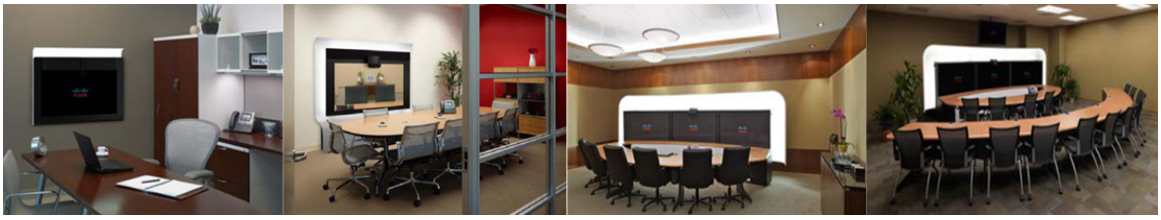


CHAPTER 4

Configuring CTRS Administration Software

October 2011

The following sections describe settings in the System Configuration pages for the Cisco TelePresence Recording Server (CTRS). System Configuration is divided into the following areas:

Logging Into the Administrative Interface

To log in to the CTRS administrative interface, do the following:

Step 1 Open a supported web browser.

Step 2 In the address bar, enter **https://***CTRS_URL***/admin**.

Note You must add **/admin** to the CTRS URL to get to the administrative user interface. If you enter the CTRS URL without appending **/admin**, you go to the Cisco TelePresence Video Portal.

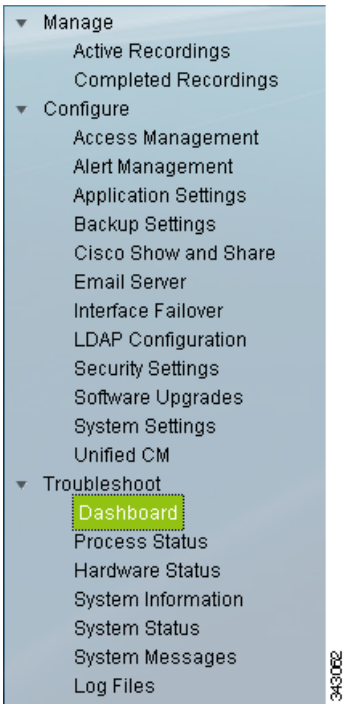
Step 3 Enter your username and password.

For more information about the initial installation of CTRS, including setting the administrator username and password for the first time, see Chapter 3, "Installing CTRS Administration Software."

Left Navigation of the Administrative User Interface

You can access any of the Configure pages from the left navigation in the CTRS user interface (see Figure 4-1):

Figure 4-1 Configure—Left Navigation



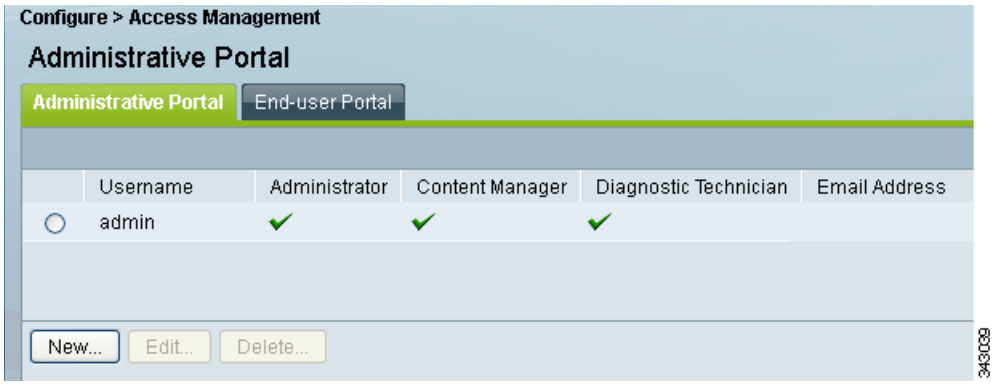
Access Management

Use the fields under Access Management to define CTRS administrators and to provide access to the Cisco TelePresence Video Portal. Access Management is divided into two tabs:

Administrative Portal

In Access Management, click the **Administrative Portal** tab to display or configure CTRS administrative roles (see Figure 4-2).

Figure 4-2 Configure > Access Management—Administrative Portal



Access to task menus within CTRS Administrative software is dependent on defined administrative roles. CTRS administration software recognizes three different administrative roles:

- **Administrator**: Administrators have the authority to perform all tasks associated with configuring, administering, monitoring and troubleshooting CTRS.
- **Content Manager**: Content Managers primarily are responsible for managing activities associated with recording. They can only access CTRS Recording Management and System Status windows.
- **Diagnostic Technician**: Diagnostic Technicians have the authority to perform CTRS monitoring and troubleshooting tasks. They can only access CTRS Troubleshooting and Monitoring windows.

Administrative Portal initially displays a table providing the following information about already-defined administrative users as described in Table 4-1:

Table 4-1 Administrative Portal Table Field Descriptions

Field	Description
User-Name	User-name of a specific CTRS user.
Administrator	Administrators have the authority to perform all tasks associated with CTRS. Administrators have access to all menus in CTRS Administration software. A green check in this field indicates that the selected user has been designated as an administrator.

Table 4-1 Administrative Portal Table Field Descriptions

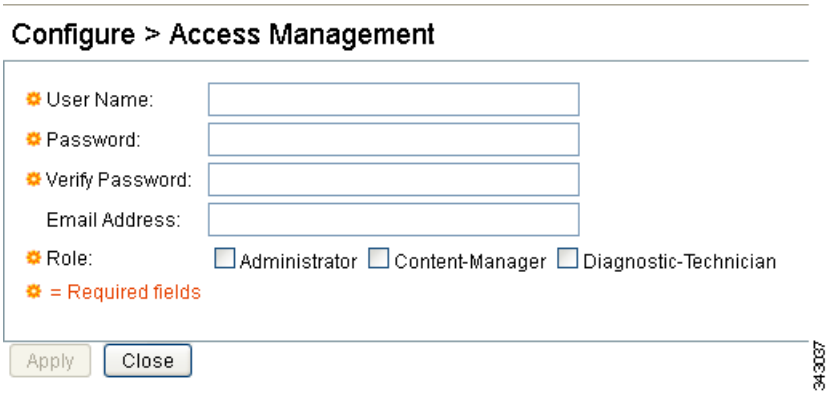
Field	Description
Content Manager	Content managers are responsible for managing activities associated with recording. They can only access CTRS Recording Management and System Status windows. A green check in this field indicates that the selected user has been designated as a content manager.
Diagnostic Technician	Diagnostic Technicians have the authority to perform CTRS monitoring and troubleshooting tasks. Diagnostic Technicians have access to the Troubleshooting and Monitoring windows in CTRS 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 define a new administrator, click **New**.
- To edit one of the defined administrators, click the radio button to the left of the table entry, and then click **Edit**.

Creating a New Administrative User

When you click **New**, a dialog box appears (see Figure 4-3).

Figure 4-3 Configure > Access Management—Administrative Portal (New)



Enter settings as described in Table 4-2.

Table 4-2 New Access Management Settings

Field or Button	Setting
User Name	Username identifying a defined role as selected from the Role field. **Note** A username must be at least 5 characters, but not more than 64 characters in length. The username must contain letters and numbers, but it cannot contain special characters, except for the underscore character. Letters can be uppercase and lowercase. The username cannot be all numbers. The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.
Password	Password for the username indicated in the User name field. **Note** Passwords must be at least 6 characters, but not more than 64 characters.
Verify Password	Re-enter the password defined for this user.
Email Address	Email address for this defined user.
Role	Defines a specific user role. In CTRS Administration software, there are three possible roles, each with specific levels of administrative access: • Administrator: Administrators have access to all pages and configuration tasks in CTRS Administration software. • Content Manager: Content managers are responsible for managing activities associated with recording. They can only access CTRS Recording Management and System Status windows. • Diagnostic Technician: Diagnostic Technicians have access only to Monitoring and Troubleshooting windows and one task (system restart) in CTRS Administration software. **Note** A single user can have more than one role. Click the appropriate radio button(s).

- To register new or modified settings, click **Apply**.
- To close the window, click **Close**.

Note When you add a new administrative user, the CTRS does not validate that administrative user against LDAP. When you add a user, the CTRS ensures that the user exists in LDAP.

Editing a Defined Administrative User

When you click the radio button for a particular administrative user and then click **Edit**, a dialog box appears. Enter settings as described in Table 4-3.

Table 4-3 Edit Administrative User Settings

Field or Button	Setting
User Name	(View only.) Administrative user's user name.
Password	Click this option to change the password for a defined user. **Note** Passwords must be at least 6 characters, but not more than 64 characters in length.
Email Address	Email address for this defined user.

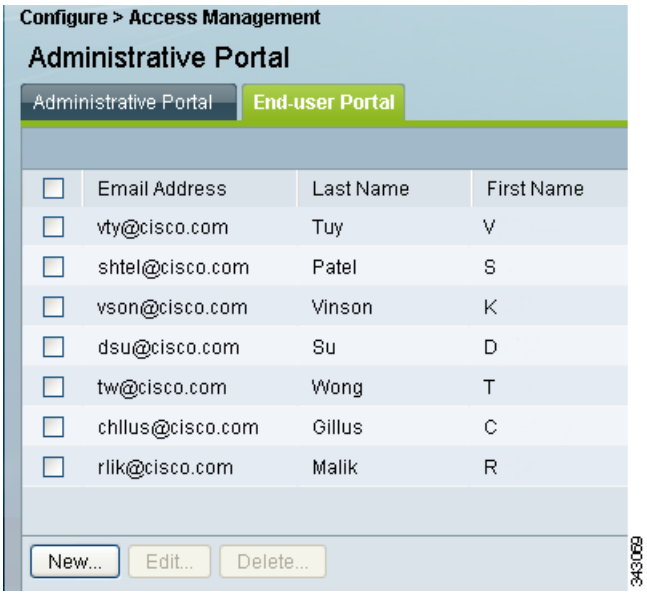
- To register new or modified settings, click **Save**.
- To close the window, click **Close**.

End-User Portal

Note You should configure LDAP servers before you create users for the user portal. To configure LDAP servers, go to System Configuration > LDAP Configuration.

In Access Management, click the **End-user Portal** tab to display or configure users of the user portal (see Figure 4-4).

