



Cisco TelePresence Content Server Administration and User Guide for Release 6.2.1

Published: August, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

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 Content Server Release 6.2.1 Administration and User Guide
© 2015 Cisco Systems, Inc. All rights reserved.



Preface vi

New in Cisco TelePresence Content Server Release 6.2.1 vi

Related Documentation vii

Obtaining Documentation and Submitting a Service Request vii

CHAPTER 1

The Management Tab 1-1

Server Overview 1-2

Cluster Overview 1-6

Server Logs 1-7

Transcoding Queue 1-8

Edit Recordings 1-9

Edit Recording 1-9

Open Content Editor 1-15

Manage Outputs 1-17

Import Recordings 1-25

Create Recording 1-27

Recording Aliases 1-33

Adding or Editing Recording Aliases 1-34

Categories 1-40

Adding and Editing Categories 1-41

Templates 1-41

Adding or Editing Templates 1-42

Media Server Configurations 1-49

Windows Media Streaming Server 1-51

QuickTime or Darwin Streaming Server 1-54

Wowza Media Server for Flash 1-58

Cisco Video Streamer Server 1-61

Media Experience Engine 3500 Server 1-61

Show and Share Server 1-62

Podcast Producer Server 1-63

iTunes U Server 1-64

Call Configurations 1-65

Adding and Editing Call Configurations	1-66
Site Settings	1-67
View all gatekeeper registrations	1-81
View all SIP registrations	1-82
Upload language pack	1-84
Groups and Users	1-85
Adding and Editing Groups and Users	1-88
Creating Automatic Personal Recording Aliases	1-90
Windows Server	1-91

CHAPTER 2

Cisco TelePresence Content Server Integration with VBrick	2-1
Integration Overview	2-1
What is the Cisco TelePresence Content Server	2-1
What is VBrick DME	2-2
Prerequisites	2-2
Limitations	2-2
Configuring Cisco TelePresence Content Server	2-3
Configuring Media Server for VBrick VoD	2-3
Configuring Template for VBrick VoD	2-4
Configuring Recording Alias for VBrick VoD	2-5
Configuring Media Server for VBrick Live	2-6
Configuring Template for VBrick Live	2-8
Configuring Recording Alias for VBrick Live	2-10
Installing vBrick DME (Software only version)	2-11
Related Documentation	2-12
Disclaimers and Notices	2-12
Obtaining Documentation and Submitting a Service Request	2-13
2-14	

CHAPTER 3

Configuring a Cisco Unified Communications Manager SIP Trunk with a Cisco TelePresence Content Server	3-15
CUCM Integration with Content Server 6.2	3-15
Cisco Content Server Standalone	3-15
SIP Route pattern Configuration Setting:	3-20
Configuring Route Patterns Using Route Group/ Route List	3-24
Cisco Content Server Cluster Configuration	3-33
Region configuration on CUCM	3-35
CUCM Configuration Setting on Content Server	3-36

CHAPTER 4**Content Server VM with BE6K 4-1**

Introduction 4-1

Content Server VM with BE6K Features: 4-1

UI changes on Content Server for BE6K solution 4-2

Management Tab 4-2

APPENDIX 5**Supported Platforms, Browsers, and Plug-ins 5-1****CHAPTER 6****Creating and Managing a Content Server Cluster 6-1**

About Content Server Clusters 6-2

System Requirements 6-4

Important Guidelines 6-5

Setting up a Content Server Cluster 6-6

Overview of the Process 6-6

Content Server Cluster Prerequisites 6-6

Configure the External SQL Server Database 6-7

Add an SQL Server Instance 6-7

Configure the SQL Server Instance 6-8

Create a Special User on the SQL Server 6-10

Configure the NAS 6-11

Manage the Windows Active Directory Domain 6-11

Choose or Create a Domain Account to Access the NAS Share 6-11

Set up a Share on the NAS 6-11

Set Permissions and Security Settings on the Share 6-12

About Creating a Content Server Cluster 6-13

The Order of Content Servers Added to the Cluster 6-13

Content Server Wizard Options 6-14

User Accounts for the Content Server Wizard 6-14

Before Running the Content Server Wizard 6-15

Create a New Content Server Cluster 6-15

Add a Content Server to an Existing Cluster 6-17

Configure Gatekeeper Registration for H.323 Cluster 6-18

Configure Gatekeeper Registration for SIP Cluster 6-19

Configure Domain Authentication 6-19

Configure Network Load Balancing (NLB) 6-19

Configure a Load Balancer 6-21

Set up a Loopback Adapter on Each Content Server in Cluster 6-22

Enter the Cluster Virtual IP Address as the Frontend Address on the Content Server 6-22

Managing a Content Server Cluster	6-23
Access Cluster Administrative Pages	6-23
View Cluster Status	6-24
Edit Information for Each Content Server in Cluster	6-25
Edit Information Common to All Content Servers in Cluster	6-25
Generate a Cluster Settings File	6-27
Update Load Balancer Configuration	6-27
Update Cluster Settings	6-28
Update the Password for MYDOMAIN\Content Server_NAS_USER Account	6-28
Change the MYDOMAIN\Content Server_NAS_USER Account to Another Domain Account	6-29
Change the Location of the Media Files to a Different NAS Share	6-29
Removing a Content Server from the Cluster	6-30
Using TMS to Schedule Calls on a Content Server Cluster	6-31
Backing Up and Restoring the Content Server Cluster	6-32
Backing Up Clustered Content Servers	6-32
Backing Up the External MS SQL Database	6-32
Backing Up Media on the NAS/External Streaming Server	6-32
Upgrading the Cluster to a New Software Version	6-33
Upgrading the External Microsoft SQL Server	6-33

CHAPTER 7

The My Recordings Tab	7-1
Edit Recordings	7-1
Edit Recording	7-2
Open Content Editor	7-5
Manage Outputs	7-8
Create Recording	7-16
Edit Recording Aliases	7-17

CHAPTER 8

Understanding Distribution Outputs	8-1
Configuring Automatic Upload to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U	8-1
Uploading Existing Recordings to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U	8-2
Understanding the Difference between Distribution Outputs and Streaming Servers	8-3

CHAPTER 9

Maintaining the Content Server	9-1
Backing Up the Content Server	9-1

	Before Backing Up	9-1
	Performing a Manual Backup	9-2
	Configuring a Scheduled Backup	9-2
	Restoring Files	9-3
	Before Restoring	9-3
	Restoring from a Backup	9-3
	Performing a Software Reimage	9-4
	Reimage Instructions	9-5
	Task 1: Clear the hard drive and install the software	9-5
	Task 2: Install the license files	9-6
	Task 3: Configure the basic settings	9-8
	Restoring Files After a Software Reimage	9-8
	Restore Files on a Reimaged Standalone Content Server	9-8
	Restore Files on a Reimaged Content Server with Network Attached Storage	9-9
	Restore Files on a Reimaged Content Server in a Cluster	9-10
	Shutting Down and Powering Off the Content Server	9-11
	Securing the Content Server	9-12
APPENDIX 10	Port Information	10-1
CHAPTER 11	Premium Resolution	11-1
	Configuring and Using the Premium Resolution Features	11-1
CHAPTER 12	Understanding Recording Aliases	12-1
CHAPTER 13	Setting Up External Media Storage	13-1
	Changing the Local Storage Location to NAS	13-1
	Reverting NAS Storage Location to the Default	13-3
	Changing NAS Storage to New Location	13-3
	Managing the Domain Account for NAS Access	13-4
CHAPTER 14	Using Cisco TMS with the Content Server	14-1
	Configuring the Content Server for Use by TMS	14-1
	Using TMS to Schedule Recording Sessions	14-2
CHAPTER 15	The View Recordings Tab	15-1
	Watching a Recording in the Content Server Web Interface	15-1

Watching a Downloaded Output on Your Computer	15-2
Watching a Downloaded Recording on a Portable Device	15-3
Sending a Link to the Recording to Others	15-3



Preface

For information about supported software upgrade paths and software upgrade instructions, system limitations, important notes, and open and resolved caveats, see the [Release Notes](#) on Cisco.com.

See these sections for release specific features and general information:

- [New in Cisco TelePresence Content Server Release 6.2.1](#)
- [Related Documentation, page vii](#)
- [Obtaining Documentation and Submitting a Service Request, page vii](#)

New in Cisco TelePresence Content Server Release 6.2.1

These are the new Content Server Release 6.2.1 features:

- This release supports configuring VBrick as a media server for both Live and on Demand calls. The file format supported is MPEG-4 for flash.
- This release also supports the Parallel Transcoding. It provides the feature to run 2 transcode engines simultaneously i.e. 2 jobs will be taken up simultaneously by the transcode engine.

Related Documentation

- Cisco TelePresence Content Server Documentation
http://www.cisco.com/en/US/products/ps11347/tsd_products_support_series_home.html
- Cisco UCS C220 Documentation
http://www.cisco.com/en/US/products/ps10493/tsd_products_support_series_home.html
- Cisco Capture Transform Share Documentation
http://www.cisco.com/en/US/products/ps12130/products_installation_and_configuration_guides_list.html

Information About Accessibility and Cisco Products

For information about the accessibility of the Cisco product, contact the Cisco accessibility team at accessibility@cisco.com.

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*, that also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/c/en/us/td/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.



The Management Tab

This chapter explains the procedures performed in the **Management** tab of the Content Server web User Interface (UI).

The **Management** tab is in four menus, and each menu has submenus:

Diagnostics

- [Server Overview, page 1-2](#)
- [Cluster Overview, page 1-6](#) (appears only with a cluster deployment)
- [Server Logs, page 1-7](#)
- [Transcoding Queue, page 1-8](#)

Recordings

- [Edit Recordings, page 1-9](#)
- [Import Recordings, page 1-25](#)
- [Create Recording, page 1-27](#)

Recording Setup

- [Recording Aliases, page 1-33](#)
- [Categories, page 1-40](#)
- [Templates, page 1-41](#)
- [Media Server Configurations, page 1-49](#)
- [Call Configurations, page 1-65](#)

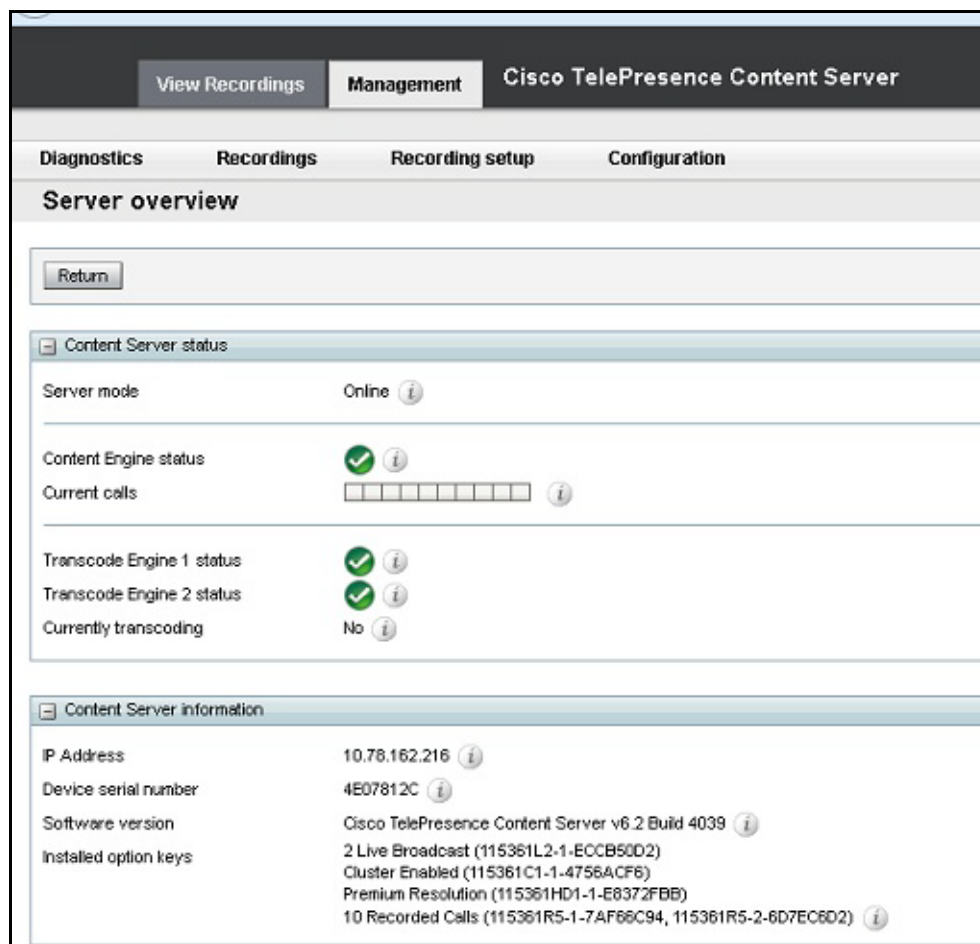
Configuration

- [Site Settings, page 1-67](#)
- [Groups and Users, page 1-85](#)
- [Windows Server, page 1-91](#)

Server Overview

To display the **Server overview** page, go to **Diagnostics > Server overview**. This page displays the status of the Content Server and is automatically updated every ten seconds. On a standalone Content Server, user can add option keys to activate features, you cannot update any fields on this page. For a Content Server in a cluster, this page is also used to set the System name, H.323 IDs and E.164 aliases.

Figure 1-1 Server Overview



The shows the server overview in the Diagnostics section.

Table 1-1 Diagnostics > Server Overview

Field	Field Description	Usage Guidelines
System information		

Table 1-1 *Diagnostics > Server Overview (continued)*

Field	Field Description	Usage Guidelines
System name	The name for the Content Server that is unique in the cluster.	<p>The System information section is displayed only for Content Servers in a cluster.</p> <p>You can set the system name for a Content Server here only if it is in a cluster. Go to Site Settings to set this field for a standalone Content Server.</p> <p>If the Content Server is in a call when this field changes, it enters into the Configuration reload mode. The change will not take effect until all calls have ended.</p>
H.323 ID	The system non-live and live H.323 IDs for this Content Server to register to the gatekeeper. It is not recommended to call the Content Server using these H.323 IDs while in a cluster.	<p>The System information section is displayed only for Content Servers in a cluster.</p> <p>You can set the H.323 ID for a Content Server here only if it is in a cluster. Go to Site Settings to set this field for a standalone Content Server.</p> <p>If the Content Server is in a call when this field changes, it enters into the Configuration reload mode. The change will not take effect until all calls have ended.</p>
E.164 alias	The system non-live and live E.164 aliases for this Content Server to register to the gatekeeper. It is not recommended to call the Content Server using these E.164 aliases while in a cluster.	<p>The System information section is displayed only for Content Servers in a cluster.</p> <p>You can set the E.164 alias for a Content Server here only if it is in a cluster. Go to Site Settings to set this field for a standalone Content Server.</p> <p>If the Content Server is in a call when this field changes, it enters into the Configuration reload mode. The change will not take effect until all calls have ended.</p>

Table 1-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
Content Server status		
Server mode	The current status of the Content Server.	<p>Online: The Content Server can accept calls and transcode outputs.</p> <p>Configuration reload: One or more of system name, gatekeeper settings, advanced H.323 settings, SIP settings or email settings have been saved in Configuration > Site settings while the Content Server was in a call. The Content Server is not accepting new calls. When current calls are complete, settings are updated. Then the server mode changes to Online.</p> <p>Maintenance: If the Content Server is in a cluster, the site manager can place it in Maintenance mode, which means that no new calls or offline transcoding jobs are accepted. Entering maintenance mode or rejoining the cluster is done on the Cluster overview page.</p> <p>Idle: The Content Server wizard is running. The Content Server is not accepting new calls or processing new offline transcoding jobs. To exit idle mode, complete or cancel the wizard.</p> <p>Offline: The Content Engine service is not running. Current calls are dropped, and new calls are not accepted. To exit offline mode, start the Content Engine service. For example, you can restart the Content Engine service by restarting the Content Server. In the web interface for Windows Server administration, go to Services > Stop the service > Restart the service.</p> <p>Error: The Content Server is out of disk space. Less than 5% disk space remains free on the C: or E: drive or on the network attached storage (NAS). Error might signify that the Content Server has lost connection to the NAS. Current calls are dropped, and new calls or offline transcoding jobs are not accepted. To exit Error mode, free up disk space, or, if the storage location is on a NAS (see below), check the NAS, the share permissions and the network.</p>
Content Engine status	The current Content Engine service status.	<ul style="list-style-type: none"> • A check in a green circle means that the service is running. • An exclamation point in a red circle means that the service is not running. The exclamation point appears with the date and time when the Content Server last contacted the database.
Current Calls	<p>A pictorial representation of the number of current calls.</p> <ul style="list-style-type: none"> • Up to 5 concurrent calls • Up to 10 concurrent calls with the 5 Additional Recording Ports option enabled 	<ul style="list-style-type: none"> • An orange bar represents a call with live streaming outputs. • A brown bar represents a call with on-demand outputs only.

Table 1-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
Playback call list	A list of recordings that are currently being played back on endpoints. Each recording is identified by its name and duration.	Click End Call to terminate playback of the recording on the endpoint. Click End all calls to terminate playback of all recordings.
Recording call list	A list of recordings that are currently being made.	Click Edit to display the Edit recording page for the recording.
Transcode Engine status	The current Transcode Engine status and Parallel Transcoding Engine2 status.	<ul style="list-style-type: none"> A check in a green circle means that the service is running. An exclamation point in a red circle means that the service is not running. The exclamation point appears with the date and time that the Content Server last contacted the database.
Currently transcoding	Whether the Content Server is currently transcoding	<p>An arrow in the counter-clockwise direction means that recordings are being transcoded. No means that no recordings are being transcoded.</p> <p>If the Content Server is currently transcoding, the transcoding job list displays a list of recording names that are currently being transcoded, the outputs being produced and the percentage completed.</p>
Transcoding job list	The list of recordings currently being transcoded.	Click Edit to display the Edit recordings page or Manage outputs to display the Manage outputs page for the recording.
End all calls	The End all calls button is displayed when there are calls in progress.	Click End all calls to terminate all current calls.
Content Server information		
IP address	The Content Server IP address.	—
Device serial number	The Content Server serial number.	The serial number is used to generate keys that are required to upgrade the Content Server.
Software version	The currently installed software version.	The software version is also displayed at the bottom of every page in the My Recordings and Management tabs.
Installed option keys	The option keys and descriptions of what they allow.	—
Server disk space		
Path, Total disk space, Free disk space, Percentage free	The total available disk space, free disk space and the free disk space as a percentage of the total for the C: and E: drives. If the media storage location is on a NAS (see below), disk space on the NAS is also displayed.	The graphic space indicators are red if free disk space is less than 10%. When free disk space is less than 5%, the Content Server drops current calls and enters Error mode (does not accept any new calls or new offline transcoding jobs).

Table 1-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
C	The Content Server C: drive.	—
E	The Content Server E: drive.	—
Database location		
Database data source	Displays the server address, port, and instance to the database for this Content Server.	On a standalone Content Server, database data source is always Local Content Server . For Content Servers in a cluster, the database is located on an external server.
Database name	The name of the Content Server database.	—
Media storage location		
Media storage location	Where media is currently stored.	The default media storage location is on the local E: drive. When a local drive is used, this field displays Local Content Server . For Content Servers that uses a Network Attached Storage (NAS) device, a path to the NAS location is displayed.
Software option		
Add option key	Content Server features can be activated by adding option keys provided by authorized Cisco resellers or partners; for example, the clustering option key, the Premium Resolution option key and the 5 Additional Recording Ports option key to enable up to 10 concurrent on-demand recordings.	After adding the option key, click the Restart service button for the installed option key to take effect.
Restart service	Click to restart the Content Engine.	Click the Restart service button to restarts the Content Engine. All current calls are dropped, but restarting the service does not affect transcoding or displaying web pages.

Cluster Overview

Up to ten Content Servers can be clustered to increase the total call capacity and improve redundancy and resilience. Such a cluster uses scalable external storage, an external Microsoft SQL Server database, and provides one web interface for viewing and managing the cluster. Calls are balanced across the cluster by the VCS. The use of a network load balancer ensures that incoming HTTP user requests are spread evenly across the servers in the cluster. All configurations and recording information are global across the cluster.

If you access a cluster from a load-balanced address, not all menu items are displayed. To access other **Management** tab menus, site managers must log in to an individual node on the cluster by using the node's IP address or fully qualified domain name (FQDN).

If you are in a cluster deployment, the Cluster overview page provides information about cluster status, as well as the number of calls and offline transcoding jobs in progress. It is automatically updated every ten seconds.

Displaying the Cluster Overview

To display the Cluster overview page, in the **Management** tab, go to **Diagnostics > Cluster overview**. The Cluster overview page does the following:

- Lists the system names and IP addresses of all the Content Servers in the cluster.
- Displays a link to the [Server Overview](#) page for each Content Server. In addition to the standard server overview information, a Content Server's system name, H.323 ID and E.164 alias are set in the Server overview page when in a cluster.
- Reports the total number of current calls for the cluster and for each Content Server.
- Reports the total number of offline transcoding jobs in progress for the cluster and for each Content Server.
- Reports the server mode for each Content Server.
- Reports the status for each Content Server. If the Content Server's mode is **Online**, then the **Status** displays a green check mark, meaning that the Content server is running correctly. If the Content Server's mode is not **Online**, then the **Status** displays a red exclamation mark. Go to [Server Overview](#) for this Content Server to see more details.
- Displays links to each Content Server's server logs and web interface for [Windows Server](#) administration.
- Allows you to **End all calls** on the whole cluster. If you want to end calls on a particular Content Server only, do this from the [Server Overview](#) page for that Content Server.
- Allows you to put a Content Server in **Maintenance** mode. In this mode, no new calls or offline transcoding jobs are accepted on that server, but current calls and jobs continue until completed. The other Content Servers in the cluster continue working as usual.

Maintenance mode should be used to ensure that no new calls are made to a Content Server—for example, if you want to defragment its drive, run a Windows security update installer or update antivirus software on that Content Server. You should also put a Content Server in Maintenance mode (after ending its current calls) if you need to shut it down and move it to another location.

To put a Content Server in Maintenance mode, click **Enter maintenance mode**. The button changes to **Rejoin cluster**, and the Server mode displays **Maintenance**. After you have completed maintenance, click **Rejoin cluster**. The button changes back to **Enter maintenance mode** and Server mode displays **Online**. This means that the Content Server is now ready to receive calls and offline transcoding jobs.

Server Logs

To view the Content Server logs, go to **Diagnostics > Server logs**. The logs from the Content Engine are displayed by default. To view other logs, select a log type from the drop-down list.

- To view a log, click the log file name. In the dialog box that appears, open or save the file.
- The list of log files might consist of more than one page. Click on a page number to display additional logs.
- To delete a log, check the box next to the file name. Then click **Delete selected**.

- The current log is displayed at the top of the list. Except for Content Library logs, the current log cannot be deleted.

You can also access logs from the E:\logs directory on the Content Server. Service event logs for the Content Engine, Transcode Engine, and Helper services can be found in the Windows Event Viewer when you Remote Desktop to the Content Server. These events show service starting and stopping information.

These are the four types of logs:

- Content Engine—generated by the Content Engine, these logs contain information about the following:
 - Incoming and outgoing calls
 - Codecs in call, call speed
 - Dual video start/stop during a call
 - Gatekeeper and SIP registrations
 - Information about the generation of live streaming and live transcoded outputs
 - Reasons for disconnected and rejected calls

A new log is created every time the Content Engine service restarts or if the current log exceeds 10 MB.

- Transcode Engine—these logs include information about offline transcoded outputs, including the output size and format, and how long the output took to transcode.

A new log is created every time the offline Transcode Engine service is restarted or if the current log exceeds 10 MB.

- Helper—generated from the Helper service, these logs include information about the following:
 - The transfer of transcoded and dump files from temporary to final storage location
 - Exporting and importing of .tcb files
 - FTP transfer
 - Hinting for MPEG-4 for QuickTime outputs
 - When recording outputs have been deleted

A new log is created every time the Helper service is restarted or if the current log exceeds 10 MB.

- Content Library—include information reported by the web interface. Most log entries can be ignored unless something unexpected has occurred while using the interface.

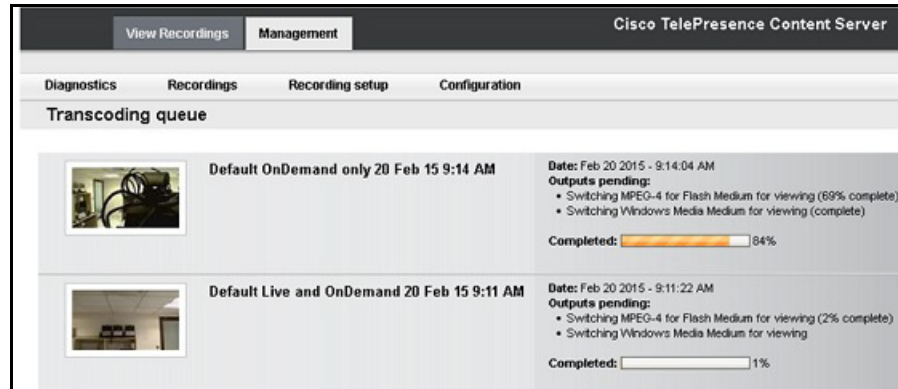
The phperror log file rolls automatically when the file size is approximately 5 MB. Click the **Roll log file** to start a new log file manually.

Transcoding Queue

To view the Content Server transcoding queue, go to **Diagnostics > Transcoding queue**. The transcoding queue shows recordings for which the Content Server is currently processing (transcoding) the outputs. The number and types of output depend on the recording alias (see the [Recording Aliases](#) section for more information) that was used for the recording. The number and types of output could also depend on what options were selected in the [Manage Outputs](#) page. See [Understanding Recording Aliases](#) for more information.

The Transcoding queue page refreshes automatically every 10 seconds.

Figure 1-2 Transcoding Queue

**Note**

When two recordings are being parallel transcoded.

Only site managers have access to the recordings transcoding queue. Guests, viewers, and creators see the transcoding icon next to recordings when outputs are queued for transcoding.

Edit Recordings

You can display a list of editable recordings by going to **Recordings > Edit recordings**. From this list, you can do the following:

- **Play**—click to play a specific recording.
- **Edit Recording**—click to edit settings for the recording, including the recording name and who can view it.
- **Content Editor**—click to access the Content Editor for various formats. Use the Content Editor to index or crop the recording. You can also concatenate another recording to one that is open in the Content Editor.
- **Manage Outputs**—click to modify output settings, including how the recording is viewable in a web interface or in what formats the recording is downloadable.
- **Delete one or more recordings**—check one or more recording boxes (to the left of each recording thumbnail). Then click the **Delete selected** button on the bottom left of the page. You can also click the **X** to the far right to delete one recording at a time.

Edit Recording

Users with the appropriate permissions and all site managers can edit recording settings at any time.

To edit recording settings, do the following:

- Step 1** Go to **Recordings > Edit recordings**. A list of recordings appears.
- Step 2** Locate the recording whose settings you want to edit.

- Step 3** Click **Edit recording**. A page that includes the settings for the recording appears.
- Step 4** Update recording settings as needed (see [Table 1-2](#)).
- Step 5** After updating the settings, click **Save**.

Table 1-2 *Recordings > Edit Recordings: Edit Recording*

Field	Field Description	Usage Guidelines
Recording information		
Name/Title	The name of the recording to be displayed in the View Recordings pages.	The default name is the type of recording (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name (maximum 255 characters) to help users find the recording when they search.
Description	Details about the recording.	Optional. The optional description (maximum 1500 characters) can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.
Keywords	Keywords that can be used to search for the recording.	Optional. This optional setting can help users find the recording when they search.
Category	Choose a category under which to list the recording in the View Recordings pages. To create a category, go to Recording setup > Categories .	Optional.
Date	The date and the time at which the recording process began.	Read only. You cannot edit these fields.
Duration	The length of the recording rounded to the nearest minute. In parentheses, length of the recording in HH:MM:SS format.	Read only. You cannot edit these fields.
Share link	The link to the recording.	Read only. You cannot edit these fields.

Table 1-2 Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Recording thumbnails		
Thumbnail images	A thumbnail is an image from the recording that helps users to identify the recording. Thumbnails images are taken at 5 seconds, 1 minute, 5 minutes, 30 minutes, and 1 hour into the recording. The image at 30 minutes into the recording is the default. If the recording is less than 30 minutes, the default is last image taken.	<p>Choose a thumbnail to represent the recording. You might need to refresh the page or restart the browser to see the thumbnail that you chose.</p> <p>Click the thumbnail to choose it. An orange frame surrounds the thumbnail that represents the recording.</p>
Recording permissions		
Who can view this recording	Groups and users who can view the recording. Click the Check access list button to validate your entries. Entries are also validated when you click the Save button.	<p>You can give viewing access to one of the following:</p> <ul style="list-style-type: none"> • Allow access to all users, including guests: If Allow guest access is selected in Site Settings, this field is displayed. If selected, all users, including guests, can view the recording. • Allow access to all authenticated users: If the Allow guest access box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list. <p>Note After you click Check access lists, Place call, or Save, the users entered have the following formats:</p> <ul style="list-style-type: none"> – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, "CN=group.name, OU=staff, DC=company, DC=com").</p>

Table 1-2 *Recordings > Edit Recordings: Edit Recording (continued)*

Field	Field Description	Usage Guidelines
Publish recording	If checked, the selected groups and users under Who can view this recording can view this recording. The groups and users in the editors list can always view and edit the recording.	This box is checked by default. When this box is unchecked, the recording does not appear in the View Recording pages. The recording still appears in the Edit recordings list. Next to the recording, the Publish recording button appears. When you click that button, all specified groups and users can view the recording.
Password (optional)	You can enter a password to restrict streaming access to this recording and the ability to download content. The password will be visible in clear text to editors of this recording and to site managers.	If a password is not entered, users who can view the recording in the View Recordings list can play the recording and download any available content. If a password is entered, users must know the password to stream or download the recording.

Table 1-2 Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Who can edit this recording	Groups and users can edit recording information and permissions, use the Content Editor (see Open Content Editor) to change the recording, add more outputs to completed recordings using the Manage Outputs page, and delete the recording. Use Check access list to validate your entries. They are also checked when you click Place call or Save .	<p>Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon).</p> <ul style="list-style-type: none"> For local authentication mode: only enter groups and users that have been added to the Groups and Users list on the Content Server in this field; otherwise, the entry will be removed when you click Check access list, Place call, or Save. For Domain or LDAP authentication mode: <ul style="list-style-type: none"> With Guest Access disabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. With Guest Access enabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. If a creator adds a user or group to the access list that does not exist on the Content Server, a site administrator must add also that user or group to the Groups and Users. <p>If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list.</p> <p>Note After you click Check access lists, Place call, or Save, the users entered have the following formats:</p> <ul style="list-style-type: none"> Local authentication mode: MACHINENAME\user.name Domain authentication mode: DOMAINNAME (optional)\user.name LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, "CN=group.name, OU=staff, DC=company, DC=com").</p>

Table 1-2 Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Play recording on endpoints		
Make recording available for playing on endpoints	Check to make the recording available for playback on an endpoint.	<p>When you check this box, either a playback H.323 ID or playback E.164 alias will appear. Depending on the Content Server configuration, both might appear. Give users the playback E.164 alias or the playback H.323 ID. Instruct them to dial the alias or ID from an endpoint. Doing so will play back the recording.</p> <p>If this check box is not on the Edit recording page, a Content Server site manager has not configured the prefixes necessary for an E.164 playback alias or H.323 playback ID. Contact a site manager for more information.</p> <p>The recording cannot be played back on an endpoint if it has not been published. See the Publish recording setting above for more information.</p> <p>A recording with restricted viewing access and no viewable interface outputs can be played back from an endpoint. The PIN (optional) field enables you to PIN protect this recording.</p> <p>Tip You can also PIN protect all new recordings created with your personal recording alias (see the Adding or Editing Recording Aliases).</p> <p>Note The content server must be in gateway mode, and have an E.164/H.323 playback prefix for playing on endpoints. See the Site Settings to configure the E.614/H.323 playback prefix.</p> <p>Note The content server must be in trunk mode, and have a SIP playback suffix for playing on endpoints. See the Trunk mode to configure the SIP playback suffix.</p>
Export recording		
Export recording	<p>Click Export record export to export the recording as a .tcb file.</p> <p>When it appears, click Download exported recording link and save the exported .tcb file to an external network location.</p> <p>If necessary, you can also click the Update exported recording link to update the previously exported recording.</p>	<p>How long export takes depends on the duration of the recording and the number of outputs. When complete, the page displays links that allow you to update the exported recording and download the .tcb file.</p> <p>If the recording cannot be exported (for example, because it has pending outputs), the Export recording section does not appear. You can try again later.</p> <p>The .tcb file remains on the source Content Server for a week from the date of exporting. Then the Content Server automatically deletes the .tcb file. Before this automatic deletion, you can update the information and outputs for this recording and export it again by clicking Update exported recording. Updating the exported recording replaces the original .tcb file with an updated one.</p>

Figure 1-3 Play recording on endpoints

The screenshot shows the 'Edit Recording' interface of the Cisco TelePresence Content Server. The 'Management' tab is selected. Under the 'Recordings' sub-tab, the 'Edit Recording' page is displayed. The 'Play recording on endpoints' section is active, showing options to make recordings available for playback on endpoints and for SIP Trunk Mode, both of which are checked. It also displays a specific playback H.323 ID and a SIP playback number.

Open Content Editor

Users with the appropriate permissions and all site managers can use the Content Editor to edit recordings. To use the Content Editor, see the following sections:

- [Indexing a Recording](#)
- [Cropping a Recording](#)
- [Removing a Middle Section from a Recording](#)
- [Joining Recordings](#)

All changes that you make to a recording are non-destructive. For example, you can change the position of the slider at the beginning or at the end of the recording many times.

Viewing the recording in a player reflects the changes immediately. Downloads need to be transcoded again. Click **Save and close** to start the transcoding process. Transcoding again removes existing downloadable outputs and replaces them with the newly transcoded output.



Note

To open a recording in the Content Editor, the recording must have outputs that can be viewed in a player. You can use the Content Editor on an Apple Mac using MPEG-4 for QuickTime or MPEG-4 for Flash. The Content Editor is not available on the Mac for Windows Media recordings using Silverlight.

To open the Content Editor, do the following:

- Step 1** Go to **Recordings > Edit Recordings**. A list of editable recordings appears.
- Step 2** Find the recording that you want to edit with the Content Editor.
- Step 3** Click **Open Content Editor**. A window that lists the formats of available outputs appears.
- Step 4** Click an output format link to open the Content Editor window.

Parts of the Content Editor window

- The top section displays the recording video on the left. The Indexes section is on the right.

- The bottom section displays controls for playing and editing the recording: the seek bar, the volume control, a pause/play button, and a **Join Recording** button.

Indexing a Recording

You can add indexes to make it easier for viewers to find important points in the recording. Index titles appear in a player when users watch the recording. When users click an index, the recording plays from that index point.

To add an index, do the following:

-
- Step 1** Pause the recording where you want an index.
 - Step 2** Click **Add index**. A new index appears in the Indexes section. Each index includes the time of the index point and a default title (Index<number>).
 - Step 3** If you want, click the default title and change it to something more meaningful to viewers.
 - Step 4** Click **Save and Close** to save your index.
-



Note

You can add, delete, or rename indexes in the Content Editor only.

Cropping a Recording

To remove time from the beginning or the ending of a recording, do the following:

-
- Step 1** Locate the seek bar.
 - Step 2** Move the sliders at either end of the seek bar to where you want them. The slider for the beginning of the recording is on the left; the slider for the end of the recording is on the right. In the player, the recording will start from and end wherever you move the sliders.
 - Step 3** Click **Save and Close** to save your slider settings.
-

Removing a Middle Section from a Recording

To remove a middle section, do the following:

-
- Step 1** Click the **Join recording** button. A list of recordings that can be joined to the one that you have open in the Content Editor appears.
 - Step 2** Click the **Join recording** link for the same exact recording. Two thumbnail images appear in the Content Editor window. The first thumbnail with the highlighted box is the original recording. The second thumbnail is the recording that you joined to the first.
 - Step 3** Ensure that you have chosen the first thumbnail by clicking it.
 - Step 4** Move the slider for the end of this recording (the right side) to the beginning of the section that you want to remove.
 - Step 5** Click the second thumbnail.
 - Step 6** Move the slider for the beginning of this recording (the left side) to end of the section that you want to remove.

