure connection, choose **Non Secure**.



Tip

Choose **Encrypted** for most situations. Choose **Non Secure** only for the following situations:

- You use another method to ensure secure communication between CTMS and Cisco Unified CM.
- You want audio and video (media) to be secure, but signaling between CTMS and Cisco Unified CM to be non-secure.

-
- **Incoming Transport Type**—Leave the default values:
 - Encrypted, choose **TLS**.
 - Non Secure, choose **TCP + UDP**.
 - **Outgoing Transport Type**—Choose one of the following values:
 - If you chose Encrypted for the device security, leave the default value **TLS**.
 - Or
 - If you chose Non Secure for the device security, choose either **TCP** or **UDP**.
 - **Enable Digest Authentication**—Leave this check box blank.
 - **X.509 Subject Name**—Enter the Subject Name (obtained when you download the LCS for CTMS. See [“Downloading LSCs on the CTMS” section on page 3-4](#)).
 - **Incoming Port**—Enter one of the following values:
 - If you chose Encrypted for the device security, enter a secure SIP port number (for example, **5061**)
 - Or
 - If you chose Non Secure for the device security, enter the non secure SIP port number **5060**.



Note Make a note of this port number. Use this port information when you configure the SIP trunk in the [“Configuring the CTMS for SIP Security” section on page 3-11](#).

- **Remaining check boxes**—Leave blank.

Step 4 Click **Save**.

Configuring the SIP Security Trunk

To configure the SIP security trunk between Cisco Unified CM and CTMS, complete one of the following:

- Configure security for an existing trunk, go to [“Configuring an Existing Trunk for SIP Security” section on page 3-9](#).
- Or
- Create a new trunk and configure security for that trunk, go to [“Creating and Configuring a New Trunk for SIP Security” section on page 3-9](#).

Configuring an Existing Trunk for SIP Security

To configure an existing trunk for SIP security, complete the following steps in the Cisco Unified CM administration interface:

-
- Step 1** Choose **Device > Trunk**.
- Step 2** Click **Find** to find the existing trunk.
- Step 3** In the Name column, click the hypertext link for the trunk that you want to configure. The Trunk Configuration window appears.
- Step 4** In the Device Information box (Cisco Unified CM Release 7.0 only), click the **SRTP Allowed** check-box to select it.
- Step 5** Enter the following in the SIP Information area:
- **Destination Trunk**—Enter the IP address for the CTMS.
 - **Destination Address is as SRV**—Leave unchecked.
 - **Destination Port**—Enter **5060** (default).



Note Do not change this port number. This is the listening port for CTMS communications, and you cannot change this port number in the CTMS.

- **Presence group**—Leave the default value
 - **SIP Trunk Security Profile**—Enter the name of the profile that you created in [Step 3](#) of the “[Configuring the CTMS for SIP Security](#)” section on page 3-11
 - **Rerouting Calling Search Space, Out-Of-Dialog Refer Calling Search Space, and SUBSCRIBE Calling Search Space**—Leave the default value (< None >).
 - **SIP Profile**—Choose **Standard SIP Profile**.
 - **DTMF Signaling Method**—Choose **No preference**.
- Step 6** Click **Save**.
-

Creating and Configuring a New Trunk for SIP Security

To create and configure an existing trunk for SIP security, complete the steps in the following sections:

- [Configuring a New Trunk in Cisco Unified CM, page 3-10](#)
- [Configuring the CTMS for SIP Security, page 3-11](#)

Configuring a New Trunk in Cisco Unified CM

To configure a new trunk in Cisco Unified CM, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **Device > Trunk**.
- Step 2** Click **Add New**. The Trunk Configuration window displays, as shown in [Figure 3-7](#).
- Step 3** Enter the following information in the Trunk Configuration area:
 - **Trunk Type**—Choose **SIP Trunk**
 - **Device Protocol**—Choose **SIP** (this is the default value).

Figure 3-7 Trunk Configuration Window

- Step 4** Click **Next**.
- Step 5** Enter the following in the Device Information area:
 - **Device Name**—Enter a name for the SIP trunk
 - **Description**—Enter a description for the SIP trunk
 - **Device pool**—Enter either **Default** or select a device pool from the drop-down list
 - **Common Device Configuration**—Choose a common device configuration or **None** (this is the default value)
 - **Call Classification**—Choose a call classification or select **Use System Default** (this is the default value)
 - **Media Resource Group List**—Choose a media resource group list or **None** (this is the default value)
 - **Location**—Choose a location
 - **AAR group**—Choose an AAR group or **None** (this is the default value)
 - **Packet capture mode**—Choose **None** (this is the default value)
 - **Packet capture duration**—Enter **0** (this is the default value)
 - **SRTP Allowed** (Cisco Unified CM release 7.0 only)—Check this box to enable SRTP for secure trunks.



Note You must check the SRTP Allowed check box to make sure that the trunk is secure.

- Step 6** Enter the following in the SIP Information area:
- **Destination Trunk**—Enter the IP address for CTMS.
 - **Destination Address is as SRV**—Leave unchecked.
 - **Destination Port**—Enter **5060** (default).



Note Do not change this port number. This is the listening port for CTMS communications, and you cannot change this port number in the CTMS.

- **Presence group**—Choose **Standard Presence Group**
 - **SIP Trunk Security Profile**—Enter the name of the profile that you created in [Step 3](#) of the “[Configuring the CTMS for SIP Security](#)” section on page 3-11.
 - **Rerouting Calling Search Space, Out-Of-Dialog Refer Calling Search Space, and SUBSCRIBE Calling Search Space**—Leave the default value (< None >).
 - **SIP Profile**—Choose **Standard SIP Profile**.
 - **DTMF Signaling Method**—Choose **No preference**.
- Step 7** Click **Save**.
-

Configuring the CTMS for SIP Security

To configure SIP security on the CTMS, follow these steps:

-
- Step 1** From the Cisco TelePresence Multipoint Switch administration interface, choose **System Configuration > Cisco Unified CM**.
- Step 2** Enter the following information in the Cisco Unified CM tab using [Figure 3-8](#) as an example:
- **Cisco Unified CM1**—Enter the IP address or host name of the Cisco Unified CM server.
 - **SIP Port**—Enter the SIP port number that you entered in Step 3 of the “[Configuring the CTMS for SIP Security](#)” section on page 3-11. If you have a non-secure trunk, enter the non-secure port number **5060**.
 - **Cisco Unified CM2, CM3, CM4, and CM5**—Enter the IP address or host name of any additional Cisco Unified CM servers. For each server, enter the secure SIP port number that you entered in Step 3 of the “[Configuring the CTMS for SIP Security](#)” section on page 3-11.

Figure 3-8 Cisco Unified CM Settings Example—CTMS Cisco Unified CM Tab

Unified CM		SIP Profile Settings
Unified CM1:	10.10.10.10	*
SIP Port:	5066	*
Unified CM2:	10.10.10.10	
SIP Port:	5066	
Unified CM3:		
SIP Port:		
Unified CM4:		

- Step 3** Click **Apply** to save your configuration.
- Step 4** Click the **SIP Settings Profile** tab.
- Step 5** In the Device Security drop-down list, choose one of the following selections:
- If you chose Encrypted for your SIP trunk profile, device security, choose one of the following:
 - If your system uses Cisco Unified CM release 6.1.x, select **Encrypted without SDP keys**.
 - Or
 - If your system uses For Cisco Unified CM release 7.0, select **Encrypted with SDP keys**.
 - If you chose Non Secure for your SIP trunk profile, choose one of the following:
 - Choose **Non-Secure**.
 - Or
 - Check the **Media Encryption** check box to the right of the Device Security drop-down list.
- Step 6** Click **Apply** to save your changes.

Removing Security from the Cisco TelePresence Multipoint Switch



Note

This task requires that you maintain one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Multipoint Switch (CTMS) administration interface

To remove the Standard CTI Secure Connection role from the default CTMS user, complete the following steps:

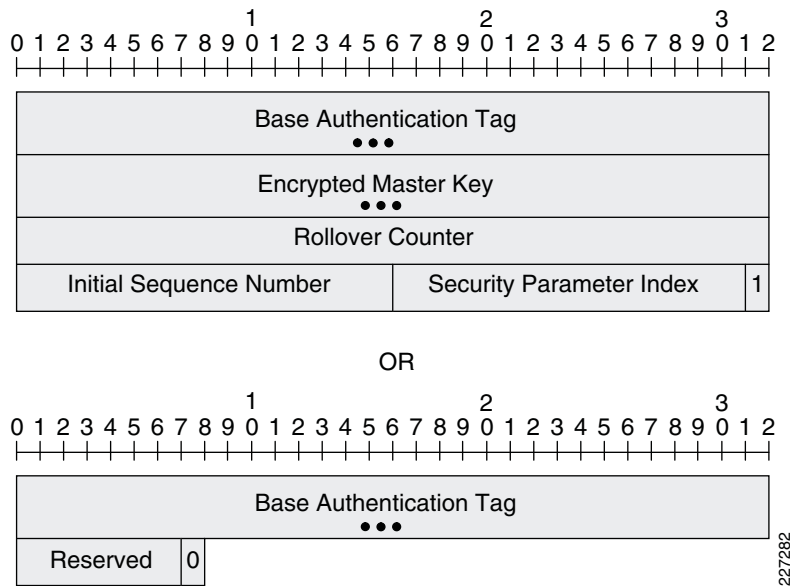
- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User**.
- a. Click the **Find** button and locate the default CTMS user.
 - b. Click the hypertext link to select that user.
 - c. In the Roles pane, click the Standard CTI Secure Connection role to highlight it.
 - d. Click **Remove from User Group**.

- Step 2** From the Cisco TelePresence Multipoint Switch administration interface, choose **System Configuration > Cisco Unified CM**.
- Click the **SIP Profile Settings** Tab.
 - From the Device Security drop-down list, choose **Non-Secure**.
 - Choose **System Configuration > Security Settings**.
 - Click the **Delete All** button to delete all security certificates. CTMS restarts and deletes all security certificates.

Understanding Encrypted Key Transport (EKT) and CTMS Secure Communications

EKT is an extension to SRTP which provides for the transport of SRTP master keys securely within SRTP and SRTCP packets. EKT accomplishes this by sub-dividing the SRTP and/or SRTCP Authentication Tag into one of the two formats shown in [Figure 9](#).

Figure 9 Encrypted Key Transport (EKT) Packet Formats



In the first (long) format, the final bit of the Authentication Tag is set to 1. This indicates the presence of the following fields:

- Base Authentication Tag**—Configured length field used to hold the message authentication data for the RTP or RTCP header and payload for the particular packet.
- Encrypted Master Key**—Variable length field which contains the encrypted SRTP master key corresponding to the SSRC within the SRTP or SRTCP packet.

