Configuring Inter-device Security for the Cisco TelePresence Infrastructure Devices

Revised: November 2014, 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 device administration interface.

Contents

This chapter describes how to configure inter-device security for Cisco TelePresence infrastructure devices, which include the Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence Recording Server (CTRS), and Cisco TelePresence Manager (CTS-MAN), and includes the following sections:

Before You Begin

- The infrastructure device automatically restarts a few times during the setup, which abruptly ends all active meetings or recordings. Therefore, we recommend performing the setup during a time when there are few or no active meetings or recordings.
- You can set up either inter-device security or browser security on a Cisco TelePresence infrastructure device. If browser security is already set up, you must disable it before you can set up inter-device security. For information on disabling browser security, see the "Disabling and Reenabling Browser Security" section on page 5-9.

Cisco TelePresence Inter-Device Security Infrastructure Device Configuration Checklist

Cisco TelePresence infrastructure devices support secure communication between 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 on an infrastructure device for the first time.

Table 3-1 Cisco Inter-Device Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Complete the following: • Activate the CAPF server. • Create an application user. • Create a CAPF profile. • Download certificates from the Cisco Unified CM to the infrastructure device. • Create the Certificate Trust List (CTL).	• Chapter 1, "Activating the Certificate Authority Proxy Function Server" • Chapter 2, "Configuring the Cisco CTL Client"
Step 2	Upload the *.der certificate files to the infrastructure device.	Installing Downloaded Security Certificates to an Infrastructure Device, page 3-3
Step 3	Download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the infrastructure device.	Downloading LSCs onto an Infrastructure Device, page 3-5
Step 4	Create and configure the SIP security trunk	• Creating a SIP Trunk Security Profile, page 3-7 • Configuring the SIP Security Trunk, page 3-10
Step 5	Configure SIP security on the infrastructure device.	Configuring a CTMS or a CTRS for SIP Security, page 3-12
Step 6	Configure the default meeting security level on the infrastructure device.	Configuring the Default Meeting Security Level on a CTMS, page 3-14

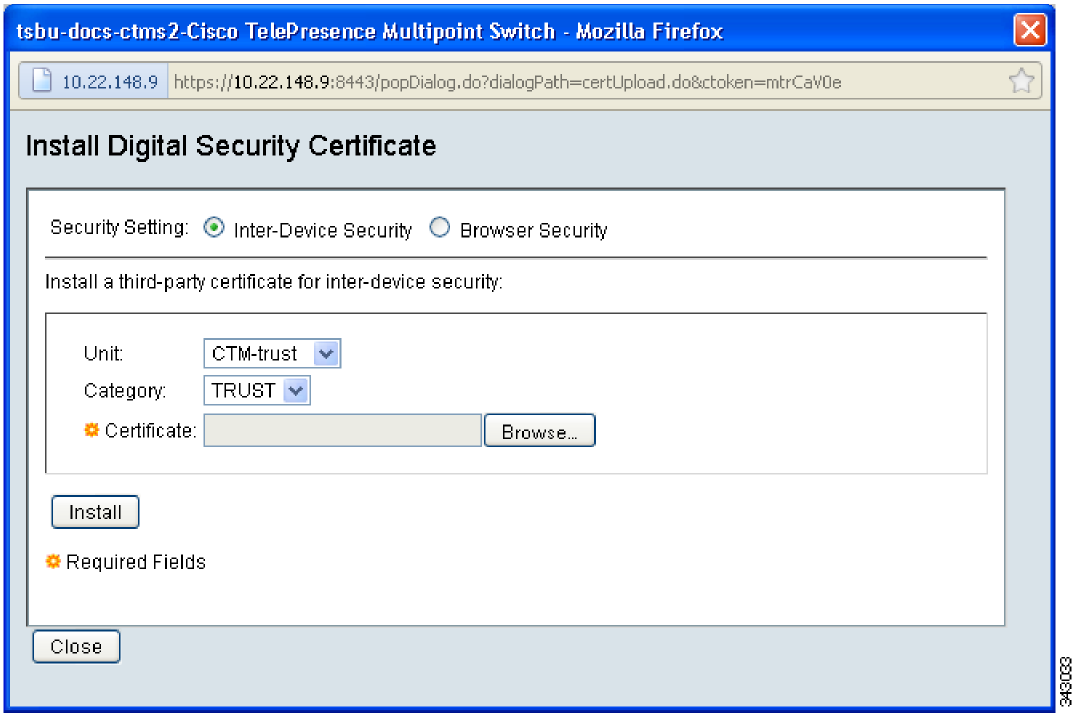
Installing Downloaded Security Certificates to an Infrastructure Device

To upload the *.der certificate files to an infrastructure device:

Step 1 From the device administration interface, choose **Configure** > **Security**.