- Step 7** Click **Save and close**. Then check the results of the removal by playing it back in a player. Redo this procedure until you have adjusted the recording properly.

Joining Recordings

You can join recordings (also know as concatenating) so that they play consecutively. You can join recordings under these conditions:

- You have editing permissions for the recordings, or you are in the site manager role.
- The recordings have streaming outputs in the same format and size (for example, Windows Media in the medium size).
- The recordings have the same dual video status. You cannot join two if only one has a dual video stream.
- The recordings must have the same resolution.

To join two recordings, do the following:

- Step 1** Click the **Join recording** button. A list of recordings that can be joined to the one that you have open in the Content Editor appears.
- Step 2** Click the **Join recording** link for the recording that you want to join to first recording.
- Step 3** Click **Save and close**. Then check the results of joining the recordings in a player. If you want, crop the recordings for a better playback experience (see [Cropping a Recording](#) for more information).

Manage Outputs

Users with the appropriate permissions and all site managers can manage recording outputs at any time.

To manage outputs, do the following:

- Step 1** Go to **Recordings > Edit recordings**. A list of recordings appears.
- Step 2** Locate the recording whose settings you want to edit.
- Step 3** Click **Manage outputs**. A page that includes the output settings for the recording appears.
- Step 4** Update settings as needed (see [Table 1-3](#)).
- Step 5** After updating the settings, click **Save**.

Table 1-3 *Recordings > Edit Recordings: Manage Outputs*

Field	Field Description	Usage Guidelines
Manage outputs		
Recording call speed (kbps)	The bit rate in kbps (kilobits per second) at which the recording was created.	This number might affect the bit rate of medium and large outputs.

Table 1-3 *Recordings > Edit Recordings: Manage Outputs (continued)*

Field	Field Description	Usage Guidelines
Recorded with dual stream	Whether or not this recording was recorded with a dual video stream.	This recording characteristic affects the layouts available for outputs. Only the single video layout is available if this recording was created without a dual video stream.
Viewable in the Content Server web interface	If you check this box, go to the Outputs to view in the Content Server web interface to select output settings for a player.	—
Downloadable for portable devices (iPod and Zune)	If you check this box, go to the Outputs to download for portable devices to select output settings for a player.	—
Downloadable for general purpose	If you check this box, go to the Outputs to download for general purpose to select output settings for a player.	—
Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U	If you check this box, go to the Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U to select output settings for a player.	—

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to view in the Content Server web interface		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, the single video layout with one stream that shows the main video source is created.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video stream. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
On Demand Formats	<p>Choose up to three formats:</p> <ul style="list-style-type: none"> • Windows Media for playback using the Silverlight player or Windows Media player on a PC or the Silverlight player on a Mac. • MPEG-4 for playback using QuickTime. • MPEG-4 for playback using Flash player. 	<p>These formats can be viewed on a PC as long as the correct plugins have been downloaded and installed.</p> <p>MPEG-4 for QuickTime, MPEG-4 for Flash, and Windows Media (played using Silverlight) are available for Apple Mac when the correct plugins have been downloaded and installed.</p>

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
On demand sizes	Choose up to two recording sizes based on your user streaming environment and internet connection.	<ul style="list-style-type: none"> • Audio only: To use when users have very poor quality internet access. • Small: The target bit rate for small outputs is 250 kbps. The target rate is displayed in the Bit rates field. • Medium: For use with broadband access. The target bit rate for medium outputs is 800 kbps. The target rate is displayed in the Bit rates field. • Large: To use with a high-speed LAN. This format takes the longest to transcode. The maximum rate is displayed in the Bit rates field.
Bit rates (kbps)	Displays the target bit rate for the small, medium and large output sizes. The number that is displayed depends on the target bit rates set in Site Settings and the call speed at which the recording was created.	—
On demand media server configuration settings	<p>Choose the Media Server Configurations for on-demand viewing of the recordings that are created with this template. Formats not selected above are dimmed.</p> <p>Click the Optimize for Motion check box to enable.</p>	<p>The media servers configurations that are shown in the drop-down lists by default are those selected in the system defaults section of Site Settings.</p> <p>The Optimize for motion check box improves the quality of high-motion recordings.</p>
Outputs to download for portable devices		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Portable devices	<p>Select portable device(s) and whether you want audio and video or audio only:</p> <ul style="list-style-type: none"> • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible) 	<p>After the Content Server transcodes the recording, these outputs are available for download from the View Recordings page. Click the Download tab for the recording. Then click the output file that you want to download for synchronization with your portable device.</p> <p>iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.</p>
Outputs to download for general purpose		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Formats	Select up to three formats.	—

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Sizes	Select up to two sizes.	<p>Because these outputs are downloaded and viewed on a computer, the quality of the Internet connection is not an issue, except as the connection affects the time it takes to download. After downloading, users can watch the recordings without being connected to the Internet.</p> <p>Note If the download time exceeds 20 minutes, the download will fail.</p>
Bit rates (kbps)	Displays the target bit rate for the small, medium and large output sizes.	—
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Media Experience Engine 3500	Select this option and a media server configuration (see Media Server Configurations) for Media Experience Engine 3500 to automate the process of uploading recorded content to your Media Experience Engine 3500 server.	The size of the output for Media Experience Engine is always large and always MPEG-4 format.
Show and Share	Select this option and a media server configuration (see Media Server Configurations) for Show and Share to automate the process of uploading recorded content to your Show and Share server.	Choose the size (Small , Medium or Large) of the output to upload to Show and Share.
Podcast Producer	Select this option and a media server configuration (see Media Server Configurations) for Podcast Producer to automate the process of uploading recorded content to your Podcast Producer server.	The size of the output for Podcast Producer is always large.
iTunes U	Select this option and a media server configuration (see Media Server Configurations) for iTunes U to automate the process of uploading recorded content to an iTunes U account.	Choose the size (Small , Medium or Large) of the output to upload to iTunes U. You can also specify an additional audio-only output.

Table 1-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Summary		
Outputs to view in the Content Server web interface	Displays information about the outputs created for viewing in the Content Server web interface.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format, layout, and size. • The status of processing the output. • The physical path and filename if the media server configuration of the output adds recordings to the default media location. • How the output was transcoded (live or offline). If the output was transcoded live and there is no offline transcoded output, there is an option to Re-transcode. • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The on-demand URL. • The bandwidth in kbps (kilobits per second) and dimensions.
Outputs to download for portable devices	Displays information about the outputs created for Portable Devices.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • The physical path to the output and the output filename. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.

Table 1-3 *Recordings > Edit Recordings: Manage Outputs (continued)*

Field	Field Description	Usage Guidelines
Outputs to download for general purpose	Displays information about the outputs created for download to users' computers.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • The physical path to the output and the output filename. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U	Displays information about the outputs created for use with Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.

Import Recordings

Site managers can copy a recording from one Content Server to other Content Servers. Copying a recording involves exporting it from one Content Server and importing it to another. Recordings must be copied one at a time.



Note

If the export time exceeds 20 minutes, the process will fail.



Note

Below is an overview of the copying procedure. See [Importing a recording](#) for how to import.

To copy a recording, do the following:

Step 1 Export the recording as a .tcb file (see “Export Recording” in [Table 1-2](#)).

- Step 2** Download the .tcb file to an external directory. The outputs served by the local Media server configurations (Local IIS Web Server and Local Windows Media Streaming Server) and the recording information and permissions are copied and packaged in a .tcb file, which is a proprietary format.
 - Step 3** Upload the .tcb file to another Content Server. Files under 2 GB in size can be uploaded using the web interface. Use Windows Remote Desktop Connection to upload files that are larger than 2 GB.
 - Step 4** Import the recording. Uploaded .tcb files are listed on the **Import recordings** page. Importing unpacks the .tcb file and displays the recording in **View Recordings**.
-

Guidelines for copying

- You must be logged in as a site manager to export recordings.
- Recordings with pending outputs cannot be exported.
- Distribution outputs (for example, for Podcast Producer) and files stored on external streaming servers are not exported.
- Unicode characters in recording names are replaced with underscores when uploaded through the web interface. When a file with unicode characters in the recording name is placed directly in the Imports shortcut on the Content Server desktop using Remote Desktop, the **Import recordings** page does not display it.
- The maximum period of time allowed for a file to be uploaded through the web interface is 15 minutes. If the upload process is incomplete after 15 minutes (for example, because of poor network conditions), the upload fails.
- You cannot export or import when the Content Server is in Error mode. The Content Server mode is shown in the [Server Overview](#).
- An exported recording can be imported to a Content Server of the same or higher software version as the Content Server that the recording was exported from. To check the software version, go to **Diagnostics > Server overview**. The export/import functionality is available from software Release 5.3 and later.

Importing a recording

Site managers can import the .tcb file of a recording to a Content Server. The .tcb file contains the outputs served by the local Media server configurations (Local IIS Web Server and Local Windows Media Streaming Server) and the recording information and permissions.

The import functionality of the Content Server web interface checks the files inside the .tcb bundle, their structure, and the signature of the bundle. The Content Server rejects invalid or corrupted .tcb files. Files with incorrect extensions (an extension other than .tcb) that are uploaded through Remote Desktop to the Content Server Imports shortcut are not displayed on the [Import Recordings](#) page.

To import a file, do the following:

-
- Step 1** In the web interface, go to **Recordings> Import recordings**.
 - Step 2** Click **Upload file**.
 - Step 3** Browse to the .tcb file of the recording that you want to import.
 - Step 4** Click **Upload**. The **Automatically import recording after upload** box is checked by default. If you leave this setting checked, you do not need to manually import the file. If you uncheck this box, the recording file is uploaded and displayed on the **Import recordings** page with the state *Not imported*.

You must import the file by going to **Recordings > Import recordings**. Next to the recording, click **Import**. Unpacking might take some time. After the recording outputs have been unpacked and recording state has changed to *Imported*, the recording is displayed in **View Recordings**.

To import a file through Windows Remote Desktop, do the following:

-
- Step 1** Access the Content Server through Remote Desktop Connection on your PC.
 - Step 2** Copy the .tcb file to the Imports shortcut on the desktop. In the web interface, the recording is then displayed on the **Import recordings** page with the state *Not imported*.
 - Step 3** Go to **Recordings > Import recordings**. Next the recording, click **Import**.
-



Note Use this method if the file is larger than 2 GB or if the file is taking too long to upload through the web interface.

You can also delete an imported .tcb file by checking the box next to the recording and clicking **Delete selected**. Deleting the .tcb file does not affect the imported recordings in **View Recordings**.

Create Recording

From the **Recordings > Create recording** in the **Management** tab, site managers can create recordings.

To create a recording, do the following:

-
- Step 1** Go to **Recordings > Create recording**.
 - Step 2** Select a recording alias from the **Recording alias** drop-down list (see [Table 1-4](#)).
 - Step 3** Enter the number or address of the endpoint or system that the Content Server should call to make the recording. You can configure the settings in the Recording information and Recording permissions sections before, during, or after recording.
 - Step 4** Update **Advanced call settings** as needed (see [Table 1-4](#)).
 - Step 5** To join a password protected MCU conference, enter the PIN.
 - Step 6** Click the **Place call** button when you are ready to start recording from the endpoint or system. If the recording alias that you use to record has the five-second countdown timer enabled, the countdown is displayed on the endpoint or system before recording starts. Recording starts when a red dot and 'Recording' is displayed on the endpoint or system.



Tip If you do not see the message or recording poster that confirms the Content Server has joined a password protected MCU conference on an endpoint that has joined the call, hang up and try the call again, ensuring that you enter the correct PIN.

Step 7 Click the **End call** button when you are ready to stop recording.

Table 1-4 Recordings > Create Recording

Field	Field Description	Usage Guidelines
Create recording		
Recording alias	Select a recording alias for this recording.	<p>You might have a personal recording alias, or you might have been advised to use a system recording alias (for example, the Default OnDemand only alias).</p> <p>If others are permitted to watch while recording is in progress, select a recording alias that allows live streaming.</p> <p>Recordings that are made with aliases that do not permit non-live streaming can be watched only after their outputs have been transcoded. How long transcoding takes depends on the length of the recording and how many other recording outputs the Content Server is processing when the recording call ends.</p> <p>You can see whether outputs for your recording are in the queue to be processed by going to Diagnostics > Transcoding queue.</p> <p>Note <i>No live resources available</i> is displayed if the Content Server is already streaming the maximum number of live recordings. When you see this message, you can only select recording aliases without live streaming.</p>
Template outputs	The outputs that are produced with the selected recording alias.	<p>The Template outputs popup displays the outputs that the template selected for this recording alias produces. This popup includes the following:</p> <ul style="list-style-type: none"> • outputs that can be watched in a player—both live and on demand with their layout, format and size. • outputs to download for portable devices. • outputs to download for playback on a computer. • outputs that will be distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U. <p>If these are not the outputs that you want, select a different recording alias.</p>
Dial number	Enter the number or address of the endpoint that the Content Server should call to make the recording	<p>The number or address can be the following:</p> <ul style="list-style-type: none"> • an IP address. • an H.323 ID or E.164 alias, if the Content Server is registered with a gatekeeper. • a SIP URI, if the Content Server is registered with a SIP registrar.

Table 1-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
PIN for MCU conference	Enter the PIN for a password protected MCU conference.	The PIN must be numeric only.
Advanced Call Settings		Click the plus sign (+) to see advanced call settings.
Bandwidth (kbps)	Select a bandwidth from the drop-down list.	By default, the bandwidth is set to 768 kbps if 768 kbps is selected in the call configuration for the selected recording alias. You can change the setting to any of the speeds selected in the call configuration (see Call Configurations) used with the selected recording alias (see Recording Aliases).
Call type	Select a call type from the drop-down list.	If you are dialing an IP address, H.323 ID or E.164 alias, the Call type should be H.323. If you are dialing a SIP URI, the Call type should be SIP. SIP might not be an available option if SIP settings are not enabled in Site Settings .
Place call	When you click Place call , the Content Server calls the endpoint or system. If the five-second countdown timer is enabled, the countdown is displayed on the endpoint or system. Recording starts when a red dot and 'Recording' is displayed on the endpoint or system.	Click Place call after you have selected a recording alias and entered the dial number (address) of the endpoint.
Full Recording Information and Permissions		Click the plus sign (+) to see full recording information and permissions.
Recording information		
Name	The name of the recording to be displayed in the View Recordings pages.	The default name is the type of recording (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name to help users find the recording when they search. If you leave the name field blank, the default name is the name of the recording alias that you use to record.
Description	Details about the recording.	Optional. This optional setting can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.

Table 1-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
Keywords	Keywords that can be used to search for the recording. These keywords are not displayed to users.	Optional. This optional setting can help users find the recording when they search.
Category	Choose a category under which to list the recording in the View Recordings pages. To create a category, go to Recording setup > Categories .	Optional.
Recording permissions		
Who can view this recording	Groups and users who can view the recording. Click the Check access list button to validate your entries.	<p>You can give viewing access to one of the following:</p> <ul style="list-style-type: none"> • Allow access to all users, including guests: If Allow guest access is selected in Site Settings, this field is displayed. If selected, all users, including guests, can view the recording. • Allow access to all authenticated users: If the <i>Allow guest access</i> box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list or Place call adds all matching groups and users to the list. <p>Note After you click Check access lists or Place call, the users entered have the following formats:</p> <ul style="list-style-type: none"> – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, “CN=group.name, OU=staff, DC=company, DC=com”).</p>

Table 1-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
Automatically publish finished recording	If checked, the selected groups and users under Who can view this recording can view this recording. The groups and users in the editors list can always view and edit the recording.	This box is checked by default. When this box is unchecked, the recording does not appear in the View Recording pages. The recording still appears in the Edit recordings list. Next to the recording, the Publish recording button appears. When you click that button, all specified groups and users can view the recording.
Password (optional)	You can enter a password to restrict streaming access to this recording and the ability to download content. The password will be visible in clear text to editors of this recording and to site managers.	If a password is not entered, users who can view the recording in the View Recordings list can play the recording and download any available content. If a password is entered, users must know the password to stream or download the recording.

Table 1-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
Who can edit this recording	Groups and users can edit recording information and permissions, use the Content Editor (see) to change the recording, add more outputs to a completed recordings using the Manage Outputs page, and delete the recording. Use Check access list to validate your entries. They are also checked when you click Place call .	<p>Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon).</p> <ul style="list-style-type: none"> For local authentication mode: only enter groups and users that have been added to the Groups and Users list on the Content Server in this field; otherwise, the entry will be removed when you click Check access list, Place call, or Save. For Domain or LDAP authentication mode: <ul style="list-style-type: none"> With Guest Access disabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. With Guest Access enabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. If a creator adds a user or group to the access list that does not exist on the Content Server, a site administrator must add also that user or group to the Groups and Users. <p>If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list.</p> <p>Note After you click Check access lists, Place call, or Save, the users entered have the following formats:</p> <ul style="list-style-type: none"> Local authentication mode: MACHINENAME\user.name Domain authentication mode: DOMAINNAME (optional)\user.name LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, “CN=group.name, OU=staff, DC=company, DC=com”).</p>

Play recording on endpoints

This option only appears on a Content Server that is configured with a Premium Resolution option key.

Table 1-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
Make finished recording available for playing on endpoints	Check to make the finished recording available for playback on an endpoint.	Users can view this finished recording by dialing a playback H.323 ID or E.164 alias from an endpoint. After the site manager creates the recording, the Content Server generates the playback ID or alias, which is available from the Edit recording link for the recording. The site manager can give users the playback E.164 alias or the playback H.323 ID and instruct them to dial the alias or ID from an endpoint. Doing so will play back the recording.
PIN (optional)	You can enter a numeric PIN to restrict access to this recording.	PINs must be four digits long.

Recording Aliases

Recording aliases are used to record calls. They contain all information about how a recording is created.

The Content Server ships with default Recording aliases:

- Default Live and OnDemand: recordings that are created with this recording alias can be streamed while the call is in progress (Live). They can also be watched after the recording is complete and transcoded (OnDemand).
- Default OnDemand only: recording that are created with this recording alias can be watched after the recording is complete and transcoded (OnDemand only).

The recording alias determines the following:

- What to dial (for example, the H.323 ID, SIP URI) to record when using this recording alias.
- How the Content Server communicates with the endpoint or system while recording based on the specified call configuration (see [Call Configurations](#)).
- How recordings that are created with this recording alias are streamed or played back, and whether they can be played live (while recording is in progress) or only on demand. These options are specified in the template (see [Templates](#)).
- If the Content Server should send an email notification to specified users when a recording that uses the recording alias has been made.
- What recording information is copied to recordings that are created with this recording alias.
- Who has access to view or edit recordings that are created with this recording alias and whether the recordings have a password that must be entered before users can watch or download them.
- If the Content Server should make a recording that uses this recording alias available for playback on an endpoint.

For more information, see [Understanding Recording Aliases](#).

Recording information (such as the name, description, speaker, location, copyright and category), recording permissions, and outputs that are specified in the recording alias are automatically copied to a recording that is created using the recording alias. This information can be edited before the call is placed, during the call, or after the call has finished.

Only site managers can add new recording aliases. Site managers can see and edit all the properties of all recording aliases. They can also decide whether a recording alias is a system or personal recording alias. Creators who own a personal recording alias can only see and edit selected properties.

In the site manager role, you can display the recording aliases list by going to **Recording setup > Recording aliases**. From the list, you can the following:

- Edit an existing recording alias—click **Edit** for the category that you want to change.
- Delete recording aliases—check the box next to a recording alias. Then click **Delete selected**.
- Add recording alias—click **Add recording alias**.

Adding or Editing Recording Aliases

Site managers can add and edit recording aliases.



Note

For Content Servers that are registered to a H.323 gatekeeper as gateway, a personal recording alias can be automatically created for each user with creator privileges when the user logs in to the Content Server web interface (see [Site Settings](#) and [Creating Automatic Personal Recording Aliases](#)).

To add a new recording alias, do the following:

-
- Step 1** Go to **Recording setup > Recording aliases**.
 - Step 2** Click **Add recording alias**.
 - Step 3** Enter settings in the configuration fields (see [Table 1-5](#)).
 - Step 4** Click **Save**.
-

To edit settings for an existing recording alias, do the following:

-
- Step 1** Go to **Recording setup > Recording aliases**.



Note

Creators can display a list of their editable aliases from the **My Recordings** tab by clicking **Create recording options**.

-
- Step 2** Click **Edit** for the alias that you want to edit.
 - Step 3** Edit settings in the configuration fields as needed (see [Table 1-5](#)).
 - Step 4** Click **Save**.
-

Table 1-5 Recording Setup > Recording Aliases: Add Recording Alias or Edit

Field	Field Description	Usage Guidelines
Recording alias		
Name	The name of the recording alias.	—
Recording alias type	The type of recording alias. Click Personal or System .	<p>Personal recording aliases can be used and edited by their owners. Owners of a personal recording alias cannot change the recording alias type, owner, dialing properties or call configuration.</p> <p>System recording aliases can be used by creators, but can only be edited by site managers. Recordings created with a system recording alias are automatically made available when the recording has finished.</p>
Personal recording alias owner	For personal recording aliases, choose the owner from the drop-down list. The list displays users and groups whose role is either site manager or creator.	<p>The owner automatically becomes an editor of any recording created using the recording alias. The owner can also edit some properties of the recording alias.</p> <p>The owner of all system recording aliases is the local administrator. You cannot change the owner for system recording aliases. For information about roles, see Groups and Users.</p>
Dialing properties		
H.323 ID	The unique H.323 ID to be dialed to record when using this recording alias.	<p>The Content Server must be registered with a gatekeeper to use an H.323 ID (this field is displayed only if a gatekeeper is enabled in Site Settings). If the Content Server is registered to the gatekeeper as a gateway, this H.323 ID must be prefixed by the H.323 gateway prefix that is specified in Site Settings when dialing.</p> <p>Because only site managers can see the site settings page, the prefix is displayed in this field before the H.323 ID so that the owners can see the complete string to dial.</p>
E.164 alias	The E.164 alias to be dialed when using this recording alias.	<p>The Content Server must be registered with a gatekeeper to use an E.164 alias (this field is displayed only if a gatekeeper is enabled in Site Settings). If the Content Server is registered to the gatekeeper as a gateway, this E.164 alias must be prefixed by the E.164 gateway prefix that is specified in Site Settings when dialing.</p> <p>Because only site managers can see the Site settings page, the prefix is displayed in this field before the E.164 alias so that owners can see the complete string to dial.</p>
SIP address (URI)	The SIP address (URI) to be dialed when using this recording alias.	The Content Server must be registered with a SIP registrar to use a SIP URI. This field is displayed only if a SIP registrar is enabled in Site Settings .
SIP display name	A display name for this recording alias.	The SIP display name is presented as a description of the SIP URI to other systems.

Table 1-5 Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)

Field	Field Description	Usage Guidelines
Recording settings		
Template	Choose a template to use with this recording alias.	Site managers can add or edit templates (click Add or Edit). The recording alias owners cannot add or edit templates, but they can choose a different one to use from the drop-down list.
Template outputs	The outputs that are associated with this template.	—
Call configuration	Choose the call configuration to use with this recording alias.	Site managers can add or edit call configurations (click Add or Edit).
Show countdown before recording	Check the box to show a five-second countdown on the endpoint before recording starts. The countdown provides time for the speaker to prepare before recording begins.	The recording alias owner can enable or disable the countdown.
Send email when recording finishes	Check the box to send an email containing a link to the recording after the recording is created.	The box for this setting must be checked and an SMTP server must be configured in Configuration > Site Settings for an email to be sent. The recording alias owner can change this field.
To email address	The email address to which emails are sent if the Send email when recording finishes box is checked.	You can test the email address by clicking the Send test email button. The recording alias owner can change this field.
Default recording information		
Name	The name of the recording to be displayed in the View Recordings pages.	The default name is the type of recording (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name to help users find the recording when they search. If you leave the name field blank, the default name is the name of the recording alias that you use to record.
Description	Details about the recording.	Optional. This optional setting can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.
Keywords	Keywords that can be used to search for the recording. Keywords do not appear in the interface.	Optional. This optional setting can help users find the recording when they search.

Table 1-5 Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)

Field	Field Description	Usage Guidelines
Category (see Categories for more information)	Choose a category under which to list the recording in the View Recordings pages.	Optional.
Default recording permissions		
Who can view this recording	Groups and users who can view the recording. Click the Check access list button to validate your entries. Entries are also validated when you click the Save button.	<p>You can give viewing access to one of the following:</p> <ul style="list-style-type: none"> • Allow access to all users, including guests: If Allow guest access is selected in Site Settings, this field is displayed. If selected, all users, including guests, can view the recording. • Allow access to all authenticated users: If the <i>Allow guest access</i> box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list. <p>Note After you click Check access lists, Place call, or Save the users entered have the following formats:</p> <ul style="list-style-type: none"> – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, “CN=group.name, OU=staff, DC=company, DC=com”).</p>

Table 1-5 *Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)*

Field	Field Description	Usage Guidelines
Automatically publish finished recordings	If checked, the selected groups and users under Who can view this recording can view recordings. The groups and users in the editors list can always view and edit the recordings.	This box is checked by default. When this box is unchecked, recordings do not appear in the View Recording pages. Recordings still appear in the Edit recordings list. Next to recordings, the Publish recording button appears. When you click that button, all specified groups and users can view the recording.
Password (optional)	You can enter a password to restrict streaming access to this recording and the ability to download content. The password will be visible in clear text to editors of this recording and to site managers.	If a password is not entered, users who can view the recording in the View Recordings list can play the recording and download any available content. If a password is entered, users must know the password to stream or download the recording.

Table 1-5 Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)

Field	Field Description	Usage Guidelines
Who can edit this recording	Groups and users can edit recording information and permissions, use the Content Editor (see) to change the recording, add more outputs_ to a completed recordings using the Manage Outputs page, and delete the recording. Use Check access list to validate your entries. They are also checked when you click Place call or Save .	<p>Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon).</p> <ul style="list-style-type: none"> For local authentication mode: only enter groups and users that have been added to the Groups and Users list on the Content Server in this field; otherwise, the entry will be removed when you click Check access list, Place call, or Save. For Domain or LDAP authentication mode: <ul style="list-style-type: none"> With Guest Access disabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. With Guest Access enabled: enter groups and users that have been added to Active Directory for the LDAP server configured for the Content Server. Otherwise, the entry will be removed when you click Check access list, Place call, or Save. If a creator adds a user or group to the access list that does not exist on the Content Server, a site administrator must add also that user or group to the Groups and Users. <p>If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list.</p> <p>Note After you click Check access lists, Place call, or Save, the users entered have the following formats:</p> <ul style="list-style-type: none"> Local authentication mode: MACHINENAME\user.name Domain authentication mode: DOMAINNAME (optional)\user.name LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, "CN=group.name, OU=staff, DC=company, DC=com").</p>

Table 1-5 *Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)*

Field	Field Description	Usage Guidelines
Play recording on endpoints		
This option only appears on a Content Server that is configured with a Premium Resolution option key.		
Make finished recording available for playing on endpoints	Check to make the recording available for playback on an endpoint.	Users can view finished recordings made with this recording alias by dialing a playback H.323 ID or E.164 alias from an endpoint. After the recording has been created, the Content Server generates the playback ID or alias, which is available from the Edit recording link for the recording. The site manager or an editor can give users the playback E.164 alias or the playback H.323 ID and instruct them to dial the alias or ID from an endpoint. Doing so will play back the recording.
PIN (optional)	You can enter a numeric PIN to restrict access to all new recordings created with your personal recording alias.	PINs must be four digits long. Tip To restrict access to a single recording, enter a PIN in the Play recording on endpoints section of the Edit recording page (see Edit Recording).

Categories

You can assign your recordings to a category to make finding them easier in View Recordings.

Six categories come with the Content Server: Announcements, Education, General, Meetings, News, and Training. Each category must have a name and can have a description.

In the site manager role, you can display the categories list by going to **Recording setup > Categories**. From the categories list, you can the following:

- Edit existing categories—click **Edit** for the category that you want to change.
- Delete categories—click the box next to a category. Then click **Delete selected**. If you delete a category that a recording or recording alias uses, the recording or recording alias will not have a category.
- Add new categories—click **Add category**. There is no limit to the number of categories that can be added.



Note

In the **View Recordings** pages, guests (unauthenticated users) and users with the viewer or creator role who have logged in only see a category in the **All categories** section at the bottom of the page if there is a recording in that category that they have permission to see. The number of recordings in each category is displayed in parentheses. All categories are displayed for site managers.

Adding and Editing Categories

Site managers can add and edit categories.

To add a new category, do the following:

-
- | | |
|---------------|--|
| Step 1 | Go to Recording setup > Categories . |
| Step 2 | Click Add category . |
| Step 3 | Enter a <i>Name</i> and, if desired, a <i>Description</i> . Descriptions are optional and are displayed on the View Recordings page. |
| Step 4 | Click Save . |
-

To edit settings for an existing category, do the following:

-
- | | |
|---------------|---|
| Step 1 | Go to Recording setup > Categories . |
| Step 2 | Click Edit for the category that you want to update. |
| Step 3 | Update the <i>Name</i> , the <i>Description</i> , or both. |
| Step 4 | Click Save . |
-

Templates

You can assign a template to a recording alias. Templates determine how a recording is streamed and played back:

- Formats supported—for example, Windows Media, MPEG-4 for QuickTime, and MPEG-4 for Flash.
- The sizes for the outputs.
- Outputs for playback in portable devices (iPod or Zune).
- Outputs for uploading to your Media Experience Engine 3500 server, Show and Share server, iTunes U account or Podcast Producer server.
- Outputs for downloading to your computer.

The Content Server ships with several pre-defined templates in the templates list. Site managers can create new templates.

A template can be updated; modified and saved as a new template; or deleted if it not being used in a recording alias. If a template is used in a recording alias, its check box is dimmed so that you cannot delete it.

When deciding whether to edit an existing template to use as the basis for a new one or to start a completely new template, examine how close the settings you require are to those in an existing template.

In the site manager role, you can display the templates list by going to **Recording setup > Templates**. From the list, you can the following:

- Edit existing templates—click **Edit** for the template that you want to change.



Note Edits that you make to templates are not used in current calls but only for new calls.

- Delete templates—click the box next to a template. Then click **Delete selected**. If the check box next to the template is dimmed, you cannot delete the template because it is used in a recording alias.
- Add new templates—click **Add template**.

Adding or Editing Templates

Site managers can add and edit templates.

To add a new recording alias, do the following:

-
- Step 1** Go to **Recording setup > Templates**.
 - Step 2** Click **Add template**.
 - Step 3** Enter settings in the configuration fields (see [Table 1-6](#)).
 - Step 4** Click **Save**.
-

To edit settings for an existing template, do the following:

-
- Step 1** Go to **Recording setup > Templates**.
 - Step 2** Click **Edit** for the template that you want to edit.
 - Step 3** Edit settings in the configuration fields as needed (see [Table 1-6](#)).
 - Step 4** Click **Save**.
-

Table 1-6 *Recording Setup > Templates: Add or Edit Template*

Field	Field Description	Usage Guidelines
Template		
Name	The name of the template.	Use a meaningful name to help users select a template for their personal recording alias. The name does not need to detail the outputs that the template creates because this information is displayed when users choose a template for a recording alias (see Recording Aliases) and when users choose a recording alias to use when calling out to record.

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Viewable in the Content Server web interface	If you check this box, go to the Outputs to view in the Content Server web interface to select output settings for a player.	—
Downloadable for portable devices (iPod and Zune)	If you check this box, go to the Outputs to download for portable devices to select output settings for a player.	—
Downloadable for general purpose	If you check this box, go to the Outputs to download for general purpose to select output settings for a player.	There is a limitation of 55 characters for UTF-8 (or 18 characters for UTF-16) for the length of the title of a recording when downloaded. We recommend using less than 55 characters in the title or renaming the downloaded recording.
Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U	If you check this box, go to the Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U to select output settings for a player.	—

Outputs to view in the Content Server web interface

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Output layout	Click the layout to use.	<p>The main video and presentation streams are composited into a single video stream. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
On Demand Formats	Choose up to three formats: <ul style="list-style-type: none"> • Windows Media for playback using the Silverlight player or Windows Media player on a PC or the Silverlight player on a Mac. • MPEG-4 for playback using QuickTime. • MPEG-4 for playback using Flash player. 	<p>These formats can be viewed on a PC as long as the correct plugins have been downloaded and installed.</p> <p>MPEG-4 for QuickTime, MPEG-4 for Flash, and Windows Media (played using Silverlight) are available for Apple Mac when the correct plugins have been downloaded and installed.</p>

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
On demand sizes	Choose up to two recording sizes based on your user streaming environment and internet connection.	<ul style="list-style-type: none"> • Audio only: For use when users have very poor quality internet access. • Small: The target bit rate for small outputs is 250 kbps. The target rate is displayed in the Bit rates field. • Medium: For use with broadband access. The target bit rate for medium outputs is 800 kbps. The target rate is displayed in the Bit rates field. • Large: For use with a high-speed LAN. This format takes the longest to transcode. The target rate is the maximum rate.
Maximum target bit rates (kbps)	Displays the target bit rate for the small, medium and large output sizes. The number that is displayed depends on the target bit rates set in Site Settings and the call speed at which the recording was created.	You can configure these bit rates in the Advanced streaming options section of Site Settings .
On demand Media server configuration settings	<p>Choose the Media Server Configurations for on-demand viewing of the recordings that are created with this template. Formats not selected above are dimmed.</p> <p>Click the Optimize for Motion check box to enable.</p>	<p>The media servers configurations that are shown in the drop-down lists by default are those selected in the system defaults section of Site Settings.</p> <p>The Optimize for motion check box improves the quality of high-motion recordings.</p>
Live stream	Click to allow the recording to be streamed while it is in progress.	<p>Choose the Format and Size. Only one live stream is available per recording. The other formats and sizes that you chose above are transcoded after the recording has finished.</p> <p>Check Re-transcode realtime movies to have the live transcoded movies transcoded again after the recording has completed. Checking this option can result in better quality viewing but also creates an additional processing load on the Content Server. If Re-transcode realtime movies is not checked and play back of the recording on demand is not satisfactory, the live transcoded movies can be re-transcoded from the Summary section of the Manage Outputs page.</p> <p>For Live Media server configuration settings, choose the media server configuration to use for live streaming. If none are configured, you see this message: Your movie(s) will not be broadcast live until you have a live enabled Media server configuration set up.</p>

Table 1-6 *Recording Setup > Templates: Add or Edit Template (continued)*

Field	Field Description	Usage Guidelines
Output layout	Click the layout to use.	<p>The main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Portable devices	<p>Select portable device(s) and whether you want audio and video or audio only:</p> <ul style="list-style-type: none"> • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible) 	<p>After the Content Server transcodes the recording, these outputs are available for download from the View Recordings page. Click the Download tab for the recording. Then click the output file that you want to download for synchronization with your portable device.</p> <p>iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.</p>
Outputs to download for general purpose		

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Output layout	Click the layout to use.	<p>The main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Formats	Select up to three formats.	—
Sizes	Select up to two sizes.	<p>Because these outputs are downloaded and viewed on a computer, the quality of the Internet connection is not an issue, except as the connection affects the time it takes to download. After downloading, users can watch the recordings without being connected to the Internet.</p> <p>Note If the download time exceeds 20 minutes, the download will fail.</p>

Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U

When you use this option, recordings from the Content Server can be automatically uploaded to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U. Users then view recordings from the web interface of those products, not from the Content Server web interface. With this option, the Content Server is a recording device; users interact with the recording (view and edit) in the web portal of the other system. If a recording on a Content Server has no other outputs except ones distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U, there is nothing for users to view on the Content Server itself.

