



CHAPTER 16

Configuring the Cisco TelePresence Multipoint Switch

Revised June 30, 2011

The following sections describe how to configure the Cisco TelePresence Multipoint Switch:

- [Configuring System Settings, page 16-1](#)
- [Configuring Unified CM Settings, page 16-5](#)
- [Configuring Cisco TelePresence Manager Settings, page 16-6](#)
- [Configuring Meeting Parameters, page 16-8](#)
- [Configuring Security Settings, page 16-11](#)

Additional information about Cisco TelePresence Multipoint Switch configuration is available at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_7/administration/guide/config.html.

Configuring System Settings

You configure system settings for the Cisco TelePresence Multipoint Switch Administration during software setup. The following sections describe how to make changes to the system settings:

- [Configuring IP Settings, page 16-1](#)
- [Editing Route Pattern Settings, page 16-2](#)
- [Configuring QoS Settings, page 16-3](#)
- [Configuring Resource Management, page 16-4](#)
- [About SNMP Settings, page 16-4](#)

Configuring IP Settings

Procedure

To configure the IP settings, do the following procedure:

-
- | | |
|---------------|---|
| Step 1 | From the left navigation pane, choose Configure > System Settings . |
| Step 2 | Click the IP tab. |

A table with IP Settings configuration fields is displayed. [Table 16-1](#) describes the fields.

Step 3 Configure the required IP Setting fields, and then do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Table 16-1 *IP Settings*

Field or Button	Setting
MAC Address	View only. MAC address of the Cisco 7800 Series Media Convergence Server (MCS) on which the Cisco TelePresence Multipoint Switch is located.
Hostname	View only. Hostname configured for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Domain Name	Domain name for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Primary DNS	IP address of the primary Domain Name System (DNS) server for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Secondary DNS	IP address of the secondary Domain Name System (DNS) server for the MCS server on which the Cisco TelePresence Multipoint Switch is located.
Ethernet Card	View only. Ethernet card on the MCU server that connects to the network.
IP Address	IP address of the Cisco TelePresence Multipoint Switch. Note After changing the IP address, close your browser window, and then log in to the Cisco TelePresence Multipoint Switch again using your new IP address.
Subnet Mask	Subnet mask associated with the IP Address.
Default Gateway	Default gateway IP address for the Cisco TelePresence Multipoint Switch.

Editing Route Pattern Settings

Route pattern settings define route patterns (strings of digits that can direct calls for specific systems) and access numbers that are associated with the Cisco TelePresence Multipoint Switch. All of the settings on the Route Pattern window match the comparable field settings that you configure for the Cisco Unified Communications Manager (Unified CM).

Procedure

To edit the route pattern settings, do the following procedure:

- Step 1** From the left navigation pane, choose **Configure > System Settings**.
- Step 2** Click the **Route Pattern** tab.

The Route Pattern window is displayed. [Table 16-2](#) describes the fields.

Step 3 Modify the route pattern settings as required, and then do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Table 16-2 *Route Pattern Settings*

Field or Button	Setting
Route Pattern Start	Defines the first number in your route pattern as configured in Cisco Unified CM.
Route Pattern End	Defines the last number in your route pattern as configured in Cisco Unified CM.
Access Number	Displays the first number in the route pattern as defined in Cisco Unified CM. The Cisco TelePresence Multipoint Switch (CTMS) automatically chooses the first number in the range. The access number serves as the dial-in number for all scheduled meetings. This number also acts as the caller ID when the CTMS dials out for ad hoc meetings. Note The access number cannot be used for static meetings.
Access Name	Descriptive name for the access number as defined in Cisco Unified CM. The maximum number of characters is 20.

Configuring QoS Settings

Differentiated Services Code Point (DSCP) markings are used by the network to classify traffic priority, enabling a common queuing strategy throughout the network. Quality of Service (QoS) values define the DSCP traffic marking values that are used for network queuing for Cisco TelePresence Systems (CTS) and signaling.



Note

Cisco recommends that the QoS settings for CTMS be consistent with the QoS settings for Unified CM and for Cisco TelePresence Systems endpoints, and that they align with your enterprise-wide queuing strategy.

Procedure

To configure QoS settings, do the following procedure:

Step 1 From the left navigation pane, choose **Configure > System Settings**.

Step 2 Click the **QoS** tab.

A table with QoS Settings configuration fields is displayed.