Step 2 Click **Install**. The Certificate Upload window displays, as shown in Figure 3-1.

Figure 3-1 Certificate Install Window



tsbu-docs-ctms2-Cisco TelePresence Multipoint Switch - Mozilla Firefox

10.22.148.9 https://10.22.148.9:8443/popDialog.do?dialogPath=certUpload.do&ctoken=mtrCaV0e

Install Digital Security Certificate

Security Setting: ● Inter-Device Security ○ Browser Security

Install a third-party certificate for inter-device security:

Unit: CTM-trust

Category: TRUST

Certificate:

Step 3 Upload the CAPF.der file to infrastructure device by completing the following steps:

a. Select the Inter-Device radio button.

b. From the Unit drop-down list, select **CAPF-trust**.

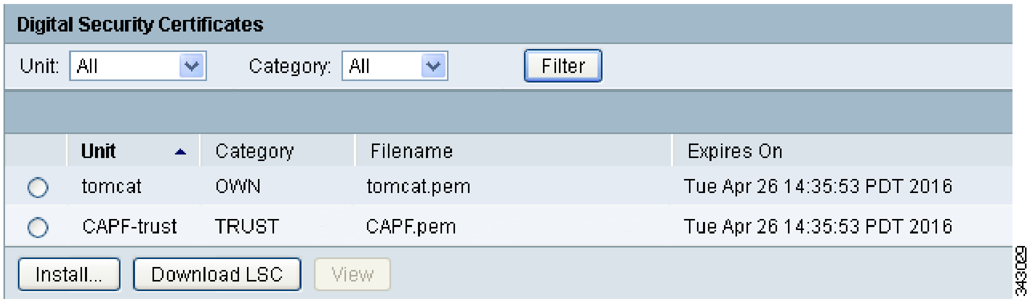
c. From the Category drop-down list, select **TRUST** (this is the default value).

d. Click the **Browse** button to upload a CAPF certificate.

e. Choose the CAPF.der that you downloaded to your local machine.

f. Click **Install**. 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



Digital Security Certificates

Unit: All   Category: All

	Unit	Category	Filename	Expires On
○	tomcat	OWN	tomcat.pem	Tue Apr 26 14:35:53 PDT 2016
○	CAPF-trust	TRUST	CAPF.pem	Tue Apr 26 14:35:53 PDT 2016

Step 4 Upload the CUCMx.der file from your local machine by completing the following steps:

a. Return to the Security Settings window.

b. Click **Install**.

c. After the Certificate Upload window displays, make sure that the following settings are present:

- The **Inter-Device Security** radio button is selected.
- **CTM-TRUST** is selected in the Unit drop-down list
- **TRUST** is selected in the Category drop-down list

d. Click the **Browse** button to upload the Cisco Unified CM root certificate.

