Cisco TelePresence Recording Server Release 1.6 Administration Guide

November 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19546-01

Cisco TelePresence Recording Server Release 1.6 Administration Guide

CONTENTS

Contents i-v

General Description i-v

System Requirements i-vi

CTRS Release 1.6 Administration Guide Organization i-vi

Obtaining Documentation and Submitting a Service Request i-vii

Using CTRS Administration Software 1-1

Contents 1-1

Overview of CTRS Tasks and Roles 1-1

Administrative Roles 1-2

Logging in to the Administrative User Interface 1-2

Overview of the Administrative User Interface 1-2

Header 1-3

System Status 1-3

Navigation Pane 1-4

Content Area 1-4

System Information 1-4

Configuring Cisco Unified Communications Manager for CTRS 2-1

Contents 2-1

Overview 2-1

Prerequisites 2-2

Logging into the Cisco Unified CM Administration Application 2-2

Creating a SIP Trunk Security Profile 2-2

Creating a SIP Trunk 2-3

Configuring a Route Pattern 2-4

Installing CTRS Administration Software 3-1

Contents 3-1

Prerequisites 3-1

Installing the CTRS Administration Software 3-2

Configuring CTRS Administration Software 4-1

Logging in to the Administrative User Interface 4-2

System Information 4-2
Left Menu of the Administrative User Interface 4-3
System Settings 4-3
IP Settings 4-4
NTP Settings 4-5
QoS Settings 4-6
SNMP Settings 4-10
Restart or Shutdown CTRS 4-12
Application Settings 4-12
Backup Settings 4-14
Archive Servers 4-14
System Backup and Restore 4-16
Export Media Files 4-19
Import Media Files 4-21
Unified CM Settings 4-21
Cisco Unified CM Settings 4-22
SIP Profile Settings 4-23
Access Settings 4-24
User Management 4-25
Administrative Portal 4-25
End-User Portal 4-29
Creating a New User or Modifying Settings for an Existing User 4-30
Software Upgrade 4-31
Security Settings 4-32
Interface Failover 4-35
Alert Management 4-36
LDAP Configuration 4-37
Configuring Multiple Domains in an LDAP Forest 4-40
Email Server 4-41

Managing CTRS Recordings 5-1

Active Recording 5-1
Completed Recordings 5-2
Exporting Recordings from the Completed Recordings List 5-4
Downloading a Recording to Your Computer 5-5

Troubleshooting CTRS 6-1

CTRS Alarms and System Errors Messages 6-1
Log Files 6-3

Monitoring CTRS System Processes 7-1

System Status 7-2

Process Status 7-3

Hardware Status 7-4

Preface

Initial Release: November 2009

Contents

- General Description, page v
- System Requirements, page vi
- System Requirements, page vi
- CTRS Release 1.6 Administration Guide Organization, page vi
- Obtaining Documentation and Submitting a Service Request, page vii

General Description

The Cisco TelePresence Recording Server (CTRS) allows users to do the following:

- Create recordings.
- Store recordings on the CTRS.
- Share recordings with others for viewing.
- Make recordings public so that anyone with access to the CTRS can view them.
- Play back recordings on a TelePresence endpoint.
- Play back recordings with a standard browser-based player.
- Download your recordings or public recordings.

CTRS enables users to record in TelePresence Studio Mode. In Studio Mode, users can create team announcements, corporate messages, training modules, video blogs, and other similar recordings.

To record, users must have access to a CTS with CTRS functionality; they control recording through the CTS IP phone interface.

All recordings are HD video and audio. All recorded content, including materials that users choose to display on a device that is connected to the VGA input or through a document camera, is shown on the TelePresence monitor from the viewer's perspective. CTRS acts as a viewer endpoint in a TelePresence session and records what it sees.

Users can then share a recording by sending it to a recipient's e-mail address. To play a recording, the recipient must sign in to the CTRS browser-based user portal with a corporate username and password (LDAP username and password). If the recipient wants to play a recording on a TelePresence display, he or she must sign in to CTRS through the CTS IP phone user interface with a corporate username and personal identification number (PIN).

System Requirements

- Cisco MCS-7845-I2 CCE4 Media Convergence Server with eight 146 gigabyte drives.
- Cisco TelePresence System software, Release 1.6 or later; IP phone with MIDlets version TSPM.1-6-0-2S or later.
- Cisco TelePresence Manager, Release 1.6 or later.
- Cisco Unified Communications Manager (Cisco Unified CM), Release 7.0.2, Release 7.1.2, or later.
- CTS-500, CTS-1000, CTS-1300, CTS-3000 and/or CTS-3200 systems.
- For the user portal, ensure that the browser that you use to play recordings includes the most recent version of Flash.

CTRS Release 1.6 Administration Guide Organization

The *CTRS Release 1.6 Administration Guide* is organized into the following chapters:

- Chapter 1: "Using CTRS Administration Software"
  This section provides information about the CTRS Administration software interface
- Chapter 2: "Configuring Cisco Unified Communications Manager for CTRS"
  This section provides instructions on how to configure Cisco Unified Communications Manager (Cisco Unified CM) so that is supports CTRS functionality.
- Chapter 3: "Installing CTRS Administration Software"
  This section describes how to install the CTRS administration software on the Cisco MCS-7800 Series Media Convergence Server.
- Chapter 4: "Configuring CTRS Administration Software"
  This section provides information about configuring the initial CTRS system settings.
- Chapter 5: "Managing CTRS Recordings"
  This section describe how to record meetings using CTRS Administration software.
- Chapter 6: "Troubleshooting CTRS"
  This section describes how to view and categorize system error messages and alerts, and how to filter and download log files.
- Chapter 7: "Monitoring CTRS System Processes"
  This section describes how to monitor the CTRS system processes using the tools available in CTRS.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Using CTRS Administration Software

Initial Release: November 2009

Contents

- Overview of CTRS Tasks and Roles, page 1-1
- Logging in to the Administrative User Interface, page 1-2
- Overview of the Administrative User Interface, page 1-2
- System Information, page 1-4

Overview of CTRS Tasks and Roles

Administrators use the CTRS Administration software to configure, to manage, to troubleshoot and to monitor activities related to the Cisco TelePresence Recording Server. Administrative tasks include the following:

- Configuring system settings. These tasks include configuring general system, security, interface failover, and LDAP settings, importing or exporting files, defining different levels of administrators, upgrading software and inporting and exporting files. System settings tasks are described in "Chapter 4: Configuring CTRS Administration Software."
- Managing Recordings. These tasks include defining recording defaults, managing active recording sessions, and viewing a list of completed recordings. Recording management tasks are described in "Chapter 5: Managing CTRS Recordings."
- Troubleshooting the system. These tasks include monitoring system errors and log files to determine the causes of system errors. Troubleshooting is described in "Chapter 7: Troubleshooting CTRS."
- Monitoring the system. These tasks include restarting the system and monitoring a variety of system processes. System monitoring tasks are described in "Chapter 6: Monitoring CTRS System Processes."

Prior to configuring CTRS Administration software, you must configure Cisco Unified Communications Manager (Cisco Unified CM) to support recording. Cisco Unified CM for CTRS configuration tasks are described in "Chapter 2: Configuring Cisco Unified Communications Manager for CTRS."

Installing CTRS Administration software is described in "Chapter 3: Installing CTRS Administration Software."

Administrative Roles

CTRS administration software recognizes three different administrative roles; access to task folders is dependent on defined 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.You can select both Content Manager and Diagnostic Technician and this will allow a combination of accessibility of both roles for the user.

Administrative role configuration is described in "Chapter 4: Configuring CTRS Administration Software."

Logging in to the Administrative User Interface

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

Step 1 Open an IE 6.x or 7.x 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 CTRS user 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."

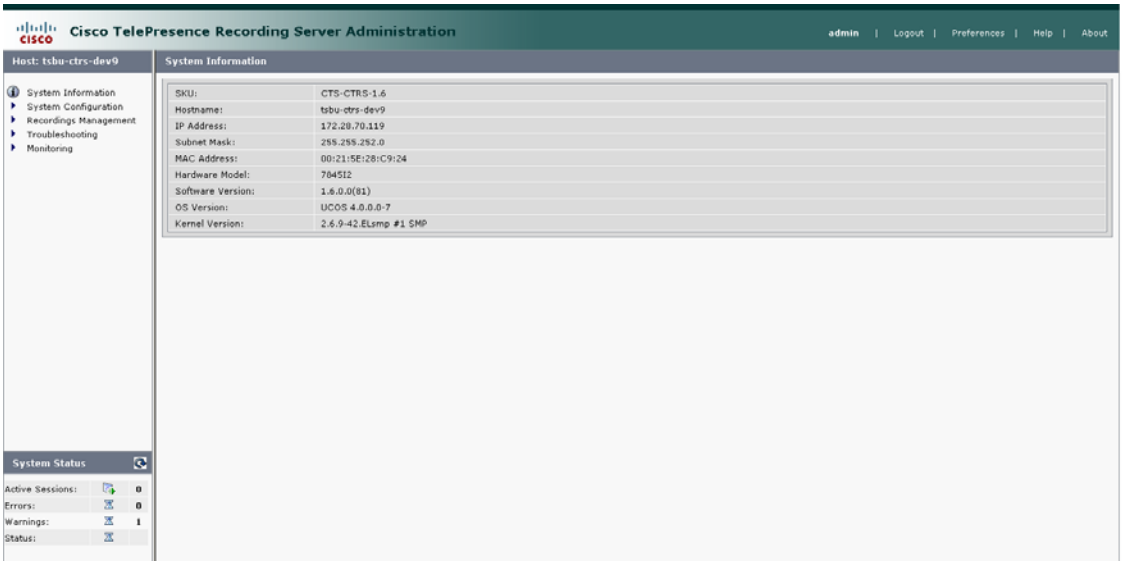
Overview of the Administrative User Interface

CTRS Administration software user interface is similar to the interface used in Cisco TelePresence System software suite. The user interface is organized as follows:

- Header, page 1-3
- System Status, page 1-3
- Navigation Pane, page 1-4
- Content Area, page 1-4

Figure 1-1 shows an example of the CTRS Administration software user interface.

Figure 1-1 CTRS Administration Software User Interface



Header

The header at the top of all CTRS Administration windows lists the name of the software application and provides links for the following functions:

- Admin—Roll your cursor over “Admin” to display the name of the user current logged in to CTRS Administration.
- Logout—Click to log out of the system.
- Preferences: Click to display the Preferences window, where you can change the time zone. The first time you login you need to specify the time zone you are in. This localizes meeting times to your location.
- Help—Click to display online help for using the CTRS Administration.
- About—Click to display software version and licensing information.