Figure 4-4 Configure > Access Management—Cisco TelePresence Video Portal



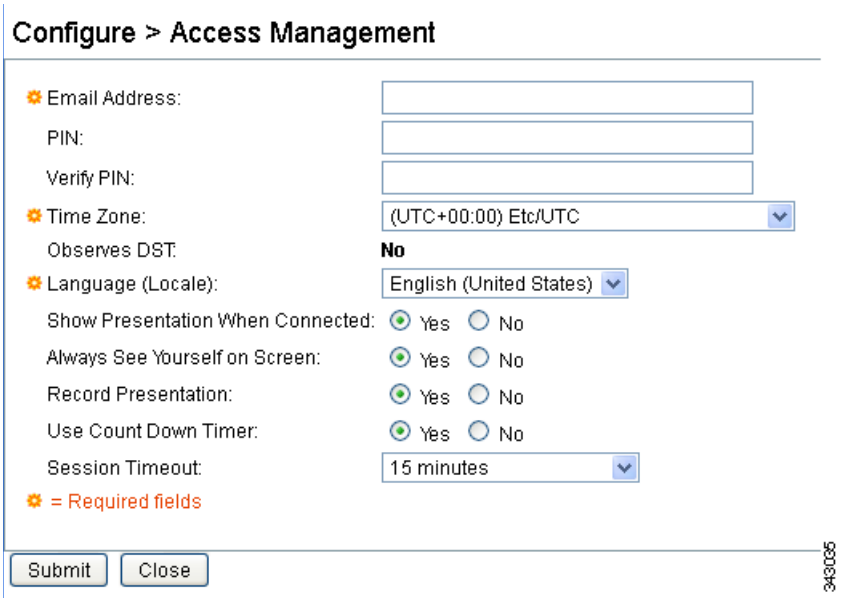
When you click the End-user Portal tab, you see a list of users with access to the Cisco TelePresence Video Portal using an IP phone, Cisco TelePresence 12” device, or through a web browser.

- To sort the list of users by Email Address, Last Name, or First Name, click the respective column header in the Configure > Access Management page, End-user Portal tab.
- To delete a user, click the radio button next to the user email address. Then click **Delete**. All recordings that belong to this user are deleted from the CTRS.
- To edit the settings for a user, click the radio button next to the user email address. Then click **Edit**. After you modify settings, click **Save**.
- To create a new user, click **New**.

Creating a New User or Modifying Settings for an Existing User

When you click **New** or **Edit**, a dialog box appears (see Figure 4-5).

Figure 4-5 Configure > Access Management—End-user Portal (New or Edit)



Enter settings as described in Table 4-4.

Table 4-4 User Settings

Field or Button	Setting
Email Address	Email address of the user.
PIN	Personal identification number for the user. **Note** A PIN must be 6 numbers. Sequential numbers in the PIN must be nonrepeating.
Verify PIN	Re-enter the PIN.
First Name	First name of the user. (This field is not editable, and only appears when editing an existing user account.)

Table 4-4 User Settings (continued)

Field or Button	Setting
Last Name	Last name of the user. (This field is not editable, and only appears when editing an existing user account.)
Time Zone	Time zone in which the user resides.
Observe DST	Whether or not the user's time zone observes Daylight Savings Time.
Language (Locale)	The language spoken by the user.
Show Presentation When Connected	Click **Yes** to display a presentation on a device (for example, a laptop) that is connected to the VGA input or to display a presentation on a document camera. With this setting enabled, the user sees the presentation on the recording screen.
Always See Yourself on Screen	Click **Yes** to display the user in the recording screen. If you click **No**, the camera records the user, but the user does not appear in the screen during recording.
Record Presentation	Click **Yes** to include the presentation in the video.
Use Count Down Timer	Click **Yes** to use the 5-second count-down timer. If you click **No**, the camera begins recording as soon as the user taps Record on the IP phone interface.
Session Timeout	Choose how much time must elapse before the IP phone or Cisco Touch 12 device times out because of inactivity.

- To save the settings for a new user, click **Apply**. To save settings for an existing user, click **Save**.
- To close the dialog box without saving the settings, click **Close**.

Note The CTRS administrator does not have to create user accounts and PINs. Users can create their own accounts and PINs to access the browser-based Cisco TelePresence Video Portal. When users create accounts, they automatically appear in the user list in the End-user Portal tab in the CTRS administrative UI (see Figure 4-4).

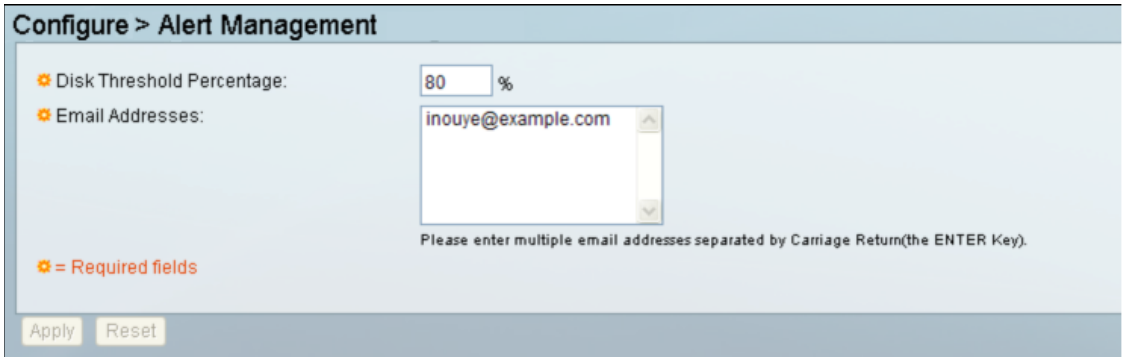
To learn how to create their own accounts, users should read the "Creating and Viewing Recordings with the Cisco TelePresence Recording Server" chapter in the *Cisco TelePresence System User Guide*:

http://www.cisco.com/en/US/docs/telepresence/cts_admin/1_6/userguide/cts1_8_ug.html

Alert Management

Click **Alert Management** in the left menu to display or configure alert management settings (see Figure 4-6).

Figure 4-6 Configure > Alert Management



Use the Alert Management page to define the CTRS disk threshold at which export data (either transfer to archive servers or data deletion) will be sent to the users and the email addresses to which these alerts will be sent. Enter settings as described in Table 4-5

Note To see current disk utilization for media storage, go to Troubleshoot > Hardware Status.

Table 4-5 Alert Management Settings

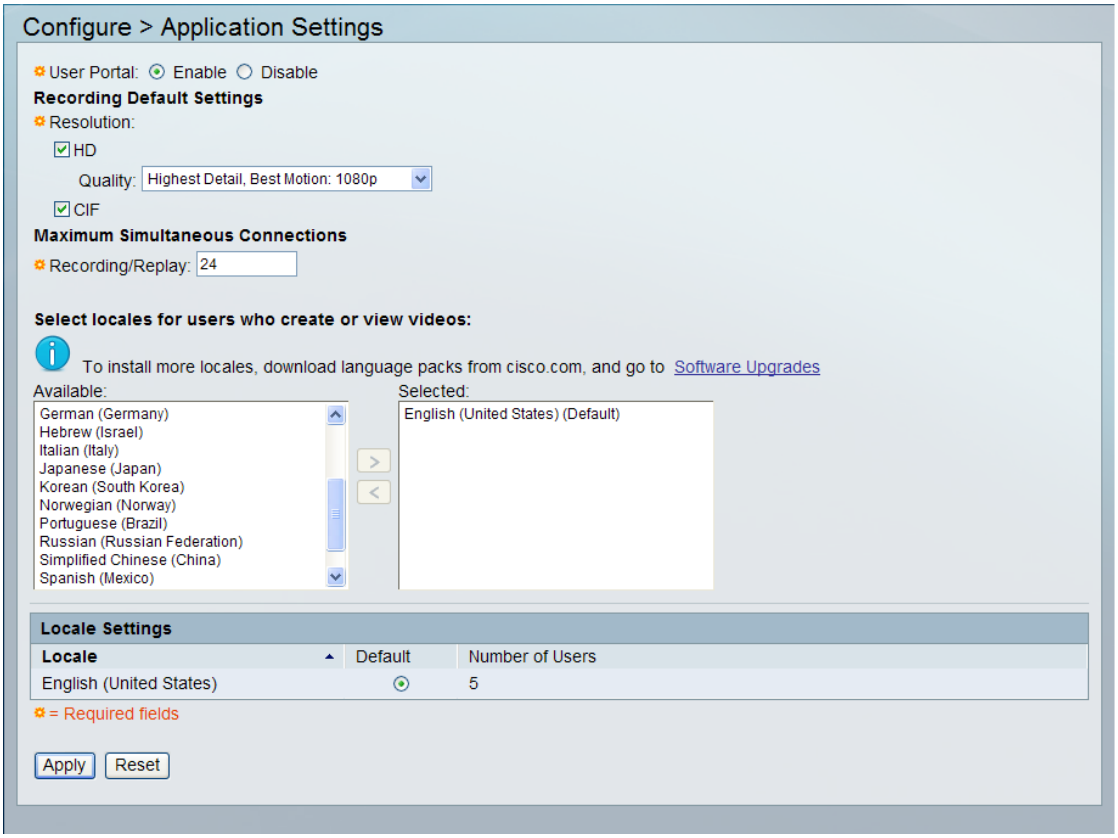
Field or Button	Setting
Disk Threshold Percentage	Enter a percentage. When the disk space reaches this threshold, CTRS sends an alert to the those listed in the Email Addresses field. 80% is the default.
Email Addresses	Enter email addresses. Recipients receive an email when the disk threshold reaches the percentage that is specified in the Disk Threshold Percentage field. **Note** If you want to add more than one email address, press the **Enter** key after you add each address.

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

Application Settings

Click **Application Settings** in the left menu to display or modify application settings (see Figure 4-7).

Figure 4-7 Configure > Application Settings



Application Settings allow you to define general CTRS recording settings (see Table 4-6).

Table 4-6 Application Settings

Field or Button	Setting
User Portal	Click **Enable** to make the Cisco TelePresence Video Portal available to users; click **Disable** to make the portal unavailable. The portal is a browser-based interface containing recordings that were made by or shared with a user. The portal also contains public videos.
Recording Default Settings	
Resolution	Resolution of the CTRS recordings. Options are **HD** and **CIF**. **Note** By default, both HD and CIF are selected.