Step 3 Choose from the drop-down list or enter the following values for the QoS settings:

- DSCP for CTS Media—**CS5(precedence 5) DSCP (101000)**
- DSCP for CUCV Media—**AF41 DSCP (100010)**

- DSCP for Signaling—**CS5(precedence 5) DSCP (101000)**

Step 4 After choosing the QoS settings, do one of the following:

- To register new or modified settings, click **Apply**.
- To restore the original settings, click **Cancel**.

Configuring Resource Management

Procedure

To configure or edit Resource Management settings, do the following procedure:

- Step 1** From the left navigation pane, choose **Configure > System Settings**.
- Step 2** Click the **Resources** tab.
- A table with the Resources configuration fields is displayed. [Table 16-3](#) describes the fields.
- Step 3** For the Maximum Segments setting, enter a value of **48**.
- Step 4** For the Adhoc Segments setting, enter a value of **48**.
- Step 5** After entering the settings, do one of the following:
- To register new or modified settings, click **Apply**.
 - To restore the original settings, click **Cancel**.

Table 16-3 Resource Management Settings

Field or Button	Setting
Maximum Segments	Defines the total number of table segments (individual video displays) that the Cisco TelePresence Multipoint Switch supports. Enter a value of 48.
Adhoc Segments	Defines the maximum number of table segments that are available for impromptu meetings. Enter a value of 48.
Schedulable Segments	View only. Displays the number of table segments that are available at any one time for scheduled meetings. Cisco TelePresence Multipoint Switch automatically derives this value by subtracting the defined number of Ad Hoc Table Segments from the defined number of Maximum Table Segments.

About SNMP Settings

You configure all SNMP settings through the Cisco TelePresence Multipoint Switch command line interface.

SNMP monitors the system status (choose Monitoring > System Status for system status details). You can designate a particular server on which the system gathers and stores SNMP trap messages. Configuration requires username and password authentication.

By default, the system enables the SNMP service and the following SNMP settings:

- SNMPv3 username set to **mrtg**.
- SNMPv2c username set to **public**. This name is for internal use of the system and should not be deleted.



Caution

Do not delete the SNMPv2c and SNMPv3 usernames that are set by the system.



Note

By default, the system does not configure a trap receiver. Use CLI commands to configure SNMP trap receiver information.

For additional information about configuring SNMP on the Cisco TelePresence Multipoint Switch, see the *Cisco TelePresence Multipoint Switch Release 1.7 Administration Guide*, at http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_7/administration/guide/CTMS_Release1_7.html.

The Cisco TelePresence Multipoint Switch MIBs are listed at <ftp://ftp-sj.cisco.com/pub/mibs/supportlists/ctms/ctms-supportlist.html>.

Configuring Unified CM Settings

The following sections describe how to make changes to the Cisco Unified Communications Manager (Unified CM) settings by using the Cisco TelePresence Multipoint Switch administration user interface:

- [Configuring Unified CM Settings, page 16-5](#)
- [Configuring SIP Profile Settings, page 16-6](#)

Configuring Unified CM Settings

You must configure an entry for each Unified CM server in the cluster. Additionally, you must configure an entry for each of the Cisco TelePresence Exchange System call engine servers, and configure an entry for the session border controller ingress interface.

Procedure

To configure Unified CM settings, do the following procedure:

- Step 1** From the left navigation pane, choose **Configure > Unified CM**.
- Step 2** Click the **Unified CM** tab.
A table with the Unified CM configuration fields is displayed. [Table 16-4](#) describes the fields.
- Step 3** Configure the Unified CM settings, and then do one of the following:
 - To register new or modified settings, click **Apply**.
 - To restore the original settings, click **Cancel**.

Table 16-4 Unified CM Settings

Field or Button	Setting
Unified CM 1 through 5	Hostnames or IP address(es) of the Unified CM server. Note Enter either the hostname or IP address of the two call engines of the Cisco TelePresence Exchange System in the first two fields. In the third field, enter the ACE virtual IP (VIP).
SIP Port	Port number for Cisco Unified SIP IP Phones that are using UDP to listen for SIP messages from Unified CM. The default setting is 5060.