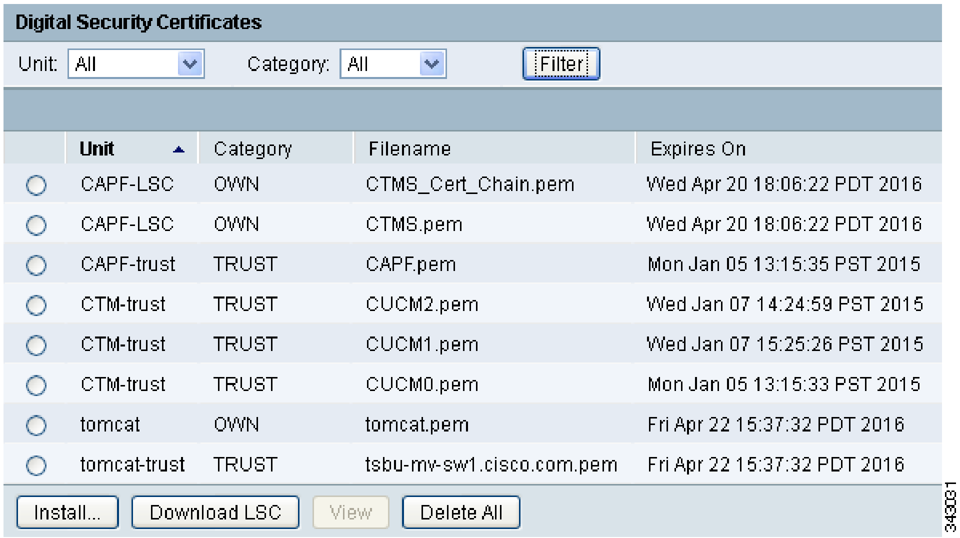
e. Choose the CUCM0.der file that you downloaded to your local machine.

f. Click **Install**. The CUCM0.der file displays as a CUCM0.pem file in the Digital Certificates Window.

g. If you have additional CUCM*x*.der files, upload each CUCM*x*.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

Unit: All Category: All

	Unit ▲	Category	Filename	Expires On
○	CAPF-LSC	OWN	CTMS_Cert_Chain.pem	Wed Apr 20 18:06:22 PDT 2016
○	CAPF-LSC	OWN	CTMS.pem	Wed Apr 20 18:06:22 PDT 2016
○	CAPF-trust	TRUST	CAPF.pem	Mon Jan 05 13:15:35 PST 2015
○	CTM-trust	TRUST	CUCM2.pem	Wed Jan 07 14:24:59 PST 2015
○	CTM-trust	TRUST	CUCM1.pem	Wed Jan 07 15:25:26 PST 2015
○	CTM-trust	TRUST	CUCM0.pem	Mon Jan 05 13:15:33 PST 2015
○	tomcat	OWN	tomcat.pem	Fri Apr 22 15:37:32 PDT 2016
○	tomcat-trust	TRUST	tsbu-mv-sw1.cisco.com.pem	Fri Apr 22 15:37:32 PDT 2016

Downloading LSCs onto an Infrastructure Device

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

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.