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Output layout	Click the layout to use.	<p>The main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Media Experience Engine 3500	Select this option and a media server configuration (see Media Server Configurations) for Media Experience Engine 3500 to automate the process of uploading recorded content to your Media Experience Engine 3500 server.	The size of the output for Media Experience Engine 3500 is always large and always MPEG-4 format.
Show and Share	Select this option and a media server configuration (see Media Server Configurations) for Show and Share to automate the process of uploading recorded content to your Show and Share server.	Choose the size (Small , Medium or Large) of the output to upload to Show and Share.
Podcast Producer	Select this option and a media server configuration (see Media Server Configurations) for Podcast Producer to automate the process of uploading recorded content to your Podcast Producer server.	The size of the output for Podcast Producer is always large.
iTunes U	Select this option and a media server configuration (see Media Server Configurations) for iTunes U to automate the process of uploading recorded content to an iTunes U account.	Choose the size (Small , Medium or Large) of the output to upload to iTunes U. You can also specify an additional audio-only output.

Summary

Table 1-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Outputs to view in the Content Server web interface	Displays information about the outputs created for viewing in the Content Server web interface. This summary includes information about on-demand and live streaming settings for the template.	The information displayed in the summary is the following: <ul style="list-style-type: none"> • Format • Size • Server configuration setting
Outputs to download for portable devices	Displays information about the outputs created for Portable Devices.	The information displayed in the summary is the following: <ul style="list-style-type: none"> • Device type • Device output (audio or video)
Outputs to download for general purpose	Displays information about the outputs created for download to users' computers.	The information displayed in the summary is the following: <ul style="list-style-type: none"> • Format • Size
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U	Displays information about the outputs created for use with Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U.	The information displayed in the summary is the following: <ul style="list-style-type: none"> • Format • Size • Server configuration setting

Media Server Configurations

Media server configurations tell the Content Server where the media for a recording is stored and how it is streamed. Media server configurations can also be used to automate the following processes:

- Uploading recorded content to Media Experience Engine 3500 server for completion and publishing
- Uploading to Cisco Show and Share for distribution
- Uploading recorded content to Apple's Podcast Producer server for completion and publishing using a Podcast Producer workflow
- Uploading to Apple's iTunes U for distribution

Streaming is specified by the two preconfigured media server configurations that cannot be deleted:

- Local Windows Media Streaming Server: can be used for streaming Windows Media live and on demand.
- Local IIS Web Server: can be used to deliver MPEG-4 for QuickTime and MPEG-4 for Flash for on-demand playback as a progressive download (HTTP or pseudo-streaming). It also delivers still images, if available, for content that was generated in software versions before 5.0.

See [Table 1-7](#) for the supported Content Server local media server streaming configurations.

Table 1-7 Local Windows Media Server and IIS Media Server Configurations

Content Server Internal Media Server	Supported Streaming
Windows Media Streaming Server	
Live unicast streaming	Yes
Live multicast streaming	No—Live multicast streaming requires an external Windows Media server. Note: The Support live multicast streaming check box is not supported in Content Server Release 6.x.
On-demand streaming	Yes
IIS Web Server MPEG-4 for QuickTime	
Live unicast streaming	No—Live unicast streaming requires an external QuickTime or Darwin server.
Live multicast streaming	Yes
On-demand streaming	Yes—HTTP-based streaming. RTSP on-demand streaming requires an external QuickTime or Darwin server.
IIS Web Server MPEG-4 for Flash	
Live unicast streaming	No—Live unicast streaming requires an external Wowza server.
On-demand streaming	Yes

Site managers set up the streaming server, and then add a Media server configuration to the Content Server that specifies how the media is streamed. The Media server configurations can then be selected in a template (see [Templates](#)) or when creating outputs by using the [Manage Outputs](#) page. If the Media server configuration is used often, it can be set as a default in **Configuration > Site settings** so that it will appear at the top of media server configurations lists in the **Recording setup > Templates** and **Manage outputs** pages.

To display the list of media server configurations, go to **Recording setup > Media server configurations**. From the list, site managers can do the following:

- Edit the Media server configurations by clicking **Edit** for the appropriate entry. See [Adding or Editing Media Server Configurations](#).
- Delete a Media server configuration that was added previously: select the entry and click **Delete selected**. Note that you cannot delete a Media server configuration that is used by a Template or recording's [Manage Outputs](#) page.
- Add new Media server configurations. Click the appropriate link for the type of server and see [Adding or Editing Media Server Configurations](#).

Adding or Editing Media Server Configurations

To create a new media server configuration, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click the link for the type of server that you want to add.

- Step 3** Enter settings in the configuration fields.
- Step 4** Click **Save**.

Alternatively, you can go to **Recording setup > Media server configurations**. Click **Edit** for the media server configuration that is to be the basis of the new one. Update the fields as required using the table in the appropriate section below and click **Save as**.

To edit settings for an existing media server configuration, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click **Edit** for the configuration that you want to edit.
- Step 3** Edit settings in the configuration fields as needed.
- Step 4** Click **Save**.
-

**Note**

If you have existing recordings that use a media server configuration and you edit that media server configuration, you can also update the streaming URLs for the outputs that are viewable in the Content Server web interface. For example, if the server address of an external streaming server has changed, update the address in the media server configuration. Recordings that use that Media server configuration will still be playable.

For more information about configuring external media servers, see the Configuring Media Servers with Cisco TelePresence Content Server documents on Cisco.com:

<http://www.cisco.com/c/en/us/support/conferencing/telepresence-content-server/products-installation-and-configuration-guides-list.html>

Windows Media Streaming Server

Only Windows Media streaming servers are supported for streaming Windows Media content.

Saving the media server configuration checks that the server is available at the specified server address and displays the server type if that information is available.

You can configure the Content Server to use either its local internal, or an external Windows Media server to provide live and/or on-demand streams with these limitations:

- Only viewers with Windows computers can view live Windows Media streams.
- The local internal Windows Media server can output only a unicast live and/or on-demand stream to Windows-based players.
- For live multicast streaming, you need an external Windows Media server. With an external Windows Media server, the Content Server sends a live unicast stream to the server which then streams multicast. For more information, see *Configuring the Cisco TelePresence Content Server Release 6.x to Use an External Windows Media Streaming Server* on Cisco.com.

**Note**

Although visible in the **Recording setup > Media server configuration > Windows media streaming server** window, the **Support live multicast streaming** check box is not supported in Content Server Release 6.x.

- An external Windows Media server can output live unicast, multicast, and on-demand streams to Windows-based players.

To configure a Windows Media streaming server, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click **Add Windows Media streaming server configuration**.
- Step 3** Under Server settings, check the **Support live unicast streaming** or the **Support on demand** box. When you check a box, configuration settings appear. Enter settings in the fields (see [Table 1-8](#)).
- Step 4** Click **Save**.
-

Table 1-8 *Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration*

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Support live unicast streaming	Whether the server is to support live unicast streaming.	If checked, enter the server address . Unicast connections are one-to-one connections between each client and the server. Each unicast client that connects to the server takes up additional bandwidth.
Support live multicast streaming	The Support live multicast streaming check box is not supported in Content Server Release 6.x.	—
Support on demand	Whether the server is to support on-demand streaming.	If checked, enter the server address .
Server address	The IP address, DNS name of the server.	—
Live unicast streaming settings		
User name	The username to authenticate to the streaming server.	—
Password/Password confirm	The password to authenticate to the streaming server.	—
Server push	Click to push the live stream to the streaming server.	If selected, complete the other fields in this section.
Port	The HTTP port of the streaming server. If you are using the Content Server's Windows Media streaming server, the port is 8080.	—

Table 1-8 *Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration (continued)*

Field	Field Description	Usage Guidelines
Publishing point: Create new	Click to have the Content Server create a new publishing point on the streaming server.	A publishing point is the way that media are distributed from the Windows Media streaming server.
Publishing point: Create new using setting from existing Publishing point name	Click to have the Content Server create a new publishing point on the streaming server by using the settings from an existing publishing point. Enter the name of the existing publishing point.	—
Publishing point: Use existing Publishing point name	Click to use an existing publishing point on the streaming server. Enter the name of the existing publishing point.	—
Network pull Port	Click to have the streaming server request the stream from the Content Server. A network publishing point must be created on the Window Media streaming server to use this functionality. Enter the port number for the network pull.	The ports used by the Content Server are listed in Port Information .
Use default live URL	Click to use the live URL that is generated by the Content Server.	—
Use alternate live URL	Click to supply your own URL for live streaming. Choose whether you want the filename (in this case, the publishing point name) to be appended to the alternate URL.	Enter an alternate URL if you have selected network pull. You might also want to use an alternate URL in other situations.
On demand settings		
Write movies to the default media location	Click to have media written to the Content Server's default media location. This location is either the E drive of the Content Server or an alternate storage location if you have a NAS configured.	Do not select this option if you are streaming from an external streaming server. You can verify the default media storage location in the Server Overview . The default media location for Windows Media files is (media location)\data\media.
Write movies to an alternate location	Click to write media to an external streaming server that uses a shared drive or UNC path.	Select this option if the streaming server is on an external server with a shared drive that is accessible to the Content Server. Enter the shared drive or UNC path (for example, \\servername\shared) in the Alternate path field.

Table 1-8 Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration (continued)

Field	Field Description	Usage Guidelines
FTP movies to location	Click to use FTP to transfer media files to an external streaming server.	Select this option if the streaming server is on, or can access a shared drive on, an external server that is running an FTP service. If you select this option, complete the other fields in this section. Then check the FTP upload functionality by clicking Test FTP . FTP upload is also tested every time you save the media server configuration.
Server address	The IP address or DNS name of the FTP server.	—
Port	The port number of the FTP service. Most FTP servers use port 21.	—
Directory	The directory relative to the root FTP directory on the FTP server. The directory should be specified using forward slashes (for example, /movies/).	If left blank, files are uploaded to the root FTP directory.
User name	The username to authenticate to the FTP server.	—
Password/Password confirm	The password to authenticate to the FTP server.	—
Use default on demand URLs	Click to use on-demand URLs that are generated by the Content Server.	—
Use alternate on demand URLs	Click to supply your own URLs for on-demand streaming (if your on-demand URLs require different paths or filenames from those that the Content Server generates). Enter the URLs for the Main and Dual video streams and select if you want the filename to be appended to the alternate URLs.	—

QuickTime or Darwin Streaming Server

The Content Server default installation supports only HTTP-based on-demand streaming of MPEG-4 for QuickTime from its local IIS web server and live multicast MPEG-4 for QuickTime directly onto the network. An external QuickTime or Darwin streaming server must be set up for live unicast and true (RTSP) on-demand streaming of MPEG-4 for QuickTime. Only QuickTime and Darwin streaming servers are supported for live unicast and on-demand streaming.

Saving the media server configuration checks that the server is available at the specified server address and displays the server type if that information is available. Unicast live streaming from QuickTime or Darwin servers (RTSP announce) is also tested when you save the media server configuration.

You can set up a media server configuration for a QuickTime or Darwin streaming server to do live streaming, on-demand streaming, or both. You have two options for configuring the media server for live MPEG-4 for QuickTime streaming:

- **Live unicast streaming:** This option requires an external QuickTime or Darwin streaming server to relay streams to clients.
- **Live multicast streaming:** This option does not require an external QuickTime or Darwin streaming server to relay streams to clients. In a multicast delivery, the server sends only one stream to the multicast IP which reaches all player clients simultaneously.

To configure a Quicktime or Darwin streaming server, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click **Add Quicktime or Darwin streaming server configuration**.
- Step 3** Under Server settings, check the **Support live unicast streaming**, the **Support live multicast streaming**, or the **Support on demand** box. When you check a box, configuration settings appear. Enter settings in the fields (see [Table 1-9](#)).
- Step 4** Click **Save**.
-

Table 1-9 *Recording Setup > QuickTime or Darwin Streaming Server Configuration*

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Support live unicast streaming	Whether the server is to support live unicast streaming.	If checked, enter the server address . Unicast connections are one-to-one connections between each client and the server. Each unicast client that connects to the server takes up additional bandwidth.
Support live multicast streaming	Whether the server is to support live multicast streaming.	In multicast delivery, the server sends only one stream which reaches all player clients simultaneously. There is no additional overhead for the server regardless of whether one or more clients are connected. Multicast delivery is generally used for broadcasting live streams on a corporate network and only works if all routers on the network are multicast enabled.
Support on demand	Whether the server is to support on-demand streaming.	If checked, enter the server address .
Server address	The IP address or DNS name of the server.	—

Table 1-9 Recording Setup > QuickTime or Darwin Streaming Server Configuration (continued)

Field	Field Description	Usage Guidelines
Live unicast streaming settings		
Streaming port range start	The port number for the start of the streaming port range (for example, 30000). The start port must be an even number. The Content Server uses the streaming start port plus 30 for streaming live calls (for example, from 30000 to 30030). Ensure that you select ports that are not being used by the Content Server.	The ports that the Content Server uses are listed in Port Information .
User name	The username to authenticate to the streaming server.	—
Password/Password confirm	The password to authenticate to the streaming server.	—
Use default live URL	Click to use a live URL that is generated by the Content Server.	—
Use alternate live URL	Click to supply your own URL for live streaming. Choose whether you want the filename (in this case, the sdp filename) to be appended to the alternate URL.	The Content Server automatically generates a Session Description Protocol (sdp) file. The QuickTime or Darwin streaming server uses this file to know how to stream the media.
Live multicast streaming settings		
Multicast IP address	The destination multicast IP address that the Content Server streams to. Your chosen multicast IP address must not conflict with any other multicast address in use in your network. Further considerations apply if you want to multicast over the public Internet. Contact your network administrator for more information.	—
Streaming port range start	The first port number in the live streaming port range. The setting is between 10000 and 65000. This port number must be even.	—

Table 1-9 Recording Setup > QuickTime or Darwin Streaming Server Configuration (continued)

Field	Field Description	Usage Guidelines
TTL	The multicast time to live (TTL) threshold.	<p>This value tells the network how far multicast packets should be allowed to travel across the network. The default threshold is LAN (TTL=32). The value “Subnet” (TTL=1) means that packets do not pass the first network router and should mean a multicast stream is viewable on any network, even those not enabled for multicast, where the client is on the same subnet as the Content Server.</p> <p>The efficacy of higher values—LAN (TTL=32), WAN (64), Internet (128), Unrestricted (255)—depends on the network configuration.</p>
On demand settings		
Write movies to the default media location	Click to have media written to the Content Server’s default media location. This location is either the E drive of the Content Server or an alternate storage location if you have a NAS configured.	<p>Do not select this option if you are streaming from an external streaming server.</p> <p>You can verify the default media storage location in the Server Overview. The default media location for MPEG-4 for QuickTime files is (media location)\data\www.</p>
Write movies to an alternate location	Click to write media to an external streaming server that uses a shared drive or UNC path.	Select this option if the streaming server is on an external server with a shared drive that is accessible to the Content Server. Enter the shared drive or UNC path (for example, \\servername\shared) in the Alternate path field.
FTP movies to location	Click to use FTP to transfer media files to an external streaming server after the recording session has ended.	<p>Select this option if the streaming server is on, or can access a shared drive on, an external server that is running an FTP service.</p> <p>If you select this option, complete the other fields in this section. Then check the FTP upload functionality by clicking Test FTP. FTP upload is also tested every time you save the media server configuration.</p>
Server address	The IP address or DNS name of the FTP server.	—
Port	The port number of the FTP service. Most FTP servers use port 21.	—
Directory	The directory relative to the root FTP directory on the FTP server. The directory should be specified using forward slashes (for example, /movies/).	If left blank, files are uploaded to the root FTP directory.
User name	The username to authenticate to the FTP server.	—
Password/Password confirm	The password to authenticate to the FTP server.	—

Table 1-9 Recording Setup > QuickTime or Darwin Streaming Server Configuration (continued)

Field	Field Description	Usage Guidelines
Use default on demand URLs	Click to use on-demand URLs that are generated by the Content Server.	—
Use alternate on demand URLs	Click to supply your own URLs for on-demand streaming (if your on-demand URLs require different paths or filenames from those that the Content Server generates). Enter the URLs for the Main and Dual video streams and select if you want the filename to be appended to the alternate URLs.	—

Wowza Media Server for Flash

The Content Server default installation supports the playing of MPEG-4 for Flash media on demand—only via HTTP progressive download from the built-in IIS web server. An external media server must be set up for live unicast and true (RTMP) on-demand streaming of MPEG-4 for Flash.

Saving the media server configuration checks that the server is available at the specified server address and displays the server type if that information is available. Unicast live streaming from the Wowza Media Server for Flash (RTSP announce) is also tested when you save the media server configuration.

You can set up a media server configuration for a Wowza Media Server for Flash to do live streaming, on-demand streaming, or both.

To configure a Wowza Media Server for Flash, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
 - Step 2** Click **Add Wowza Media Server for Flash configuration**.
 - Step 3** Under Server settings, check the **Support live unicast streaming** or the **Support on demand**. When you check a box, configuration settings appear. Enter settings in the fields (see [Table 1-10](#)).
 - Step 4** Click **Save**.
-

Table 1-10 Recording Setup > Wowza Media Server for Flash Configuration

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Server address	The IP address or DNS name of the server.	—

Table 1-10 Recording Setup > Wowza Media Server for Flash Configuration (continued)

Field	Field Description	Usage Guidelines
Support live unicast streaming	Whether the server is to support live unicast streaming.	Unicast connections are one-to-one connections between each client and the server. Each unicast client that connects to the server takes up additional bandwidth.
Support on demand	Whether the server is to support on-demand streaming.	—
Live unicast streaming settings		
Streaming port range start	The port number for the start of the streaming port range (for example, 30000). The start port must be an even number. The Content Server uses the streaming start port plus 30 for streaming live calls (for example, from 30000 to 30030). Ensure that you select ports that are not being used by the Content Server.	The ports that the Content Server uses are listed in Port Information .
User name	The username to authenticate to the streaming server.	—
Password/Password confirm	The password to authenticate to the streaming server.	—
Use default live URL	Click to use the live URL that is generated by the Content Server.	If you select this option, enter a directory in Application directory .
Application directory	The name of the directory that was created in applications on the Wowza Media Server to stream live. This directory is used in the default live URL.	If you followed Cisco recommendations when you set up the Wowza Media Server, this directory is called “live.”
Use static URL (optional)	—	If you want to publish a live URL before streaming begins, use this option.
Static stream name	A descriptive name for the static stream.	—
Static URL	The static URL for the specified stream name.	A static URL is constructed from the media server address, application directory, and static stream name (required).
Use alternate live URL	Click to supply your own URL for live streaming. Choose whether you want the filename to be appended to the alternate URL.	—

Table 1-10 Recording Setup > Wowza Media Server for Flash Configuration (continued)

Field	Field Description	Usage Guidelines
On demand settings		
Write movies to the default media location	Click to have media written to the Content Server's default media location. This location is either the E drive of the Content Server or an alternate storage location if you have a NAS configured.	Do not select this option if you are streaming from an external streaming server. You can verify the default media storage location in the Server Overview . The default media location for MPEG-4 for Flash files is (media location)\data\www
Write movies to an alternate location	Click to write media to an external streaming server that uses a shared drive or UNC path.	Select this option if the streaming server is on an external server with a shared drive that is accessible to the Content Server. Enter the shared drive or UNC path (for example, \\servername\shared) in the Alternate path field.
FTP movies to location	Click to use FTP to transfer media files to an external streaming server after the recording session has ended.	Select this option if the streaming server is on, or can access a shared drive on, an external server that is running an FTP service. If you select this option, complete the other fields in this section. Then check the FTP upload functionality by clicking Test FTP . FTP upload is also tested every time you save the media server configuration.
Server address	The IP address or DNS name of the FTP server.	—
Port	The port number of the FTP service. Most FTP servers use port 21.	—
Directory	The directory relative to the root FTP directory on the FTP server. The directory should be specified using forward slashes (for example, /movies/).	If left blank, files are uploaded to the root FTP directory.
User name	The username to authenticate to the FTP server.	—
Password/Password confirm	The password to authenticate to the FTP server.	—
Use default on demand URLs	Click to use on-demand URLs that are generated by the Content Server.	If you select this option, enter a directory in Application directory .

Table 1-10 Recording Setup > Wowza Media Server for Flash Configuration (continued)

Field	Field Description	Usage Guidelines
Application directory	The name of the directory that was created in applications on the Wowza Media Server to stream on demand. This directory is used in the default on-demand URL.	If you followed Cisco recommendations when you set up the Wowza Media Server, this directory is called “vod.”
Use alternate on demand URLs	Click to supply your own URLs for on-demand streaming (if your on-demand URLs require different paths or filenames from those that the Content Server generates. Enter the URLs for the Main and Dual video streams and select if you want the filename to be appended to the alternate URLs.	—

Cisco Video Streamer Server

Cisco TelePresence Content Server Release 6.x does not support Cisco Video Streamer media server configuration capabilities. Although these capabilities are visible on the Content Server User Interface, the underlying infrastructure is currently unsupported.

Media Experience Engine 3500 Server

The Content Server default installation supports only FTP upload to Cisco Media Experience Engine 3500 server.

Saving the media server configuration checks that the server is available at the specified server address and displays the server type if that information is available.

For step-by-step instructions to configure the Media Experience Engine 3500 integration, see the *Integration Note for Configuring Cisco MXE 3500 with Cisco TelePresence Content Server* at http://www.cisco.com/en/US/products/ps12130/products_installation_and_configuration_guides_list.html.

To configure a Media Experience Engine 3500 server, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
 - Step 2** Click **Add Media Experience Engine 3500 server configuration**.
 - Step 3** Enter settings in the fields (see).
 - Step 4** Click **Save**.
-

Table 1-11 Recording Setup > Media Experience Engine 3500 Server Configuration

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Server address	The IP address or DNS name of the server.	—
FTP settings		
User name	The username to authenticate to the FTP server.	—
Password/Password confirm	The password to authenticate to the FTP server.	Check the FTP upload functionality by clicking Test FTP. FTP upload is also tested every time you save the media server configuration.
API settings		
User Name	The user name to authenticate to the Media Experience Engine 3500 server.	The user name must belong to an account with administrative rights on the Media Experience Engine 3500 server.
Password/Password confirm	The password to authenticate to the Media Experience Engine 3500 server.	The password must belong to an account with administrative rights on the Media Experience Engine 3500 server. Click Get profiles to connect to the Media Experience Engine 3500 server and display a list of available profile spaces and job profiles.
Profile space	Choose a profile space from the drop-down list. The profile space defines the set of available profiles on the Media Experience Engine 3500 server.	—
Profile	Choose a profile name from the drop-down list. The profile defines the set of encoding and publishing tasks for Media Experience Engine 3500 server to perform.	—

Show and Share Server

For step-by-step instructions to configure the Content Server and Show and Share integration, see the *Cisco TelePresence Content Server and Show and Share Integration Guide* at

http://www.cisco.com/en/US/products/ps11347/products_installation_and_configuration_guides_list.html.

To configure a Cisco Show and Share server, do the following:

Step 1 Go to **Recording setup > Media server configurations**.

- Step 2** Click **Add Show and Share server configuration**.
- Step 3** Enter settings in the fields (see [Table 1-12](#)).
- Step 4** Click **Save**.

Table 1-12 *Recording Setup > Media Server Configurations: Add Show and Share Server Configuration*

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	—
Server address	The IP address or DNS name of the server.	—
User name	The username of an account which will be used for authenticating media uploads to the Cisco Show and Share server.	The account must belong to a superuser or a user with publishing rights on the Show and Share server. See the Cisco TelePresence Content Server and Show and Share Integration Guide for details.
Password/Password confirm	The password of an account which will be used for authenticating media uploads to the Cisco Show and Share server.	—
Publish recording on Show and Share server	Check to automatically publish recordings that are uploaded to the Show and Share server.	—
Get public categories	Click this button to get a list of categories from the Show and Share server using this server address, user name, and password.	—
Show and Share category	Choose the Show and Share category. Recordings that are uploaded to Show and Share are published to this category on the Show and Share server.	—

Podcast Producer Server

Podcast Producer is a third-party product provided by Apple. For setup and support information, go to <http://www.apple.com/support/macossxserver/podcastproducer/>.

To configure a Podcast Producer server, do the following:

- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click **Add Podcast Producer server configuration**.
- Step 3** Enter settings in the fields (see [Table 1-13](#)).

Step 4 Click **Save**.

Table 1-13 *Recording Setup > Media Server Configurations: Podcast Producer Server Configuration*

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Server address	The IP address or DNS name of the server.	—
User name	The username to authenticate to the Podcast Producer server.	—
Password/Password confirm	The password to authenticate to the Podcast Producer server.	—
Get workflows	Click to connect to the Podcast Producer server and display a list of available workflows.	—
Workflow name	Choose a workflow name from the drop-down list. The workflow defines the set of encoding and publishing tasks for Podcast Producer to perform.	—

iTunes U Server

iTunes U is a third-party product provided by Apple. For setup and support information, go to http://www.apple.com/support/itunes_u/

To configure an iTunes U server, do the following:

-
- Step 1** Go to **Recording setup > Media server configurations**.
- Step 2** Click **Add iTunes U server configuration**.
- Step 3** Enter settings in the fields (see [Table 1-14](#)).
- Step 4** Click **Save**.
-

Table 1-14 *Recording Setup > Media Server Configurations: Add iTunes U Server Configuration*

Field	Field Description	Usage Guidelines
Server settings		
Name	A descriptive name for the media server configuration.	The name is used in the template (see Templates) and Manage Outputs pages when you select a media server configuration.
Site URL	The site URL that Apple provides. The URL identifies this iTunes U account.	—
Share secret/Shared secret confirm	Enter and confirm the shared secret that Apple provides for this iTunes U account.	—
Administrator credentials	The credentials string that Apple provides. The credentials specify administrator access permissions.	—
Display name	The actual name of the account that is used to upload content to iTunes U.	—
User name	The username of the account that is used to upload content to iTunes U.	—
Email address	The email address of the account that is used to upload content to iTunes U.	—
User identifier	The user identifier for the account that is used to upload content to iTunes U.	—
Tab ID	The iTunes U upload location (for example, 1234567890.01498307570).	This ID is the suffix of the URL found by dragging a tab within iTunes while browsing your iTunes U account.

Call Configurations

You can configure a call configuration to be used by recording aliases. A call configuration determines the following:

- Dual video support
- Content channel sharpness setting (global configuration)
- Supported call speeds
- Maximum call length
- Encryption support
- Supported video and audio codecs

Displaying the Call Configurations List

To display the call configurations list, go to **Recording setup > Call configurations**. The Content Server is delivered with a default call configuration for the system. This call configuration is used in the pre-installed [Recording Aliases](#)—Default OnDemand Only and Default Live and OnDemand.

From **Recording setup > Call configurations**, site managers can do the following:

- Add new call configurations—click **Add call configuration**. You can then select this or an existing configuration as part of a recording alias (see [Recording Aliases](#)).
- Edit a call configuration: click **Edit** next to the call configuration to modify the settings.
- Delete a call configuration: check the box next to the call configuration that you want to delete. Then click the **Delete selected** button.



Note You cannot delete a call configuration that is used by a recording alias. Its check box is dimmed.

Adding and Editing Call Configurations

Site managers can add and edit call configurations.

To add a new call configuration, do the following:

-
- Step 1** Go to **Recording setup > Call configurations**.
- Step 2** Click **Add Call configuration**.
- Step 3** Enter settings in the configuration fields (see [Table 1-15](#)).
- Step 4** Click **Save**.
-



Note You can also create a new call configuration by using an existing one. Modify the settings of an existing call configuration, and click **Save as**. Give the call configuration a new name, and then click **Save**.

To edit an existing call configuration, do the following:

-
- Step 1** Go to **Recording setup > Call configurations**.
- Step 2** Click **Edit** next to the call configuration that you want to modify.
- Step 3** Edit settings in the configuration fields as needed (see [Table 1-15](#)).
- Step 4** Click **Save**.
-

Table 1-15 *Recording Setup > Call Configurations: Add Call Configuration or Edit*

Field	Field Description	Usage Guidelines
Call configuration		
Name	A name or short description for this call configuration.	A meaningful name or description helps site managers to select the correct call configuration when creating or editing Recording Aliases .
Dual video capabilities		

Table 1-15 Recording Setup > Call Configurations: Add Call Configuration or Edit (continued)

Field	Field Description	Usage Guidelines
Dual video enabled	Dual video capabilities are enabled by default. If dual video is not required, this capability can be disabled.	Dual video is used so that everyone in a call can see what is displayed on a computer (such as a PowerPoint presentation), as well as seeing the main video (other participants). Dual video is also known as “extended video,” a “content channel,” H.239 capabilities when using H.323, or BFCP capabilities when using SIP.
Sharpness enabled	Check this box to globally enable content channel sharpness.	<p>You can use the Sharpness enabled check box to set the content channel video for high resolution endpoint playback by reducing the frame rate of the content channel.</p> <p>Although the Sharpness check box is visible in user-created call configurations, it does not enable the feature. It is used only for the default System Call Configuration settings.</p>
Call options		
Supported call speeds (kbps)	Check the boxes next to the call speeds to be supported in this call configuration.	This setting determines available call bandwidths when dialing out to create a recording when using a recording alias (see Recording Aliases) with this call configuration.
Maximum call length (minutes)	Recording calls that use this call configuration are terminated after the specified number of minutes have elapsed.	The default setting is 0 (zero), which means that the Content Server will not automatically end the call. Zero is also the default value for new call configurations.
Support encryption	Check this box to allow calls that use this call configuration to be encrypted.	<p>The Content Server negotiates the level of encryption with the endpoint.</p> <p>The solution supports media encryption only for the H.323 protocol.</p>
Advertised codecs		
Video codecs	Check the boxes next to the video codecs to be advertised for calls that use this call configuration.	You cannot uncheck H.261. The check box is dimmed, due to standards compliance.
Audio codec	Check the boxes next to the audio codecs to be advertised for calls that use this call configuration.	You cannot uncheck G.711, due to standards compliance. The check box is dimmed

Site Settings

Site settings must be configured before using the Content Server. To configure these settings, go to **Configuration > Site settings**.

Most settings in the site settings page can be applied while the Content Server is in a call without affecting current calls. However, if you change settings that requires all calls to have ended before the settings can take effect, the Content Server automatically enters configuration reload mode and will not accept new incoming calls or make outgoing calls. When the call or calls currently in progress are completed, the new settings are applied and the Content Server is then able to receive and make calls.

In configuration reload mode, the following occurs:

- The **Configuration > Site settings** page displays this message: “The Content Engine is currently in *<x number>* calls. The Content Server is in configuration reload mode and will not accept any further calls or apply the new settings until all current calls have ended. To apply new settings now, click **End all calls**.”
- The **Recordings > Create recording** page displays this message: “There are no resources available to make a call, please try again later.”
- The **Diagnostics > Server overview** page displays this message: “Reloading configurations.”

Site managers can override configuration reload mode and apply changes immediately by clicking **End all calls** on the **Configuration > Site settings** page. Clicking this button terminate calls on the Content Server and applies the new settings.

The settings that trigger configuration reload mode are the following:

- System name
- Cluster name (if in a cluster)
- Gatekeeper settings
- Advanced H.323 settings
- SIP settings
- Email settings



Note

The site settings page automatically refreshes every 10 seconds.