Configuring SIP Profile Settings

Procedure

To configure SIP Profile settings, do the following procedure:

-
- Step 1** From the left navigation pane, choose **Configure > Unified CM**.
- Step 2** Click the **SIP Profile Settings** tab.
- Step 3** From the Transport Layer Protocol drop-down list, choose **TCP**.
- Step 4** Do one of the following:
- To register new or modified settings, click **Apply**.
 - To restore the original settings, click **Cancel**.
-

Configuring Cisco TelePresence Manager Settings

The Cisco TelePresence Manager (CTS Manager) manages Cisco TelePresence Multipoint Switch resources for scheduled meetings.

This section describes the settings that are necessary to build the communication channel between the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager by using the Cisco TelePresence Multipoint Switch administration user interface.

Procedure

To configure Cisco TelePresence Manager settings, do the following procedure:

-
- Step 1** From the left navigation pane, choose **Configure > CTS Manager**.
- A table with the CTS Manager configuration fields is displayed. [Table 16-5](#) describes the fields.
- Step 2** Configure the CTS Manager settings as necessary, and then do one of the following:
- To register new or modified settings, click **Apply**.
 - To restore the original settings, click **Cancel**.
-

Table 16-5 *Cisco TelePresence Manager Settings*

Field or Button	Setting
Description	Text describing or identifying this particular Cisco TelePresence Multipoint Switch. The maximum number of characters for this field is 62.
Time Zone	Indicates the time zone in which the Cisco TelePresence Multipoint Switch is located. CTS Manager uses this setting to identify the closest Cisco TelePresence Multipoint Switch for all scheduled Cisco TelePresence endpoints. Select the appropriate time zone from the Time Zone drop-down list.
User	Username that is used by Cisco TelePresence Multipoint Switch web services to communicate with CTS Manager. Note Usernames must be at least 5 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown. Note You must configure the same username and password on both the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager.
Password	Password that is used by Cisco TelePresence Multipoint Switch web services to communicate with CTS Manager. Note Passwords must be at least 5 characters, but not more than 64 characters in length, and can contain upper and lower case alphanumeric characters and the underscore and dash characters. Note You must configure the same username and password on both the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager.
Host	IP address or hostname of the Cisco TelePresence Manager.
Dial Plan	The following fields define the dialing system that the Cisco TelePresence Multipoint Switch and Cisco TelePresence Manager use to establish intercompany communication telepresence meetings.
Site Access Code	Defines the dialed numbers that are prepended to a Cisco TelePresence endpoint extension number to create a fully qualified domain name (FQDN) in a Cisco Unified CM cluster.
Inter Site Access Code	Defines the dialed prefix that is used to reach another site within the same company in a Cisco Unified CM cluster.
External Access Code	Defines the dialed prefix that is dialed from within a company to reach a local outside line.
National Dialing Digits	Defines the specific digits used to place a national call. For example, in the United States, the national dialing digit is 1.
International Dialing Digits	Defines the specific digits used to place an international call. For example, in the United States, the international dialing digits are 011.
Directory Number	The following fields define the E.164 numbering plan that is used for intercompany communication.

Table 16-5 Cisco TelePresence Manager Settings (continued)

Field or Button	Setting
Country Code	A unique set of digits that are used to identify a specific country as part of an E.164 number, as defined by the International Telecommunications Union (ITU). The country code can consist of 1, 2, or 3 digits.
National Destination Code	A unique set of digits that identify a specific national destination (area code) as part of an E.164 number, as defined by the International Telecommunications Union (ITU).
Local Number	A unique set of digits that identify a subscriber as part of an E.164 number, as defined by the International Telecommunications Union (ITU).
Registration Status	View only. Status of the registration between the Cisco TelePresence Multipoint Switch and the Cisco TelePresence Manager that is defined in the host entry.

Configuring Meeting Parameters

The following topics describe the configurations necessary on the Cisco TelePresence Multipoint Switch to support Meet-Me meetings and static meetings:

- [Configuring the Meet-Me User, page 16-8](#)
- [Creating Static Meetings, page 16-9](#)
- [Static Meeting Fields, page 16-10](#)

Configuring the Meet-Me User

To enable the two minute warning functionality for Meet-Me meetings, you must create a specific Meet-Me user and password on the Cisco TelePresence Multipoint Switch.

Procedure

To create the Meet-Me user and password, do the following procedure:

- Step 1

From the left navigation pane, choose **Configure > Access Management**.
The Access Management window displays a summary of current users.
- Step 2

To add a new user, click **New**.
The New User entry window appears.
- Step 3

Enter **meetme** in the User Name field.



