



Cisco TelePresence Recording Server Release 1.8 Administration Guide

October 2011

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-24271-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

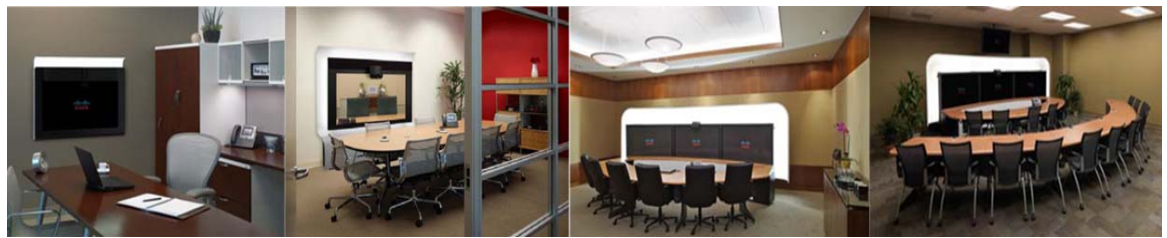
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco TelePresence Recording Server Release 1.8 Administration Guide
© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Contents i-vii

Obtaining Documentation and Submitting a Service Request i-x

CHAPTER 1

Using CTRS Administration Software 1-1

Contents 1-1

Overview of CTRS Tasks and Roles 1-1

Administrative Roles 1-2

Supported Web Browser Types 1-2

Logging in to the CTRS Administrative Interface 1-2

Overview of the Administrative Interface 1-2

Header 1-3

System Status 1-3

Left Navigation 1-4

Content Area 1-4

System Information 1-4

CHAPTER 2

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

CHAPTER 3

Installing CTRS Administration Software 3-1

Contents 3-1

Overview 3-1

Prerequisites 3-1

Preparing an UCS C-210 M2 Server for CTRS Software Installation 3-2

Requirements 3-2

Firmware Recommendation and Upgrade 3-3

Checking the Firmware Version on the UCS Server	3-3
Upgrading the Firmware on the UCS Server	3-3
Configuring RAID on the UCS Server	3-4
Installing VMware on the UCS Server	3-6
Installing the VMware Client and Creating the Virtual Machine	3-7
Disabling LRO (ESXi 4.1 only)	3-9
Importing the OVF Template	3-10
Installing CTRS Software	3-11
Upgrade VMware Tools	3-11
Installing the VMware License	3-12
Installing the CTRS Administration Software	3-13
Replacing a Hard Disk Drive	3-15

CHAPTER 4

Configuring CTRS Administration Software	4-1
Logging Into the Administrative Interface	4-2
Left Navigation of the Administrative User Interface	4-2
Access Management	4-3
Administrative Portal	4-3
End-User Portal	4-6
Creating a New User or Modifying Settings for an Existing User	4-7
Alert Management	4-9
Application Settings	4-10
Backup Settings	4-12
Archive Servers	4-12
Backup and Restore	4-15
Export Media Files	4-18
Import Media Files	4-20
Cisco Show and Share	4-21
Configuring the CTRS UI for Cisco Show and Share	4-22
Understanding the DMM User Name LDAP Attribute Field	4-23
Installing the Cisco Show and Share Server Security Certificate on the CTRS	4-23
CTS-Manager	4-25
Email Server	4-26
Interface Failover	4-27
LDAP Configuration	4-28
Configuring Multiple Domains in an LDAP Forest	4-31
Security Settings	4-32
Software Upgrades	4-32

System Settings	4-34
IP Settings	4-34
NTP Settings	4-36
QoS	4-37
SNMP	4-41
Configuring SNMP Traps on CTRS	4-42
Restart or Shutdown CTRS	4-46
Unified CM	4-46
Unified CM	4-47
SIP Profile Settings	4-48
Access Settings	4-50

CHAPTER 5**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

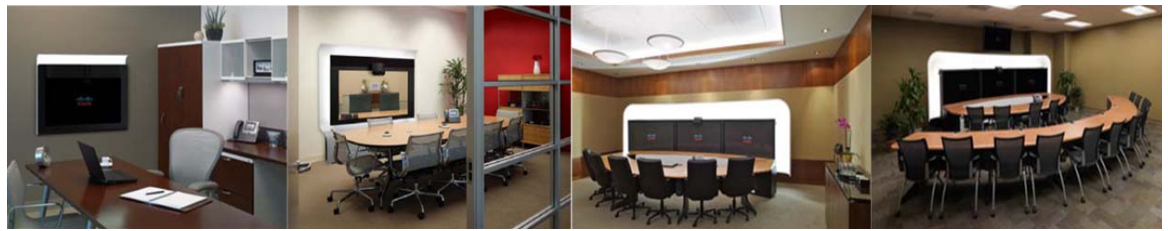
CHAPTER 6**Troubleshooting CTRS 6-1**

Dashboard	6-1
Process Status	6-4
Hardware Status	6-5
System Information	6-6
System Status	6-7
CTRS Alarms and System Errors Messages	6-8
Log Files	6-10

APPENDIX A**System Messages A-1**

System Message Overview	A-1
System Messages By Source	A-2
SVR Messages	A-2
DISK Messages	A-3
LDAP Messages	A-5
RMGR Messages	A-7
SNS Messages	A-10
SOAP Messages	A-12
CERT Messages	A-15

SMTP Messages	A-16
LCAL Messages	A-18
CCS Messages	A-18
MEDIA Messages	A-32
POST Messages	A-38
EXEMGR Messages	A-38



Preface

October 2011

Contents

- [General Description, page vii](#)
- [New in CTRS Release 1.8, page viii](#)
- [System Requirements, page x](#)
- [CTRS Release 1.8 Administration Guide Organization, page x](#)
- [Obtaining Documentation and Submitting a Service Request, page x](#)

General Description



Note

The initial release of CTRS is release 1.6.

The Cisco TelePresence Recording Server (CTRS) allows users to create recordings in Cisco TelePresence Studio Mode and using the Event Recording feature. The CTRS stores recordings created by both of these sources and enables users to manage the recordings as described:

- 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.
- Upload your recordings to a Cisco Show and Share video portal for editing and distribution.

Cisco TelePresence Studio Mode

CTRS enables users to record in 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.

The recordings can be either HD video and audio, or Common Intermediate Format (CIF). 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 log into the browser-based Cisco TelePresence Video 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).

Event Recording

Event Recording enables event controllers to record highly scripted events, such as company meetings. A CTRS records the event, while the Cisco TelePresence Multipoint Switch (CTMS) manages the recording session with the CTRS.

An event controller can manage an Event Recording session from the CTMS Administrative UI only. The CTMS Administrative UI enables the event controller to start, pause/resume, and stop the recording of the event.

After the event controller finishes recording an event, the recording is available through these interfaces:

- Cisco TelePresence Video Portal, which you can access using the following:
 - Cisco Unified IP Phone
 - Cisco Touch
 - A web browser
- CTRS Administrative UI

New in CTRS Release 1.8

The following features are new in Release 1.8.0:

- [Event Recording](#)
- [Troubleshoot > Dashboard Page](#)
- [Browser Security](#)
- [UCS Server](#)
- [TIP Support](#)

Event Recording

For information about the Event Recording feature, see the following:

- For a description of this feature, see the [“Event Recording” section on page viii](#).
- For information about creating an Event Recording from the CTMS Administrative UI, see the [Cisco TelePresence Multipoint Switch Administration Guide](#).

- For information about managing event recordings from the Cisco TelePresence Video Portal and using a Cisco Unified IP Phone or web browser, see the [Cisco TelePresence System User Guide](#).
- For information about managing event recordings using the Cisco TelePresence Touch 12, see the [Cisco TelePresence Touch 12 User Guide](#).
- For information about managing event recordings from the CTRS Administrative UI, see [Chapter 5, “Managing CTRS Recordings.”](#)

Troubleshoot > Dashboard Page

After you log into the CTRS Administrative UI, the Troubleshoot > Dashboard page appears. You can also access this page by clicking **Dashboard** in the left navigation.

The Troubleshoot > Dashboard page enables you to scan high-level reports on the following aspects of the CTRS:

- Disk usage for media storage
- Users
- Recordings
- Time
- Services

For more information on this page, see the [“Dashboard” section on page 6-1](#).

Browser Security

This new feature secures communication between the CTRS web server and the browser through which you access the CTRS Administrative UI. Browser security eliminates website security certificate warnings, which you receive if your web server is not secure.



Note

To implement browser security, you must buy a Secure Sockets Layer (SSL) certificate from a certificate authority (CA), then install it on the CTRS.



Note

Note On a CTRS, you can set up either inter-device security, which is an existing feature, or browser security, which is introduced in CTRS release 1.8. We do not support the deployment of both security features at the same time.

For more information on browser security, see the [“Configuring Cisco TelePresence Browser Security”](#) chapter of [Securing Cisco TelePresence Products, Release 1.8](#).

UCS Server

CTRS release 1.8 can be installed and run on a UCS C-210 M2 server. For more information about configuring and setting up the server before the CTRS software is installed, see [Chapter 3, “Installing CTRS Administration Software.”](#)

TIP Support

CTRS release 1.8 introduces support of Telepresence Interoperability Protocol (TIP) version 6.0 and version 7.0.

System Requirements

For Release 1.8 system requirements and hardware compatibility, please see the [Release Notes for Cisco TelePresence Recording Server, Release 1.8](#).

CTRS Release 1.8 Administration Guide Organization

The *CTRS Release 1.8 Administration Guide* is organized into the following chapters:

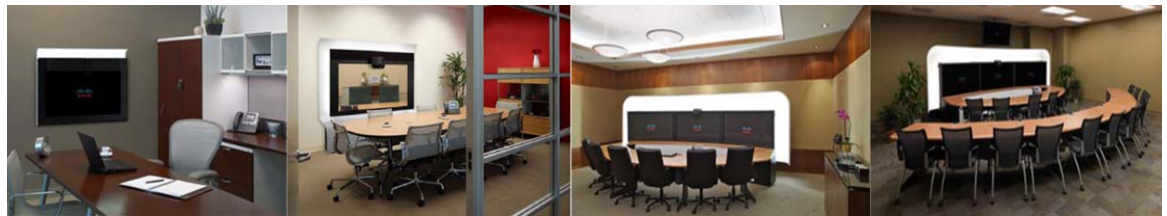
- Chapter 1: “Using CTRS Administration Software”
This section provides information about the CTRS Administration software interface
- Chapter 2: “Configuring Cisco Unified Communications Manager for CTRS”
This section provides instructions on how to configure Cisco Unified Communications Manager (Cisco Unified CM) so that it supports CTRS functionality.
- Chapter 3: “Installing CTRS Administration Software”
This section describes how to install the CTRS administration software on the Cisco UCS-C210-M2 server and 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 describes how to record meetings using CTRS Administration software.
- Chapter 6: “Troubleshooting CTRS”
This section describes how to monitor the CTRS system processes using the tools available in CTRS. It also explains how to view and categorize system error messages and alerts, and how to filter and download log files.

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

October 2011

Contents

- [Overview of CTRS Tasks and Roles, page 1-1](#)
- [Supported Web Browser Types, page 1-2](#)
- [Logging in to the CTRS Administrative Interface, page 1-2](#)
- [Overview of the Administrative 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 importing 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.”

Supported Web Browser Types

You can access the CTRS administrative interface using Internet Explorer version 7.x or 8.x, or with Firefox version 3.6.

Logging in to the CTRS Administrative Interface

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

-
- Step 1** Open a supported web browser.
- Step 2** In the address bar, enter **https://CTRS_URL/admin**.



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

- Step 3** Enter your username and password.
-

For more information about the initial installation of CTRS, including setting the administrator username and password for the first time, see [Chapter 3, “Installing CTRS Administration Software,”](#)

Overview of the Administrative 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](#)

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

Cisco TelePresence Recording Server

Admin Preferences Log Out Help

Manage
Active Recordings
Completed Recordings
Configure
Access Management
Alert Management
Application Settings
Backup Settings
Cisco Show and Share
Email Server
Interface Failover
LDAP Configuration
Security Settings
Software Upgrades
System Settings
System CUI
Troubleshoot
System Status
Process Status
Hardware Status
System Information
System Status
System Messages
Log Files

System Status
Active Sessions 1
Errors 0
Warnings 0
Status 0

Troubleshoot > Dashboard

Disk Usage for Media Storage

Total Size	5.0TB
Disk Utilization	21.85 (4.2% Full)

Users

End Users

Total Online Sessions:	0
Total Registered Users:	6

Administrator Users

Total Online Sessions:	2
Total Registered Users:	1

Recordings

Active Recordings and Playback:	0
Completed Recordings:	1,200

Error

System Time	Monday, September 12, 2011 8:47:55 PM (GMT +5)
Local Time	Monday, September 12, 2011 1:48:30 PM (GMT -07:00)

Services

LDAP:	OK
Show and Share	OK
Active Sessions	OK
CTS Manager	N/A

As of 12:38:28

© 2006-2011 Cisco Systems, Inc.

- `<username>`—In [Figure 1-1](#), the username is **admin**.
- 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 recording times to your location.
- Help—Click to display online help.
- Logout—Click to log out of the system.
- About—Click to display software version and licensing information.

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 Emergency, Alert, Critical, 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 6: 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 6: 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 7: Monitoring CTRS System Processes.”

Left Navigation

In the left navigation, CTRS tasks are organized under Manage, Configure, and Troubleshoot. The most frequently performed tasks are at the top of the navigation and the lesser tasks are toward the bottom.

When you click a link in the left navigation, content specific to that task is displayed in the content area of the page.

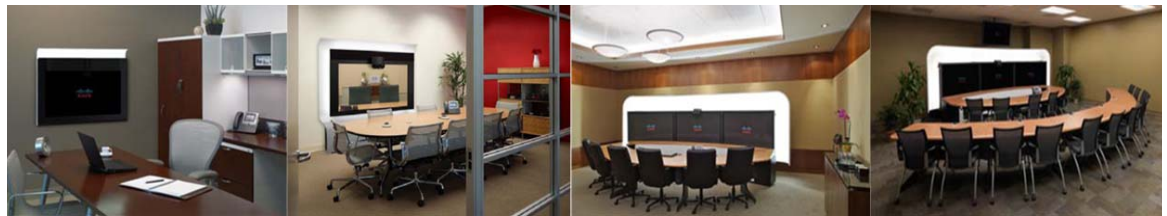
Content Area

The right side of the page is the content area. When you click a link in the left navigation, the content associated with that item displays in the content area.

System Information

Click **System Information** under **Troubleshooting** in the left navigation to view information about the Cisco TelePresence Recording Server. 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-I3 CCE4 Media Convergence Server on which the CTRS is running
- **Hardware Model:** Model number of the Cisco MCS-7845-I3 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

October 2011

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-I3 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 Communications Manager (Cisco Unified CM), Release 7.1.5, Release 8.5.1, or Release 8.6.1.



Note If recording meetings that will include Cisco TelePresence TC version 5.0 endpoints, Cisco Unified CM Release 8.6.1 is required

- 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 [Cisco TelePresence Administration Software Compatibility Information](#).

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 <i>Non Secure</i> . If you are running SIP security, select <i>Encrypted</i> .
Incoming Transport Type	Yes	Select <i>TCP+UDP</i> . If Encrypted is selected, TLS will be entered automatically.
Outgoing Transport Type	Yes	Select <i>TCP</i> .
Incoming Port	Yes	Enter <i>5060</i> 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 <i>Default</i> .
SIP Information		
Destination Address	Yes	Enter the IP address of the CTRS.

Table 2-2 SIP Trunk Settings

Field	Required	Setting
SIP Trunk Security Profile	Yes	Select the SIP trunk security profile that you created for CTRS.
SIP Profile	Yes	Select <i>Standard SIP Profile</i> .