System Status

System status is always in view in the lower left corner of the CTRS Administration window. The system status is updated every 60 seconds. Click the **Refresh** button in the upper right corner of the box to obtain an immediate update.

The system status box shows the following information:

- Active Sessions: Shows the number of active recording sessions currently in progress.
- Errors: Shows the total number of system errors that are defined as either CRIT or ERROR. If the total number of system errors is 0, a green check is displayed. If the total number of system errors is more than 0, a red cross is displayed. System errors are described in “Chapter 7: Troubleshooting CTRS.”

- Warnings: Shows the total number of system errors defined as WARN. If the total number of system errors is 0, a green check is displayed. If the total number of system errors is more than 0, a red cross is displayed. System warnings are described in "Chapter 7: Troubleshooting CTRS."
- Status: Shows the current state of all system processes. If all system processes are in the RUNNING state, a green check is displayed. If one or more processes are in the STOPPED state, a red check is displayed. System processes are described in "Chapter 6: Monitoring CTRS System Processes."

Navigation Pane

In the navigation pane at the left side of the CTRS Administration window, the System Configuration, Recording Management, Troubleshooting, and Monitoring folders display lists of tasks associated with CTRS. Lists of tasks are also displayed in the content area of the window when you click any folder in the navigation pane. Click the task name or the arrows in the left panel, or click the highlighted name in the content area to navigate to tasks.

Content Area

The right frame is the content area. When you select a folder or a task from the navigation pane, the content associated with that item displays in the content area. The gray bar above the content area shows the navigational path so you can quickly identify where you are at any time.

System Information

Choose **System Information** from the Navigation Pane to view information about the Cisco TelePresence Multipoint Switch. The information displayed under System Information is configured during CTRS software installation.

- SKU
- Hostname: Hostname of the CTRS.
- IP Address and subnet mask: IP address and corresponding subnet mask of the Cisco TelePresence Recording Server.
- MAC Address: MAC address of the Cisco MCS-7845-I2 CCE4 Media Convergence Server on which the CTRS is running
- Hardware Model: Model number of the Cisco MCS-7845-I2 CCE4 Media Convergence Server on which the CTRS is running.
- Software Version: Version of CTRS Administration software currently installed.
- Operating System (OS) Version
- Kernel Version

CHAPTER 2

Configuring Cisco Unified Communications Manager for CTRS

Initial Release: November 2009

Contents

- Overview, page 2-1
- Prerequisites, page 2-2
- Logging into the Cisco Unified CM Administration Application, page 2-2
- Creating a SIP Trunk Security Profile, page 2-2
- Creating a SIP Trunk, page 2-3
- Configuring a Route Pattern, page 2-4

Overview

Before installing the CTRS Administration software on your Cisco MCS-7845 Media Convergence Server, you need to perform the following configuration tasks in Cisco Unified Communications Manager (Cisco Unified CM):

- Create a SIP security profile. This security profile will be used on the SIP trunk between CTRS and Cisco Unified CM.
- Create a Session Initiation Protocol (SIP) trunk. The SIP trunk is used for communication between Cisco Unified CM and CTRS.
- Create route patterns. A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns are used for routing conferences numbers to the CTRS.

Prerequisites

Before starting the tasks in this chapter, make sure that the following conditions are met or that you understand the following information:

- Cisco Unified CM is running and using Release 7.0.2 or Release 7.1.2 or later.
- Cisco TelePresence System is running Release 1.6 or later software.

For additional information about configuring Cisco Unified CM for Cisco TelePresence System, refer to the *Cisco Unified Communications Manager Installation Guide for the Cisco TelePresence System*.

For compatibility information, refer to *Compatibility Information for Cisco TelePresence System Release 1.6*.

Logging into the Cisco Unified CM Administration Application

To log into the Cisco Unified CM Administration application:

Step 1 Open a web browser.

Step 2 Access a web browser that is supported by the Cisco Unified CM Administration application from any user PC in your network. In the address bar of the web browser, enter the following URL:

```
https://CUCM-server-name
```

where *CUCM-server-name* is the name or IP address of the server.

Note You may need to specify the address of the server where Cisco Unified CM is installed. If your network uses DNS services, you can specify the hostname of the server. If your network does not use DNS services, you must specify the IP address of the server.

Step 3 Log in with your assigned administrative privileges.

Step 4 Select ***Cisco Unified Communications Manager Administration*** in the **Navigation** field at the upper right corner of the page and click ***Go*** to return to the Cisco Unified Communications Manager Administration home page.

Creating a SIP Trunk Security Profile

To create a SIP trunk security profile:

Step 1 Click ***System***. Under **Security Profile**, click ***SIP Trunk Security Profile***.

Step 2 Click the ***Add New*** button at the bottom of the page or click the ***+ sign*** at the top of the page.

Step 3 Enter the settings as indicated in Table 2-1 to configure the SIP trunk security profile. Leave default settings for fields not included in Table 2-1.

.

Table 2-1 SIP Trunk Security Profile Settings

Field	Required	Setting
Name	Yes	Enter a text string identifying this SIP trunk security profile.
Description	—	Enter a text string describing this SIP trunk security profile.
Device Security Mode	Yes	If you are running in non-secure mode, select ***Non Secure***. If you are running SIP security, select ***Encrypted***.
Incoming Transport Type	Yes	Select ***TCP+UDP***. If Encrypted is selected, TLS will be entered automatically.
Outgoing Transport Type	Yes	Select ***TCP***.
Incoming Port	Yes	Enter ***5060*** for non-secure trunk. If running SIP security, then enter a different unused port, for example 5275.

Step 4 Click the ***Save*** button at the bottom of the page.

Creating a SIP Trunk

To create a SIP trunk:

Step 1 Click ***Device***. Click ***Trunk***.

Step 2 Click the ***Add New*** button at the bottom or click the ***+ sign*** at the top of the Trunk Configuration page.

Step 3 Select ***SIP Trunk*** from the **Trunk Type** pull-down menu, then click ***Next***.

Step 4 Enter the settings as indicated in Table 2-2 to configure the SIP trunk. Leave default settings for fields not included in Table 2-2.

.

Table 2-2 SIP Trunk Settings

Field	Required	Setting
Device Information		
Device Name	Yes	Enter a text string identifying this SIP trunk.
Description	—	Enter a text string describing this SIP trunk.
Device Pool	Yes	Select ***Default***.
SIP Information		
Destination Address	Yes	Enter the IP address of the CTRS.
SIP Trunk Security Profile	Yes	Select the SIP trunk security profile that you created for CTRS.
SIP Profile	Yes	Select ***Standard SIP Profile***.

Step 5 Click the ***Save*** button at the bottom of the page.

Configuring a Route Pattern

A route pattern allows a Cisco Unified CM-managed device to access another device by dialing its number. Such devices may include gateways, CTRS, CTMS and CTS systems, or Cisco Unified Videoconferencing 5230 (CUVC) MCUs. Each device requires its own unique route pattern.

To configure a route pattern:

Step 1 Click ***Call Routing***. Under **Route/Hunt**, click ***Route Pattern***.

Step 2 Click the ***Add New*** button at the bottom or click the ***+ sign*** at the top of the Route Pattern Configuration page.

Step 3 Enter the settings as indicated in Table 2-3 to configure the SIP trunk. Leave default settings for fields not included in Table 2-3.

.

Table 2-3 Route Pattern Configuration Settings

Field	Required	Setting
Pattern Definition		
Route Pattern	Yes	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. The uppercase characters A, B, C, and D are valid characters. **Note** See the "Wildcards and Special Characters in Route Patterns and Hunt Pilots" section in the *Cisco CallManager System Guide* for more information about wildcards.
Description	—	Enter a text string describing this route pattern.
Gateway/Route List	Yes	Select the SIP trunk that you created for CTRS.
Call Classification	Yes	Select ***OnNet***.

Step 4 Click the ***Save*** button at the bottom of the page.

CHAPTER 3

Installing CTRS Administration Software

Initial Release: Month Day, Year

Contents

- Prerequisites, page 3-1
- Installing the CTRS Administration Software, page 3-2

Prerequisites

Before you install the Cisco TelePresence Recording Server (CTRS) Administration software system files, you need the following equipment and information:

- Cisco TelePresence System (CTS 500, CTS 1000, CTS 1300, CTS 3000 and/or CTS 3200) assembled and configured to support TelePresence conferencing. For more information, refer to the *Cisco TelePresence System Release 1.6 Administrator's Guide* and the appropriate *Cisco TelePresence Assembly Guide*.
- Cisco MCS-7845-I2 CCE4 Media Convergence Server with eight 146 gigabytes drives, installed and connected to a Domain Name System (DNS) server and your network.
- Console able to access the Cisco MCS-7845-I2 CCE4 Media Convergence Server.
- DVD that contains the CTRS Administration software application.
- Cisco Unified Communications Manager (Cisco Unified CM) Release 7.0.2, Release 7.1.2 or higher configured to support CTS Release 1.6 and integrated to work with CTRS, meaning that a SIP security profile, SIP trunk, and route pattern specific to CTRS have been created. For more information about Cisco Unified CM for CTS configuration, refer to *Cisco Unified Communications Manager Installation Guide for the Cisco TelePresence System Release 1.6*.

Installing the CTRS Administration Software

To install the CTRS Administration software application:

Step 1 Insert the CTRS Administration software application DVD into the appropriate drive in the Cisco MCS-7845-I2 CCE4 Media Convergence Server and boot up the host.

Step 2 **Media Check**: The system asks if you wish to perform a media check on the inserted DVD. Select ***Yes*** or ***No*** and press the Enter key. If you select ***No***, the system bypasses the media check. If you select ***Yes***, the system performs a checksum to make sure that the media on the DVD is intact. When the checksum has successfully completed, select ***Okay*** and press the Enter key.

Note If the checksum fails, it could be because of a problem with either the DVD or the DVD drive. The DVD or the DVD drive could need cleaning; the DVD data could be corrupted; or the software image you are trying to load could be the wrong image.

Step 3 **Hard Drive Check**: The system then checks the status of the hard drives in the server. When cued to update BIOS or to overwrite the hard drive, select *Yes* and press the Enter key to continue.

Step 4 **Platform Installation Wizard**: Select ***Proceed*** and press the Enter key to continue.

Step 5 **Automatic Negotiation of Ethernet NIC Speed and Duplex**: Select ***Yes*** and press the Enter key to continue.

Step 6 **DHCP**: Cisco Systems recommends that you use a static IP address instead of DHCP. Select ***No*** to define a specific static IP address and press the Enter key. Enter the following information:

- Hostname: Hostname of the CTRS server
- IP Address: IP address of the CTRS server
- IP Mask: Subnet mask for the CTRS server IP address
- Gateway Address: IP address for the gateway to the CTRS server

Select ***Okay*** and press the Enter key to continue.