- **Rollover Counter**—32-bit field used to hold the value of the SRTP rollover counter associated with the SSRC contained within the SRTP or SRTCP packet. Since the RTP sequence number is only a 16-bit long field, the rollover counter is necessary for codecs to maintain synchronization and minimize re-keying in long term media streams.
- **Initial Sequence Number**—Indicates the RTP sequence number of the first RTP packet which will be protected by the SRTP master key contained within the Encrypted Master Key field of this SRTP or SRTCP packet.
- **Security Parameter Index**—16-bit field similar to the IPsec SPI. It is used to identify a particular security context (Key Encrypting Key (KEK) used to produce the Encrypted Master Key, KEK cipher, SRTP cipher, SRTP master salt, etc.) corresponding to a particular SRTP flow.

In the second (short) format, the final bit of the Authentication Tag is set to 0. This indicates the presence of the following fields:

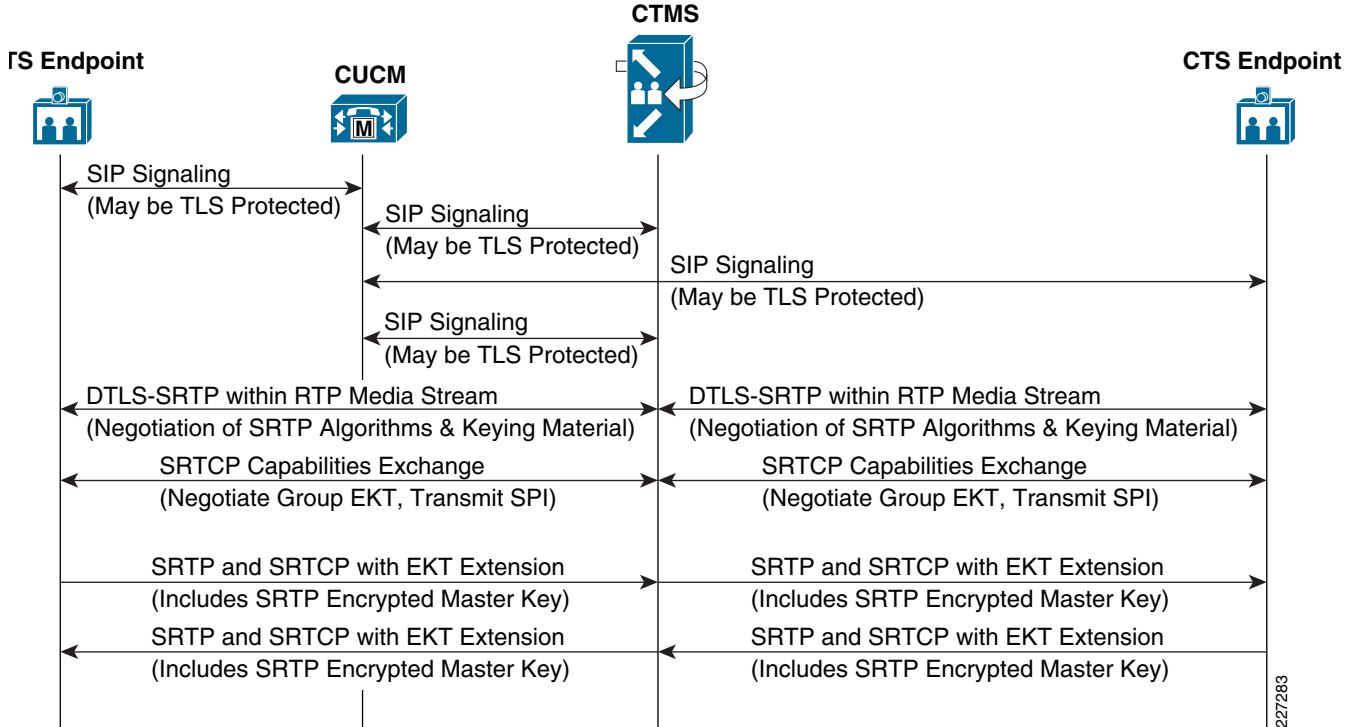
- **Base Authentication Tag**—Configurable length field used to hold the message authentication data for the RTP or RTCP header and payload for the particular packet.
- **Reserved**—7-bit field reserved for future use.

With EKT, the SRTP master key is distributed directly between CTS endpoints (CTS 3200s, CTS 3000s, CTS 1300s, CTS 1000s, and CTS 500s) in a multipoint call by encrypting it with a Key Encrypting Key (KEK), and sending it within SRTP and SRTCP packets which contain the long format of the EKT extension shown in [Figure 9](#) above. This is done for each of the voice and video media streams. The following section provides a high-level overview of the key exchange process within a multipoint Cisco TelePresence call using DTLS-SRTP and EKT.

Cisco TelePresence Multipoint Call Operation

[Figure 10](#) shows the process that occurs for establishing a secure multipoint Cisco TelePresence meeting. [Figure 11](#) shows two CTS 1000 systems in a multipoint meeting via a CTMS. As with previous figures, only one set signaling and media has been shown for simplicity.

Figure 10 Multipoint Cisco TelePresence Key Exchange



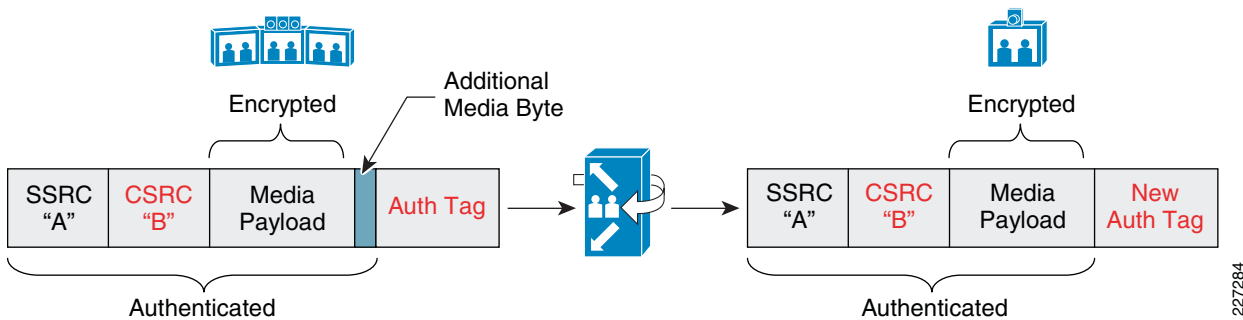
SIP signaling occurs first between the CTS endpoints and the Cisco Unified CM, as well as between the CTMS and the Cisco Unified CM. SIP establishes the RTP media streams and the RTCP control streams between the CTS endpoints and the CTMS. Immediately after the RTP media streams are set up, a DTLS-SRTP session is established over each media stream between the CTS endpoints and the CTMS. This is used to negotiate the SRTP encryption and authentication algorithms, as well as keying material. Following this, the CTS endpoints and the CTMS exchange SRTCP packets (using the SRTP keys established within DTLS) in order to discover their capabilities.

During this step the CTS endpoints discover that they are communicating with a CTMS, and that EKT is required for SRTP master key exchange between the CTS endpoints. EKT is necessary for SRTP master key exchange because the CTMS does not actually de-encrypt the SRTP media packets and re-encrypt them. Therefore, each CTS endpoint needs the SRTP master keys used to encrypt the media flows from each of the other CTS endpoints in order to decrypt the media. Also during this step, a group EKT parameter set is established. The group EKT parameter set includes the Key Encrypting Key (KEK), which will be used to encrypt the SRTP master keys sent within SRTCP and SRTP packets which include the long format of the EKT extension shown in Figure 9 above.

SRTP encrypted master keys are sent by the individual CTS endpoints to the CTMS via SRTCP Source Description (SDES) packets which contain the long format of the EKT extension. The CTMS will forward these packets to other CTS endpoints within the multipoint call. Additionally, for video streams, the first SRTP packet of each video frame contains the EKT extension with the SRTP encrypted master key. All other packets of the frame contain the shorter, second format of the EKT extension shown in Figure 9 above. For voice, every third RTP audio packet contains the EKT extension with the SRTP encrypted master key. The other audio RTP packets contain the shorter EKT extension. By forwarding these voice and audio SRTP EKT packets to the other CTS endpoints, the CTMS further guarantees that each endpoint acquires the SRTP encryption key for each transmitter.

Figure 11 shows a high-level example of the video media switching performed by the CTMS during a secure multipoint Cisco TelePresence meeting. The SRTP packet has been intentionally simplified for this example.

Figure 11 Media Switching in a Secure Multipoint Cisco TelePresence Meeting



Cisco TelePresence endpoints use the Contributing Source Identifier (CSRC) field to indicate the source camera or microphone position of the media stream, as well as the destination display or speaker of the media stream, as opposed to the Synchronization Source Identifier (SSRC) which was previously used. The CTMS may modify the CSRC value in cases such as when the video from CTS 3000 *right* camera needs to be displayed on the *right* display of a CTS 3000 and on the *center* display of a CTS 1000 within the same multipoint meeting. However, the SSRC value of the media packets is not modified, as they are switched through the CTMS.

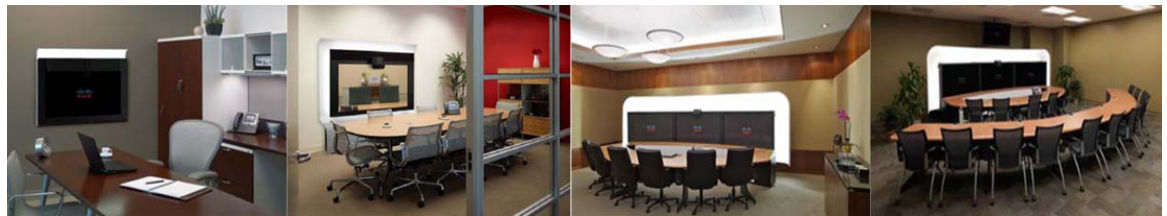
CTS endpoints also append an additional unencrypted byte to the payload of audio and video media packets before sending the packets to the CTMS. For audio packets, the additional byte is used to determine the level of audio energy within the packet. This is used by the CTMS to determine which CTS endpoints should be transmitting video streams. For video packets, the additional byte is used to determine if the video packet is the beginning of a new reference frame (IDR). For both the audio and video packets, the CTMS strips off the additional byte before forwarding it to the CTS endpoints.

Therefore, the CTMS does need to recompute the authentication tag as it switches the media, as shown in Figure 11 above. However, the CTMS does not decrypt and re-encrypt the actual media streams. This helps to ensure high performance and low delay of the CTMS even with encryption enabled on the multipoint call, as well as preserving the existing hardware investment of the CTMS.

For more information about EKT and Cisco TelePresence secure communications and signaling, see the [Design Zone for Video: Cisco TelePresence Secure Communications and Signaling Guide](#) on Cisco.com.