Table 1-16 *Site Setting*

Field	Field Description	Usage Guidelines
System information		
System name	The name for the Content Server.	The system name is used in the Cisco TelePresence Management Suite to identify Content Servers. The system name can also be displayed in the browser title bar when using the web interface. If the Content Server is in a cluster, its system name is not set here but in the Diagnostics > Server overview page.
Cluster name	The name for the cluster.	The cluster name can only be set when the Content Server is in a cluster. Used in the Cisco TelePresence Management Suite to identify the cluster. The cluster name can also be displayed in the browser title bar when using the web interface.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Show in browser title	Click the box to display the system name or cluster name in the browser title bar. The name can be used to brand or identify the Content Server or cluster when using the web interface.	Refresh the page to show changes to the browser title. For a cluster, if you go to the web interface via the frontend address, then the cluster name is shown in the title bar. Otherwise, the browser displays the system name of the Content Server.
Website name	This name is the text that is displayed in the heading of the Content Server website. Enter a meaningful name to brand or identify the website.	—
Frontend address	The IP address or DNS name of the Content Server. Clicking Save checks the address. Changes to this page are not saved if a connection cannot be made to the specified address or if the address does not belong to this Content Server.	If specified, this address is used for the Share link displayed on the View Recordings page and the recording URL displayed on the Edit Recordings page. Otherwise, links to recordings use the address that you typed in the browser URL to log in to the Content Server.
H.323		
Registration status	Displays the status of Content Server registration with the gatekeeper (registered or not registered).	Click S to display a page that shows all the system and recording alias registration details.
Gatekeeper enabled	Click the box to register with the gatekeeper.	Enter the Gatekeeper address, an H.323 ID, and/or an E.164 alias and choose the registration mode. The gatekeeper must be enabled for a cluster. You cannot disable the gatekeeper functionality.
Gatekeeper discovery	Always <i>Manual</i> .	Manual gatekeeper discovery means that the Content Server registers with one specific gatekeeper, identified by its IP address or fully qualified domain name.
Gatekeeper address	The IP address or DNS name of the gatekeeper.	—

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
H.323 ID	Other systems can call the Content Server using the H.323 ID if the Content Server is registered to the gatekeeper.	If the Content Server is in a cluster, its H.323 ID is not set here but in the Server Overview page.
E.164 alias	Other systems can call the Content Server using the E.164 alias if the Content Server is registered to the gatekeeper.	If the Content Server is in a cluster, its E.164 alias is not set here but in the Server Overview page.
Registration status	Choose to register the Content Server as a <i>Terminal</i> or as a <i>Gateway</i> .	<p>If you select Gateway, enter the H.323 gateway prefix and the E.164 gateway prefix. Gateway registration mode is required for:</p> <ul style="list-style-type: none"> Content Server clusters. Automatic creation of personal recording aliases for creators. Playback of recording from an endpoint. <p>When registered as a terminal, the maximum number of registrations allowed to the gatekeeper from a Content Server is 25, meaning that the maximum number of recording aliases is 25. When registered as a gateway, there is no maximum.</p>
H.323 gateway prefix	If registered as a gateway, this prefix must be entered before the <i>H.323 ID</i> of a Recording alias when calling the Content Server.	<p>For a cluster, enter non-live and live H.323 and E.164 gateway prefixes. The prefixes you enter cannot be subsets of each other. Ensure that they are unique and that they follow the dialing plan set up on your VCS.</p> <p>The non-live gateway prefix is used for recording aliases with no live streaming outputs. The live gateway prefix is used for recording aliases with live streaming outputs.</p>
E.164 gateway prefix	If registered as a gateway, this prefix must be entered before the E.164 alias of a recording alias when calling the Content Server.	<p>For a cluster, enter non-live and live H.323 and E.164 gateway prefixes. The prefixes you enter cannot be subsets of each other. Ensure that they are unique and that they follow the dialing plan set up on your VCS.</p> <p>The non-live gateway prefix is used for recording aliases with no live streaming outputs. The live gateway prefix is used for recording aliases with live streaming outputs.</p>

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Playback H.323 gateway prefix	When registered as a gateway, enter either the playback H.323 gateway prefix or playback E.164 gateway prefix to enable recordings to be played on endpoints. This prefix is added to a recording's playback address to make the playback H.323 ID that the user dials to play the recording on the endpoint.	Ensure that the prefix that you enter is unique, not a subset of another prefix, and that the prefix follows the dialing plan that is set up on your VCS. The playback prefix field is displayed only if the Content Server or the Content Server cluster has the Premium Resolution option key installed.
Playback E.164 gateway prefix	When registered as a gateway, enter either the playback H.323 gateway prefix or playback E.164 gateway prefix to enable recordings to be played on endpoints. This prefix is added to a recording's playback address to make the playback E.164 alias that the user dials to play the recording on the endpoint.	Ensure that the prefix that you enter is unique, not a subset of another prefix, and that the prefix follows the dialing plan that is set up on your VCS. The playback prefix field is displayed only if the Content Server or the Content Server cluster has the Premium Resolution option key installed.
Authentication	By default, authentication is off.	If the gatekeeper requires systems to authenticate with it before they are allowed to register, select <i>Auto</i> and supply the username and password to be used by the Content Server.
User name	The username to authenticate to the gatekeeper.	—
Password	The password to authenticate to the gatekeeper.	—
Password confirm		—
Advanced H.323 settings		
Use static ports	Disabled by default (the box is unchecked). When this setting is disabled, the ports to use are allocated dynamically when opening a TCP/UDP connection.	Static ports can be enabled by clicking the check box and specifying the required port range. Specifying static ports might be necessary if the Content Server is to make calls through a firewall.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Port range	The standard firewall port range is 3230 to 3270. Choose the range that is appropriate to your local firewall settings.	—
NAT	Network Address Translation (NAT) is used when the Content Server is connected to a router with NAT support. The default setting is Off .	<p>If set to On, the Content Server uses the specified NAT address in place of its own IP address within Q.931 and H.245.</p> <p>If set to Auto, the Content Server tries to determine whether the NAT address or the real IP address should be used. This setting makes it possible to call endpoints on both sides of the NAT router.</p> <p>If you select either On or Auto, enter the NAT address.</p>
NAT address	The global, external address to a router with NAT support.	<p>In the router, the following ports must be routed to the system IP address:</p> <ul style="list-style-type: none"> Port 1720 for a standalone Content Server. If the Content Server is in a cluster, the ports specified as the non-live and live Q.931 ports in the gatekeeper settings section above. The port range specified in port range (for example, 3230 to 3270, the standard firewall port range).
SIP settings		
The Status	Displays the status of Content Server registration with the SIP registrar.	<p>Click View all SIP registrations to display a page showing all the system and recording alias registration details.</p> <p>Note If you select Terminal in Registration field, status will be Registered (3 of 3 aliases registered).</p> <p>Note If you select Trunk in Registration field, status will be Trunk Active. This option is available for Content Server users having CUCM call manager. If the trunk between Content Server & CUCM is not active or unreachable, status will be Trunk In-Active.</p>
SIP enabled	Select to enable registration with a SIP registrar. SIP is not available for a cluster.	Enter the SIP display name, SIP address (URI), server address and choose the Transport method from the drop-down list.
SIP display name	The Content Server SIP display name.	This display name is presented as a description of the SIP URI by the SIP registrar to other systems.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
SIP address (URI)	Other systems can call the Content Server using the SIP Address or URI (Uniform Resource Identifier) if the Content Server is registered to a SIP registrar.	—
Server discovery	Always manual.	—
Registration	Select to register the Content Server in terminal or trunk mode.	<p>This displays detailed information about the Content Server registration mode.</p> <p>There are two modes of registration:</p> <ul style="list-style-type: none"> • Terminal • Trunk <p>Note When using the CUCM call manager, you can only use the trunk option to configure the Content Server.</p> <p>Note Content Server with CUCM call manager will not support TMS scheduling because Cisco TelePresence Management Suite (TMS) does not support SIP call scheduling. You cannot configure the Content Server with CUCM call manager to schedule calls.</p>
Trunk Peer Polling Interval	Select the time interval to send the option message to CUCM.	<p>Enter the time interval to send the option message to CUCM. Choose the time interval from the drop-down list.</p> <p>Note The option message verifies that the trunk between the Content Server and its peer node is active.</p>
Playback Domain Suffix	Enter the playback domain suffix if SIP is in trunk mode.	<p>This displays the domain suffix route address.</p> <p>Note To route the calls, a trunk between Content Server and CUCM with the same route pattern should exist.</p> <p>Note When using the CUCM call manager, you can only use the trunk option to configure the Content Server.</p>
Server address	The IP address or DNS name of the SIP registrar.	When changing the address of the SIP registrar, you need to change the server address in all SIP URIs of recording aliases (for example, from SIPalias@SIP.registrar.1 to SIPalias@SIP.registrar.2).v
Server type	Always Auto , which supports registering to standard SIP registrars, such as OpenSIPS.	—

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Transport	The transport protocol for SIP. The default is <i>TCP</i> (Transmission Control Protocol). <i>UDP</i> (User Datagram Protocol) can also be used.	—
User name	The username to authenticate to the SIP registrar.	—
Password	The password to authenticate to the SIP registrar.	—
Password confirm		—
Authentication		
Authentication	<p>Choose the authentication method for the Content Server.</p> <p>If you select either <i>Domain</i> or <i>LDAP</i> authentication, expand the LDAP server section and enter the details of a Microsoft Active Directory server. To enter details for more than one LDAP server, click Add LDAP server. Currently, only Microsoft Active Directory Server is supported. Clicking Save checks the LDAP server settings because the Content Server attempts to bind to the LDAP server. Changes to this page are not saved if the LDAP server settings are incorrect.</p>	<p>There are three modes of authentication (for more information, see Groups and Users):</p> <ul style="list-style-type: none"> • <i>Local</i>: Only users with valid local accounts added through the Groups and Users page can log in. Local groups are not supported. • <i>Domain</i>: Users with domain accounts and local users are able to log in. The local administrator account can be used to configure the Content Server, or other local or domain users can be given a site manager role. Domain authentication can only be used if the Content Server has been added to a domain. If you add the Content Server to an existing domain, you need to define a separate security policy for the Content Server. If you do not define a separate security policy, the existing security policies might prevent the Content Server from functioning correctly. The recommended authentication mode for a cluster is domain authentication. • <i>LDAP</i>: LDAP authentication does not require the Content Server to be added to a domain. Before changing authentication from <i>Local</i> to <i>LDAP</i>, the site manager must add at least one LDAP user with the site manager role to the Content Server. To add a site manager, go to Configuration > Groups and users and click Add groups or users. Enter at least one valid username in the site manager role. Under LDAP authentication, local users cannot log in using the standard login method. However, the local administrator can log in by adding <code>#page:login&rescue:true</code> to the end of the Content Server URL in the browser.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
LDAP	You can add up to five servers that the Content Server will use to look up to authenticate users.	Only active if you have selected Domain or LDAP as the authentication mode.
Server address	The IP address or DNS name of your LDAP server.	Only Microsoft Active Directory Server is currently supported.
Port	Port 389 is the default port for most domain controllers. Global catalog servers may use port 389 or 3268.	Note Content Server supports port 389 and 3268 for LDAP communication.
Base DN	The search base that the Content Server uses to search for user records. (DN = Distinguished Name)	<p>The Content Server searches the object specified and any objects beneath it. The base DN is a unique name for this container. It typically consists of OU, CN, and DC components.</p> <p>Base DN examples:</p> <ul style="list-style-type: none"> • OU=employees,DC=company,DC=com • OU=marketing,OU=employees,DC=company,DC=com <p>In this example, OU marketing is contained within the OU employees. OU=employees,DC=company,DC=com identifies all employees, including the marketing department and OU=marketing,OU=employees,DC=company, DC=com identifies users from the marketing department only.</p>

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
User DN	<p>The LDAP identifier of the account in your domain that the Content Server uses to identify who is trying to log in. The User DN (distinguished name) is a unique name for this account comprising:</p> <ul style="list-style-type: none"> • CN (Common Name) of the special account • OU (Organizational Unit) • DC (Domain Object Class) <p>User DN examples: CN=user_account,OU=employees,DC=company,DC=com CN=user_account,OU=marketing,DC=company,DC=com</p> <p>Note DNs can have many more than four parts.</p>	<p>This account must have read membership privileges—that is, privileges to retrieve users’ “memberOf” attributes from Active Directory using LDAP. You can use an existing account or create a new special account with those privileges. This account does not need to be inside the search tree specified in the <i>Base DN</i>.</p>
Password	The password for the account identified above.	—
Password confirm	—	—
User properties		
Allow guest access	Click this box to enable unauthenticated access to the Content Server as a guest user (guest users do not have to log in).	<ul style="list-style-type: none"> • With guest access enabled, users do not have to authenticate to view recordings. Guest users can view all recordings that have Allow access to all users selected in recording permissions. • The RSS feeds icon is displayed for all users. Recordings that allow access to all users and that are not password-protected can be viewed from an RSS reader.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Automatically create personal recording aliases for creators	Click this box to create a personal recording alias for each user with creator privileges when the user logs in to the Content Server.	<p>Only for Content Servers that are registered to an H.323 gatekeeper as a gateway and requires the API to be enabled.</p> <p>If you have a Content Server cluster, see the “Important Guidelines” section on page 6-5 about recording aliases and adding or removing live output from a template.</p> <p>See the “Creating Automatic Personal Recording Aliases” section on page 1-90 for more information about configuring an automatic recording alias.</p> <p>Personal recording aliases can also be created in a bulk operation using the AddRecordingAlias function in the Content Server’s API. See the Cisco TelePresence Content Server API Guide for details.</p>
Recording alias settings to copy	Select the system recording alias to use for all newly created recording aliases.	<p>All settings for the selected system recording alias settings will be copied except name, owner, H.323 ID, E.164 alias, SIP URI, SIP display name and email address.</p> <p>The name will be the user display name and user name, for example John Smith (jsmith). The H.323 alias will consist of the H.323 gateway prefix with the username appended, for example record.jsmith. The E.164 alias will consist of the E.164 gateway prefix with a random six digit number appended. SIP URI and SIP display name fields will be blank.</p>
Email address suffix	Enter the email address suffix and SIP URL in the form @company.com.	The personal recording aliases will use the creator’s user name with the email address suffix appended at the end to create the email address.
Email settings		
Send email when recording finishes	<p>Click this box to send an email when a recording finishes. The other settings in this section must be configured to have emails sent successfully.</p> <p>Clicking Save checks the email SMTP settings. A warning is displayed if a connection to the SMTP server fails. Changes to the page are still saved, even if the email settings are incorrect.</p>	The email is sent to the address specified in the recording alias (see Recording Aliases) that was used to make the recording. The email contains a link to find the recording in the recordings page.
From email address	The email address that emails are sent from.	—

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
SMTP server address	The address of the mail server to use to send email.	—
SMTP server authentication (if required)		—
User name	Enter a username if the SMTP server requires authentication.	—
Password	Enter a password if the SMTP server requires authentication.	—
Password confirm		—
Languages		
Preferred language	The default language to use in the interface display for users who have not chosen their own language.	When users choose another language option, their choice (not the default language) is applied every time that they log in.
Figure 1-5SIP registration	Click this link to upload a language pack to the Content Server. The language or languages that the pack contains are then available in the web interface after successful upload.	—
API		
API enabled	The Content Server includes an Application Programmer Interface (API) that is designed to provide mechanisms for external systems and services to get information from and to add information to the Content Server. The API must be enabled for a cluster.	<p>The API is designed for integration with the Cisco TelePresence Management Suite (TMS) but can also be used with other management systems.</p> <p>The API is enabled by default and must stay enabled in the following cases:</p> <ul style="list-style-type: none"> • If integration with TMS is required. • If the API is used for customized integration with other systems. Refer to the Cisco TelePresence Content Server API Guide for details about available API calls. • If you select the Automatically create personal recording aliases for creators checkbox. • If the Content Server is a cluster member. <p>If none of these cases apply, you can disable the API.</p>
Username	The Content Server API username is <i>admin</i> .	Username cannot be modified.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
Password	The password for accessing the Content Server API.	The default API password is the serial number of the Content Server (49A3xxxx). Cisco strongly recommends that you change this password if you want the API to remain enabled. If you clear the password and the password field remains empty, API clients will not receive an authentication challenge. To change the API password, go to Management > Configuration > Site settings . In the API section, enter a new password in the Password and Password confirm fields. Click Save .
Password confirmed	—	—
System defaults		
Default recording alias	The default alias must be a system recording alias.	If the system H.323 ID, E.164 alias, SIP URI, or Content Server IP address is called from an endpoint, the recording alias that you choose is used for recording or streaming and recording the call.
Default media services configurations	Specify which Media server configuration is shown by default in the Media server configurations lists when adding or editing a template or in the Manage outputs page of a recording.	—
Windows Media	The preconfigured media server configuration—Local Windows Media Streaming Server—is used by default.	A media server configuration for the local or an external Windows Media Streaming Server can be added and then chosen instead.
MPEG-4 for QuickTime	By default, it is not possible to stream MPEG-4 for QuickTime live from the Content Server. The preconfigured media server configuration—Local IIS Web Server—is used by default. This server delivers MPEG-4 for QuickTime as a progressive download (HTTP streaming).	A media server configuration for an external Darwin or QuickTime streaming server can be added and then chosen here.

Table 1-16 Site Setting (continued)

Field	Field Description	Usage Guidelines
MPEG-4 for Flash	The preconfigured media server configuration—Local IIS Web Server—is used by default.	A media server configuration for a Wowza streaming server can be added and then chosen here. By default, it is not possible to stream MPEG-4 for Flash live from the Content Server.
Advanced streaming options		
Target bit rates	Choose the maximum output bit rates for each output size. These changes affect the bit rates of outputs created by the Templates and Manage outputs pages.	—
Small	The target bit rate for small outputs in the range 150–512 kbps. 250 is the default.	—
Medium	The target bit rate for Medium outputs in the range 512–1152 kbps. 800 is the default.	—
Large	This field cannot be edited.	—
Preferred player	Choose the preferred player for viewing recordings.	By default, the preferred player is Silverlight.

Figure 1-4 Site setting

S

The screenshot displays the 'Site settings' configuration page. At the top, there are four tabs: 'Diagnostics', 'Recordings', 'Recording setup', and 'Configuration'. Below the tabs, the 'Site settings' section is active, showing a 'Save' button and a 'Return' button. A collapsible section titled 'SIP settings' is expanded, revealing a warning: 'Changes to any of these fields will not take effect on a given Content Server until all its calls have ended.' The settings include:

- Status:** Trunk Active, with a link to 'View all SIP registrations'.
- SIP enabled:** A checked checkbox.
- SIP display name:** An empty text input field.
- SIP address (URI):** An empty text input field.
- Server discovery:** Set to 'Manual'.
- Registration:** Radio buttons for 'Termino' and 'Trunk', with 'Trunk' selected.
- Trunk Peer Polling Interval:** A dropdown menu set to '10'.

View all gatekeeper registrations

To display detailed information about gatekeeper registrations, in the **Management** tab, go to **Configuration > Site Settings**. Click **View all gatekeeper registrations**. The page that appears is a status page. User cannot edit any fields. The following information is displayed:

Table 1-17 Configuration > Site settings: View all gatekeeper registrations

Field	Field Description	Usage Guidelines
Gatekeeper registration status		
Registered	The IP address or DNS name of the H.323 gatekeeper that the Content Server is currently registered to	A green check mark displays that the content server is registered to a gatekeeper.
System registrations		
Alias	The name of the H.323 ID or E.164 alias that is registered. This is configured in Site Settings .	—
Current status	The current status of the registration with the gatekeeper. If the status is 'Not Registered,' then check that the alias is not a duplicate of another system registered to this gatekeeper.	A red exclamation point means that there is a problem. The accompanying error message explains why.
Alias type	Either H.323 ID or E.164 Alias.	—

Table 1-17 Configuration > Site settings: View all gatekeeper registrations (continued)

Field	Field Description	Usage Guidelines
Recording alias registrations		
Alias	The name of the H.323 ID or E.164 alias that is registered. This is set in a recording alias (see the Adding or Editing Recording Aliases section).	—
Current status	The current status of the registration with the gatekeeper. If the status is 'Not Registered,' then check that the alias is not a duplicate of another system registered to this gatekeeper.	—
Alias type	Either H.323 ID or E.164 Alias.	—
Recording alias	The name of the recording alias that uses this alias	Click on an entry to display its details (see the Adding or Editing Recording Aliases section).

View all SIP registrations

To display detailed information about registrations with a SIP registrar, in the Management tab, go to **Configuration > Site Settings**. Then click **View all SIP registrations**. The page that appears is a status page. You cannot edit any fields. The following information is displayed:





Table 1-18 Configuration > Site settings: View all SIP registrations

Field	Field Description	Usage Guidelines
SIP registration status	The current status of SIP registration.	SIP registration status as enabled means that the trunk between Content Server and CUCM is not active.
SIP Trunk status Note When using the CUCM call manager, you can only use the trunk option to configure the Content Server.	The current status of SIP Trunk.	SIP Trunk status as active means that the trunk between Content Server and CUCM is active.
System registration		
SIP address	The SIP address (URI) that is registered. This address is set in Site Settings .	—

Table 1-18 Configuration > Site settings: View all SIP registrations (continued)

Field	Field Description	Usage Guidelines
SIP display name	The SIP display name sent with the registration. This is set in Site Settings .	This is presented as a description of the SIP URI by the SIP registrar to other systems.
Current status	The status of Content Server's system registration with the SIP registrar.	A red exclamation point means that there is a problem. The accompanying error message explains why.
Recording alias registrations		
SIP address	The SIP address (URI) that is registered. This is set in a recording alias (see the Adding or Editing Recording Aliases section).	—
SIP display name	The SIP display name sent with the registration. This is set in a recording alias (see the Adding or Editing Recording Aliases section).	—
Registration status	The status of the registration with the SIP registrar.	—
Recording alias	The name of the recording alias that uses this registration.	Click on an entry to display its details (see the Adding or Editing Recording Aliases section).

Figure 1-5 SIP registration

Diagnostics	Recordings	Recording setup	Configuration
SIP registrations			
Return			
<input type="checkbox"/> SIP registration status			
 Disabled			
<input type="checkbox"/> SIP Trunk status			
 Active			
<input type="checkbox"/> System registration			
SIP address (URI) 	SIP display name 	Trunk status	
SIP216@tcs216.com	SIP216@tcs216.com	Active	
<input type="checkbox"/> Recording alias registrations			
Recording aliases are not registered with the trunk when the sip is in trunk mode.			
Return			

Upload language pack

To upload a language pack to the Content Server, do the following:

- Step 1** Download language packs that are available for this release from Cisco.com
- Step 2** In the Content Server web interface, click **Upload language pack**. The Install language pack dialog box appears.
- Step 3** Browse to the language pack .zip file that you downloaded from Cisco.com. Then click **Upload**.
- Step 4** Return to **Site Settings**, and refresh the page. Check that the language appears in the **Preferred language** drop-down menu.
- Step 5** If you want the language in the downloaded language pack to be the preferred language for the Content Server interface for all Content Server users, you must choose it from the **Preferred language** drop-down menu. Then click **Save**.

Content Server users view the interface in the language that was set by a site manager until the users choose another language option from the **Select language** link in the top right corner of the interface.

The English (default) language pack cannot be uninstalled.

To remove a previously uploaded language pack, do the following:

-
- | | |
|---------------|--|
| Step 1 | Open a Remote Desktop Connection to the Content Server. Log in as an administrator. |
| Step 2 | Navigate to E:\lang. |
| Step 3 | Delete the language folder (for example, zh_CN) for the language pack that you want to remove. |
| Step 4 | Log out of the Remote Desktop Connection session. |
-

After you delete the folder, the language pack does not appear in the **Preferred language** drop-down menu in **Configuration > Site Settings**. It also does not appear as language in the **Select language** menu at the top right of the interface.

Groups and Users

A group or user with access to the Content Server can have one of three roles. Each role has access to different menus in the interface when you log in as a user with a specific role.

The roles and available menus are as follows:

- **Viewer**—groups or users who can view the recordings they have been given access to. Viewers have access to all recordings that have been made available to them for viewing. Viewers can also view all recordings with guest access.
- **Creator**—groups or users who can create recordings. When logged in as creators, they have access to all recordings that they created and recordings that others have given them permission to edit. Creators possess all the properties of viewers.
- **Site manager**—groups or users who can use all the Content Server's functionality. A site manager has access to all recordings on the server **View Recordings** and **Management** tabs. Site managers possess all the properties of viewers and creators.

Understanding Group and User Accounts

Groups and users have to be Windows group or user accounts before they can be added to the Content Server. Adding users to the Content Server might happen automatically, depending on whether or not guest access is enabled in **Configuration > Site settings**. You must also consider the authentication mode set in site settings (LDAP, Domain, or Local). The appropriate authentication mode depends on how user accounts are organized in your company:

- You use Active Directory, but your Content Server is not in a domain or is in a different domain from the domain that contains your groups and users. (See [Option 1: LDAP](#).)
- You use Active Directory, and your Content Server is in the same domain as your groups and users. This option is recommended for a Content Server cluster. (See [Option 2: Domain](#).)
- You do not use Active Directory. This option is the least preferred because it is more time consuming to configure and maintain user accounts. This option is not recommended for a Content Server cluster. (See [Option 3: Local](#).)

Option 1: LDAP

You use Active Directory, but your Content Server is not in a domain or is in a different domain from the domain that contains your groups and users.

**Note**

Before changing authentication mode to LDAP, a site manager must add at least one LDAP group or user with the site manager role to the Content Server. Under LDAP authentication, local users (user accounts set up through the Windows Server administration interface) and the local administrator cannot log in using the login dialog. However, the local administrator can log in by adding `#page:login&rescue:true` to the end of the Content Server URL in the browser: `http://<ContentServerIPAddress>/ContentServer/#page:login&rescue:true`.

-
- Step 1** From the **Management** tab, go to **Configuration > Site settings**.
- Step 2** For Authentication mode, click **LDAP**.
- Step 3** Enter the details of your LDAP server or servers.
- Step 4** From the **Management** tab, go to **Configuration > Groups and users**.
- Step 5** Add the LDAP groups or users to the Content Server in the appropriate format. Assign an appropriate role (Viewer, Creator or Site manager).
- If the **Allow guest access** setting is enabled in site settings, you need to manually add all the groups and users who you want to log in. If users do not exist on the Content Server before they attempt to log in for the first time, but a group to which they belong does exist, their account is created automatically, and they are given the role of viewer. When they actually log in, their role is whichever is higher—their group role or their individual user role.
 - If **Allow Guest Access** is disabled in site settings, you only need to add the groups and users who need a role higher than viewer. If users do not exist on the Content Server before they attempt to log in for the first time (regardless of whether there is a group added to the Content Server that they are a member of), their account is created automatically, and they are given the role of viewer. When they actually log in, their role is whichever is higher—their group role or their individual user role.
-

All users and all members of the added groups now automatically have access to the Content Server using their normal Active Directory username and password. Groups and users with their roles are listed in **Configuration > Groups and users**.

Option 2: Domain

You use Active Directory, and your Content Server is in the same domain as your groups and users. (This option is recommended for a Content Server cluster.)

-
- Step 1** From the **Management** tab, go to **Configuration > Site settings**.
- Step 2** For Authentication mode, click **Domain**.
- Step 3** Enter the details of your LDAP server or servers so that the Content Server has access to group information.
- Step 4** From the **Management** tab, go to **Configuration > Groups and users**.
- Step 5** Add the domain groups or users to the Content Server in the format `group.name` or `DOMAINNAME(optional)\username: Display Name(optional)>`. Assign the correct role (Viewer, Creator or Site manager).

- If the **Allow guest access** setting is enabled in site settings, you need to manually add all the groups and users who you want to log in. If users do not exist on the Content Server before they attempt to log in for the first time, but a group to which they belong does exist, their account is created automatically, and they are given the role of viewer. When they actually log in, their role is whichever is higher—their group role or their individual user role.
- If **Allow Guest Access** is disabled in site settings, you only need to add the groups and users who need a role higher than viewer. If users do not exist on the Content Server before they attempt to log in for the first time (regardless of whether there is a group added to the Content Server that they are a member of), their account is created automatically, and they are given the role of viewer. When they actually log in, their role is whichever is higher—their group role or their individual user role.

All users and all members of the added groups now automatically have access to the Content Server using their normal Active Directory username and password. Groups and users with their roles are listed in **Configuration > Groups and users**.

Option 3: Local

You do not use Active Directory. (This option is the least preferred because it is more time consuming to configure and maintain accounts.)

-
- Step 1** Create local user accounts on the Content Server for every user. Open a Remote Desktop Connection to the Content Server. Log in as an administrator. Create the accounts in the Windows Server administration interface. (See the [Managing Local Users and Groups](#) for more information.)
- Step 2** From the **Management** tab, go to **Configuration > Site settings**.
- Step 3** For Authentication mode, click **Local**.
- Step 4** From the **Management** tab, go to **Configuration > Groups and users**.
- Step 5** Add every user individually to the Content Server in the Add groups or users page with the correct role (Viewer, Creator, or Site manager). Local users must be entered in the format MACHINENAME\username:Display Name (optional).
-

All users now have access to the Content Server using the username and password of their local account. Users with their roles are listed in **Configuration > Groups and users**. Their role is displayed next to the name.



Note

Local authentication does not support groups.

Displaying the Groups and Users List

To display the groups and users list, go to **Configuration > Groups and users**. The list shows both groups and users alphabetically by name and additional information about the groups and users (see [Table 1-19](#)).

The icon for each entry tells you whether it is a group or a user.

To see only groups or only users, choose **Only groups** or **Only users** from the **Show** drop-down list.

From **Configuration > Groups and users**, a site manager can do the following:

- Edit a group or user by clicking **Edit**.

- Delete a group or user. To delete, check the box next to the group or user that you want to delete. Then click **Delete selected**. You cannot delete the local administrator or the user you are logged in as.
- Add a new group or user by clicking **Add groups or users**.

Table 1-19 Configuration > Groups and Users List

Field	Field Description	Usage Guidelines
Groups and users		
Name	The name of the user or the Base DN of the group.	—
Display name	The user display name or the group name.	For users, the name that is shown in the upper right corner of the screen when you log in.
Role	One of the three roles: site manager, creator or viewer. <ul style="list-style-type: none"> • Site managers have access to all Content Server functions. • Creators can create recordings and can have personal recording aliases. • Viewers can browse and view recordings. 	If a user is a member of a group and has been added automatically to the Content Server, the role is displayed as viewer, even though the group that the user is a member of might have higher privileges. Site managers can change the user role. If this is a group or a user who has been added manually, the role that is displayed is the one set by a site manager.
Recording aliases owned	The number of recording aliases that belong to this user or group.	—

Adding and Editing Groups and Users

Site managers can add new groups or users to assign them a role. Site managers can also update existing ones. We recommend that you work with groups whenever possible; then users can be added automatically.

To add a new call configuration, do the following:

-
- Step 1 Go to **Configuration > Groups and users**.
 - Step 2 Click **Add groups or users**.
 - Step 3 Enter settings in the configuration fields (see [Table 1-20](#)).
 - Step 4 Click **Add**.
-

To edit an existing group or user, do the following:

-
- Step 1 Go to **Configuration > Groups and users**.

- Step 2** Click **Edit** next to the group or user that you want to modify.
- Step 3** Edit settings in the configuration fields as needed (see [Table 1-15](#)).
- Step 4** Click **Save**.

Table 1-20 Configuration > Groups and Users: Add

Field	Field Description	Usage Guidelines
Add groups or users		
Site manager role	Groups and users that are entered here have site manager privileges.	Users who are members of a group automatically have the role that is assigned to the group. Users who are members of more than one group have the highest role (role with the most privileges) of any group that they belong to. For example, if a user is a member of two groups, one with viewer privileges and one with creator privileges, then the user has creator privileges. If a user who is a member of a group has been added automatically to the Content Server, the user has the highest privileges based on group membership, but the user role is displayed as viewer. Site managers can change the role of individual users by editing them.
Creator role	Groups and users that are entered here can create recordings with their personal recording aliases. Creators can edit recordings with recording aliases that give them editing privileges. Creators can also edit parts of their own personal recording aliases.	—
Viewer role	Groups and users that are entered here can view recordings that they have access to. Viewers can also view all recordings with guest access.	—

Table 1-21 Configuration > Groups and Users: Edit

Field	Field Description	Usage Guidelines
Details		
Name	The name of the user or the Base DN of the group.	—

Table 1-21 Configuration > Groups and Users: Edit (continued)

Field	Field Description	Usage Guidelines
Role	Whether the group or user has site manager, creator, or viewer privileges.	—
Display name	The name of the group or user as displayed in the upper right corner of the screen.	—
Internet speed detection		
Automatically determine internet speed	Check this box to have the Content Server automatically calculate the internet connection speed the first time that a user logs in with a browser through a computer or after the user rechecks the recording play properties. This box is checked by default.	—
Internet speed	If you uncheck the Automatically determine internet speed box, choose an internet speed for the connection.	—
Recording aliases owned by this group or user		
Below are the recording aliases owned by this group or user	The recording aliases that belong to the group or user.	Click Edit next to the recording alias to open the Edit recording alias page.

Creating Automatic Personal Recording Aliases

For Content Servers that are registered to an H.323 gatekeeper as a gateway, site managers can configure the Content Server to automatically create personal recording aliases for users with creator privileges. When a creator logs in to the Content Server web interface, a unique recording alias containing a personal SIP URI and/or H.323 ID is automatically assigned to them. The automatically created recording alias then becomes the user's personal recording alias.

For example, the site manager can create an LDAP user group called *Content Server_creators* and enter this group into the creator role when adding users and groups. When a member of the *Content Server_creators* group logs in with their LDAP credentials, they can use the Content Server to record TelePresence sessions by including their LDAP username in the SIP URI (*username@content_server_sip_domain*), or in the H.323 ID (*record.username*).

Guidelines and Limitations

Observe these guidelines and limitations:

- The Content Server group authentication mode must be LDAP.

- The Content Server must register to an H.323 gatekeeper as a gateway to automatically create personal recording aliases. Registering in *terminal mode* is not supported.
- The settings for the creator's new personal recording alias are copied from a system recording alias that is designated by the site manager. The name, owner, H.323 ID, E.164 alias, SIP URI, SIP display name and email address are set to unique values based on the creator's username.

The name of the recording alias will be the user display name and username, for example *John Smith (jsmith)*. The H.323 alias will consist of the H.323 gateway prefix with the username appended, for example *record.jsmith*. The E.164 alias will consist of the E.164 gateway prefix with a random six-digit number appended. SIP URI and SIP display name fields will be blank.

- The site manager can manually create personal recording aliases for creators *before* they log in to the Content Server. In this case, the creator would not receive an auto-created recording alias.
- The site manager can also manually create additional personal recording aliases for creators *after* they have received an auto-created recording alias.
- For more information about creating system recording aliases that support the transforming and sharing of recorded content, see the [Capture Transform Share](#) configuration guides on Cisco.com.

Procedure

-
- Step 1** Follow the instructions in [“Option 1: LDAP” section on page 1-86](#) to configure an LDAP creator group, and enter a unique name such as *Content Server_creators*.
- Step 2** From the **Management** tab, go to **Configuration > Site settings > User properties**.
- Step 3** To enable automatic recording alias creation, click the **Automatically create personal recording aliases for creators** check box.
- Step 4** Select a system alias in the **Recording alias settings to copy** drop-down menu.
- Step 5** Enter the email address suffix and SIP URL in the form *@company.com*.
The creator will receive an email each time that a recording is completed.
- Step 6** Click **Save**.
-

Windows Server



Note

The Content Server does not support running Windows services such as Active Directory Domain Services (ADDS), DNS server, or file services. You should configure an external server for all Windows-based services.

Beginning with Cisco Content Server Release 6.0, all Windows Server 2008 administration and configuration is accomplished by using Windows Remote Desktop Connection to access the server administration interface.

Using Windows Remote Desktop Connection from Your Computer for Windows Server Administration

To access Windows Server 2008 administration interface, do the following:

-
- Step 1** On your computer, go to **Start > All Programs > Accessories > Remote Desktop Connection**. (On some computers, the path is **Start > All Programs > Accessories > Communications > Remote Desktop Connection**.)
- Step 2** In the Remote Desktop Connection dialog box, enter the IP address or DNS name of the Content Server.
- Step 3** If you are upgrading software, applying security updates, or manually copying in a recording import file to the Content Server, you need to share your disk drives:
- In the Remote Desktop Connection dialog box, click **Options**.
 - Click the **Local Resources** tab. In the Local devices and resources section, check **Drives** (click **More** if you do not see this option).
- Step 4** Click **Connect**.
- Step 5** Log in with an administrator account username and password. This account can be the local administrator account, or if the Content Server is in a domain, a domain administrator account.
- Step 6** The Server Manager user interface appears.
-

Changing the Local Administrator Account Password

The local administrator account is a built-in Windows account that has complete access to the local system. It has been added to the Content Server groups and users list as <machine-name>\Administrator with a site manager role. This account cannot be deleted from the list.

You can use this account to log in to the Content Server web interface, the Windows Server administration interface, and the Remote Desktop Connection.

Because this account has complete access to the Content Server, we recommend that you change the local administrator password regularly.



Note Do not change the local administrator account username.

To change the local administrator account password, do the following:

-
- Step 1** Log in to the Content Server by using a Remote Desktop Connection. Go to **Start > Control Panel > User Accounts > Change your Windows password**. The User Account window appears.
- Step 2** Click **Change your password**.
- Step 3** Enter the current password and new password. Then confirm the new password.
- Step 4** Click **Change password**.
-

Updating the System Date and Time

The system date, time, and time zone must be correct. They were set during installation, but you can update them if necessary. To update, do the following:

-
- Step 1** Log in to the Content Server by using a Remote Desktop Connection and the Administrator password.
- Step 2** In the Server Manager window, click the time and date box in the lower right corner to open the settings window. Or, go to **Start > Control Panel > Clock, Language, and Region > Set the time and date**.
-

- Step 3** Click **Change date and time settings**.
 - Step 4** Update the date, time, and time zone. Click **OK**.
 - Step 5** Restart the server. Go to **Start > Log Off > Restart**.
-

Managing Local Users and Groups

Depending on the Content Server authentication method, you might need to create, edit, or delete local user or group accounts in the Server Manager user interface. To verify the Content Server authentication method, go to Configuration > Site settings in the Content Server web UI.

To manage local users and groups, do the following:

-
- Step 1** Log in to the Content Server by using a Remote Desktop Connection.
 - Step 2** In the Server Manager window, go to **Local Users and Groups**.
 - Step 3** Select a Local User or Groups folder. In the Actions window, select **More Actions > New User** or **New Group** to add a new user or group.
 - Step 4** After entering the account settings, click **Create**.
-



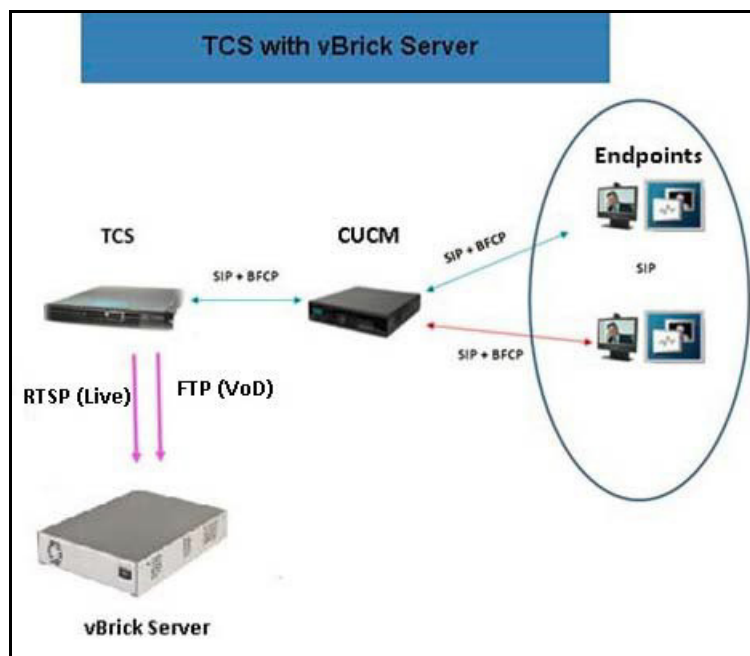
Cisco TelePresence Content Server Integration with VBrick

Integration Overview

What is the Cisco TelePresence Content Server

The Cisco TelePresence Content Server (Cisco TCS) is a network appliance that enables organizations to share knowledge and enhance communication by recording their video conferences and multimedia presentations for live and on demand access. The Cisco TCS can be scheduled by Cisco TMS to automatically include the Cisco TCS into any scheduled event or be used in an ad - hoc manner. The Cisco TCS workflow will automatically produce high quality videos of any standards based on conference from a MCU, TelePresence Server, or directly from a TelePresence endpoint including the video participants and any secondary content for example a presentation. Whether it's a university lecture, a corporate training session, an executive meeting or any other critical event – the Cisco TelePresence Content Server streamlines the process of capturing content throughout the organization.