Step 7 **DNS Client**: Select ***Yes*** and press the Enter key. Enter the following information:

- Primary DNS: IP address of the primary Domain Name System server
- Secondary DNS: IP address of the secondary Domain Name System server

Domain: Domain name for your company

Select ***Okay*** and press the Enter key to continue.

Step 8 **Platform Administrator Username and Password**: Enter the following information:

- Administration ID
- Password
- Confirm Password

Select ***Okay*** and press the Enter key to continue.

Step 9 **Certificate Information**: Enter the following information:

- Organization
- Unit
- Location

- State
- Country

Select ***Okay*** and press the Enter key to continue.

Step 10 **Network Time Protocol (NTP) Client Information**: Enter the following information:

- NTP Server 1: IP address of the primary NTP server
- NTP Server 2: IP address of the secondary NTP server
- NTP Server 3 through 5: IP addresses of additional NTP servers

Select ***Okay*** and press the Enter key to continue.

Note The NTP servers identified must be the same for CTRS, CTMS, CTS and CTM. It is recommended that you provide at least three NTP servers.

Step 11 **Database password**: Enter the database password and then press the Enter key to continue.

Step 12 **Platform Configuration Confirmation**: Select ***Okay*** to continue with installation. select ***Back*** to go to previous screens in the installation procedure, or ***Cancel*** to abort the installation. When you have made your selection, press the Enter key. If you select ***Okay***, platform and application installation takes approximately 30 to 45 minutes. During installation, allow the default selection for the custom kernel to proceed.

Step 13 After the CTRS Administration software application files have been installed, the system automatically reboots. The system then performs a check of the network connectivity and setup. If the system determines that any of the information you entered during the preceding steps is incorrect, a message is displayed on the console, giving the you the following options:

- Retry: Select this option (and press the Enter key) to retry the installation procedure.
- Review: Select this option (and press the Enter key) if you need to change any of the data you entered during the preceding installation steps. If you select this option, navigate to the appropriate installation data entry screen, re-enter the data, and then proceed to the **Platform Configuration** screen to re-initiate installation.
- Halt: Select this option (and press the Enter key) if you need to abort installation.
- Ignore: Select this option (and press the Enter key) to ignore the system warning.

Step 14 After the network connectivity and setup check, the system reboots again. Following this reboot, the CTRS Administration software log-on screen is displayed. Enter your username and password to continue with CTRS Administration software configuration.

CHAPTER 4

Configuring CTRS Administration Software

Revised: November 2009

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

- Logging in to the Administrative User Interface, page 4-2
- System Information, page 4-2
- Left Menu of the Administrative User Interface, page 4-3
- System Settings, page 4-3
- Application Settings, page 4-12
- Backup Settings, page 4-14
- Unified CM Settings, page 4-21
- User Management, page 4-25
- Software Upgrade, page 4-31
- Security Settings, page 4-32
- Interface Failover, page 4-35
- Alert Management, page 4-36
- LDAP Configuration, page 4-37
- Email Server, page 4-41

Logging in to the Administrative User Interface

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

Step 1 Open an IE 6.x or 7.x 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 CTRS user 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."

System Information

Click **System Information** in the left menu to view information about the CTRS. The information displayed under System Information is configured during CTRS software installation.

- SKU
- Hostname: Hostname of the CTRS.
- IP Address and subnet mask: IP address and corresponding subnet mask of the Cisco TelePresence Recording Server.
- MAC Address: MAC address of the Cisco MCS 7800 Series Media Convergence Server on which the Cisco TelePresence Recording Server is running
- Hardware Model: Model number of the Cisco MCS 7800 Series Media Convergence Server on which the Cisco TelePresence Recording server is running.
- Software Version: Version of CTRS Administration software currently installed.
- Operating System (OS) Version
- Kernel Version

Left Menu of the Administrative User Interface

You can access any of the System Configuration screens from the left menu in the CTRS user interface (see Figure 4-1):

Figure 4-1 System Configuration—Left Menu

System Settings

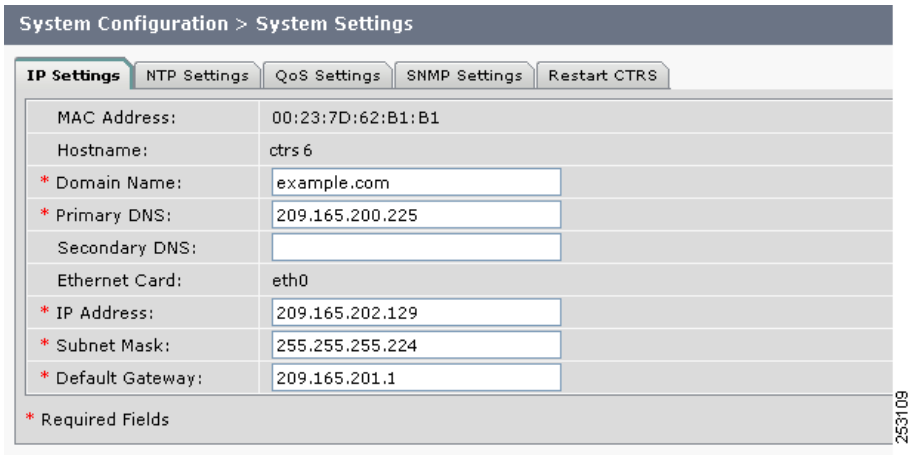
System Settings are initially configured during CTRS Administration software set up. Use the System Settings to make changes to these initial settings. System Settings consists of the following configuration areas:

- IP Settings, page 4-4
- NTP Settings, page 4-5
- QoS Settings, page 4-6
- SNMP Settings, page 4-10
- Restart or Shutdown CTRS, page 4-12

IP Settings

In System Settings, click the **IP Settings** tab to display or configure IP settings (see Figure 4-2).

Figure 4-2 System Configuration > System Settings—IP Settings



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

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

Table 4-1 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.

Table 4-1 IP Settings (continued)

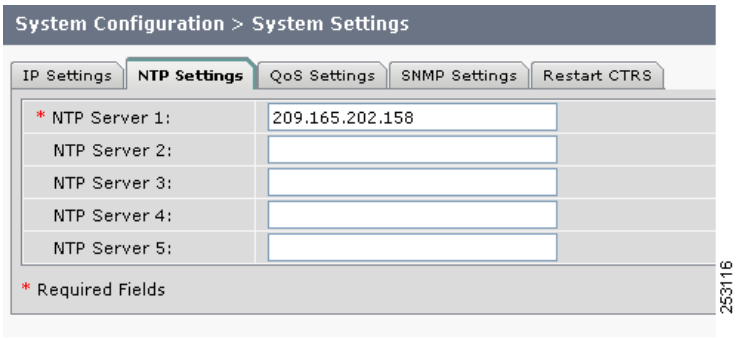
Field or Button	Setting
IP Address	IP address of the Cisco TelePresence Recording Server. **Note** After changing the IP address, close your browser window, then log into CTRS again using your new IP address.
Subnet Mask	Subnet mask of the Cisco TelePresence Multipoint Switch.
Default Gateway	Default 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 Settings** tab to display or configure Network Time Protocol (NTP) servers (see Figure 4-3).

Figure 4-3 System Configuration > System Settings—NTP Settings



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 4-2 NTP Settings

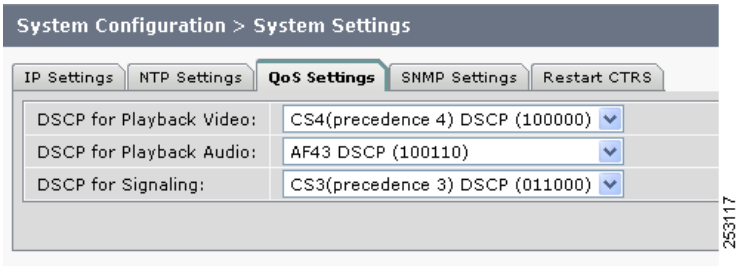
Field or Button	Setting
NTP Server 1-5	IP address of the NTP server. To add an NTP server to the configuration, type the IP address in an NTP Server field. To change an NTP server in the configuration, highlight and delete the IP address in the NTP Server field and type in the new address.

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

QoS Settings

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

Figure 4-4 System Configuration > System Settings—QoS Settings



QoS values define the traffic marking values used for network queuing for CTRS. Enter or edit settings as described in Table 4-3.

Table 4-3 QoS Settings

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 4-3 QoS Settings (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 4-3 QoS Settings (continued)

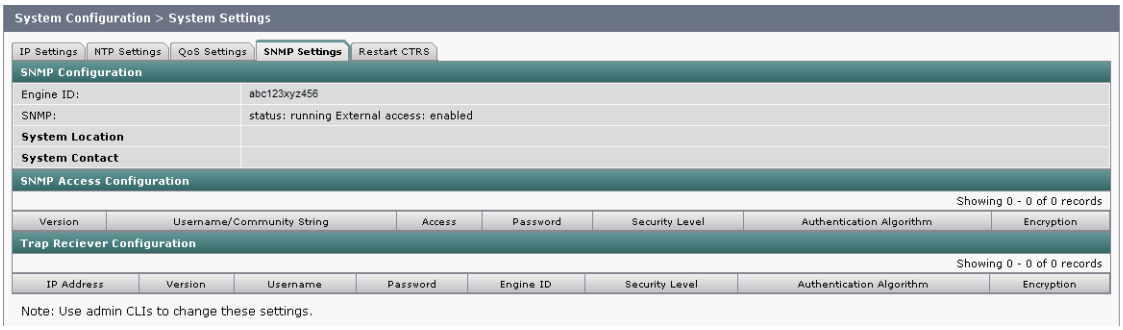
Field or Button	Setting
DSCP for Signaling	Quality of Service marking for SIP Signaling packets. Available settings are: • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 DSCP (011010) • AF32 DSCP (011100) • AF33 DSCP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

SNMP Settings

In System Settings, click the **SNMP Settings** tab to display or configure Simple Network Management Protocol (SNMP) settings (see Figure 4-5).

Figure 4-5 System Configuration > System Settings—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 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.

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

Table 4-4 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.

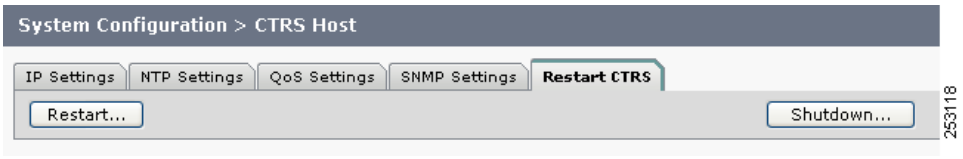
Table 4-4 SNMP Settings (continued)

Field or Button	Setting
System Location	(View only) Physical location of the SNMP system associated with CTRS.
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.

