CHAPTER 4

Configuring CTMS Administration Software

Revised: February 25, 2009, OL-12906-03

Contents

Overview

The following sections describe the System Configuration parameters for the Cisco TelePresence Multipoint Switch (CTMS). System Configuration is divided into the following areas:

- System Settings, page 4-2
- Cisco Unified Communications Manager Settings, page 4-14

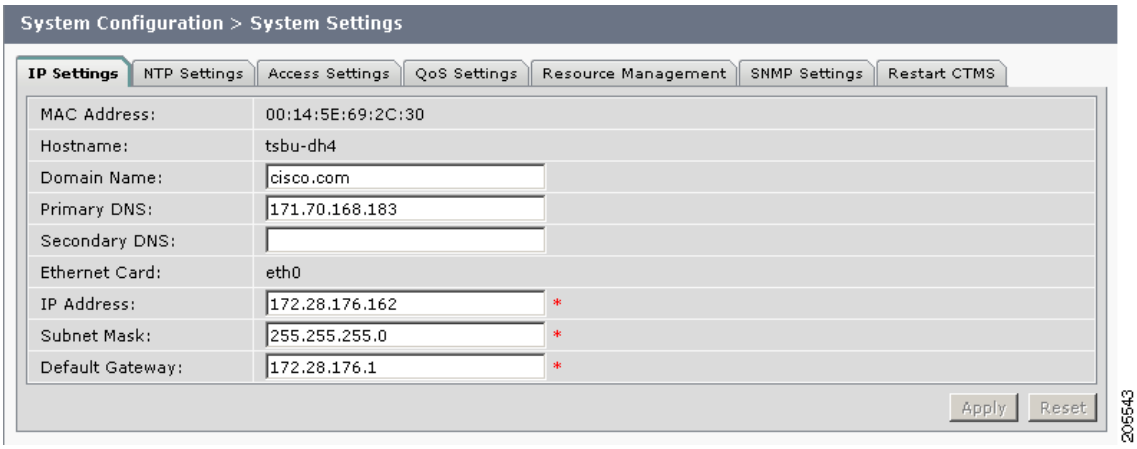
System Settings

System Settings are initially configured during Cisco TelePresence Multipoint Switch (CTMS) Administration software set up. Use the System Settings to make changes to these initial settings. System Settings consists of four configuration areas:

Editing IP Settings

Figure 4-1 shows the IP Settings screen.

Figure 4-1 IP Settings



To edit IP settings:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane.

Click the ***IP Settings*** tab. IP Settings screen displays a table providing the IP Settings fields. Some of the settings displayed on the IP Settings screen are configured during initial installation of the Cisco TelePresence Multipoint Switch Administration software. The following fields can be configured on this screen:

- Domain Name

- Primary DNS
- Secondary DNS
- IP Address
- Subnet Mark
- Default Gateway

Step 2 Edit settings (as needed) as described in Table 4-1

Table 4-1 IP Settings

Field or Button	Setting
MAC Address	(View only) MAC address of the MCU device on which the Cisco TelePresence Multipoint Switch is located.
Hostname	(View only) Hostname configured for the MCU device on which the Cisco TelePresence Multipoint Switch is located.
Domain Name	(View only) Domain name in which the MCU device on which the Cisco TelePresence Multipoint Switch is located.
Primary DNS	(View only) IP address of the primary Domain Name System(DNS) server for the MCU device on which the Cisco TelePresence Multipoint Switch is located.
Secondary DNS	(View only) IP address of the secondary Domain Name System (DNS) server for the MCU device on which the Cisco TelePresence Multipoint Switch is located.
Ethernet Card	(View only) Ethernet card being used on the MCU server to connect to the network.
IP Address	IP address of the Cisco TelePresence Multipoint Switch. **Note** After changing the IP address, close your browser window, then log into CTMS again using your new IP address.
Subnet Mask	Subnet mask of the Cisco TelePresence Multipoint Switch.
Default Gateway	Default gateway IP address for the Cisco TelePresence Multipoint Switch.

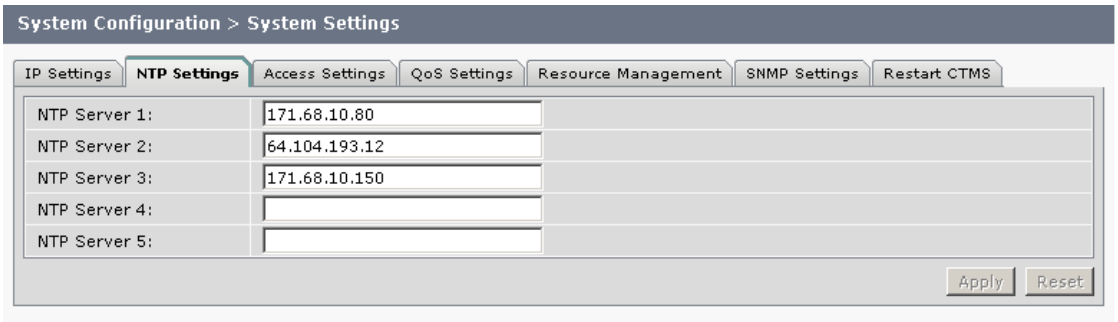
- To register new or modified settings, click ***Apply***.
- To restore the original settings, click ***Reset***.

Editing NTP Settings

Network Time Protocol (NTP) is used to synchronize the clocks on Cisco IP telephony servers with an external network time server that uses NTP.

Figure 4-1 shows the NTP Settings screen.

Figure 4-2 NTP Settings



To edit NTP settings:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane.

Click the ***NTP Settings*** tab to list the configured IP address of the NTP servers.

Step 2 Edit settings (as needed) as described in Table 4-2

Table 4-2 NTP Settings

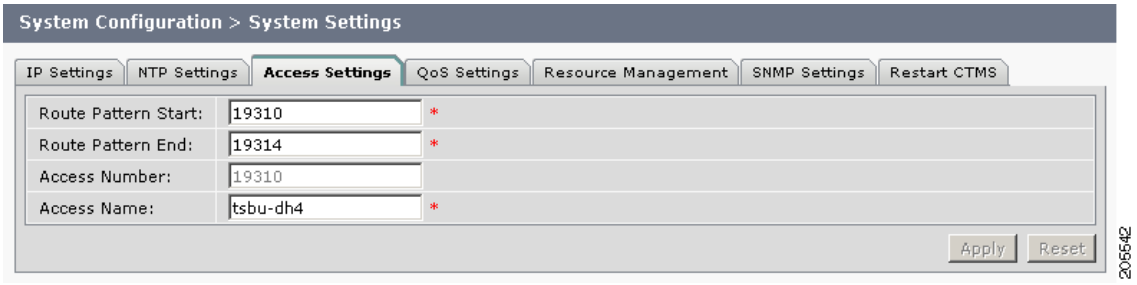
Field or Button	Setting
NTP Server 1-5	IP address of the NTP server. To add an NTP server to the configuration, type the IP address in an NTP Server field. To change an NTP server in the configuration, highlight and delete the IP address in the NTP Server field and type in the new address.