Table 4-6 Application Settings (continued)

Field or Button	Setting
HD	High Definition. Click checkbox to choose. **Note** CTRS can generate two recording files. The file called "*xxx*_ts.mp4" is for playback on an endpoint. The file called "*xxx*_lo.mp4" is for playback in the browser-based Cisco TelePresence Video Portal. If you uncheck the HD checkbox, the CTRS does not generate the file for playback on an endpoint.
CIF	Common Intermediate Format (CIF). Click checkbox to choose. **Note** CTRS can generate two recording files. The file called "*xxx*_ts.mp4" is for playback on an endpoint. The file called "*xxx*_lo.mp4" is for playback in the browser-based Cisco TelePresence Video Portal. If you uncheck the CIF checkbox, the CTRS does not generate the file for playback in the browser-based Cisco TelePresence Video Portal.
Quality	Defines the recording quality. Choices are: • Highest Details, Best Motion: 1080p • Highest Details, Better Motion: 1080p • Highest Details, Good Motion: 1080p • High Detail, Best Motion: 720p • High Detail, Better Motion: 720p • High Detail, Good Motion: 720p • High Detail, Limited Motion: 720P (Lite) Highlight option to choose. Default value is **Highest Detail, Best Motion: 1080p**. If the CTS is in 720p Lite mode, the CTRS generates only the HD version of the recording, not the CIF version. Used for playback on an endpoint, the HD version filename includes "ts" (*xxx*_ts.mp4).
Maximum Simultaneous Connections	
Recording/Replay	Defines the number of simultaneous recording and replaying sessions that can occur. Range is from 1 to 24. Default is **24**.
Select locales for users who create or view videos	
Available and Selected locales	By default, English (United States) is the selected as well as the default locale. The Available and Selected windows allow you to select more locales that are available to users who create videos using Studio Mode and Event Recording and view videos using the Cisco TelePresence Video Portal. **Note** Currently, language packs are not yet available on Cisco.com, so more locales cannot be selected.

Table 4-6 Application Settings (continued)

Field or Button	Setting
Local Settings	
Locale	Displays each selected locale.
Default	Indicates which of the selected locales is the default.
Number of Users	Displays the number of users that have access to the Cisco TelePresence Video Portal. For information on managing access to the portal, see the "End-User Portal" section on page 4-6.

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

Backup Settings

Backup Settings consist of the following tabs:

- Archive Servers, page 4-12
- Backup and Restore, page 4-15
- Export Media Files, page 4-18
- Import Media Files, page 4-20

Archive Servers

In Backup Settings, click the **Archive Servers** tab to display or configure archive servers (see Figure 4-8).

Figure 4-8 Configure > Backup Settings—Archive Servers

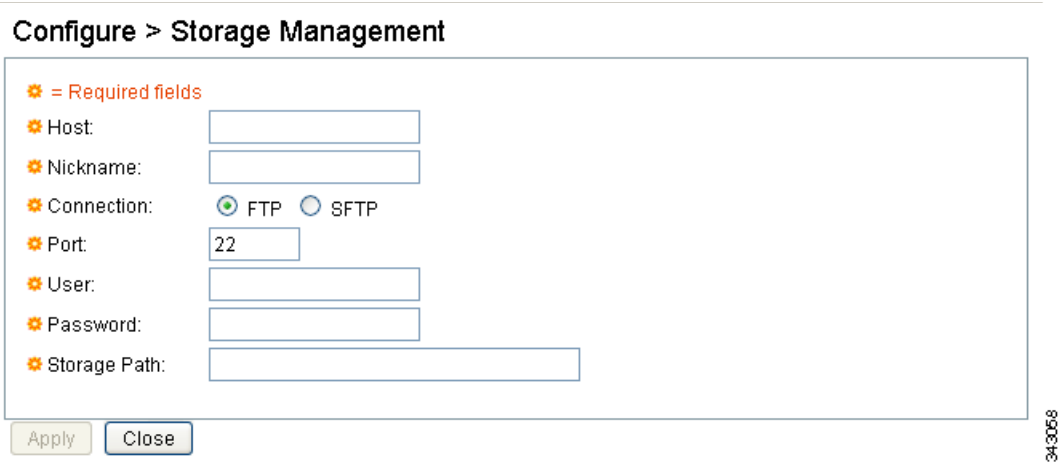
The Archive Servers tab displays a table providing the following information about previously defined archive servers:

Table 4-7 Archive Servers Table Field Descriptions

Field	Description
Host	Defined host name of the archive server.
Nickname	Defined alias of the archive server. **Note** In the CTRS Administration software, the nickname value is frequently used to identify the archive server.
Connection	Web protocol through which this archive server is reached.
Port	Port number over which this archive server is reached and is dependent on the connection type.
User	FTP and SFTP usernames and passwords.
Remote Path	Defines the directory on the FTP or SFTP server where CTRS files are stored.

- To display a defined number of table rows, click the down arrow next to **Rows per page**. Highlight and choose predetermined amounts.
- If the number of entries exceeds the Rows per Page value, click **First** to view the entries listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.
- To delete one of the defined archive servers, check the box to the left of the table entry, and then click **Delete**.
- To test whether your defined FTP or SFTP username, password and path are valid, check the box to the left of the table entry and then click **Test Connection**. If the connection is valid, CTRS displays a text box stating that the connection is valid. If the connection is not valid, CTRS displays a text box describing what part of the connection process failed.
- To edit one of the defined archive servers, check the box to the left of the table entry. Then click **Edit**. A dialog box appears (see Figure 4-9).
- To define a new server, click **New**. A dialog box appears (see Figure 4-9).

Figure 4-9 Configure > Backup Settings—Archive Servers (New or Edit)



When you click **Edit** or **New**, CTRS administration software takes you to the Storage Management dialog box, as described in Table 4-8. Use this dialog box to edit existing archive server settings or to define new archive servers.

Table 4-8 Storage Management Configuration Field Descriptions

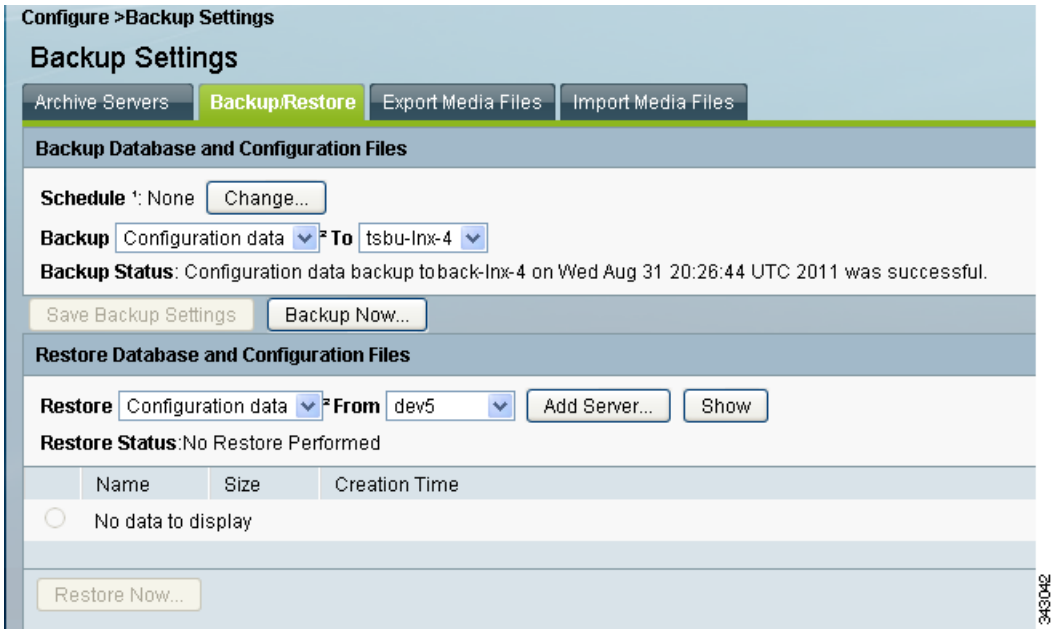
Field	Description
Host	Enter the host name of the archive server.
Nickname	Enter the nickname of the archive server. This nickname is used to identify the archive server throughout CTRS.
Connection	Click the appropriate radio button to define the connection through which this archive server is reached. Choices are File Transfer Protocol (**FTP**) and Secure File Transfer Protocol (**SFTP**).
Port	Enter the protocol-specific port number over which this server is reached.
User	Enter the FTP or SFTP username.
Password	Enter the password for FTP or SFTP.
Storage Path	Enter the directory on the FTP or SFTP server where CTRS files are stored.

- To register new or modified settings, click **Apply.**
- To close this window and return to the Archive Servers list, click **Close.**

Backup and Restore

In Backup Settings, click the **Backup/Restore** tab to display or configure settings for backup or system restoration (see Figure 4-10). From this tab, you can also perform a system backup or restoration.

Figure 4-10 Configure > Backup Settings—Backup/Restore



The System Backup and Restore window is divided into two sections:

- Backup Database and Configuration Files (top part of the window)
- Restore Database and Configuration Files (bottom part of the window)

To schedule a system backup:

Step 1 In **Schedule**, click the **Change** button to set the backup schedule. In the dialog box that appears, set the backup start time and frequency. Click **OK** to apply.

Step 2 Choose the content to be backed up from the **Backup** drop-down list. Options are **Configuration data** and **Full system data**. Full system data includes configuration files, videos, and video metadata.

Step 3 Choose the archive server where the data will be stored from the **To** drop-down list.

Step 4 Click **Save Backup Settings**. The contents of the CTRS database will be sent to the indicated server on the defined day(s) at the scheduled time.

Note The CTRS saves only the current system backup settings. The CTRS does not save previous backup settings.

To perform an immediate system backup:

- Click **Backup Now**. The CTRS content is sent to the indicated archive server.

Backup database fields are described in Table 4-9.

Table 4-9 Back Up Database and Configuration Files Field Descriptions

Field	Description
Schedule Daily at <time>	This field shows the time (U.S. Pacific time zone, twenty-four hour format) when automatic backups are scheduled to occur. To change the time scheduled for the automatic backup, click **Change**. From the Change window: • **Start Time**: Choose the hour and minute (U.S. Pacific time zone, twenty-four hour format) from the drop-down menu for the scheduled backup. • **Frequency: Resend every**: Defines the frequency of the backup. Click the appropriate radio button to choose **Daily** or **Weekly** backups; if you click **Weekly**, also choose the days of the week on which you want the backup to occur. • Click **OK** to apply your changes, or **Cancel** to cancel your new changes.
Backup	Define the content that you want to backup. Click the down arrow to view choices; highlight choice to select. Choices are: • **Configuration data** • **Full system data**
To	Indicates the already defined archive server on which you want to store the backup content.

To restore the CTRS database:

Step 1 Choose the CTRS database content that you want to restore from the **Restore** drop-down menu. Options are **Configuration data** and **Full system data**. Full system data includes configuration files, videos, and video metadata

Step 2 Choose the archive server (where the content you want to restore is saved) from the **From** drop-down menu. If you need to add a new archive server to the list, click **Add Server**. CTRS takes you to the Archive Server: Storage Management window to add a new server.

Step 3 After you have chosen the appropriate archive server, click **Show** to display the databases available to be used to restore the CTRS database.

- To display a defined number of table rows, click the down arrow next to **Rows per page**. Click to highlight and choose predetermined amounts.
- If the number of files exceeds the Rows per Page value, click **First** to view the files listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.

Step 4 Click the radio button to the left of the appropriate database file.