Where to Go Next

See Chapter 4, “Configuring Security for the Cisco TelePresence Recording Server” to configure inter-device security for the Cisco TelePresence Recording Server (CTRS).



CHAPTER 4

Configuring Security for the Cisco TelePresence Recording Server

Revised: September, 2010, OL-18391-01



Tip

When performing the tasks in this chapter, it can be helpful to keep two browser sessions open, with one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Recording Server (CTRS) administration interface.

Contents

This chapter describes how to configure inter-device security for the Cisco TelePresence Recording Server and includes the following sections:

- [Cisco TelePresence Recording Server Configuration Checklist, page 4-1](#)
- [Uploading the CAPF Root Certificate to the CTRS, page 4-2](#)
- [Downloading the Cisco Unified CM Root Certificate, page 4-3](#)
- [Uploading the Cisco Unified CM Root Certificate to the CTRS, page 4-4](#)
- [Downloading the LSC to the CTRS, page 4-4](#)
- [Setting the Default Security Level, page 4-5](#)
- [Configuring the SIP Security Trunk, page 4-6](#)
- [Configuring the CTRS for SIP Security, page 4-9](#)
- [Removing Security from the Cisco TelePresence Recording Server, page 4-10](#)
- [Where to Go Next, page 4-11](#)

Cisco TelePresence Recording Server Configuration Checklist

CTRS supports secure communication between Cisco TelePresence devices using Certificate Authority Proxy Function (CAPF). Each Cisco TelePresence product downloads a Locally Significant Certificate (LSC) from a CAPF server; communication between devices is then authenticated using LSCs, Cisco Unified Communications Manager (Cisco Unified CM) Root Certificates, and a CAPF Root Certificate.

Table 4-1 provides a list of configuration tasks that you perform to configure inter-device security for the CTRS for the first time.

Table 4-1 Cisco CTRS Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: <ul style="list-style-type: none"> • Activate the CAPF service. • Create the Certificate Trust List (CTL). 	<ul style="list-style-type: none"> • Chapter 1, “Activating the Certificate Authority Proxy Function Server” • Chapter 2, “Configuring the Cisco CTL Client”
Step 2	Upload the CAPF Root certificate.	Uploading the CAPF Root Certificate to the CTRS, page 4-2
Step 3	Download the Cisco Unified CM Root certificate.	Downloading the Cisco Unified CM Root Certificate, page 4-3
Step 4	Upload the Cisco Unified CM Root certificate.	Uploading the Cisco Unified CM Root Certificate to the CTRS, page 4-4
Step 5	Download the LSC.	Downloading the LSC to the CTRS, page 4-4
Step 6	Choose the default meeting security level.	Setting the Default Security Level, page 4-5
Step 7	Configure the SIP security trunk.	Configuring the SIP Security Trunk, page 4-6
Step 8	Configure SIP security.	Configuring the CTRS for SIP Security, page 4-9
Step 9	(Optional) Remove the Standard CTI Secure Connection role from the default CTRS user.	Removing Security from the Cisco TelePresence Recording Server, page 4-10

Uploading the CAPF Root Certificate to the CTRS

To upload the CAPF Root certificate to the CTRS, follow these steps:

-
- Step 1** Log in to the CTRS administration interface.
- Step 2** Choose **System Configuration > Security Settings**. The Security Settings window appears, as shown in [Figure 4-1](#).

Figure 4-1 System Configuration > Security Settings

System Configuration > Security Settings

Security Settings
Web Services Security: Secure Unsecure Best-Effort

Apply Reset

Digital Security Certificates

Category: All Unit: All Filter

	Unit	Category	Certificate Name
<input type="radio"/>	CAPF-trust	TRUST	CAPF.pem
<input type="radio"/>	CTM-trust	TRUST	CUCM0.pem
<input type="radio"/>	CAPF-LSC	OWN	CTMS.pem
<input checked="" type="radio"/>	CAPF-LSC	OWN	CTMS_Cert_Chain.pem
<input type="radio"/>	tomcat	OWN	tomcat.pem

Upload Download LSC View Delete All...

- Step 3** Click **Upload**, then select the following:
- Unit**—CAPF-Trust
 - Category**—TRUST
 - Certificate**—Choose the CAPF Root certificate that you downloaded from Cisco Unified CM (CAPF.der).
- Step 4** Click **Upload** to upload the CAPF Root certificate.
- Step 5** Proceed to [Downloading the Cisco Unified CM Root Certificate](#).

Downloading the Cisco Unified CM Root Certificate

To download the Cisco Unified CM Root certificate, follow these steps:

- Step 1** If you have not already done so, log in to the Cisco Unified CM administration interface.
- Step 2** In the Navigation area at the top right of the page, select **Cisco Unified OS Administration** from the drop-down menu and click **Go**.
- Step 3** Log in to the Cisco Unified Operating System administration interface and choose **Security > Certificate Management**.
- Step 4** Enter search criteria into the fields provided and click **Find** to display a list of certificates.
- Step 5** Find the Cisco Unified CM Root Certificate (for example, *.der), and select the hypertext link for that certificate.
- Step 6** Click **Download** and follow the download instructions.
- Step 7** Save the Cisco Unified CM Root Certificate for Publisher, for example CUCM0.der.



Note Names must be in the following format: CUCM#.der, where # is 0 for Publisher and 1 through 6 for Subscribers.

Step 8 Proceed to [Uploading the Cisco Unified CM Root Certificate to the CTRS](#).

Uploading the Cisco Unified CM Root Certificate to the CTRS

To upload the Cisco Unified CM Root certificate to the CTRS, follow these steps:

-
- Step 1** If you haven't already done so, log in to the CTRS administration interface.
- Step 2** From the **Security Settings** window, Click **Upload**.
- Step 3** Select the following:
- Unit**—CTM-Trust
 - Category**—TRUST
 - Certificate**—Choose the Cisco Unified CM root certificate that you created in Cisco Unified CM (CUCM0.der).
- Step 4** Click **Upload** to upload the Cisco Unified CM root certificate.
- Step 5** Proceed to [Downloading the LSC to the CTRS](#).
-

Downloading the LSC to the CTRS

After you have created the application user and application user CAPF profile, download the LSC to the CTRS by following these steps:

-
- Step 1** Click **Security Settings**. The Security Settings window appears, as shown in [Figure 4-2](#).

Figure 4-2 System Configuration > Security Settings

System Configuration > Security Settings

Security Settings
Web Services Security: Secure Unsecure Best-Effort

Apply Reset

Digital Security Certificates

Category: All Unit: All Filter

	Unit	Category	Certificate Name
<input type="radio"/>	CAPF-trust	TRUST	CAPF.pem
<input type="radio"/>	CTM-trust	TRUST	CUCM0.pem
<input type="radio"/>	CAPF-LSC	OWN	CTMS.pem
<input checked="" type="radio"/>	CAPF-LSC	OWN	CTMS_Cert_Chain.pem
<input type="radio"/>	tomcat	OWN	tomcat.pem

Upload Download LSC View Delete All...

- Step 2** Click **Download LSC** and fill out the following fields:
- **CAPF Instance ID**—Must match the instance ID created in Cisco Unified CM.
 - **CAPF Auth String**—Must match the authorization string created in Cisco Unified CM.
 - **TFTP Server Host**—Cisco Unified CM TFTP server.
 - **TFTP Server Port**—Must be 69 (default).
 - **CAPF Server Host**—Cisco Unified CM CAPF server host.
 - **CAPF Server Port**—Must be 3804 (default).
- d. Click **Download LSC**. After the LSC has been successfully downloaded, the CTRS reboots automatically.
- Step 3** Proceed to [Setting the Default Security Level](#).

Setting the Default Security Level

After the system reboots, choose the default meeting security level by following these steps in the CRTS administration interface:

- Step 1** Choose **System Configuration > Security**. The System Security screen appears, as shown in [Figure 4-1](#).
- Step 2** In the Web Services Security section at the top of the screen, select one of the following security levels:
- **Non-Secure**—Selected devices do not have to have valid Locally Significant Certificates (LSCs) from a Certificate Authority Proxy Function (CAPF) server.
 - **Secure**—Selected devices must have valid LSCs from a CAPF server.

- **Best Effort**—If a selected device has an LSC and others do not, the security level is Non-Secure.

Step 3 Click **Apply**.

Step 4 Set device security by doing the following:

- a. Choose **System Configuration > Unified CM**.
 - b. Select the **SIP Profile Settings** tab.
 - c. Choose one of the following Device Security encryption types:
 - **Encrypted without SDP Keys for 6.1.2 Cisco Unified CM**Or
 - **Encrypted with SDP Keys for 7.0 Cisco Unified CM**
-

Configuring the SIP Security Trunk

To configure the SIP security trunk between Cisco Unified CM and CTRS, complete one of the following:

- Configure security for an existing trunk, go to [“Configuring an Existing Trunk for SIP Security” section on page 4-7](#).
- Or
- Create a new trunk and configure security for that trunk, go to [“Creating and Configuring a New Trunk for SIP Security” section on page 4-7](#).

Configuring an Existing Trunk for SIP Security

To configure an existing trunk for SIP security, complete the following steps in the Cisco Unified CM administration interface:

-
- Step 1** Choose **Device > Trunk**.
- Step 2** Click **Find** to find the existing trunk.
- Step 3** In the Name column, click the hypertext link for the trunk that you want to configure. The Trunk Configuration window appears.
- Step 4** In the Device Information box (Cisco Unified CM Release 7.0 only), click the **SRTP Allowed** check-box to select it.
- Step 5** Enter the following in the SIP Information area:
- **Destination Trunk**—Enter the IP address for the CTRS.
 - **Destination Address is as SRV**—Leave unchecked.
 - **Destination Port**—Enter **5060** (default).



Note Do not change this port number. This is the listening port for CTRS communications, and you cannot change this port number in the CTRS.