Restart or Shutdown CTRS

In System Settings, click the **Restart CTRS** tab to restart or to shut down the CTRS (see Figure 4-6).

Figure 4-6 System Configuration > 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.

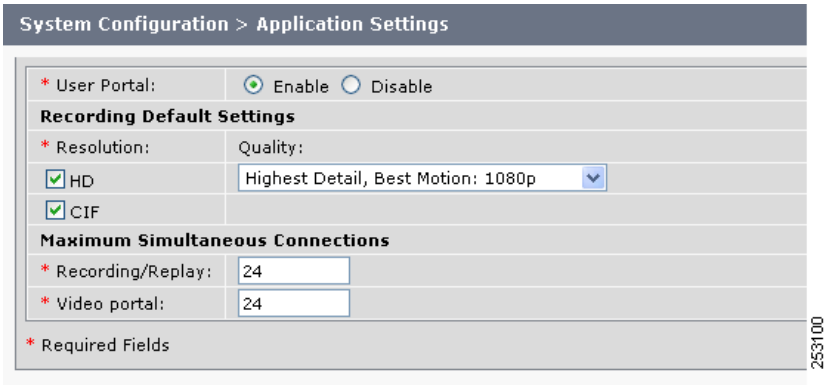
Step 2 Click the **Restart CTRS** tab.

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

Application Settings

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

Figure 4-7 System Configuration > Application Settings



Application Settings allow you to define general CTRS recording settings (see Table 4-5).

Table 4-5 Application Settings

Field or Button	Setting
User Portal	Click **Enable** to make the user portal available to users; click **Disable** to make the user portal unavailable. The user 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.
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 user 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 user portal. If you uncheck the CIF checkbox, the CTRS does not generate the file for playback in the browser-based user 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).

Table 4-5 Application Settings (continued)

Field or Button	Setting
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**.

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

Backup Settings

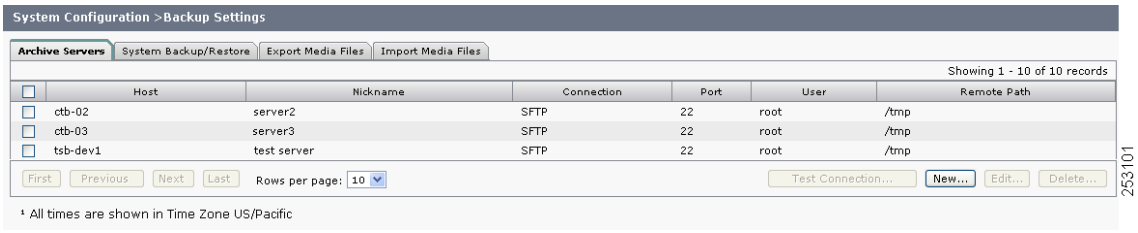
Backup Settings consist of the following tabs:

- Archive Servers, page 4-14
- System Backup and Restore, page 4-16
- Export Media Files, page 4-19
- Import Media Files, page 4-21

Archive Servers

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

Figure 4-8 System Configuration > Backup Settings—Archive Servers



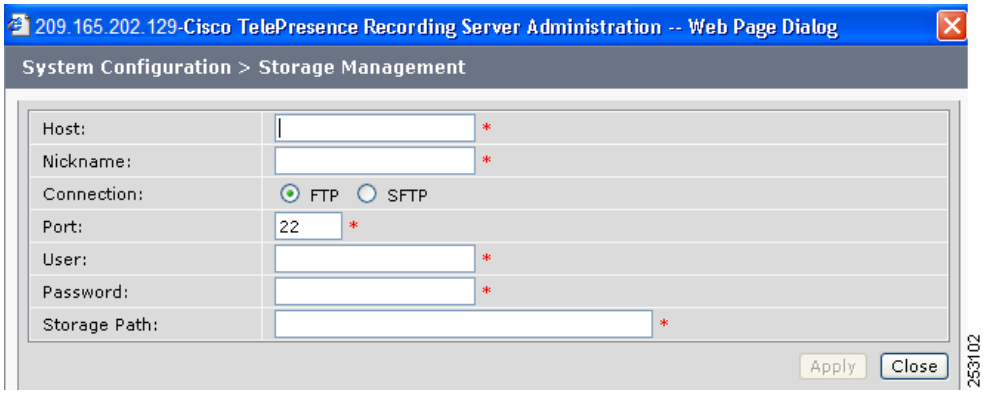
The Archive Servers screen displays a table providing the following information about previously defined archive servers:

Table 4-6 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 System Configuration > Backup Settings—Archive Servers (New or Edit)



When you click **Edit** or **New**, CTRS administration software takes you to the Storage Management screen, as described in Table 4-7. Use this screen to edit existing archive server settings or to define new archive servers.

Table 4-7 Storage Management Configuration Field Descriptions

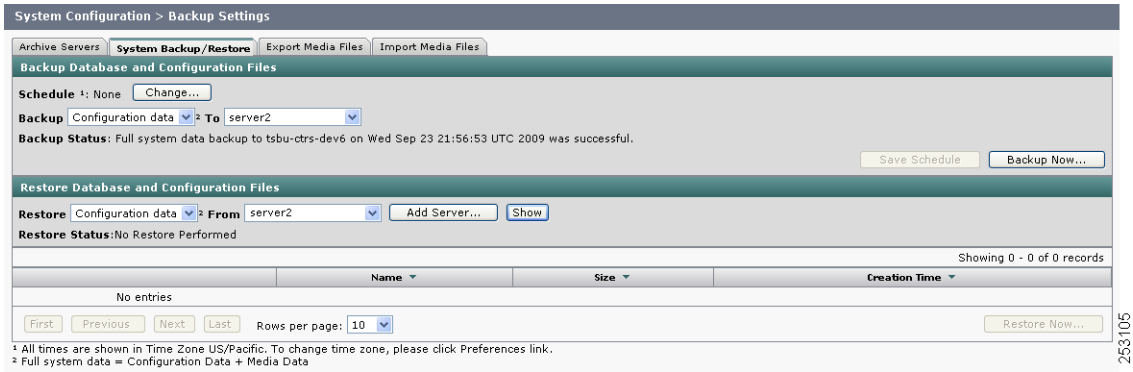
Field	Description
Host	Enter the host name of the archive server.
Nickname	Enter the nickname of the archive server. This nickname is used to identify the archive server throughout CTRS.
Connection	Click the appropriate radio button to define the connection through which this archive server is reached. 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**.

System Backup and Restore

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

Figure 4-10 System Configuration > Backup Settings—System 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 To define the time scheduled for the automatic backup, click **Change**. From the Change window, enter information for the following fields:

a. **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.

b. **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.

c. Click **OK** to apply your changes.

Step 2 Choose the content to be backed up from the **Backup** drop-down list.

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

Step 4 Click **Save Schedule**. 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 4-8.

Table 4-8 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.

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.

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 4-9.

Table 4-9 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 System Configuration > Backup Settings—Export Media Files

Use the Export Media Files screen to configure when CTRS transfers CTRS media data to a specified archive server. Export Media Files fields are described in Table 4-10.

Table 4-10 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.
Policy	Policy lets you establish additional rules governing the data that is transferred.
Media is older than:	Enter the number of days in the text box to determine the minimum age of the data exported. 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	Check this box if you want CTRS to export this data to an archive server.
Export to	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.
Notify video owner	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 reset to default values, click **Reset**.

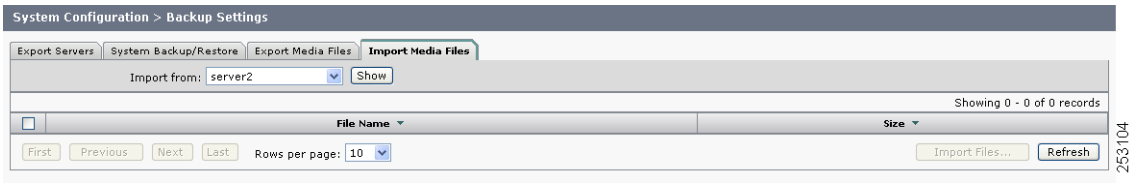
For example, in the Schedule field, you click the **Change** button. For Start Time, you choose **23:45**, and for Frequency, you choose **Daily**. In the Media is older than field, you enter **60**. As the Action to be taken daily at 23:45, you check the **Export** box and specify a server to which 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 System Configuration > Backup Settings—Import Media Files



The Import Media Files screen 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**.

Unified CM Settings

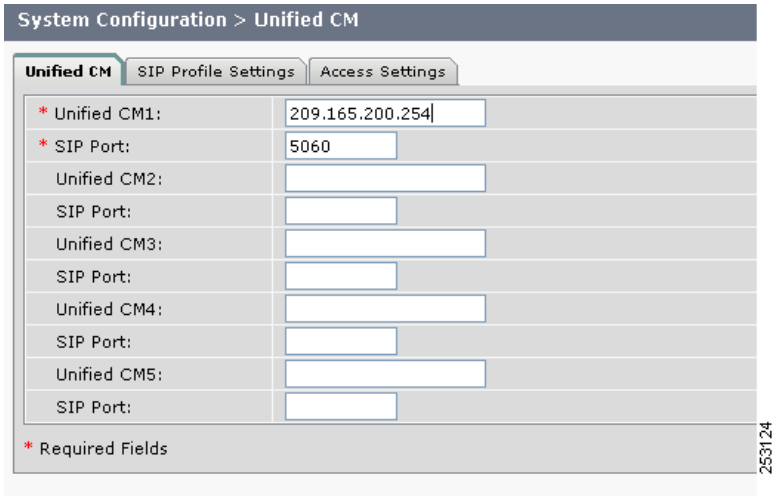
Cisco Unified Communications Manager Settings (Cisco Unified CM) consists of two configuration areas:

- Cisco Unified CM Settings, page 4-22
- SIP Profile Settings, page 4-23
- Access Settings, page 4-24

Cisco Unified CM Settings

In Unified CM, click the **Unified CM** tab to display or configure Cisco Unified CM servers and SIP ports (see Figure 4-13).

Figure 4-13 System Configuration > Unified CM—Unified CM



From the Unified CM tab, you can specify Cisco Unified Communications Manager servers and SIP ports (see Table 4-11).