Caution Ensure that the database file that you want to restore was created successfully. Restoring a database file that was created during a failed backup will cause the CTRS to become corrupted, requiring re-installation of the CTRS Administrative software.

Step 5 Click **Restore Now**. CTRS content is retrieved from the indicated archive server and loaded on the CTRS.

Restore task fields are described in Table 4-10.

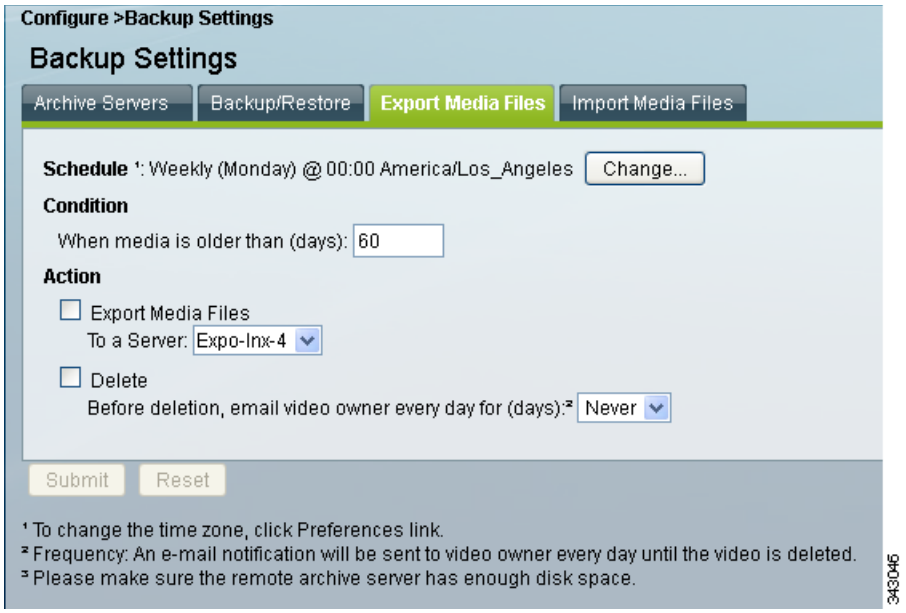
Table 4-10 Restore Database and Configuration Files Field Descriptions

Field	Description
Restore	Choose the content that you want to restore on this CTRS. Click the down arrow to view choices; highlight the choice to select: Options are: • **Configuration data** • **Full system data**
From	Indicates the already-defined archive server from which you want to retrieve content. Click the down arrow to view archive server choices; highlight the choice to select.
Add Server	To add a new archive server to the list, click **Add Server**. CTRS takes you to the Archive Server: Storage Management window to add a new server.
Show	Click **Show** to display the backed-up content available for restore.
Name	Data file to be used for restoring content. Click the radio button to the left of **Name** to choose it.
Size	Size of the data file in bytes.
Creation Time	Date and time that the data file was created.

Export Media Files

In Backup Settings, click the **Export Media Files** tab to display or configure settings to export media files (see Figure 4-11).

Figure 4-11 Configure > Backup Settings—Export Media Files



Use the Export Media Files tab to configure when CTRS transfers CTRS media data to a specified archive server. Export Media Files fields are described in Table 4-11.

Table 4-11 Export Media Files Field Descriptions

Field	Description
Schedule <frequency> at <start_time>	Check this box if you want to export CTRS data on a scheduled basis. This field shows the time in 24-hour format when automatic data exports are scheduled to occur. U.S Pacific time is the default. Click **Preferences** in the top right corner of the user interface to change the time zone. To change the time scheduled for the automatic data export, click **Change**. From the Change window: • **Start Time**: Choose the hour and minute in 24-hour format from the drop-down menus • **Frequency:** Defines the frequency of the export. Click the appropriate radio button to choose **Daily** or **Weekly** export. If you choose **Weekly**, also choose the days of the week on which you want the export to occur. • Click **OK** to apply your changes or **Cancel** to cancel your new changes.
Condition	Condition lets you establish additional rules governing the data that is transferred.
When media is older than (days):	Enter the number of days for the minimum age of the exported data. Valid values are 0–90 days. The default is 60 days.
Action	Defines whether CTRS exports the data to an archive server, deletes the data, or both.
Export Media Files	Check this box if you want CTRS to export this data to an archive server.
To a Server:	Select the archive server where the data will be stored. Click the arrow to display a drop-down list of available archive servers.
Delete	Check this box if you want CTRS to delete the specified data.
Before deletion, email video owner every day for (days):	CTRS sends an e-mail to the owner of the video (the person who created it) every day before the deletion date for the number of days that you specify. This e-mail notification advises the owner to download a copy of the video if desired.

- To register new or modified settings, click **Submit.**
- To restore the values that were last submitted, click **Reset**.

For example, in the Schedule field, you click the **Change** button. For Start Time, you choose **23:45**, and for Frequency, you choose **Daily**. In the Media is older than field, you enter **60**. As the Action to be taken daily at 23:45, you check the **Export** box and specify a server to which the CTRS will export videos that are older than 60 days. You also check **Delete**, and in the Notify video owner field, you enter **10**.

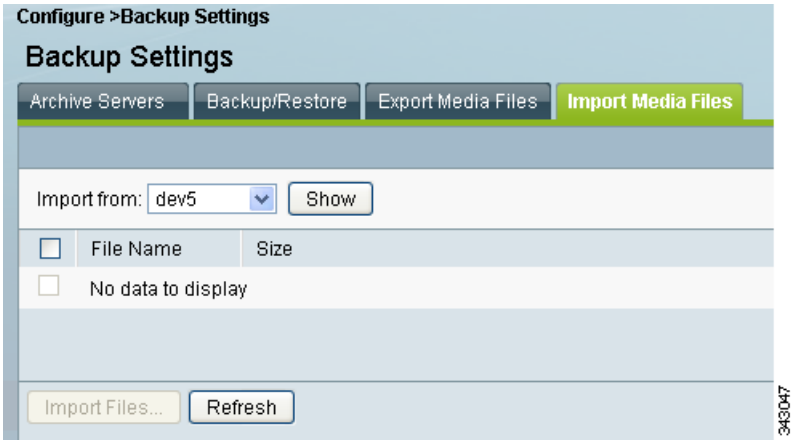
With this configuration, daily at 23:45, CTRS exports each video that is older than 60 days to the specified server. CTRS also marks for deletion each video that it exported. For the next ten days, CTRS marks the status of the video as “Delete Pending” (CTRS displays the status of each video in the list in

Recordings Management > Completed Recordings). CTRS also sends an e-mail notification to the video owner to alert the owner of the upcoming deletion. This notification is sent every day for ten days. At the end of the ten-day period, the video is deleted from CTRS.

Import Media Files

In Backup Settings, click the **Import Media Files** tab to display or configure settings to import media files (see Figure 4-12).

Figure 4-12 Configure > Backup Settings—Import Media Files



The Import Media Files tab lets you choose data files from a list of defined archive servers to be imported into the CTRS database.

To import media files:

Step 1 Click the down arrow to the right of **Import From** to display the list of available archive servers; highlight to select.

Step 2 After you have selected the appropriate archive server, click **Show** to display the files available to be imported.

- To display a defined number of table rows, click the down arrow next to **Rows per page**. Click to highlight and select predetermined amounts.
- If the number of files exceeds the Rows per Page value, click **First** to view the files listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.
- To refresh the list of files displayed, click **Refresh**.

Step 3 Check the box to the left of the file to choose it. To choose all files listed, check the box in the upper left of the table.

Step 4 Click **Import Files**.

Cisco Show and Share

You can configure a connection between a CTRS running version 1.8 and a Cisco Show and Share server running version 5.2.2 or 5.2.3. After the connection is established, Cisco Show and Share can be used for uploading, managing, sharing, and viewing video and audio content in your enterprise network.

To configure a connection between a CTRS and a Cisco Show and Share server, you will need:

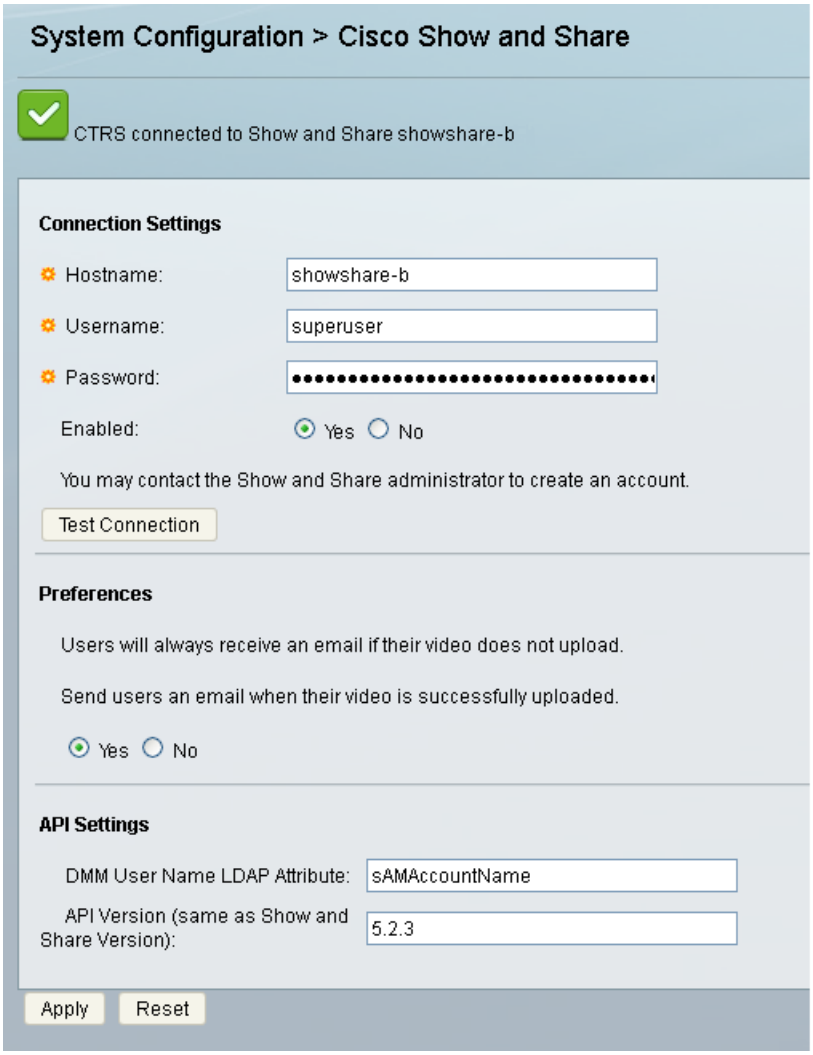
- The superuser account credentials—The CTRS requires superuser access to the Cisco Show and Share server in order to upload media files.
- The Cisco Show and Share server security certificate—The CTRS uses the installed Cisco Show and Share server certificate to establish a trusted, secure connection between the CTRS and the Cisco Show and Share server. The Cisco Show and Share server security certificate file can be obtained from the Cisco Show and Share server administrator.