- **Presence group**—Leave the default value
 - **SIP Trunk Security Profile**—Enter the name of the profile that you created in the [“Configuring the CTRS for SIP Security”](#) section on page 4-9.
 - **Rerouting Calling Search Space, Out-Of-Dialog Refer Calling Search Space, and SUBSCRIBE Calling Search Space**—Leave the default value (< None >).
 - **SIP Profile**—Choose **Standard SIP Profile**.
 - **DTMF Signaling Method**—Choose **No preference**.
- Step 6** Click **Save**.
-

Creating and Configuring a New Trunk for SIP Security

To create and configure an existing trunk for SIP security, complete the steps in the following sections:

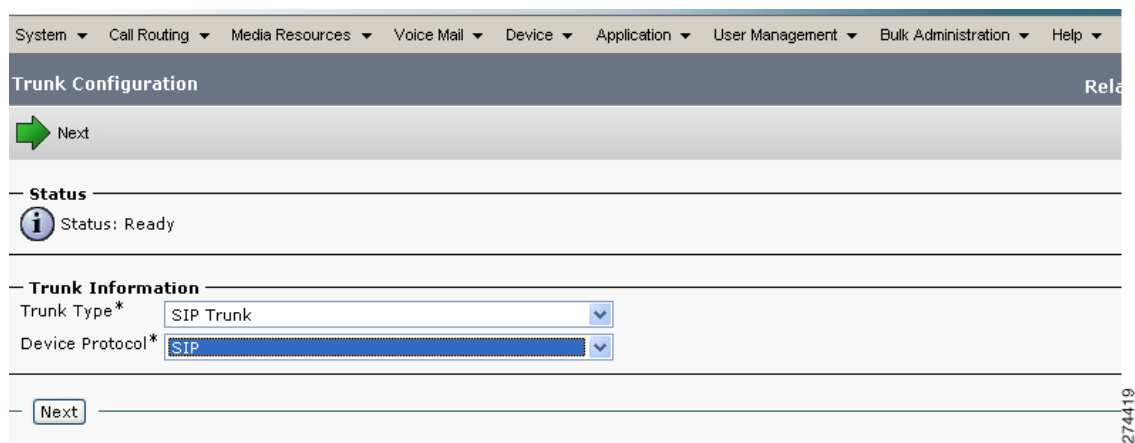
- [Configuring a New Trunk in Cisco Unified CM, page 4-8](#)
- [Configuring the CTMS for SIP Security, page 3-11](#)

Configuring a New Trunk in Cisco Unified CM

To configure a new trunk in Cisco Unified CM, follow these steps:

- Step 1** From the Cisco Unified CM administration interface, choose **Device > Trunk**.
- Step 2** Click **Add New**. The Trunk Configuration window displays, as shown in [Figure 4-3](#).
- Step 3** Enter the following information in the Trunk Configuration area:
 - **Trunk Type**—Choose **SIP Trunk**
 - **Device Protocol**—Choose **SIP** (this is the default value).

Figure 4-3 Trunk Configuration Window



- Step 4** Click **Next**.
- Step 5** Enter the following in the Device Information area:
 - **Device Name**—Enter a name for the SIP trunk
 - **Description**—Enter a description for the SIP trunk
 - **Device pool**—Enter either **Default** or select a device pool from the drop-down list
 - **Common Device Configuration**—Choose a common device configuration or **None** (this is the default value)
 - **Call Classification**—Choose a call classification or select **Use System Default** (this is the default value)
 - **Media Resource Group List**—Choose a media resource group list or **None** (this is the default value)
 - **Location**—Choose a location
 - **AAR group**—Choose an AAR group or **None** (this is the default value)
 - **Packet capture mode**—Choose **None** (this is the default value)
 - **Packet capture duration**—Enter **0** (this is the default value)
 - **SRTP Allowed** (Cisco Unified CM release 7.0 only)—Check this box to enable SRTP for secure trunks.



Note You must check the SRTP Allowed check box to make sure that the trunk is secure.

Step 6 Enter the following in the SIP Information area:

- **Destination Trunk**—Enter the IP address for CTRS.
- **Destination Address is as SRV**—Leave unchecked.
- **Destination Port**—Enter **5060** (default).



Note Do not change this port number. This is the listening port for CTRS communications, and you cannot change this port number in the CTRS.

- **Presence group**—Choose **Standard Presence Group**
- **SIP Trunk Security Profile**—Enter the name of the profile that you created in the [“Configuring the CTRS for SIP Security”](#) section on page 4-9.
- **Rerouting Calling Search Space, Out-Of-Dialog Refer Calling Search Space, and SUBSCRIBE Calling Search Space**—Leave the default value (< None >).
- **SIP Profile**—Choose **Standard SIP Profile**.
- **DTMF Signaling Method**—Choose **No preference**.

Step 7 Click **Save**.

Configuring the CTRS for SIP Security

To configure SIP security on the CTRS, follow these steps:

Step 1 From the Cisco TelePresence Recording Server administration interface, choose **System Configuration > Cisco Unified CM**.

Step 2 Enter the following information in the Cisco Unified CM tab using [Figure 4-4](#) as an example:

- **Cisco Unified CM1**—Enter the IP address or host name of the Cisco Unified CM server.
- **SIP Port**—Enter the SIP port number that you entered in Step 3 of the [“Configuring the CTRS for SIP Security”](#) section on page 4-9. If you have a non-secure trunk, enter the non-secure port number **5060**.
- **Cisco Unified CM2, CM3, CM4, and CM5**—Enter the IP address or host name of any additional Cisco Unified CM servers. For each server, enter the secure SIP port number that you entered in Step 3 of the [“Configuring the CTRS for SIP Security”](#) section on page 4-9.

Figure 4-4 Cisco Unified CM Settings Example—CTRS Cisco Unified CM Tab

Unified CM		SIP Profile Settings	
Unified CM1:	10.10.10.10	*	
SIP Port:	5066	*	
Unified CM2:	10.10.10.10		
SIP Port:	5066		
Unified CM3:			
SIP Port:			
Unified CM4:			

Step 3 Click **Apply** to save your configuration.

Step 4 Click the **SIP Settings Profile** tab.

Step 5 In the Device Security drop-down list, choose one of the following selections:

- If you chose Encrypted for your SIP trunk profile, device security, choose one of the following:
 - If your system uses Cisco Unified CM release 6.1.x, select **Encrypted without SDP keys**.
 - Or
 - If your system uses For Cisco Unified CM release 7.0, select **Encrypted with SDP keys**.
- If you chose Non Secure for your SIP trunk profile, choose one of the following:
 - Choose **Non-Secure**.
 - Or
 - Check the **Media Encryption** check box to the right of the Device Security drop-down list.

Step 6 Click **Apply** to save your changes.

Removing Security from the Cisco TelePresence Recording Server



Note

This task requires that you maintain one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Recording Server (CTRS) administration interface.

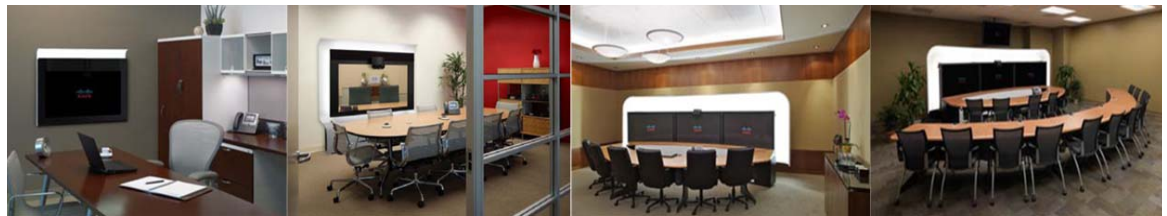
To remove the Standard CTI Secure Connection role from the default CTRS user, complete the following steps:

- Step 1** From the Cisco Unified CM administration interface, choose **User Management > Application User**.
- a. Click the **Find** button and locate the default CTRS user.
 - b. Click the hypertext link to select that user.
 - c. In the Roles pane, click the Standard CTI Secure Connection role to highlight it.
 - d. Click **Remove from User Group**.

- Step 2** From the Cisco TelePresence Recording Server administration interface, choose **System Configuration > Cisco Unified CM**.
- a. Click the **SIP Profile Settings** Tab.
 - b. From the Device Security drop-down list, choose **Non-Secure**.
 - c. Choose **System Configuration > Security Settings**.
 - d. Click the **Delete All** button to delete all security certificates. CTRS restarts and deletes all security certificates.
-

Where to Go Next

See [Chapter 5, “Configuring Security for Cisco TelePresence Manager”](#) to configure inter-device security for Cisco TelePresence Manager.



CHAPTER 5

Configuring Security for Cisco TelePresence Manager

Revised: September, 2010, OL-18391-01



Tip

When performing the tasks in this chapter, it can be helpful to keep two browser sessions open, with one session logged in to the Cisco Unified CM administration interface and one session logged in to the Cisco TelePresence Manager administration interface.

Contents

This chapter describes how to configure inter-device security for Cisco TelePresence Manager and includes the following sections:

- [Cisco TelePresence Manager Configuration Checklist, page 5-1](#)
- [Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications, page 5-2](#)
- [Uploading Downloaded Security Certificates to Cisco TelePresence Manager, page 5-4](#)
- [Downloading LSCs to Cisco TelePresence Manager, page 5-5](#)
- [Removing Security from Cisco TelePresence Manager, page 5-6](#)
- [Where to Go Next, page 5-7](#)

Cisco TelePresence Manager Configuration Checklist

CTS-Manager supports secure communication between Cisco TelePresence devices using Certificate Authority Proxy Function (CAPF). Each Cisco TelePresence product downloads a Locally Significant Certificate (LSC) from a CAPF server; communication between devices is then authenticated using LSCs, Cisco Unified Communications Manager (Cisco Unified CM) Root Certificates, and a CAPF Root Certificate.

[Table 5-1](#) provides a list of configuration tasks that you perform to configure inter-device security for the CTS-Manager for the first time.

Table 5-1 Cisco CTL Client Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: <ul style="list-style-type: none"> • Activate the CAPF server. • Create the Certificate Trust List (CTL). • Download the CAPF.der file. 	<ul style="list-style-type: none"> • Chapter 1, “Activating the Certificate Authority Proxy Function Server” • Chapter 2, “Configuring the Cisco CTL Client” • Downloading Certificates from Cisco Unified CM, page 1-9
Step 2	Configure Cisco Unified CM for secure communications with Cisco TelePresence Manager.	Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications, page 5-2
Step 3	Upload the *.der certificate files to CTS-Manager.	Uploading Downloaded Security Certificates to Cisco TelePresence Manager, page 5-4
Step 4	Download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the CTS-Manager.	Downloading LSCs to Cisco TelePresence Manager, page 5-5
Step 5	(Optional) Remove the Standard CTI Secure Connection role from the default CTS-Manager user.	Removing Security from Cisco TelePresence Manager, page 5-6

Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications

To configure Cisco Unified CM for secure communications with Cisco TelePresence Manager, follow these steps:

-
- Step 1** Log in to the Cisco Unified CM administration interface.
- Step 2** Assign the Standard CTI Secure Connection role to the Cisco TelePresence Manager application user by completing the following steps:
- From the Cisco Unified CM administration interface, choose **User Management > Application User**.
 - Find the Cisco TelePresence Manager application user by clicking the **Find** button, locating the user ID, and clicking the hypertext link to select that user.
 - Click **Add to User Group**.
 - Check the check box next to Standard CTI Secure Connection.
 - Click **Add Selected**. Cisco Unified CM automatically adds the information that you choose in the Groups field to the Roles field.
- Step 3** To add a CAPF profile for the Cisco TelePresence Choose **User Management > Application User CAPF Profile**.
- Step 4** Click the **Add New** button. The CAPF Profile window appears, as shown in [Figure 5-1](#).