Table 4-11 Cisco Unified CM Settings

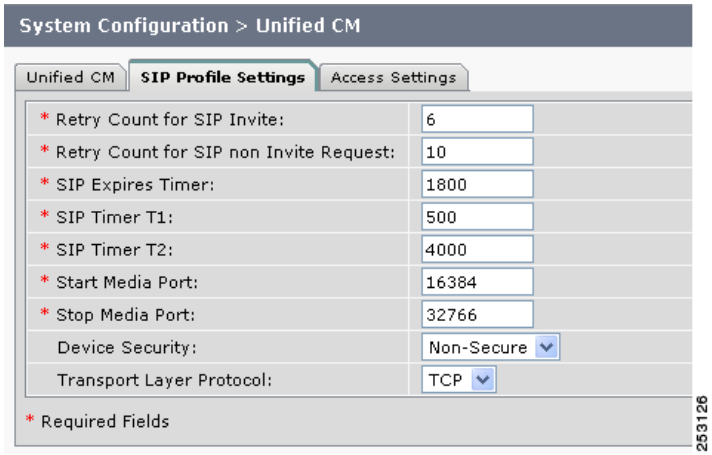
Field or Button	Setting
Cisco Unified CM 1 through 5	Hostnames or IP address(es) of the Cisco Unified Communications Manager (Unified CM) server. **Note** It is important to add all Unified CM servers in the cluster.
SIP Port	Port number for Cisco Unified SIP IP Phones that are using UDP to listen for 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 4-14).

Figure 4-14 System Configuration > Unified CM—SIP Profile Settings



SIP profile settings, which are described in Table 4-12, are applied to all SIP ports that you specify in the Unified CM tab.

Table 4-12 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.
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.

Table 4-12 SIP Profile Settings (continued)

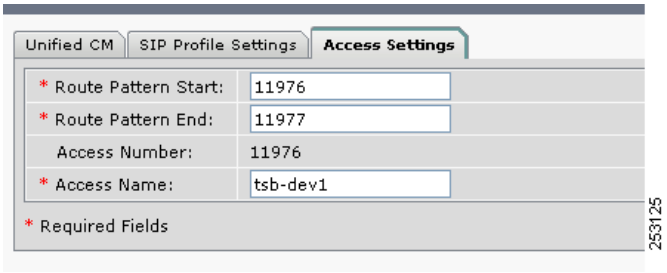
Field or Button	Setting
Stop Media Port	Designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. The default is for Cisco Unified Communications Manager (Unified CM) is 32766.
Device Security	Specifies the type of security applied to this CTRS. Available choices 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 4-15).

Figure 4-15 System Configuration > Unified CM—Access Settings



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

Table 4-13 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**.

User Management

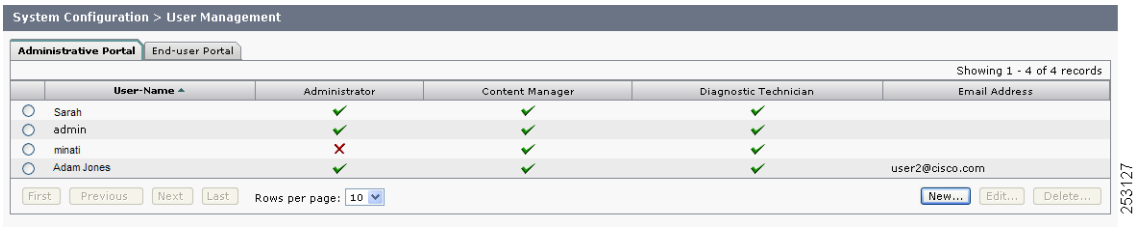
Use the fields under User Management to define CTRS administrators and to provide access to the user portal. User Management is divided into two tabs:

- Administrative Portal, page 4-25
- End-User Portal, page 4-29

Administrative Portal

In User Management, click the **Administrative Portal** tab to display or configure CTRS administrative roles (see Figure 4-16).

Figure 4-16 System Configuration > User 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 4-14:

Table 4-14 Administrative Portal Table Field Descriptions

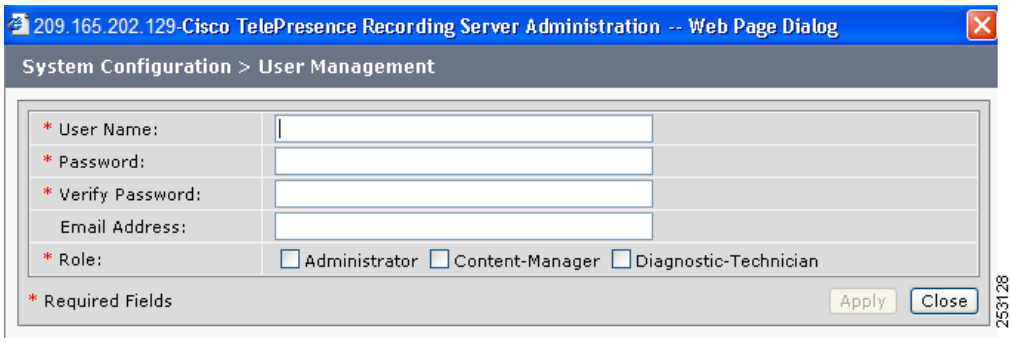
Field	Description
User-Name	User-name of a specific CTRS user.
Administrator	Administrators have the authority to perform all tasks associated with CTRS. Administrators have access to all menus in CTRS Administration software. A green check in this field indicates that the selected user has been designated as an administrator.
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 display a defined number of table rows, click the down arrow next to **Rows per page**. Highlight and select 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 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 4-17).

Figure 4-17 System Configuration > User Management—Administrative Portal (New)



Enter settings as described in Table 4-15.

Table 4-15 New User Management Settings

Field or Button	Setting
User Name	User name 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 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.

Table 4-15 New User Management Settings (continued)

Field or Button	Setting
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 screens 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 4-16.

Table 4-16 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.

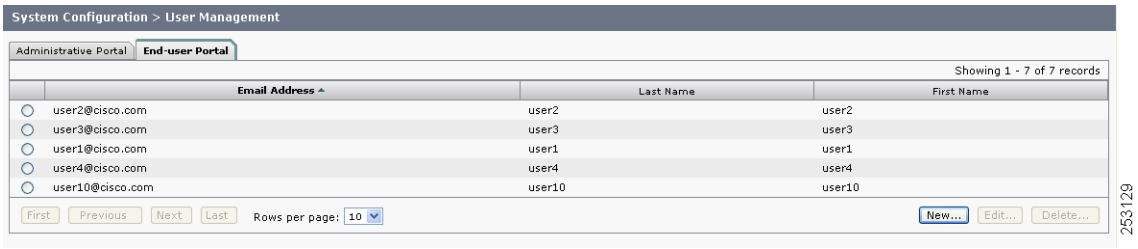
- To register new or modified settings, click **Save**.
- To close the window, click **Close**.

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 User Management, click the **End-user Portal** tab to display or configure users of the user portal (see Figure 4-18).

Figure 4-18 System Configuration > User Management—End-user Portal



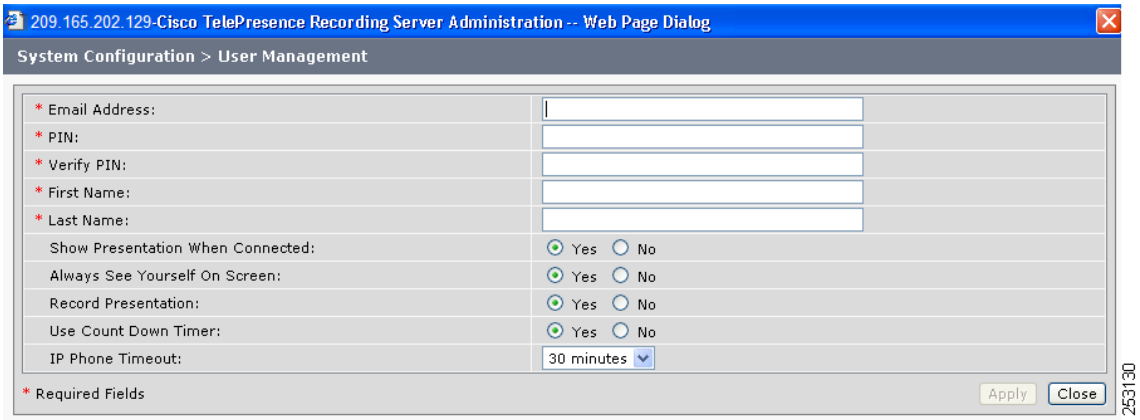
When you click the End-user Portal tab, you see a list of users with access to the CTRS user portal on an IP phone or through a web browser. Through the IP phone or the web browser, users can edit, view, and share videos. From the IP phone, users can also record videos.

- To specify the number of user entries that are displayed on the page, click the down arrow next to **Rows per page**. Click a number to display more or fewer entries.
- 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 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 4-19).

Figure 4-19 System Configuration > User Management—End-user Portal (New or Edit)



Enter settings as described in Table 4-17.

Table 4-17 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.
Last Name	Last name of 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 screen.
IP Phone Timeout	Choose how much time must elapse before the IP phone 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 user 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 4-18).

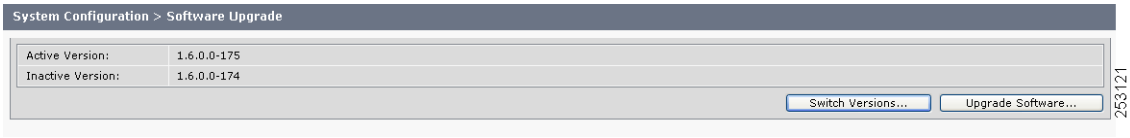
To learn how to create their own accounts, users should read the "Creating and Viewing Recordings with the Cisco TelePresence Recording Server" chapter in the *Cisco TelePresence System User Guide*:

http://www.cisco.com/en/US/docs/telepresence/cts_admin/1_6/userguide/cts1_6_ug.html

Software Upgrade

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

Figure 4-20 System Configuration > 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. 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 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

CTRS 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 (Unified CM) Root Certificates and a CAPF Root Certificate.

To configure CTRS for security, you need to first complete preliminary steps in Unified CM. You must activate and start CAPF service, create application users, create Unified CM root certificates for every Unified CM server associated with Cisco TelePresence service, and create a CAPF root certificate. Then from the Security Settings window in CTRS, you upload the applicable Unified CM and CAPF root certificates, and download the appropriate LSCs. When all certificates are in place and the LSC is downloaded, the CTRS reboots so that the security settings to take effect.

To configure CAPF Security for CTRS:

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 1.6*.

Step 2 **From Cisco Unified CM**: Create an application user in Cisco Unified CM. From the **Cisco Unified CM Administration** page, click **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, CTRS 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, Click **Application User CAPF Profile** from the ***User Management*** drop-down menu. Click **Add New**. Choose 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: Choose "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 CTRS 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, click **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: Choose "Encrypted"
- Incoming Transport Type: TLS
- Outgoing Transport Type TLS
- X.509 Subject Name: Enter the subject name of the CTRS 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, Click **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 select 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.