  For information about downloading and installing the Cisco Show and Share server security certificate, see the "Installing the Cisco Show and Share Server Security Certificate on the CTRS" section on page 4-23.

Configuring the CTRS UI for Cisco Show and Share

Click **Cisco Show and Share** in the left menu to display or modify server settings (see Figure 4-13).

Figure 4-13 Configure > Cisco Show and Share



Use the Cisco Show and Share page to define the Show and Share server that CTRS uses as a video portal. Fields in the Cisco Show and Share page are described in Table 4-12.

Table 4-12 Cisco Show and Share Field Descriptions

Field or Button	Setting
Hostname	Enter the hostname of the Cisco Show and Share server.
Username	Enter the server superuser username. Contact the Cisco Show and Share server administrator for this information.
Password	Enter the server superuser password. Contact the Cisco Show and Share server administrator for this information

Table 4-12 Cisco Show and Share Field Descriptions

Field or Button	Setting
Enabled	Click **Yes** to enable connection to the server. Click **No** to disable connection.
Test Connection	Click **Test Connection** after entering the Show and Share hostname, username, and password.
Send users an email when their video is successfully uploaded	Click **Yes** or **No**. **Note** Users always receive emails when their videos do not upload.
DMM User Name LDAP Attribute	The default setting of this field is sAMAccountName, which should work for most organizations. To understand the circumstances under which you might need to change the default, see the "Understanding the DMM User Name LDAP Attribute Field" section on page 4-23.
API Version (same as Show and Share Version)	The default setting of this field is 5.2.2. If the Cisco Show and Share server is running version 5.2.3, you must change the setting of this field accordingly.

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

Understanding the DMM User Name LDAP Attribute Field

The DMM User Name LDAP Attribute field maps to the LDAP attribute specified in the Login User Name field of the Digital Media Manager (DMM), which manages Cisco Show and Share. This mapping ensures that the CTRS associates the correct username to a video while it is being uploaded to the Cisco Show and Share server. If the username is incorrect, the video will not be saved to the correct user account on the Cisco Show and Share server.

You need to change the default setting if your organization does not use the values of the LDAP samAccountName attribute as the source for the Cisco Show and Share usernames. Instead, your organization might use the values of another LDAP attribute or have created a customized LDAP attribute.

If one of these scenarios applies to your organization, contact the Show and Share administrator to get the LDAP attribute specified in the Login User Name field of the DMM, then enter the attribute in the DMM "Login User Name Attribute" field of the Cisco Show and Share page in the CTRS Administrative UI.

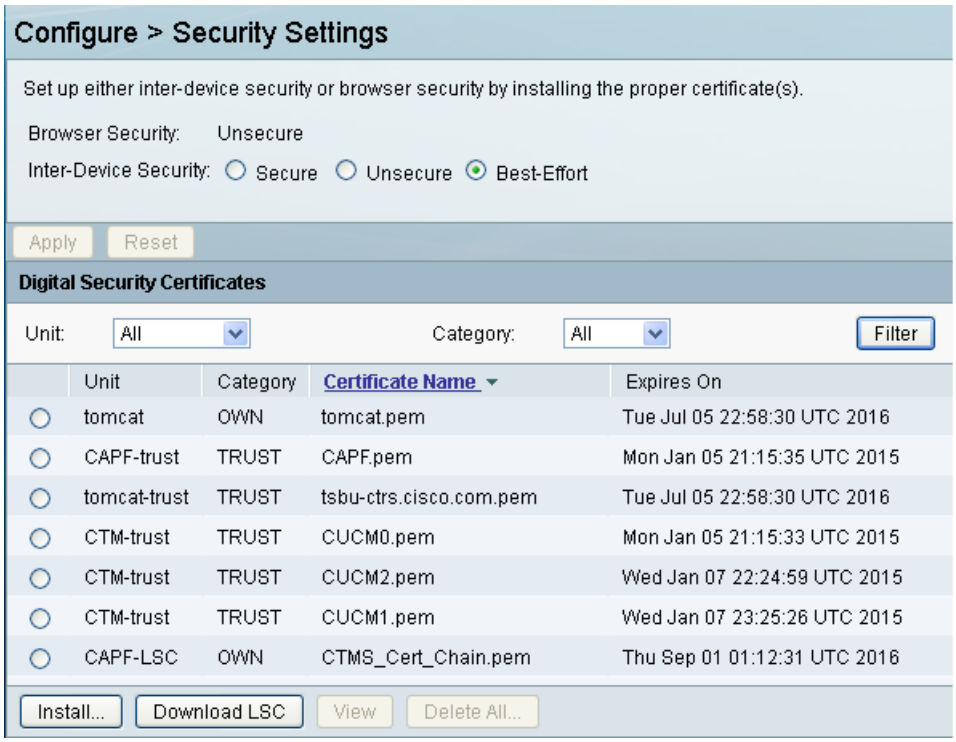
Installing the Cisco Show and Share Server Security Certificate on the CTRS

Once you have obtained the Cisco Show and Share server security certificate file from the Cisco Show and Share server administrator, perform the following steps to install it on the CTRS:

Step 1 Click **Security Settings** in the left menu.

Step 2 Click **Install**. The Certificate Upload window displays, as shown in Figure 4-14.

Figure 4-14 Configure > Security Settings

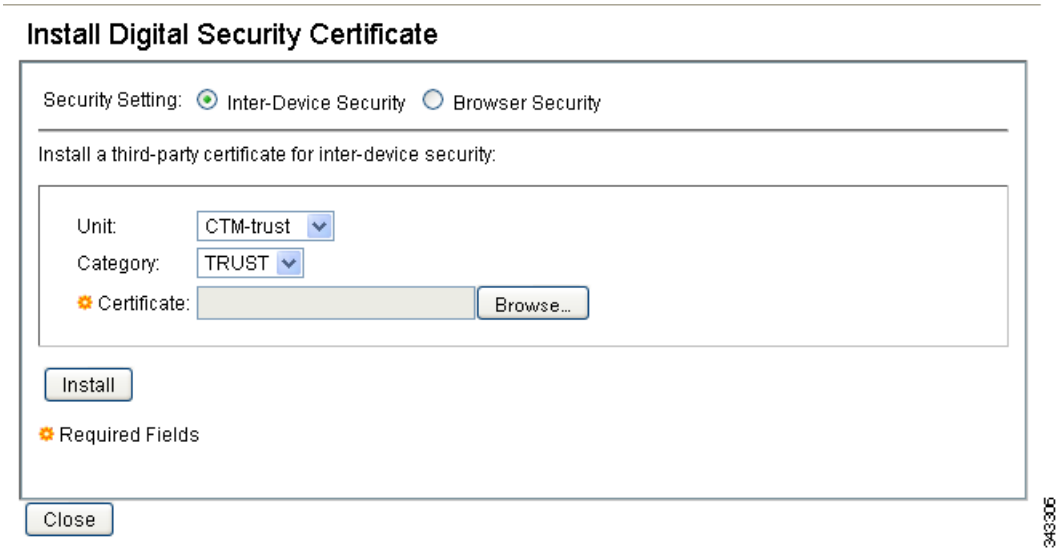


Step 3 If the Browser Security field is set to anything other than **Unsecure**, click the **Unsecure** radio button in the Browser Security field. Remember your previous setting, you will need to return this field to that setting after installing the security certificate.

Step 4 Click Install...

The Install Security Certificate Dialog Box appears.

Figure 4-15 Install Digital Security Certificate Dialog Box



Step 5 Upload the Cisco Show and Share security certificate file to the CTRS by completing the following steps:

a. Select the Inter-Device Security radio button.

b. From the Unit drop-down list, select **CTM-trust** (this is the default value).

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

d. Click the **Browse** button.

e. Navigate to the folder in which you stored the Cisco Show and Share security certificate file, and choose that file.

f. Click **Install**.

The Cisco Show and Share security certificate file installs on the CTRS.

Step 6 If you changed the Browser Security field setting in Step 3, click the appropriate radio button in the Browser Security field to return your Browser Security setting to the previous setting.

CTS-Manager

Note The CTS-Manager page appears only for the CTRS application on a Cisco TelePresence Commercial Express platform.

Use the parameters in CTS-Manager to register a CTS-Manager in the CTRS admin interface. Parameters are described in Table 4-13.

Table 4-13 CTS-Manager Registration in CTRS

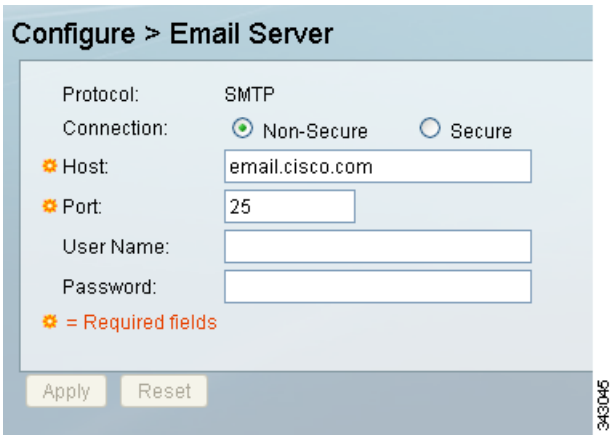
Field or Button	Setting
Description	Description of the CTRS. This description of the CTRS appears in the CTS-Man administrative interface in the Bridges and Servers list.
Time Zone	Time zone of the CTRS.
User	Administrative username of the CTS-Manager.
Password	Administrative password of the CTS-Manager.
Host	Hostname of the CTS-Manager.

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

Email Server

Click **Email Server** in the left menu to display or modify e-mail server settings (see Figure 4-16).

Figure 4-16 Configure > Email Server



Use the Email Server page to define the e-mail server that CTRS uses to send out alerts and video attachments. Fields in the Email Server page are described in Table 4-14.

Table 4-14 Email Server Field Descriptions

Field or Button	Setting
Protocol	View only. Email protocol.
Connection	Click the **Non-Secure** or the **Secure** radio button. If the SMTP server requires a secure connection, select **Secure**.
Host	Enter the hostname of the email server.
Port	Enter the port number associated with the email server.
SMTP User Name	Username of SMTP admin.
Password	Password of SMTP admin.

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

Interface Failover

Click **Interface Failover** in the left menu to display or modify failover settings for Ethernet adapters (see Figure 4-17).

Figure 4-17 Configure > Interface Failover

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 both network interfaces are not available or active, you cannot enable interface failover. If the **Enable** and **Disable** radio buttons are dimmed, check the connectivity of the interfaces.

