What's in This Guide

Revised: November 2014, OL-18391-01

Contents

Security Solutions Overview

This document describes two different security features available on Cisco TelePresence infrastructure devices, the Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence Recording Server (CTRS), and Cisco TelePresence Manager (CTS-Manager).

Inter-device security provides secure communication between devices on your Cisco TelePresence network. In the case of the CTMS, this security feature also enables you to determine the default security policy (secure or best effort) for mulitpoint meetings.

Browser security secures communication between a web browser and your infrastructure device administrative interface.

Note You can configure either inter-device security or browser security on an infrastructure device. You cannot configure both security features on one device.

Inter-Device Security 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.

Browser Security Overview

You can set up an encrypted link between the web server of a Cisco TelePresence infrastructure device (a CTMS, CTRS, or CTS-Manager), and the browser through which you access the Administrative UI. If multiple infrastructure devices exist in your Cisco TelePresence topology, you can optionally set up browser security for each one.

Setting up browser security is comprised of these steps, which can be performed over one or more days:

5. Request a Secure Sockets Layer (SSL) certificate from a certificate authority (CA), which is comprised of these substeps:
   a. Generate a Certificate Signing Request (CSR).
   b. Apply for the SSL certificate from a CA.
   c. Wait for the SSL certificate from the CA, which can take a few seconds to a few days.
6. Install the certificate on the device.

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 v 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:

Related Documents

Related Topic	Document Title
How to navigate to Cisco TelePresence System (CTS) hardware and software documentation, including information about CTS devices.	• Cisco.com **Products** > **TelePresence** > **Cisco TelePresence System** > **TelePresence System**
Cisco Unified CM security operational details.	• *Cisco Unified Communications Manager Security Guide*
Configuration, maintenance, and monitoring tasks using Cisco TelePresence administration software.	• Cisco TelePresence Administration Software home page on Cisco.com
Cisco TelePresence administration software documentation and software download page.	• Cisco TelePresence Administration Software Download
Describes new features and open and closed hardware and software caveats for Cisco TelePresence System (CTS) software releases.	• Cisco TelePresence Administration Software Release Notes home page on Cisco.com

Cisco Unified CM installation with the Cisco TelePresence System.	• *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
Cisco command-line interface (CLI) information for configuring the Cisco TelePresence System.	• 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.	• 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.	• Cisco TelePresence Administration Software End-User Guides on Cisco.com
Cisco TelePresence System system message information.	• *Cisco TelePresence System Message Guide*
Cisco TelePresence Manager documentation home page.	• Cisco TelePresence Manager home page on Cisco.com
Information about the Cisco TelePresence Multipoint Switch (CTMS).	• Cisco TelePresence Multipoint Switch home page on Cisco.com
Cisco TelePresence Recording Server information.	• *Cisco TelePresence Recording Server* home page on Cisco.com
Complete guide to the CTS software and hardware documentation.	• *Cisco TelePresence System Documentation Roadmap*
Cisco Unified CM documentation types and locations.	• Cisco Unified Communications Manager (CallManager) Documentation Roadmaps
Cisco Unified Communications Manager Support page.	• 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.	• *Cisco TelePresence Network Systems 2.0 Design Guide*
Information about Key Exchange via Encrypted Key Transport (EKT) and other Cisco TelePresence security solutions.	• *Design Zone for Video: Cisco TelePresence Secure Communications and Signaling Guide*
Information about the Cisco TelePresence Server.	• Cisco TelePresence Server home page
Information about managing your videoconferencing network.	• Cisco TelePresence Management Suite
Cisco Unified IP Phone firmware download instructions.	• 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 sysop 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.