- 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:

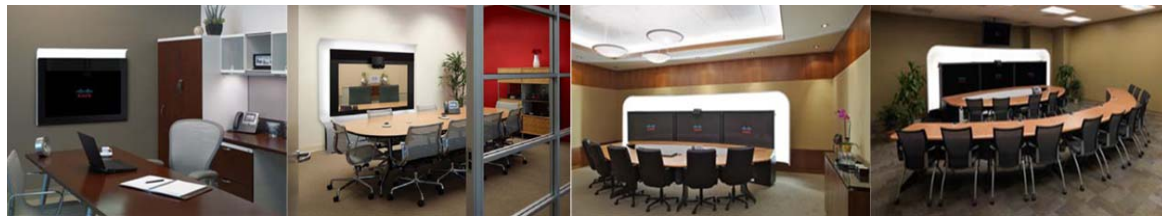
-
- Step 1** Click *Call Routing*. Under **Route/Hunt**, click *Route Pattern*.
- Step 2** Click the *Add New* button at the bottom or click the + *sign* at the top of the Route Pattern Configuration page.

- 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	<p>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.</p> <p> Note See the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the <i>Cisco CallManager System Guide</i> for more information about wildcards.</p>
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 <i>OnNet</i> .

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



CHAPTER 3

Installing CTRS Administration Software

October 2011

Contents

- [Overview, page 3-1](#)
- [Prerequisites, page 3-1](#)
- [Preparing an UCS C-210 M2 Server for CTRS Software Installation, page 3-2](#)
- [Installing the CTRS Administration Software, page 3-13](#)
- [Replacing a Hard Disk Drive, page 3-15](#)

Overview

This chapter explains how to install Cisco TelePresence Recording Server (CTRS) release 1.8 software on the following servers:

- UCS C-210 M2 server
- Cisco MCS-7845-XX-CTRS server, where XX can be I2 or I3

Before installing CTRS software on a UCS C-210 M2 server, you must configure the server and install VMWare. For an MCS-7845-XX-CTRS server, no server preparation is required. You simply install the software on the server.

Prerequisites

Before you install the CTRS administration software system files, you need the following equipment and information:

- Cisco TelePresence System assembled and configured to support TelePresence conferencing. For more information, refer to the appropriate *Cisco TelePresence System Administrator's Guide* and the appropriate *Cisco TelePresence Assembly Guide*.
- Cisco MCS-7845-XX-CTRS server, where XX can be I2 or I3, 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-XX-CTRS server, where XX can be I2 or I3.

- DVD that contains the CTRS Administration software application.
- Cisco Unified Communications Manager (Cisco Unified CM) Release 7.0.2, Release 7.1.5, Release 8.5.1, or Release 8.6.1, 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 Configuration Guide for the Cisco TelePresence System](#).



Note If recording meetings that will include Cisco TelePresence TC version 5.0 endpoints, Cisco Unified CM Release 8.6.1 is required

Preparing an UCS C-210 M2 Server for CTRS Software Installation

Before installing CTRS administration software on a UCS C-210 M2 server, you must configure and install VMWare on the server. This section is comprised of the following topics:

- [Requirements, page 3-2](#)
- [Configuring RAID on the UCS Server, page 3-4](#)
- [Installing VMware on the UCS Server, page 3-6](#)
- [Installing the VMware Client and Creating the Virtual Machine, page 3-7](#)
- [Disabling LRO \(ESXi 4.1 only\), page 3-9](#)
- [Importing the OVF Template, page 3-10](#)
- [Installing CTRS Software, page 3-11](#)
- [Upgrade VMware Tools, page 3-11](#)
- [Installing the VMware License, page 3-12](#)

Requirements

Before you begin, make sure you have the following items:

- Hostname and IP address for the VMware ESXi host
- Hostname and IP address for the CTRS
- IP address of DNS server
- Subnet mask
- Default gateway
- Domain name
- IP address of NTP server
- Cisco UCS Server Configuration Utility CD
- VMware ESXi 4.1/vSphere 5 Standard for 1 processor (Purchase from Cisco or VMware.)
 - When purchasing from Cisco, use the following SKU: VMW-VS5-STD-1A
 - When downloading the VMware software, make sure to select ESXi 4.1.

- ESXi 4.0 is also supported.
- OVF template file for CTRS (Download from Cisco.com)
- PC running Microsoft Windows connected to the same network as the UCS server

Firmware Recommendation and Upgrade

For the best results, Cisco recommends UCS firmware version 1.2.2d or later.

Checking the Firmware Version on the UCS Server

To check the firmware version on the UCS server:

-
- Step 1** Set up Cisco Integrated Management Controller (CIMC) for your UCS Server.
For details, refer to:
http://www.cisco.com/en/US/products/ps10493/products_configuration_example09186a0080b10d66.shtml
- Step 2** In the CIMC Configuration Utility, configure the IP address and save the changes:
- NIC mode: dedicated
 - NIC redundancy: none
- Step 3** Open a browser and go to the CIMC IP address.
- Step 4** Log in to the CIMC
By default, the username is **admin** and the password is **password**.
- Step 5** Go to **Admin > Firmware Management**.
The firmware version is displayed here. It is also displayed on the login page.
- Step 6** If you want to upgrade the firmware, go to the next section: [Upgrading the Firmware on the UCS Server, page 3-3](#)
-

Upgrading the Firmware on the UCS Server

To upgrade the firmware on the UCS server:

-
- Step 1** Download the firmware from Cisco:
- a. Go to: <http://cisco.com/support>
 - b. Click the **Downloads** tab
 - c. Click in the Find field, enter **UCS** and click **Find**.
The Select a Product page appears.
 - d. Click the link for the **Cisco UCS C-210 M2 Rack-Mount Server Software**.
The Download Software page appears.
 - e. Click the link for **Unified Computing System (UCS) Server Firmware**.
The available firmware releases are displayed.

- f. Select a firmware release and click **Download Now**.
- g. Log in to Cisco.com (if required).
- h. In the Download Cart page, click **Proceed With Download**.
The End User License Agreement page appears.
- i. Click **Agree**.
- j. Select one of the available download options.
- k. Click the **Download** link.

Step 2 Log in to the CIMC (if not already logged in).

Step 3 Go to **Admin > Firmware Management**

Step 4 Click **Install CIMC Firmware through Browser Client**.

The Install Firmware window appears.

Step 5 Click **Browse**, select the firmware you downloaded and click **Install Firmware**.

Step 6 When a message appears indicating the upgrade is completed successfully, click **Activate CIMC Firmware**.

Step 7 The upgrade takes about 20 minutes.

Step 8 When the upgrade is complete, reboot the UCS server.

Configuring RAID on the UCS Server

This section describes the process for configuring RAID on the UCS server. RAID must be configured before installing VMware, setting up the virtual machine and installing the CTRS software.



Note

If the UCS server was purchased from the TelePresence Technology Group (TTG) or Voice Technology Group (VTG) at Cisco, the RAID will be preconfigured. In this case, skip this section and start in the [“Installing VMware on the UCS Server”](#) section on page 3-6.

To configure RAID on the UCS Server:

Step 1 Insert the Cisco UCS Server Configuration Utility CD and reboot UCS server.

Cisco UCS Server Configuration Utility version 1.0.0 screen appears.

Step 2 Wait for application to load and the License Agreement screen to appear.

Step 3 Click **I Accept** and click **Next**.

The My Server screen appears.

Step 4 Click **RAID Configuration**

The Choose RAID Controllers screen appears.

Step 5 Click **LSI MegaRAID SAS 9261-8i (External)** and click **Next**.

Step 6 The RAID Configuration screen appears.

- Step 7** Click **Create custom or multiple RAID Arrays (advanced)** and click **Next**.
The Select Drives for Logical Drive screen appears.
- Step 8** Select Disks **0** and **1** and click **Next**.
The Select Hotspare Drives screen appears.
- Step 9** Click **Next**.
The Define Array Attributes screen appears.
- Step 10** Set the fields the following way:
- RAID Level: **1**
 - Stripe size: **64k** (only option)
 - Read policy: **Read Ahead** (other options: No Read Ahead, Adaptive Read Ahead)
 - Write Policy: **Write Through** (other option: Write Back)
 - Cache Policy: **Direct IO** (other option: Cache IO)
 - Size (MB): **139236**
- Step 11** Click **Next**.
The Summary screen appears displaying RAID array information.
- Step 12** Click **Create Array**.
The Array Definition Complete screen appears with the message “Virtual Drive Created Successfully”.
- Step 13** Click **Create Another Array**.
The Choose RAID Controllers screen appears.
- Step 14** Click **LSI MegaRAID SAS 9261-8i (External)** and click **Next**.
- Step 15** Click **Create custom or multiple RAID Arrays (advanced)** and click **Next**.
The Select Drives for Logical Drive screen appears.
- Step 16** Select disks **2** through **9** and click **Next**.
The Define Array Attributes screen appears.
- Step 17** Set the fields the following way:
- RAID Level: **5**
 - Stripe size: **64k** (only option)
 - Read policy: **Read Ahead** (other options: No Read Ahead, Adaptive Read Ahead)
 - Write Policy: **Write Through** (other option: Write Back)
 - Cache Policy: **Direct IO** (other option: Cache IO)
 - Size (MB): **974652**
- Step 18** Click **Next**.
The Summary screen appears displaying RAID array information.
- Step 19** Click **Create Array**.
The Array Definition Complete screen appears with the message “Virtual Drive Created Successfully.”
- Step 20** Click **Finish**.
The My Server screen appears.

Step 21 Eject the CD.

Installing VMware on the UCS Server

This section describes how to install VMware on the UCS C-210 M2 server. VMware ESXi 4.0 and 4.1 are supported for this version of CTRS on the UCS C-210 M2 server.

To install VMware on the UCS server:

Step 1 Insert the VMware Installer CD.

Step 2 Reboot the UCS server by doing either of the following:

- If RAID on your UCS server was preconfigured by Cisco: Reboot the UCS server.
- If you configured RAID on your UCS (following the steps in the previous section): In the My Server screen, click **Exit** and then click **OK** to confirm and reboot the UCS server.

The VMware screen appears.

Step 3 Wait for the bootup process to complete. Do not press any keys.

The bootup is complete when the VMware ESXi Installer screen appears with a welcome message.

Step 4 Press **Enter** to install VMware.

The End User License Agreement (EULA) screen appears.

Step 5 Press **F11** to accept the agreement and continue.

The Select a Disk screen appears displaying the installed disks and their size.

Step 6 Use the arrow keys to select the disk for the RAID 1 array and press **Enter**.



Note

The RAID 1 array is the smaller of the two RAID arrays.

The Confirm Install screen appears.

Step 7 Press **F11** to start the installation.

The installation begins.

The installation is finished when the Installation Complete screen appears.

Step 8 Eject the VMware CD.

Step 9 Press **Enter** to reboot the UCS server.

When bootup is complete, the VMware ESXi screen appears with the message:

“Download tools to manage this host from:” followed by a URL.

Step 10 Press **F2** to customize the system.

The System Customization screen appears.

Step 11 Select Configure Password (selected by default) and press **Enter**.

The Configure Password screen appears.

Step 12 In the New Password field, enter a password and press **Tab**.

- Step 13** In the Confirm Password field, re-enter that password and press **Enter**.
- Step 14** Select **Configure Management Network** and press **Enter**.
The Configure Management Network screen appears.
- Step 15** Select Network Adaptors (selected by default) and press **Enter**.
The Network Adaptors screen appears.
- Step 16** Select the adaptor which is connected and press **Enter**.
- Step 17** Select IP configuration and press **Enter**.
The IP Configuration screen appears.
- Step 18** Select **Set Static IP address and network configuration**.
- Step 19** Enter IP address, Subnet Mask and Default Gateway and press **Enter**.
- Step 20** Select **DNS Configuration** and press **Enter**.
- Step 21** The DNS Configuration screen appears.
- Step 22** Select **Use the following DNS server addresses and hostname**.
- Step 23** Enter Primary DNS Server and Hostname and press **Enter**.
- Step 24** Select **Custom DNS Suffixes** and press **Enter**.
The Custom DNS Suffixes screen appears.
- Step 25** Enter your company's domain followed by a comma, a space and "localdomain" and press **Enter**.
For example: `yourcompany.com, localdomain`
- Step 26** In the Configure Management Network window, press **Esc** to return to the System Customization window.
- Step 27** Select Test Management Network and press **Enter**.
The Test Management Network screen appears.
- Step 28** Press **Enter**.
The VMware software will attempt to ping your default gateway, DNS server and hostname. The test should display "OK" for each ping attempt.
- Step 29** Press **Enter**.
The System Customization window appears.
- Step 30** Log out of the VMware ESXi Installer by pressing **Esc**.
The VMware ESXi screen appears.
- Step 31** Note the IP address displayed on this screen. You will use this IP address to download the VMware vSphere client to your PC to create your virtual machine in the next section.
-

Installing the VMware Client and Creating the Virtual Machine

This section describes how to install the VMware vSphere Client and create the virtual machine. To complete this procedure, you must use a PC that is connected to the same network as your UCS server.

To set up the virtual machine:

Step 1 From your PC, open a web browser and go to the IP address displayed on the VMware ESXi screen at the end of the previous section.

The VMware ESXi Welcome page appears.

Step 2 Click Download vSphere Client and follow the on-screen instructions to install the vSphere Client on your PC.

Step 3 Open the VMware vSphere Client.

Step 4 Log in to the ESXi host on the UCS server using the following information:

- IP address / name: IP address of UCS server (used in step 1)
- User name: **root**
- Password: VMware password created during installation on the UCS server

A Security Warning window appears, indicating that an untrusted SSL certificate is installed.

Step 5 Click the checkbox for “Install this certificate and do not display any security warnings” and click **Ignore**.

A VMware Evaluation Notice window appears, indicating that you must upgrade your ESX Host license. The initial evaluation license expires 60 after installation.

Step 6 You can upgrade it now, by following the instructions starting in step 2 of [Installing the VMware License, page 3-12](#) or click **OK** if you want to upgrade later.

The vSphere Client window opens with the UCS server (identified by IP address) displayed in the left-hand side of the window.

The next step is to align the datastore on which you will set up your virtual machine (the largest volume). This improves disk performance and prevents disk blocks from being fragmented.

Step 7 Click the **Summary** tab.

Step 8 In the Datastore area, right-click the datastore with the largest capacity and select **Delete**.

A confirmation window appears.

Step 9 Click **Yes** to confirm you want to delete the datastore.

In the Recent Tasks area at the bottom of the window, the Remove Datastore task appears.

Step 10 Wait for the task to display a status of “Completed.”

Step 11 Click the **Configuration** tab.

Step 12 In the Hardware area on the left, click **Storage**.

In the Datastores area, the remaining datastore is displayed.

Step 13 In the upper right above the Datastores area, click **Add Storage....**

The Add Storage window opens and the Select Storage Type screen is displayed.

Step 14 **Select Disk/LUN** (selected by default) and click **Next**.

The Select Disk/LUN screen appears.

Step 15 Click the **Local LSI Disk** and click **Next**.

The Current Disk Layout screen appears confirming the disk partition you will create.

Step 16 Click **Next**.

The Properties screen appears.

- Step 17** Enter a name for your datastore and click **Next**.
The Disk/LUN Formatting screen appears.
- Step 18** From the Maximum file size drop-down list, choose **256 GB**, **Block size: 1 MB** and make sure **Maximize Capacity** is checked.
- Step 19** Click **Next**.
The Ready to Complete screen appears.
- Step 20** Click **Finish**.
In the Recent Tasks area at the bottom of the window, the Create VMFS Datastore task appears.
- Step 21** Wait for the task to display a status of “Completed.”
After completion, you have two datastores. The datastore with the smaller capacity is the RAID 1 configuration, where the VMware software is installed, and the datastore with the larger capacity is the RAID 5 configuration, where you will deploy the virtual machine and install the CTRS software.
-

Disabling LRO (ESXi 4.1 only)

If you are running VMware ESXi 4.1 on the UCS server, you may experience slow TCP performance of the virtual machine. You can resolve this by disabling Large Receive Offload (LRO) on the ESXi host.

To disable LRO:

-
- Step 1** Log into the ESXi host on the UCS server with the VMware vSphere Client (if not already logged in).
- Step 2** Click the UCS server icon in the left-hand side of the window.
- Step 3** Click the **Configuration** tab.
- Step 4** In the Software section, click **Advanced Settings**.
- Step 5** Select **Net** and scroll down slightly more than half way.
- Step 6** Set the following parameters from 1 to 0:
- Net.VmxnetSwLROSL
 - Net.Vmxnet3SwLRO
 - Net.Vmxnet3HwLRO
 - Net.Vmxnet2SwLRO
 - Net.Vmxnet2HwLRO
- Step 7** Right-click the UCS server and select **Reboot**.
Your virtual machine should now have normal TCP networking performance.
-

Importing the OVF Template

This section describes how to deploy the Open Virtualization Format (OVF) template for CTRS to create the virtual machine on which to install the CTRS software. OVF is a standard for packaging and distributing virtual machines. The OVF template streamlines the process of setting provided by Cisco contains all the virtual machine settings required for the CTRS.