To disable interface failover:

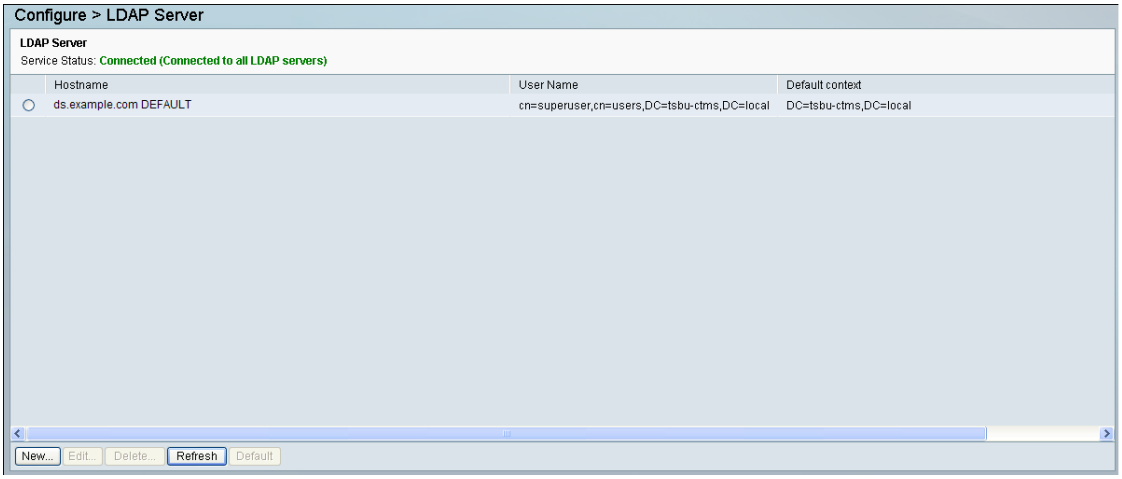
Step 1 With no active meetings in progress, click the **Disable** button.

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

LDAP Configuration

Click **LDAP Configuration** in the left menu to display or modify the Lightweight Directory Access Protocol (LDAP) configuration (see Figure 4-18).

Figure 4-18 Configure > LDAP Server



Use the LDAP Server page to assign and make changes to designated LDAP servers to be used with CTRS.

When you first open the LDAP Configuration window, CTRS displays a table listing all of the already-defined LDAP servers. LDAP table fields are described in Table 4-15.

Table 4-15 LDAP Configuration Table Field Descriptions

Field or Button	Setting
Hostname	Hostname of the LDAP server.
Username	Username for LDAP administration
Default context	Default naming context for the domain name, identifying the top entry in the local directory hierarchy.

- To refresh the list of available LDAP servers, click **Refresh**.
- To delete one of the LDAP servers, check the box to the left of the table entry, and then click **Delete**.
- To edit one of the definitions for an LDAP server, check the box to the left of the table entry, and then click **Edit**.
- To define a new LDAP server, click **New**.

When you click **Edit** or **New**, CTRS administration software takes you to the New LDAP Server configuration dialog box (see Figure 4-19), as described in Table 4-16. Use this dialog box to edit existing archive server settings or to define new archive servers.

Figure 4-19 System Configuration > LDAP Configuration (New or Edit)

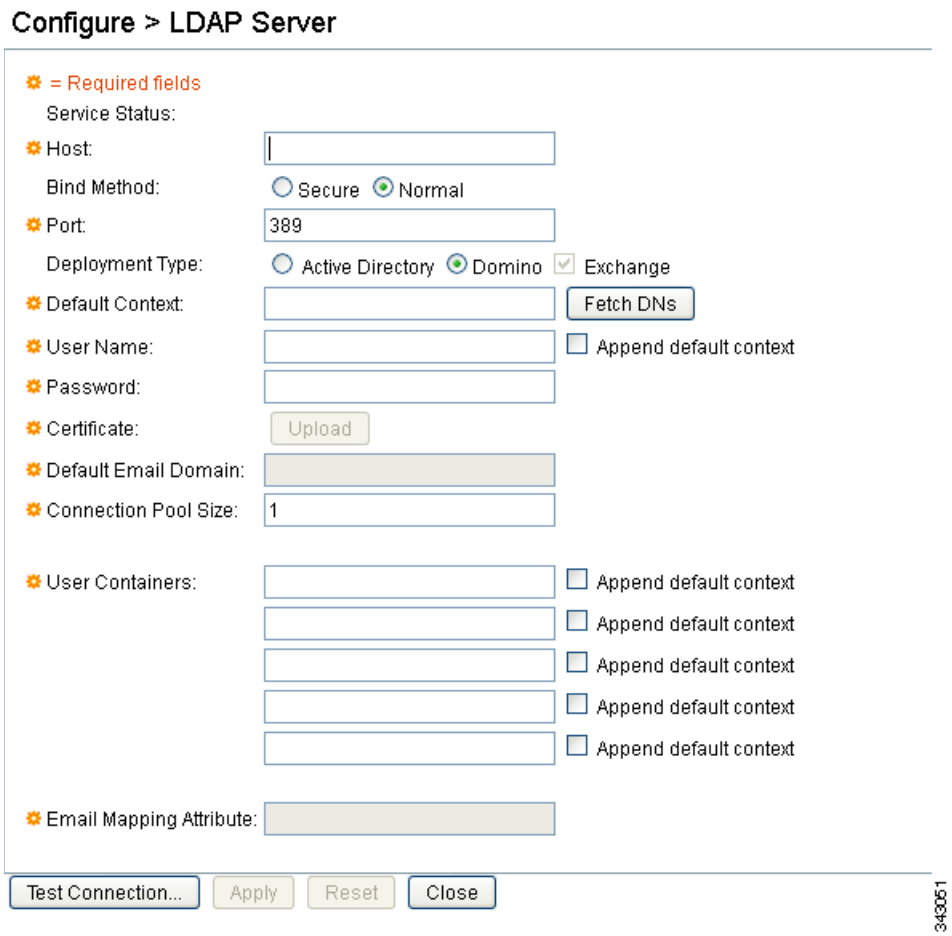


Table 4-16 New or Edit LDAP Configuration Table Field Descriptions

Field or Button	Setting
Host	Enter the hostname of the LDAP server.
Bind Method	Click the appropriate radio button to choose the binding method. For CTRS, options are **Secure** and **Normal**. • Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. • Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP.
Port	Enter the appropriate port number depending on the bind method selected. For Normal bind mode, the port setting is 389. For Secure bind mode, the port setting is 636. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port.

Table 4-16 New or Edit LDAP Configuration Table Field Descriptions

Field or Button	Setting
Deployment Type	Defines the LDAP server type. Options are Active Directory and Domino. Click the appropriate radio button. When Active directory is selected and the Exchange box is checked, the Active Directory is partnered with Exchange. This partnering means that a user account on the Active Directory server has an e-mail mapping attribute value that is prepended with SMTP. If the checkbox is unchecked, the CTRS does not prepend. By default, the Exchange box is checked.
Default Context	Enter the default naming context for the distinguished name (DN), identifying the top entry in the local directory hierarchy. For a list of domain names, click **Fetch DNs**. Choose the context from the drop-down list.
User Name	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=administrator,cn=users,dc=<mydomain>,dc=com) To append the DN, click **Append default context**.
Password	Enter the password to access the LDAP server.
Certificate	The name of the LDAP certificate. This is needed only if you are using the Secure Bind Mode. Click **Upload** to upload the appropriate security certificate.
Default Email Domain	Enter the LDAP email domain. If this LDAP server is set as the default email server, then users logging into the Cisco TelePresence Video Portal do not need to append their email domain information to their username. **Note** You can enter a Default Email Domain for only the default LDAP server. **Note** The CTRS only validates that the default email domain is a valid email domain. Clicking the **Test Connection** button validates that the CTRS can connect to the LDAP server, not to the email server specified in the Default Email Domain field.
Connection Pool Size	The number of concurrent connections used by the CTRS server to retrieve data from the LDAP server. This is primarily used for optimizing the server's access to the LDAP server.

Table 4-16 New or Edit LDAP Configuration Table Field Descriptions

Field or Button	Setting
User Containers	The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication. To append the default context, check the **Append default context** box next to the user container field. **Note** If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, "cn=users,dc=domain2,dc=com." When specifying the container and context information for your peer domain, DO NOT check the **Append default context** box.
Email Mapping Attribute	Enter the LDAP server tag (proxyAddresses) for mapping email addresses. **Note** You can enter an Email Mapping Attribute for only the default LDAP server.

- To test the connection between CTRS and the LDAP server, click **Test Connection**. If the connection is valid, CTRS displays a text box stating that the connection is valid. If the connection is not valid, CTRS displays a text box describing what part of the connection process failed.
- To register new or modified settings, click **Apply**.
- To restore default settings, click **Reset**.
- To exit without applying changes, click **Close**.

Configuring Multiple Domains in an LDAP Forest

To configure multiple domains in an LDAP forest, you must configure all subsequent domains as user containers in the first domain's LDAP configuration page.

For example, you have these two servers:

- LDAP server 1: corporate-cor1

  Default context: DC=cor1, DC=com

  User container: cn=users, DC=cor1, DC=com
- LDAP server 2: corporate-cor2

  Default context: DC=cor2, DC=com

  User container: cn=users, DC=cor2, DC=com

For CTRS, you must configure LDAP server 1 to include LDAP server 2's user containers. In the configuration page for LDAP server 1, in the User Containers fields, you would enter the following, each in its own field:

- cn=users, DC=cor1, DC=com
- cn=users, DC=cor2, DC=com

Note Users in subsequent domains must sign in to the CTRS with their username and domain name—username@example.com.

Security Settings

The CTRS supports these security types:

- Inter-device—Secures communication between Cisco TelePresence devices, which include the CTRS, Cisco TelePresence Manager (CTS-Manager), and Cisco TelePresence Multipoint Switch (CTMS).
- Browser—Secures communication between the CTRS web server and the browser through which you access the CTRS Administrative UI. Browser security eliminates website security certificate warnings, which you receive if your web server is not secure.

You can set up either inter-device security or browser security on a CTRS, but not both at the same time.