Figure 2-1 TCS Integration with VBrick



What is VBrick DME

The VBrick Distribute Media Engine (DME) is a multi-faceted platform that performs a variety of serving, reflecting, transmuxing, and transrating activities. DME receives a unicast stream over the WAN link (often over TCP) to effectively traverse the LAN and pass through firewalls. The DME streams via unicast and/or multicast to a variety of different clients in the streaming protocol of choice for each client.

The DME has a fully functional web server that uses File Transfer Protocol (FTP) to populate the DME with files for progressive download. You can FTP to the FTP folder on the DME or to a sub folder.

It is a versatile, high configurable media distribution engine that moves streaming media to and from a wide variety sources and endpoints. You can distribute your video to anyone with the DME.

Prerequisites

- Cisco TCS software requirements
 - TCS 6.2.1

Limitations

- VBrick VoD and VBrick Live playback does not support on TCS User Interface (UI). TCS will act as a recoding device for VBrick integration.

Configuring Cisco TelePresence Content Server

Perform these tasks:

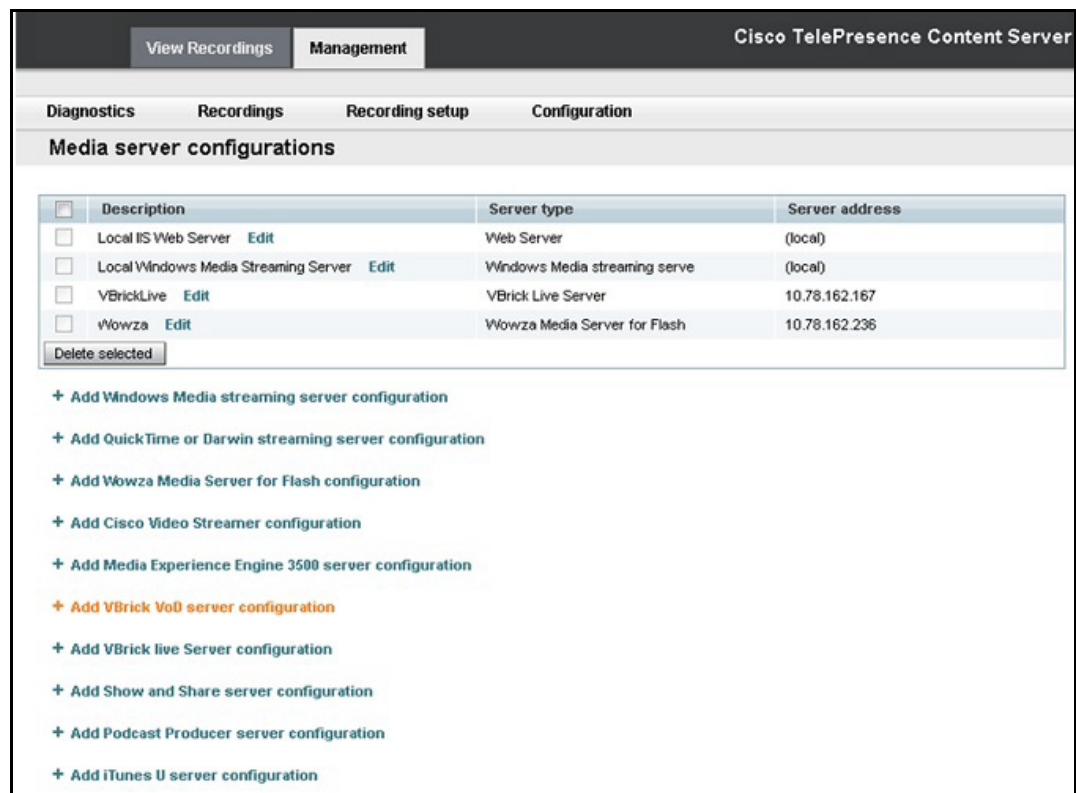
1. [Configuring Media Server for VBrick VoD](#)
2. [Configuring Template for VBrick VoD](#)
3. [Configuring Recording Alias for VBrick VoD](#)

Configuring Media Server for VBrick VoD

You need to create the Media server configuration in the Cisco TCS. Follow these steps for VBrick VoD:

- Step 1** Log in to Cisco TCS
- Step 2** Click **Management** tab.
- Step 3** Navigate to **Recording setup > Media server configurations**.
- Step 4** Click **VBrick VoD server configuration**.

Figure 2-2 VBrick VoD server configuration



- Step 5** Enter the name for VBrick server.
- Step 6** Enter the VBrick server address, **ftp** username and password.

- Click the **Test FTP** button to test the FTP connection.



Note An error message is displayed, if FTP connection is not established.

Step 7 Click **Save**.

Figure 2-3 FTP settings

The screenshot shows the 'Media server configuration: VBrick server' page. At the top, there are tabs for 'View Recordings', 'Management', 'Diagnostics', 'Recordings', 'Recording setup', 'Configuration', and 'Help'. The 'Management' tab is selected. Below the tabs, there are buttons for 'Save', 'Save as', and 'Return'. A green check mark and the message 'Media server configuration updated.' are displayed. The 'Server settings' section includes fields for 'Name' (VBrickServerVoD), 'Server address' (10.78.162.21), and 'FTP settings' (User name: admin, Password: *****, Password confirm: *****). A 'Test FTP' button is present, and a green check mark with the message 'FTP test successful to server 10.78.162.126:21.' is shown below it. At the bottom, there are buttons for 'Save', 'Save as', and 'Return', and another green check mark with the message 'Media server configuration updated.'

Green check mark indicates the successful connection of FTP.

Step 8 Click **Return**.

Configuring Template for VBrick VoD

You need to associate the template to the recording alias to automate the delivery of the transformed recording to VBrick. Follow these steps:

- Step 1** Click the **Management** tab, appearing at the top of the screen.
- Step 2** Click **Recording > Setup > Templates > Add Template**.
- Step 3** Under Template section do the following:
 - a. Add Template name for **VBrick VoD**.
 - b. Check the option '**Distribute to Media Experience Engine 3500, VBrick, Show and Share, Podcast Producer or iTunes U**'.

- c. Decide which media layout to be displayed Cisco TCS web interface. For this example, **Switching** is chosen.
- d. Under '**Outputs for Distribution to Podcast Producer, VBrick, or iTunes U**', choose the media layout for VBrick output. By default switching would be selected.
- e. Check the box next to the VBrick to enable the media server. Under Media Server Configuration list, select VBrick Server from the VBrick drop down.

**Note**

This media server has been created in step 1 under the '**Media Server Configuration**' section.

- f. Choose the size of the output that will be used to upload to VBrick.

**Note**

The SAM account name will be written into the media file and shared to the VBrick system.

Figure 2-4 *Output distribution*

Step 4 Scroll to the top or bottom, click **Save** and click **Return**.

Configuring Recording Alias for VBrick VoD

Step 1 Click the tab at the top labeled **Management**.

Step 2 Click **Recording Setup > Recording Aliases > Add Recording Alias**.

Step 3 A new page will appear, fill the recording aliases information.

- a. Enter a Name for the recording alias, **VBrick VoD**.



Note

The “Personal Recording Alias owner” for VBrick should match with the user on VBrick Rev

- b. Enter the **H323ID**, **e164alias**, **SIP URI**, and SIP display name. Below is an example of the configuration.
- c. Under the Recording Setting, select **VBrick VoD** template from the Template drop down.



Note

This is the same template created in **Configuring Template for VBrick VoD** section > **Step 3**> point a.

Figure 2-5 Recording Alias

The screenshot displays the 'Edit recording alias' configuration page in the Cisco TelePresence Content Server interface. The page is divided into several sections:

- Recording alias:**
 - Name: VBrickVoDAlias
 - Recording alias type: Personal (selected)
 - Personal recording alias owner: System Administrator (VIN-FHGEOS2GMEFAdministrator)
- Dialing properties:**
 - Enter at least one of the following:
 - H.323 ID: VBrickVodh323id
 - E.164 alias: (empty)
 - SIP settings are disabled in Site Settings so it is not possible to specify a SIP URI for dialing this recording alias.
- Recording settings:**
 - Template: VBrickVoDTemplate
 - Template outputs: Distribution - VBrick Switching MPEG-4 for Flash Large
 - Call configuration: System Call Configuration
 - Show countdown before recording: [checked]
 - Email is disabled in Site Settings so it is not possible to receive email when a recording has been created using this recording alias.

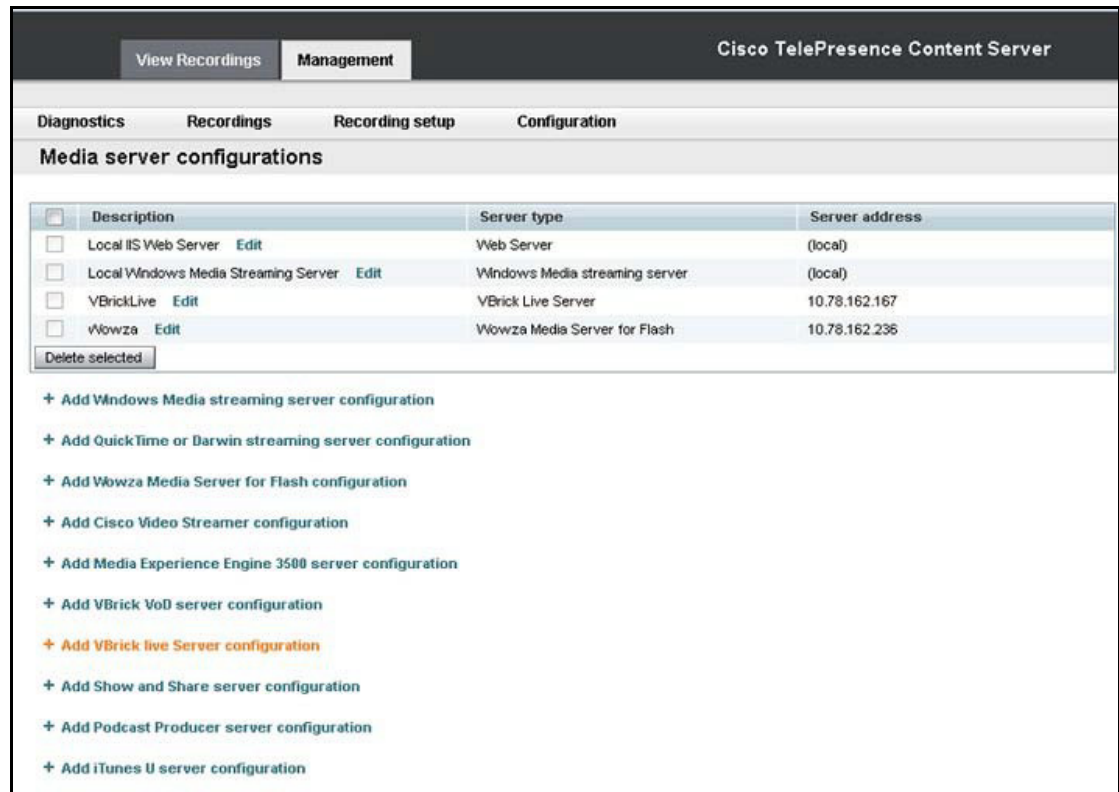
Step 4 Click **Save** and click **Return**.

Configuring Media Server for VBrick Live

You need to create the Media server configuration in the Cisco TCS. Follow these steps for VBrick Live:

- Step 1** Log in to Cisco TCS, and click the Management tab.
- Step 2** Navigate to Recording setup > Media server configurations.
- Step 3** Click **VBrick live Server for Flash configuration**.

Figure 2-6 Media server configuration



- Step 4** Enter the name for VBrick Live server.
- Step 5** Enter the VBrick server address, **VBrick server** username and password.



Note The default username and password for VBrick server is '**broadcast**'.

- Step 6** Enter the RTSP port.



Note The default value of **RTSP** port for VBrick is **5544**.

- Step 7** Click **Save**.



Note An error message is displayed, if RTSP connection is not established.

Figure 2-7 Media Server Configuration: VBrick Server



Note To view Live recording on VBrick Rev Portal, it is mandatory to give static stream name.

Green checkmark indicates the successful connection of RTSP.

Step 8 Click **Return**.

Configuring Template for VBrick Live

You need to associate the template to the recording alias to automate the delivery of the transformed recording to VBrick. Follow these steps:

- Step 1** Click the **Management** tab, appearing at the top of the screen.
- Step 2** Click **Recording > Setup > Templates > Add Template**.
- Step 3** Under Template section do the following:
 - a. Add Template name for VBrick Live.
 - b. Check the 'Viewable in the Content Server web interface'.

- c. Decide which media layout to be displayed on Cisco TCS web interface. For this example, **Switching** is chosen.

Figure 2-8 *Layout display*

Choose how you want to make any recordings made with this template available and edit your options below:

- ☒ Viewable in the Content Server web interface [Choose options](#)
- ☐ Downloadable for portable devices (iPod and Zune) [Choose options](#)
- ☐ Downloadable for general purpose [Choose options](#)
- ☐ Distributed to Media Experience Engine 3500, vBrick, Show and Share, Podcast Producer or iTunes U [Choose options](#)

Outputs to view in the Content Server web interface

Outputs to view in the Content Server web interface

Switching [i](#) Joined [i](#) Stacked [i](#) Picture in picture [i](#)

☐ Force 16:9 [i](#)

On demand

Formats [i](#)

- Windows Media
- MPEG-4 for QuickTime
- MPEG-4 for Flash**

Sizes (choose up to 2) [i](#)

- Audio only
- Small
- Medium
- Large**

Maximum target bit rates (kbps) [i](#)

- Small: 250
- Medium: 800
- Large: Maximum

On demand media server configuration settings

Windows Media: Local Windows Media Streaming Server [i](#)

MPEG-4 for QuickTime: Local IS Web Server [i](#)

MPEG-4 for Flash: Local IS Web Server [i](#)

Optimize for motion: ☐ [i](#)

- d. Choose the MPEG-4 for Flash and size of the output that will be used to upload to VBrick. For this example a large output was chosen.

Figure 2-9 *Live stream*

☒ **Live stream** [i](#)

Format: MPEG-4 for Flash [i](#)

Size: Medium [i](#)

Re-transcode realtime movies: ☒ [i](#)

Live media server configuration settings

Media server configuration: VBrickServerLive [i](#)

- e. Select the **Live stream** check box.
- f. Choose the **VBrick Media Server** from the drop-down list.
- g. Click **Save**.



Note

You must select the option in Media server configuration that you have selected for VBrick server.

**Note**

VBrick Live and VBrick VoD can be configured in a single template.

Configuring Recording Alias for VBrick Live

- Step 1** Click the tab at the top labeled **Management**.
- Step 2** Click **Recording Setup > Recording Aliases > Add Recording Alias**.
- Step 3** A new page will appear to fill out the recording aliases information.
- a.** Enter a Name for the recording alias, for VBrick Live.

**Note**

The “Personal Recording Alias owner” for VBrick should match with the user on VBrick Rev

- b.** Enter the **H323ID**, **e164alias**, **SIP URI**, and SIP display name. Below is an example of the configuration.
- c.** Under the Recording Setting, select **VBrick Live** template from the Template drop down list.

**Note**

The template you select under **Step 3 > c** is the same the template that was created in **Configuring Template for VBrick Live** section **Step 3 > a**.

Figure 2-10 Recording alias

The screenshot displays the 'Edit recording alias' configuration page in the Cisco TelePresence Content Server Management interface. The page is organized into several sections:

- Navigation Tabs:** View Recordings, Management (selected), Diagnostics, Recordings, Recording setup, Configuration.
- Section Header:** Edit recording alias.
- Buttons:** Save, Save as, Return.
- Recording alias section:**
 - Name:** VBrickLiveAlias
 - Recording alias type:** Personal (selected), System
 - Personal recording alias owner:** System Administrator (TCS48\Administrator)
- Dialing properties section:**
 - Enter at least one of the following:**
 - H.323 ID:** VBrickLive323id
 - E.164 alias:** (empty field)
 - SIP settings:** SIP settings are disabled in Site Settings so it is not possible to specify a SIP URI for dialing this recording alias.
- Recording settings section:**
 - Template:** VBrickLiveTemplate
 - Template outputs:**
 - Live stream
 - Switching MPEG-4 for Flash Medium
 - On demand
 - Switching MPEG-4 for Flash Medium (Offline transcoded)
 - Switching MPEG-4 for Flash Medium (Live transcoded)
 - Call configuration:** System Call Configuration
 - Show countdown before recording:** ☒
- Footer Note:** Email is disabled in Site Settings so it is not possible to receive email when a recording has been created using this recording alias.

Step 4 Scroll to the top or bottom, click **Save**.

Step 5 Click **Return**.

Installing VBrick DME (Software only version)

For VBrick DME Admin Guide, see the link

<http://www.vbrick.com/doc/DME/v344/AdminGuide/wwhelp/wwhimpl/js/html/wwhelp.htm>

Related Documentation

For additional product information, see these resources on Cisco.com.

VBrick

<http://www.vbrick.com/doc/DME/v344/AdminGuide/wwhelp/wwhimpl/js/html/wwhelp.htm>

http://www.vbrick.com/doc/DME/v344/PDF_Files/DME_ReleaseNotes.pdf

Disclaimers and Notices

The objective of this guide is to provide the reader with assistance in using and configuring this product. Product capabilities of Cisco and other manufacturers' products change over time and so the required configuration may be different from that indicated here. If you have any suggestions for changes to this document, please feed them back to Cisco through your Cisco Authorized Service Representative.

If you need technical support, please contact your Cisco Authorized Service Representative.

The specifications for the product and the information in this Guide are subject to change at any time, without notice, by Cisco. Every effort has been made to supply complete and accurate information in this Guide; however, Cisco assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Cisco® is a registered trademark belonging to Cisco ASA. Other trademarks used in this document are the property of their respective holders.

This Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of this product. Except for the limited exception set forth in the previous sentence, no part of this Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of Cisco.

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.

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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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

© 2012 Cisco Systems, Inc. All rights reserved.



Configuring a Cisco Unified Communications Manager SIP Trunk with a Cisco TelePresence Content Server

This document includes instructions for configuring a Cisco Unified Communications Manager version 9.1.2 and 10.5 Session Initiation Protocol (SIP) trunk with Cisco TelePresence Content Server (Content Server) Release 6.2.

Before integrating Cisco Content Server 6.2 with CUCM through a SIP trunk, confirm that the Cisco Content Server is ready for the integration completing the applicable tasks in the Content Server installation guide. See the

http://www.cisco.com/c/en/us/td/docs/telepresence/tcs/6_0/installation/guide/tcs-vm-install.html

CUCM Integration with Content Server 6.2

After installing the CUCM software is installed, complete these procedures in the following order:

- **CUCM Integration with Cisco Content Server Standalone**
- **Cisco TCS 6.2 with a Content Server cluster configured**

Cisco Content Server Standalone

To create a SIP Trunk between CUCM and Content Server.

1. [Create the SIP Trunk Security Profile](#)
2. [To Create the SIP Profile](#)
3. [Create the SIP Trunk](#)

Complete these steps in the order given:

Create the SIP Trunk Security Profile

-
- | | |
|---------------|---|
| Step 1 | Login to the Cisco Unified Communication Manager Administration Interface. |
| Step 2 | Choose Security > SIP Trunk Security Profile . |
| Step 3 | On the Find and List SIP Trunk Security Profiles page, click Add New . |

- Step 4** On the SIP Trunk Security Profile Configuration page, under **SIP Trunk Security Profile Information**, enter the following:

Field	Setting
Name	Enter SIP Trunk Security Profile or another name.
Description	Enter SIP trunk security profile for Cisco TCS or another description.
Device Security Mode	If you will not enable CUCM authentication and encryption, accept the default of Non Secure .
X.509 Subject Name	If you will not enable CUCM authentication and encryption, leave this field blank. If you will enable CUCM authentication and encryption, enter the name. This name must match the Subject Name field for the SIP certificate on the Cisco TCS.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Check this check box.

Save

Status: Ready

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode: Non Secure

Incoming Transport Type*: TCP+UDP

Outgoing Transport Type: TCP

☐ Enable Digest Authentication

Nonce Validity Time (mins)*: 600

X.509 Subject Name

Incoming Port*: 5060

☐ Enable Application level authorization

☐ Accept presence subscription

☐ Accept out-of-dialog refer**

☐ Accept unsolicited notification

☐ Accept replaces header

☐ Transmit security status

☐ Allow charging header

SIP V.150 Outbound SDP Offer Filtering*: Use Default Filter

Save

- Step 5** Click **Save**.

To Create the SIP Profile

- Step 1** In Cisco Unified CM Administration, expand **Device> Device Settings** and select **SIP Profile**.
- Step 2** On the Find and List SIP Profiles page, click **Find**.
- Step 3** To the right of the SIP profile (Standard SIP Profile BFCP), click **Copy**.
- Step 4** On the SIP Profile Configuration page, under SIP Profile Information, enter the following settings.

Field	Setting
Name	Enter TCS SIP Trunk or another name.
Description	Enter SIP profile for Cisco TCS or another description.



Note

To create the SIP profile, in the Early Offer support for voice and video call field, select Best Effort (no MTP inserted) from the drop-down list.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾

SIP Profile Configuration

Save Delete Copy Reset Apply Config Add New

☒ Fall back to local RSVP

SIP Rel1XX Options* Disabled ▾

Video Call Traffic Class* Mixed ▾

Calling Line Identification Presentation* Default ▾

Session Refresh Method* Invite ▾

Early Offer support for voice and video calls* Best Effort (no MTP inserted) ▾

☐ Enable ANAT

☐ Deliver Conference Bridge Identifier

☐ Allow Passthrough of Configured Line Device Caller Information

☐ Reject Anonymous Incoming Calls

☐ Reject Anonymous Outgoing Calls

☐ Send ILS Learned Destination Route String

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

SIP Profile Configuration

Save Delete Copy Reset Apply Config Add New

SDP Information

☒ Send send-receive SDP in mid-call INVITE

☒ Allow Presentation Sharing using BFCP

☐ Allow iX Application Media

☐ Allow multiple codecs in answer SDP

Save Delete Copy Reset Apply Config Add New

Step 5 Click **Save**.

Create the SIP Trunk

- Step 1** In Cisco Unified CM Administration, expand **Device** and click **Trunk**.
- Step 2** On the Find and List Trunks page, click **Add New**.
- Step 3** On the Trunk Configuration page, in the **Trunk Type** field, click **SIP Trunk**.
- Step 4** In the **Device Protocol** field, click **SIP** and click **Next**.
- Step 5** Under Device Information, enter the following:

Field	Setting
Device Name	Enter TCS_SIP_Trunk or another name.
Description	Enter SIP trunk for Cisco TCS or another description.
SRTP Allowed	If you will enable CUCM authentication and encryption, check this check box.

Step 6 (Optional) If user phones are contained in a calling search space, under Inbound Calls, enter the following.

Field	Setting
Calling Search Space	Select the name of the calling search space that contains the user phones.
Redirecting Diversion Header Delivery - Inbound	Check this check box.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration ▼ Go

admin | Search Documentation | About | Logout

System ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼ Device ▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼

Trunk Configuration Related Links: Back To Find/List ▼ Go

Save

Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name *	<input type="text" value="sip_trunk"/>
Description	<input type="text" value="sip_trunk"/> X
Device Pool *	Default ▼
Common Device Configuration	< None > ▼
Call Classification *	Use System Default ▼
Media Resource Group List	< None > ▼
Location *	Hub_None ▼
AAR Group	< None > ▼
Tunneled Protocol *	None ▼
QSIG Variant *	No Changes ▼
ASN.1 ROSE OID Encoding *	No Changes ▼
Packet Capture Mode *	None ▼
Packet Capture Duration	<input type="text" value="0"/>

Step 7 Under SIP Information, enter the following.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration ▼ Go

admin | Search Documentation | About | Logout

System ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼ Device ▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼

Trunk Configuration Related Links: Back To Find/List ▼ Go

Save

Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name *	<input type="text" value="sip_trunk"/>
Description	<input type="text" value="sip_trunk"/> X
Device Pool *	Default ▼
Common Device Configuration	< None > ▼
Call Classification *	Use System Default ▼
Media Resource Group List	< None > ▼
Location *	Hub_None ▼
AAR Group	< None > ▼
Tunneled Protocol *	None ▼
QSIG Variant *	No Changes ▼
ASN.1 ROSE OID Encoding *	No Changes ▼
Packet Capture Mode *	None ▼
Packet Capture Duration	<input type="text" value="0"/>

Field	Setting
Destination Address	Enter the IP address of the Cisco TCS to which CUCM will connect.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “Create the SIP Trunk Security Profile” procedure on page 3-15 . For example, click “Cisco TCS SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile” procedure on page 3-17 . For example, select “Cisco TCS 6.2 SIP Profile.”

Step 8 Click **Save**.
SIP Trunk created successfully.

Step 9 Click **Reset**.

SIP Route pattern Configuration Setting:

There are two way to configure call Routing for a SIP Trunk:

1. Using Route pattern (For IP Address/ Domain based Routing).

- Recording Alias URI Suffix on TCS should match with suffix based SIP route pattern that configured on CUCM.

Eg: If SIP route pattern configured on CUCM is '@tcs-cisco.com' then the recording alias URI configured on TCS must be 'xxx@tcs-cisco.com'.

2. Using Number Based Routing.

- Recording Alias URI Suffix on TCS should match with IP or FQDN configured on CUCM SIP trunk created for TCS.

Eg: If number based route pattern configured on CUCM is 555X, then the recording alias URI configured on TCS must be '555X@<IP>' or 'FQDN configured on CUCM Sip Trunk for TCS'.

In Cisco Unified Communications Manager Administration, use the Call Routing > SIP Route Pattern menu path to configure SIP route patterns.

CUCM uses SIP route patterns to route or block both internal and external calls.

The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.



Note Because no default SIP route patterns exist in CUCM, the administrator must configure them. Domain name examples: cisco.com, my-pc.cisco.com, *.com, rtp-ccm[1-5].cisco.com Valid characters for domain names: [, - , . , 0-9, A-Z, a-z, *, and]. IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18/21 (IP subnet). Valid characters for IP addresses: 0-9, ., and /

Field	Description
Pattern Usage	(Required) From the drop-down list, choose either Domain Routing or IP Address Routing.
IPv4 Pattern	<p>(Required) Enter the domain, sub-domain, IPv4 address, or IP subnetwork address.</p> <p>If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.</p> <p>Note For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the address that will be the network address.</p>
IPv6 Pattern	<p>Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6.</p> <p>If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 Pattern.</p>
Description	For this optional entry, enter a description of the SIP Route Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the Find button displays next to the drop-down list box. Click the Find button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click Add Selected.
SIP Trunk	(Required) Use the drop-down list to choose the SIP trunk to which the SIP route pattern should be associated.
Block Pattern	If you do not want this pattern to be used for routing calls, click the Block Pattern check box.

Calling Party Transformation

Field	Description
Use Calling Party's External Phone Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place.
Prefix Digits (Outgoing Calls)	<p>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9 and the wildcard characters asterisk (*) and octothorpe (#).</p> <p>Note The appended prefix digit does not affect which directory numbers route to the assigned device.</p>
Calling Line ID Presentation	<p>Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis.</p> <p>Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this SIP route pattern.</p> <p>Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number.</p>
Calling Line Name Presentation	<p>Cisco Unified Communications Manager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis.</p> <p>Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party name on the called party phone display for this SIP route pattern.</p> <p>Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified Communications Manager to display the calling name information. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling name information.</p>
Connected Party Transformations	

Field	Description
Connected Line ID Presentation	<p>Cisco Unified Communications Manager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis.</p> <p>Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party phone number on the calling party phone display for this SIP route pattern.</p> <p>Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party phone number.</p>
Connected Line Name Presentation	<p>Cisco Unified Communications Manager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis.</p> <p>Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party name on the calling party phone display for this SIP route pattern.</p> <p>Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party name. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party name.</p>

The screenshot displays the 'SIP Route Pattern Configuration' page in the Cisco Unified CM Administration console. The page is titled 'SIP Route Pattern Configuration' and includes a 'Save' button at the top left. The 'Status' section shows 'Status: Ready'. The 'Pattern Definition' section contains the following fields:

- Pattern Usage: Domain Routing (dropdown)
- IPv4 Pattern: (text input)
- IPv6 Pattern: (text input)
- Description: (text input)
- Route Partition: < None > (dropdown)
- SIP Trunk/Route List: -- Not Selected -- (dropdown with an 'Edit' link)
- ☐ Block Pattern

The 'Calling Party Transformations' section contains the following fields:

- ☐ Use Calling Party's External Phone Mask
- Calling Party Transformation Mask: (text input)
- Prefix Digits (Outgoing Calls): (text input)
- Calling Line ID Presentation: Default (dropdown)

Configuring Route Patterns Using Route Group/ Route List

A route pattern is a string of digits (an address) and a set of associated digit manipulations that can be assigned to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

Configuring Route Group

A route group allows you to designate the order in which gateways and trunks are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

The following procedure describes how to configure a route group:

- Step 1** Choose **Call Routing > Route/Hunt > Route Group**.
- Step 2** Add a new route group, click the Add New button, and continue with Step 3.
- Step 3** In the Route Group Configuration window that displays, enter a name in the Route Group Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.
- Step 4** Choose the appropriate settings as described in Table.



Note You must choose at least one device for a new route group before adding the new route group.

- Step 5** Click **Save**.

Field	Description
Route Group Information	
Route Group Name	Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.
Distribution Algorithm	<p>Choose a distribution algorithm from the options in the drop-down list box:</p> <ul style="list-style-type: none"> • Top Down—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member. • Circular—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which Cisco Unified Communications Manager most recently extended a call. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group. <p>The default value specifies Circular.</p>
Route Group Member Information	
Find Devices to Add to Route Group	

Field	Description
Device Name contains	<p>Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box.</p> <p>Note To find all available devices, leave the text box blank and click the Find button.</p>
Available Devices	<p>Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group.</p> <p>If the route group contains a gateway that uses the QSIG protocol, only gateways that use the QSIG protocol display in the list. If the route group contains a gateway that uses the non-QSIG protocol, gateways that use the controlled intercluster trunks, which are QSIG protocol do not display in the list.</p> <p>If you included the route group in a route list that contains QSIG gateways, the H.323 gateways do not display in the list.</p>
Port(s)	<p>If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (All or None Available, depending upon the device that is chosen). For a device that has no ports available (None Available), the device may be already added to the Route Group, or cannot be added to the route group.</p>
Current Route Group Members	
Selected Devices	<p>To change the priority of a device, choose a device name in the Selected Devices list box. Move the device up or down in the list by clicking the arrows on the right side of the list box.</p> <p>To reverse the priority order of the devices in the Selected Devices list box, click Reverse Order of Selected Devices.</p> <p>For more information about the order of devices in a route group, see “Route Plan Overview” in the Cisco Unified Communications Manager System Guide.</p>
Removed Device	<p>Choose a device in the Selected Devices list box and add it to the Removed Devices list box by clicking the down arrow button between the two list boxes.</p> <p>Note You must leave at least one device in a route group.</p>
Route Group Members	
List of Device	<p>This pane displays links to the devices that have been added to this route group. Click one of the device names to go to the configuration window for that particular device.</p> <p>Note When you are adding a new route group, this list does not display until you save the route group.</p>

Route List Configuration

A route list associates a set of route groups in a specified priority order. A route list then associates with one or more route patterns and determines the order in which those route groups are accessed. The order controls the progress of the search for available devices for outgoing calls.

A route list can contain only route groups.

Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified Communications Manager can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

A Route Group can be added to any number of Route Lists.

The following procedure describes how to configure a route list:

Step 1 Choose **Call Routing > Route/Hunt > Route List**.

Step 2 Click **Add New**.

Step 3 In the Route List Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan.

Step 4 From the drop-down list box, choose a Cisco Unified Communications Manager group.



Note

The Route List registers with the first Cisco Unified Communications Manager in the group which is its primary Cisco Unified Communications Manager.



Note

If you choose a Cisco Unified Communications Manager group that has only one Cisco Unified Communications Manager configured, you receive the following warning:



Warning

The selected Cisco Unified Communications Manager Group has only one Cisco Unified Communications Manager configured. For the control process to have redundancy protection, please select a Cisco Unified Communications Manager Group with more than one Cisco Unified Communications Manager

Step 5 Click **Save**.



Note

A popup message reminds you that you must add at least one route group to this route list for it to accept calls.

The Route List Configuration window displays the newly added route list.

Step 6 By default, the system checks the Enable this Route List check box for the new route list.



Note

If you want to disable this route list, uncheck this check box. A popup window explains that calls in progress are not affected, but this route list will not accept additional calls.

Step 7 Add at least one route group to the new route list.

To add a route group to this list, click **Add Route Group** and perform Step 4 through Step 8 of the “Adding Route Groups to a Route List” section.



Note For called party and calling party transformation information, you can click the name of a route group that belongs to this route list. The route group names display in the Route List Details list box at the bottom of the Route List Configuration window. This action displays the Route List Detail Configuration window for the route group that you choose.

Adding Route Groups to a Route List

You can add route groups to a new route list or to an existing route list. Route groups can exist in one or more route lists. The following procedure describes adding a route group to an existing route list.

The following procedure describes to adding route groups to a route list:

-
- Step 1** Choose **Call Routing > Route/Hunt > Route List**.
 - Step 2** Click **Add Route Group**.
The Route List Detail Configuration window displays.
 - Step 3** From the Route Group drop-down list box, choose a route group to add to the route list.
 - Step 4** If you need to manipulate the calling party number on calls that are routed through this route group, set up the calling party transformations in the appropriate fields.
 - Step 5** If you need to manipulate the dialed digits on calls that are routed through this route group, set up the called party transformations in the appropriate fields.
 - Step 6** Click **Save**.
The route group details information appears in the Route List Details list on the left side of the window.
 - Step 7** Click **Add Route Group** and repeat Step 3 through Step 7, to add more route groups to this list.
 - Step 8** Click **Save**.
 - Step 9** Click **Reset** for changes to take effect. When the popup windows display, click **OK**.
-

Configuring Route Pattern

The following procedure describes how to configure a route pattern:

-
- Step 1** Choose **Call Routing > Route/Hunt > Route Pattern**.
 - Step 2** Click the Add New Button and continue with step 3.
 - Step 3** .Choose the gateway or route list for which you are adding a route pattern.

Step 4 Click **Save**.