The OVF template for CTRS is provided by Cisco.

To install the OVF template:

-
- Step 1** Download the OVF template from Cisco:
- Go to: <http://cisco.com/support>
 - Click the **Downloads** tab
 - Click in the Find field, enter **Cisco TelePresence Recording Server** and click **Find**.
The Select a Product page appears.
 - Click the link for the **Cisco TelePresence Recording Server Release 1.8**.
The Download Software page appears.
 - Select **CTRS.ova** and click **Download Now**.
 - Log in to Cisco.com (if required).
 - In the Download Cart page, click **Proceed With Download**.
The End User License Agreement page appears.
 - Click **Agree**.
 - Select one of the available download options.
 - Click the **Download** link.
- Step 2** Log into the ESXi host on the UCS server with VMware vSphere Client (if not already logged in).
- Step 3** Select **File > OVF Template**.
The Deploy OVF Template window opens.
- Step 4** Select **Deploy from File**.
- Step 5** Click **Browse**
- Step 6** Select the OVF template for the TelePresence product you want to install and click **Open**.
- Step 7** Click **Next**.
The OVF Template Details page appears.
- Step 8** Click **Next**.
- Step 9** Enter a name for your virtual machine and click **Next**.
The Datastore page appears.
- Step 10** Click the largest datastore and click **Next**.
The Ready to Complete page appears.
- Step 11** Click **Finish**.
-

Installing CTRS Software

This section describes how to install CTRS software on the virtual machine you created and configured.

To install CTRS administration software:

-
- Step 1** Insert the installer DVD into your PC.
 - Step 2** Log into the ESXi host on the UCS server with VMware vSphere Client (if not already logged in).
 - Step 3** In the left-hand side of the window, click the virtual machine you created and click the **Console** tab.
 - Step 4** Right-click your virtual machine and choose **Power > Power On**.
 - Step 5** On the toolbar, click the button with the CD and Wrench icon and wait for the menu to pop up.
 - Step 6** Choose **CD/DVD Drive 1 > Connect to ISO image on local disk. . .** and open the .iso image for CTRS.

**Note**

If you have a DVD inserted in your PC instead of an .iso, you can connect to the CD/DVD drive by selecting for the CD/DVD drive letter.

In the console window, the installer startup process begins.

- Step 7** Click inside the console window to make it active, so you can use your keyboard during the installation process.

**Note**

After clicking in the console window, you can no longer use your mouse. This is normal behavior, because you cannot use the mouse in the console. If at any time you need to regain control of your mouse, press **Ctrl+Alt**. To make the console window active again, click in the console window.

- Step 8** Follow the rest of the installation as detailed in [“Installing the CTRS Administration Software” section on page 3-13](#)
 - Step 9** After completing the installation, press **Ctrl+Alt** to exit the console window and regain control of your mouse.
 - Step 10** Close the VMware vSphere Client by selecting **File > Exit**.
-

Upgrade VMware Tools

This section describes how to upgrade the VMware tools which is required after installing CTRS.

To upgrade VMware tools:

-
- Step 1** Log into the ESXi host on the UCS server with VMware vSphere Client.
 - Step 2** Make sure the virtual machine for CTRS is powered on.
 - Step 3** Right-click the CTRS virtual machine, and choose **Guest > Install/Upgrade VMware Tools**.

- Step 4** In the popup window that appears, choose **Automatic Tools Upgrade** and click **OK**.
 - Step 5** In the Recent Tasks area at the bottom of the vSphere Client window, wait for the VMware Tools Installer Mount to display a status of Completed.
-

Installing the VMware License

This section describes how to install the VMware software license. After installation, the VMware vSphere Client software works for 60 days, after which you must upgrade to a host license to continue using it to manage the CTRS.

To install the VMware license:

- Step 1** Log in to the VMware vSphere Client.
The VMware vSphere Client opens and a VMware Evaluation Notice window appears, indicating that you must upgrade your ESX Host license.
- Step 2** Click **Upgrade your ESX host license**.
A browser window opens and the VMware vSphere page appears.
- Step 3** Enter your First Name, Last Name, Email Address and click **Continue**.
The Evaluate VMware Products page appears.
- Step 4** Enter the additional required information, agree to the terms and conditions and click **Register**.
The VMware vSphere Product Evaluation Center page appears.
- Step 5** Check the email account for the email address you provided in step 4 and open the email titled “Activate VMware Account.”
- Step 6** Click **Activate Now**.
A browser window opens and the Enter Your Password page appears.
- Step 7** Enter the password you created in step 4 and click **Continue**.
The Account Activate page appears informing you that your account has been activated and then the VMware vSphere Product Evaluation Center page appears.
- Step 8** In the VMware vSphere Client, close the VMware Evaluation Notice window by clicking **OK**.
- Step 9** Click the **Configuration** tab.
- Step 10** In the Software area on the left side of the vSphere Client window, click **Licensed Features**.
The Licensed Features information for the ESX Server License Type appears.
- Step 11** In the upper-right part of the window, click **Edit**.
The Assign License window appears.
- Step 12** Click **Assign a new license key to this host** and click **Enter Key**.
- Step 13** The Add License Key window appears.
- Step 14** Enter the license key you received from VMware and click **OK**.
License information appears below the key you entered.

- Step 15** Click **OK**.
- Step 16** In the Recent Tasks area at the bottom of the vSphere Client window, wait for the Installing license and Decode license tasks to display a status of Completed.
-

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 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 pages 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 page, re-enter the data, and then proceed to the **Platform Configuration** page 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 page is displayed. Enter your username and password to continue with CTRS Administration software configuration.

Replacing a Hard Disk Drive

This section describes how to replace a hard disk drive in a Cisco MCS-7845-Ix server on which CTRS software is running.



Caution

We do not recommend replacing a hard disk drive while the CTRS is powered on, a process known as hot swapping. Hot swapping a hard disk drive can result in configuration data loss as well as loss of stored videos.

Step 1 Perform a backup of the CTRS configuration data only.

A backup of the CTRS configuration data may be needed if the scenario described in step 6 occurs. If this scenario occurs, the CTRS configuration data cannot be restored from a backup of the full system data, so make sure to perform a backup of the CTRS configuration data only.

Step 2 Export the media files (videos) to an archive server.

Step 3 Power down the CTRS.

Step 4 Replace the hard disk drive.

Step 5 Power on the CTRS.

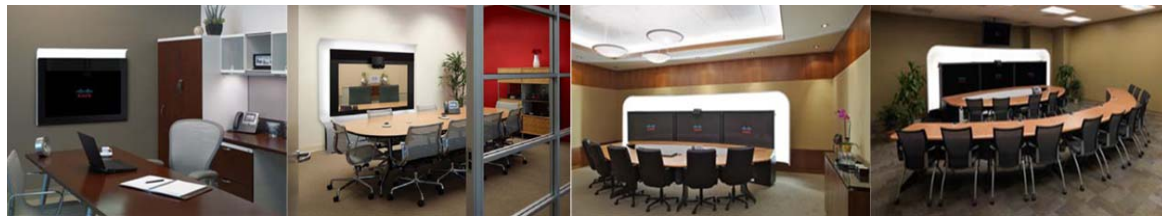
Step 6 If the CTRS is unresponsive, you must re-install the CTRS software.

For complete information on how to install the software, see the *Cisco TelePresence Recording Server Administration Guide* at this location:

http://www.cisco.com/en/US/products/ps10341/prod_maintenance_guides_list.html

Step 7 Restore the configuration data.

Step 8 Import the archived media files to the CTRS.



CHAPTER 4

Configuring CTRS Administration Software

October 2011

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

- [Logging Into the Administrative Interface, page 4-2](#)
- [Left Navigation of the Administrative User Interface, page 4-2](#)
- [Access Management, page 4-3](#)
- [Alert Management, page 4-9](#)
- [Application Settings, page 4-10](#)
- [Backup Settings, page 4-12](#)
- [Cisco Show and Share, page 4-21](#)
- [CTS-Manager, page 4-25](#)
- [Email Server, page 4-26](#)
- [Interface Failover, page 4-27](#)
- [LDAP Configuration, page 4-28](#)
- [Security Settings, page 4-32](#)
- [Software Upgrades, page 4-32](#)
- [System Settings, page 4-34](#)
- [Unified CM, page 4-46](#)

Logging Into the Administrative Interface

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

-
- Step 1** Open a supported web browser.
- Step 2** In the address bar, enter **https://CTRS_URL/admin**.



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

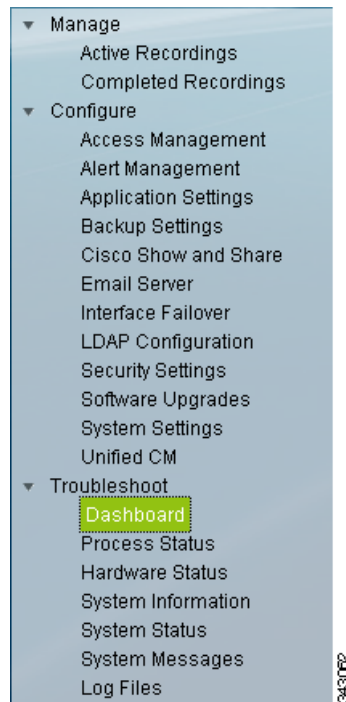
- Step 3** Enter your username and password.
-

For more information about the initial installation of CTRS, including setting the administrator username and password for the first time, see [Chapter 3, “Installing CTRS Administration Software.”](#)

Left Navigation of the Administrative User Interface

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

Figure 4-1 *Configure—Left Navigation*



Access Management

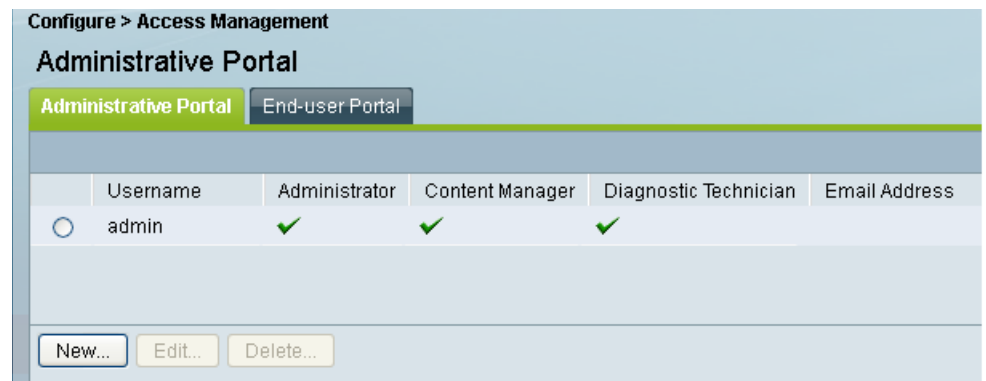
Use the fields under Access Management to define CTRS administrators and to provide access to the Cisco TelePresence Video Portal. Access Management is divided into two tabs:

- [Administrative Portal, page 4-3](#)
- [End-User Portal, page 4-6](#)

Administrative Portal

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

Figure 4-2 *Configure > Access Management—Administrative Portal*



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

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

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

Table 4-1 *Administrative Portal Table Field Descriptions*

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

Table 4-1 Administrative Portal Table Field Descriptions

Field	Description
Content Manager	Content managers are responsible for managing activities associated with recording. They can only access CTRS Recording Management and System Status windows. A green check in this field indicates that the selected user has been designated as a content manager.
Diagnostic Technician	Diagnostic Technicians have the authority to perform CTRS monitoring and troubleshooting tasks. Diagnostic Technicians have access to the Troubleshooting and Monitoring windows in CTRS Administration software. A green check in this field indicates that the selected user has been designated as a diagnostic technician.

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

Creating a New Administrative User

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

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

Configure > Access Management

* User Name:

* Password:

* Verify Password:

Email Address:

* Role: ☐ Administrator ☐ Content-Manager ☐ Diagnostic-Technician


* = Required fields

Apply Close

343037

Enter settings as described in [Table 4-2](#).

Table 4-2 **New Access Management Settings**

Field or Button	Setting
User Name	<p>Username identifying a defined role as selected from the Role field.</p> <p>Note A username must be at least 5 characters, but not more than 64 characters in length. The username must contain letters and numbers, but it cannot contain special characters, except for the underscore character. Letters can be uppercase and lowercase.</p> <p>The username cannot be all numbers.</p> <p>The following usernames are not allowed: apache, daemon, nobody, operator, and shutdown.</p>
Password	<p>Password for the username indicated in the User name field.</p> <p>Note Passwords must be at least 6 characters, but not more than 64 characters.</p>
Verify Password	Re-enter the password defined for this user.
Email Address	Email address for this defined user.
Role	<p>Defines a specific user role. In CTRS Administration software, there are three possible roles, each with specific levels of administrative access:</p> <ul style="list-style-type: none"> • Administrator: Administrators have access to all pages and configuration tasks in CTRS Administration software. • Content Manager: Content managers are responsible for managing activities associated with recording. They can only access CTRS Recording Management and System Status windows. • Diagnostic Technician: Diagnostic Technicians have access only to Monitoring and Troubleshooting windows and one task (system restart) in CTRS Administration software. <p></p> <p>Note A single user can have more than one role.</p> <p>Click the appropriate radio button(s).</p>

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

**Note**

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

Editing a Defined Administrative User

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

Table 4-3 Edit Administrative User Settings

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

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

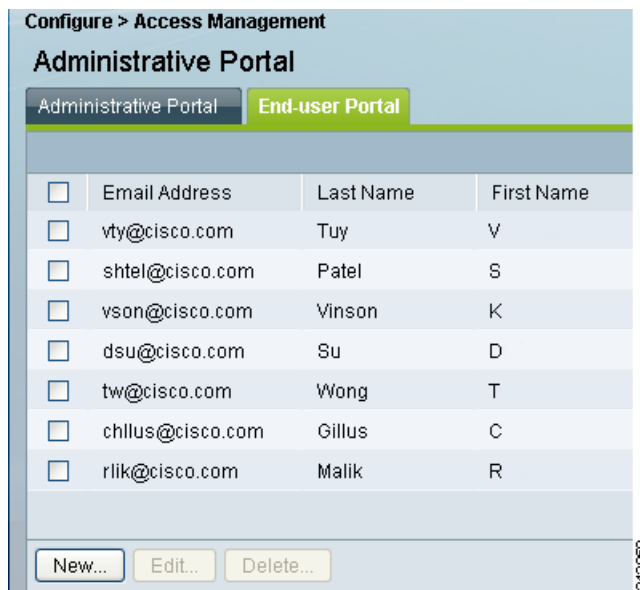
End-User Portal



Note

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

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

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

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

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

Creating a New User or Modifying Settings for an Existing User

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

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

Configure > Access Management

✱ Email Address:

PIN:

Verify PIN:

✱ Time Zone: (UTC+00:00) Etc/UTC ▼

Observes DST: **No**

✱ Language (Locale): English (United States) ▼

Show Presentation When Connected: ☒ Yes ☐ No

Always See Yourself on Screen: ☒ Yes ☐ No

Record Presentation: ☒ Yes ☐ No

Use Count Down Timer: ☒ Yes ☐ No

Session Timeout: 15 minutes ▼

✱ = Required fields

Enter settings as described in [Table 4-4](#).