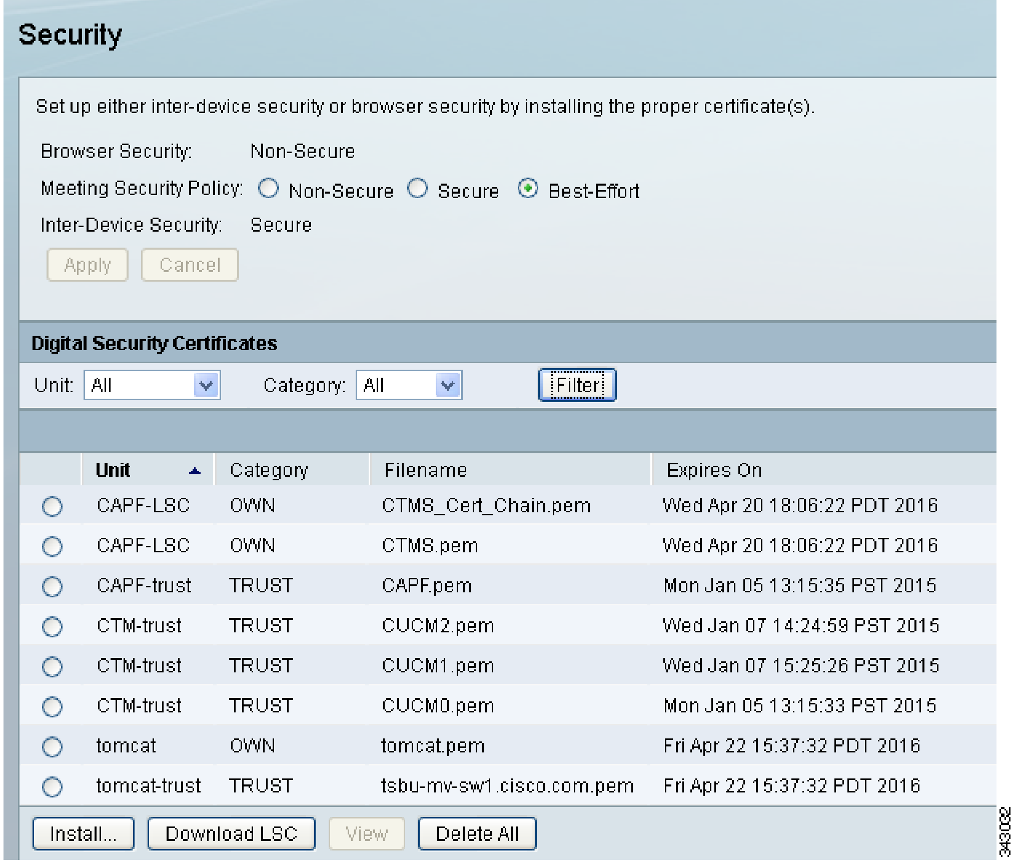
Procedure

To download LSCs:

Step 1 From the device administration interface, choose **Configure** > **Security**.

Step 2 Click **Download LSC**. The Download CAPF LSC window appears, as shown in Figure 3-4.

Figure 3-4 Download CAPF LSC Window



Security

Set up either inter-device security or browser security by installing the proper certificate(s).

Browser Security: Non-Secure

Meeting Security Policy: ○ Non-Secure ○ Secure ● Best-Effort

Inter-Device Security: Secure

Digital Security Certificates

Unit: All Category: All

	Unit	Category	Filename	Expires On
○	CAPF-LSC	OWN	CTMS_Cert_Chain.pem	Wed Apr 20 18:06:22 PDT 2016
○	CAPF-LSC	OWN	CTMS.pem	Wed Apr 20 18:06:22 PDT 2016
○	CAPF-trust	TRUST	CAPF.pem	Mon Jan 05 13:15:35 PST 2015
○	CTM-trust	TRUST	CUCM2.pem	Wed Jan 07 14:24:59 PST 2015
○	CTM-trust	TRUST	CUCM1.pem	Wed Jan 07 15:25:26 PST 2015
○	CTM-trust	TRUST	CUCM0.pem	Mon Jan 05 13:15:33 PST 2015
○	tomcat	OWN	tomcat.pem	Fri Apr 22 15:37:32 PDT 2016
○	tomcat-trust	TRUST	tsbu-mv-sw1.cisco.com.pem	Fri Apr 22 15:37:32 PDT 2016

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.

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

Note The infrastructure device 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.

- **CAPF Server Port**—Leave the default value.

Step 4 Click **Download LSC**.

Step 5 Click **OK** to confirm your choice. The LSCs are created.

Note After successfully creating the LSCs, the infrastructure device will restart.

Step 6 After the infrastructure device restarts, from the device administration interface, choose **Configure** > **Security**.

Verify that the Inter-Device Security field is set to secure, and that the Digital Security Certificate window displays the LSC certificates that were created, as listed in Table 3-1:

Table 3-2 LSC Certificate File Names

CTMS LSC Certificates	CTRS LSC Certificates	CTS-Man LSC Certificates
• CTMS_Cert_Chain.pem • CTMS.pem	• CTRS_Cert_Chain.pem • CTRS.pem	• CTM_Cert_Chain.pem • CTM.pem

Step 7 Obtain the SIP security trunk information by completing the following steps:

a. Click the radio button for the device .pem file.

b. Click the **View** button.

c. 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 infrastructure device and Cisco Unified CM communication secure, create a secure SIP trunk.