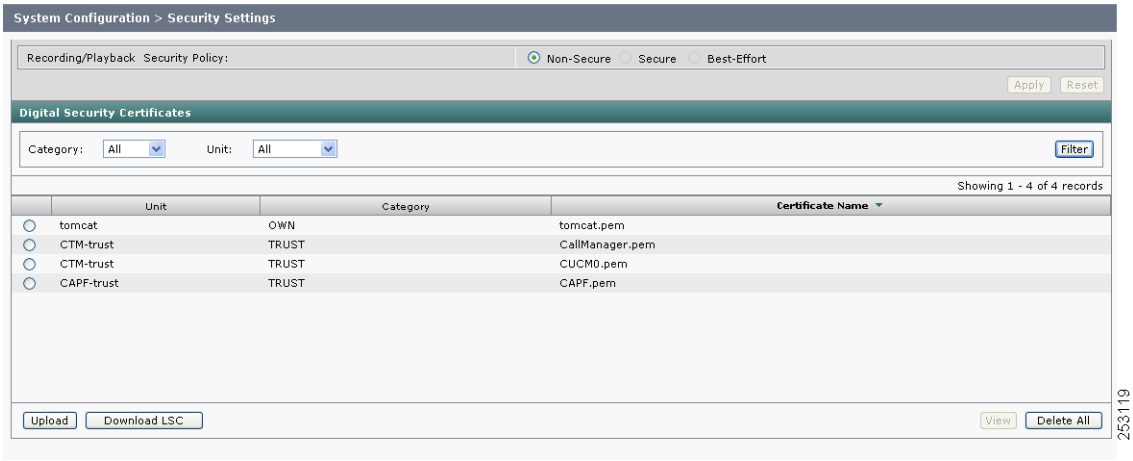
Step 6 **From CTRS**: Upload the CAPF Root Certificate in CTRS. From the **Security Settings** window in CTRS (see Figure 4-21), click **Upload**, then select:

- Unit: CAPF-Trust
- Category: TRUST

- Certificate: Choose the CAPF Root certificate that you downloaded from Cisco Unified CM (CAPF.der).

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

Figure 4-21 System Configuration > Security Settings



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, click **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 select 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 CTRS**: Upload the Cisco Unified CM Root Certificate(s) in CTRS. From the **Security Settings** window in CTRS, Click **Upload**. Select:

- Unit: CTM-Trust
- Category: TRUST
- Certificate: Choose 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 CTRS**: Download the LSC in CTRS. After creating the application user and application user CAPF profile, from CTRS, 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 CTRS reboots automatically.

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

To choose the default security level:

Step 1 **From CTRS**: After the system reboots, you can choose the default meeting security level. In System Configuration > Security, go to the Recording/Playback Security Policy area (see Figure 4-21).

Step 2 Click **Non-Secure**, **Secure**, or **Best Effort**.

- **Non-Secure** means that devices do not have to have valid Locally Significant Certificates (LSCs) from a Certificate Authority Proxy Function (CAPF) server.
- **Secure** means that devices must have valid LSCs from a CAPF server.
- **Best Effort** means that if a device has an LSC and others do not, the security level is Non-Secure.

Note To verify device security settings, go to System Configuration > Unified CM and click the SIP Profile Settings tab. If you choose Non-Secure from the Device Security drop-down menu, only Non-Secure is available as the Recording/Playback Security Policy setting.

Step 3 Click **Apply**.

Interface Failover

Click **Interface Failover** in the left menu to display or modify failover settings for Ethernet adapters (see Figure 4-22).

Figure 4-22 System Configuration > 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:

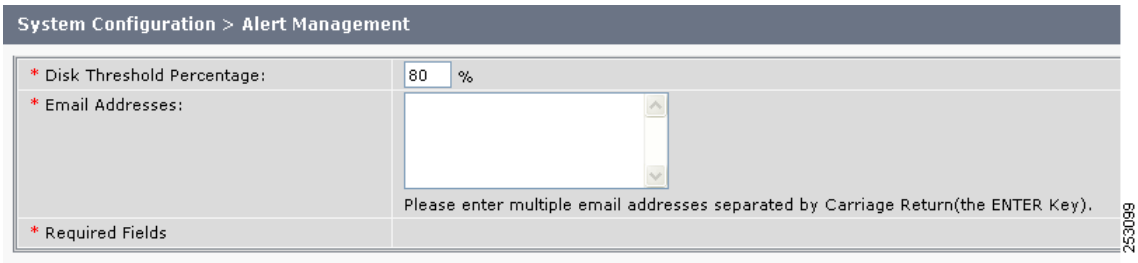
Step 1 With no active meetings in progress, click the **Disable** button.

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

Alert Management

Click **Alert Management** in the left menu to display or configure alert management settings (see Figure 4-23).

Figure 4-23 System Configuration > Alert Management



Use the Alert Management screen 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 4-18

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

Table 4-18 Alert Management Settings

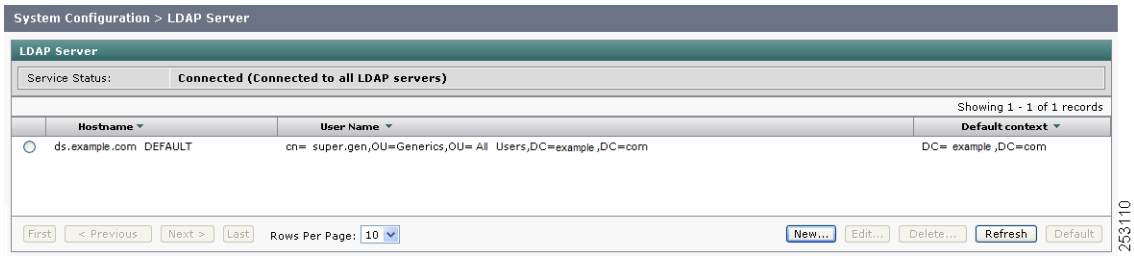
Field or Button	Setting
Disk Threshold Percentage	Enter a percentage. When the disk space reaches this threshold, CTRS sends an alert to the those listed in the Email Addresses field. 80% is the default.
Email Addresses	Enter email addresses. Recipients receive an email when the disk threshold reaches 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 **Submit**.
- To restore default settings, click **Reset**.

LDAP Configuration

Click **LDAD Configuration** in the left menu to display or modify the Lightweight Directory Access Protocol (LDAP) configuration (see Figure 4-24).

Figure 4-24 System Configuration > LDAP Configuration



Use the LDAP Configuration screen 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 4-19.

Table 4-19 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 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 table 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 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 screen (see Figure 4-25), as described in Table 4-20. Use this screen to edit existing archive server settings or to define new archive servers.

Figure 4-25 System Configuration > LDAP Configuration (New or Edit)

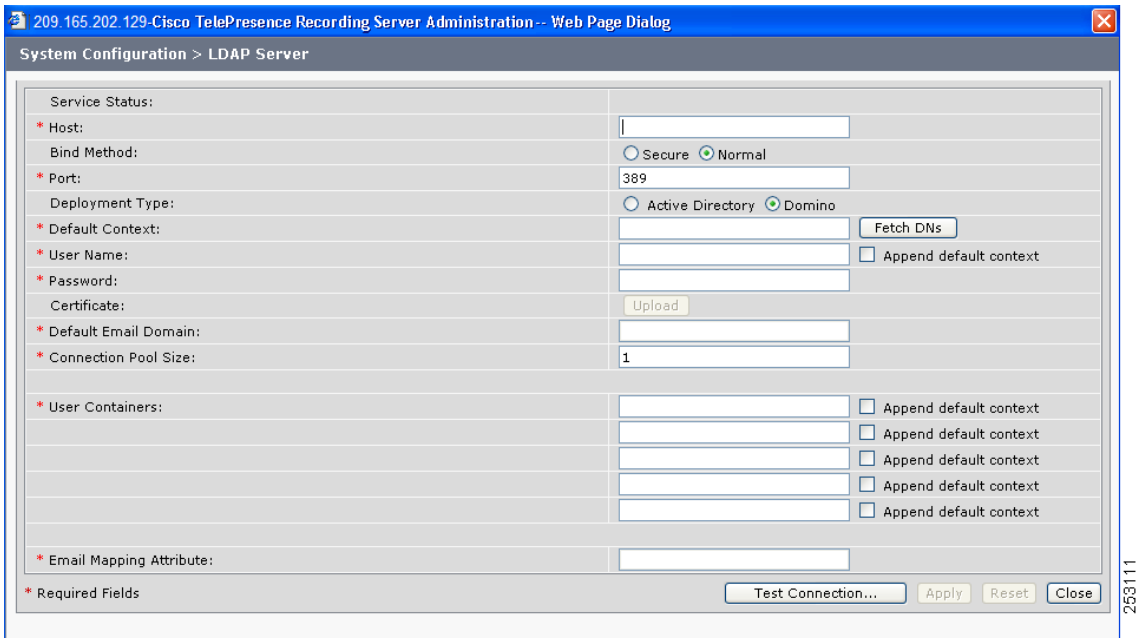


Table 4-20 New or Edit LDAP Configuration Table Field Descriptions

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.

Table 4-20 New or Edit LDAP Configuration Table Field Descriptions

Field or Button	Setting
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.
Deployment Type	Defines the LDAP server type. Options are **Active Directory** and **Domino**. click the appropriate radio button.
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 CTRS 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 4-20 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:

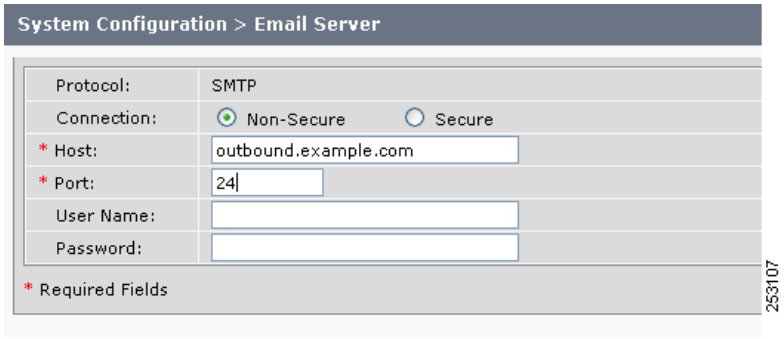
- cn=users, DC=cor1, DC=com
- cn=users, DC=cor2, DC=com

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

Email Server

Click **Email Server** in the left menu to display or modify e-mail server settings (see Figure 4-26).

Figure 4-26 System Configuration > Email Server



Use the Email Server screen to define the e-mail server that CTRS uses to send out alerts and video attachments. Fields in the Email Server screen are described in Table 4-21.