Table 4-4 *User Settings*

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

Table 4-4 **User Settings (continued)**

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

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

**Note**

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

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

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

Alert Management

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

Figure 4-6 *Configure > Alert Management*

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



Note

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

Table 4-5 *Alert Management Settings*

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

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

Application Settings

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

Figure 4-7 *Configure > Application Settings*

Configure > Application Settings

User Portal: ☒ Enable ☐ Disable

Recording Default Settings

Resolution: ☒ HD ☒ CIF
 Quality: Highest Detail, Best Motion: 1080p

Maximum Simultaneous Connections

Recording/Replay: 24

Select locales for users who create or view videos:

To install more locales, download language packs from [cisco.com](#), and go to [Software Upgrades](#)

Available: German (Germany), Hebrew (Israel), Italian (Italy), Japanese (Japan), Korean (South Korea), Norwegian (Norway), Portuguese (Brazil), Russian (Russian Federation), Simplified Chinese (China), Spanish (Mexico)

Selected: English (United States) (Default)

Locale	Default	Number of Users
English (United States)	<input checked="" type="radio"/>	5

= Required fields

Apply Reset

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

Table 4-6 *Application Settings*

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

Table 4-6 **Application Settings (continued)**

Field or Button	Setting
HD	<p>High Definition. Click checkbox to choose.</p> <p>Note CTRS can generate two recording files. The file called “xxx_ts.mp4” is for playback on an endpoint. The file called “xxx_lo.mp4” is for playback in the browser-based Cisco TelePresence Video Portal.</p> <p>If you uncheck the HD checkbox, the CTRS does not generate the file for playback on an endpoint.</p>
CIF	<p>Common Intermediate Format (CIF). Click checkbox to choose.</p> <p>Note CTRS can generate two recording files. The file called “xxx_ts.mp4” is for playback on an endpoint. The file called “xxx_lo.mp4” is for playback in the browser-based Cisco TelePresence Video Portal.</p> <p>If you uncheck the CIF checkbox, the CTRS does not generate the file for playback in the browser-based Cisco TelePresence Video Portal.</p>
Quality	<p>Defines the recording quality. Choices are:</p> <ul style="list-style-type: none"> • 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) <p>Highlight option to choose. Default value is Highest Detail, Best Motion: 1080p.</p> <p>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).</p>
Maximum Simultaneous Connections	
Recording/Replay	<p>Defines the number of simultaneous recording and replaying sessions that can occur. Range is from 1 to 24. Default is 24.</p>
Select locales for users who create or view videos	
Available and Selected locales	<p>By default, English (United States) is the selected as well as the default locale. The Available and Selected windows allow you to select more locales that are available to users who create videos using Studio Mode and Event Recording and view videos using the Cisco TelePresence Video Portal.</p> <p>Note Currently, language packs are not yet available on Cisco.com, so more locales cannot be selected.</p>

Table 4-6 *Application Settings (continued)*

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

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

Backup Settings

Backup Settings consist of the following tabs:

- [Archive Servers, page 4-12](#)
- [Backup and Restore, page 4-15](#)
- [Export Media Files, page 4-18](#)
- [Import Media Files, page 4-20](#)


Archive Servers

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

Figure 4-8 *Configure > Backup Settings—Archive Servers*

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

Table 4-7 *Archive Servers Table Field Descriptions*

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

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

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

Configure > Storage Management

✱ = Required fields

✱ Host:

✱ Nickname:

✱ Connection: ☒ FTP ☐ SFTP

✱ Port:

✱ User:

✱ Password:

✱ Storage Path:

343058

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

Table 4-8 *Storage Management Configuration Field Descriptions*

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

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

Backup and Restore

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

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

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

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

To schedule a system backup:

- Step 1** In **Schedule**, click the **Change** button to set the backup schedule. In the dialog box that appears, set the backup start time and frequency. Click **OK** to apply.
- Step 2** Choose the content to be backed up from the **Backup** drop-down list. Options are **Configuration data** and **Full system data**. Full system data includes configuration files, videos, and video metadata.
- Step 3** Choose the archive server where the data will be stored from the **To** drop-down list.
- Step 4** Click **Save Backup Settings**. The contents of the CTRS database will be sent to the indicated server on the defined day(s) at the scheduled time.



Note

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

To perform an immediate system backup:

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

Backup database fields are described in [Table 4-9](#).

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

Field	Description
Schedule Daily at <time>	<p>This field shows the time (U.S. Pacific time zone, twenty-four hour format) when automatic backups are scheduled to occur.</p> <p>To change the time scheduled for the automatic backup, click Change. From the Change window:</p> <ul style="list-style-type: none"> • 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	<p>Define the content that you want to backup. Click the down arrow to view choices; highlight choice to select. Choices are:</p> <ul style="list-style-type: none"> • Configuration data • Full system data
To	Indicates the already defined archive server on which you want to store the backup content.

To restore the CTRS database:

-
- Step 1** Choose the CTRS database content that you want to restore from the **Restore** drop-down menu. Options are **Configuration data** and **Full system data**. Full system data includes configuration files, videos, and video metadata
- Step 2** Choose the archive server (where the content you want to restore is saved) from the **From** drop-down menu. If you need to add a new archive server to the list, click **Add Server**. CTRS takes you to the Archive Server: Storage Management window to add a new server.
- Step 3** After you have chosen the appropriate archive server, click **Show** to display the databases available to be used to restore the CTRS database.
- To display a defined number of table rows, click the down arrow next to **Rows per page**. Click to highlight and choose predetermined amounts.
 - If the number of files exceeds the Rows per Page value, click **First** to view the files listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.

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



Caution

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

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

Restore task fields are described in [Table 4-10](#).

Table 4-10 *Restore Database and Configuration Files Field Descriptions*

Field	Description
Restore	Choose the content that you want to restore on this CTRS. Click the down arrow to view choices; highlight the choice to select. Options are: <ul style="list-style-type: none"> • Configuration data • Full system data
From	Indicates the already-defined archive server from which you want to retrieve content. Click the down arrow to view archive server choices; highlight the choice to select.
Add Server	To add a new archive server to the list, click Add Server . CTRS takes you to the Archive Server: Storage Management window to add a new server.
Show	Click Show to display the backed-up content available for restore.
Name	Data file to be used for restoring content. Click the radio button to the left of Name to choose it.
Size	Size of the data file in bytes.
Creation Time	Date and time that the data file was created.

Export Media Files

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

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

The screenshot displays the 'Configure > Backup Settings' interface. The 'Export Media Files' tab is selected. The configuration includes a schedule, a condition for when media is older than a certain number of days, and actions for exporting or deleting media files. The 'Export Media Files' checkbox is checked, and the 'Delete' checkbox is unchecked. The 'To a Server' dropdown is set to 'Expo-Inx-4'. The 'Before deletion, email video owner every day for (days)' dropdown is set to 'Never'.

Configure > Backup Settings

Backup Settings

Archive Servers Backup/Restore **Export Media Files** Import Media Files

Schedule *: Weekly (Monday) @ 00:00 America/Los_Angeles [Change...](#)

Condition

When media is older than (days):

Action

☒ Export Media Files
To a Server:

☐ Delete
Before deletion, email video owner every day for (days):*

[Submit](#) [Reset](#)

* To change the time zone, click Preferences link.
 * Frequency: An e-mail notification will be sent to video owner every day until the video is deleted.
 * Please make sure the remote archive server has enough disk space.

343046

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

Table 4-11 Export Media Files Field Descriptions

Field	Description
Schedule <frequency> at <start_time>	<p>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.</p> <p>To change the time scheduled for the automatic data export, click Change. From the Change window:</p> <ul style="list-style-type: none"> • Start Time: Choose the hour and minute in 24-hour format from the drop-down menus • Frequency: Defines the frequency of the export. Click the appropriate radio button to choose Daily or Weekly export. If you choose Weekly, also choose the days of the week on which you want the export to occur. • Click OK to apply your changes or Cancel to cancel your new changes.
Condition	Condition lets you establish additional rules governing the data that is transferred.
When media is older than (days):	Enter the number of days for the minimum age of the exported data. Valid values are 0–90 days. The default is 60 days.
Action	Defines whether CTRS exports the data to an archive server, deletes the data, or both.
Export Media Files	Check this box if you want CTRS to export this data to an archive server.
To a Server:	Select the archive server where the data will be stored. Click the arrow to display a drop-down list of available archive servers.
Delete	Check this box if you want CTRS to delete the specified data.
Before deletion, email video owner every day for (days):	CTRS sends an e-mail to the owner of the video (the person who created it) every day before the deletion date for the number of days that you specify. This e-mail notification advises the owner to download a copy of the video if desired.

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

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

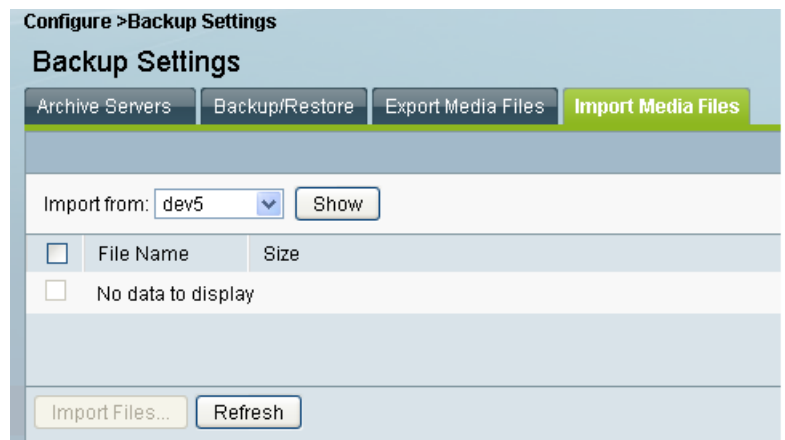
With this configuration, daily at 23:45, CTRS exports each video that is older than 60 days to the specified server. CTRS also marks for deletion each video that it exported. For the next ten days, CTRS marks the status of the video as “Delete Pending” (CTRS displays the status of each video in the list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

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

Import Media Files

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

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



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

To import media files:

-
- Step 1** Click the down arrow to the right of **Import From** to display the list of available archive servers; highlight to select.
- Step 2** After you have selected the appropriate archive server, click **Show** to display the files available to be imported.
- To display a defined number of table rows, click the down arrow next to **Rows per page**. Click to highlight and select predetermined amounts.
 - If the number of files exceeds the Rows per Page value, click **First** to view the files listed on the first page, **Next** to view the next page in sequence, **Previous** to view the preceding page, and **Last** to view the last page.
 - To refresh the list of files displayed, click **Refresh**.
- Step 3** Check the box to the left of the file to choose it. To choose all files listed, check the box in the upper left of the table.
- Step 4** Click **Import Files**.
-

Cisco Show and Share

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

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

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

For information about downloading and installing the Cisco Show and Share server security certificate, see the [“Installing the Cisco Show and Share Server Security Certificate on the CTRS” section on page 4-23](#).

Configuring the CTRS UI for Cisco Show and Share

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

Figure 4-13 *Configure > Cisco Show and Share*

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

Table 4-12 *Cisco Show and Share Field Descriptions*

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

Table 4-12 Cisco Show and Share Field Descriptions

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

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

Understanding the DMM User Name LDAP Attribute Field

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

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

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

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

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

-
- Step 1** Click **Security Settings** in the left menu.
- Step 2** Click **Install**. The Certificate Upload window displays, as shown in [Figure 4-14](#).

Figure 4-14 *Configure > Security Settings*

Configure > Security Settings

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

Browser Security: ☐ Unsecure

Inter-Device Security: ☐ Secure ☐ Unsecure ☒ Best-Effort

Digital Security Certificates

Unit: Category:

	Unit	Category	Certificate Name	Expires On
<input type="radio"/>	tomcat	OWN	tomcat.pem	Tue Jul 05 22:58:30 UTC 2016
<input type="radio"/>	CAPF-trust	TRUST	CAPF.pem	Mon Jan 05 21:15:35 UTC 2015
<input type="radio"/>	tomcat-trust	TRUST	tsbu-ctrs.cisco.com.pem	Tue Jul 05 22:58:30 UTC 2016
<input type="radio"/>	CTM-trust	TRUST	CUCM0.pem	Mon Jan 05 21:15:33 UTC 2015
<input type="radio"/>	CTM-trust	TRUST	CUCM2.pem	Wed Jan 07 22:24:59 UTC 2015
<input type="radio"/>	CTM-trust	TRUST	CUCM1.pem	Wed Jan 07 23:25:26 UTC 2015
<input type="radio"/>	CAPF-LSC	OWN	CTMS_Cert_Chain.pem	Thu Sep 01 01:12:31 UTC 2016

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

Step 4 Click Install...

The Install Security Certificate Dialog Box appears.

Figure 4-15 *Install Digital Security Certificate Dialog Box*

Install Digital Security Certificate

Security Setting: ☒ Inter-Device Security ☐ Browser Security

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

Unit:

Category:

☒ Certificate:

☒ Required Fields

- Step 5** Upload the Cisco Show and Share security certificate file to the CTRS by completing the following steps:
- Select the Inter-Device Security radio button.
 - From the Unit drop-down list, select **CTM-trust** (this is the default value).
 - From the Category drop-down list, select **TRUST** (this is the default value).
 - Click the **Browse** button.
 - Navigate to the folder in which you stored the Cisco Show and Share security certificate file, and choose that file.
 - Click **Install**.

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

- Step 6** If you changed the Browser Security field setting in [Step 3](#), click the appropriate radio button in the Browser Security field to return your Browser Security setting to the previous setting.

CTS-Manager



Note

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

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

Table 4-13 CTS-Manager Registration in CTRS

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

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

Email Server

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

Figure 4-16 *Configure > Email Server*

Configure > Email Server

Protocol: SMTP

Connection: ☒ Non-Secure ☐ Secure

Host:

Port:

User Name:

Password:

= Required fields

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

Table 4-14 *Email Server Field Descriptions*

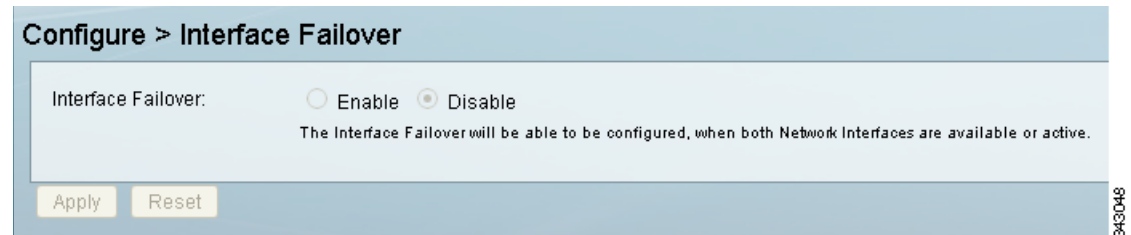
Field or Button	Setting
Protocol	View only. Email protocol.
Connection	Click the Non-Secure or the Secure radio button. If the SMTP server requires a secure connection, select Secure .
Host	Enter the hostname of the email server.
Port	Enter the port number associated with the email server.
SMTP User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

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

Interface Failover

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

Figure 4-17 *Configure > Interface Failover*



When enabled, the secondary adapter handles all network traffic if the primary adapter or its connection fails.

To enable interface failover:

- Step 1** Make sure that the primary Ethernet adapter (Ethernet interface 0) is connected to the network and that its static IP address and gateway parameters were correctly configured during system installation.
- Step 2** Connect the secondary Ethernet cable (Ethernet interface 1) to a network switch. The connection port can be on the same switch as Ethernet interface 0 or on a different switch, but both Ethernet interface 0 and Ethernet interface 1 must be on the same gateway.
- Step 3** From the **Interface Failover** window, click the **Enable** button, then click **Apply**.



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

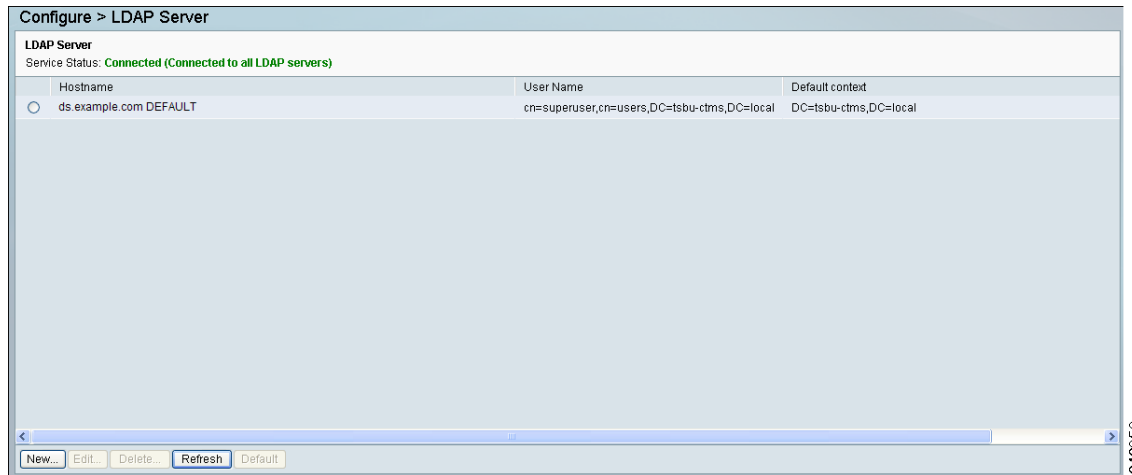
To disable interface failover:

- Step 1** With no active meetings in progress, click the **Disable** button.
- Step 2** Click **Apply**. Your network adapters will be configured and restarted and the interface failover disabled.