Note Beginning with Cisco TelePresence Exchange System Release 1.0(3), you can enter a user name of your choice rather than entering **meetme**.

- Step 4

Enter **ciscotxbu** in the Password field.



Note Beginning with Cisco TelePresence Exchange System Release 1.0(3), you can enter a password of your choice rather than entering **ciscotxbu**.

- Step 5** To confirm the password, enter the password again.
- Step 6** Check the **Conference-Scheduler** role check box.
- Step 7** To save new or modified settings, click **Apply**.

Creating Static Meetings

Static meetings are permanently available after you configure them. Each static meeting has its own associated meeting number, which the meeting attendees dial to attend the static meeting. You can also add participants to a static meeting through the Active Meetings page.

Static meetings must be contiguous values within a range of numbers such as 4085551000 through 4085551009.



Note On the Cisco TelePresence MSE 8000 Series, static meetings are called permanent meetings. On the Cisco TelePresence Exchange System, static meetings are called standing meetings.

You must configure two separate ranges for static meetings and interop meetings. You do not need to configure interop meetings at this point; however, the parameters for configuring interop meetings are seen in [Table 16-6](#).



Note You must enter the same range of static meeting (and interop meeting numbers) when you add a new CTMS resource to the Cisco TelePresence Exchange System by using the Administration Console. See the [“Configuring CTMS Resources”](#) section on page 9-6.

Before You Begin

Ensure that you have one contiguous range of access numbers that you can use for static meetings.

Procedure

To create a static meeting, do the following procedure:

- Step 1** From the left navigation pane, choose **Manage > Static Meetings**.
The Static Meetings window displays all previously-configured static meetings.
- Step 2** To add a static meeting entry, click **New**.
The Static Meetings entry window is displayed. [Table 16-6](#) describes the fields.
- Step 3** Enter values in the New Static Meetings window.
- Step 4** To save new or modified settings, click **Apply**.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each static meeting entry.

Static Meeting Fields

Table 16-6 *Static Meeting Field Descriptions*

Field or Button	Description
Access Number	Defines the phone number that participants call to attend this static meeting.
Meeting Description	Text describing or identifying this static meeting. The maximum number of characters for this field is 62 characters.
Switching Policy	Defines how Cisco TelePresence Multipoint Switch calls display during a meeting. Cisco TelePresence Multipoint Switch displays active speakers on screen. There are two active speaker display options; click the appropriate radio button to select: • Speaker—Each speaker is displayed on the screen as that speaker becomes the active speaker. • Room—All table segments for a particular room display on screen when any speaker in that room becomes the active speaker. If you are running CTS 1.3 or later, you can control how Cisco TelePresence calls display from the Cisco TelePresence phone interface. Press the Speaker softkey to display the active speaker; press the Room softkey to display all table segments from a particular room.
Maximum Rooms	Defines the maximum number of Cisco TelePresence rooms that can dial in to in a static multi-point meeting. The range for this setting is from 2 to 48.
Video Announce	When a new attendee joins the meeting, the new attendee appears on the screen for 2 seconds. Options are Yes and No .
Hosted Meeting	Identifies one room as the host for a meeting; other meeting rooms are not added to the meeting until the host room dials in. When you select Video Announce as an option, each meeting room is displayed in 2-second intervals in the order in which they join the meeting. Options are Yes and No. Click the appropriate radio button to select.
Host Room Number	Defines the host Cisco TelePresence System room number.
Interop	Determines whether the Cisco TelePresence Multipoint Switch handles interop meetings. Click the No radio button. Cisco TelePresence Server MSE 8710 and Cisco TelePresence MCU MSE 8510 manage interop meetings in the Cisco TelePresence Exchange Solution. Interop meetings include any standards-based H323 and ISDN endpoints.

Table 16-6 **Static Meeting Field Descriptions (continued)**

Field or Button	Description
Quality	This field sets the maximum default video quality for multipoint meetings: • Highest Detail, Best Motion: 1080p • Highest Detail, Better Motion: 1080p • Highest Detail, Good Motion: 1080p • High Detail, Best Motion: 720p • High Detail, Better Motion: 720p • High Detail, Good Motion: 720p The default is Highest Detail, Best Motion: 1080p
Meeting Security Policy	Click the appropriate radio button to select: Secure—Only secure Cisco TelePresence systems (and secure audio add-in attendees) can join this meeting; if non-secured Cisco TelePresence systems try to join, they are rejected. If a non-secure audio attendee joins the meeting (Conf/Join from the phone UI), that CTS will be dropped from the meeting. Non-Secure—Any Cisco TelePresence system can join the meeting. Best-Effort—The meeting is secure as long as all CTS and audio add-in attendees are secure. The meeting is downgraded to non-secured if a non-secured CTS or audio-add-in joins the meeting.