Figure 5-1 Configuring the CAPF Profile with an Existing User ID and Unique Instance ID

Step 5 Enter the following information in the fields:

- **Application User**—From the drop-down list, select the Cisco TelePresence Manager application user ID.
- **Instance Id**—Enter a unique string for Cisco TelePresence Manager.



Note Make a note of the Instance ID that you create. You use this information later in this chapter.

- **Certificate Operation**—Choose **Install//Upgrade**.
- **Authentication Mode**—Choose **By Authentication String** (default).
- **Authentication String**—Click this text box, then click the **Generate String** button to create an authentication string.



Note Make a note of the authentication string. You use this information later in this chapter.

- **Key size (Bits)**—Choose 1024 (default).
- **Operation Completes By**—Leave the default value.



Note To avoid regenerating a new authentication string, complete the procedure in the [“Downloading LSCs to Cisco TelePresence Manager”](#) section on page 5-5 before the date and time that is specified in the Operation Completes By field.

Step 6 Click **Save**.

Uploading Downloaded Security Certificates to Cisco TelePresence Manager

To upload the *.der files to Cisco TelePresence Manager, follow these steps.

- Step 1** From the Cisco TelePresence Manager administration interface, choose **System Information > System Configuration > Security Settings**.
- Step 2** Click **Upload**. The Certificate Upload window appears, as shown in [Figure 5-2](#).

Figure 5-2 Certificate Upload Window

- Step 3** Upload the CAPF.der file to Cisco TelePresence Manager by completing the following steps:
- From the Unit drop-down list, select **CAPF-trust**.
 - From the Category drop-down list, select **TRUST** (default).
 - Click the **Browse** button to upload a CAPF certificate.
 - Choose the CAPF.der that you downloaded to your local machine.
 - Click **Upload**. The CAPF.der file displays as a CAPF.pem file in the Digital Certificates Window, as shown in [Figure 5-3](#).

Figure 5-3 CAPF.pem (CAPF.der) File in Digital Certificates Window

	Unit	Category	Certificate Name
<input type="radio"/>	tomcat	OWN	tomcat.pem
<input checked="" type="radio"/>	CAPF-trust	TRUST	CAPF.pem

Downloading LSCs to Cisco TelePresence Manager

Download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the Cisco TelePresence Manager.

Before You Begin

You need the information that you created in previous steps in this section to download LSCs:

- CAPF Instance ID.
- CAPF authentication string.

In addition, you must have the following information:

- The TFTP server IP address.
- The CAPF server IP address.

Procedure

To download LSCs, follow these steps:

- Step 1** From the Cisco TelePresence Manager administration interface, choose **System Information > System Configuration > Security Settings**.
- Step 2** Click the **Download LSC** button. The Download CAPF LSC window appears, as shown in [Figure 5-4](#).

Figure 5-4 Download CAPF LSC Window

Unified CM:	tsbu-domino-ccm1
CAPF Instance ID:	
CAPF Auth. String:	
TFTP Server Host:	
TFTP Server Port:	69
CAPF Server Host:	
CAPF Server Port:	3804
Certificate Install Directory:	/usr/local/ctis/.security/certs/capf-lsc/

Download LSC Close



Note

CTS-Manager supports multiple Cisco Unified CMs.

Step 3 Enter the following information in the fields:

- **CAPF Instance ID**—Enter the ID that you obtained in the “Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications” section on page 5-2.
- **CAPF Auth. String**—Enter the string that you obtained in the “Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications” section on page 5-2.
- **TFTP Server Host**—Enter the IP address of the TFTP server.



Note If your Cisco Unified CM server is configured as the TFTP server, use the IP address of the Cisco Unified CM that is configured as the publisher.

- **CAPF Server Port**—Leave the default value.
- **CAPF Server Host**—Enter the IP address of the CAPF server.



Note If you use your Cisco Unified CM publisher as the TFTP server, Cisco TelePresence Manager automatically enters the IP address of the publisher Cisco Unified CM in this field.

Step 4 Click **Download LSC**.

Step 5 Click **OK** to confirm your choice.

Cisco TelePresence Manager creates the LSCs and restarts the system. The Digital Security Certificate window displays the LSC certificates that Cisco TelePresence Manager created:

- CTSMAN.pem
- CAPF.pem

Step 6 Select the **Secure** radio button on the top of the screen and click **Apply**.

Removing Security from Cisco TelePresence Manager

To remove security from Cisco TelePresence Manager, follow these steps:

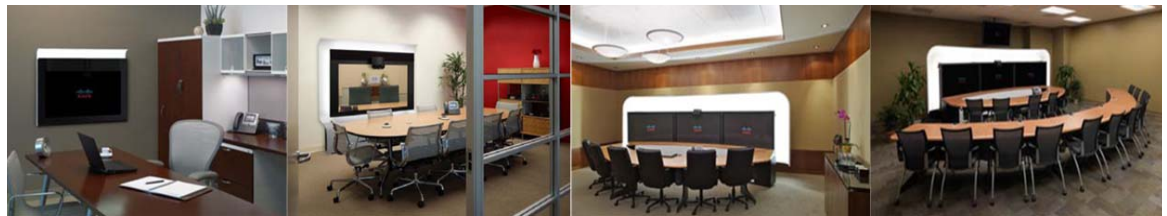
Step 1 Remove the Cisco CTI Secure role from the Cisco TelePresence Manager application user by completing the following steps:

- Log in to the Cisco Unified CM administration interface.
- Locate the existing Cisco TelePresence Manager application user by clicking the **Find** button.
- Locate the user ID and click the hypertext link to select that user.
- In the Roles pane, click the Standard CTI Secure Connection role to highlight it.
- Click **Remove from User Group**.

- Step 2** Remove the security configuration from Cisco TelePresence Manager by completing the following steps:
- a. Log in to the Cisco TelePresence Manager administration interface.
 - b. Choose **System Information > System Configuration > Security Settings**.
 - c. In the Web Security Settings area, click the **Unsecure** radio button.
 - d. Click **Apply**. Cisco TelePresence Manager restarts and deletes the CAPF security certificates.
-

Where to Go Next

See [Chapter 6, “Configuring and Verifying Cisco TelePresence Security”](#) to configure inter-device security in Cisco Unified CM.



CHAPTER 6

Configuring and Verifying Cisco TelePresence Security

Revised: September, 2010, OL-18391-01

Contents

This chapter describes how to configure inter-device security for the Cisco TelePresence System and includes the following sections:

- [Cisco TelePresence Security Configuration Checklist, page 6-1](#)
- [Configuring Cisco TelePresence Phone Profile Security, page 6-2](#)
- [Adding Authentication Information to the Cisco TelePresence System, page 6-3](#)
- [Verifying Security Status, page 6-4](#)
- [Where to Go Next, page 6-5](#)

Cisco TelePresence Security Configuration Checklist

[Table 6-1](#) provides a list of configuration tasks that you perform to configure and verify inter-device security.

Table 6-1 *Cisco TelePresence Security Configuration Checklist*

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: <ul style="list-style-type: none"> • Activate the CAPF server. • Create the Certificate Trust List (CTL). • Download the CAPF.der file. 	<ul style="list-style-type: none"> • Chapter 1, “Activating the Certificate Authority Proxy Function Server” • Chapter 2, “Configuring the Cisco CTL Client” • Downloading Certificates from Cisco Unified CM, page 1-9
Step 2	Create a phone security profile.	Configuring Cisco TelePresence Phone Profile Security, page 6-2

Table 6-1 Cisco TelePresence Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Add authentication information to the Cisco TelePresence System.	Adding Authentication Information to the Cisco TelePresence System, page 6-3
Step 4	Verify security status.	<ul style="list-style-type: none"> • Verifying Security Status Between the Cisco TelePresence System and Cisco TelePresence Manager, page 6-4 • Verifying Security Status Between the CTMS and Cisco TelePresence Manager, page 6-4

Configuring Cisco TelePresence Phone Profile Security

To configure the Cisco TelePresence phone security profile, follow these steps:

-
- Step 1** Log in to Cisco Unified CM administration interface.
- Step 2** Create the phone security profile by following these steps:
- Choose **System > Security Profile > Phone Security Profile**.
 - Click the **Add New** button. The Phone Security Profile Configuration window appears.
 - In the Phone Security Profile Type drop-down list, specify the type of Cisco TelePresence system that you are configuring. For example, Cisco 7975.
 - Click **Next**.
 - In the Select the phone security profile protocol drop-down list, select **SIP** and click **Next**.
 - Enter the following information in the Phone Security Profile Information box:
 - **Name**—Enter a unique name for the profile. For example, **CTS_3000_encrypted**
 - **Description**—Enter descriptive information for the profile.
 - **Nonce Validity Time**—Leave the default value of **600**.
 - **Device Security Mode**—Choose **Encrypted**.
 - **Transport Type**—Choose **TLS** (default).
 - **Enable Digest Authentication**—Unchecked.
 - **TFTP Encrypted Config**—Unchecked.
 - **Exclude Digest Credentials in Configuration File**—Unchecked.
 - Enter the following information in the Phone Security Profile CAPF Information box:
 - **Authentication Mode**—Choose **By Authentication String**.
 - **Key Size (Bits)**—Choose **1024** (default).
 - Enter the following information in the Parameters used in Phone box:
 - **SIP Phone Port**—Enter **5060** (default).
 - **Operation Completes B**—Leave the default value.
- Step 3** Click **Save**.

- Step 4** Add the security Profile to the Cisco TelePresence System by completing the following steps:
- Choose **Device > Phone**.
 - Click **Find** to find the existing Cisco TelePresence device that you want to configure.
 - In the Device Name (Line) column, click the hypertext link for the Cisco TelePresence device that you want to configure. The Phone Configuration window appears.
 - Scroll down to the Protocol Specific Information box and locate the Device Security drop-down list.
 - In the Device Security Profile drop-down list, choose the security profile that you created in [Step 2](#).
For example, if you named the device profile **CTS_3000_encrypted**, choose **CTS_3000_encrypted** in the drop-down list.
 - Change the following settings in the Certification Authority Proxy Function (CAPF) Information box:
 - Certificate Operation—Choose **Install/Upgrade**.
 - Authentication Mode—Choose **By Authentication String**.
 - Key Size (Bits)—Choose **1024** default).
 - Click **Generate String** to generate a unique string.



Note Make a note of the string that was generated, you use this string in the [“Adding Authentication Information to the Cisco TelePresence System”](#) section on page 6-3.