LDAP Configuration

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

Figure 4-18 *Configure > LDAP Server*



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

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

Table 4-15 *LDAP Configuration Table Field Descriptions*

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

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

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

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

*** = Required fields**

Service Status:

* Host:

Bind Method: ☐ Secure ☒ Normal

* Port:

Deployment Type: ☐ Active Directory ☒ Domino ☒ Exchange

* Default Context:

* User Name: ☐ Append default context

* Password:

* Certificate:

* Default Email Domain:

* Connection Pool Size:

* User Containers:

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

* Email Mapping Attribute:

343061


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

Field or Button	Setting
Host	Enter the hostname of the LDAP server.
Bind Method	Click the appropriate radio button to choose the binding method. For CTRS, options are Secure and Normal . <ul style="list-style-type: none"> Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP.
Port	Enter the appropriate port number depending on the bind method selected. For Normal bind mode, the port setting is 389. For Secure bind mode, the port setting is 636. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port.

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

Field or Button	Setting
Deployment Type	<p>Defines the LDAP server type. Options are Active Directory and Domino. Click the appropriate radio button.</p> <p>When Active directory is selected and the Exchange box is checked, the Active Directory is partnered with Exchange. This partnering means that a user account on the Active Directory server has an e-mail mapping attribute value that is prepended with SMTP.</p> <p>If the checkbox is unchecked, the CTRS does not prepend.</p> <p>By default, the Exchange box is checked.</p>
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	<p>The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=adminstrator,cn=users,dc=<mydomain>,dc=com)</p> <p>To append the DN, click Append default context.</p>
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	<p>Enter the LDAP email domain. If this LDAP server is set as the default email server, then users logging into the Cisco TelePresence Video Portal do not need to append their email domain information to their username.</p> <p>Note You can enter a Default Email Domain for only the default LDAP server.</p> <p>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.</p>
Connection Pool Size	The number of concurrent connections used by the CTRS server to retrieve data from the LDAP server. This is primarily used for optimizing the server's access to the LDAP server.

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

Field or Button	Setting
User Containers	<p>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.</p> <p>To append the default context, check the Append default context box next to the user container field.</p> <div>  <p>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.</p> </div>
Email Mapping Attribute	<p>Enter the LDAP server tag (proxyAddresses) for mapping email addresses.</p> <div> <p>Note You can enter an Email Mapping Attribute for only the default LDAP server.</p> </div>

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

Configuring Multiple Domains in an LDAP Forest

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

For example, you have these two servers:

- LDAP server 1: corporate-cor1
 Default context: DC=cor1, DC=com
 User container: cn=users, DC=cor1, DC=com
- LDAP server 2: corporate-cor2
 Default context: DC=cor2, DC=com
 User container: cn=users, DC=cor2, DC=com

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

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

**Note**

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

Security Settings

The CTRS supports these security types:

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

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

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

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

Software Upgrades

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

Figure 4-20 *Configure > Software Upgrade*

Configure > Software Upgrades

Active Version: 1.8.0.0-151
Inactive Version: 1.7.4.0-149

Switch Versions... Upgrade Software...

Most Recent Upgrade Attempt

Hostname	IP Address	Status
ctrs78.cisco.com	10.22.17.178	Upgrade Not in Progress

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

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

To switch software versions:

- Click the **Switch Version** button.

The system will swap the software versions and reboot.

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

To upgrade software:

- Step 1** To start the software upgrade process, click the **Upgrade Software** button.
The Source Selection dialog box appears.
If you need to stop the software installation, click the *Cancel* button when the button is active.
- Step 2** Click the **CD-ROM** or **Network** radio button to choose the location of the patch file.
If you chose CD-ROM, click **Next** to go to the **File Selection** window.
If you chose **Network**, provide the hostname, login username, password, and the path to the patch file. By default, port 22 is used to access the server; supply the correct port number, if required. Click *Next* to go to the **File Selection** window.
- Step 3** At the **File Selection** window, choose the file to load by clicking its radio button. Then click **Next**.
- Step 4** The **Patch File** Preparation window appears. Watch this window to monitor the progress of the file download. Buttons will be inactive until the patch file is loaded.
Once the file is loaded, the window displays a Confirmation message.
The software wizard displays the software versions that are installed and provides radio buttons so you can choose to switch the newly loaded software to the active partition.
- Step 5** Click **Yes** or **No** to make your choice. Then click **Next** to finish the software upgrade task.
The install wizard displays a dialog window that logs the progress of the update.
- Step 6** When the log indicates that the files have been switched, click **Finish** to complete this task.
-

System Settings

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

- [IP Settings, page 4-34](#)
- [NTP Settings, page 4-36](#)
- [QoS, page 4-37](#)
- [SNMP, page 4-41](#)
- [Restart or Shutdown CTRS, page 4-46](#)

IP Settings

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

Figure 4-21 *Configure > System Settings—IP*

The screenshot displays the 'Configure > System Settings' interface. Under the 'System Settings' heading, there are five tabs: 'IP' (selected), 'NTP', 'QoS', 'SNMP', and 'Restart CTRS'. The 'IP' tab contains the following configuration fields:


MAC Address:	EF:1F:1F:F5:F4:0F
Hostname:	ctr78.cisco.com
Domain Name:	<input type="text" value="cisco.com"/>
Primary DNS:	<input type="text" value="10.70.168.183"/>
Secondary DNS:	<input type="text" value="10.68.226.120"/>
Ethernet Card:	eth0
IP Address:	<input type="text" value="10.22.157.178"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="10.22.157.1"/>

A legend at the bottom left of the form states: **= Required fields**. At the bottom of the form are 'Apply' and 'Reset' buttons. The page number '343049' is visible in the bottom right corner.

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

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

Table 4-17 **IP Settings**

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

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

NTP Settings

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

Figure 4-22 *Configure > System Settings—NTP*

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

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

Table 4-18 *NTP Settings*

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

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

QoS

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

Figure 4-23 *Configure > System Settings—QoS*

Configure > System Settings

System Settings

IP NTP **QoS** SNMP Restart CTRS

DSCP for Playback Video: AF41 DSCP (100010) ▼

DSCP for Playback Audio: EF DSCP (101110) ▼

DSCP for Signaling: CS3(precedence 3) DSCP (011000) ▼

Apply Reset

343003

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

Table 4-19 QoS

Field or Button	Setting
DSCP for Playback Video	<p>Quality of Service marking for the video packets during CTRS playback to CTS. Available settings are:</p> <ul style="list-style-type: none"> • 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) <p>The default value for this field is CS4 (precedence 4) (100000). It is recommended that you use the default value for this field.</p>

Table 4-19 QoS (continued)

Field or Button	Setting
DSCP for Playback Audio	<p>Quality of Service marking for the audio packets during CTRS Playback to CTS. Available settings are:</p> <ul style="list-style-type: none"> • 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) <p>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.</p>

Table 4-19 **QoS (continued)**

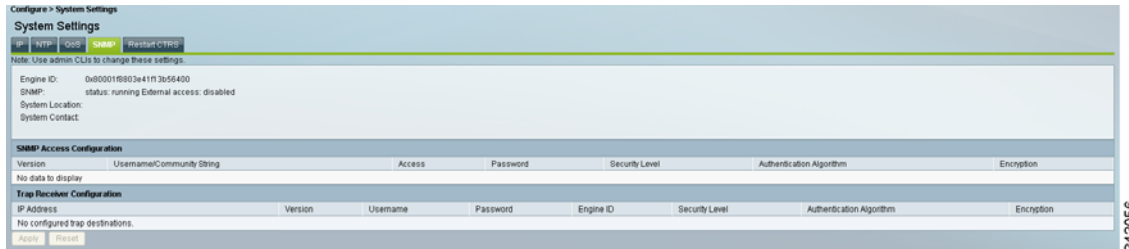
Field or Button	Setting
DSCP for Signaling	<p>Quality of Service marking for SIP Signaling packets.</p> <p>Available settings are:</p> <ul style="list-style-type: none"> • AF11 DSCP (001010) • AF12 DSCP (001100) • AF13 DSCP (001110) • AF21 DSCP (010010) • AF22 DSCP (010100) • AF23 DSCP (010110) • AF31 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) <p>The default value for this field is CS3 (precedence 3) (011000). It is recommended that you use the default value for this field.</p>

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

SNMP

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

Figure 4-24 System Configuration > System Settings—SNMP



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

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

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


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

[Table 4-20](#) describes the SNMP fields. All fields in this tab are view-only.

Table 4-20 SNMP Settings

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

Table 4-20 *SNMP Settings (continued)*

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

Configuring SNMP Traps on CTRS

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

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

- Start the SNMP service
- Configure an SNMP user

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

Starting the SNMP Service

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

-
- Step 1** Log in to the CTRS CLI.
- Step 2** Run the **utils service start** command:
- ```
utils service start Cisco SNMP Service
```
- 

### Configuring an SNMP User

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

- 
- Step 1** In the CTRS CLI, configure an SNMP user with the command:
- ```
set snmp user add version username access [passphrase] [level]
```

Syntax Description

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



Note

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

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

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

Configuring an SNMP Trap Destination

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

- Step 1** In the CTRS CLI, configure an SNMP trap destination with the command:
- ```
set snmp trapdest add version username destination [passphrase] [level] [engineID]
```

### Syntax Description

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

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

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

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

## Enabling CTRS to Send SNMP Trap Notifications

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

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

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

SNMP Trap notifications are now enabled for CTRS.

## Modifying SNMP Trap Settings

You can modify existing SNMP trap destinations and user access.

To modify an SNMP trap destination, do the following:

- Step 1** Delete the existing trap destination with the command:



**set snmp trapdest del**

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

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

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

For details on the syntax, refer to [Syntax Description, page 4-44](#).

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

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

---

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

**Step 1** Delete an existing SNMP user with the command:

**set snmp user del** *version username*

**Syntax Description**

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

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

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

**Step 2** Configure the new SNMP user with the command:

**set snmp user add** *version username access [passphrase] [level]*

For details on the syntax, refer to [Syntax Description, page 4-43](#).

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

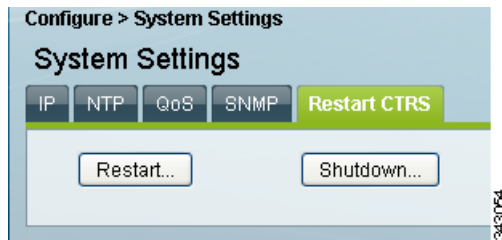
```
set snmp user add 3 newusr rw newpass
```

---

## Restart or Shutdown CTRS

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

**Figure 4-25** *Configure > System Settings—Restart CTRS*



### To restart CTRS:

- 
- Step 1** Click **System Settings** in the left menu.
  - Step 2** Click the **Restart CTRS** tab.
  - Step 3** Click **Restart** to restart CTRS. Restart means that the CTRS shuts down and then reboots.
- 

### To shutdown CTRS:

- 
- Step 1** Click **System Settings** in the left menu.
  - Step 2** Click the **Restart CTRS** tab.
  - Step 3** Click **Shutdown** to shut down CTRS.
- 

## Unified CM

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

- [Unified CM, page 4-47](#)
- [SIP Profile Settings, page 4-48](#)
- [Access Settings, page 4-50](#)

## Unified CM

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

**Figure 4-26** *Configure > Unified CM—Unified CM*

Configure > System Settings

### System Settings

IP NTP QoS SNMP Restart CTRS

MAC Address: EF:1F:1F:F5:F4:0F

Hostname: ctrs78.cisco.com

\* Domain Name: cisco.com

\* Primary DNS: 10.70.168.183

Secondary DNS: 10.68.226.120

Ethernet Card: eth0

\* IP Address: 10.22.157.178

\* Subnet Mask: 255.255.255.0

\* Default Gateway: 10.22.157.1


\* = Required fields

Apply Reset

343049

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

**Table 4-21** *Cisco Unified CM Settings*

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

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

# SIP Profile Settings

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

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

The screenshot shows the 'Configure > Unified CM' interface with the 'SIP Profile Settings' tab selected. The settings are as follows:

- Retry Count for SIP Invite: 6
- Retry Count for SIP non Invite Request: 10
- SIP Expires Timer: 1800
- SIP Timer T1: 500
- SIP Timer T2: 4000
- Start Media Port: 16384
- Stop Media Port: 32766
- Device Security: Encrypted with SDP Keys
- Transport Layer Protocol: TLS


A legend at the bottom left states: **= Required fields**. At the bottom of the form are 'Apply' and 'Reset' buttons. A vertical text '343065' is visible on the right side of the form.

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

**Table 4-22** *SIP Profile Settings*

| Field or Button                        | Setting                                                                                                                                                                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Retry Count for SIP Invite             | Specifies the number of times that Cisco Unified Communications Manager (Unified CM) will re-send the INVITE message. This is a required field. Minimum is 1. Maximum is 10 Default is 6.                                                                                   |
| Retry Count for SIP non-Invite Request | Specifies the number of times that Unified CM will re-send the non-INVITE message. This is a required field. Minimum is 1. Maximum is 10 Default is 6.                                                                                                                      |
| SIP Expires Timer                      | Specifies the maximum time that an INVITE message remains valid. If Unified CM has not received an answer before this timer expires, Unified CM tears down the call. This is a required field. Minimum is 60000 (msec). Maximum is 300000 (msec). Default is 180000 (msec). |
| SIP Timer T1                           | Specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.                                                                                                                 |

**Table 4-22 SIP Profile Settings (continued)**

| Field or Button          | Setting                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Timer T2             | Specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.                                                                                                                                                                                                                                                              |
| Start Media Port         | Designates the start real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. The default for Cisco Unified Communications Manager (Unified CM) is 16384.                                                                                                                                                                                                                                           |
| Stop Media Port          | Designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. The default is for Cisco Unified Communications Manager (Unified CM) is 32766.                                                                                                                                                                                                                                         |
| Device Security          | Specifies the type of security applied to this CTRS. Available choices are the following: <ul style="list-style-type: none"> <li>• Non-Secure</li> <li>• Authenticated</li> <li>• Encrypted with SDP Keys</li> <li>• Encrypted without SDP Keys (select this option if you are using a version of Unified CM that does not support encryption with SDP keys)</li> </ul>                                                    |
| Transport Layer Protocol | Defines the transport protocol used. Available choices are: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> </ul> <div>  <b>Note</b> 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. </div> |

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

## Access Settings

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

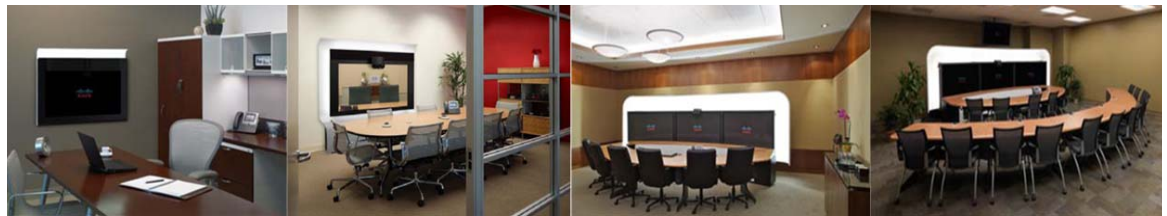
**Figure 4-28** *Configure > Unified CM—Access Settings*

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

**Table 4-23** *Access Settings*

| Field or Button     | Setting                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Route Pattern Start | Defines the first number in your defined route pattern as configured in Cisco Unified CM.                                                                                                                            |
| Route Pattern End   | Defines the last number in your defined route pattern as configured in Cisco Unified CM.                                                                                                                             |
| Access Number       | Displays the first number in the route pattern as defined in Cisco Unified CM. After you set the “SIP Trunk Minimum Number” value in Cisco Unified CM, CTRS automatically selects that number as this access number. |
| Access Name         | Descriptive name for the access number as defined in Cisco Unified CM. Maximum number of characters is 20.                                                                                                           |

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



# CHAPTER 5

## Managing CTRS Recordings

October 2011

The Cisco TelePresence Recording Server (CTRS) stores and enables you to manage recordings created by the following sources:

- Cisco TelePresence Studio Mode
- Event Recording

The following sections describe the CTRS Recordings Management features. 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 currently being created (see [Figure 5-1](#)).