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

Editing Access Settings

Figure 4-3 shows the Access Settings screen.

Figure 4-3 Access Settings



To edit Access settings:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane.

Step 2 Click the ***Access Settings*** tab. Access Settings displays a table providing the Access Settings configuration fields. All of the settings on the Access Screen are derived from settings you configured in Cisco Unified Communications Manager (Cisco Unified CM).

Edit settings (as needed) as described in Table 4-3

Table 4-3 Access Settings

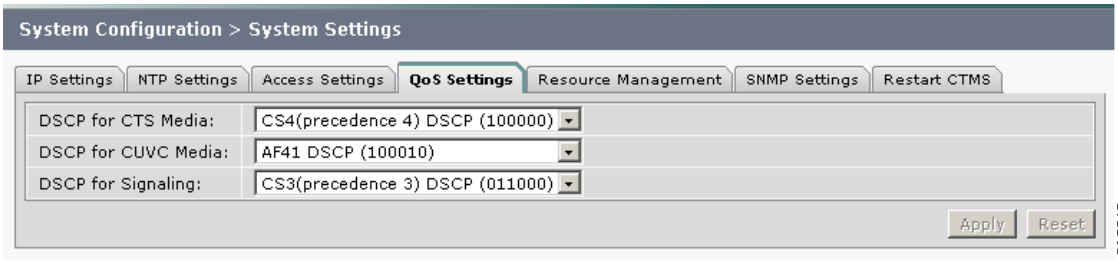
Field or Button	Setting
Route Pattern Start	Defines the first number in your defined route pattern as configured in Cisco Unified CM.
Route Pattern End	Defines the last number in your defined route pattern as configured in Cisco Unified CM.
Access Number	Displays the first number in the route pattern as defined in Unified CM. CTMS Administration software automatically selects that number as the access number. That number is used for scheduled meetings and cannot be used for static meetings.
Access Name	Descriptive name for the access number. Maximum number of characters is 20.

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

Configuring and Editing QoS Settings

Figure 4-4 shows the QoS Settings screen.

Figure 4-4 QoS Settings



To configure or edit QoS settings:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane to open the **System Settings** window.

Step 2 Click the ***QoS Settings*** tab. QoS Settings displays a table providing the QoS Settings configuration fields.

Enter or edit settings (as needed) as described in Table 4-4

Table 4-4 QoS Settings

Field or Button	Setting
DSCP for Media	Traffic marking values for voice and video traffic used for network queuing. Available settings are: • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 DSCP (011010) • AF32 DSCP (011100) • AF33 DSCP (011110) • AF41 DSCP (100010) • AF42 DSCP (100100) • AF43 DSCP (100110) • CS1 (precedence 1) DSCP (001000) • CS2 (precedence 2) DSCP (010000) • CS3 (precedence 3) DSCP (011000) • CS4 (precedence 4) DSCP (100000) • CS5 (precedence 5) DSCP (101000) • CS6 (precedence 6) DSCP (110000) • CS7 (precedence 7) DSCP (111000) • Default DSCP (000000) • EF DSCP (101110) The default value for this field is CS4 (precedence 4) (100000). It is recommended that you use the default value for this field.

Table 4-4 QoS Settings

Field or Button	Setting
DSCP for Signaling	Traffic queuing techniques that define per-hop behavior based on the Differentiated Services Code Point (DSCP) value in the IP header of a packet. control stream Available settings are: • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 DSCP (011010) • AF32 DSCP (011100) • AF33 DSCP (011110) • AF41 DSCP (100010) • AF42 DSCP (100100) • AF43 DSCP (100110) • CS1 (precedence 1) DSCP (001000) • CS2 (precedence 2) DSCP (010000) • CS3 (precedence 3) DSCP (011000) • CS4 (precedence 4) DSCP (100000) • CS5 (precedence 5) DSCP (101000) • CS6 (precedence 6) DSCP (110000) • CS7 (precedence 7) DSCP (111000) • Default DSCP (000000) • EF DSCP (101110) The default value for this field is CS3 (precedence 3) (011000). It is recommended that you use the default value for this field.

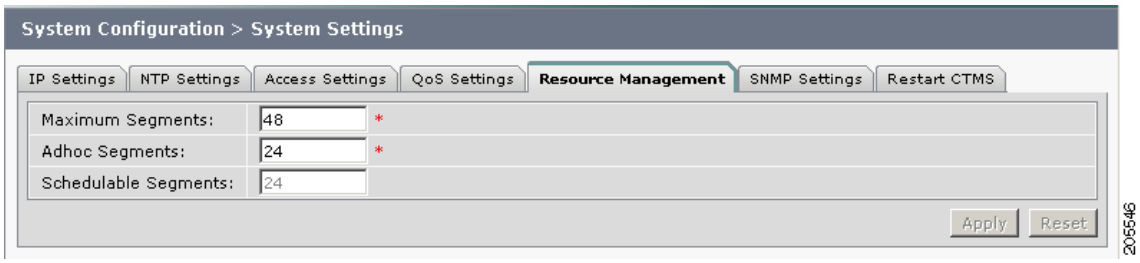
- To register new or modified settings, click ***Apply***.
- To restore the original settings, click ***Reset***.

Note We recommend that you use the same Quality settings for CTSM that you have configured in Cisco Unified Communications Manager for Cisco TelePresence Systems endpoints.

Configuring and Editing Resource Management

Figure 4-5 shows the Resource Management Settings screen.

Figure 4-5 Resource Management Settings



To configure or edit Resource Management settings:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane.

Step 2 Click the ***Resource Management*** tab. Resource Management displays a table providing the Resource Management Settings configuration fields.

Enter or edit settings (as needed) as described in Table 4-5

Table 4-5 Resource Management Settings

Field or Button	Setting
Maximum Segments	Defines the total number of table segments (individual video displays) this CTMS handles. Maximum number is 48.

Table 4-5 Resource Management Settings (continued)

Field or Button	Setting
Adhoc Segments	Defines the maximum number of table segments available for impromptu meetings. By defining the number of table segments available for adhoc meetings, you ensure that there will be sufficient table segments available for scheduled meetings. Maximum number is 48. **Note** Combined total for Schedulable Table Segments and Ad hoc Table Segments cannot exceed 48. **Note** In Interop calls (meaning that the teleconference includes both CTS and legacy teleconferencing (Cisco Unified Video Conferencing (CUVC)), CUVC occupies one segment per call. Segment use is dependent on the number of Interop calls; for example, if there are three on-going Interop calls, then three CTMS segments will be used to establish calls to CUVC.
Schedulable Segments	(View only) This field displays the number of table segments available at any one time for scheduled meetings; CTMS automatically derives this value by subtracting the defined number of Ad Hoc Table Segments from the defined number of Maximum Table Segments.