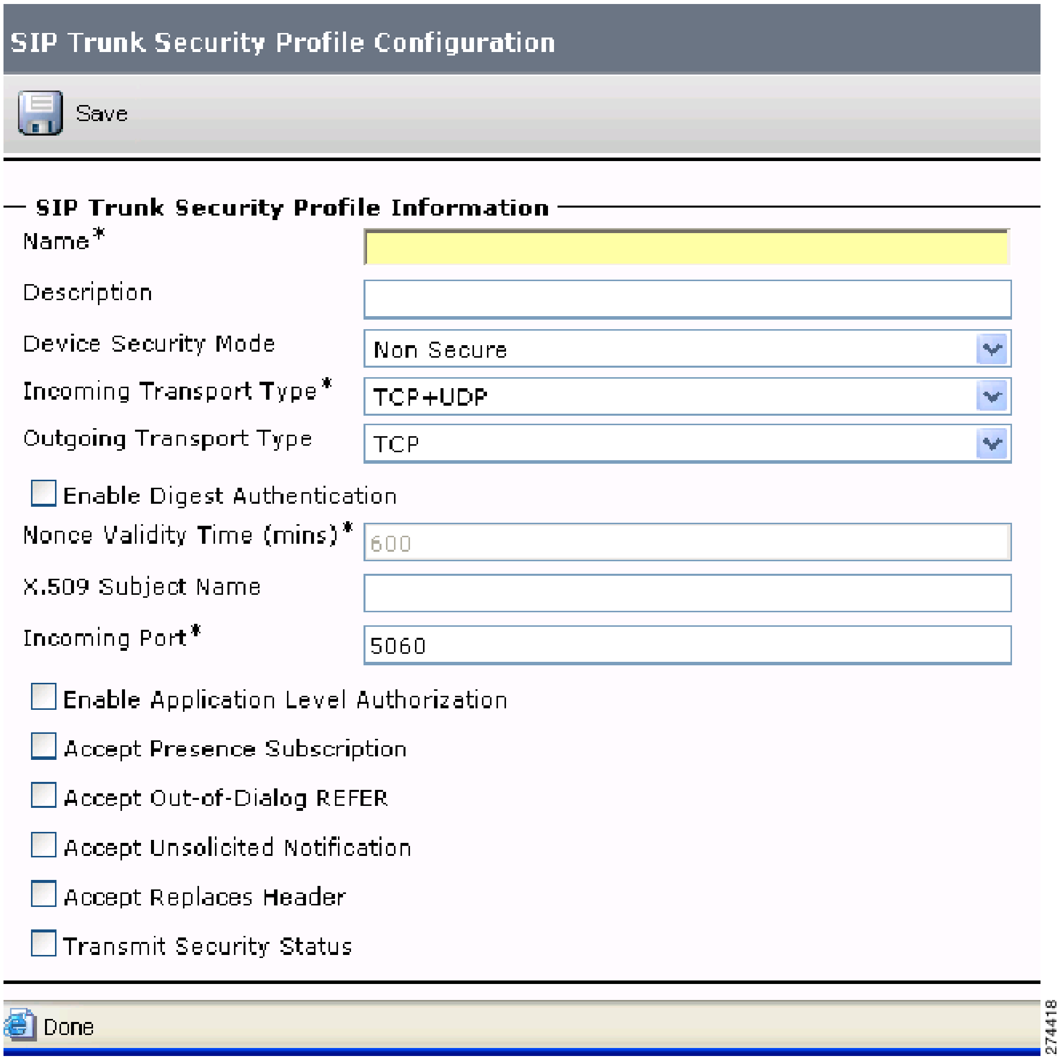
Note A SIP trunk security profile is not required for CTS-Manager or CTRS.

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 3-5.

Figure 3-5 Entering SIP Security Profile Information



SIP Trunk Security Profile Information

Name*

Description

Device Security Mode: Non Secure

Incoming Transport Type*: TCP+UDP

Outgoing Transport Type: TCP

□ Enable Digest Authentication

Nonce Validity Time (mins)*: 600

X.509 Subject Name

Incoming Port*: 5060

□ Enable Application Level Authorization

□ Accept Presence Subscription

□ Accept Out-of-Dialog REFER

□ Accept Unsolicited Notification

□ Accept Replaces Header

□ Transmit Security Status

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 3-10.

- **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 the device and Cisco Unified CM.
- You want audio and video (media) to be secure, but signaling between the device 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. See "Downloading LSCs onto an Infrastructure Device" section on page 3-5).
- **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 a CTMS or a CTRS for SIP Security" section on page 3-12.

- **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 an infrastructure device, complete one of the following:

- Configure security for an existing trunk, go to "Configuring an Existing Trunk for SIP Security" section on page 3-10.

  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 3-11.