**Figure 5-1** *Manage > Active Recordings*

| Manage > Active Recordings |                        |       |                          |                 |               |
|----------------------------|------------------------|-------|--------------------------|-----------------|---------------|
| <input type="checkbox"/>   | Recording ID           | Room  | Type                     | User            | Duration      |
| <input type="checkbox"/>   | 2011091223011968592926 | 88001 | Ad Hoc Meeting Recording | Acorn@cisco.com | 1 min 13 secs |

The Active Recordings page 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                                                                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recording ID | Identification number for this recording session.                                                                                                                                                                                                              |
| Room         | <ul style="list-style-type: none"> <li>For Studio Mode recordings, Cisco TelePresence room in which the recording is taking place.</li> <li>For Event Recordings, the CTMS Directory Number configured on the CTMS that initiated the recording.</li> </ul>    |
| Type         | Type of recording.                                                                                                                                                                                                                                             |
| User         | <ul style="list-style-type: none"> <li>For Studio Mode recordings, the user who logged in and started the recording.</li> <li>For Event Recordings, the CTRS User ID with which the CTMS administrator logged into the CTRS to start the recording.</li> </ul> |
| Duration     | Length of time for this recording.                                                                                                                                                                                                                             |

- 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 Manage > Completed Recordings**

Manage > Completed Recordings

Completed Recordings Showing 1-10 of 76 10 per page Go

Start on: 05/05/2011 End on: 05/26/2011 Status: All

Owner: Title: Filter

| <input type="checkbox"/>            | Recording ID           | Title                      | Owner              | Room  | Date                | Type    | Duration        | Status    |
|-------------------------------------|------------------------|----------------------------|--------------------|-------|---------------------|---------|-----------------|-----------|
| <input type="checkbox"/>            | 2011052614361873944501 | Barb's ad hoc meeting      | bmatsumu@cisco.com | 88001 | 05/26/2011 07:36 AM | Meeting | 16 mins 42 secs | Available |
| <input type="checkbox"/>            | 2011052523400847082156 | switch source 500m         | vtuy@cisco.com     | 88001 | 05/25/2011 04:40 PM | Meeting | 1 min 20 secs   | Available |
| <input type="checkbox"/>            | 2011052523340767826100 | shaan patch                | vtuy@cisco.com     | 88001 | 05/25/2011 04:34 PM | Meeting | 1 min 13 secs   | Available |
| <input type="checkbox"/>            | 2011052523135657334279 | Quarterly meeting          | vtuy@cisco.com     | 88001 | 05/25/2011 04:14 PM | Meeting | 54 secs         | Available |
| <input checked="" type="checkbox"/> | 2011052522472734431591 | Quarterly meeting          | bmatsumu@cisco.com | 88001 | 05/25/2011 03:47 PM | Meeting | 18 secs         | Available |
| <input type="checkbox"/>            | 2011052521495834433205 | missing audio with patched | vtuy@cisco.com     | 88001 | 05/25/2011 02:50 PM | Meeting | 3 mins 12 secs  | Available |
| <input type="checkbox"/>            | 2011052518154182591211 | missing part of audio      | vtuy@cisco.com     | 88001 | 05/25/2011 11:15 AM | Meeting | 3 mins 33 secs  | Available |
| <input type="checkbox"/>            | 2011052501543295102912 | downgrade no audio         | vtuy@cisco.com     | 96810 | 05/24/2011 06:54 PM | Meeting | 6 mins 33 secs  | Available |
| <input type="checkbox"/>            | 2011052421350189446519 | downgrade no audio         | vtuy@cisco.com     | 13113 | 05/24/2011 02:35 PM | Studio  | 20 secs         | Available |
| <input type="checkbox"/>            | 2011052421281749102644 | downgrade no audio         | vtuy@cisco.com     | 96810 | 05/24/2011 02:28 PM | Meeting | 4 mins 7 secs   | Available |

Details... Download... Delete... Export... Refresh

Page 1 of 8

Use the Completed Recording page 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        | <ul style="list-style-type: none"> <li>• For Studio Mode recordings, the user who created and owns the recording.</li> <li>• For Event Recordings, the CTRS User ID with which the CTMS administrator logged into the CTRS to create the recording.</li> </ul>      |
| Room         | <ul style="list-style-type: none"> <li>• For Studio Mode recordings, the Cisco TelePresence System room in which recording was produced.</li> <li>• For Event Recordings, the CTMS Directory Number configured on the CTMS that initiated the recording.</li> </ul> |
| Date         | Date on which recording was produced.                                                                                                                                                                                                                               |
| Type         | Displays the recording type, which can be one of the following: <ul style="list-style-type: none"> <li>• Meeting—Recording made using the Event Recording feature.</li> <li>• Studio—Recording made while in Studio Mode.</li> </ul>                                |

**Table 5-2** *Completed Recordings Table Field Descriptions*

| Field    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duration | Recording length.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Status   | Recording status. Statuses are as follows: <ul style="list-style-type: none"> <li>• All—all videos in the list.</li> <li>• Available—videos that are available for deletion or export.</li> <li>• 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 &gt; Backup Settings—Export Media Files tab).</li> </ul> |

- 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 click **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                               | <ul style="list-style-type: none"> <li>• For Studio Mode recordings, the user who created and owns the recording.</li> <li>• For event recordings, the CTRS User ID with which the CTMS administrator logged into the CTRS to create the recording.</li> </ul> |
| Recording Date                      | Date on which recording was produced.                                                                                                                                                                                                                          |
| Quality                             | Image quality of the recording.                                                                                                                                                                                                                                |
| Recording Type                      | Whether the recording is a Studio Mode recording, or an Event Recording.                                                                                                                                                                                       |
| 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 4-12](#) 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

You can download the standard definition (SD) or high definition (HD) version of a recording to your computer. For a recording made using Event Recording, you can also download the presentation materials displayed during the meeting.

Because of video resolution changes, recordings made using Event Recording could be stored in multiple files. Before downloading multiple files to your computer, the CTRS transcodes the files into one file, which can be a lengthy process.

To download, do the following:

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

**Step 2** Click **Download**.

The Download Recording dialog box appears as shown in [Figure 5-3](#).

**Figure 5-3** Download Recording Dialog Box

### Download Recording

Title: 1 131

Standard-Definition Video: Download

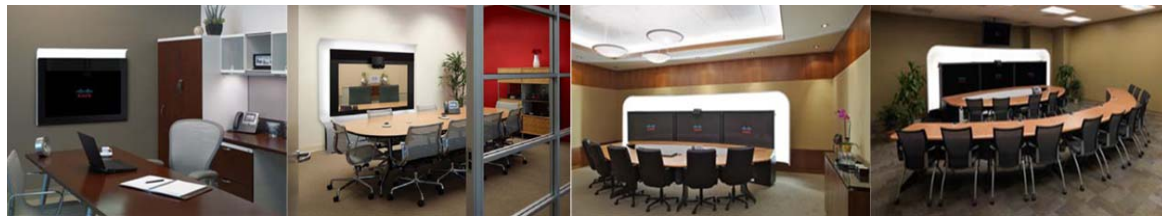
High-Definition Video: Download

Presentation Video: Download Presentation

Close

343061

- Step 3** Decide which version of the recording you want to download, and click the corresponding button.
- If the Process File for Download button appears, the recording was written to multiple files, which must be transcoded into one file then downloaded. The transcoding process can be lengthy; therefore, a percentage complete counter provides an update of the progress.
- Step 4** After the download is complete, click **Save** in the dialog box that appears, and specify where you want to save the file on your computer.
-



## CHAPTER 6

# Troubleshooting CTRS

---

October 2011

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

- [Dashboard, page 6-1](#)
- [Process Status, page 6-4](#)
- [Hardware Status, page 6-5](#)
- [System Information, page 6-6](#)
- [System Status, page 6-7](#)
- [CTRS Alarms and System Errors Messages, page 6-8](#)
- [Log Files, page 6-10](#)

## Dashboard

After you log into the CTRS Administrative UI, the Troubleshoot > Dashboard page appears. You can also access this page by clicking **Dashboard** in the left navigation.

As shown in [Figure 6-1](#), the Troubleshoot > Dashboard page enables you to view high-level reports on the following aspects of the CTRS:

- Disk usage for media storage
- Users
- Recordings
- Time
- Services

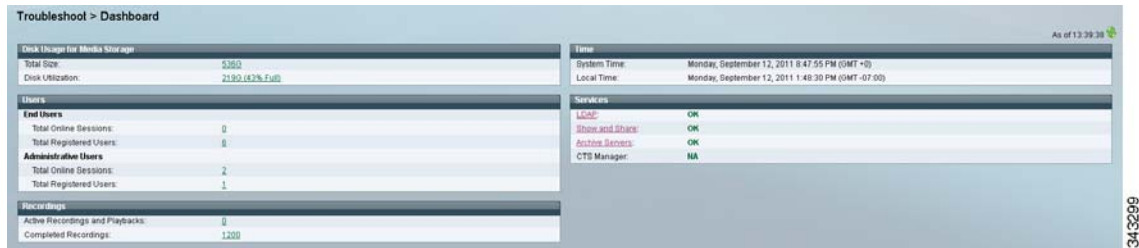
**Figure 6-1**      **Troubleshoot > Dashboard**

Table 6-1 describes each Dashboard field. Each field name or entry is a link, which you can click to get more detailed information.

You can refresh the data in the Dashboard at any time by clicking the refresh icon in the upper right corner of the page.

**Table 6-1**      **Dashboard Field Descriptions**

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disk Usage for Media Storage</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Total Size                          | Displays the total amount of disk space, in gigabytes, available to store videos.<br><br>For more information on disk status, click the link to access the Troubleshoot > Hardware Status page.                                                                                                                                                                                                                                                                                                    |
| Disk Utilization                    | Displays the amount of disk space, in gigabytes and as a percentage of the total disk size, currently used for video storage.<br><br>For more information on disk status, click the link to access the Troubleshoot > Hardware Status page.                                                                                                                                                                                                                                                        |
| <b>Users</b>                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>End Users</b>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Total Online Sessions               | Displays the number of end users who are currently logged into the web-based Cisco TelePresence Video Portal.<br><br>For information on recordings currently being made or played back by a CTS endpoint, see the Active Recordings and Playbacks field, which is described later in this table.<br><br>For more information on end users who can access the Cisco TelePresence Video Portal, click the link to access the Configure > Access Management page, then click the End-user Portal tab. |
| Total Registered Users              | Displays the number of end users who have accounts to access to the Cisco TelePresence Video Portal.<br><br>For more information on end users who can access the Cisco TelePresence Video Portal, click the link to access the Configure > Access Management page, then click the End-user Portal tab.                                                                                                                                                                                             |

**Table 6-1**      **Dashboard Field Descriptions (continued)**

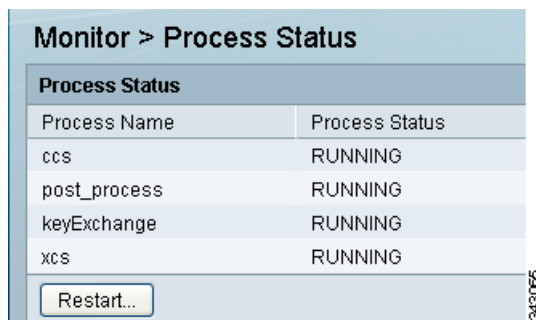
| Field                           | Description                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative Users            |                                                                                                                                                                                                                                                                                                                                                                        |
| Total Online Sessions           | <p>Displays the number of administrative users who are currently logged into the CTRS Administrative UI.</p> <p>For more information on administrative users who can access the CTRS Administrative UI, click the link to access the Configure &gt; Access Management page, Administrative Portal tab.</p>                                                             |
| Total Registered Users          | <p>Displays the number of administrative users who have accounts to access to the CTRS Administrative UI.</p> <p>For more information on administrative users who can access the CTRS Administrative UI, click the link to access the Configure &gt; Access Management page, Administrative Portal tab.</p>                                                            |
| <b>Recordings</b>               |                                                                                                                                                                                                                                                                                                                                                                        |
| Active Recordings and Playbacks | <p>Displays the number of recordings with the following status:</p> <ul style="list-style-type: none"> <li>• Currently being made in Studio Mode or using Event Recording.</li> <li>• Currently being played back by a CTS endpoint.</li> </ul> <p>For more information on the active recordings, click the link to access the Manage &gt; Active Recordings page.</p> |
| Completed Recordings            | <p>Displays the number of completed recordings that are archived on the CTRS.</p> <p>For more information on the completed recordings, click the link to access the Manage &gt; Completed Recordings page.</p>                                                                                                                                                         |
| <b>Time</b>                     |                                                                                                                                                                                                                                                                                                                                                                        |
| System Time                     | <p>Displays the time determined by the value of the set timezone command in the CTRS command-line interface (CLI). (The default value of this command is Greenwich Mean Time (GMT)/Coordinated Universal Time (UTC)). This time typically corresponds to the location of the server running the CTRS application.</p>                                                  |
| Local Time                      | <p>Displays the time determined by the value of the Time Zone field, which you can access by clicking <b>Preferences</b> in the upper right corner of the CTRS Administrative UI. This time typically corresponds to the location of the CTRS administrator.</p>                                                                                                       |

**Table 6-1**      *Dashboard Field Descriptions (continued)*

| Field                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Services</b>                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| LDAP, Show and Share, Archive Servers, and CTS-Manager | <p>Displays the status of the LDAP, Show and Share, and archive servers, with which the CTRS could be registered. The status can be one of the following:</p> <ul style="list-style-type: none"> <li>OK—The CTRS is registered with a particular server, and the connection to the server is operational.</li> <li>Error—The CTRS is registered with a particular server, but the connection to the server is not operational.</li> <li>NA—You cannot register this version of CTRS with CTS-Manager. Only the Commercial Express version of CTRS can be registered with CTS-Manager.</li> </ul> <p>For more information on a particular server, click the link to access the respective server page in the CTRS Administrative UI.</p> |

## Process Status

Click **Process Status** in the left navigation to display processes that are currently running (see [Figure 6-2](#)).

**Figure 6-2**      *Troubleshoot > Process Status*


The screenshot shows the 'Monitor > Process Status' page. It contains a table with two columns: 'Process Name' and 'Process Status'. The table lists four processes: 'ccs', 'post\_process', 'keyExchange', and 'xcs', all of which are in a 'RUNNING' state. Below the table is a 'Restart...' button. A vertical text '343065' is visible on the right side of the screenshot.

| Process Status |                |
|----------------|----------------|
| Process Name   | Process Status |
| ccs            | RUNNING        |
| post_process   | RUNNING        |
| keyExchange    | RUNNING        |
| xcs            | RUNNING        |

Restart...

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

**Table 6-2**      *Process Status Table Field Descriptions*

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



- Click **Restart** to restart all of the processes.
- The information in the Process Status page 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 6-3](#)).