Note If you do not have Cisco TelePresence Manager installed, all table segments must be ad hoc.

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

Configuring and Editing SNMP Settings

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices; it enables network administrators to manage network performance, find and solve network problems, and plan for network growth by analyzing information gathered using MIBs. You configure all SNMP settings through the CTMS command line interface (CLI) commands.

With SNMP for CTMS, you first enable (or disable) SNMP; when you enable SNMP, you turn on the SNMP daemon so CTMS is registered with SNMP (SNMP can then begin monitoring CTMS and gathering data). You can also designate a particular server where SNMP trap messages are gathered and stored. Both of these configuration steps require separate username and password authentication.

By default, SNMP service is disabled. Once SNMP is enabled, the following default SNMP settings are also enabled:

- One SNMP username set to “admin.” This name cannot be changed.
- SNMP service password set to “snmppassword.” The password should be changed.
- No trap receiver is configured. Use CTMS CLI commands to configure SNMP trap receiver information.

Figure 4-6 shows the SNMP Settings screen. All fields in this screen are read-only.

Figure 4-6 SNMP Settings

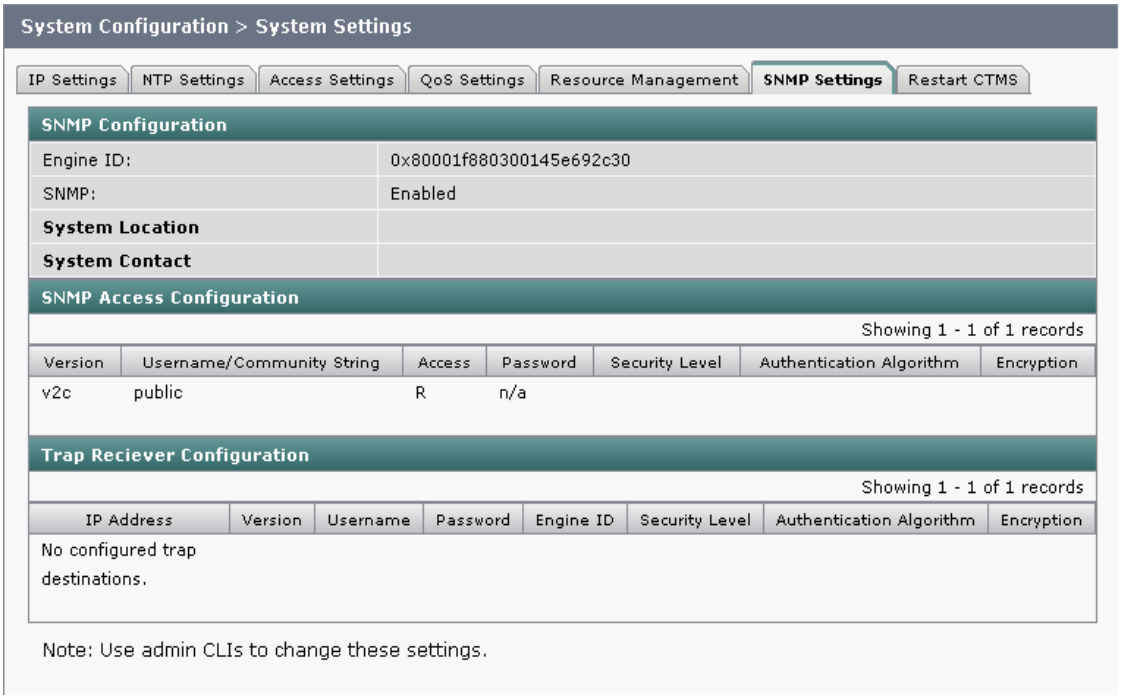


Table 4-6 describes the SNMP fields.

Table 4-6 SNMP Settings

Field or Button	Setting
Engine ID	(View only) The engine ID for the SNMP agent on this Cisco TelePresence Multipoint Switch. This number is usually based on the CTMS MAC address. If you configure the trap receiver, this engine ID is used to create a trap user on the trap receiver system and to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
SNMP	(View only) Shows whether SNMP is enabled or disabled.
System Location	(View only) Physical location of the SNMP system associated with CTMS.

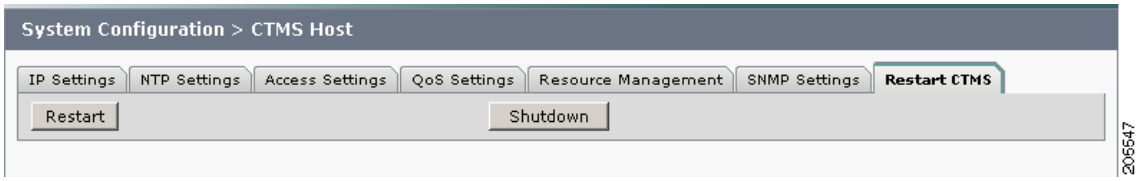
Table 4-6 SNMP Settings

Field or Button	Setting
System Contact	(View only) Name of the SNMP system contact associated with CTMS.
SNMP Access Configuration	
Version	(View only) Lists the configured SMNP version, either 3 or 2C.
User Name/ Community String	(View only) SNMP server username.
Access	(View only) Indicates whether the access is read, writer or read/write.
Current Password	(View only) SNMP server password. The password must be 8 characters long. Enter it twice for verification.
Security Level	(View only) Level of security supported by the SNMP server.
Authorization Algorithm	(View only) Authentication algorithm supported by the SNMP server. Currently only MD5 algorithm is supported.
Encryption	(View only) Encryption used for SNMP requests.
Trap Receiver Configuration	
IP Address	(View only) IP address or hostname of the SNMP trap receiver (the remote SNMP system) where SNMP traps will be sent.
Version	(View only) Lists the configured SNMP version, either 3 or 2C.
User Name	(View only) Username used to access the system where SNMP traps are received. **Note** SNMP trap user names can be from 1 to 32 characters.
Current Password	(View only) Password used to access the system where SNMP traps are received.
Engine ID	(View only) Engine ID to use for trap; default is system engine ID.
Security Level	(View only) Level of security supported by the SNMP Trap Receiver.
Authentication Algorithm	(View only) Authentication algorithm supported by the SNMP Trap Receiver. Currently only MD5 algorithm is supported.
Encryption	(View only) Encryption used for SNMP requests.

Restarting CTMS

Figure 4-7 shows the Restart CTMS screen.

Figure 4-7 Restart CTMS Settings



To restart CTMS or to shutdown CTSM:

Step 1 Click ***System Settings*** under the **System Configuration** folder in the Navigation Pane.