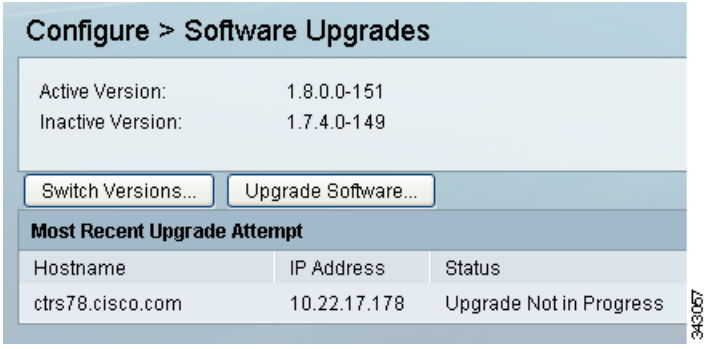
For information on how to set up inter-device and browser security, see the *Cisco TelePresence Security Solutions for Release 1.8*, which you can access at this location:

http://www.cisco.com/en/US/docs/telepresence/security_solutions/1_8/CTSS.html

Software Upgrades

Click **Software Upgrades** in the left menu to display, switch, or upgrade software versions (see Figure 4-20).

Figure 4-20 Configure > Software Upgrade



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

- **Switch Version**: The hard drive on the server on which CTRS 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**: CTRS 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.

To switch software versions:

- Click the **Switch Version** button.

The system will swap the software versions and reboot.

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 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.

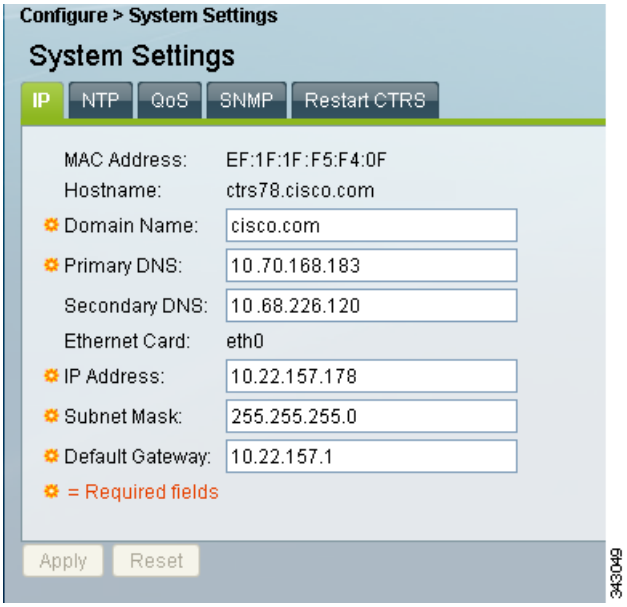
System Settings

System Settings are initially configured during CTRS Administration software set up. Use the System Settings to make changes to these initial settings. System Settings consists of the following configuration areas:

IP Settings

In System Settings, click the **IP** tab to display or configure IP settings (see Figure 4-21).

Figure 4-21 Configure > System Settings—IP



Some of the settings displayed on the IP tab are configured during initial installation of the CTRS administration software. The following fields are configurable on this tab:

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

Table 4-17 IP Settings

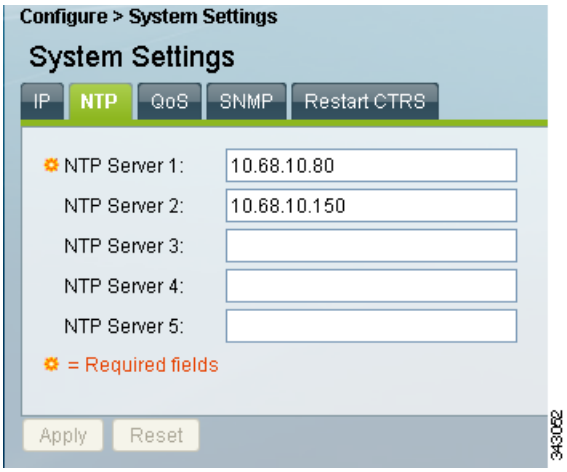
Field or Button	Setting
MAC Address	View only. MAC address of the MCU device on which the CTRS is located.
Hostname	View only. Hostname configured for the MCU device on which the CTRS is located.
Domain Name	Domain name in which the MCU device on which the CTRS is located.
Primary DNS	IP address of the primary DNS for the MCU device on which the CTRS is located.
Secondary DNS	IP address of the secondary DNS for the MCU device on which the CTRS 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 Recording Server. **Note** After changing the IP address, close your browser window, then log into CTRS 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**.

NTP Settings

In System Settings, click the **NTP** tab to display or configure Network Time Protocol (NTP) servers (see Figure 4-22).

Figure 4-22 Configure > System Settings—NTP



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

Click the **NTP Setting** tab in the System Settings window to list the configured IP address of the NTP servers.

Table 4-18 NTP Settings

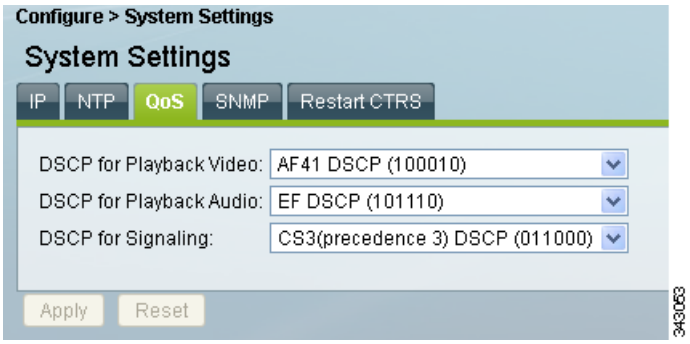
Field or Button	Setting
NTP Server 1-5	IP address of the NTP server. To add an NTP server to the configuration, type the IP address in an NTP Server field. To change an NTP server in the configuration, highlight and delete the IP address in the NTP Server field and type in the new address.

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

QoS

In System Settings, click the **QoS** tab to display or configure quality of service (QoS) settings (see Figure 4-23).

Figure 4-23 Configure > System Settings—QoS



QoS values define the traffic marking values used for network queuing for CTRS. Enter or edit settings as described in Table 4-19.

Table 4-19 QoS

Field or Button	Setting
DSCP for Playback Video	Quality of Service marking for the video packets during CTRS playback to CTS. 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 4-19 QoS (continued)

Field or Button	Setting
DSCP for Playback Audio	Quality of Service marking for the audio packets during CTRS Playback to CTS. 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 EF DSC (101110). We recommend that you set the value to CS4 (precedence 4) DSCP (100000) to match the default for DSCP for Playback Video.

Table 4-19 QoS (continued)

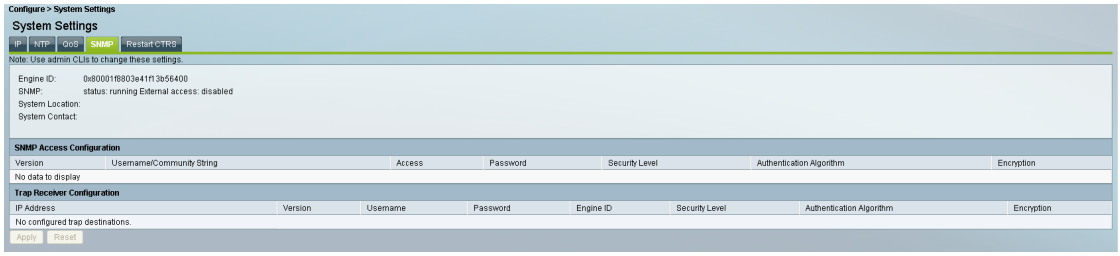
Field or Button	Setting
DSCP for Signaling	Quality of Service marking for SIP Signaling packets. Available settings are: • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 DSCP (011010) • AF32 DSCP (011100) • AF33 DSCP (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**.

SNMP

In System Settings, click the **SNMP** tab to display or configure Simple Network Management Protocol (SNMP) settings (see Figure 4-24).

Figure 4-24 System Configuration > System Settings—SNMP



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 CTRS command line interface (CLI) commands.

SNMP is enabled by default, and it monitors the CTRS system status (go to Monitoring > System Status for system status details). You can designate a particular server where SNMP trap messages are gathered and stored. Configuration requires username and password authentication.

By default, SNMP service is enabled. The following default SNMP settings are also enabled:

- SNMPv3 username set to “mrtg.” This name is for internal use of the system and should not be deleted.
- SNMPv2c username set to “public.” This name is for internal use of the system and should not be deleted.
- No trap receiver is configured. Use CTRS CLI commands to configure SNMP trap receiver information. For information about configuring SNMP traps, see the “Configuring SNMP Traps on CTRS” section on page 4-42.

Table 4-20 describes the SNMP fields. All fields in this tab are view-only.

Table 4-20 SNMP Settings

Field or Button	Setting
Engine ID	View only. The engine ID for the SNMP agent on this Cisco TelePresence Recording Server. This number is usually based on the CTRS 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 CTRS.

Table 4-20 SNMP Settings (continued)

Field or Button	Setting
System Contact	View only. Name of the SNMP system contact associated with CTRS.
SNMP Access Configuration	
Version	View only. Lists the configured SMNP version, either 3 or 2C.
Username/Community String	View only. SNMP server username.
Access	View only. Indicates whether the access is read, writer or read/write.
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.
Username	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.
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.

Configuring SNMP Traps on CTRS

SNMP provides the ability to send traps, or notifications, to inform the system administrator when one or more conditions have occurred. Traps are network packets that contain information about a component of CTRS. The information is status or error-related.

To configure SNMP traps on CTRS, you must complete all of the following steps:

- Start the SNMP service
- Configure an SNMP user

- Configure an SNMP trap destination
- Enable CTRS to send SNMP trap notifications

Starting the SNMP Service

To start the SNMP service, you must do the following:

Step 1 Log in to the CTRS CLI.

Step 2 Run the **utils service start** command:

```
utils service start Cisco SNMP Service
```

Configuring an SNMP User

To configure an SNMP user on CTRS, you must do the following:

Step 1 In the CTRS CLI, configure an SNMP user with the command:

set snmp user add v*ersion username access* [*passphrase*] [*level*]

Syntax Description

- *version* is the SNMP version, either 3 or 2c (both SNMP v3 and v2c are supported)
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)
- *access* defines which SNMP tasks can be accessed; values are r (read), w (write), and rw (read and write)
- *passphrase* (optional) is the SNMP v3 user passphrase
- *level* (optional) is the SNMP v3 level; value is one of the following:
  - *authNoPriv* (default) is authentication with no encryption. The correct authentication key is required to write messages, but no encryption/decryption key is required to read the contents of the message.
  - *authPriv* is authentication with encryption. The correct authentication key is required to write messages and the correct encryption/decryption key is required to read the contents of the message.
  - *noauthNoPriv* is no authentication with no encryption. Neither an authentication key nor encryption/decryption key is required to write and read messages.

Note The *passphrase* and *level* parameters are not required for SNMP v2c.