Table 4-21 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**.

CHAPTER 5

Managing CTRS Recordings

Revised: November 2009

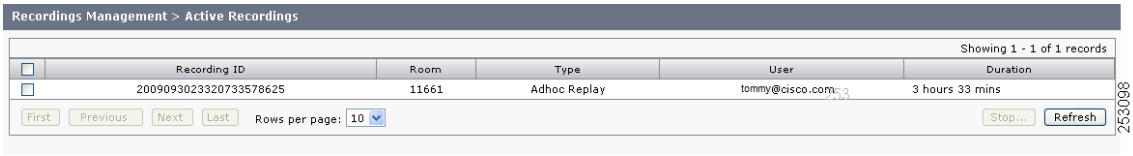
The following sections describe the Recordings Management features for the Cisco TelePresence Recording Server (CTRS). Recordings Management is divided into the following areas:

- Active Recording, page 5-1
- Completed Recordings, page 5-2
  - Exporting Recordings from the Completed Recordings List, page 5-4
  - Downloading a Recording to Your Computer, page 5-5

Active Recording

Click **Active Recordings** in the left menu to display all recordings that are being created currently (see Figure 5-1).

Figure 5-1 Recordings Management > Active Recordings



The Active Recordings screen displays a table that lists the following information about recording sessions that are currently in progress:

Table 5-1 Active Recording Table Field Descriptions

Field	Description
Select All	Check this box to select all active recording sessions.
Recording ID	Identification number for this recording session.
Room	Cisco TelePresence Room in which the recording is taking place.
Type	Type of recording.

Table 5-1 Active Recording Table Field Descriptions

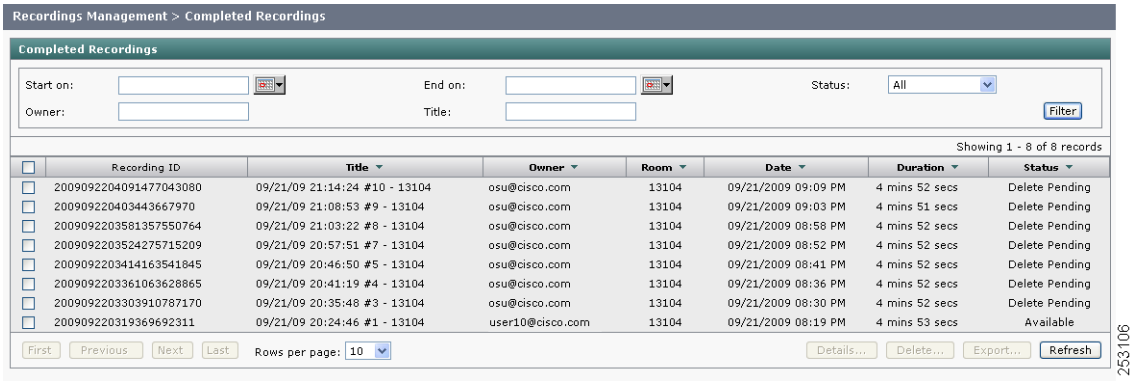
Field	Description
User	User who logged in and started the recording.
Duration	Length of time for this recording.

- To display a defined number of table rows, select the down arrow next to **Rows per page**. Click to highlight and select predetermined amounts.
- If the number of active recording sessions exceeds the Rows per Page value, click **First** to view the sessions 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 stop a recording in progress, click **Stop**.
- To refresh the information displayed, click **Refresh**.

Completed Recordings

Click **Completed Recordings** in the left menu to display completed recordings (see Figure 5-2).

Figure 5-2 Recordings Management > Completed Recordings



Use the Completed Recording screen to view or edit a list of all completed recordings that are currently stored on CTRS.

To filter entries in the Completed Recordings table:

Step 1 Click the calendar icon to the right of the **Start on:** text box to display a calendar. Click the beginning date for filtering completed recordings information.

Step 2 Click the calendar icon to the right of the **End on:** text box to display a calendar. Click the ending date for filtering completed recording information.

Step 3 Choose the appropriate value from the **Status** drop-down list. Choices are:

- All
- Available
- Delete Pending

Step 4 To filter using the owner of a recording, enter the owner name in the **Owner** text box.

Step 5 To filter using the title of a recording, enter the recording title in the **Title** text box.

Step 6 Click **Filter**.

Completed Recordings displays a table providing the following information about completed recordings, as described in Table 5-2:

Table 5-2 Completed Recordings Table Field Descriptions

Field	Description
Select All	Check this box to select all defined static meetings.
Recording ID	Recording identification number.
Title	Recording title.
Owner	Recording owner.
Room	Cisco TelePresence System room in which recording was produced.
Date	Date on which recording was produced.
Duration	Recording length
Status	Recording status. Statuses are as follows: • All—all videos in the list. • Available—videos that are available for deletion or export. • Delete Pending—videos that are scheduled for deletion. Videos show the Delete Pending status based on the number of days that are configured in the Delete field (System Configuration > Backup Settings—Export Media Files tab).

- To display a defined number of table rows, click the down arrow next to **Rows per page**. Highlight to select predetermined amounts.
- If the number of recordings exceeds the Rows per Page value, click **First** to view the recordings 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 displayed recordings, click **Refresh**.
- To delete a recording, check the box for that recording and then click **Delete**.
- To see details about a recording, check the box for that recording and then select Details. CTRS displays the following information about the recording, as described in Table 5-3. After viewing details about the recording, click **Close** to return to the Complete Recordings window.

Table 5-3 Recording Detail Table Field Descriptions

Field	Description
Recording ID	Recording identification number.
Title	Recording title (if defined)
Description	Description of recording (if defined)
Owner	Recording owner.
Recording Date	Date on which recording was produced.
Quality	Image quality of the recording.
Files	Files associated with the recording. To download and save a copy of the recording, click the file name.
Make recording viewable by everyone	Select this checkbox to make this recording available to all CTRS users.

Exporting Recordings from the Completed Recordings List

You can export recordings to a specified archive server. To export recordings, do the following:

Step 1 Check the box for the recording(s) that you want to export.

Step 2 Click **Export**. CTRS displays a table listing all of the recordings you selected for export.

Step 3 Choose the appropriate export destination server from the **Export to:** drop-down list.

Step 4 Click **Export**.

Note For more information about configuring export destination servers, see the "Archive Servers" section on page 4-14 of this guide.

Note When you export recording files, they remain on the CTRS. To delete recordings, check the boxes next to the recordings. Then click **Delete**.

Downloading a Recording to Your Computer

In addition to exporting a completed recording to an archive server, you can download a recording to your computer. To download, do the following:

Step 1 Check the box for the recording that you want to download.

Step 2 Click **Details**. The Recording Detail dialog box for that recording appears.

Step 3 In the Files section, click the filename of the file that you want to download. The "*xxx*_lo.mp4" file is the CIF version of the recording. The "*xxx*_ts.mp4" file is the HD version of the recording.

Step 4 In the dialog box that appears, click **Save** and specify where you want to save the file on your computer.

CHAPTER 6

Troubleshooting CTRS

Revised: November 2009

The following sections describe the Troubleshooting tools for the Cisco TelePresence Recording Server (CTRS):

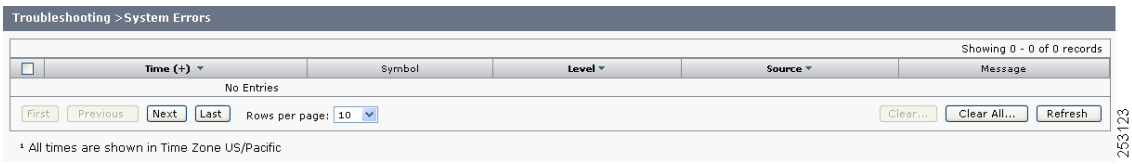
- CTRS Alarms and System Errors Messages, page 6-1
- Log Files, page 6-3

CTRS Alarms and System Errors Messages

You can view CTRS alarms, systems error and system warning messages in one of two ways:

- Click **System Errors** in the left menu (see Figure 6-1). The System Errors screen displays a list of all warning and error messages.

Figure 6-1 Troubleshooting > System Errors



- From the **System Status** bar, click the icon for **Warnings** or **Errors**.

If you click the icon for **Warnings**, you will see endpoint alert information. Warnings are issued every 20 seconds when an endpoint crosses its packet loss threshold. If congestion continues for more than 40 seconds, the endpoint will be dropped.

If you click the icon for **Errors**, you will see endpoint drop information. Whenever an endpoint drops from high packet loss, an error is issued with the error code “CONGESTION.”

The following table provides field descriptions for all system error and warning displays:

Table 6-1 System Error Field Descriptions

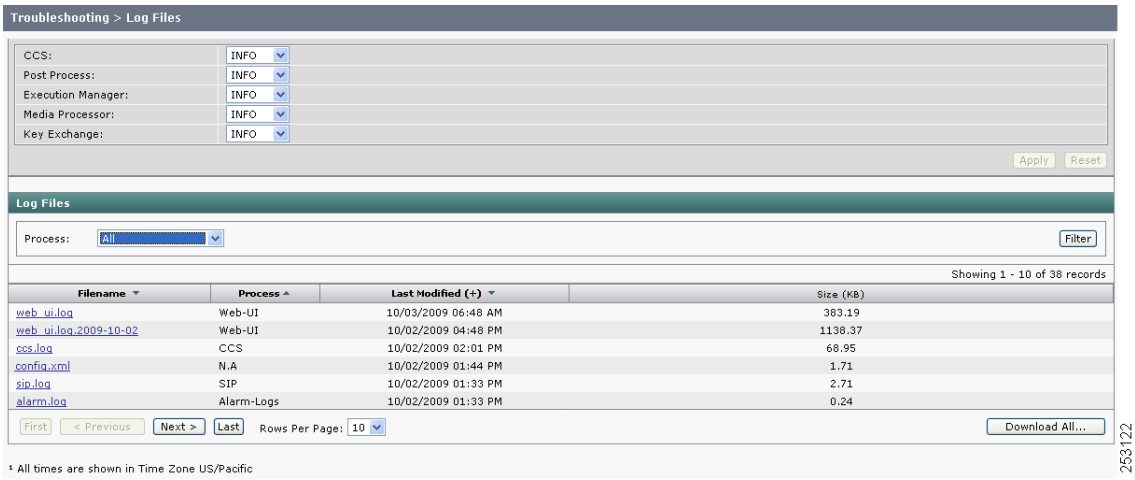
Field	Description
Select All	Check this box to select all system errors table entries listed.
Time	Displays the time at which this error occurred. Click the arrow to change the order (descending, ascending based on time) in which the errors are displayed.
Symbol	Text string (name) of the error message.
Level	Indicates the severity level of the error. There are eight severity levels as follows: • OFF • CRIT • ERROR • WARN • INFO • DEBUG Click the arrow to change the order (descending, ascending based on level) in which the errors are displayed.
Source	Indicates the CTRS system process associated with this alarm or error message. Click the arrow to change the order (descending, ascending based on source) in which the errors are displayed.
Message	Message describing the error.