Step 2 Click the ***Restart CTMS*** tab.

Step 3 Click ***Restart*** to restart—meaning shutdown and then reboot—CTMS.

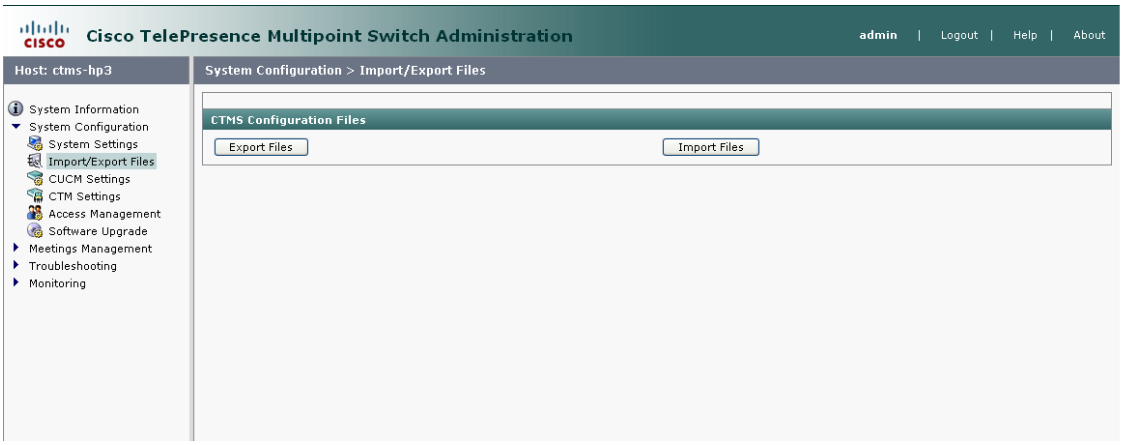
Step 4 Click ***Shutdown*** to completely shutdown CTMS.

Importing and Exporting Files

Import/Export Files enables you to reuse previously defined user and configuration files (such as meeting templates) when upgrading to a new version of CTMS Administration Software. To reuse previously defined user and configuration files, you must first export the files to a secure location, upgrade to the new version of CTMS Administration software, and then import the files.

Figure 4-8 shows the Restart CTMS screen.

Figure 4-8 Import/Export Files Settings



To import or export files:

Step 1 Click ***Import/Export Files*** under the **System Configuration** folder in the Navigation Pane.

Step 2 Click ***Export Files*** to export configuration files.

Step 3 Click ***Import Files*** to import defined user and configuration files. Click ***Browse*** to select the exported user and configuration files, then click ***Install Config Files*** to unzip and install the files.

Cisco Unified Communications Manager Settings

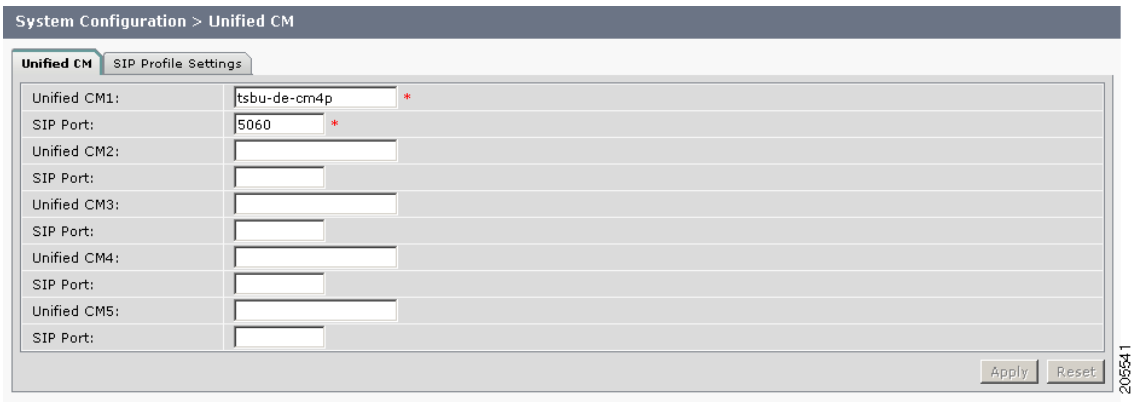
Cisco Unified Communications Manager Settings (Cisco Unified CM) consists of two configuration areas:

- Configuring and Editing Cisco Unified CM Settings, page 4-14
- Configuring and Editing SIP Profile Settings, page 4-15

Configuring and Editing Cisco Unified CM Settings

Figure 4-9 shows the Cisco Unified CM Settings screen.

Figure 4-9 Cisco Unified CM Settings



To configure or edit Cisco Unified CM settings:

Step 1 Click ***Cisco Unified CM Settings*** under the **System Configuration** folder in the Navigation Pane.

Step 2 Click the ***Cisco Unified CM Settings*** tab. Cisco Unified CM Settings displays a table providing the Cisco Unified CM Settings configuration fields. Enter settings (as needed) as described in Table 4-7

Table 4-7 Cisco Unified CM Settings

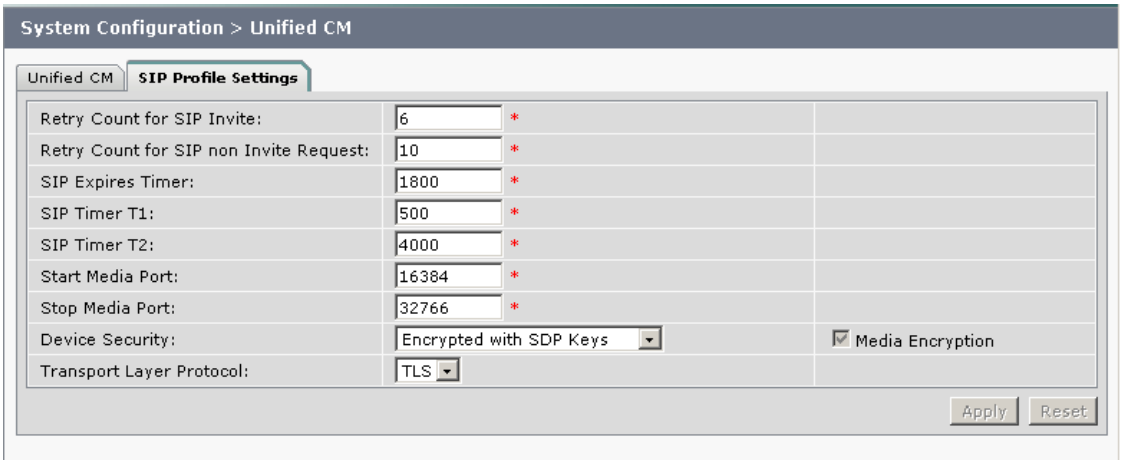
Field or Button	Setting
Cisco Unified CM 1 through 5	Hostnames or IP address(es) of the Cisco Unified Communications Manager (Cisco Unified CM) server. **Note** It is important to add all Cisco Unified CM servers in the cluster.
SIP Port	Port number for Cisco Unified SIP IP Phones that are using UDP to listen for SIP messages from Cisco Unified CM. The default setting equals 5060.