Field	Description
Pattern Definition	
Route Pattern	<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 Ensure that the directory route pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report.</p>
Route Partition	<p>If you want to use a partition to restrict access to the route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the route pattern, choose <None> for the partition.</p> <p>You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Partitions window. Find and choose a partition name by using the Finding a Partition procedure in the Cisco Unified Communications Manager Administration Guide.</p> <p>Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAAdmin Parameters.</p> <p>Note Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</p>
Description	Enter a description of the route pattern.
Numbering Plan	Choose a numbering plan
Route Filter	<p>If your route pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.</p> <p>The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</p> <p>You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Route Filters window.</p>

Field	Description
MLPP Precedence	<p>Choose an MLPP precedence setting for this route pattern from the drop-down list box:</p> <ul style="list-style-type: none"> Flash Override—Second highest precedence setting for MLPP calls. Flash—Third highest precedence setting for MLPP calls. Immediate—Fourth highest precedence setting for MLPP calls. Priority—Fifth highest precedence setting for MLPP calls. Routine—Lowest precedence setting for MLPP calls. Default—Does not override the incoming precedence level but rather lets it pass unchanged.
Gateway/Route List	<p>Choose the gateway or route list for which you are adding a route pattern.</p> <p>If the gateway is included in a Route Group, this drop-down list box does not display the gateway. When a gateway is chosen in the drop-down list box, Cisco Unified Communications Manager uses all the ports in the gateway to route/block this route pattern. This action does not apply for MGCP gateways.</p>
Route Option	<p>The Route Option designation indicates whether you want this route pattern to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button.</p> <p>If you choose the Block this pattern radio button, you must choose the reason for which you want this route pattern to block calls. Choose a value from the drop-down list box.</p> <ul style="list-style-type: none"> No Error Unallocated Number Call Rejected Number Changed Invalid Number Format Precedence Level Exceeded
Call Classification	<p>Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. The default value specifies OffNet. When adding a route pattern, if you uncheck the Provide Outside Dial Tone check box, you set Call Classification as OnNet.</p>
Allow Device Override	<p>This check box remains unchecked by default. When the check box is checked, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet.</p>
Provide Outside Dial Tone	<p>Check this check box to provide outside dial tone. To route the call in the network, leave the check box unchecked.</p>

Field	Description
Allow Overlap Sending	<p>With overlap sending enabled, when Cisco Unified Communications Manager passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Check this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending.</p> <p>The CMC and FAC features do not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Require Forced Authorization Code or the Require Client Matter Code check box, the Allow Overlap Sending check box becomes disabled.</p>
Urgent Priority	<p>If the dial plan contains overlapping route patterns, Cisco Unified Communications Manager would not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately.</p>
Require Forced Authorization Code	<p>If you want to use forced authorization codes with this route pattern, check this check box.</p> <p>The FAC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code check box becomes disabled.</p>
Authorization Level	<p>Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern.</p> <p>To activate the authorization code, you must check the Require Forced Authorization Code. If you do not check the check box, a message displays when you insert the route pattern that indicates that the authorization code cannot be activated. To activate the code, click Cancel, check the Require Forced Authorization Code check box, and click Insert. To activate the code at a later time, click OK.</p>
Require Client Matter Code	<p>If you want to use client matter codes with this route pattern, check this check box.</p> <p>The CMC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Client Matter Code check box become disabled.</p>

Calling Party Transformations

Field	Description
Use Calling Party's External Phone Number Mask	<p>Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.</p> <p>Note The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list.</p>
Calling Party Transform Mask	<p>Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place.</p>
Prefix Digits (Outgoing Calls)	<p>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank.</p> <p>Note The appended prefix digit does not affect which directory numbers route to the assigned device.</p>
Calling Line ID Presentation	<p>Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis.</p> <p>Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern.</p> <p>Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number.</p>
Calling Name Presentation	<p>Cisco Unified Communications Manager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis.</p> <p>Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party name on the called party phone display for this route pattern.</p> <p>Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified Communications Manager to display the calling name information. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling name information.</p>
Connected Party Transformations	

Field	Description
Connected Line ID Presentation	<p>Cisco Unified Communications Manager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis.</p> <p>Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party phone number on the calling party phone display for this route pattern.</p> <p>Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party phone number.</p>
Connected Name Presentation	<p>CUCM uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis.</p> <p>Choose whether you want CUCM to allow or restrict the display of the connected party name on the calling party phone display for this route pattern.</p> <p>Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party name. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party name.</p>
Called Party Transformations	
Discard Digits	<p>From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this route pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</p> <p>Note The called party transformation settings that are assigned to the route groups in a route list override any called party transformation settings that are assigned to a route pattern that is associated with that route list.</p>
Called Party Transform Mask	<p>Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If the field is blank, no transformation takes place. CUCM sends the dialed digits exactly as dialed.</p>
Prefix Digits (Outgoing Calls)	<p>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank.</p> <p>Note The appended prefix digit does not affect which directory numbers route to the assigned device.</p>
ISDN Network-Specific Facilities Information Element	
Network Service Protocol	<p>From the Network Service Protocol drop-down list box, choose the PRI protocol that matches the protocol of the terminating gateway.</p>

Field	Description
Carrier Identification Code	<p>Enter the appropriate carrier identification code (0, 3, or 4 digits) in the Carrier Identification Code field. Carrier identification codes allow customers to reach the services of interexchange carriers.</p> <p>The following list shows examples of commonly used carrier identification codes:</p> <ul style="list-style-type: none"> • ATT—0288 • Sprint—0333 • WorldCom/MCI—0222 <p>For a complete list of NANP carrier identification codes, go to http://www.nanpa.com/.</p>
Network Service	Choose the appropriate network service. The values vary depending on the network service protocol that you choose from the Network Service Protocol field.
Service Parameter Name	This field displays the service parameter name that is associated with the chosen network service. If no service parameter exists for the network service, the field displays <Not Exist>.
Service Parameter Value	Enter the appropriate service parameter value. Valid entries include the digits 0 through 9. If a service parameter does not exist for the network service, Cisco Unified CM Administration disables this field.

Cisco Content Server Cluster Configuration

To Content Server cluster configuration:

- [Create the SIP Trunk Security Profile](#)
- [To Create the SIP Profile](#)
- [Create the SIP Trunk](#)

Complete these steps in the order given:

Create a Route Group (for a TCS Cluster)

-
- Step 1** On the Call Routing menu, click **Route/Hunt > Route Group**.
- Step 2** On the Find and List Route Groups page, click **Add New**.
- Step 3** On the Route Group Configuration page, enter the following settings.

Field	Setting
Route Group Name	Enter Route Group name.
Distribution Algorithm	Click Top Down .

- Step 4** Confirm that both SIP trunks appear in the Available Devices field. Otherwise, click **Find**.

- Step 5** Click **Add to Route Group**.
- Step 6** Under Current Route Group Members, confirm that the SIP trunk that connects to the subscriber TCS 6.2 appears first in the list. You can select the up or down arrows to change the order of the SIP trunks.
- Step 7** Click **Save**.

Create a Route List (for a TCS Cluster)

- Step 1** On the Call Routing menu, click **Route/Hunt > Route List**.
- Step 2** On the Find and List Route Lists page, click **Add New**.
- Step 3** On the Route List Configuration page, enter the following settings.

Field	Setting
Name	Enter SIP_Trunk_Route_List or another name.
Description	Enter SIP Trunk Route List or another description.
Cisco Unified Communications Manager Group	Click Default .

- Step 4** Click **Save**.
- Step 5** Confirm that the **Enable This Route List** check box is checked.
- Step 6** Under Route List Member Information, click **Add Route Group**.
- Step 7** On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the [Create a Route Group \(for a TCS Cluster\)](#) and click **Save**.
- Step 8** When prompted that the route list settings will be saved, click **OK**.
- Step 9** On the Route List Configuration page, click **Reset**.
- Step 10** When prompted to confirm resetting the route list, click **Reset**.
- Step 11** Click **Close**.

Create a Route Pattern (for a TCS Cluster)

- Step 1** On the Call Routing menu, click **Route/Hunt > Route Pattern**.
- Step 2** On the Find and List Route Patterns page, click **Add New**.
- Step 3** On the Route Pattern Configuration page, enter the following settings.
- Step 4** Click **Save** and then click **Close**.

Field	Setting
Route Pattern	Enter the route pattern for TCS trunk.
Gateway/Route List	Select the name of the route list that you created in the Create a Route List (for a TCS Cluster) . For example, click “SIP_Trunk_Route_List.”

Region configuration on CUCM

- Step 1** Login to the **Cisco Unified Communication Manager Administration** Interface.
- Step 2** Select **System > Region Information > Region**.
- Step 3** Click **Find**.
- Step 4** Select **Default**.
- Step 5** Under the **Maximum Session Bit rate for Video Calls** section, select the last radio button and enter **32000 kbps** as highlighted in the snapshot.

Region Configuration

Save Delete Reset Apply Config Add New

Region Information

Name * Default

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	32000 kbps
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default

Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
Default	Keep Current Setting	Keep Current Setting	Keep Current Setting
		kbps	Use System Default
			None
			kbps

Save Delete Reset Apply Config Add New

CUCM Configuration Setting on Content Server

After ensuring that CUCM and Content Server are ready for the integration, do the following procedure to set up the integration and to enter the port settings.

To Create the Integration

- Step 1** In Content Server Administration, expand the Management tab, go to **Configuration> Site Setting >SIP Setting**.

- Step 2** Check the **SIP enabled** check box to enable registration with a SIP registrar.
- Step 3** Enter the display name in the **SIP display name** text box.
- Step 4** Enter the SIP address in the **SIP address URL** text box.
- Step 5** Select the registration mode of the content server in the **Registration** field. The available options are **Terminal** or **Trunk**.
- Step 6** Select the time interval in seconds, in the **Trunk Peer Polling Interval** drop-down.
- Step 7** Enter the playback domain suffix.



Note This option will display, if SIP is in Trunk mode.

- Step 8** Enter the server address in the **Server address** text box.
- Step 9** Select the transport protocol from the **Transport** drop-down. The available options are **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol).
- Step 10** In the User name text box, leave the box blank.
- Step 11** In the Password text box, leave the box blank.



Note The **User name** and the **Password** is not required as authentication is not enabled in CUCM SIP Trunk profile.



Content Server VM with BE6K

Introduction

Cisco Business Edition 6000 (BE6K) is a packaged solution optimized for medium-sized business requirements. It offers the mid-size business reduced the cost through server consolidation, operational efficiency, and scalability.

This chapter describes the main features, system requirements, setup, and management of the BE6K solution. Configuration of BE6K is performed on the Management tab. You must have the role of site manager or system administrator to see the Management tab.

Content Server VM with BE6K Features:

These are the supported media format:

- MPEG-4 for playback using Quick Time.
- MPEG-4 for playback using Flash Player.

These features are supported in Content Server Release 6.2:

- One Live Streaming recording in FLASH or QT with output sizes as small, medium or large using External Streaming Server.
- One On-Demand recording in FLASH or QT with output sizes as small, medium or large using Internet Information Server (IIS) as well as External Media Server.
- HD video.

These features are not supported:

- In-Box streaming
- WMV format
- Content Server Cluster

For installing the Virtual Content Server on BE6K, refer [Cisco TelePresence Content Server VM Installation Guide](#).

For the information regarding licensing, refer [Cisco TelePresence Content Server Licensing Information Virtual Content Server on BE6K Features](#)

UI changes on Content Server for BE6K solution

Management Tab

Following are the pages updated for BE6K solution:

1. Management Tab > Server Overview > **Current Calls**

Only two Concurrent calls are supported for BE6K solution.

Figure 4-1 Server Overview

The screenshot displays the 'Server overview' page in the Cisco TelePresence Content Server management interface. The page is organized into several sections:

- Content Server status:** Shows 'Server mode' as Online, 'Content Engine status' as a green checkmark, 'Current calls' as 0, 'Transcode Engine status' as a green checkmark, and 'Currently transcoding' as No.
- Content Server information:** Lists 'IP Address', 'Device serial number', 'Software version' (Cisco TelePresence Content Server v6.2 Build 3546), and 'Installed option keys'.
- Server disk space:** A table showing disk usage for paths C and E.

Path	Total disk space	Free disk space	Percentage free
C	22.5 GB	7.46 GB	33%
E	127 GB	46.1 GB	43%
- Database location:** Shows 'Database data source' as Local Content Server and 'Database name' as TCSDb3.
- Media storage location:** Includes a note about changing the media storage location via remote desktop and the 'TC3 Wizard'. The 'Media storage location' is set to Local Content Server.
- Software option:** Includes an 'Add option key' field and a 'Restart service' button.

2. Management Tab> Manage Outputs> **On Demand Formats**

BE6K solution does not support the Window Media Format for playback.

Figure 4-2 Manage Output

Save Return

Manage outputs

wowza_live 10 Oct 14 3:05 PM

Recording call speed (kbps): 1152

Recorded with dual stream: No

Choose how you want to make this recording available and edit your options below:

☒ Viewable in the Content Server web interface Choose options

☐ Downloadable for portable devices (iPod and Zune)

☐ Downloadable for general purpose

☐ Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U

Outputs to view in the Content Server web interface

Outputs to view in the Content Server web interface

Single video

On demand

Formats

MPEG-4 for QuickTime

MPEG-4 for Flash

Sizes (choose up to 2)

Audio only

Small

Medium

Large

Bit rates (kbps)

Small: 250

Medium: 800

Large: 1728

On demand media server configuration settings

MPEG-4 for QuickTime Local IIS Web Server

MPEG-4 for Flash Local IIS Web Server

Optimize for motion ☐

3. Management Tab> Create recordings>Recording alias

Default Live and OnDemand recording alias is not supported in BE6K solution.

Figure 4-3 Recording alias

View Recordings

Management

Cisco TelePresence Content Server

System Administrator (WIN-NT5AIKDD7VS\Administrator) Log out
Select language

Diagnostics

Recordings

Recording setup

Configuration

Help

Recording aliases

<input type="checkbox"/>	Name ▲	H.323 ID	E.164 alias	SIP address (URI)	Owner
<input type="checkbox"/>	Default OnDemand only Edit	OnDemand4E58E408			WIN-NT5AIKDD7VS\Administrator
Delete selected					

4. Management Tab> Template

Window Media Format is not supported for BE6K solution.

**Note**

Default Flash Single on Demand Only and Default Flash Stacked on Demand Only template are enabled by default.

Figure 4-4 *Templates*

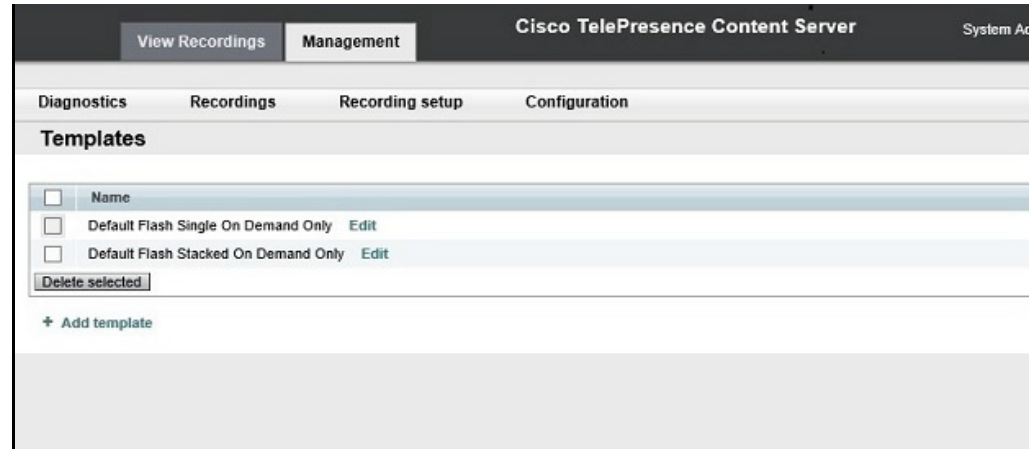
The screenshot shows the 'Add template' configuration page in the Cisco TelePresence Content Server Management interface. The page is titled 'Add template' and includes a 'Save' button and a 'Return' button. Below the buttons, there is a 'Template' section with a 'Name' input field. A message states: 'Choose how you want to make any recordings made with this template available and edit your options below:'. There are four checkboxes: 'Viewable in the Content Server web interface' (checked), 'Downloadable for portable devices (iPod and Zune)', 'Downloadable for general purpose', and 'Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U'. Below these is an 'Outputs to view in the Content Server web interface' section with four radio button options: 'Switching' (selected), 'Joined', 'Stacked', and 'Picture in picture'. There is also a 'Force 18:9' checkbox. The 'On demand' section includes a 'Formats' dropdown menu with 'MPEG-4 for QuickTime' and 'MPEG-4 for Flash' (selected). There is a 'Sizes (choose up to 2)' dropdown menu with 'Audio only', 'Small', 'Medium' (selected), and 'Large'. To the right, there is a table for 'Maximum target bit rates (kbps)':

Size	Maximum target bit rates (kbps)
Small	250
Medium	800
Large	Maximum

5. Management Tab> Add Templates> [Viewable in the Content Server web interface](#)

BE6K user can edit the options to make any recordings.

Figure 4-5 Add Template



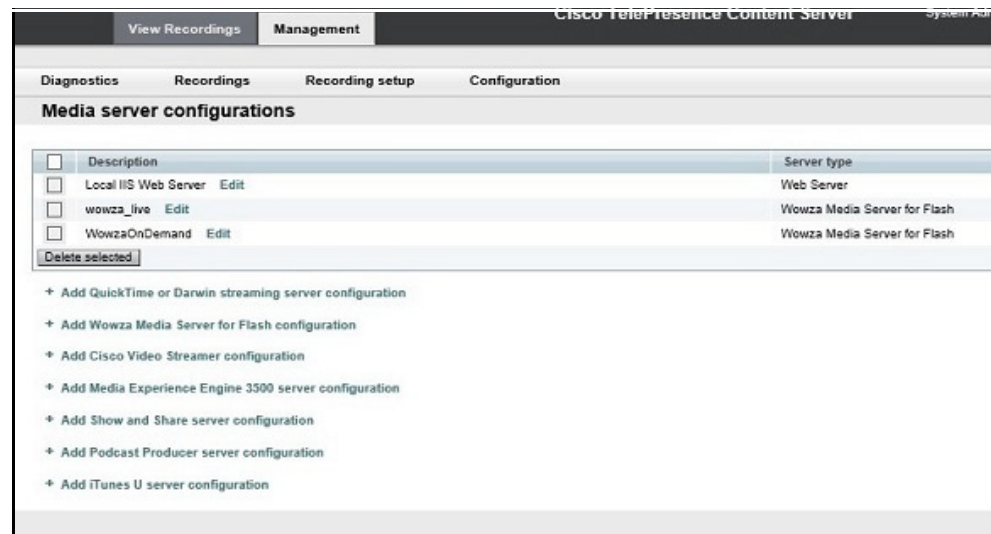
6. Management Tab> Recording Setup> Media Server Configurations

BE6k solution does not supports the External Windows Media Streaming servers.

The supported formats are:

- Add Quick Time or Darwin streaming server configuration
- Add Wowza Media server for Flash configuration, etc.

Figure 4-6 Media server configuration



7. Management Tab> Configuration> Site Setting> Preferred player

BE6K, Flash is the preferred player to view recordings.

Figure 4-7 *Advanced streaming options*

Advanced streaming options

Target bit rates ⓘ

Small

Up to kbps ⓘ

Allowed range: 150 - 512 kbps.

Medium

Up to kbps ⓘ

Allowed range: 512 - 1152 kbps.

Large

Maximum ⓘ

Preferred player

ⓘ

Save

Return



Supported Platforms, Browsers, and Plug-ins

[Table 5-1](#) describes the supported platforms, browsers, and plug-ins for Content Server Release 6.0.x and Release 6.2.1 software.

Table 5-1 *Supported Platforms, Browsers, and Plug-ins*

Operating System	Browsers	Silverlight ¹	Flash ²	Windows Media Player	QuickTime ³
Windows	Mozilla Firefox 26, 27, 27.0.1	5.1	12.0	12.0	7.6.80
	Internet Explorer 9, 10, 11	5.1	11.7	12.0	7.6.80
Mac version 10.5 or higher	Mozilla Firefox 3.6.x and 21 ⁴	5.1	11.7	Not supported	7.6.6
	Safari 6	5.1	11.7	Not supported	7.6.6

1. Requires Silverlight plugin 5.1.20913.0
2. Requires Shockwave Flash 12.0.0.44
3. Requires QuickTime plugin 7.6
4. Firefox 21 requires Shockwave for Director Version 12.0.2.122

Microsoft Internet Explorer 11 HTTP Login Error

When using IE 11 to access a Content Server with a self-signed certificate, HTTP login is not allowed. Instead, the browser returns a certificate blocking error “Continue to this website (not recommended)”.

These are the workarounds:

- Install an SSL certificate signed by a certificate authority on the Content Server. For more information, see the [Cisco TelePresence Content Server Release 6.x Public SSL Certificate Installation Guide](#) on Cisco.com.
- Install the Content Server default self-signed certificate in the browser’s Trusted Root certificate authority.
- Use HTTPS login—Ignore the warning page and continue to the Content Server UI. Internet Explorer will remember the certificate while the browser is open. You can return to the site without receiving another warning for the certificate until IE is restarted.

Microsoft Windows Media Browser Plugin

The Microsoft Windows Media browser plug-in is required to display movies in the legacy player in Windows Media WMV format in Mozilla Firefox. The browser plug-in is available as a free download at the time of publishing from the URL:

<http://www.interoperabilitybridges.com/windows-media-player-firefox-plugin-download>

See the [Release Notes](#) for open caveats that are applicable to the supported browsers and plug-ins.



Creating and Managing a Content Server Cluster

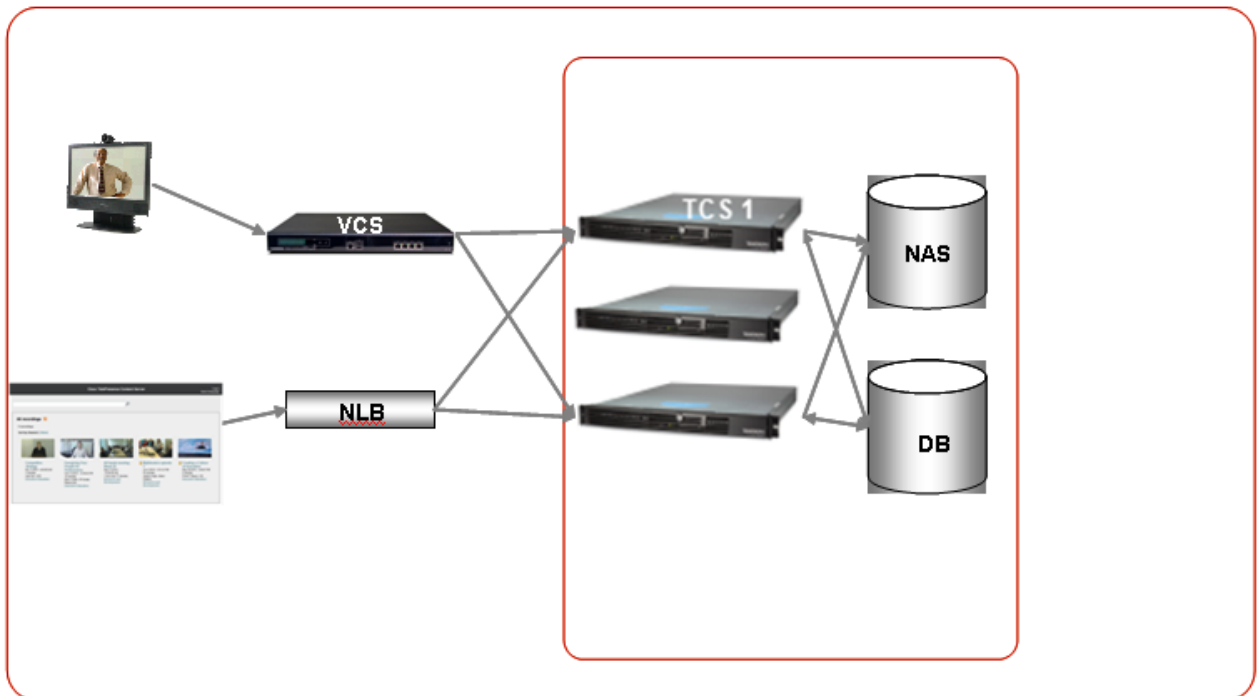
This chapter describes the main features, system requirements, setup, and management of a Cisco TelePresence Content Server cluster. A Content Server cluster has a much greater capacity for recording, streaming, and serving the web interface.

- [About Content Server Clusters, page 6-2](#)
- [System Requirements, page 6-4](#)
- [Important Guidelines, page 6-5](#)
- [Setting up a Content Server Cluster, page 6-6](#)
- [Managing a Content Server Cluster, page 6-23](#)
- [Removing a Content Server from the Cluster, page 6-30](#)
- [Using TMS to Schedule Calls on a Content Server Cluster, page 6-31](#)
- [Backing Up and Restoring the Content Server Cluster, page 6-32](#)
- [Upgrading the Cluster to a New Software Version, page 6-33](#)
- [Upgrading the External Microsoft SQL Server, page 6-33](#)

About Content Server Clusters

You can cluster multiple Content Servers to increase total recording and playback capacity. In a cluster architecture, there is no controller; each Content Server performs exactly the same tasks. If a Content Server is taken out of the cluster, the only effect on the cluster is a decrease in the total capacity of recording and playback.

You can manage a cluster from any Content Server in the cluster. The Cluster Overview page provides information about the number of calls and transcoding jobs in progress on the cluster members, along with the calls, transcoding jobs, and the status of essential services on each Content Server in the cluster.



HTTP Load Balancing

The use of a network load balancing (NLB) solution ensures that incoming user HTTP requests are spread across the cluster. While multiple solutions are available to manage NLB, the recommendation in this document is a hardware solution: Loadbalancer.org.

Inbound H.323 Call Routing

Inbound call load balancing is managed by the Video Communications Server (VCS) to which the cluster is registered. Each Content Server is capable of two transcoded live streaming outputs out of a total call capacity of five calls. Using a live streaming alias means that others can watch the recording while it is in progress and then also view the recording on demand later. Using a non-live streaming alias means that the call is recorded, but it cannot be viewed until recording is finished and the offline transcoder has processed the output for on-demand viewing.

While standalone Content Servers have a mixture of live and non-live aliases, they only require one gateway prefix for both. However, a Content Server cluster requires two gateway registrations with separate prefixes—one for live transcoded calls and one for non-live (offline transcoded) calls. This ensures good load balancing of both types of calls across the cluster. Resource Allocation Indication

messages are used to signal the VCS when a Content Server in the cluster is out of resources for a particular call type. These messages allow the gatekeeper to route calls appropriately. A Content Server that signals that it is out of resources for a live call type prefix will not be allocated any more calls on that prefix until it signals that resources are available.

Additionally, for registrations with the VCS, each Content Server needs four system aliases: live H.323 ID and E.164 and non-live H.323 ID and E.164. It is important that each of these aliases is unique on each Content Server and in the cluster. There must be no duplicate aliases.

System aliases should not be used for calling the cluster, as they are routed to a particular Content Server. If the Content Server is busy, calls to its system alias will be rejected even if other Content Servers are not busy at that time. Calls are appropriately load balanced across the cluster only when recording aliases are used for dialing a cluster.

Outbound H.323 Calls Load Balancing

Outbound calls can be made by using the web interface or the ClusterDial API command. Load balancing is based on current call load; the Content Server with the smallest call load is chosen to handle the call. Because there is no controller in the cluster architecture, the API commands can be sent to any of the Content Servers in the cluster. For added API redundancy, and to ensure that the external implementation does not artificially create a controller, you should distribute the API commands among all Content Servers in the cluster to manage server availability.

Scalable Storage

One Network Attached Storage (NAS) is used for the entire cluster. All media files are hosted on the NAS. Using NAS ensures that storage can grow as the cluster grows and is not constrained by the Content Server hardware capacity. Because transcoded media files are stored on the NAS, on-demand streaming of any recording is possible from any Content Server.

External Microsoft SQL Server Database

All Content Servers in the cluster connect to one external Microsoft SQL Server 2005 or 2008 database. Using one SQL server ensures that cluster configurations and recording information are global across the cluster. If a Content Server is taken out of the cluster, the recordings that were created by that Content Server are accessible from the interface of any of the other Content Servers remaining in the cluster.

It is the responsibility of the cluster implementer to provide the external Microsoft SQL Server 2005 or 2008 instance. It should be noted that the SQL server instance on a Content Server cannot be used to configure an external database for other Content Servers in the cluster. While there are multiple ways to configure external databases, configurations that are required for the correct functioning of a cluster are described in more detail later in this document.

API Support

The cluster is supported by the Application Programmer Interface (API) that provides a special command for dialing out of the cluster. The API also provides cluster status documents that report status and configuration across all nodes. The cluster API commands are documented in the [Cisco TelePresence Content Server API Guide](#) on Cisco.com.

System Requirements

Content Server Release 6.1 or 6.2 Requirements

- Third-generation Content Server hardware running software Release 6.1 or 6.2.
- Server hardware running VM Content Server Release 6.1 or 6.2.

Content Server Release 6.0.x Requirements

- Third-generation Content Server hardware running software Release 6.0.x.

Content Server Requirements for All Software Versions

- Each Content Server in the cluster and the NAS must be added to the same Windows Active Directory domain.
- A Cluster Enabled option key installed on each Content Server that is going to be added to a cluster. The option key must be installed before running the Content Server Wizard so that the clustering option is accessible in the wizard.
- A valid HTTPS security certificate from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.) installed on each Content Server in the cluster.

External SQL Server database

- Microsoft SQL Server 2005 (Service Pack 2 or higher) or Microsoft SQL Server 2008 Standard or Enterprise supported by S4.x. The cluster requires an external database instance to be configured on a separate machine (not a Content Server).
- The database server requires dual 3 GHz processors and a minimum of 4 GB RAM.
- Microsoft .NET Framework 2 or higher must be installed on the server where the Microsoft SQL Server is installed.

See the [“Configure the External SQL Server Database” section on page 6-7](#) for information about database configuration.

Gatekeeper

- Video Communications Server (VCS) X2.1 or higher.
- Cisco Unified Communication Manager (CUCM) 9.1.2 or 10.2 (support from TCS Release 6.2 onwards).

Network Attached Storage (NAS)

- Compatible systems include any NAS device built on the Windows Storage server and that is Windows Hardware Quality Lab certified. The file sharing protocol used by the Content Server to the NAS is Microsoft SMB.
- The NAS device must be added to the same Windows Domain as the Content Servers.
- The NAS should be dedicated to media storage. Installing your Domain Controller on the NAS device is not supported and might cause the Content Server cluster to stop functioning.

See [“Configure the NAS” section on page 6-11](#) for information about the required NAS share configuration.

Network Load Balancer (NLB) solution

There are a number of options for load balancing HTTP page requests.

The recommended solution for a Content Server cluster includes hardware-based NLB. This document describes the setup for a Loadbalancer.org hardware load balancer.

For installations where optimized load balancing of page requests is not important, DNS round robin can also be used.

Important Guidelines

Observe these guidelines when configuring a Content Server cluster. Also see the [Cisco TelePresence Content Server Release Notes](#) on Cisco.com for a list of other known issues for this release.

Content Server Release 6.1 or 6.2 Guidelines

- Content Servers in a cluster must all be running Release 6.1 or 6.2. You cannot mix software versions in a cluster with Content Servers running Release 6.1 or 6.2.
- Content Servers in a cluster can be a third-generation Content Servers and VM Content Servers all running software Release 6.1 or 6.2.

Content Server Release 6.0.x Guidelines

- Content Servers in a cluster must all be third-generation hardware. You cannot mix older (first- or second-generation) servers in a cluster with third-generation Content Servers.

Guidelines for All Software Versions

- This release supports up to ten Content Servers in a cluster.
- A cluster supports Content Servers with mixed 5-and-10-port capacity.
- All Content Servers in a cluster must be at the same physical site, within a network round-trip time (RTT) to the NAS and SQL servers not exceeding 10 ms.
- The solution support SIP and H.323 protocol from TCS Release 6.2 onwards. Only H.323 protocol was supported on prior to Release 6.2.
- Dialing into the cluster using the load balanced frontend address or IP addresses of Content Servers in the cluster is not supported. The cluster design relies on call balancing done by the gatekeeper, and this call balancing can occur only when recording aliases (or playback addresses in a Premium Resolution cluster) are dialed.
- Adding or removing the live output from a template results in a change of the gateway prefix of recording aliases that use the template.

For example, the live gateway prefix on your cluster is *Content Servercluster.live* and the non-live gateway prefix is *Content Servercluster.nonlive*.

A recording alias with an H.323 ID of *Content Servercluster.nonlive.myalias@company.com* uses a Windows Media switching template with no live streaming output. If a live streaming output is added to the template, the H.323 ID of the recording alias changes from *Content Servercluster.nonlive.myalias@company.com* to *Content Servercluster.live.myalias@company.com*. Calls to the original alias will fail.

- A Premium Resolution Content Server that you add to a non-Premium Resolution cluster behaves like a non-Premium Resolution Content Server until Premium Resolution keys are added to all Content Servers in the cluster. Each Content Engine checks the database at startup and once per hour to see if other Content Servers in the cluster are Premium Resolution or not. If all Content Servers are restarted after Premium Resolution keys have been added to each, the cluster behaves as a

Premium Resolution cluster immediately. If the Content Servers with newly installed Premium Resolution keys are not restarted, the cluster behaves as a Premium Resolution cluster approximately one hour after the keys are installed.

If you add a non-Premium Resolution Content Server to a Premium Resolution cluster, the cluster becomes a non-Premium Resolution cluster. If the Content Servers are restarted after the non-Premium Resolution Content Server is added, the cluster behaves as a non-Premium Resolution cluster immediately. If they are not restarted, the cluster behaves as a non-Premium Resolution cluster approximately one hour later.

See [Chapter 11, “Premium Resolution”](#) for more information about Premium Resolution.

Setting up a Content Server Cluster

Setting up a Content Server cluster consists of eight steps. To set up a cluster successfully, follow the steps in the order that is given below.

We recommend that you familiarize yourself with the [“Important Guidelines” section on page 6-5](#) before setting up a cluster.

Overview of the Process

-
- | | |
|--------|--|
| Step 1 | Content Server Cluster Prerequisites, page 6-6 |
| Step 2 | Configure the External SQL Server Database, page 6-7 |
| Step 3 | Configure the NAS, page 6-11 |
| Step 4 | About Creating a Content Server Cluster, page 6-13 |
| Step 5 | Create a New Content Server Cluster, page 6-15 |
| Step 6 | Add a Content Server to an Existing Cluster, page 6-17 |
| Step 7 | Configure Gatekeeper Registration for H.323 Cluster, page 6-18 |
| Step 8 | Configure Domain Authentication, page 6-19 |
| Step 9 | Configure Network Load Balancing (NLB), page 6-19 |
-

Content Server Cluster Prerequisites

Before creating a Content Server cluster, confirm that you have met these cluster prerequisites:

- For a mixed hardware Content Server cluster, verify that all the Content Servers are running Release 6.1 or 6.2.
- For a third-generation hardware Content Server cluster, verify that all the Content Servers are running Release 6.0.x.
- Add all Content Servers that you want to cluster to a Windows Active Directory domain. The general requirements for adding a Content Server to a Windows domain must be adhered to.

- Add the cluster option key. A cluster option key should be installed on each Content Server. To install the key, go to the **Management** tab. Then go to **Diagnostics > Server overview**, and locate the **Software option** section. The option key must be installed before running the Content Server Wizard so that the clustering option is accessible in the wizard.
- Install a security certificate from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.) on each Content Server in the cluster. Using a common certificate on all the Content Servers ensures that users do not have to obtain unique certificates for each Content Server in the cluster when they access the cluster.

For more information on installing security certificates, see the *Install a Security Certificate* section in the [Cisco TelePresence Content Server Release 6.0.x and 6.1 Quick Start Guide](#) on Cisco.com.

- Confirm that the time zone, time, and date settings are identical on all Content Servers to be clustered.

Configure the External SQL Server Database

Ensure that your existing Microsoft SQL server is compatible with the Content Server cluster system requirements (see “[System Requirements](#)” section on page 6-4).

The process of configuring the external SQL server consists of the following steps. Each step is described in a separate section:

-
- Step 1 [Add an SQL Server Instance, page 6-7](#)
 - Step 2 [Configure the SQL Server Instance, page 6-8](#)
 - Step 3 [Create a Special User on the SQL Server, page 6-10](#)
-

Add an SQL Server Instance

One SQL server database is used by all Content Servers in a cluster. This database must not be hosted on any of the Content Servers used in the cluster.

The Content Server cluster requires its own instance of the SQL server. If Microsoft SQL Server is already installed, you should add a new instance to your existing SQL server installation. If Microsoft SQL Server is not already installed, you must install it. See the “[System Requirements](#)” section on page 6-4 to ensure that you use the correct version of the SQL server installer to create the new instance.



Note

Only installation wizard steps that are required for a Content Server cluster are included in this document.

Using the Microsoft SQL Server 2005 or 2008 installation media to add a new instance:

-
- Step 1 Insert the Microsoft SQL Server installation media into the disk drive of the machine that will host your SQL server. Start the Microsoft SQL Server Installation Wizard.
 - Step 2 In Components to Install, check the **SQL Server Database Services** box.
 - Step 3 In Instance Name, click the **Named instance** radio button, and enter the instance name.
 - Step 4 In Service Account, choose Use the built-in System account (Local system, or Network service).