- Step 5** Click **Save** to save your settings.
-

Adding Authentication Information to the Cisco TelePresence System

To add authentication information to the Cisco TelePresence System, follow these steps:

- Step 1** Log in to the Cisco TelePresence System administration interface.
- Step 2** Choose **Device Information > Configuration > Cisco Unified CM Settings**.
- Step 3** In the CAPF Authentication String field, enter the authentication string that you generated in the [“Configuring Cisco TelePresence Phone Profile Security”](#) section on page 6-2.
- Step 4** Click **Apply** to apply your changes.
-

Verifying Security Status

This section describes how to verify security status and includes the following sections:

- [Verifying Security Status Between the Cisco TelePresence System and Cisco TelePresence Manager, page 6-4](#)
- [Verifying Security Status Between the CTMS and Cisco TelePresence Manager, page 6-4](#)

Verifying Security Status Between the Cisco TelePresence System and Cisco TelePresence Manager

To verify the security status between the Cisco TelePresence system and Cisco TelePresence Manager, follow these steps:

-
- Step 1** Log in to the Cisco TelePresence Manager administration interface.
- Step 2** Choose **System Information > Support > Rooms**.
- Step 3** Click the **Capability** tab.
- Step 4** Observe the icon that displays in the Web Services Security column:
- An icon of a closed lock (media is encrypted) indicates that communication between the Cisco TelePresence System and Cisco TelePresence Manager is secure.
 - An icon of an open lock indicates that communication between the Cisco TelePresence System and Cisco TelePresence Manager is not secure.
-

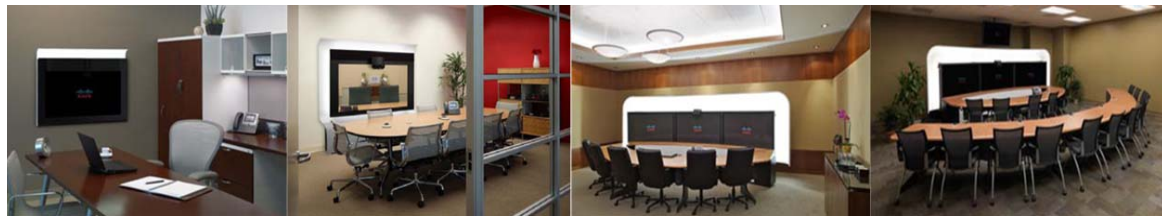
Verifying Security Status Between the CTMS and Cisco TelePresence Manager

To verify the security status between the CTMS and Cisco TelePresence Manager, follow these steps:

-
- Step 1** Log in to the Cisco TelePresence Manager administration interface.
- Step 2** Choose **System Information > Support > MCU Devices**.
- Step 3** Click the **Capability** tab.
- Step 4** View the icon that displays in the Web Services Security column.
- An icon of a lock that is locked indicates that communication between CTMS and Cisco TelePresence Manager is secure.
 - An icon of a lock that is unlocked indicates that communication between CTMS and Cisco TelePresence Manager is not secure.
-

Where to Go Next

See [Chapter 7, “Troubleshooting Security Configuration on the Cisco TelePresence System”](#) to manage security settings.



CHAPTER 7

Troubleshooting Security Configuration on the Cisco TelePresence System

Revised: September, 2010, OL-18391-01

Contents

This chapter describes how to troubleshoot security configuration on the Cisco TelePresence System and includes the following sections:

- [Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch, page 7-1](#)
- [Resetting Administrator and Security Passwords, page 7-3](#)
- [Where to Go Next, page 7-4](#)

Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch

The Cisco TelePresence Multipoint Switch (CTMS) generates log messages when it detects any of the following security configuration problems:

- Security negotiation between Cisco TelePresence elements could not be established or completed.
- Some elements of Cisco TelePresence are secure, while others are non-secure (this condition is known as a *security mismatch*).

To view the CTMS logs for security configuration, log in to the CTMS administration interface, choose **Troubleshooting > Log Files**, and view files with the file type of .properties.

[Table 7-1](#) contains system messages that you might encounter after setting up Cisco TelePresence security.

Table 7-1 Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch

Message Type	Possible Cause	Solution
Log Message Call in state=Connected, call id=x, conference id = xxxxxxxxxxx received error from Confmgr with error='security mismatch' during verification of security policy. Num=xxxxx	A non-secure Cisco TelePresence endpoint attempted to join a secure meeting.	Make sure that all Cisco TelePresence endpoints are secure before they join a secure meeting.
Log Message The security property of conference xxxxxxxxxxx does not allow endpoint xxxxx to join	One of the Cisco TelePresence endpoints is not running a Cisco TelePresence System software that is release 1.5 or higher. Cisco TelePresence treats the endpoint as a non-secure, even if this endpoint is configured as secure.	Make sure that all endpoints are running Cisco TelePresence System software with a minimum version of 1.5.
Log Message Conference Manager Conf Id xxxxxxxxxxx: will downgrade security from secure to non-secure. All existing endpoints will be downgraded to non-secure.	A non-secure Cisco TelePresence endpoint, an audio-only call that is added in, or an endpoint that is running Cisco TelePresence System software that is release 1.5 or lower has joined a Best-Effort meeting after a meeting has been started as secure.	No action is required, but be aware that the best-effort meeting is now non-secure.
Log Message Conf Id xxxxxxxxxxx: will start as non-secure	A non-secure Cisco TelePresence endpoint started a Best-Effort meeting.	No action is required, but be aware that the best-effort meeting is now non-secure.
Log Message Could not connect to Cisco Unified CM	The secure port numbers that are used by either CTMS, Cisco TelePresence Manager or the Cisco TelePresence system software do not match the port number for Cisco Unified CM.	Check the port numbers between the Cisco TelePresence elements to make sure that they match.
Log Message Dialing xxxxx received 403 Forbidden from Cisco Unified CM. Check SIP trunk config.	The Subject Names for the LSCs do not match.	Check the Subject Name that you created in the “Downloading LSCs on the CTMS” section on page 3-4 and make sure that it matches the Subject name in the “Configuring the CTMS for SIP Security” section on page 3-11
Log Message Dialing xxxxx received 488 Not Acceptable Here from Cisco Unified CM. Check SIP trunk config	The SRTP Allowed check box is not selected in the Cisco Unified CM configuration.	Follow the instructions in the “Configuring an Existing Trunk for SIP Security” section on page 3-9 and make sure that you check the SRTP Allowed check box.
Log Message TLS error: Error loading Private key file	The key file is from a different CTMS or Cisco Unified CM than the one that is being configured.	Make sure that the CTMS.key file being used is from the CTMS or Cisco Unified CM that is being configured.

Table 7-1 Troubleshooting Log Messages on the Cisco TelePresence Multipoint Switch (continued)

Message Type	Possible Cause	Solution
<p>Log Message TLS error: TLS connect failed because client side post-connection verification failed</p> <p>TLS error: TLS: didn't find matching cert</p>	The certificates from Cisco Unified CM are not valid.	Download new certificates by following the procedure in the “Downloading Certificates from Cisco Unified CM” section on page 1-9, then upload those certificates to CTMS by following the procedure in the “Uploading Downloaded Security Certificates to CTMS” section on page 3-2.
<p>Log Message Media Timeout occurred for call : called num = 13105</p>	Multiplexer negotiation has failed. One possible cause of this failure is that CTMS did not received an ACK message from the Cisco TelePresence System.	Recheck your security settings and the procedures you followed in Chapter 3, “Configuring Security for the Cisco TelePresence Multipoint Switch.”
<p>Log Message SPIMAP timeout, Dropping the call</p>	An ACK message for Group Security Parameters (GSPs) was not received by CTMS. The Cisco TelePresence System will either end the meeting or downgrade the meeting to non-secure.	Recheck your security settings and the procedures you followed in Chapter 3, “Configuring Security for the Cisco TelePresence Multipoint Switch.”
<p>Log Message “606 Not acceptable” message in the system log.</p>	The most likely cause of this error is that your system uses Cisco Unified CM release 6.1.x, but you selected Encrypted with SDP keys in the CTMS setup.	Check your Cisco Unified CM release. If your system is running Cisco Unified CM release 6.1.x, complete the steps in the “Creating and Configuring a New Trunk for SIP Security” section on page 3-9, and in the “Configuring the CTMS for SIP Security” section on page 3-11, select Encrypted without SDP keys .

Resetting Administrator and Security Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords in Cisco Unified CM.

To perform the password reset process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot reset a password when connected to the system through a secure shell session.



Caution

The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.



Caution

You must reset each server in a cluster after you change its security password. Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

**Note**

During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

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

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

**Note**

For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

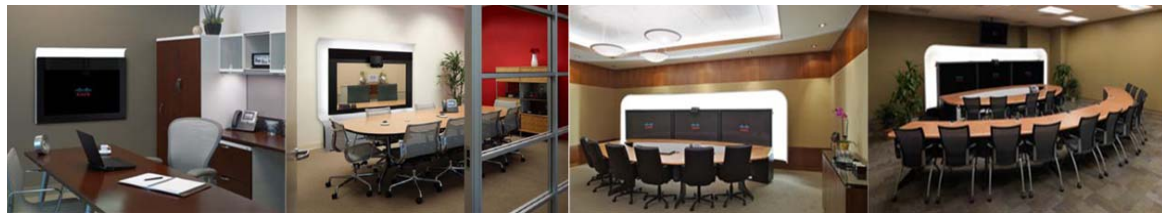
Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

Where to Go Next

See the [Cisco TelePresence Multipoint Switch](#) home page on Cisco.com.



APPENDIX **A**

Cisco TelePresence Firewall and Access List Considerations

Revised: September, 2010, OL-18391-01
Cisco TelePresence Software Solution Release 1.7(x)

Contents

This appendix contains the following sections:

- [Overview, page A-1](#)
- [TCP and UDP Ports for Cisco TelePresence, page A-2](#)

Overview

Cisco TelePresence is a component of the Cisco Unified Communications suite and is designed to be deployed on a converged IP network. Many enterprise customers rely on firewalls and/or Access Control Lists (ACLs) to protect their Unified Communications network from various sorts of malicious threats. ACLs are also frequently used to enforce Quality of Service (QoS) settings, including marking, shaping and policing traffic at various places in the network, such as at the access edge of a local area network (LAN), or at the intersection of a LAN and wide area network (WAN).

The Cisco Unified Communications suite already fully supports a proven security framework, which in turn is one component of the Security Architecture for Enterprises (SAFE) Blueprint for Unified Communications. As a SIP-based end user device of Cisco Unified Communications Manager, Cisco TelePresence fits into this framework and the existing concepts, methodologies and best practices for deploying firewalls and ACLs with Cisco Unified Communications. For more details on these and related security concepts, please refer to the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html

There are three key considerations for using Firewalls and/or Access Control Lists with Cisco TelePresence:

1. The specific TCP and UDP ports that need to be permitted between each component of the solution.
2. The bandwidth required for the audio and video media streams of a Cisco TelePresence meeting is significantly higher and far less tolerant to latency, jitter and loss than a typical voice call and should be taken into consideration when considering specific router, firewall and intrusion prevention (IPS) platforms and their performance characteristics.