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

Configuring and Editing SIP Profile Settings

Figure 4-10 shows the SIP Profile Settings screen.

Figure 4-10 SIP Profile Settings



To configure or edit SIP Profile settings:

Step 1 Click ***Cisco Unified CM Settings*** under the **System Configuration** folder in the Navigation Pane to open the **Cisco Unified CM Settings** window.

Step 2 Click the ***SIP Profile Settings*** tab. SIP Profile Settings displays a table providing the SIP Profile Settings configuration fields.

Enter or edit settings (as needed) as described in Table 4-8

Table 4-8 SIP Profile Settings

Field or Button	Setting
Retry Count for SIP Invite	Specifies the number of times that Cisco Unified Communications Manager (Cisco Unified CM) will re-send the INVITE message. This is a required field. Minimum is 1. Maximum is 10 Default is 6.
Retry Count for SIP non-Invite Request	Specifies the number of times that Cisco Unified CM will re-send the non-INVITE message. This is a required field. Minimum is 1. Maximum is 10 Default is 6.
SIP Expires Timer	Specifies the maximum time that an INVITE message remains valid. If Cisco Unified CM has not received an answer before this timer expires, Cisco Unified CM tears down the call. This is a required field. Minimum is 60000 (msec). Maximum is 300000 (msec). Default is 180000 (msec).
SIP Timer T1	Specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.
SIP Timer T2	Specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.
Start Media Port	Designates the start real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 16384.
Stop Media Port	Designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 32766.
Device Security	Specifies the type of security applied to this CTMS. Available choices are: • Non-Secure (with media encryption if the ***Media Encryption*** check box is checked.) • Encrypted without SDP Keys for 6.1.2 Cisco Unified CM • Encrypted with SDP Keys for 7.0 Cisco Unified CM For more information about Device Security, see Security Settings.
Media Encryption	Click this check box if you want to have non-secure SIP signaling mode but with encrypted media.
Transport Layer Protocol	Defines the transport protocol used. Available choices are: • TCP • UDP Transport Layer Security (TLS) is automatically selected or filled in when "Encrypted with SDP Keys" or "Encrypted without SDP Keys" is chosen for Device Security. **Note** Whenever the transport type is modified in CTMS, the corresponding transport type for the Cisco Unified CM trunk setting must be changed to match the CTMS transport type.

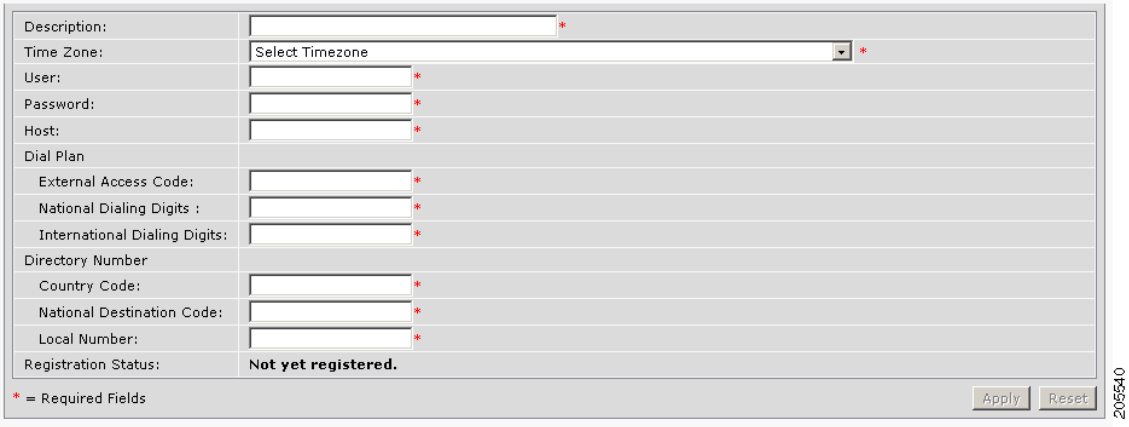
- To register new or modified settings, click ***Apply***.
- To restore the original settings, click ***Reset***.

Configuring and Editing Cisco TelePresence Manager Settings

These setting are used to register CTMS with Cisco TelePresence Manager (CTS-Man) for scheduled meetings.

Figure 4-11 shows the Cisco TelePresence Manager Settings screen.

Figure 4-11 Cisco TelePresence Manager Settings



To configure or edit CTS-Manager settings:

Step 1 Click ***CTM Settings*** under the **System Configuration** folder in the Navigation Pane to open the **CTM Settings** window.

Step 2 CTM Settings displays a table providing the Cisco TelePresence Manager Settings configuration fields.

Enter or edit settings (as needed) as described in Table 4-9

Table 4-9 Cisco TelePresence Manager Settings

Field or Button	Setting
Description	Text describing or identifying this particular CTMS. The maximum number of characters for this field is 62 characters.
Time Zone	Indicates the time zone in which the CTMS is located. Click “Time Zone” to display the list of available time zone options. Click option to highlight and select.

Table 4-9 Cisco TelePresence Manager Settings

Field or Button	Setting
User	Username with which CTMS web services communicates 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** User name and password configured on the CTMS and CTS-Man need to be the same.
Password	Password with which CTMS web services communicates 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. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown. **Note** User name and password configured on the CTMS and CTS-Man need to be the same.
Host	IP address or host name of the CTS-Man.
Dial Plan	The following fields define the dialing system CTMS and CTS-Man use to establish intercompany communication TelePresence meetings.
External Access Code	Defines the dialed prefix from within a company to reach a local outside line.
National Dialing Digits	Defines the specific digit(s) used to place a national call. For example, in the United States, the national dialing digit is "1."
International Dialing Digits	Defines the specific digit(s) 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 used for intercompany communication.
Country Code	A unique set of digits 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 used to 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 used to 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 CTMS and CTS-Man defined in the host entry.