- Step 5** In Authentication Mode, click the **Mixed Mode (Windows Authentication and SQL Server Authentication)** radio button. Enter and confirm the SA (system administrator) password.
- Step 6** SQL server collation should be set to **Latin1_General_CI_AS, 'Dictionary, case insensitive, 1252 character set'**.



Note Don't install Reporting Services with SQL server, as it has some issues with Content Server Cluster creation.



Note For SQL Server 2005 installations, Service Pack 2 or later must be applied to the newly created instance. If you apply an earlier service pack, the Content Server Wizard database connection test fails, and you cannot create a Content Server cluster with this instance.

For more information on installing a Microsoft SQL Server, see the online documentation:

<http://msdn.microsoft.com/en-us/library/bb545450.aspx>

Configure the SQL Server Instance

To configure the SQL server instance for a Content Server cluster, follow these steps:

- Step 1** Open the SQL Server Configuration Manager (usually located from the **Start** menu under **All Programs > Microsoft SQL Server 2005 (or 2008) > Configuration Tools**).
- Step 2** In **SQL Server 2005 (or 2008) Network Configuration**, select Protocols for *instance_name*. The *instance_name* is the name you specified when creating an SQL Server instance (see the “[Add an SQL Server Instance](#)” section on page 6-7).
- Step 3** Ensure that these parameters are configured as follows:
- Shared Memory is enabled.
 - Named Pipes are disabled.
 - TCP/IP is enabled.
 - VIA is disabled.
- Step 4** Right click **TCP/IP** and click properties. Click the **IP Addresses** tab:
- For each IP address, set **Enabled** to **No**.
 - Clear all **TCP Dynamic Ports** fields. Delete any zeros that appear in those fields.
 - Clear all **TCP Ports** fields from all IP Addresses.

- d. Under **IP All**, enter the TCP port that the Content Server will use to connect to this instance:

An example for TCP Port is 2090.

You can use any port in the range of between 1000 and 64000 that is open on the firewall and is not used by other software on Content Server or on the server that is hosting the SQL server. The port that you specify here also must not conflict with ports set up for other instances on the server.

- Step 5** Click **SQL Server 2005 (or 2008) Services**, select the instance you just created, right-click, and then click **Restart Service**.
-

Create a Special User on the SQL Server

The user that you create in the following steps are used by the Content Servers to connect to the SQL server external database. For security reasons, we recommend that you do not use the existing system administrator (SA) user account. Instead, create a new user account.

The new user account requires administrative privileges and CREATE TABLE and ALTER TABLE authorization.

To create a special user on the SQL server, follow these steps:

-
- Step 1** Using the sqlcmd utility, open a command prompt on the machine on which the SQL server is running.
- Step 2** To connect to the SQL Server, enter one of the following commands:
- To use a trusted connection, enter `sqlcmd -S (local)\instance_name -E`
 - To connect with SQL authentication, enter `sqlcmd -S (local)\instance_name -U login_id -P password`
- The `instance_name` is the name you specified when creating an SQL Server instance (see the [“Add an SQL Server Instance” section on page 6-7](#)).
- Step 3** At the Command Utility prompt `1>`, enter the following command to create a user:
- ```
CREATE LOGIN user_name WITH PASSWORD='strong_password'
```
- Step 4** Add administrator permissions to the new user account.
- ```
sp_addsrvrolemember '<Login>', 'sysadmin'
```
- Step 5** At the prompt, enter **GO** and press **Enter**.
- Step 6** Enter **EXIT** and press **Enter** to exit sqlcmd.
-

This example shows how to create user Content Server_DB_USER on the SQL server:

```
C:\Documents and Settings\Administrator>sqlcmd -S (local)\my_instance -E
1> CREATE LOGIN Content Server_DB_USER WITH PASSWORD='xxxxxxxxxxxxxxxx'
2> sp_addsrvrolemember 'Content Server_db_user', 'sysadmin'
2> GO
1>EXIT
```


Configure the NAS

The Content Server cluster uses a share on the network attached storage (NAS) as its media storage location. See “[System Requirements](#)” section on [page 6-4](#) first to ensure that your NAS is compatible with Content Server cluster system requirements.

The process of configuring the NAS consists of the following steps. Each step is described in a separate section:

-
- | | |
|---------------|--|
| Step 1 | Manage the Windows Active Directory Domain, page 6-11 |
| Step 2 | Choose or Create a Domain Account to Access the NAS Share, page 6-11 |
| Step 3 | Set up a Share on the NAS, page 6-11 |
| Step 4 | Set Permissions and Security Settings on the Share, page 6-12 |
-

Manage the Windows Active Directory Domain

All Content Servers in the cluster and the NAS must be added to the same Windows Active Directory domain.

Choose or Create a Domain Account to Access the NAS Share

Choose or create a domain user. You can choose any username. In this document, we refer to this user as MYDOMAIN\Content Server_NAS_USER. MYDOMAIN\Content Server_NAS_USER is used by the Content Server cluster to access the NAS share.



Note

You must enter the username and password for MYDOMAIN\Content Server_NAS_USER when you run the Content Server Wizard.

Set up a Share on the NAS

-
- | | |
|---------------|---|
| Step 1 | Log in to the NAS by using Windows Remote Desktop Connection. |
| Step 2 | Create a folder on the NAS. |
| Step 3 | Make the folder a shared folder. |
-



Note

You must enter the path to this share when you run the Content Server Wizard.

Set Permissions and Security Settings on the Share

All Content Servers and the domain account that the Content Server cluster uses to access the share on the NAS must be given full control over the share. You must set up the NAS share correctly to successfully use the Content Server Wizard.

-
- Step 1** Right-click the shared folder and select **Properties**.
- a. Select the Sharing tab. Click **Share**.
 - b. In the File Sharing window, select a name and click **Share**; or type a name, click **Add** and then click **Share**.
 - c. In the Sharing tab, Advanced Sharing section, click **Advanced Sharing**.
 - d. Click **Permissions**. In the Select Users, Computers, Service Accounts, or Groups window:
 - Enter the DNS names of the Content Servers that you want to cluster.
 - Enter the name of the domain user (for example, *MYDOMAIN\Content Server_NAS_USER*) account.
 Click **OK**.
 - e. In the Share Permission window, give the Content Servers and the shared account full permission:
 - Select each Content Server and click **Allow** in the Full Control, Change, and Read check boxes.
 - Select the *MYDOMAIN\Content Server_NAS_USER* and click **Allow** in the Full Control, Change, and Read check boxes.
 Click **OK**.
 - f. In the Advanced Sharing window, click **Apply** to apply the configuration. Click **OK** to exit the window.
- Step 2** Click the **Security** tab.
- a. Click **Edit**. Add the Content Servers and the *MYDOMAIN\Content Server_NAS_USER* that you added in Step 1 above.
 - b. In the Security Permission window, give the Content Servers and the shared account full permission:
 - Click **Allow** in all check boxes for each of the Content Servers and the *MYDOMAIN\Content Server_NAS_USER*.
 - c. In the Advanced Sharing window, click **Apply** to apply the configuration. Click **OK** to exit the window.
 - d. Click **Apply** in the Security tab window. Click **Close** to close the Properties window.
-

About Creating a Content Server Cluster

In order to create a cluster of Content Servers, you must run the Content Server Wizard from Remote Desktop on one of the Content Servers. Then you must run the Content Server Wizard on all the remaining Content Servers to add them to the cluster. See these sections:

- [The Order of Content Servers Added to the Cluster, page 6-13](#)
- [Content Server Wizard Options, page 6-14](#)
- [User Accounts for the Content Server Wizard, page 6-14](#)
- [Before Running the Content Server Wizard, page 6-15](#)

The Order of Content Servers Added to the Cluster



Caution

If you cluster Content Servers that have existing recorded content and configurations that you want to keep, the order in which you add Content Servers to the cluster is important.

- **The first Content Server in the cluster.** Existing content and configurations (recording aliases, templates, call configurations, media servers) from the first Content Server that you use to create a new cluster are added and available to other Content Servers in the cluster.

Only the first Content Server preserves its playback addresses to play back recordings on endpoints. The playback addresses of all subsequently added Content Servers are modified to avoid duplicates.

For example, these are playback addresses of three standalone content servers:

Playback addresses for standalone Content Server 1:

- 13115 Recording 1
- 14117 Recording 2
- 21416 Recording 3

Playback addresses for standalone Content Server 2:

- 1521 Recording A
- 1635 Recording B

Playback addresses for standalone Content Server 3:

- 1521 Recording X
- 2142 Recording Y
- 21413 Recording Z

Notice that standalone Content Servers 2 and 3 have a playback address that is the same (1521). If all three Content Servers are added in order to the cluster, playback aliases are modified for all servers added after the first server to avoid duplicate aliases. The playback aliases for the servers in the cluster would look like this:

All three Content Servers in the same cluster

- 13115 Recording 1 (Content Server 1–playback aliases are retained)
- 14117 Recording 2
- 21416 Recording 3
- 101 Recording A (Content Server 2–playback aliases are modified)
- 102 Recording B
- 103 Recording X (Content Server 3–playback aliases are modified)
- 104 Recording Y

- 105 Recording Z
- **The second and any additional Content Servers.** All content from the second and any other Content Servers that you add to the cluster is imported into the cluster. The following configurations are not imported:
 - Configurations that are added include media servers associated with recordings and categories associated with recordings.
 - Configurations that are not added include recording aliases; templates; call configurations; media servers not associated with recordings; categories not associated with recordings; and LDAP servers and users.

For all Content Servers that are added to the cluster, the wizard does not move any media files that are not associated with the Content Server's database. Media files that are not moved include orphaned temporary files not used in any recordings; .tcb import or export files; or files placed in the data folder by the user. These files are not moved to the NAS from the local Content Server disk drive and are deleted. If you move media between NAS locations or from the NAS to a local Content Server disk drive, the wizard does not move or delete the files.

Content Server Wizard Options

The Content Server Wizard available as a shortcut from the Remote Desktop of the Content Server has the following options:

- Alternate Storage (NAS) Wizard for a standalone Content Server.
- Cluster Management Wizard.

If you select the Cluster Management Wizard on a standalone Content Server, you see these options:

- Create a new cluster.
- Add to an existing cluster.

If you select the Cluster Management Wizard on a clustered Content Server, you see these options:

- Generate Cluster Settings File.
- Configure Load Balancer Configuration.
- Update Cluster Settings.
- Remove from Cluster.

User Accounts for the Content Server Wizard

The Content Server Wizard can run under the following user accounts:

- A domain administrator account.
- The special domain account you set up in the [“Configure the NAS” section on page 6-11](#).
- The local default administrator account.



Note

Unless explicitly stated otherwise, this document assumes that the Content Server Wizard is run under a domain administrator account.

Before Running the Content Server Wizard

Before you run the Content Server Wizard, confirm that you have:

- Performed a backup of the Content Server
- Turned off any antivirus software
- Stopped all recordings on the Content Server

Make sure that you have the following information available:

- External SQL server IP address or name.
- Name of the SQL database instance.
- The TCP/IP port you have chosen for your instance. The Content Server Wizard uses this TCP/IP port to connect to your instance. The wizard does not verify that this port is the correct one for your instance; the wizard connects to whatever database instance is available from that port. Make sure that this port is the port that you specified for your instance and that no other instance is using it.
- The password for system administrator (SA) user or the username and password of an SQL user with create and alter privileges (not Content Server_DB_USER).
- The username and password of Content Server_DB_USER.
- Path to the NAS share in the format of \\servername\sharefolder. IP addresses cannot be used for the NAS path.
- The username and password of the MYDOMAIN\Content Server_NAS_USER domain account.

Create a New Content Server Cluster

Follow these steps to create a new Content Server cluster:

-
- | | |
|---------------|--|
| Step 1 | Using Windows Remote Desktop Connection as a domain administrator, log in to the first Content Server that you want to cluster. |
| Step 2 | Go to Start > Control Panel > User Accounts > Manage User Accounts . Add the domain account MYDOMAIN\Content Server_NAS_USER to the Administrators group on the Content Server. |
| Step 3 | Double click the Content Server Wizard icon on the desktop, or go to Start > All Programs > Cisco > Content Server > Content Server Wizard . Click Next from the Welcome screen. |
| Step 4 | The wizard overview screen appears and then runs through an initialization phase. When the wizard finishes initialization, it puts the Content Server in Idle mode. No calls can be made, and no transcoded outputs are processed. (The Content Server returns to online mode when the wizard process is completed or is cancelled.) |
| Step 5 | Click the Cluster Management Wizard radio button. Click Next . |
| Step 6 | The wizard verifies cluster prerequisites. Click Next . |
| Step 7 | Click the Create a new cluster radio button. Click Next . Read the informational screen. Click Next . |
| Step 8 | Choose H.323 or SIP to create a cluster using specified protocol. |
| Step 9 | At the Connect to an external SQL Server Database screen, enter the information for the database instance: <ul style="list-style-type: none">• SQL server IP address or name.• Name of the database instance. |

- Content Server/IP port that was chosen for the instance.
- Assign a database (catalog) prefix to your instance. It can be any string that you want. The wizard appends “3” to the end of the string that you specify. The wizard uses this prefix to distinguish the database instance from other versions that might be added later to the instance.
- The username and password of the SA user, or the username and password of another SQL user with create and alter privileges (not Content Server_DB_USER). The credentials of the SA user are used to create and configure the cluster database when running the wizard. The Content Server does not store the credentials of the SA user.

Step 10 Click **Next**.

Step 11 Enter the username and password of the database user that you created. The Content Server uses these user credentials to connect to the database. Click **Next**.

Step 12 Enter the path for the NAS share that you set up. The path is in this format: \\server\share. Make sure that you enter the NAS server computer name, not the IP address of the NAS. Click **Next**.

Step 13 In the IIS Anonymous User Account screen, enter the username and password of the domain account that you created, MYDOMAIN\Content Server_NAS_USER. The Content Server uses these credentials to access the share on the NAS. Click **Next**.

Step 14 In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for the Content Server. The defaults suggested by the wizard are based on the current settings of the standalone Content Server. For factory new Content Servers, it is the serial number for the non-live H.323ID and the serial number with “.live” appended (*serial number.live*) for the live H.323 ID.



Note Skip this step for SIP Cluster.

Step 15 In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed).

Step 16 The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to configure the cluster.

When you click **Configure**, the wizard configures your system and moves the media files to the NAS share. This process might take some time, depending on the amount of media to be moved to the NAS.

If you click **Finish**, the system exits the wizard without creating the cluster or making any changes. If any of the tests failed, you cannot continue to run the wizard.



Note Media files that are not associated with the Content Server's database include orphaned temporary files not used in any recordings, .tcb import file, and .tcb export files. These files are not moved to the NAS and are deleted from the local disk.

Step 17 After the configuration process is complete, in the Cluster: Save Cluster Settings File screen, save the cluster settings file. Browse to the location where you want to save the file. Click **Save**.

You can also generate the cluster settings file by running this Content Server Wizard again after you finish creating the cluster (see “[Generate a Cluster Settings File](#)” section on page 6-27). You need the cluster settings file if you want to add other Content Servers to the cluster.

Step 18 When the configuration is complete, click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

You have successfully set up a new cluster with one Content Server. You can now add additional Content Servers to this cluster.

**Note**

Your cluster cannot make calls until you have registered it to a gatekeeper. See the [“Configure Gatekeeper Registration for H.323 Cluster”](#) section on page 6-18.

Add a Content Server to an Existing Cluster

To add a Content Server to an existing cluster, you must meet the following prerequisites:

- Additional Content Servers must meet the criteria that are described in the [“Content Server Cluster Prerequisites”](#) section on page 6-6.
- Additional Content Servers must be given full control over the NAS share that you created. If they are not given full control, you cannot successfully add these Content Servers to an existing cluster.
- You must copy the cluster settings file to the desktop of the Content Server that you want to add. You can generate a cluster settings file at any time by running a Content Server Wizard on any of the Content Servers that are already in the cluster. See the [“Generate a Cluster Settings File”](#) section on page 6-27.
- Review the [“The Order of Content Servers Added to the Cluster”](#) section on page 6-13 to understand how the Content Server configurations and media content are added to the cluster.
- Review the information in the [“Before Running the Content Server Wizard”](#) section on page 6-15.

After confirming that additional Content Servers meet the prerequisites, run the Content Server Wizard on the Content Server that you want to add to the cluster.

-
- Step 1** Using Windows Remote Desktop Connection as a domain administrator, log in to the first Content Server that you want to cluster.
- Step 2** Go to **Start > Control Panel > User Accounts > Manage User Accounts**. Add the domain account MYDOMAIN\Content Server_NAS_USER to the Administrators group on the Content Server.
- Step 3** Double click the Content Server Wizard icon on the desktop, or go to **Start > All Programs > Cisco > Content Server > Content Server Wizard**. Click **Next** from the Welcome screen.
- Step 4** The wizard overview screen appears and then runs through an initialization phase. When the wizard finishes initialization, it puts the Content Server in Idle mode. No calls can be made, and no transcoded outputs are processed. (The Content Server returns to online mode when the wizard process is completed or is canceled.)
- Step 5** Click the **Cluster Management Wizard** radio button. Click **Next**.
- Step 6** The wizard verifies cluster prerequisites. Click **Next**.
- Step 7** Click the **Add to an existing cluster** radio button.
- Step 8** In the Cluster: Load Cluster Settings File window, browse to the cluster settings file that you copied to the desktop.
- Step 9** In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for the Content Server. The defaults suggested by the wizard are based on the current settings of the standalone Content Server. For factory new Content Servers, it is the serial number for the non-live H.323ID and the serial number with “.live” appended (*serial number.live*) for the live H.323 ID.

- Step 10** In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed).
- Step 11** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to configure the cluster.
- When you click **Configure**, the wizard configures your system and moves the media files to the NAS share. This process might take some time, depending on the amount of media to be moved to the NAS.
- If you click **Finish**, the system exits the wizard without creating the cluster or making any changes. If any of the tests failed, you cannot continue to run the wizard.
- Step 12** When the configuration is complete, click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.
-

You have successfully added another Content Server to a cluster. Repeat this process for each new Content Server that you want to add to the cluster.

Configure Gatekeeper Registration for H.323 Cluster

After you add Content Servers to the cluster, you must configure your gatekeeper registration before you can start making calls to record. The gatekeeper is permanently enabled for a Content Server cluster; it is not possible to disable the gatekeeper functionality.

A Content Server cluster needs two gateway registrations with separate prefixes: a live gateway prefix for live transcoded calls and a non-live gateway prefix for offline transcoded calls. Having two gateway registrations with separate prefixes ensures good load balancing of both types of calls across the cluster. In Premium Resolution clusters, you also have the option of entering playback gateway prefixes to enable playing recordings back from endpoints.

To register the cluster with the VCS, each Content Server needs four system IDs/aliases: live and non-live H.323 IDs and live and non-live E.164 system aliases. It is important that each is unique on that Content Server and on the Content Server cluster. See the [“Inbound H.323 Call Routing” section on page 6-2](#) for more information.

To configure the gatekeeper registration, follow these steps:

-
- Step 1** Log in to the web interface of any of the Content Servers in the cluster as an administrator. From the **Management** tab, go to **Configuration > Site settings**.
- Step 2** In the Gatekeeper settings section, enter a gatekeeper address.
- Step 3** Enter Live and Non-Live H.323 and E.164 gateway prefixes. In Premium Resolution clusters, you also have the option of entering playback gateway prefixes to enable playing recordings back from endpoints. The prefixes that you enter cannot be subsets of one another. Ensure that they are unique and that they follow the dialing plan set up on the VCS.
- Step 4** Check the Q.931 and Ras ports—the H.323 call setup and registration ports. By default, a Content Server cluster uses the range of 1719 to 1722 so that it can independently register OOR (out of resources) for live calls (recordings that are transcoded live) and non-live calls (recordings that are transcoded after recording finishes). The ports are editable because you can instruct the cluster to listen on different ports (for example, non-standard ports). Ensure that the ports you enter do not conflict with each other or with ports that are used by other services on the Content Server. Conflicts with other ports will prevent users from making recordings.

- Step 5** Click **Save**. Wait until Registration Status displays that registration is successful.
-

If you are experiencing problems registering to the gatekeeper, verify that you do not have duplicate gateway prefixes or a duplicate system H.323 ID or E.164 alias. Duplications might cause the gatekeeper to reject registration.

If you want to change a system H.323 ID and E.164 alias for a Content Server, do the following:

- Step 1** From the **Management** tab, go to **Diagnostics > Cluster overview**.
- Step 2** Locate the Content Server whose H.323 ID or E.164 alias you want to change. Click the **Server overview** link for that Content Server.
- Step 3** Update the H.323 ID or the E.164 alias, and click **Save**.
- Step 4** Repeat this procedure for any other Content Server whose H.323 ID or E.164 alias you want to change.
-

Configure Gatekeeper Registration for SIP Cluster

After you add Content Servers to the cluster, you must configure your gatekeeper registration before you can start making calls to record. The gatekeeper is permanently enabled for a Content Server cluster; it is not possible to disable the gatekeeper functionality.

To create a TCS Trunk and Route pattern on CUCM, refer the section [Cisco Content Server Cluster Configuration](#).

To configure the gatekeeper registration, refer the section [CUCM Configuration Setting on Content Server](#).

Configure Domain Authentication

The recommended authentication mode for the Content Server cluster is domain authentication. Domain authentication ensures that Active Directory users can log in to the cluster network load balanced frontend address.

To use domain authentication, click the **Management** tab and go **Configure > Site settings**. In the Authentication section, click the **Domain** radio button. Add details for your domain LDAP servers. See the [“Groups and Users” section on page 1-85](#) for more information about how to configure domain authentication.

The use of local authentication is not recommended in a Content Server cluster because local users would have to be added to every Content Server to view pages that are served from the network load balanced interface.

Configure Network Load Balancing (NLB)

To ensure that web page requests are spread across all Content Servers in a cluster rather than going to one specific Content Server interface, Cisco recommends that you set up an NLB solution. With an NLB solution, users access the cluster with the Virtual IP (VIP) address that you configure for the cluster on the load balancer. Users would not access the cluster with individual Content Server IP addresses.

The VIP address of the cluster is also referred to as the network load balanced frontend address of the cluster.

The load balancer as configured in this chapter works in direct routing mode. With direct routing, the load balancer changes the MAC address of a packet to the MAC address of the server that it sends the packet on to. In order for the Content Server to respond to this routing request it must assume the position of the VIP specified in the request and yet not advertise this address to the rest of the network. The Content Server cannot advertise this address because all Content Servers in the cluster assume the same VIP position. To verify this process, you must install a loopback adapter and set its IP to the VIP.

To set up network load balancing for a Content Server cluster, do the following:

-
- Step 1** [Configure a Load Balancer, page 6-21.](#)
 - Step 2** [Set up a Loopback Adapter on Each Content Server in Cluster, page 6-22.](#)
 - Step 3** [Enter the Cluster Virtual IP Address as the Frontend Address on the Content Server, page 6-22.](#)
-

Configure a Load Balancer

The following procedure is based on Loadbalancer.org Enterprise version and should be applicable to any Loadbalancer.org product.

The steps below outline the process for configuring a load balanced cluster of three Content Servers. The IP addresses in the steps are examples.

-
- Step 1** Go to the web interface for the load balancing device.
 - Step 2** Set up a virtual server.

The virtual server represents the entire cluster. The VIP address will be accessed by Content Server users. When successfully configured, the load balancer receives a request on the VIP address and forwards the request to one of the Content Servers in the cluster.

The VIP in this example is 10.10.2.111. In the example, we configure four virtual servers for the cluster, one for each port needed for a Content Server to operate. The four ports are 80 (HTTP), 443 (HTTPS), 8080 (Windows Media HTTP streaming) and 554 (RTSP). If you want to load balance MMS streams, you also need a virtual server for port 1755.

 - a. To configure the virtual server, go to **Edit Configuration > Virtual Servers**. Click **Add a new Virtual Server**. For the label, give the server an appropriate name (you might want to include the protocol name). Enter the VIP address that you want to use, followed by the port for the virtual server.

In this example, 10.10.2.111:80 is for the HTTP virtual server, with the persistent option set to **Yes**.
 - b. Create one virtual server for each of the ports that you want to load balance. Use different labels each time but the same VIP address.
 - Step 3** Configure the virtual server.
 - a. Click **Modify** for each server.
 - b. Change the **Check Type** to **connect**. Ensure that **Service to check** is set to none.
 - c. The **Check Port** should be set to 80 for HTTP, 8080 for Windows Media HTTP streaming, 554 for RTSP, 443 for HTTPS, and 1755 for MMS.
 - d. Leave the other options at their default values.
 - Step 4** Add each of the Content Servers in the cluster to each of the virtual servers you configured.
 - a. Go to **Edit Configuration > Real Servers**.
 - b. For the first virtual server in the list, click **Add a new Real Server**. Enter a label for the Content Server along with the server IP address, followed by virtual server port (for example, 80 for the HTTP virtual server).

- c. Ensure the weight is 1. A weight of 0 disables the server so that it receives no traffic. Also ensure that the forwarding method is set to DR.
- d. Repeat this procedure to add each additional server in the cluster to each of the virtual servers.

Set up a Loopback Adapter on Each Content Server in Cluster

The Content Server Wizard is used to set up a loopback adapter for network load balancing. This operation must be repeated on each Content Server in the cluster.

- Step 1** Log in to the Content Server using Windows Remote Desktop Connection. Run the Content Server Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click **Configure Load Balancer Configuration**.
- Step 3** In the Frontend address field, enter the virtual IP (VIP) address of the cluster that you set up on the load balancer. In the Subnet mask field, enter the subnet mask of your network.



Note Ensure that you enter the correct VIP address. An incorrect VIP address results in unexpected behavior when users attempt to access the cluster interface.

- Step 4** Click **Next**.
- Step 5** Click **Configure** for the wizard to install the loopback adapter.
- Step 6** Click **Finish**.
- Step 7** Repeat this procedure for all the other Content Servers in the cluster.

See the [“Update Load Balancer Configuration”](#) section on page 6-27 for details about updating the load balancer configuration.

Enter the Cluster Virtual IP Address as the Frontend Address on the Content Server

The virtual IP address or DNS name of the cluster as set up on the load balancer must be entered in the Frontend address field in Site settings. To enter the VIP address or DNS name, click the **Management** tab. Then go to **Configure > Site settings**. Entering the frontend address ensures that all recording links that are generated by a Content Server and on Cisco TelePresence Management Suite (TMS) use the frontend address.

Managing a Content Server Cluster

This section describes cluster management functions that are different from a standalone Content Server.

- [Access Cluster Administrative Pages, page 6-23](#)
- [View Cluster Status, page 6-24](#)
- [Edit Information for Each Content Server in Cluster, page 6-25](#)
- [Edit Information Common to All Content Servers in Cluster, page 6-25](#)
- [Generate a Cluster Settings File, page 6-27](#)
- [Update Load Balancer Configuration, page 6-27](#)
- [Update Cluster Settings, page 6-28](#)

Access Cluster Administrative Pages

You can access the web interface of a Content Server cluster by logging in to the IP address or DNS name of a specific Content Server in the cluster. If you set up load balancing, you log in with the network load balanced frontend address of the cluster. The items available in the Management tab vary depending on the address that you log in to.

If you log in with the IP address or DNS name of a specific Content Server in the cluster, the Management tab includes these four menus and their sub-menus:

- Diagnostics—Cluster overview, Server overview, Server logs, Transcoding queue
- Recordings—Edit recordings, Import recordings, Create recording
- Recording Setup—Recording aliases, Categories, Templates, Media server configurations, Call configurations
- Configuration—Site settings, Groups and users, Window server

If you log in to the cluster with the network load balanced frontend address (the VIP address), the Management tab includes these four menus and their sub-menus:

- Diagnostics—Cluster overview, Transcoding queue
- Recordings—Edit recordings, Import recordings, Create recording
- Recording Setup—Recording aliases, Categories, Templates, Media server configurations, Call configurations
- Configuration—Site settings, Groups and users

When accessing the cluster through the network load balanced frontend address, you do not see Server logs, Server overview, and Windows server because these sub-menus are specific to each Content Server. To see these sub-menus for a specific Content Server, access the specific server from Cluster overview page.

View Cluster Status

Management: Diagnostics > Cluster overview

The Cluster overview page does the following:

- Lists the system names and IP addresses of all Content Servers in the cluster.
- Displays a link to the Server overview page for each Content Server.
- Reports the total number of current calls for the cluster and for each Content Server.
- Reports the total number of offline transcodes for the cluster and for each Content Server.
- Reports the server mode for each Content Server.
- Reports the status for each Content Server. If the Content Server mode is online, then the status displays a green check, which means that the Content Server is running correctly. If the server mode is not online, then the status displays a red exclamation mark. Go to the Server overview page for the specific Content Server to see more details. From the Server overview page, you can check which of the services is not running.
- Displays links to each Content Server's logs and Windows Server administration interface.
- Allows you to End all Calls on the entire cluster. You can end recording calls on a specific Content Server from the Server overview page for the selected Content Server.
- Allows you to put a Content Server in maintenance mode. When the Content Server is in maintenance mode, the server cannot accept new recording calls. Current calls and transcoding jobs continue until finished. The other Content Servers in the cluster continue working as usual.

Maintenance mode should be used to ensure that no new calls are made to a Content Server—for example, when you want to defragment the server drive, run a Windows security update installer, or update antivirus software on the server. You should also put a Content Server in maintenance mode (after ending current recording calls on that server) if you need to shut it down and move it to another location.

To enter maintenance mode, click the **Enter maintenance mode** button. The button label changes to **Rejoin cluster**, and server mode shows that the server is in maintenance. When you finish maintenance on the server, click the **Rejoin cluster** button. The button label changes to **Enter maintenance mode** and Server mode is online. The Content Server is now ready to receive calls.

Server overview with log in to a specific Content Server—Management: Diagnostics > Server overview

Server overview with log in to the network load balanced frontend address—Management: Cluster overview > Server overview link

The Server overview page provides this additional information relevant to the cluster:

- Total disk space and free disk space on the cluster media storage location (in addition to the disk space information for the C and E drives of this Content Server).



Caution

If remaining disk space on the NAS is below the critical 10% level, it is displayed in red as a warning to the administrator. The administrator should free up space on the NAS. If free disk space on that share falls below 5%, the cluster stops receiving recording calls and processing offline transcoded jobs.

- Database data source—displays the address of the external database server, port, and instance name.
- Database name—displays the database (catalog) prefix that you entered when you created the cluster and a suffix added by the Content Server Wizard (3).
- Cluster media storage location—displays the external NAS share name.

Edit Information for Each Content Server in Cluster

Go to the Server overview page to edit information specific to each Content Server in a cluster.

From the Server overview page, you can edit the following:

- System name
- Non-live and live H.323 IDs and non-live and live E.164 system aliases

Non-Live and Live system IDs/aliases are required for registering to the gatekeeper.



Note You should not use those system IDs/aliases for dialing the cluster because they will always (and only) be routed to a specific Content Server. Only calls made to recording aliases or playback addresses are balanced across the cluster by the gatekeeper.

Any changes made to the system name and to non-Live and live system IDs/aliases fields are applied to a Content Server that is not currently in a recording call. Changes cannot be applied to a Content Server in a call. Saving changes on this page automatically puts this server in Configuration reload mode. In Configuration reload mode, incoming calls are not accepted and outgoing calls cannot be made from that Content Server.

The administrator might also choose to override Configuration reload mode and apply changes immediately by ending recording calls manually on the Content Server. Clicking **End all calls** from the Server overview page stops all calls on the Content Server. When calls have ended, the new settings are applied to the Content Server. When the Content Server comes back online, it is ready to accept new calls.

Edit Information Common to All Content Servers in Cluster

Any changes made in these areas are applied to all Content Servers in the cluster through the shared database:

- Cluster overview
- Import recordings
- Recording aliases
- Categories
- Templates
- Media server configurations
- Call configurations
- Site settings
- Groups and users

This section highlights some exceptions and special considerations when managing the cluster.

Import recordings

When importing files smaller than 2 GB, log in to the IP address of one of the Content Servers. Do not use the network load balanced frontend address.

Click the **Management** tab, then go to **Recordings > Import recordings** to import recording files through the web interface.

When importing files larger than 2 GB in size, place the .tcb file in the Imports folder on a desktop of one of the clustered Content Servers. You then need to log in to the web interface of this Content Server (using its IP address or DNS name) to import the .tcb file. After it is imported, the recording is available to the whole cluster. However, the import file is only visible on the Import recordings page for the Content Server to which it was uploaded.

Site settings

The Site settings page (from the **Management** tab, **Configuration > Site settings**) is available for editing even if Content Servers are in recording calls.

Most settings from the Site settings page can be changed and applied while Content Servers are in recording calls. Settings that cannot be changed and applied when recording calls are in progress are the following:

- Cluster name
- Gatekeeper settings
- Advanced H.323 settings
- E-mail settings
- Default recording alias

Any changes that are made in those areas are applied only to Content Servers that are not currently in recording calls. Changes cannot be applied to Content Servers that are in calls, so saving Site settings automatically puts those servers in Configuration reload mode.



Note In Configuration reload mode, incoming calls are not accepted and outgoing calls cannot be made from that Content Server.

After all current calls are complete, the new settings are applied and the Content Server mode changes back to online.

The administrator might also choose to override Configuration reload mode and apply changes immediately by ending calls manually on all Content Servers. Clicking **End all calls** from the Cluster overview page stops all calls in the cluster. When recording calls end, new settings are applied to the Content Servers and all Content Servers are in online mode again, ready to accept calls.

API

The clustering functionality requires that API be enabled. You cannot disable the API when Content Servers are clustered.

Generate a Cluster Settings File

You need a cluster settings file to add more Content Servers to an existing cluster (see the [“Add a Content Server to an Existing Cluster”](#) section on page 6-17). Cluster settings are in an XML file that contains details of the external database and the Content Server_NAS_USER. If cluster settings change from the original cluster setup, you must generate a new cluster settings file to use when you want to add more Content Servers to the cluster.

To generate a cluster settings file, do the following:

-
- | | |
|---------------|---|
| Step 1 | Log in to a Content Server by using Windows Remote Desktop Connection. Run the Content Server Wizard.

The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available. |
| Step 2 | Click the Generate Cluster Settings File radio button. |
| Step 3 | Click Browse if you want to save the cluster settings file in a location other than the Content Server desktop. Click Next . |
| Step 4 | Click Finish to exit the wizard. |
-

Update Load Balancer Configuration

If you have changed the cluster VIP address on the load balancer, you need to update it on each Content Server by using the Content Server Wizard.

-
- | | |
|---------------|---|
| Step 1 | Log in to the Content Server by using Windows Remote Desktop Connection. Run the Content Server Wizard.

The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available. |
| Step 2 | Click the Configure Load Balancer Configuration . |
| Step 3 | Click Update Load Balancer Configuration . |
| Step 4 | Enter the cluster VIP address that you set up on the load balancer and/or the subnet mask of your network. Click Next . |
| Step 5 | Click Configure for the wizard to update the loopback adapter. This process might take some time. |
| Step 6 | Click Finish . |
| Step 7 | Repeat this procedure for each Content Server in the cluster. |
| Step 8 | In Site settings page, update the frontend address in Site Settings to the new VIP. See “Enter the Cluster Virtual IP Address as the Frontend Address on the Content Server” section on page 6-22 for details. |
-

**Note**

The loopback adapter is automatically removed when you remove the Content Server from a cluster. You can also remove it using the Content Server Wizard. Run the wizard as described above and click the **Remove Load Balancer Configuration** option. Applying this option only uninstalls the loopback adapter on the specific Content Server. You will need to manually remove the Content Server from your load balancer configuration.

Update Cluster Settings

You can update alternate media location (NAS) settings for the cluster by using the Content Server Wizard.