- Firewalls that rely on Application Layer Inspection in order to dynamically open/close certain UDP ports may not support the specific SIP protocol implementation of Cisco TelePresence, or may not be able to inspect the contents of the application layer protocol because it is encrypted.

This document only addresses the first of the above three considerations. It provides the list of TCP and UDP ports used by Cisco TelePresence. It does not provide guidance on which router, firewall or IPS platforms or configurations customers should use. General firewall design guidance for Cisco TelePresence can be found in Chapter 13 of the [Cisco TelePresence Network Systems Design Guide](#) at the following path:

<http://www.cisco.com/go/cvd> > Design Zone for Video > Cisco TelePresence

This document should be used in conjunction with the above chapter.


Note

Customers are advised to thoroughly test Cisco TelePresence against their specific firewall, ACL, or IPS configurations prior to deploying them in production.

Table A-1 contains document terminology definitions.

Table A-1 Terminology Used in This Document

Term	Definition
CTS Primary Codec	Cisco TelePresence System Primary Codec.
Phone	Cisco Unified 797X Series IP Phone which is attached to the Cisco TelePresence System.
CTS-Manager	Cisco TelePresence Manager.
CTMS	Cisco TelePresence Multipoint Switch.
CUCM (Cisco Unified CM)	Cisco Unified Communications Manager.
ephemeral	A random range of TCP or UDP ports which are dynamically assigned. Many protocols use ephemeral source ports with well-known destination ports. However, TFTP is an exception, as noted in the tables below, which uses ephemeral ports in both directions.

TCP and UDP Ports for Cisco TelePresence

This appendix contains information about ports used by Cisco TelePresence that are relevant to a firewall or ACL administrator. Ports used for internal communications, such as between the Cisco TelePresence Primary and Secondary Codecs, and between the Cisco TelePresence Primary Codec and the Cisco Unified IP Phone 797X are not included in this appendix. For a comprehensive list of all ports used by Cisco Unified CM release 7.0, please refer to the following information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/7_0/CCM_7.0PortList.pdf

The following tables provide lists of TCP and UDP ports that are used by the Cisco TelePresence solution.

- [Cisco TelePresence System \(CTS\) Primary Codec, page A-3](#)
- [Cisco Unified IP Phone 797X, page A-5](#)
- [Cisco TelePresence Manager \(CTS-Manager\), page A-7](#)
- [Cisco TelePresence Multipoint Switch \(CTMS\), page A-11](#)

- [Cisco TelePresence Recording Server \(CTRS\)](#), page A-13
- [Cisco IOS IP Service Level Agreements \(IPSLA\)](#), page A-14
- [Cisco Media Experience Engine \(MXE\) 5600](#), page A-15

Cisco TelePresence System (CTS) Primary Codec

Table A-2 contains information about the CTS Primary Codec in CTS Release 1.7(x).

Table A-2 Cisco TelePresence System Primary Codec - Release 1.7(x)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	CTS Primary Codec: N/A	Switch: N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached and learn what Virtual LAN (VLAN) it should tag its packets with. Note CDP is a layer-2 protocol and hence does not use TCP or UDP for transport.
DHCP	UDP	0.0.0.0: 68 CTS Primary Codec: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP on every CTS endpoint.
	UDP	0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS Primary Codec: 123	NTP: 123	Synchronizes the hardware clock on the CTS with an NTP server.
DNS	UDP	CTS Primary Codec: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-2 Cisco TelePresence System Primary Codec - Release 1.7(x)

HTTP	TCP	CTS Primary Codec: Ephemeral	CUCM: 6970	Downloads configuration and firmware files from the Cisco Unified CM TFTP service. Note The CTS Primary Codec uses HTTP instead of TFTP for accessing these files.
		CTS Primary Codec: Ephemeral	CUCM: 8080	Used by the Directories feature on the CTS Cisco Unified IP Phone user interface to search the Cisco Unified CM LDAP directory.
		<ul style="list-style-type: none"> CTS Primary Codec: Ephemeral CTS-Manager: Ephemeral 	<ul style="list-style-type: none"> CTS-Manager: 8080, 8443 CTS Primary Codec: 8081, 9501 	Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager: <ul style="list-style-type: none"> When security is enabled, the CTS uses port 8443 and CTS-Manager uses port 9501 on the CTS (recommended). When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		ANY: Ephemeral	CTS Primary Codec: 80, 443	Accesses the administrative web interface of the CTS Codec. Port 80 is automatically redirected to port 443.
		CTS Primary Codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock.
SSH	TCP	ANY: Ephemeral	CTS Primary Codec: 22	Accesses the CTS codec administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS Primary Codec: 161	Receives SNMP queries from a management station.
		CTS Primary Codec: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS Primary Codec: Ephemeral	CUCM: 3804	Registers its Manufacturing Installed Certificate (MIC), or obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS Primary Codec: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service.
SIP	UDP	CTS Primary Codec: Ephemeral	CUCM: 5060	Used for registration and call signaling between the CTS and Cisco Unified CM. Can be one of the following: <ul style="list-style-type: none"> UDP port 5060 TCP port 5060 TCP port 5061 if SIP over TLS is enabled (recommended).
	TCP		CUCM: 5060, 5061	
RTP	UDP	CTS Primary Codec: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.

Table A-2 Cisco TelePresence System Primary Codec - Release 1.7(x)

XML-R PC	TCP	CTS Primary Codec: Ephemeral	Phone: 61456	Autostarts the MIDlet phone user interface (UI).
		Phone: Ephemeral	CTS Primary Codec: 61457	Sends notifications to the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61458	Receives notifications from the MIDlet phone UI.

Cisco Unified IP Phone 797X

Table A-3 contains information about the Cisco Unified IP Phone 797x for Cisco Unified CM Release 8.5(3).

Table A-3 Cisco Unified IP Phone 797x - Release 8.5(3)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	Phone: N/A	Switch: N/A	Advertises its existence to the CTS Primary Codec and to the upstream Cisco Catalyst Ethernet Switch to which it is attached to learn what Virtual LAN (VLAN) it should tag its packets with and to negotiate Power over Ethernet. Note CDP is a layer-2 protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 Phone: 68	Broadcast: 67	Requests an IP address from the DHCP server.
	UDP	0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	Phone: 123	NTP: 123	Synchronizes the hardware clock on the phone with an NTP server.
DNS	UDP	Phone: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
TFTP	UDP	Phone: Ephemeral	TFTP: 69	Downloads configuration and firmware files from the Cisco Unified CM TFTP service.
		TFTP: Ephemeral	Phone: Ephemeral	The initial TFTP request to port 69 spawns unique sessions for each configuration and firmware file downloaded. These sessions are established using ephemeral source and destination ports.
HTTP	TCP	ANY: Ephemeral	Phone: 80	Accesses the administrative web interface for the CTS Cisco Unified IP phone (for troubleshooting purposes only).

Table A-3 Cisco Unified IP Phone 797x - Release 8.5(3)

SSH	TCP	ANY: Ephemeral	Phone: 22	Accesses the administrative command-line interface (CLI) of the CTS Cisco Unified IP Phone (for troubleshooting purposes only).
CAPF	TCP	Phone: Ephemeral	CUCM: 3804	Registers its Manufacturing Installed Certificate (MIC), or obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	Phone: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service.
SIP	UDP	Phone: Ephemeral	CUCM: 5060	Used for registration and call signaling between the phone and Cisco Unified CM. Can be UDP port 5060, TCP port 5060, or TCP port 5061 if SIP over TLS is enabled. SIP over TLS is recommended.
	TCP	—	CUCM: 5060, 5061	
RTP	UDP	Phone: 16384 – 32768	ANY: ANY	Sends and receives audio media.
XML-RPC	TCP	CTS Primary Codec: Ephemeral	Phone: 61456	Autostarts the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61457	Sends notifications to the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61458	Receives notifications from the MIDlet phone UI.

Cisco TelePresence Manager (CTS-Manager)

See the following tables for CTS-Manager support:

- [Cisco TelePresence Manager \(CTS Manager\) for Microsoft Exchange, page A-7](#)
- [Cisco TelePresence Manager for IBM Domino, page A-9](#)

Cisco TelePresence Manager (CTS Manager) for Microsoft Exchange

Table A-4 contains information about CTS Manager Release 1.7(x) with Microsoft Exchange 2003 WebDAV and 2010 EWS.

Table A-4 Cisco TelePresence Manager 1.7(x) – for Microsoft Exchange 2003 WebDAV and 2010 EWS

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTS-Manager: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS-Manager: 123	NTP: 123	Synchronizes the hardware clock on the CTS-Manager with an NTP server.
DNS	UDP	CTS-Manager: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-4 Cisco TelePresence Manager 1.7(x) – for Microsoft Exchange 2003 WebDAV and 2010 EWS

HTTP	TCP	CTS Primary Codec: Ephemeral	CTS-Manager: 8080, 8443	Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager. <ul style="list-style-type: none"> When security is enabled, the CTS uses port 8443 on CTS-Manager and CTS-Manager uses port 9501 on the CTS (recommended). When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		CTS-Manager: Ephemeral	CTS Primary Codec: 8081, 9501	
		CTMS: Ephemeral	CTS-Manager: 8080, 8443	Uses XML/SOAP over HTTP or HTTPS to coordinate meeting schedule and system operational status between CTS-Manager and the CTMS.
		CTS-Manager: Ephemeral	CTMS: 8080, 8443	
		CTS-Manager: Ephemeral	CUCM: 8443	Uses XML/SOAP over HTTPS to the AXL Web Services on Cisco Unified CM to interrogate the Cisco Unified CM database to discover the existence of CTS endpoints.
		ANY: Ephemeral	CTS-Manager: 80,443	Accesses the administrative web interface of CTS-Manager. Port 80 is automatically redirected to port 443.
SSH	TCP	ANY: Ephemeral	CTS-Manager: 22	Accesses the CTS-Manager administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS-Manager: 161	Receives SNMP queries from a management station.
		CTS-Manager: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS-Manager: Ephemeral	CUCM: 3804	Obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS-Manager: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service.
JTAPI	TCP	CTS-Manager: Ephemeral	CUCM: 2748, 2749	Uses JTAPI to register with Cisco Unified CM CTI Manager service to receive device event status of CTS endpoints. <ul style="list-style-type: none"> When security is enabled, CTS-Manager uses port 2749 on Cisco Unified CM (recommended). Otherwise, port 2748 is used.
LDAP	TCP	CTS-Manager: Ephemeral	AD: 389,3268,636	Discovers the Microsoft Exchange mailbox name of each CTS endpoint and authenticates users logging into CTS-Manager. <ul style="list-style-type: none"> Port 389 is used for single AD server deployments. If AD deployment uses a Global Catalogue Server, then port 3268 is used. If AD uses LDAP over Secure Sockets Layer (LDAP/SSL), then port 636 is used (recommended).