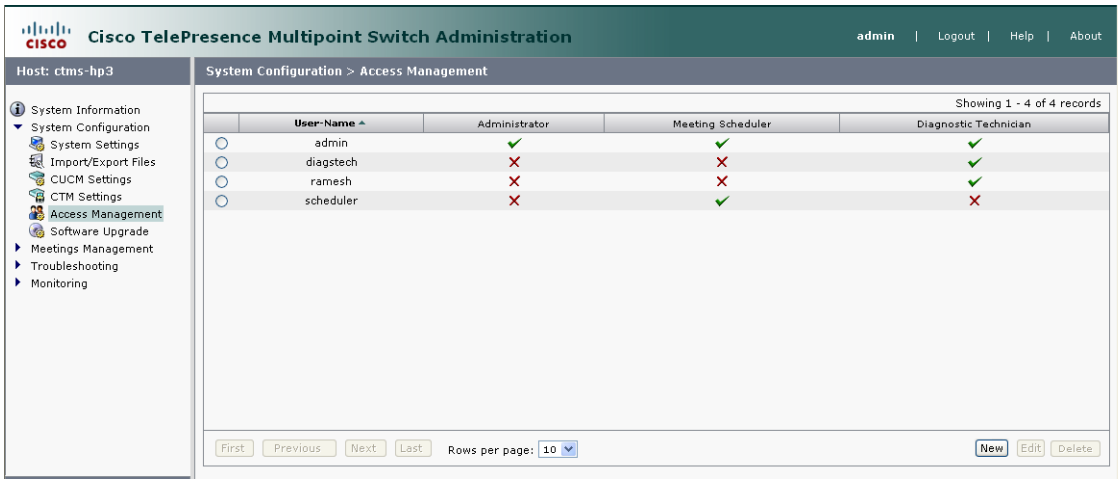
- To register new or modified settings, click ***Apply***.
- To restore the original settings, click ***Reset***.

Configuring and Editing Access Management

CTMS administration software recognizes three different administrative roles; access to task folders is dependent on defined administrative roles. So, administrative roles are considered a form of access management and are defined using Access Management settings.

Figure 4-12 shows the Access Management screen.

Figure 4-12 Access Management



To configure or edit Access Management settings:

Step 1 Click ***Access Management*** under the **System Configuration** folder in the Navigation Pane to open the **Access Management** window.

Step 2 Access Management initially displays a table providing the following information about already-defined users as described in Table 4-10.

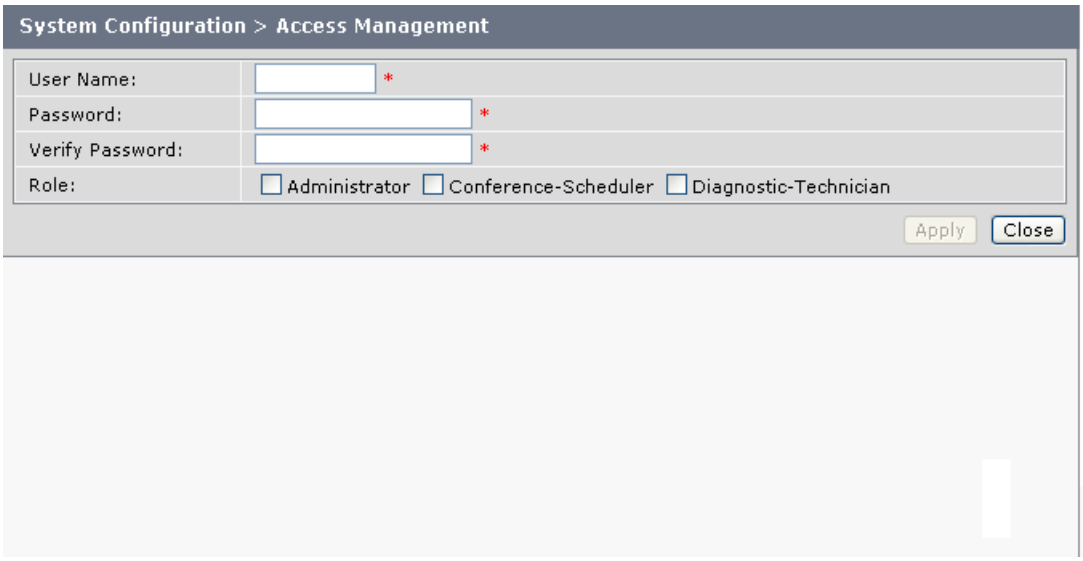
Table 4-10 Access Management Table Field Descriptions

Field	Description
User-Name	Username of a specific CTMS user.
Administrator	Administrators have the authority to perform all tasks associated with CTMS, including configuring system settings, managing multipoint meetings, maintaining, monitoring and troubleshooting CTMS. Administrators have access to all folders in CTMS Administration software. A green check in this field indicates that the selected user has been designated as an administrator.
Meeting Scheduler	Meeting Schedulers have the authority to perform multipoint meeting management tasks, such as defining meeting templates, and setting up (and breaking down, as necessary) ad hoc, static and scheduled meetings. Meeting Schedulers have access to the Meeting Management folder in CTMS Administration software. A green check in this field indicates that the selected user has been designated as a meeting scheduler.
Diagnostic Technician	Diagnostic Technicians have the authority to perform CTMS monitoring and troubleshooting tasks. Diagnostic Technicians have access to the Troubleshooting and Monitoring folders in CTMS Administration software. A green check in this field indicates that the selected user has been designated as a diagnostic technician.

- To delete one of the defined administrators, click the radio button to the left of the table entry, and then click ***Delete***.
- To edit one of the defined administrators, click the radio button to the left of the table entry, and then click ***Edit***.
- To define a new administrator, click ***New***,

Step 3 When you click ***New*** from the Access Management screen, CTMS Administration software takes you to the New User Settings table as shown in Figure 4-13.

Figure 4-13 New User Settings



Step 4 Enter settings as described in Table 4-11

Table 4-11 New User Settings

Field or Button	Setting
Username	Username identifying a defined role as selected from the Role field. **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. The username must contain letters and numbers, and cannot contain special characters except for the underscore character. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.
Password	Password for the username indicated in the Username field. **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.

Table 4-11 New User Settings

Field or Button	Setting
Verify Password	Re-enter the password defined for this user.
Role	Defines a specific user role. In CTMS Administration software, there are three possible roles, each with specific levels of administrative access: • Administrator: Administrators have access to all screens and configuration tasks in CTMS Administration software. • Conference Scheduler: Conference-Schedulers have access only to the Meeting Management screens and associated configuration tasks in CTMS Administration software. • Diagnostic Technician: Diagnostic Technicians have access only to Monitoring and Troubleshooting screens and one task (system restart) in CTMS Administration software. **Note** A single user can have more than one role. Click the appropriate radio button to select.

- To register new or modified settings, click ***Apply***.
- To close this window without applying settings, click ***Close***.

Step 5 To edit an existing user profile, click the radio button to the left of the table entry to select the user, and then click ***Edit***. When you click ***Edit*** from the Access Management screen, CTMS Administration software takes you to the Edit User Settings table. Enter settings (as needed) as described in Table 4-12

Table 4-12 Edit User Settings

Field or Button	Setting
User-Name	(View only.) Defined role.
Current password	Current password for the user indicated in the User-Name field.
New Password	New password for the user indicated in the User-Name field. **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.
Verify New Password	Re-enter the password defined for this user.