The following example configures an SNMP v3 user, with the username **testusr**, granting read and write access, and with the passphrase **testpass**:

```
set snmp user add 3 testusr rw testpass
```

Configuring an SNMP Trap Destination

To configure an SNMP trap destination on CTRS, you must do the following:

Step 1 In the CTRS CLI, configure an SNMP trap destination with the command:

set snmp trapdest add *version username destination* [*passphrase*] [*level*] [*engineID*]

Syntax Description

- *version* is the SNMP version, either 3 or 2c
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)
- *destination* is the destination host, in the format n.n.n.n[:*port*}
- *passphrase* (optional) is the SNMP v3 user passphrase
- *level* (optional) is the SNMP v3 level; value is one of the following:
  - *authNoPriv* (default) is authentication with no encryption. The correct authentication key is required to write messages, but no encryption/decryption key is required to read the contents of the message.
  - *authPriv* is authentication with encryption. The correct authentication key is required to write messages and the correct encryption/decryption key is required to read the contents of the message.
  - *noauthNoPriv* is no authentication with no encryption. Neither an authentication key nor encryption/decryption key is required to write and read messages.
- *engineID* (optional) is the SNMP v3 engine ID to use for the trap

The following example configures an SNMP v3 trap destination with the username **testusr**, at host **64.101.180.49:162**, passphrase **testpass**, and engine ID **0x8000DEECAFE8111BEEFADE**:

```
set snmp trapdest add 3 testusr 64.101.180.49:162 testpass authpriv
0x8000DEECAFE8111BEEFADE
```

Step 2 Configure the SNMP client device according to the instructions for that device. For instructions on configuring a CTS Release 1.8 endpoint, for example, see the SNMP Settings sections of the *Cisco TelePresence Administration Guide for CTS Software Release 1.8*.

Enabling CTRS to Send SNMP Trap Notifications

The final step to configuring an SNMP trap on CTRS is to enable CTRS to send SNMP trap notifications.

To enable CTRS to send SNMP trap notifications, you must do the following:

- Using an SNMP client, set the **clognotificationsenabled** MIB to **True**.

SNMP Trap notifications are now enabled for CTRS.

Modifying SNMP Trap Settings

You can modify existing SNMP trap destinations and user access.

To modify an SNMP trap destination, do the following:

Step 1 Delete the existing trap destination with the command:

set snmp trapdest del

After entering the above command, the CTRS CLI lists all configured SNMP trap destinations and prompts you to specify the trap destination to delete.

Step 2 Configure the new SNMP trap destination with this command:

set snmp trapdest add *version username destination* [*passphrase*] [*engineID*] [*level*]

For details on the syntax, refer to Syntax Description, page 4-44.

The following example configures an SNMP v3 trap destination with the username **testusr**, at host **192.168.180.122**, passphrase **testpass**, and engine ID **0x8000DEECAFE8111BEEFADE**:

```
set snmp trapdest add 3 testusr 192.168.180.122 testpass 0x8000DEECAFE8111BEEFADE
```

To modify SNMP user access to CTRS SNMP traps, do the following:

Step 1 Delete an existing SNMP user with the command:

set snmp user del *version username*

Syntax Description

- *version* is the SNMP version, either 3 or 2c
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)

The following example deletes the SNMP v3 user **testusr**:

```
set snmp user del 3 testusr
```

Step 2 Configure the new SNMP user with the command:

set snmp user add v*ersion username access* [*passphrase*] [*level*]

For details on the syntax, refer to Syntax Description, page 4-43.

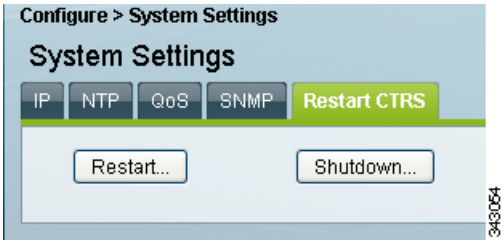
The following example configures an SNMP v3 user, with the username **newusr**, granting read and write access, and with the passphrase **newpass**:

```
set snmp user add 3 newusr rw newpass
```

Restart or Shutdown CTRS

In System Settings, click the **Restart CTRS** tab to restart or to shut down the CTRS (see Figure 4-25).

Figure 4-25 Configure > System Settings—Restart CTRS



To restart CTRS:

Step 1 Click **System Settings** in the left menu.

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

Step 3 Click **Restart** to restart CTRS. Restart means that the CTRS shuts down and then reboots.

To shutdown CTRS:

Step 1 Click **System Settings** in the left menu.

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

Step 3 Click **Shutdown** to shut down CTRS.

Unified CM

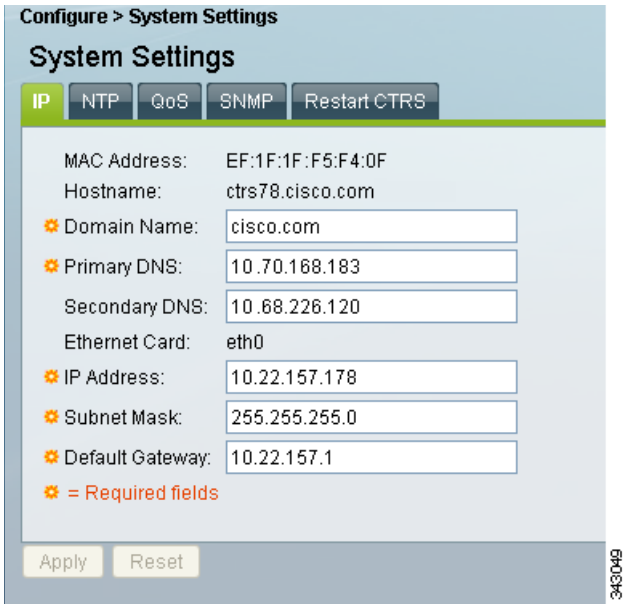
Cisco Unified Communications Manager (Unified CM) settings consist of these configuration areas:

- Unified CM, page 4-47
- SIP Profile Settings, page 4-48
- Access Settings, page 4-50

Unified CM

In Unified CM, click the **Unified CM** tab to display or configure Cisco Unified CM servers and SIP ports (see Figure 4-26).

Figure 4-26 Configure > Unified CM—Unified CM



From the Unified CM tab, you can specify Cisco Unified Communications Manager servers and SIP ports (see Table 4-21).

Table 4-21 Cisco Unified CM Settings

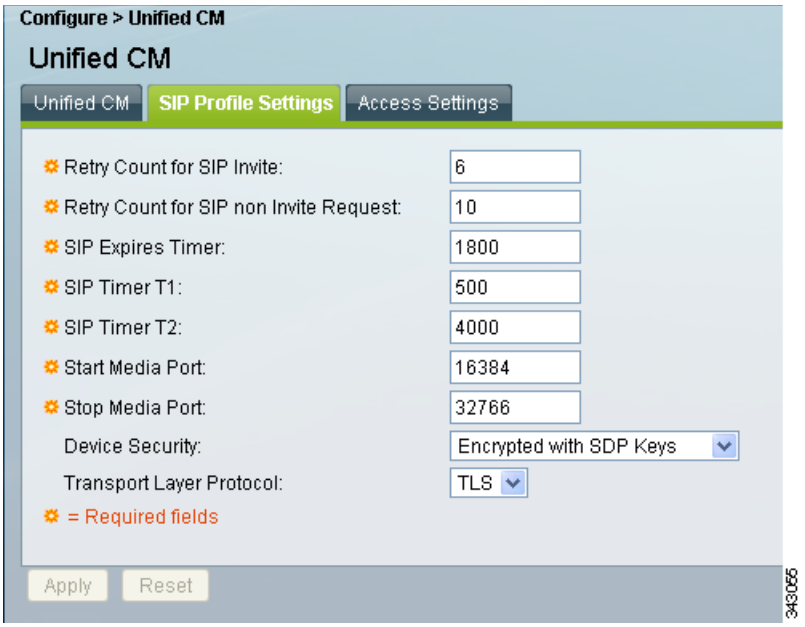
Field or Button	Setting
Cisco Unified CM 1 through 5	Hostnames or IP address(es) of the Cisco Unified Communications Manager (Unified CM) server. **Note** It is important to add all Unified CM servers in the cluster.
SIP Port	Port number for Cisco Unified SIP IP Phones that are using UDP to listen for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

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

SIP Profile Settings

In Unified CM, click the **SIP Profile Settings** tab to display or configure SIP profile settings (see Figure 4-27).

Figure 4-27 Configure > Unified CM—SIP Profile Settings



SIP profile settings, which are described in Table 4-22, are applied to all SIP ports that you specify in the Unified CM tab.

Table 4-22 SIP Profile Settings

Field or Button	Setting
Retry Count for SIP Invite	Specifies the number of times that Cisco Unified Communications Manager (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 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 Unified CM has not received an answer before this timer expires, 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.

Table 4-22 SIP Profile Settings (continued)

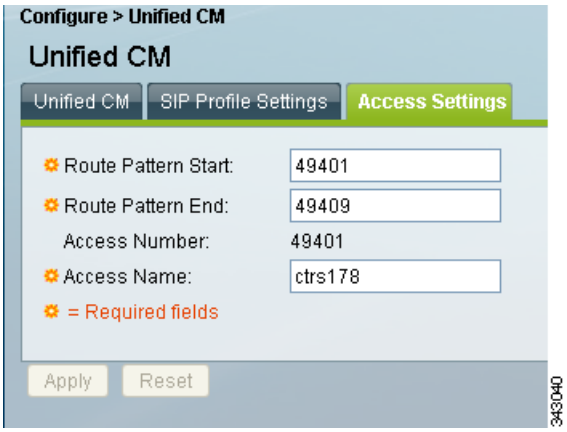
Field or Button	Setting
SIP Timer T2	Specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.
Start Media Port	Designates the start real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. The default for Cisco Unified Communications Manager (Unified CM) is 16384.
Stop Media Port	Designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. The default is for Cisco Unified Communications Manager (Unified CM) is 32766.
Device Security	Specifies the type of security applied to this CTRS. Available choices are the following: • Non-Secure • Authenticated • Encrypted with SDP Keys • Encrypted without SDP Keys (select this option if you are using a version of Unified CM that does not support encryption with SDP keys)
Transport Layer Protocol	Defines the transport protocol used. Available choices are: • TCP • UDP  **Note** Whenever the transport type is modified in CTRS, the corresponding transport type for the Cisco Unified CM trunk setting must be changed to match the CTRS transport type.

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

Access Settings

In Unified CM, click the **Access Settings** tab to display or configure route patterns or access settings (see Figure 4-28).

Figure 4-28 Configure > Unified CM—Access Settings



All of the settings on the Access Settings tab are derived from settings you configured in Cisco Unified Communications Manager (Cisco Unified CM).

Table 4-23 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 Cisco Unified CM. After you set the "SIP Trunk Minimum Number" value in Cisco Unified CM, CTRS automatically selects that number as this access number.
Access Name	Descriptive name for the access number as defined in Cisco Unified CM. Maximum number of characters is 20.

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