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 infrastructure device.
- **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 infrastructure device communications, and you cannot change this port number on the infrastructure device.

- 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 a CTMS or a CTRS for SIP Security" section on page 3-12
- **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 3-11
- Configuring a CTMS or a CTRS for SIP Security, page 3-12

Configuring a New Trunk in Cisco Unified CM

To configure a new trunk in Cisco Unified CM:

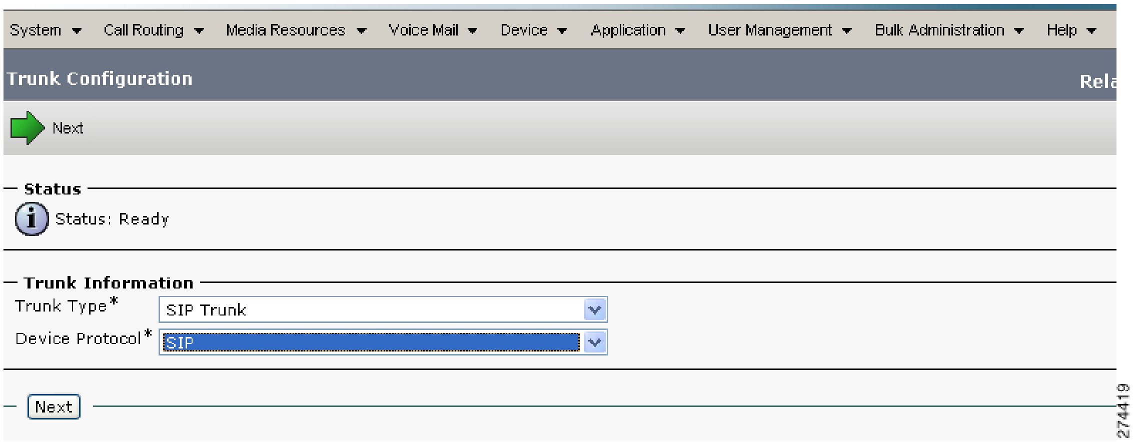
Step 1 From the Cisco Unified CM administration interface, choose **Device** > **Trunk**.

Step 2 Click **Add New**. The Trunk Configuration window displays, as shown in Figure 3-6.

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 3-6 Trunk Configuration Window



Status: Ready

Trunk Type* SIP Trunk

Device Protocol* SIP

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 the infrastructure device.
- **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 infrastructure device communications, and you cannot change this port number on the infrastructure device.

- **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 a CTMS or a CTRS for SIP Security" section on page 3-12.
- **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 a CTMS or a CTRS for SIP Security

To configure SIP security on a CTMS or CTRS, follow these steps:

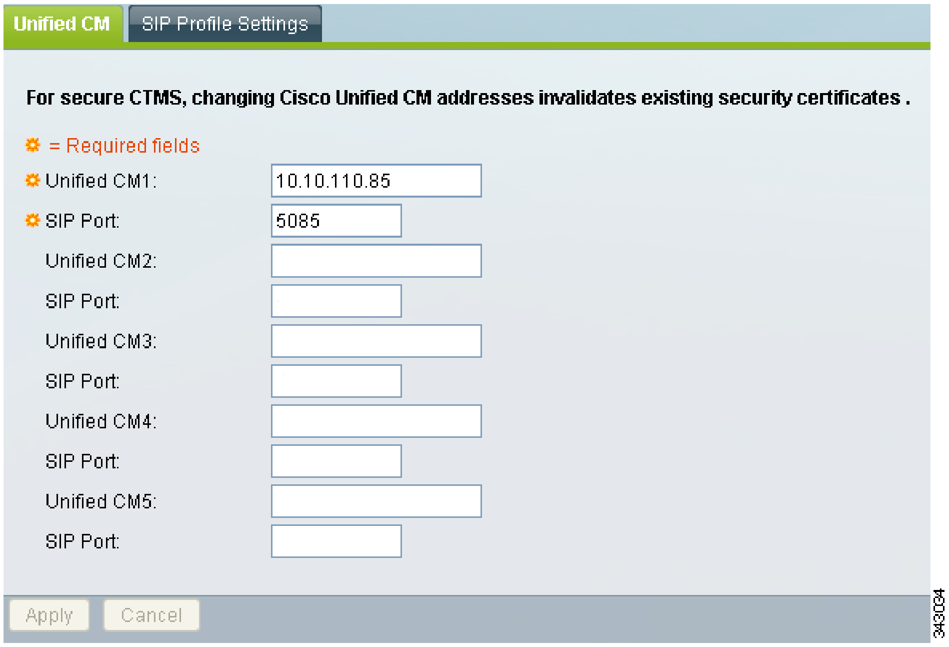
Note This procedure is not required on the CTS-Manager.