- To register new settings, click ***Save***.
- To close this window without applying settings, click ***Close***.

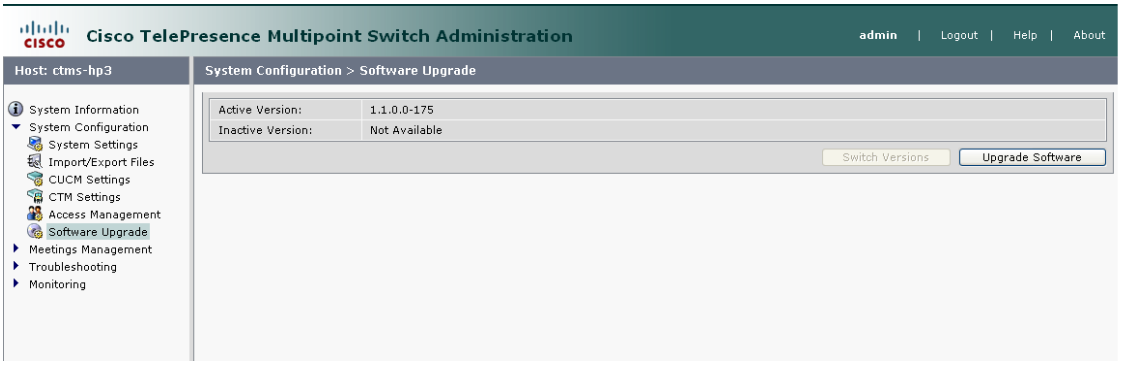
Upgrading Software Version

There are also two functions to assist you in maintaining the system software, as follows:

- Switch Version: The hard drive on the server on which CTMS is installed is partitioned into two areas. Each area can contain a system image. Switch Version allows you to switch the location of two stored versions of the system software.
- Upgrade Software: CTMS provides a patch file for upgrading system software. The Cisco-supplied patch file can be stored on a CD-ROM or a Secure FTP (SFTP) host network. A wizard displays dialog boxes to prompt you through the process.

Figure 4-14 shows the Software Upgrade screen.

Figure 4-14 System Upgrade Screen



To switch software versions:

- Click the **Switch Version** button.

The system will swap the software versions and reboot. Screens will describe activity.

The active partition in the server hard drive contains the active system image. The software versions that are loaded will be displayed in the Active Version and Inactive Version fields.

To upgrade software:

Step 1 To start the software upgrade process, click the **Upgrade Software** button.

The Source Selection dialog box appears.

If you need to stop the software installation, click the ***Cancel*** button when the button is active.

Step 2 Click the ***CD-ROM*** or ***Network*** radio button to choose the location of the patch file.

If you chose CD-ROM, click **Next** to go to the ***File Selection*** window.

If you chose Network, provide the hostname, login username, password, and the path to the patch file. By default, port 22 is used to access the server; supply the correct port number, if required. Click **Next** to go to the ***File Selection*** window.

Step 3 At the ***File Selection*** window, choose the file to load by clicking its radio button. Then click **Next**.

Step 4 The ***Patch File*** Preparation window appears. Watch this window to monitor the progress of the file download. Buttons will be inactive until the patch file is loaded.

Once the file is loaded, the window displays a Confirmation message.

The software wizard displays the software versions that are installed and provides active Yes and No radio buttons so you can choose to switch the newly loaded software to the active partition.

Step 5 Click **Yes** or **No** to make your choice. Then click **Next** to finish the software upgrade task.

The install wizard displays a dialog window that logs the progress of the update.

Step 6 When the log indicates that the files have been switched, click **Finish** to complete this task.

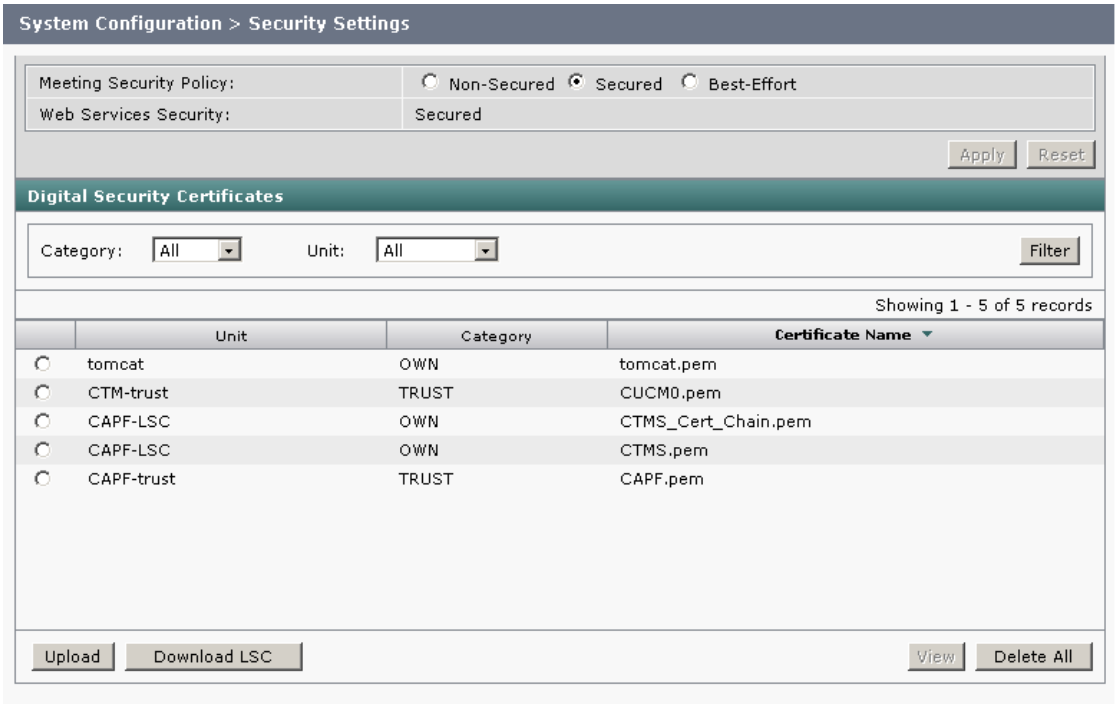
Security Settings

Starting with CTMS Release 1.5, 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.

To configure CTMS for security, you need to first complete preliminary steps in Cisco Unified CM. You must activate and start CAPF service, create application users, create Cisco Unified CM root certificates for every Cisco Unified CM server associated with Cisco TelePresence service, and create a CAPF root certificate. Then from the Security Settings window in CTMS, you 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 CTMS reboots so that the security settings to take effect.

Figure 4-15 shows the CTMS Security Settings screen.

Figure 4-15 Security Settings



To configure CAPF Security for CTMS:

Step 1 **From Cisco Unified CM**: Configure Cisco Unified CM to run in secured mode. For more information, refer to *Cisco Unified Communications Manager Installation Guide for the Cisco TelePresence System Release 1.5*.

