Configuring and Verifying Cisco TelePresence Security

Revised: March 20, 2015, 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

Table 4-1 provides a list of configuration tasks that you perform to configure and verify inter-device security.

Table 4-1 Cisco TelePresence Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: • Activate the CAPF server. • Create the Certificate Trust List (CTL). • Download the CAPF.der file.	• 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 4-2

Table 4-1 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 4-3
Step 4	Verify security status.	• Verifying Security Status Between the Cisco TelePresence System and Cisco TelePresence Manager, page 4-4 • Verifying Security Status Between the CTMS and Cisco TelePresence Manager, page 4-4

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:

a. Choose **System > Security Profile > Phone Security Profile**.

b. Click the **Add New** button. The Phone Security Profile Configuration window appears.

c. In the Phone Security Profile Type drop-down list, specify the type of Cisco TelePresence system that you are configuring. For example, Cisco 7975.

d. Click **Next**.

e. In the Select the phone security profile protocol drop-down list, select **SIP** and click **Next**.

f. 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.

g. Enter the following information in the Phone Security Profile CAPF Information box:

- **Authentication Mode**—Choose **By Authentication String**.
- **Key Size (Bits)**—Choose **1024** (default).

h. 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:

a. Choose **Device > Phone**.

b. Click **Find** to find the existing Cisco TelePresence device that you want to configure.

c. 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.

d. Scroll down to the Protocol Specific Information box and locate the Device Security drop-down list.

e. 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.

f. 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).

g. 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 4-3.

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 4-2.

Step 4 Click **Apply** to apply your changes.

Note To configure an IX5000 or IX5200 system, open a SSH CLI session with the system as the user **admin**, then enter the command **set security authstring** *string*, where *string* is the authentication string that you generated in the "Configuring Cisco TelePresence Phone Profile Security" section on page 4-2.

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

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 5, "Configuring Cisco TelePresence Browser Security" to configure browser security for Cisco TelePresence infrastructure devices.