Configuring Security Settings

Cisco TelePresence Multipoint Switch provides support for secure communication between Cisco TelePresence devices by 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 by using LSCs, Unified CM Root Certificates, and a CAPF Root Certificate.

To configure Cisco TelePresence Multipoint Switch for security, complete the following steps from the Unified CM administration window:

1. Activate and start the CAPF service.
2. Create application users.
3. Create Cisco Unified CM root certificates for every Unified CM server that is associated with the Cisco TelePresence Exchange System.
4. Create a CAPF root certificate.

After configuring security, complete the following steps from the Cisco TelePresence Multipoint Switch Security Settings window:

1. Upload the applicable Unified CM and CAPF root certificates.
2. Download the appropriate LSCs.

When all certificates are in place and the LSC is downloaded, the Cisco TelePresence Multipoint Switch reboots so that the security settings can take effect.

Security setting configuration is described in the following topics:

- [Configuring CAPF Profiles on Unified CM, page 16-12](#)
- [Creating a SIP Trunk Security Profile, page 16-13](#)
- [Downloading CAPF Root Certificates from Unified CM, page 16-14](#)
- [Downloading Root Certificates from Unified CM, page 16-14](#)
- [Uploading CAPF Certificates, page 16-14](#)
- [Downloading LSC to Cisco TelePresence Multipoint Switch, page 16-15](#)
- [Setting Cisco TelePresence Multipoint Switch as Secure, page 16-15](#)

Configuring CAPF Profiles on Unified CM

Procedure

To configure CAPF profiles for the Cisco TelePresence Multipoint Switch, do the following procedure from the Unified CM administration software:

-
- Step 1** Browse to `https:// <Unified CM-server-name>:[8443]/ccmadmin/showHome.do`.
- For the Unified CM server, you can enter either its server name (if DNS is active) or its IP address. Optionally, you can also specify the port number (8443).
- Step 2** From the Unified CM administration window, enter the username and password that you specified during Unified CM installation.
- Step 3** Click **Login**.
- Step 4** To create an application user in Unified CM, do the following:
- a. In the administration window, from the **User Management** drop-down menu, choose **Application User**.
 - b. Click **Add New**.
- The Application User Information window appears.
- c. Enter data in all necessary fields.
- Ensure that the user is included in the Standard CTI Enabled group, the Standard CTI Secure group, and the Standard CTS Secured Connection role under Permission Information.
- d. To save your changes, click **Save**.
 - e. Repeat [Step 4a](#) to [Step 4d](#) to create an application user for each Cisco TelePresence Multipoint Switch in your network.
- Step 5** To create an Application User CAPF profile in Unified CM, do the following:
- a. In the administration window, from the **User Management** drop-down menu, choose **Application User CAPF Profile**.
 - b. Click **Add New**.
 - c. From the Application User drop-down list, choose the application user that you created in [Step 4](#) and enter the appropriate CAPF profile fields for that user:

- Instance ID—Enter a unique identifier (alphanumeric) for each Cisco TelePresence Multipoint Switch.
- Certificate Operation—Choose **Install/Upgrade**.



Note Certificate Operation resets automatically to No Pending Operation after the system downloads a certificate. You must reset this field to Install/Upgrade for additional certificate downloads.

- Authentication String—Enter the value of **123456**.
 - Key size—Leave this field with the default value of **1024**.
- To save your configuration, click **Save**.
 - To create an Application User CAPF Profile for each Cisco TelePresence Multipoint Switch in your network, click **Copy**, and then increment the Instance ID value by one for each Cisco TelePresence Multipoint Switch.

Creating a SIP Trunk Security Profile

Procedure

To create a SIP trunk security profile, do the following procedure:

- Step 1** Choose **System > Security Profile > SIP Trunk Security Profile**.
- Step 2** To add a new profile, click **Add New** at the bottom of the page or click the + sign at the top of the page.
- Step 3** Enter the settings as indicated in [Table 16-7](#) to configure the SIP trunk security profile.
- Step 4** To save your configuration, click **Save**.