Table A-4 Cisco TelePresence Manager 1.7(x) – for Microsoft Exchange 2003 WebDAV and 2010 EWS

WebDAV	TCP	CTS-Manager: Ephemeral	Exchange: 80,443	Subscribes to the Microsoft Exchange mailbox of each Cisco TelePresence endpoint to process meeting requests. <ul style="list-style-type: none"> If Exchange is setup to support SSL, then port 443 is used (recommended). Otherwise, port 80 is used.
	UDP	Exchange: Ephemeral	CTS-Manager: 3621	Notifies CTS-Manager of any events in the mailboxes to which it is subscribed.

Cisco TelePresence Manager for IBM Domino

Table A-5 contains information about Cisco TelePresence Manager 1.7(x) for IBM Domino.

Table A-5 Cisco TelePresence Manager 1.7(x) – for IBM Domino

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTS-Manager: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS-Manager: 123	NTP: 123	Synchronizes the hardware clock on the CTS-Manager with an NTP server.
DNS	UDP	CTS-Manager: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-5 Cisco TelePresence Manager 1.7(x) – for IBM Domino

HTTP	TCP	<ul style="list-style-type: none"> CTS Primary Codec: Ephemeral CTS-Manager Ephemeral 	<ul style="list-style-type: none"> CTS-Manager : 8080, 8443 CTS Primary Codec: 8081, 9501 	<p>Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager.</p> <ul style="list-style-type: none"> When security is enabled, the CTS uses port 8443 on CTS-Manager and CTS-Manager uses port 9501 on the CTS (recommended). When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		<ul style="list-style-type: none"> CTMS: Ephemeral CTS-Manager Ephemeral 	<ul style="list-style-type: none"> CTS-Manager : 8080, 8443 CTMS: 8080, 8443 	
		CTS-Manager: Ephemeral	CUCM: 8443	Uses XML/SOAP to interrogate the Cisco Unified CM database to discover the existence of CTS endpoints.
		ANY: Ephemeral	CTS-Manager: 80,443	Accesses the administrative web interface of CTS-Manager. Port 80 is automatically redirected to port 443.
SSH	TCP	ANY: Ephemeral	CTS-Manager: 22	Accesses the CTS-Manager administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS-Manager: 161	Receives SNMP queries from a management station.
		CTS-Manager: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS-Manager: Ephemeral	CUCM: 3804	Obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS-Manager: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List Provider service.
JTAPI	TCP	CTS-Manager: Ephemeral	CUCM: 2748, 2749	<p>Uses JTAPI to register with Cisco Unified CM CTI Manager service to receive device event status of CTS endpoints.</p> <ul style="list-style-type: none"> When security is enabled, CTS-Manager uses port 2749 on Cisco Unified CM (recommended). Otherwise, port 2748 is used.
LDAP	TCP	CTS-Manager: Ephemeral	Domino: 389,636	<p>Discovers the Domino mailbox name of each CTS endpoint, and authenticates users logging into CTS-Manager.</p> <ul style="list-style-type: none"> If Domino uses LDAP over Secure Sockets Layer (LDAP/SSL), then port 636 is used (recommended). Otherwise, port 389 is used.

Table A-5 Cisco TelePresence Manager 1.7(x) – for IBM Domino

IIOP	TCP	CTS-Manager: Ephemeral	Domino: 80,443	Negotiates an Internet Inter-ORB Protocol (IIOP) session to the Domino mailbox of each CTS endpoint to process meeting requests. <ul style="list-style-type: none"> If Domino is setup to support SSL, then port 443 is used (recommended). Otherwise, port 80 is used.
	UDP	CTS-Manager: Ephemeral	Domino: 63148	Queries and synchronizes the Domino mailboxes it is subscribed to.

Cisco TelePresence Multipoint Switch (CTMS)

Table A-6 contains information about the Cisco TelePresence Multipoint Switch for Release 1.7(x).

Table A-6 Cisco TelePresence Multipoint Switch – Release 1.7(x)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTMS: 68	Broadcast: 67	Requests an IP address from the DHCP server. Note It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTMS: 123	NTP: 123	Synchronizes the hardware clock on the CTMS with an NTP server.
DNS	UDP	CTMS: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-6 Cisco TelePresence Multipoint Switch – Release 1.7(x)

HTTP	TCP	<ul style="list-style-type: none"> CTMS: Ephemeral CTS-Manager: Ephemeral 	<ul style="list-style-type: none"> CTS-Manager: 8080, 8443 CTMS: 8080, 8443 	<p>Uses XML/SOAP over HTTP or HTTPS to coordinate meeting schedule and system operational status between CTS-Manager and the CTMS.</p> <ul style="list-style-type: none"> When security is enabled, the CTMS uses port 8443 on CTS-Manager and CTS-Manager uses port 8443 on the CTMS (recommended). When security is not enabled, CTMS uses port 8080 on CTS-Manager, and CTS-Manager uses port 8080 on the CTMS.
		ANY: Ephemeral	CTMS: 80,443	Accessed the CTMS administrative web interface. Port 80 is automatically redirected to port 443.
		CTS Primary Codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock. This port is the same for both secure and non-secure modes.
SSH	TCP	ANY: Ephemeral	CTMS: 22	Accesses the CTMS administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTMS: 161	Receives SNMP queries from a management station.
		CTMS: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
SIP	UDP	CTMS: Ephemeral	CUCM: 5060, 5061	<p>Used for call signaling with Cisco Unified CM.</p> <ul style="list-style-type: none"> When security is not enabled, use UDP or TCP port 5060. When security is enabled, use UDP or TCP. <p>Note Unlike the CTS endpoints which always initiate the SIP TCP socket to Cisco Unified CM, in the case of CTMS either side can initiate the connection.</p>
		CUCM: Ephemeral	CTMS: 5060, 5061	
	TCP	CTMS: Ephemeral	CUCM: 5060, 5061	
		CUCM: Ephemeral	CTMS: 5060, 5061	
RTP	UDP	CTMS: 16384 – 32768	ANY: ANY	Send and receives audio and video media.

Cisco TelePresence Recording Server (CTRS)

Table A-7 contains information about Cisco TelePresence Recording Server for Release 1.7(X).

Table A-7 Cisco TelePresence Recording Server – Release 1.7(X)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTRS: 68	Broadcast: 67	Requests an IP address from the DHCP server. It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTRS: 123	NTP: 123	Synchronizes the hardware clock on the CTRS with an NTP server.
DNS	UDP	CTRS: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
HTTP	TCP	ANY: Ephemeral	CTRS: 80,443	Accesses the CTRS administrative web interface. Port 80 is automatically redirected to port 443.
		<ul style="list-style-type: none"> CTRS: Ephemeral CTS-Manager; Ephemeral 	<ul style="list-style-type: none"> CTRS: 8080, 8443 CTS-Manager : 8080, 8443 	Uses XML/SOAP over HTTP or HTTPS to maintain a heartbeat with the CTS-Manager, if configured.
SSH	UDP	ANY: Ephemeral	CTRS: 22	Accesses the CTRS administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTRS: 161	Receives SNMP queries from a management station.
		CTRS: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.

Table A-7 Cisco TelePresence Recording Server – Release 1.7(X)

SIP	UDP	CTRS: Ephemeral	CUCM: 5060, 5061	Used for call signaling with Cisco Unified CM: <ul style="list-style-type: none"> When security is not enabled, CTRS uses UDP or TCP port 5060. When security is enabled, CTRS uses UDP or TCP port 5061.
	TCP	CTRS: Ephemeral	CUCM: 5060, 5061	
RTP	UDP	CTRS: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.

Cisco IOS IP Service Level Agreements (IPSLA)

Cisco IOS IP Service Level Agreements (IPSLA) is commonly used prior to the installation of Cisco TelePresence to measure and assess the network path.

[Table A-8](#) lists the specific ports relevant for the IPSLA UDP Jitter probe operation used to conduct Cisco TelePresence Network Path Assessment (NPA) testing. The term “Agent” refers to the router who generates the IPSLA test packets, and “Responder” refers to the router which replies to those requests. “Both” means that either the Agent or the Responder could generate such a packet.


Note

[Table A-8](#) provides the ports most commonly used by IPSLA Agent and IPSLA Responder routers. Because IPSLA runs on Cisco IOS, there may be other ports used for communications by those routers.

Table A-8 Cisco IOS IP Service IPSLA Support

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. Note CDP is a layer-2 management protocol and hence does not use TCP or UDP.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	Both: 123	NTP: 123	Synchronizes the hardware clock on the Cisco IOS IPSLA router with an NTP server.
DNS	UDP	Both: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
SSH	TCP	ANY: Ephemeral	Both: 22	Accesses the Cisco IOS IPSLA router administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	Both: 161	Receives SNMP queries from a management station.
		Both: Ephemeral	ANY: 162	Sends SNMP traps to a management station.

Table A-8 Cisco IOS IP Service IPSLA Support

IPSLA	UDP	Agent: Ephemeral	Responder: 1967	Signals a new IPSLA operation between the Agent and the Responder.
RTP	UDP	Agent: Ephemeral	Responder: 16384 – 32768 (configurable)	Sends and receives audio and video media from the Agent to the Responder. The Responder then returns these packets back to the Agent. The specific destination UDP ports can be defined in the IPSLA Agent configuration.

Cisco Media Experience Engine (MXE) 5600

The Cisco Media Experience Engine (MXE) 5600 provides interoperability between Cisco TelePresence and video conferencing devices. The port assignments listed in [Table A-9](#) are valid for Cisco Media Experience Engine Operating System (Cisco MXE-OS) Release 1.0.(x).

Table A-9 MXE Support for Release 1.0.(x)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachable may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
DNS	UDP	MXE: Ephemeral	Server: 53	Used for name resolution.
NTP	UDP	MXE: 123	NTP: 123	Synchronizes the hardware clock on MXE with an NTP server.
SSH	TCP	ANY: Ephemeral	MXE: 22	Accesses MXE administrative command-line interface (CLI).
TELNET	TCP	ANY: Ephemeral	MXE: 23	
SNMP	UDP	ANY: Ephemeral	MXE: 161	Receives SNMP queries from a management station.
		MXE: Ephemeral	MXE: 162	Sends SNMP traps to a management station.
SIP	TCP	CUCM: 5060	MXE: Ephemeral	Used for call signaling with Cisco Unified CM (configurable).
		CUCM: Ephemeral	MXE: 5060	Used for call signaling with Cisco Unified CM (configurable).
RTP	UDP	CTMS: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.