- 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 there are multiple pages listing log files, click the **First**, **Previous**, **Next**, or **Last** button to navigate to the desired page.
- To delete one of the system error messages, click the radio button to the left of the table entry, and then click **Clear**.
- To delete all error messages displayed, click **Clear All**.

Log Files

Click **Log Files** in the left menu to display or modify log information (see Figure 6-2).

Figure 6-2 Troubleshooting > Log Files



Use the Log File screen to set severity levels for alarms associated with specific system processes, to filter log files displayed, and to download log files.

Configuring the Severity Level of System Error Messages

To configure the severity level of system level error messages and alarms for specific process areas:

Step 1 Click **Log Files** under **Troubleshooting** in the left menu to access the **Log Files** screen.

Step 2 At the top of the Log Files screen, there is a table listing the following CTRS system processes:

- CCS
- Post Processor
- Execution Manager
- Media Processor
- Key Exchange

To the right of each process is a drop-down list, listing the following severity levels:

- OFF
- CRIT
- ERROR
- WARN
- INFO
- DEBUG

Click the down arrow to display the drop-down list of defined levels of severity, and then highlight to select a specific severity level for all error messages and alarms associated a particular CTRS system process.

Note Log levels create varying amounts of data; for example, DEBUG creates more log entries than CRIT. Because verbose logs can impact system performance, use verbose logs only to track a problem.

Filtering the Log File Table Listings

To filter the log files displayed in the Log File Table:

Step 1 Click **Log Files** under **Troubleshooting** in the left menu to access the **Log Files** screen.

Step 2 At the middle of the Log Files screen, click the down arrow to the right of **Processes** to display a list of CTRS process areas, then click to highlight and select a specific process area on which to filter log files. Choices are the following:

- All
- CCS
- Execution Manager
- Media Processor
- Post Process
- Key Exchange
- SIP
- Web-UI
- CDR Logs
- Core
- Alarm Logs
- CTRS Sysop

Step 3 Click the **Filter** button to display the logs files associated with the selected process area in the Log Files table.

Downloading Log Files

To download log files from the Log File table:

Step 1 Click **Log Files** under **Troubleshooting** in the left menu to open the **Log Files** screen.

Step 2 At the bottom of the Log Files screen is the Log File table, which lists the available log files. The table is organized as described in Table 6-2.

Table 6-2 Log Table Field Descriptions

Field	Description
Filename	Filename of the log file. Click the arrow to change the order (descending, ascending based on alphabetical order of the filenames) in which the log files are displayed.
Process	CTRS system process area. Click the arrow to change the order (descending, ascending based on alphabetical order of the processes) in which the log files are displayed.
Last Modified	Time (Greenwich Mean Time, Pacific Standard Time) at which the log file was collected. Click the arrow to change the order (descending, ascending based on time) in which the log files are displayed.
Size	Size (in kilobytes) of the compressed log file.

Step 3 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 there are multiple pages listing log files, click the **First**, **< Previous**, **Next >**, or **Last** button to navigate to the desired page.

Step 4 Click the filename of a log file to download that file. Click the **Download All** button to download all log files listed.

CHAPTER 7

Monitoring CTRS System Processes

Revised: November 2009

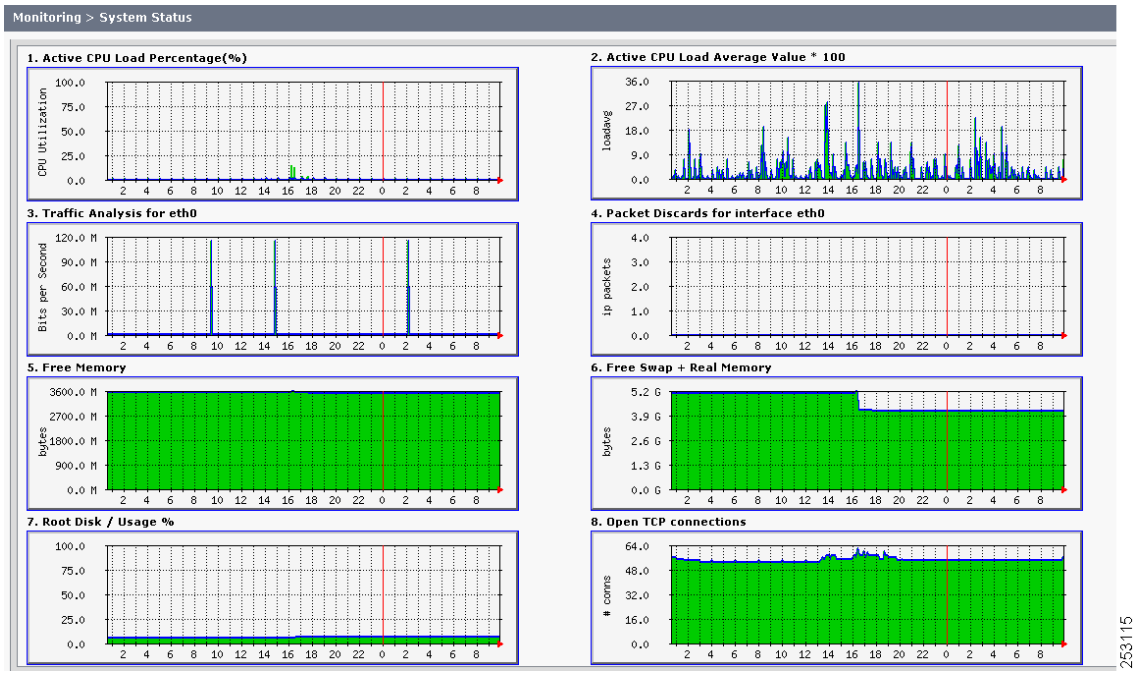
The Monitoring screen contains tools that enable you to monitor the overall CTRS system state and the running state of individual processes. The following sections describe the monitoring tools:

- System Status, page 7-2
- Process Status, page 7-3
- Hardware Status, page 7-4

System Status

Click **System Status** in the left menu to display statistics that are related to system status (see Figure 7-1).

Figure 7-1 Monitoring > System Status



The System Status screen provides snapshots of the following:

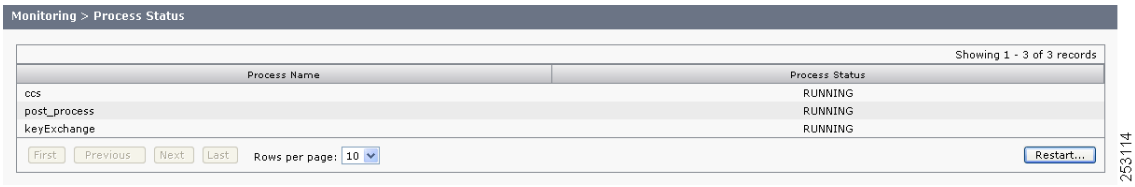
- Active CPU Load Percentage
- Active CPU Load Average Value
- Traffic Analysis for <interface>
- Packet Discards for <interface>
- Free Memory
- Free Swap + Real Memory
- Root Disk / Usage %
- Open TCP Connections

Click each snapshot to reveal daily, weekly, monthly and yearly averages.

Process Status

Click **Process Status** in the left menu to display processes that are currently running (see Figure 7-2).

Figure 7-2 Monitoring > Process Status



The Process Status screen displays a table that provides the following information:

Table 7-1 Process Status Table Field Descriptions

Field	Description
Process Name	Process name
Status	Status of this particular process.

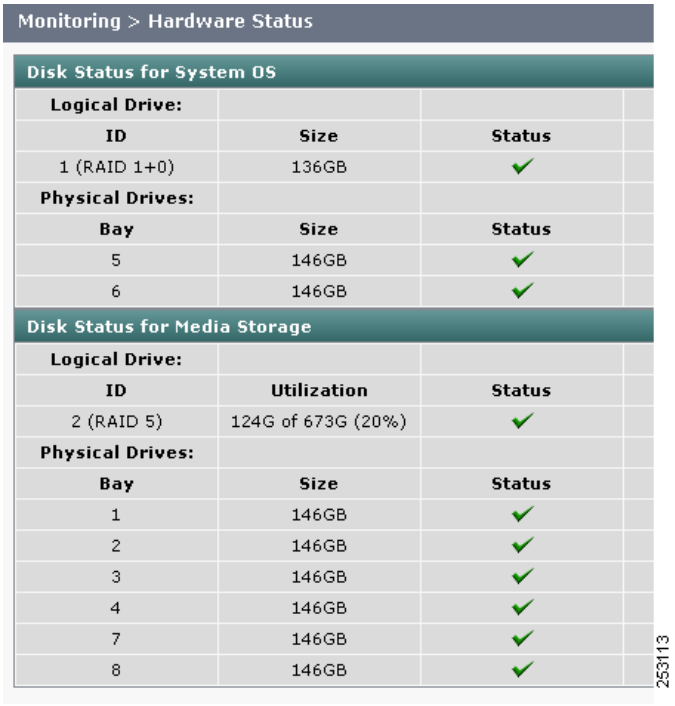
- To display a defined number of table rows, click the down arrow next to **Rows per page**. Click to highlight and select predetermined amounts.
- If the number of static meetings exceeds the Rows per Page value, click **First** to view the meetings listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.
- Click **Restart** to restart all of the processes.
- The information in the Process Status screen automatically refreshes every 10 seconds.

Caution When you restart CTRS system processes, all active meetings are dropped. Check for active meetings before using this command.

Hardware Status

Click **Hardware Status** in the left menu to display hardware-related information (see Figure 7-3).

Figure 7-3 Monitoring > Hardware Status



The Hardware Status screen lists the status of CTRS hardware. The information in this screen automatically refreshes every 10 seconds.

Table 7-2 Hardware Status Field Descriptions

Field	Description
Disk Status for System OS	
Logical Drive	
ID	Identification number
Size	Size of the partition
Status	Current status of that area of the hard drive.
Physical Drives	
Bay	Bay number
Size	Size of the partition
Status	Current status of that area of the hard drive.

Table 7-2 Hardware Status Field Descriptions (continued)

Field	Description
Disk Status for Media Storage	
Logical Drive	
ID	Identification number
Utilization	Current utilization of the drive
Status	Current status of that area of the hard drive.
Physical Drives	
Bay	Bay number
Size	Size of the partition
Status	Current status of that area of the hard drive.