**Figure 6-3** *Troubleshoot > Hardware Status*

Troubleshoot > Hardware Status

Disk Status for System OS

Logical Drive:

| ID         | Size  | Status |
|------------|-------|--------|
| 1 (RAID 1) | 135GB | ✓      |

Physical Drives:

| Bay   | Size  | Status |
|-------|-------|--------|
| Bay_0 | 136GB | ✓      |
| Bay_1 | 136GB | ✓      |

Disk Status for Media Storage

Logical Drive:

| ID         | Utilization        | Status |
|------------|--------------------|--------|
| 2 (RAID 5) | 412G of 536G (81%) | ✓      |

Physical Drives:

| Bay   | Size  | Status |
|-------|-------|--------|
| Bay_2 | 136GB | ✓      |
| Bay_3 | 136GB | ✓      |
| Bay_4 | 136GB | ✓      |
| Bay_5 | 136GB | ✓      |
| Bay_6 | 136GB | ✓      |

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

**Table 6-3** *Hardware Status Field Descriptions*

| Field                            | Description                                    |
|----------------------------------|------------------------------------------------|
| <b>Disk Status for System OS</b> |                                                |
| <b>Logical Drive</b>             |                                                |
| ID                               | Identification number                          |
| Size                             | Size of the partition                          |
| Status                           | Current status of that area of the hard drive. |
| <b>Physical Drives</b>           |                                                |

**Table 6-3** Hardware Status Field Descriptions (continued)

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

## System Information

Click **System Information** in the left navigation to view information about the CTRS (see [Figure 6-4](#)). The information displayed under System Information is configured during CTRS software installation.

**Figure 6-4** Troubleshoot > System Information

| System Information |                       |
|--------------------|-----------------------|
| SKU:               | CTS-CTRS-1.7          |
| Hostname:          | ctrs6                 |
| IP Address:        | 209.165.202.129       |
| Subnet Mask:       | 255.255.255.224       |
| MAC Address:       | 00:23:7D:62:B1:B1     |
| Hardware Model:    | 784512                |
| Software Version:  | 1.7.0                 |
| OS Version:        | UCOS 4.0.0.0-31       |
| Kernel Version:    | 2.6.9-78.ELsmp #1 SMP |

- 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

## System Status

Click **System Status** in the left navigation to display statistics that are related to system status (see Figure 6-5).

**Figure 6-5** *Troubleshoot > System Status*



The System Status page 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.

# CTRS Alarms and System Errors Messages

You can view CTRS system messages in one of two ways:

- Click **System Messages** in the left navigation (see [Figure 6-6](#)). The System Messages page displays a list of messages.

**Figure 6-6**      *Troubleshoot > System Messages*

| Troubleshoot > System Messages                                                                                                                                                                                                                                                                                                                    |                     |          |                                            |                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|----------|--------------------------------------------|-----------------------|
| System Messages                                                                                                                                                                                                                                                                                                                                   |                     |          |                                            |                       |
| Start on: 10/10/2011  End on: 10/11/2011  Severity: All  <input type="button" value="Filter"/> |                     |          |                                            |                       |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | Time*               | Severity | Summary                                    | Recommendation        |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 01:24 PM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 12:12 PM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 11:00 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 09:48 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 08:36 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 07:24 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 06:12 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 05:00 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 03:48 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |
| <input type="checkbox"/>                                                                                                                                                                                                                                                                                                                          | 10/11/2011 02:36 AM | warning  | Above Threshold. Please Reduce Disk Usage. | Contact administrator |

- From **System Status** at the bottom of the left navigation, 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 6-4**      **System Error Field Descriptions**

| Field          | Description                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time           | Displays the time at which the condition occurred.                                                                                                                                                                                                                      |
| Severity       | Indicates the severity level of the error. There are eight severity levels as follows: <ul style="list-style-type: none"><li>• Emergency</li><li>• Alert</li><li>• Critical</li><li>• Error</li><li>• Warning</li><li>• Notice</li><li>• Info</li><li>• Debug</li></ul> |
| Summary        | Message describing the error.                                                                                                                                                                                                                                           |
| Recommendation | Recommended action to deal with the condition.                                                                                                                                                                                                                          |

- 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 6-7](#)).

**Figure 6-7**      *Troubleshoot > Log Files*

**Troubleshoot > Log Files**

CCS:

Post Process:

Execution Manager:

Media Processor:

Key Exchange:

Transcode Processor:

**Log Files**

Process:

| Filename                          | Process         | Last Modified*      | Size (KB) |
|-----------------------------------|-----------------|---------------------|-----------|
| <a href="#">rma00014.log</a>      | Media-Processor | 09/11/2011 03:59 PM | 399.9     |
| <a href="#">sip00001.log</a>      | SIP             | 09/09/2011 05:41 PM | 0.04      |
| <a href="#">transcode_status</a>  | N.A             | 09/09/2011 11:31 PM | 16.0      |
| <a href="#">rma00013.log</a>      | Media-Processor | 09/11/2011 03:01 PM | 400.0     |
| <a href="#">rma00009.log</a>      | Media-Processor | 09/11/2011 11:11 AM | 399.95    |
| <a href="#">kevexchange.log</a>   | Key-Exchange    | 09/11/2011 07:44 PM | 2.95      |
| <a href="#">rma00012.log</a>      | Media-Processor | 09/11/2011 02:04 PM | 400.0     |
| <a href="#">post_process.log2</a> | Post-Process    | 09/09/2011 05:33 PM | 0.37      |
| <a href="#">rma00002.log</a>      | Media-Processor | 09/10/2011 02:52 AM | 399.95    |
| <a href="#">kevexchange.log2</a>  | Key-Exchange    | 09/09/2011 05:33 PM | 0.11      |

343067

Use the Log File page 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** page.
- Step 2** At the top of the Log Files page, there is a table listing the following CTRS system processes:
  - CCS
  - Post Processor
  - Execution Manager
  - Media Processor
  - Key Exchange
  - Transcode Processor

To the right of each process is a drop-down menu with these severity levels:

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

Click the down arrow to display the defined levels of severity. Choose the level at which logs are captured.

**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** page.
- Step 2** Click the down arrow to the right of **Processes** to display a list of CTRS processes. Click a specific process on which to filter log files. Choices are the following:
- All
  - Alarm-Logs
  - CCS
  - CDR-Logs
  - Core
  - CTRS-Sysop
  - Exe-Exchange
  - Media-Processor
  - Post-Process
  - SIP
  - Web-UI
  - Transcode-Processor
- Step 3** Click the **Filter** button to display the logs files associated with the chosen process.
-

### Downloading Log Files

To download log files from the Log File table:

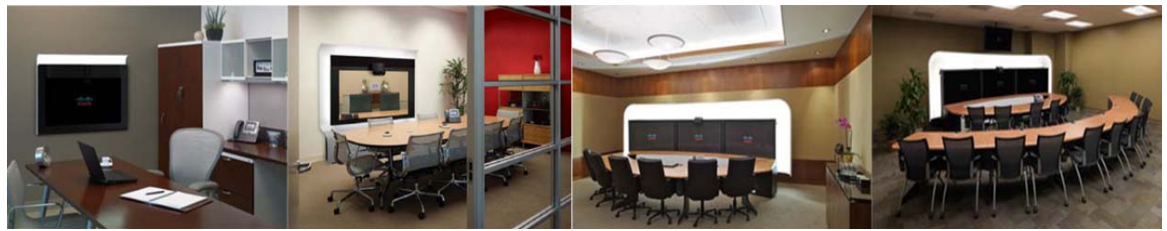
- Step 1** Click **Log Files** under **Troubleshooting** in the left navigation.
- Step 2** At the bottom of the Log Files page is the Log File list. The table is organized as described in [Table 6-5](#).

**Table 6-5** *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** Click the filename of a log file to download that file. Click the **Download All** button to download all log files listed.





# APPENDIX **A**

## System Messages

---

October 2011

- [System Message Overview, page A-1](#)
- [System Messages By Source, page A-2](#)

## System Message Overview

When trying to find documentation for a particular system message, consider the following:

- The system messages in this appendix are grouped by the CTRS component that generated them. For example, all LDAP messages appear in the same section.
- Each system message condition has a severity level. From most severe to least severe, the severity levels are the following:
  - Alert
  - Critical
  - Error
  - Warning
  - Info
- Some system messages in this appendix include “%s,” “%d,” “\$1,” “\$2,” or “\$3,” which are variables. When these variables appear in the CTRS administration interface or in the system log files, they are replaced by a text string that provides specific information about the condition or a numerical value, such as a dial number.
- You can resolve some conditions that are described in the system messages by correcting network configuration or connectivity issues. On occasion, you might not be able to resolve a condition by following the recommended action. In such cases, collect CTRS log files and contact your technical support representative. If the condition also involves other devices in your network, for example, a CTS endpoint, collect the log files for those devices whenever possible.

# System Messages By Source

The following sections present information on these system messages:

- [SVR Messages, page A-2](#)—general server
- [DISK Messages, page A-3](#)—disk manager
- [LDAP Messages, page A-5](#)—Lightweight Directory Access Protocol
- [RMGR Messages, page A-7](#)—recording manager module
- [SNS Messages, page A-10](#)—Cisco Show and Share
- [SOAP Messages, page A-12](#)—web services Simple Object Access Protocol
- [CERT Messages, page A-15](#)—certificate management
- [SMTP Messages, page A-16](#)—email manager
- [LCAL Messages, page A-18](#)—messages about publishing or deleting locales
- [CCS Messages, page A-18](#)—call control system
- [MEDIA Messages, page A-32](#)—media
- [POST Messages, page A-38](#)—post-processing
- [EXEMGR Messages, page A-38](#)—execution manager

## SVR Messages

### INTERNAL\_ERROR

**Severity**

Error

**Message**

The system has encountered an unexpected condition (\$1)

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SVR 1000

### CONFIG\_PARSER\_ERROR

**Severity**

Critical

**Message**

Unable to parse system configuration file '\$1' because \$2.

**Recommendation**

The system configuration file cannot be processed. Contact your support team.

**Application Name and Message Code**

SVR 1001

## DISK Messages

**CTRS\_VIDEO\_EXPORT\_NO\_SPACE****Severity**

Critical

**Message**

There is not enough space for video export. Current available space on '\$1' is \$2 KB. The size of to-be exported video is \$3 KB"

**Recommendation**

There is not enough space on the remote server for video export. Contact your support team.

**Application Name and Message Code**

DISK 1700

**CTRS\_VIDEO\_EXPORT\_START****Severity**

Info

**Message**

The recordings exported to \$1 was started.

**Recommendation**

No action is required.

**Application Name and Message Code**

DISK 1701

**CTRS\_VIDEO\_EXPORT\_END****Severity**

Info

**Message**

The recordings exported to '\$1' was finished. Detailed export report was emailed to administrator

**Recommendation**

No action is required.

**Application Name and Message Code**

DISK 1702

**CTRS\_VIDEO\_IMPORT****Severity**

Info

**Message**

%s

**Recommendation**

The character string indicates the status of recording import. No action is required.

**Application Name and Message Code**

DISK 1703

**CTRS\_DISK\_ALERT\_NOTIFICATION****Severity**

Critical

**Message**

Disk Level Reached Above Threshold

**Recommendation**

The CTRS disk space has reached a threshold. Contact your support team.

**Application Name and Message Code**

DISK 1704

**CTRS\_DISK\_ALERT\_ERROR****Severity**

Critical

**Message**

Could Not Obtain Disk Usage Stats

**Recommendation**

The system is unable to obtain disk usage statistics. Contact your support team.

**Application Name and Message Code**

DISK 1705

**CTRS\_DISK\_ALERT\_CRITICAL\_LEVEL****Severity**

Critical

**Message**

Disk Hit Critical Threshold. All Recording Sessions Dropped.

**Recommendation**

Contact your support team.

**Application Name and Message Code**

DISK 1706

**CTRS\_DISK\_ALERT\_EMAIL\_ADDRESSES****Severity**

Warning

**Message**

No Email Addresses Configured To Alert

**Recommendation**

No email addresses are configured in alerts management. Configure email addresses so that CTRS administrators receive notifications about disk space usage.

**Application Name and Message Code**

DISK 1707

## LDAP Messages

**CTRS\_LDAP\_CONFIGURATION\_NO\_HOST****Severity**

Critical

**Message**

Ldap Hostname Not Configured

**Recommendation**

Include a valid LDAP hostname in the CTRS administrative interface.

**Application Name and Message Code**

LDAP 1400

**CTRS\_LDAP\_AUTHENTICATION\_NO\_CONNECTION****Severity**

Critical

**Message**

Unable to connect to '\$1'

**Recommendation**

CTRS is unable to connect to the LDAP server. Verify connectivity and whether or not the LDAP server is operating properly.

**Application Name and Message Code**

LDAP 1401

**CTRS\_LDAP\_AUTHENTICATION\_NO\_LDAP\_MANAGER****Severity**

Critical

**Message**

Could Not Obtain LDAP Manager

**Recommendation**

Contact your support team.

**Application Name and Message Code**

LDAP 1402

**CTRS\_LDAP\_AUTHENTICATION\_CONFIG****Severity**

Critical

**Message**

No default email domain configured

**Recommendation**

Configure a default email domain.

**Application Name and Message Code**

LDAP 1403

**CTRS\_LDAP\_AUTHENTICATION\_NO\_AUTH****Severity**

Critical

**Message**

Could Not Obtain LDAP Authenticator

**Recommendation**

Contact your support team.

**Application Name and Message Code**

LDAP 1404

## RMGR Messages

### CTRS\_RECMGR\_SESSION\_PACKET\_LOSS

**Severity**

Error

**Message**

Recording Session [\$1,%2] heavy packet loss, recording unrecoverable

**Recommendation**

No action is required.

**Application Name and Message Code**

RMGR 1200

### CTRS\_RECMGR\_SESSION\_INIT

**Severity**

Error

**Message**

Recording Session [\$1,\$2] error while in init

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1201

### CTRS\_RECMGR\_SESSION\_PROGRESS

**Severity**

Error

**Message**

Recording Session [\$1,\$2] error while in progress

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1202

**CTRS\_RECMGR\_SESSION\_TEARDOWN****Severity**

Error

**Message**

Recording Session [\$1,\$2] error while in teardown

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1203

**CTRS\_RECMGR\_SESSION\_FINISHING****Severity**

Error

**Message**

Recording Session [\$1,\$2] error while in finishing

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1204

**CTRS\_RECMGR\_SESSION\_CLEANUP****Severity**

Info

**Message**

Cleaning up Active Sessions

**Recommendation**

No action is required.

**Application Name and Message Code**

RMGR 1205



**CTRS\_RECMGR\_CONFIGURATION****Severity**

Critical

**Message**

HD and SD are both disabled. Recording aborted

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1206

**CTRS\_RECMGR\_SESSION\_TIMER****Severity**

Info

**Message**

Recording Session [\$1,\$2] has exceeded maximum call duration. Stopping Session

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1207

**CTRS\_DISK\_ALERT\_REMINDER****Severity**

Warning

**Message**

Above Threshold. Please Reduce Disk Usage

**Recommendation**

Contact your support team.

**Application Name and Message Code**

RMGR 1208

# SNS Messages

## CTRS\_SNS\_INVALID\_CREDENTIALS

**Severity**

Critical

**Message**

Invalid Show and Share Credentials.

**Recommendation**

Contact the Cisco Show and Share administrator for valid credentials.

**Application Name and Message Code**

SNS 1300

## CTRS\_SNS\_INVALID\_HOSTNAME

**Severity**

Critical

**Message**

Invalid Show and Share Host

**Recommendation**

Contact the Cisco Show and Share administrator for a valid host.

**Application Name and Message Code**

SNS 1301

## CTRS\_SNS\_NO\_CONNECTIVITY

**Severity**

Critical

**Message**

No Connectivity to Show and Share Server.

**Recommendation**

Contact Show and Share administrator to validate path to server.

**Application Name and Message Code**

SNS 1302

**CTRS\_SNS\_API\_ERROR****Severity**

Critical

**Message**

\$1 API Request Error

**Recommendation**

An error occurred with a Cisco Show and Share API request. The API request error is specified in the message. Contact your support team.

**Application Name and Message Code**

SNS 1303

**CTRS\_SNS\_INVALID\_ENDUSER****Severity**

Critical

**Message**

Invalid Show and Share User \$1

**Recommendation**

An invalid end user was set to Cisco Show and Share. Contact your support team.

**Application Name and Message Code**

SNS 1304

**CTRS\_SNS\_UPLOAD\_ERROR****Severity**

Critical

**Message**

Show and Share Upload Error User \$1 Recording ID \$2

**Recommendation**

A condition prevented video upload to Cisco Show and Share. Contact your support team.