Step 2 **From Cisco Unified CM**: Create an application user in Cisco Unified CM. From the ***Cisco Unified CM Administration*** page, select **Application User** from the ***User Management*** drop-down menu. Click **Add New** and then complete all necessary Application User Information fields. Be sure that the user is included in the "Standard CTI Enabled" group, and the "Standard CTI Secure" group and the "Standard CTS Secured Connection" role under Permission Information. When finished, click **Save**.

Note Create an application user for each Cisco TelePresence product (such as CTS, CTMS and CTS-Man) in your network.

Step 3 **From Cisco Unified CM**: Create an Application User CAPF profile in Cisco Unified CM. From the ***Cisco Unified CM Administration*** page, select **Application User CAPF Profile** from the ***User Management*** drop-down menu. Click **Add New**. Select the application user you previously created from the Application User drop-down list and then complete the appropriate CAPF profile fields for that user:

- Instance ID: Unique identifier (alpha-numeric) for the cluster
- Certificate Operation: Select "Install/Upgrade."

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

- Authorization String: Click "Generate String" to get a one-time authorization code to download certificates
- Key size: Default value is 1024.

When finished, click **Save**.

Note Create an Application User CAPF Profile for each CTMS in your network.

Step 4 **From Cisco Unified CM**: Configure SIP Trunk Security in Cisco Unified CM. From the ***Cisco Unified CM Administration*** page, from the ***System*** menu, select **Security Profile** and then **SIP Trunk Security Profile**. Click **Find** to display a list of SIP Trunk Security profiles. Find the appropriate profile and click the hypertext link for that profile. Enter:

- Name: Unique profile name
- Description: Identifying description for this profile
- Device Security Mode: Select "Encrypted"
- Incoming Transport Type: TLS
- Outgoing Transport Type TLS
- X.509 Subject Name: Enter the subject name of the CTMS Root Certificate
- Incoming Port: Unique port number

Note Port 5060 is for the non-secure device security mode.

Click **Save** if you are revising an existing profile; click **Add New** if you are creating a new profile.

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

Step 6 **From CTMS**: Upload the CAPF Root Certificate in CTMS. From the ***Security Settings*** window in CTMS, click **Upload**. Select:

- Unit: CAPF-Trust
- Category: TRUST
- Certificate: Select the CAPF Root certificate that you downloaded from Cisco Unified CM (CAPF.der).

Click **Upload** to upload the CAPF Root certificate.

Step 7 **From Cisco Unified CM**: Download Cisco Unified CM Root Certificate in Cisco Unified CM. From ***Cisco Unified OS Administration*** in Cisco Unified CM, select **Certificate Management** from the ***Security*** drop-down menu. Click **Find** to display a list of certificates. Find the Cisco Unified CM Root

Certificate (for example, CallManager.der), and click the hypertext link for that certificate. Click **Download** and follow the download instructions. 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.

Step 8 **From CTMS**: Upload the Cisco Unified CM Root Certificate(s) in CTMS. From the ***Security Settings*** window in CTMS, click **Upload**. Select:

- Unit: CTM-Trust
- Category: TRUST
- Certificate: Select the Cisco Unified CM root certificate that you created in Cisco Unified CM (CUCM0.der).

Click **Upload** to upload the Cisco Unified CM root certificate.

Step 9 **From CTMS**: Download the LSC in CTMS. After creating the application user and application user CAPF profile, from CTMS, click **Security Settings** to open the ***Security Settings*** window. Click **Download LSC** and fill out the fields:

- CAPF Instance ID: Must match instance ID created in Cisco Unified CM.
- CAPF Auth String: Must match authorization string created in Cisco Unified CM.
- TFTP Server Host: Cisco Unified CM TFTP server.
- TFTP Server Port: Must be 69, which is the default value.
- CAPF Server Host: Cisco Unified CM CAPF server host.
- CAPF Server Port: Must be 3804, which is the default value.

Click **Download LSC**. After the LSC has been successfully downloaded, the CTMS reboots automatically.

Step 10 **From CTMS**: Secure CTMS. From the ***Cisco Unified CM*** window in CTMS, click the **SIP Profile Settings** tab. For Device Security, select either ***Encrypted without SDP Keys for 6.1.2 Cisco Unified CM*** or ***Encrypted with SDP Keys for 7.0 Cisco Unified CM***.

To select the default meeting security level:

Step 1 After the system reboots, you can select the default meeting security level : secure, non-secure or best effort security mode. From the Security Settings window, make the appropriate selection(s) as necessary:

Table 4-13 Security Settings

Field or Button	Setting
Meeting Security Policy	Indicates the meeting security policy for this CTMS. Choices are Secure, Non-Secure, and Best Effort. If no security certificates have been downloaded, CTMS automatically selects "Non-Secure."
Web Services Security	Indicates the web services security policy for this CTMS. This field will display "Secured" when CTMS is secured. This field will display "Non-secured" when CTMS is not secured.

If the security certificates expire, or you change the Cisco Unified CM server with which you are interfacing, you need to delete all security certificates and then add new ones. Until you reestablish new security certificates, you will not be able to make secure Cisco TelePresence calls.

To delete security certificates from a secured CTMS:

Step 1 From the Security settings page, click the **Delete All** button. Follow the appropriate instructions as displayed:

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

Step 2 After you have followed the instructions as displayed, click the **Delete All** button again. Then click **OK** or **Cancel** as appropriate.

Interface Failover

Interface failover provides a backup mechanism for Ethernet adapters. When enabled, the secondary adapter handles all network traffic if the primary adapter or its connection fails.

To enable interface failover:

Step 1 Make sure that the primary Ethernet adapter (Ethernet interface 0) is connected to the network and that its static IP address and gateway parameters were correctly configured during system installation.

Step 2 Connect the secondary Ethernet cable (Ethernet interface 1) to a network switch. The connection port can be on the same switch as Ethernet interface 0 or on a different switch but both Ethernet interface 0 and Ethernet interface 1 must be on the same gateway.

Step 3 From the ***Interface Failover*** window, click the **Enable** button, then click **Apply**.

Note If the **Enable** button is grayed out, check your network connection.

To disable interface failover:

Step 1 With no active meetings in progress, click the **Disable** button.

Step 2 Click **Apply**. Your network adapters will be configured and restarted and the interface failover disabled.

Service Settings

Use ***Service Settings*** to configure an inbound HTTP Proxy for CTMS. The external URL provides CTMS web services for external third-party web service clients in an intercompany communication environment. Enter an HTTP address for the inbound HTTP Proxy in the "External URL" field.

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

Note When you modify the URL and apply the change, WebUI will automatically restart all CTMS processes to have Confgmr/CCS reload the new URL.