Table 16-7 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string that identifies this SIP trunk security profile.
Description	—	Enter a text string that describes this SIP trunk security profile.
Device Security Mode	Yes	Drop-down list. Choose Encrypted .
Incoming Transport Type	Yes	TCP will be entered automatically.
Outgoing Transport Type	Yes	Drop-down list. Select TCP .
X.509 Subject Name	Yes	Enter the subject name of the Cisco TelePresence Multipoint Switch Root Certificate.
Incoming Port	Yes	Enter 5060 for non-secure trunk. If using SIP security, enter a different unused port (such as 5275).

Downloading CAPF Root Certificates from Unified CM

Procedure

To download the CAPF root certificate from Unified CM, do the following procedure:

-
- Step 1** In the **Cisco Unified OS Administration** in Cisco Unified CM, from the Security drop-down menu, choose **Certificate Management**.
 - Step 2** To display a list of certificates, click **Find**.
 - Step 3** Find the CAPF Root Certificate (for example, CAPF.der), and click the hypertext link for that certificate.
 - Step 4** To download the certificate, click **Download** and follow the download instructions.
 - Step 5** Save the CAPF Root Certificate to your desktop with the following name: **CAPF.der**.
-

Downloading Root Certificates from Unified CM

Procedure

To download Root certificates from Unified CM, do the following procedure:

-
- Step 1** In the **Cisco Unified OS Administration** in Cisco Unified CM, from the Security drop-down menu, choose **Certificate Management**.
 - Step 2** To display a list of certificates, click **Find**.
 - Step 3** Find the Cisco Unified CM Root Certificate (for example, CallManager.der), and click the hypertext link for that certificate.
 - Step 4** To download the certificate, click **Download** and follow the download instructions.
 - Step 5** Save the Cisco Unified CM Root Certificate for the Publisher as **CUCM0.der**.



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

Uploading CAPF Certificates

Procedure

To upload CAPF certificates to the Cisco TelePresence Multipoint Switch, do the following procedure from the Cisco TelePresence Multipoint Switch administration software:

-
- Step 1** From the Cisco TelePresence Multipoint Switch administration window, choose **Configure > Security**.
 - Step 2** At the Security window, click **Upload**.
 - Step 3** In the Certificate Upload panel that appears, do the following:
 - a. From the Unit drop-down list, choose **CAPF-Trust**.

- b. From the Category drop-down list, choose **TRUST**.
- c. Select the CAPF Root certificate that you downloaded from Cisco Unified CM (**CAPF.der**).
- d. To upload the file onto the Cisco TelePresence Multipoint Switch, click **Upload**.

The newly uploaded file appears on the Security window.

Downloading LSC to Cisco TelePresence Multipoint Switch

Before You Begin

Create the application user and application user CAPF profile.

Upload the CAPF profile to the Cisco TelePresence Multipoint Switch.

Procedure

To download the LSC to the Cisco TelePresence Multipoint Switch, do the following procedure:

-
- Step 1** From the Cisco TelePresence Multipoint Switch administration window, choose **Configure > Security**.
 - Step 2** At the Security window, click **Download LSC**.
 - Step 3** In the panel that appears, do the following:
 - a. In the CAPF Instance ID field, enter the CAPF instance ID that you created in Unified CM.
 - b. In the CAPF Auth String field, enter the CAPF Auth String that you created in Unified CM.
 - c. In the TFTP Server Host field, enter the Unified CM TFTP server host.
 - d. In the TFTP Server Port field, enter **69**, which is the default value.
 - e. In the CAPF Server Host field, enter the Unified CM CAPF server host.
 - f. In the CAPF Server Port field, enter **3804**, which is the default value.
 - Step 4** To download LSC, click **Download LSC**.
- After the LSC successfully downloads, the Cisco TelePresence Multipoint Switch reboots automatically.
-

Setting Cisco TelePresence Multipoint Switch as Secure

Procedure

To set the Cisco TelePresence Multipoint Switch as secure, do the following procedure:

-
- Step 1** Choose **Configure > Cisco Unified CM**.
The Unified CM window is displayed.
 - Step 2** Click the **SIP Profile Settings** tab.
 - Step 3** From the Device Security drop-down list, select **Non-Secure**.
 - Step 4** From the Transport Layer Protocol drop-down list, choose **UDP**.
 - Step 5** To save your changes, click **Apply**.

Step 6 After reading the notice that is displayed, click **OK**.