**Application Name and Message Code**

SNS 1305

**CTRS\_SNS\_EMAIL\_ERROR****Severity**

Critical

**Message**

Show and Share Email Error \$1 Recording ID \$2

**Recommendation**

An email to the end user was not sent. Contact your support team.

**Application Name and Message Code**

SNS 1306

## SOAP Messages

### CTRS\_CTS\_SOAP\_REQUEST\_PLAYBACK

**Severity**

Critical

**Message**

Stopped Playback Session for \$1. Problem starting playback

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1800

### CTRS\_CTS\_SOAP\_REQUEST\_PLAYBACK\_INVALID\_USER

**Severity**

Critical

**Message**

Aborted Replaying for \$1. Unauthorized User \$2 Attempting to Play \$3.

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1801

### CTRS\_CTS\_SOAP\_REQUEST\_PLAYBACK\_NO\_HD\_FILE

**Severity**

Critical

**Message**

Aborted Replaying for \$1. User \$2 Attempting to Play \$3, But no HD File Available.

**Recommendation**

No high-definition file is available for playback. Contact your support team.

**Application Name and Message Code**

SOAP 1802

**CTRS\_CTS\_SOAP\_REQUEST\_RECORDING****Severity**

Critical

**Message**

Aborted Recording Session for \$1. Error starting recording

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1803

**CTRS\_CTS\_SOAP\_REQUEST\_RECORDING\_NO\_DISK****Severity**

Critical

**Message**

Aborted Recording Session for \$1. No Disk Available

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1804

**CTRS\_CTS\_SOAP\_REQUEST\_RECORDING\_NO\_PORTS****Severity**

Warning

**Message**

Aborted Recording Session for \$1. No Ports Available

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1805

**CTRS\_CTS\_SOAP\_REQUEST\_PLAYBACK\_NO\_PORTS****Severity**

Warning

**Message**

Aborted Playback Session for \$1. No Ports Available

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1806

**CTRS\_CTS\_SOAP\_REQUEST\_RECORDING\_REPEAT****Severity**

Warning

**Message**

Aborted Recording Session for \$1. A repeat request to record from a remote participant

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1807

**CTRS\_CTS\_SOAP\_REQUEST\_PLAYBACK\_REPEAT****Severity**

Warning

**Message**

Aborted Playback Session for \$1. A repeat request to playback from a remote participant

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SOAP 1808

**CTRS\_CTSMAN\_WS\_INVALID\_RESPONSE****Severity**

Error

**Message**

The multiple CTRS web service request returns invalid response. \$1

**Recommendation**

No action is required. This issue is handled by the software.

**Application Name and Message Code**

SOAP 1820

## CERT Messages

### CERT\_LOAD\_ERROR

**Severity**

Error

**Message**

Unable to load certificate because \$1.

**Recommendation**

Follow the recommendation in the message, and try the operation again.

**Application Name and Message Code**

CERT 1900

### CERT\_LOAD\_EXTENSION\_ERROR

**Severity**

Error

**Message**

Invalid certificate file name '\$1'. Valid certificate file extensions are .cer and .der.

**Recommendation**

Try to load a valid certificate file.

**Application Name and Message Code**

CERT 1901

# SMTP Messages

## CTRS\_USER\_DATABASE\_ACCESS

**Severity**

Critical

**Message**

Failed to access user database

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1600

## CTRS\_SMTP\_SECURE\_MAIL

**Severity**

Critical

**Message**

Smtp secure mail cannot be sent

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1601

## CTRS\_SMTP\_SEND\_MAIL

**Severity**

Critical

**Message**

Failed to send mail to '\$1

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1602



**CTRS\_SMTP\_INVALID\_HOSTNAME****Severity**

Critical

**Message**

Smtp hostname id invalid

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1603

**CTRS\_SMTP\_SECURE\_CREDENTIALS****Severity**

Critical

**Message**

Username or Password is not configured

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1604

**CTRS\_SMTP\_CONFIGURATION****Severity**

Critical

**Message**

SMTP Hostname Not Configured

**Recommendation**

Contact your support team.

**Application Name and Message Code**

SMTP 1605

# LCAL Messages

## CTRS\_LCAL\_MODIFIED

**Severity**

Info

**Message**

\$1

**Recommendation**

Locales have been modified. No action is required.

**Application Name and Message Code**

LCAL 2000

# CCS Messages

## DIAL\_OUT

**Severity**

Info

**Message**

CTRS dialed out to URI=%s

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2000

## DIAL\_IN

**Severity**

Info

**Message**

CTRS received dial in from URI=%s

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2001

**HANG\_UP****Severity**

Info

**Message**

CTRS sent hang up to remote participants

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2002

**LOCAL\_HOLD****Severity**

Info

**Message**

CTRS sent hold to remote participants

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2003

**REMOTE\_HOLD****Severity**

Info

**Message**

CTRS received hold from remote participant

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2004

**LOCAL\_RESUME****Severity**

Info

**Message**

CTRS sent resume to remote participants

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2005

**REMOTE\_RESUME****Severity**

Info

**Message**

CTRS received resume from remote participant

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2006

**LOCAL\_REINVITE****Severity**

Info

**Message**

CTRS sent reinvoke to remote participants

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2007

**REMOTE\_REINVITE****Severity**

Info

**Message**

CTRS received reinvite from remote participant

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2008

**LOCAL\_CANCEL****Severity**

Info

**Message**

CTRS sent cancel to remote participants

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2009

**REMOTE\_CANCEL****Severity**

Info

**Message**

CTRS received cancel from remote participant

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2010

**CREATE\_MSG\_QUEUE\_FAIL****Severity**

Info

**Message**

System Error -- Could not create %s message queue

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2011

**FIND\_MSG\_QUEUE\_FAIL****Severity**

Info

**Message**

System Error -- Could not find %s message queue

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2012

**MSG\_RCV\_ERROR****Severity**

Info

**Message**

System Error -- Message receive error %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2013

**MSG\_SEND\_ERROR****Severity**

Info

**Message**

System Error -- Message send error %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2014

**UCM\_CONFIG\_INCOMPLETE****Severity**

Info

**Message**

System Error -- Unified CM/Access Configuration is incomplete

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2015

**TRANSACTION\_ID\_WRAP****Severity**

Info

**Message**

System Error -- Transaction ID wrapped around

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2016

**BW\_NEG\_FAIL****Severity**

Info

**Message**

Bandwidth negotiation failed, cause = %d, calling number = %s

**Recommendation**

Check the bandwidth and video quality configuration on the endpoint.

**Application Name and Message Code**

CCS 2017

**MAX\_PARTICIPANTS****Severity**

Info

**Message**

Call being terminated due to maximum participants exceeded

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2018

**QUALITY\_MISMATCH****Severity**

Info

**Message**

Call being terminated due to quality mismatch

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2019

**PROCESS\_STARTED****Severity**

Info

**Message**

System -- Process started

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2020



**DIAL\_NUM\_NONEXISTENT****Severity**

Info

**Message**

Call being terminated as dialed number does not exist

**Recommendation**

Verify that the dialed number is correct. Ensure that the Cisco Unified CM trunk settings are correct.

**Application Name and Message Code**

CCS 2021

**XMLRPC\_INIT\_FAIL****Severity**

Info

**Message**

System Error -- Failed to create XML/RPC interface

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2022

**QUALITY\_MISMATCH****Severity**

Info

**Message**

Call being terminated due to quality mismatch

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2023

**INTEROP\_FAIL****Severity**

Info

**Message**

CTRS does not support interop. Cannot join interop meeting

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2024

**UCM\_CONFIG\_READ\_ERROR****Severity**

Info

**Message**

Configuration Error -- Cannot read UCM configuration file

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2025

**MAC\_ADDRESS\_READ\_ERROR****Severity**

Info

**Message**

Configuration Error -- Cannot get primary MAC address, CCS halting

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2026

**MAC\_ADDRESS\_WRITE\_ERROR****Severity**

Info

**Message**

Configuration Error -- Cannot set MAC address in configuration table, CCS halting

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2027

**IP\_ADDRESS\_READ\_ERROR****Severity**

Critical

**Message**

Cannot get primary IP address, CCS halting

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2028

**UCM\_CONFIG\_ERROR****Severity**

Error

**Message**

Error in Unified CM configuration file

**Recommendation**

Verify that the Cisco Unified CM configuration in the administrative UI is correct.

**Application Name and Message Code**

CCS 2029

**NO\_UCM\_CONFIG****Severity**

Warning

**Message**

Unified CM IP address not in Unified CM configuration file

**Recommendation**

Verify that the Cisco Unified CM configuration in the administrative UI is correct.

**Application Name and Message Code**

CCS 2030

**ACCESS\_NOT\_CONFIG****Severity**

Warning

**Message**

Access name not in the Unified CM configuration file

**Recommendation**

Verify that the Cisco Unified CM configuration in the administrative UI is correct.

**Application Name and Message Code**

CCS 2031

**RESUME\_FAIL****Severity**

Error

**Message**

Resume participant returned failure

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2032

**DISCONNECT****Severity**

Info

**Message**

Call from %s being disconnected

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2034

**PLAY\_FINISH****Severity**

Info

**Message**

Endpoint %s finished playback

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2035

**RECV\_NOT\_ACCEPTABLE****Severity**

Info

**Message**

Dialing %s received 488 Not Acceptable Here from Unified CM. Check SIP trunk config.

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2037

**RECV\_FORBIDDEN****Severity**

Info

**Message**

Dialing %s received 403 Forbidden from Unified CM. Check SIP trunk config.

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2039

**NUM\_NOT\_FOUND****Severity**

Info

**Message**

Dialed Number %s does not exist, Number Not Found recv from Unified CM

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2040

**QUALITY\_MISMATCH****Severity**

Info

**Message**

Failed to replay video %s since remote participant %s has insufficient bandwidth

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2041

**SPAWN\_MEDIA\_FAIL****Severity**

Critical

**Message**

Media Process (RMA) failed to spawn for call %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2042

**XMLRPC\_INIT\_FAIL****Severity**

Critical

**Message**

XmlRpc listen socket for server could not be opened

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2043

**NO\_ACCESS\_NAME****Severity**

Critical

**Message**

Access name not defined in ccm config file

**Recommendation**

Contact your support team.

**Application Name and Message Code**

CCS 2044

**NEG\_QUALITY****Severity**

Info

**Message**

Call dial=%s recid=%s negotiated quality=%d

**Recommendation**

No action is required.

**Application Name and Message Code**

CCS 2045

**SECURITY\_MISMATCH****Severity**

Info

**Message**

Failed to setup session due to security mismatch with remote participant %s

**Recommendation**

Check the security configuration of the CTRS and the remote participant.

**Application Name and Message Code**

CSS 2046

**SERVICE\_UNAVAILABLE****Severity**

Critical

**Message**

Service is unavailable. Call dial=%s failed.

**Recommendation**

Check security and the trunk configuration of the CTRS. Potential mismatch possible between CTRS configuration and the Cisco Unified CM configuration.

**Application Name and Message Code**

CSS 2047

## MEDIA Messages

**FILE\_INIT\_FAIL****Severity**

Alert

**Message**

File %s failed to initialize

**Recommendation**

Check previous alarms to help determine the cause of this condition.

**Application Name and Message Code**

MEDIA 3000

**FILE\_CLOSE\_FAIL****Severity**

Alert

**Message**

File %s failed to close

**Recommendation**

Check previous alarms to help determine the cause of this condition.

**Application Name and Message Code**

MEDIA 3001



**FILE\_OPTIMIZE\_FAIL****Severity**

Alert

**Message**

File %s failed to optimize

**Recommendation**

Play the recording without optimization to evaluate its quality.

**Application Name and Message Code**

MEDIA 3002

**FILE\_OPEN\_FAIL****Severity**

Alert

**Message**

File %s failed to open

**Recommendation**

Check previous alarms to help determine the cause of this condition.

**Application Name and Message Code**

MEDIA 3003

**REMOTEHOST\_RESOLVE\_FAIL****Severity**

Alert

**Message**

Failed to resolve remote hostname %s

**Recommendation**

Verify that the remote hostname is correct.

**Application Name and Message Code**

MEDIA 3004

**OVERRUN****Severity**

Alert

**Message**

Received too many frames in jitter buffer, unable to recover

**Recommendation**

Monitor to see if the condition is temporary. It is possible that media processor could not handle the load, or a network burst occurred.

**Application Name and Message Code**

MEDIA 3005

**UNDERRUN****Severity**

Alert

**Message**

Lost too many frames, unable to recover

**Recommendation**

Monitor to see if the condition is temporary. It is possible that media processor could not handle the load, or a network condition occurred.

**Application Name and Message Code**

MEDIA 3006

**CONNECTION\_LOSS****Severity**

Alert

**Message**

Lost network connection with remote side

**Recommendation**

Check the network connection between endpoints.

**Application Name and Message Code**

MEDIA 3007

**UNKNOWN\_MEDIA\_FORMAT****Severity**

Alert

**Message**

Unknown media format %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

MEDIA 3008

**PROCESS\_INIT\_FAIL****Severity**

Alert

**Message**

Failed to spawn media process

**Recommendation**

Contact your support team.

**Application Name and Message Code**

MEDIA 3009

**RECORDING\_CLOSE****Severity**

Alert

**Message**

Recording %s saved, duration %d seconds

**Recommendation**

No action is required.

**Application Name and Message Code**

MEDIA 3010

**RECORDING\_CLOSE\_FAIL****Severity**

Alert

**Message**

Recording not saved, duration %d seconds too short

**Recommendation**

Contact your support team.

**Application Name and Message Code**

MEDIA 3011

**NEG\_TIMEOUT****Severity**

Alert

**Message**

Call being terminated due to media timeout

**Recommendation**

Try again. It is possible that media negotiation failed timed out because of a network condition.

**Application Name and Message Code**

MEDIA 3012

**SSRC\_COLLISION****Severity**

Warning

**Message**

SSRC collision. More than one media source had the same source identifier.

**Recommendation**

Retry the call.

**Application Name and Message Code**

MEDIA 3013

**NO\_MEDIA****Severity**

Warning

**Message**

No media received for session calling number %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

MEDIA 3014

**READ\_ERROR****Severity**

Warning

**Message**

Error reading mp4 file %s

**Recommendation**

Download the recording and play with any player.

**Application Name and Message Code**

MEDIA 3015

**SAMPLE\_ERROR****Severity**

Warning

**Message**

Error reading mp4 sample in mp4 file %s

**Recommendation**

Download the recording and play with any player.

**Application Name and Message Code**

MEDIA 3016

**INVALID\_DIR****Severity**

Warning

**Message**

Invalid media direction %d

**Recommendation**

Contact your support team.

**Application Name and Message Code**

MEDIA 3017

# POST Messages

## MSG\_RCV\_ERROR

**Severity**

Info

**Message**

System Error -- Message receive error %s

**Recommendation**

Contact your support team.

**Application Name and Message Code**

POST 5000

## CREATE\_MSG\_QUEUE\_FAIL

**Severity**

Info

**Message**

System Error -- Could not create %s message queue

**Recommendation**

Contact your support team.

**Application Name and Message Code**

POST 5001

# EXEMGR Messages

## ALARM\_EXECMGMT\_STARTED

**Severity**

Info

**Message**

Execution Manager have started all CTRS processes

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6000

**ALARM\_EXECMGMT\_SHUTDOWN****Severity**

Info

**Message**

Execution Manager received signal=%d, shutdowns all CTRS processes now

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6001

**ALARM\_PROCESS\_EXIT****Severity**

Critical

**Message**

Execution Manager detected a process(%s exit=%d) exit, will try restarting CTRS processes shortly

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6002

**ALARM\_PROCESS\_DEAD****Severity**

Critical

**Message**

Execution Manager detected a process(%s signal=%d) dead, will try restarting CTRS processes shortly

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6003

**ALARM\_PROCESS\_ABORT****Severity**

Critical

**Message**

Execution Manager detected a process(%s %s=%d) abort, will try shutdown CTRS processes shortly

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6004

**ALARM\_EXECMGMT\_ABORT****Severity**

Critical

**Message**

Execution Manager is aborted because %s

**Recommendation**

No action is required.

**Application Name and Message Code**

EXEMGR 6005