Step 1 From the device administration interface, choose **Configure** > **Unified CM**.

Step 2 Enter the following information in the Unified CM tab using Figure 3-7 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 a CTMS or a CTRS for SIP Security" section on page 3-12. 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 a CTMS or a CTRS for SIP Security" section on page 3-12.

Figure 3-7 Cisco Unified CM Settings Example—Cisco Unified CM Tab



For secure CTMS, changing Cisco Unified CM addresses invalidates existing security certificates .

✲ = Required fields

✲ Unified CM1:	10.10.110.85
✲ SIP Port:	5085
Unified CM2:	
SIP Port:	
Unified CM3:	
SIP Port:	
Unified CM4:	
SIP Port:	
Unified CM5:	
SIP Port:	

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.

Configuring the Default Meeting Security Level on a CTMS

To specify the default meeting security level:

Step 1 From the device administration interface, choose **Configure > Security Settings**.

Step 2 In the Meeting Security Policy field, choose either:

- **Secure**—Only secure endpoints can join multipoint meetings.
- **Best Effort**—Both secure and non-secure endpoints can join multipoint meetings.

Step 3 Click **Apply**.

The infrastructure device restarts.

Removing Security from an Infrastructure Device

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 device administration interface.

Note The infrastructure device will automatically restart a few times while removing inter-device security. All active meetings or recordings will be ended when the device restarts. Cisco recommends you perform this task when there are few or no active meetings or recordings.

To remove inter-device security from an infrastructure device:

Step 1 From the Cisco Unified CM administration interface, choose **User Management > Application User**.

a. Click the **Find** button and locate the default device 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 device administration interface, choose **Configure > Unified CM**.

a. Click the **SIP Profile Settings** Tab.

b. From the Device Security drop-down list, choose **Non-Secure**.

Step 3 Choose **Configure** > **Security**.

a. Change the Meeting Security Policy field to **Non-Secure**.

b. Click **Apply**.

c. Click the **Delete All** button to delete all security certificates.

Note On the CTS-Manager, you must select each security certificate individually, and click **Delete**.

The infrastructure device restarts and deletes all security certificates.

What To Do If Inter-Device Certificates Expire or if Cisco Unified CM Server Changes

If the inter-device security certificates expire, or you change the Unified CM server with which the infrastructure device interfaces, you must delete all certificates installed in the infrastructure device, then add new ones. Until you add new certificates, the infrastructure device is not secure, and secure Cisco TelePresence calls cannot be made.

To delete inter-device security certificates from the infrastructure device:

Step 1 From the left navigation in the device administrative interface, click **Configure** > **Security**.

The Security page displays.

Step 2 Click **Delete All**.

Step 3 Select **Configure** > **Unified CM** and select the page **SIP Profile Settings** tab:

- Change Device Security to Non-Secure
- Uncheck the Media Encryption checkbox

Step 4 Return to the **Configure** > **Security** page, click **Delete All** again.

After the certificates are deleted, you must do one of the following:

- If the certificates expired, you must install a new CAPF root certificate, Unified CM root certificate, and LSC. Perform the task described in the "Downloading Certificates from Cisco Unified CM" section on page 1-9, and then in the "Cisco TelePresence Inter-Device Security Infrastructure Device Configuration Checklist" section on page 3-2, perform steps 2-6.
- If the Unified CM server changed, you must set up inter-device security again. In the "Cisco TelePresence Inter-Device Security Infrastructure Device Configuration Checklist" section on page 3-2, perform all steps.

Where to Go Next

See Chapter 4, "Configuring and Verifying Cisco TelePresence Security" to configure inter-device security for Cisco TelePresence endpoints.