The Content Server Wizard allows you to:

- [Update the Password for MYDOMAIN\Content Server_NAS_USER Account, page 6-28](#)
- [Change the MYDOMAIN\Content Server_NAS_USER Account to Another Domain Account, page 6-29](#)
- [Change the Location of the Media Files to a Different NAS Share, page 6-29](#)

**Note**

As an alternative to the procedures described below, you could remove all Content Servers from the cluster (see [“Removing a Content Server from the Cluster” section on page 6-30](#)) and run the Alternate Storage (NAS) wizard option on the last Content Server removed from the cluster to update the password, change the account, or change the media location. Then create a new cluster and add the Content Servers to the cluster again.

Update the Password for MYDOMAIN\Content Server_NAS_USER Account

If the MYDOMAIN\Content Server_NAS_USER password expires, the cluster cannot connect to the NAS and media files cannot be moved to their media location. Users will not be able to view recordings.

You need to set a new password for the account on the domain and then run the Content Server Wizard on each Content Server in the cluster to update the password. Follow these steps:

-
- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection as a domain administrator. Run the Content Server Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click the **Update Cluster Settings** radio buttons.
- Step 3** The wizard displays the username and password for the account that the cluster uses to connect to the NAS. Change the password, and click **Next**.
- Step 4** The wizard displays the current media location. Click **Next**.
- Step 5** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
- When you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
- Step 6** When the configuration is complete, click **Finish** to exit the wizard.

Step 7 Repeat the procedure on all Content Servers in the cluster.

Change the MYDOMAIN\Content Server_NAS_USER Account to Another Domain Account

If you need to change the MYDOMAIN\Content Server_NAS_USER account, follow these steps:

-
- Step 1** Add the new account (for example, MYDOMAIN\Content Server_NEW_NAS_USER) to the permissions on the NAS share. Give the account full control (see [“Set Permissions and Security Settings on the Share”](#) section on page 6-12).
- Step 2** Log in as a domain administrator to one of the Content Servers in the cluster by using Windows Remote Desktop Connection.
- Step 3** Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add MYDOMAIN\Content Server_NEW_NAS_USER to the Administrators group.
- Step 4** Start the Content Server Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 5** Click the **Update Cluster Settings** radio button.
- Step 6** The wizard displays the username and password of the account that the cluster uses to connect to the NAS. Change the username and password to the new account, MYDOMAIN\Content Server_NEW_NAS_USER. Click **Next**.
- Step 7** The wizard displays the current media location. Click **Next**.
- Step 8** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
- When you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
- Step 9** When the configuration is complete, click **Finish** to exit the wizard.
- Step 10** Repeat this procedure on all Content Servers in the cluster.
-

Change the Location of the Media Files to a Different NAS Share

If you need to change the default media location for the cluster to a different NAS share, follow these steps:

-
- Step 1** Set up a new NAS share (see the [“Configure the NAS”](#) section on page 6-11). The permissions on this share must allow all Content Servers in the cluster and the MYDOMAIN\Content Server_NAS_USER full control of the share. You can continue to use the same MYDOMAIN\Content Server_NAS_USER, or create and use a different domain account.
- Step 2** Manually copy the data folder from the old NAS share to the new NAS share.

**Note**

You cannot copy files that are in use (files that are being watched or downloaded by users). We recommend that the cluster not be active during the copy process. Follow your usual file server migration procedures when copying the files. Putting the Content Servers in maintenance mode alone is not sufficient to guarantee a safe copy of media because maintenance mode still allows users to watch and download recordings.

- Step 3** After the copy process is complete, verify that the number of files and size of the data folder on the new NAS share is identical to the old NAS share.
- Step 4** Log in to a Content Server in the cluster by using Windows Remote Desktop Connection. Start the Content Server Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 5** Click the **Update Cluster Settings** radio button.
- Step 6** The wizard displays the username and password of the account that the cluster uses to connect to the NAS. Change the username and password to a new account, if required. Click **Next**.
- Step 7** The wizard displays the current media location. Enter the location of the new NAS share in the format `\\servername\share`.
- Step 8** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to update the cluster settings.
- At this stage you can also click **Finish** to exit the wizard without updating the cluster settings.
- When you click **Configure**, the wizard configures your system and updates settings. This process might take some time.
- Step 9** When the configuration is complete, click **Finish** to exit the wizard.
- Step 10** Repeat this procedure on all Content Servers in the cluster to set the new media location information in IIS.

Removing a Content Server from the Cluster

You can run the Content Server Wizard to remove one or more Content Servers from the cluster at any time.

**Note**

If you are removing Content Servers from a cluster, the order in which you remove them is important.

None of the media or cluster configurations are available on a Content Server after it is removed from the cluster. When removed from a cluster, the Content Server becomes a standalone server with no content or configuration. The exception is the last Content Server that is removed from the cluster. When you run the Content Server Wizard on the last Content Server remaining in a cluster and click **Remove from cluster**, the server becomes a standalone server with media on a NAS. The last server retains all content recorded by the cluster and all cluster configurations. The external database instance is dropped, and all data are copied to the local database, while all media files remain on a NAS.

On the standalone Content Server, you can use the Alternate Storage (NAS) wizard option to move the media files to another NAS location or to move them back to the local drive on the Content Server (if the size of the recorded media allows it).

To remove a Content Server from the cluster:

-
- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection. Run the Content Server Wizard.
- The wizard scans your system. If the Content Server is in a cluster, only the Cluster Management Wizard option is available.
- Step 2** Click the **Remove from Cluster** radio button.
- Step 3** In the Content Server Checks screen, confirm that the Content Server is backed up and that antivirus software is stopped (if it is installed). If the Content Server is backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again.
- Step 4** The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to remove the Content Server from the cluster.
- When you click **Configure**, the wizard configures your system and removes the Content Server from the cluster. This process might take some time.
- Step 5** When the configuration is complete, click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.
-

The Content Server can be added back to the same or a different cluster at any time.



Caution

Removing a Content Server from a cluster deletes the network load balanced loopback adapter from the Content Server, but the server is not removed from the load balancer setup. You must manually remove the Content Server from the load balancer configuration. If you do not remove the server from the configuration, the load balancer continues to direct traffic to a Content Server that no longer belongs to the cluster.



Caution

If the cluster frontend address was pointing to a load balanced address, you must delete the load balanced address manually from the Site settings page of the last Content Server that you removed from the cluster. Otherwise, you cannot save the site settings.

Using TMS to Schedule Calls on a Content Server Cluster

Cisco TelePresence Management Suite (TMS) 12.2 or higher can be used to schedule recording calls on a cluster. We recommend that clusters use either TMS to schedule calls or ad hoc dialing. A mixture of scheduled and ad hoc dialing is not recommended.

To use TMS to schedule recording calls on a cluster, do the following:

-
- Step 1** Ensure that the cluster name in the Site settings page is a meaningful name. The TMS displays the name in the Recording drop-down menu on the Conference Booking page.

**Note**

When registering a cluster in TMS, ensure that the cluster name in the Site settings page is not blank. If you do not include a cluster name, cluster resource allocation in TMS might not be correct.

- Step 2** Ensure that the frontend address in the Site settings page is entered and that it is the correct network load balanced address. This address is used to generate conference links in TMS.
- Step 3** Add one or more Content Servers in the cluster to TMS. You only need to add one Content Server in the cluster to make calls to the whole cluster.
- Step 4** Check that users can select at least one live and one non-live recording alias in the Recording drop-down menu on the TMS New Conference Booking page. Each recording alias type (live and non-live) can be used to schedule a number of calls to the maximum cluster capacity for this call type.

Backing Up and Restoring the Content Server Cluster

We recommend that you back up the cluster regularly and also before an upgrade or when installing a security update.

It is very important to follow the procedure described here. If you do not follow the procedures, future upgrades might not work or you might lose your data.

There are three parts to backing up and restoring a Content Server cluster from backup:

- [Backing Up Clustered Content Servers, page 6-32](#)
- [Backing Up the External MS SQL Database, page 6-32](#)
- [Backing Up Media on the NAS/External Streaming Server, page 6-32](#)

Backing Up Clustered Content Servers

To back up and restore the Content Servers in a cluster, follow the backup and restoring procedures as described in [Chapter 9, “Maintaining the Content Server.”](#)

Backing Up the External MS SQL Database

To back up and restore the external SQL server database, follow the administrative guidelines for your SQL server.

Ensure that you back up the database at the same time as the Content Server and the NAS. If you restore from backup, you must restore the database backup that was done at the same time as your Content Server and NAS backups; otherwise, you might not be able to view some recordings.

Backing Up Media on the NAS/External Streaming Server

To back up cluster media, follow the administrative guidelines for backing up your file servers. To ensure all media are backed up, back up all files in the share on the NAS that is used by the cluster and also any media on external streaming servers.

To restore the media, copy the relevant backup back to the share on the NAS (and the correct location on the external streaming server).

Ensure that you back up your NAS or an external media server at the same time as the Content Server and the SQL server database. If you restore from backup, you must restore the NAS and external streaming server backup that was done at the same time as your Content Server and SQL server database backup; otherwise, you might not be able to view some recordings.

Upgrading the Cluster to a New Software Version

Before upgrading a Content Server Cluster to a new software version, do the following:

- Ensure that the Content Server Cluster is backed up (see [Backing Up and Restoring the Content Server Cluster](#)). If the upgrade installer fails, you can restore from the backup in order to downgrade to the previous version.
- Stop any antivirus software, if running.
- The cluster is not operational for the duration of the upgrade of the first Content Server in the cluster. The cluster operates at a reduced capacity until all the Content Servers are upgraded. Cisco recommends that you take a system outage into account when scheduling the upgrade.
- Ensure that you have release keys available if you are upgrading to a major version. Release keys need to be entered at the time that the installer is run.

To upgrade the Content Server Cluster, log in to each of the Content Servers using Windows Remote Desktop Connection and run the software upgrade installer on one Content Server at a time.



Caution

Running upgrade installers simultaneously on two or more clustered Content Servers cause SQL server errors and might damage your cluster installation.

You do not need to put clustered Content Servers into maintenance mode before starting the upgrade. The installer ensures that they are not available for accepting recording calls during the upgrade. After the installation process is complete on the first Content Server, it automatically becomes available for making and accepting calls to its capacity.

During the upgrade, the web interface of the Content Servers that are not yet upgraded display this message: “Server under maintenance. This Content Server is being upgraded and is currently unavailable. For more information, please contact your local Administrator.” The Cluster overview page display their mode as “Upgrading” and their status as “Not OK.” Each server becomes available to the cluster after the installation is completed on each.

Upgrading the External Microsoft SQL Server

Content Server clusters supports MSSQL Server 2005 or MSSQL Server 2008.

If you need to upgrade the external Microsoft SQL server from MSSQL Server 2005 to MSSQL Server 2008, do the following:

-
- Step 1** Back up the cluster (see the [“Backing Up and Restoring the Content Server Cluster”](#) section on page 6-32).

- Step 2** We recommend that you shut down all the Content Servers in a cluster when upgrading your external SQL server.
- Shutting down the Content Servers prevents them from trying to access the database while upgrading your external SQL server. Putting the Content Servers in maintenance mode alone does not ensure that they stop communicating with the database.
- Step 3** Upgrade the instance the cluster uses on the external Microsoft SQL server from MSSQL Server 2005 to MSSQL Server 2008.
- Step 4** Power on the Content Servers.
- Step 5** Verify that the upgrade was successful by logging in to the web interface of the cluster. Click on the **Management** tab, and go to **Diagnostics > Cluster overview** to check that the server mode for all Content Servers is online and that the status is OK (a green check). We also recommend making a test call to the cluster.
-



The My Recordings Tab

This chapter explains what users can do in the **My Recordings** tab of the Content Server web UI. To see this tab when you log in, a Content Server site manager must first give you the role of creator.

The **My Recordings** tab is a list of recordings that you have created or recordings that others have given you permission to edit. This tab has three sub-menus:

- **Edit Recordings**—From the list in this sub-menu, locate the recording that you want to modify. You can edit the recording settings (**Edit recordings > Edit Recording**), use the Content Editor (**Edit recordings > Open Content Editor**), or manage recording outputs (**Edit recordings > Manage Outputs**).

From this sub-menu, you can play the recording by clicking the **Play** link.

If the recording is currently in draft state, you can click the **Publish recording** button. Publishing the recording permits groups and users under 'Who can view this recording' to access the recording. If the recording has been published, this button does not appear.

If recording is currently in progress, you can click the **End call** button to stop recording.

- **Create Recording**—From the list in this sub-menu, you can enter the number or address of an endpoint or system that the Content Server should call to make a recording.
- **Create Recording Options**—From the list in this sub-menu, you can locate H.323 ID, E.164 alias, or SIP address that is available to you for recording. Use one of them to call the Content Server from an endpoint or system (see **Create Recording**). From this sub-menu, you can also edit your personal recording alias if you have one (see **Edit Recording Aliases**).

Edit Recordings

You can display a list of editable recordings from the **My Recordings** tab by clicking **Edit recordings**. This list includes recordings that you created and recordings that others have given you permission to edit. From this list, you can do the following:

- **Play**—click to play a specific recording.
- **Edit Recording**—click to edit settings for the recording, including the recording name and who can view it.
- **Open Content Editor**—click to access the Content Editor for various formats. Use the Content Editor to index or crop the recording. You can also concatenate another recording to one that is open in the Content Editor.

- **Manage Outputs**—click to modify output settings, including how the recording is viewable in a web interface or in what formats the recording is downloadable.
- Delete one or more recordings—check one or more recording boxes (to the left of each recording thumbnail). Then click the **Delete selected** button on the bottom left of the page. You can also click the **X** to the far right to delete one recording at a time.

Edit Recording

To edit settings for one of the recordings in the My Recordings list, do the following:

-
- Step 1** Click the **My Recordings** tab.
- Step 2** Click **Edit recordings**. A list of recordings that you created appears. This list also include recordings that others have given you permission to edit.
- Step 3** Locate the recording whose settings you want to edit.
- Step 4** Click **Edit recording**. A page that includes the settings for the recording appears.
- Step 5** Update recording settings as needed (see [Table 7-1](#)).
- Step 6** After updating the settings, click **Save**.
-

Table 7-1 *My Recordings > Edit Recordings: Edit Recording*

Field	Field Description	Usage Guidelines
Recording information		
Name/Title	The name of the recording to be displayed in the View Recordings pages.	If you created the recording, the default name is the name of your personal recording alias and a date/time stamp. You can edit this name (maximum 255 characters) to help users find the recording when they search. If you edit a recording that you did not create, the name could be the name of the creator's recording alias and a date/time stamp. The name could also be the type of recording (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp.
Description	Details about the recording.	Optional. The optional description (maximum 1500 characters) can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.
Keywords	Keywords that can be used to search for the recording.	Optional. This optional setting can help users find the recording when they search.

Table 7-1 My Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Category	Choose a category under which to list the recording in the View Recordings pages. To create a category, go to Recording setup > Categories .	Optional.
Date	The date and the time at which the recording process began.	Read only. You cannot edit these fields.
Duration	The length of the recording rounded to the nearest minute. In parentheses, length of the recording in HH:MM:SS format.	Read only. You cannot edit these fields.
Share link	The link to the recording.	Read only. You cannot edit these fields.
Recording thumbnails		
Thumbnail images	A thumbnail is an image from the recording that helps users to identify the recording. Thumbnails images are taken at 5 seconds, 1 minute, 5 minutes, 30 minutes, and 1 hour into the recording. The image at 30 minutes into the recording is the default. If the recording is less than 30 minutes, the default is last image taken.	Choose a thumbnail to represent the recording. You might need to refresh the page or restart the browser to see the thumbnail that you chose. Click the thumbnail to choose it. An orange frame surrounds the thumbnail that represents the recording.

Table 7-1 My Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Recording permissions		
Who can view this recording	Groups and users who can view the recording. Click the Check access list button to validate your entries. Entries are also validated when you click the Save button.	<p>You can give viewing access to one of the following:</p> <ul style="list-style-type: none"> • Allow access to all users, including guests: If Allow guest access is selected in Site Settings, this field is displayed. If selected, all users, including guests, can view the recording. • Allow access to all authenticated users: If the Allow guest access box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list or Place call adds all matching groups and users to the list. <p>Note After you click Check access lists or Place call, the users entered have the following formats:</p> <ul style="list-style-type: none"> – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, "CN=group.name, OU=staff, DC=company, DC=com").</p>
Publish recording	If checked, the selected groups and users under <i>Who can view this recording</i> can view this recording. The groups and users in the editors list can always view and edit the recording.	<p>This box is checked by default.</p> <p>When this box is unchecked, the recording does not appear in the View Recording pages. The recording still appears in the Edit recordings list. Next to the recording, the Publish recording button appears. When you click that button, all specified groups and users can view the recording.</p>
Password (optional)	You can enter a password to restrict streaming access to this recording and the ability to download content. The password will be visible in clear text to editors of this recording and to site managers.	If a password is not entered, users who can view the recording in the View Recordings list can play the recording and download any available content. If a password is entered, users must know the password to stream or download the recording.

Table 7-1 My Recordings > Edit Recordings: Edit Recording (continued)

Field	Field Description	Usage Guidelines
Who can edit this recording	Groups and users can edit recording information and permissions, use the Content Editor (see Open Content Editor) to change the recording, add additional outputs (see Manage Outputs), and delete the recording. Use Check access list to validate your entries. They are also checked when you click Place call .	<p>Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list or Place call adds all matching groups and users to the list.</p> <p>Note After you click Check access lists or Place call, the users entered have the following formats:</p> <ul style="list-style-type: none"> – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name <p>All groups will be in the format group.name where the group name is expanded to the full LDAP name (for example, “CN=group.name, OU=staff, DC=company, DC=com”).</p>
Play recording on endpoints		
Make recording available for playing on endpoints	Check to make the recording available for playback on an endpoint.	<p>When you check this box, either a playback H.323 ID or playback E.164 alias will appear. Depending on the Content Server configuration, both might appear. Give users the playback E.164 alias or the playback H.323 ID. Instruct them to dial the alias or ID from an endpoint. Doing so will play back the recording.</p> <p>If this check box is not on the Edit recording page, a Content Server site manager has not configured the prefixes necessary for an E.164 playback alias or H.323 playback ID. Or the Content Server does not support the playback feature. Contact a site manager for more information.</p> <p>The recording cannot be played back on an endpoint if it has not been published. See the Publish recording setting above for more information.</p> <p>A recording with restricted viewing access and no viewable interface outputs can be played back from an endpoint.</p> <p>Password protection is not applied when a recording is played back from an endpoint unless you add a PIN.</p> <p>Tip You can also PIN protect all new recordings created with your personal recording alias (see Edit Recording Aliases).</p>

Open Content Editor

Users with the appropriate permissions and all site managers can use the Content Editor to edit recordings. To use the Content Editor, see the following sections:

- [Indexing a Recording](#)
- [Cropping a Recording](#)

- [Removing a Middle Section from a Recording](#)
- [Joining Recordings](#)

All changes that you make to a recording while editing are non-destructive. For example, you can change the position of the slider at the beginning or at the end of the recording many times.

Viewing the recording in a player reflects the changes immediately. Downloads need to be transcoded again. Click **Save and close** to start the transcoding process. Transcoding again removes existing downloadable outputs and replaces them with the newly transcoded output.

**Note**

- To open a recording in the Content Editor, the recording must have outputs that can be viewed in a player.
- You can use the Content Editor on an Apple Mac using MPEG-4 for QuickTime or MPEG-4 for Flash. The Content Editor is not available on the Mac for Windows Media recordings using Silverlight.

To open the Content Editor, do the following:

-
- Step 1** Go to **Recordings > Edit Recordings**. A list of editable recordings appears.
- Step 2** Find the recording that you want to edit with the Content Editor.
- Step 3** Click **Open Content Editor**. A window that lists the formats of available outputs appears.
- Step 4** Click an output format link to open the Content Editor window.
-

Parts of the Content Editor window

- The top section displays the recording video on the left. The Indexes section is on the right.
- The bottom section displays controls for playing and editing the recording: the seek bar, the volume control, a pause/play button, and a **Join Recording** button.

Indexing a Recording

You can add indexes to make it easier for viewers to find important points in the recording. Index titles appear in a player when users watch the recording. When users click an index, the recording plays from that index point.

To add an index, do the following:

-
- Step 1** Pause the recording where you want an index.
- Step 2** Click **Add index**. A new index appears in the Indexes section. Each index includes the time of the index point and a default title (Index<number>).
- Step 3** If you want, click the default title and change it to something more meaningful to viewers.
- Step 4** Click **Save and Close** to save your index.
-

**Note**

You can add, delete, or rename indexes in the Content Editor only.

Cropping a Recording

To remove time from the beginning or the ending of a recording, do the following:

-
- Step 1** Locate the seek bar.
 - Step 2** Move the sliders at either end of the seek bar to where you want them. The slider for the beginning of the recording is on the left; the slider for the end of the recording is on the right. In the player, the recording will start from and end wherever you move the sliders.
 - Step 3** Click **Save and Close** to save your slider settings.
-

Removing a Middle Section from a Recording

To remove a middle section, do the following:

-
- Step 1** Click the **Join recording** button. A list of recordings that can be joined to the one that you have open in the Content Editor appears.
 - Step 2** Click the **Join recording** link for the same exact recording. Two thumbnail images appear in the Content Editor window. The first thumbnail with the highlighted box is the original recording. The second thumbnail is the recording that you joined to the first.
 - Step 3** Ensure that you have chosen the first thumbnail by clicking it.
 - Step 4** Move the slider for the end of this recording (the right side) to the beginning of the section that you want to remove.
 - Step 5** Click the second thumbnail.
 - Step 6** Move the slider for the beginning of this recording (the left side) to end of the section that you want to remove.
 - Step 7** Click **Save and close**. Then check the results of the removal by playing it back in a player. Redo this procedure until you have adjusted the recording properly.
-

Joining Recordings

You can join recordings (also known as concatenating) so that they play consecutively. You can join recordings under these conditions:

- You have editing permissions for the recordings, or you are in the site manager role.
- The recordings have streaming outputs in the same format and size (for example, Windows Media in the medium size).
- The recordings have the same dual video status. You cannot join two if only one has a dual video stream.

To join two recordings, do the following:

-
- Step 1** Click the **Join recording** button. A list of recordings that can be joined to the one that you have open in the Content Editor appears.
 - Step 2** Click the **Join recording** link for the recording that you want to join to first recording.

- Step 3** Click **Save and close**. Then check the results of joining the recordings in a player. If you want, crop the recordings for a better playback experience (see [Cropping a Recording](#) for more information).

Manage Outputs

Recording creators, users with the appropriate permissions, and all site managers can manage recording outputs at any time.

To manage outputs, do the following:

- Step 1** Go to **My Recordings > Edit recordings**. A list of recordings appears.
- Step 2** Locate the recording whose settings you want to edit.
- Step 3** Click **Manage outputs**. A page that includes the output settings for the recording appears.
- Step 4** Update settings as needed (see [Table 7-2](#)).
- Step 5** After updating the settings, click **Save**.

Table 7-2 *Recordings > Edit Recordings: Manage Outputs*

Field	Field Description	Usage Guidelines
Manage outputs		
Recording call speed (kbps)	The bit rate in kbps (kilobits per second) at which the recording was created.	This number might affect the bit rate of medium and large outputs.
Recorded with dual stream	Whether or not this recording was recorded with a dual video stream.	This recording characteristic affects the layouts available for outputs. Only the single video layout is available if this recording was created without a dual video stream.
Viewable in the Content Server web interface	If you check this box, go to the Outputs to view in the Content Server web interface to select output settings for a player.	—
Downloadable for portable devices (iPod and Zune)	If you check this box, go to the Outputs to download for portable devices to select output settings for a player.	—
Downloadable for general purpose	If you check this box, go to the Outputs to download for general purpose to select output settings for a player.	There is a limitation of 55 characters for UTF-8 (or 18 characters for UTF-16) for the length of the title of a recording when downloaded. We recommend using less than 55 characters in the title or renaming the downloaded recording.

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U	If you check this box, go to the Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U to select output settings for a player.	—
Outputs to view in the Content Server web interface		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, the single video layout with one stream that shows the main video source is created.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video stream. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
On demand formats	Choose up to three formats: <ul style="list-style-type: none"> Windows Media for playback using the Silverlight player or Windows Media player on a PC or the Silverlight player on a Mac. MPEG-4 for playback using QuickTime. MPEG-4 for playback using Flash player. 	These formats can be viewed on a PC as long as the correct plugins have been downloaded and installed. MPEG-4 for QuickTime, MPEG-4 for Flash, and Windows Media (played using Silverlight) are available for Apple Mac when the correct plugins have been downloaded and installed.
On demand sizes	Choose up to two recording sizes based on your user streaming environment and internet connection.	<ul style="list-style-type: none"> Audio only: For use when users have very poor quality internet access. Small: The target bit rate for small outputs is 250 kbps. The target rate is displayed in the Bit rates field. Medium: For use with broadband access. The target bit rate for medium outputs is 800 kbps. The target rate is displayed in the Bit rates field. Large: For use with a high-speed LAN. This format takes the longest to transcode. The maximum rate is displayed in the Bit rates field.
Bit rates (kbps)	Displays the target bit rate for the small, medium and large output sizes. The number that is displayed depends on the target bit rates set in Site Settings and the call speed at which the recording was created.	—
On demand media server configuration settings	Choose the Media Server Configurations for on-demand viewing of the recordings that are created with this template. Formats not selected above are dimmed. Click the Optimize for Motion check box to enable.	The media servers configurations that are shown in the drop-down lists by default are those selected in the system defaults section of Site Settings . The Optimize for motion check box improves the quality of high-motion recordings.

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to download for portable devices		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Portable devices	<p>Select portable device(s) and whether you want audio and video or audio only:</p> <ul style="list-style-type: none"> • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible) 	<p>After the Content Server transcodes the recording, these outputs are available for download from the View Recordings page. Click the Download tab for the recording. Then click the output file that you want to download for synchronization with your portable device.</p> <p>iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.</p>

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to download for general purpose		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Formats	Select up to three formats.	—
Sizes	Select up to two sizes.	Because these outputs are downloaded and viewed on a computer, the quality of the internet connection is not an issue, except as the connection affects the time it takes to download. After downloading, users can watch the recordings without being connected to the internet.
Bit rates (kbps)	Displays the target bit rate for the small, medium and large output sizes.	—

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U		
Output layout	Click the layout to use.	<p>If the recording was created without a dual video stream, a file that shows the single video layout is created. The file shows the main video source.</p> <p>If the recording was created with a dual video stream, the main video and presentation streams are composited into a single video file. These different layouts determine where the main video and the presentation are placed in the composited video:</p> <ul style="list-style-type: none"> • Switching: the main video is replaced by the presentation when the presentation is activated. • Joined: the main video and presentation are displayed side by side. The main video is centered in the frame when the presentation is not activated. <ul style="list-style-type: none"> – Force 16:9: an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. • Stacked: the main video is reduced in size and displayed above the presentation. The main video is centered in the frame when the presentation is not activated. • Picture in picture: the main video is reduced in size and displayed in the selected corner of the frame over the presentation. The main video fills the whole frame when the presentation is not activated.
Media Experience Engine 3500	Select this option and a media server configuration (see Media Server Configurations) for Media Experience Engine 3500 to automate the process of uploading recorded content to your Media Experience Engine 3500 server.	The size of the output for Media Experience Engine 3500 is always large and always MPEG-4 format.
Show and Share	Select this option and a media server configuration (see Media Server Configurations) for Show and Share to automate the process of uploading recorded content to your Show and Share server.	Choose the size (Small , Medium or Large) of the output to upload to Show and Share.

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Podcast Producer	Select this option and a media server configuration (see Media Server Configurations) for Podcast Producer to automate the process of uploading recorded content to your Podcast Producer server.	The size of the output for Podcast Producer is always large.
iTunes U	Select this option and a media server configuration (see Media Server Configurations) for iTunes U to automate the process of uploading recorded content to an iTunes U account.	Choose the size (Small , Medium or Large) of the output to upload to iTunes U. You can also specify an additional audio-only output.
Summary		
Outputs to view in the Content Server web interface	Displays information about the outputs created for viewing in the Content Server web interface.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format, layout, and size. • The status of processing the output. • The physical path and filename if the media server configuration of the output adds recordings to the default media location. • How the output was transcoded (live or offline). If the output was transcoded live and there is no offline transcoded output, there is an option to Re-transcode. • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The on-demand URL. • The bandwidth in kbps (kilobits per second) and dimensions.

Table 7-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to download for portable devices	Displays information about the outputs created for Portable Devices.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • The physical path to the output and the output filename. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.
Outputs to download for general purpose	Displays information about the outputs created for download to users' computers.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • The physical path to the output and the output filename. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U	Displays information about the outputs created for use with Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U.	<p>The following information is shown for each output:</p> <ul style="list-style-type: none"> • A description: the format and layout. • The status of processing the output. • How the output was transcoded (offline). • The system name of the Content Server that did the transcoding (this may be a different Content Server if the Content Server is in a cluster). • The bandwidth in kbps (kilobits per second) and dimensions.

Create Recording

You can create a recording by:

- Entering the number or address of the endpoint or system that the Content Server should call to make the recording.
- Calling the Content Server from an endpoint or system. Call the Content Server with an H.323 ID, an E.164 alias, or a SIP address (URI).

To create a recording by entering the number or address that the Content Server should call, do the following:

-
- Step 1** In the web interface, log in to the Content Server as a creator.
- Step 2** From the **My Recordings** tab, click **Create recording**.
- Step 3** Select a recording alias from the **Recording alias** drop-down list.



Note For information about the create recording parameters, see the [Create Recording](#) section (Table 1-4).

- Step 4** Enter the number or address of the endpoint or system that the Content Server should call to make the recording. You can configure the settings in the Recording information and Recording permissions sections before, during, or after recording.
- Step 5** To join a password protected MCU conference, enter the PIN.
- Step 6** Update **Advanced call settings** as needed.
- Step 7** Click the **Place call** button when you are ready to start recording from the endpoint or system. If the recording alias that you use to record has the five-second countdown timer enabled, the countdown is displayed on the endpoint or system before recording starts. Recording starts when a red dot and 'Recording' is displayed on the endpoint or system.



Tip If you do not see the message or recording poster that confirms the Content Server has joined a password protected MCU conference on an endpoint that has joined the call, hang up and try the call again, ensuring that you enter the correct PIN.

- Step 8** Click the **End call** button when you are ready to stop recording.
- Step 9** Return to the web interface. Look for your recording in the **View Recordings** or **My Recordings** tab. From the My Recordings tab, you can [Edit Recordings](#).
-

To find the H.323 ID, E.164 alias, or SIP address to call, do the following:

-
- Step 1** In the web interface, log in to the Content Server as a creator.
- Step 2** From the **My Recordings** tab, click **Create recording options**.
- Step 3** Identify the H.323 ID, E.164 alias, or SIP address that you must use to record.

- Step 4** On the endpoint or system from which you are making the recording, call the Content Server by using the H.323 ID, E.164 alias, or SIP address to dial. When your endpoint or system is connected to the Content Server, you might see a five-second countdown timer before recording starts. Seeing this timer depends on how the recording alias that you are using was configured. Recording starts when a red dot and 'Recording' is displayed on the endpoint or system.
- Step 5** End the call when you are finished recording.
- Step 6** Return to the web interface. Look for your recording in the **View Recordings** or **My Recordings** tab. From the My Recordings tab, you can [Edit Recordings](#).
-

Edit Recording Aliases

From the **My Recordings** tab, the **Create recording options** page includes your personal recording alias if a site manager has made one for you. You can edit your recording alias by clicking **Edit** next to the alias name. From there, you can edit recording alias settings that are available for you to modify. For more information about recording aliases, see the [Recording Aliases](#) section. For information about the recording alias parameters, see the [Adding or Editing Recording Aliases](#) section ([Table 1-5](#)).

The following usage guidelines apply to editing recording aliases:

- Creators cannot add new recording aliases.
- Creators cannot edit the following recording alias properties:
 - Recording alias name
 - Recording alias type and owner
 - Call configuration
 - Dialing properties



Understanding Distribution Outputs

Site managers can configure the Content Server to upload recordings automatically to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U. Users with the appropriate permissions then can interact with uploaded recordings—for example, view, further distribute, or if possible, edit them—from those product interfaces.

If the Content Server has appropriate media server configurations, users with permissions can manually upload existing recordings to these products.



Note

For information about what users can do to recordings from the Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U interface, see the documentation for those products.

If you opt for this type of distribution, the Content Server acts as a recording and capture device. If recordings have no other outputs except the distribution output types through Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U, users cannot view these recordings on the Content Server.

This chapter includes these sections:

- [Configuring Automatic Upload to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U, page 8-1](#)
- [Uploading Existing Recordings to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U, page 8-2](#)
- [Understanding the Difference between Distribution Outputs and Streaming Servers, page 8-3](#)

Configuring Automatic Upload to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U

To automatically upload recordings from the Content Server to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U, site managers must configure a media server configuration and a template:

- Step 1** Create a media server configuration for the desired product. From the **Management** tab, go to **Recording Setup > Media server configurations**.

- Step 2** Click one of the following: **Add Media Experience Engine 3500 server configuration**, **Add Show and Share server configuration**, **Add Podcast Producer server configuration**, or **Add iTunes U server configuration**.
- Step 3** In the page that appears, configure settings to set up a relationship between the Content Server and the media server. See the [“Media Server Configurations” section on page 1-49](#) for information about these settings.
- Step 4** Create a template that has a distribution output that uses the server configuration that you created. From the **Management** tab, go to **Recording Setup > Templates**.
- Step 5** Click **Add template**.
- Step 6** In the page that appears, check **Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U**.
- Step 7** In Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U section, check the **Media Experience Engine 3500, Show and Share, Podcast Producer**, or **iTunes** box. You can check the box only if Content Server has a media server configuration for Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U.
- Step 8** From the Media server configuration drop-down menu, choose the desire media server configuration.
- Step 9** Configure any other settings for the template. See the [“Templates” section on page 1-41](#) for information about the other template settings.

Any recording that is created with a recording alias that uses the template that you made is automatically uploaded to the media server that is configured in that template. (See [Understanding Recording Aliases](#))

After the recording call is finished, the Content Server transcodes the recording in the specified size. When transcoding is finished, the Content Server uploads the recording file to the media server with the credentials that were specified in the media server configuration.

If a user uses the Content Editor on the Content Server to edit the length of a recording that has an output that was already uploaded to the media server, the Content Server transcodes the recording and uploads the newly edited version to the external media server. Previous versions of the recording on that media server are not overwritten; the media server can have a number of recordings of different lengths that are from one Content Server recording.

Uploading Existing Recordings to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U

Users with appropriate permissions can upload any existing recording to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U:

-
- Step 1** Locate the recording that you want to upload to an external media server. For that recording, click **Manage outputs**.
 - Step 2** In the page that appears, check **Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U**.

- Step 3** In the Outputs for distribution to Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U section, check the **Media Experience Engine 3500, Show and Share, Podcast Producer**, or **iTunes U** box. You can check the box only if Content Server has a media server configuration for Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U.
- Step 4** From the Media server configuration drop-down menu, choose the desired media server configuration.
- Step 5** For Show and Share or iTunes U, choose the recording size from the **Size** drop-down menu.
- Step 6** Click **Save**.
-

After you click **Save**, the Content Server transcodes the recording in the specified size. When transcoding is finished, the Content Server uploads the recording file to the media server with the credentials that were specified by the site manager in the media server configuration.

If a user uses the Content Editor on the Content Server to edit the length of a recording that has an output that was already uploaded to the media server, the Content Server transcodes the recording and uploads the newly edited version to the external media server. Previous versions of the recording on that media server are not overwritten; the media server can have a number of recordings of different lengths that are from one Content Server recording.

Understanding the Difference between Distribution Outputs and Streaming Servers

From the **Management** tab, you can configure both media servers for distribution outputs and media servers for streaming by going to **Configure > Media server configurations**. You can configure a relationship between the Content Server and one of the these types of media servers in your network:

- Windows Media streaming server
- QuickTime or Darwin streaming server
- Wowza Media Server for Flash
- Media Experience Engine 3500
- Show and Share
- Podcast Producer
- iTunes U

The first four media servers stream recordings from those servers, but users view those recordings through the Content Server web interface. Streaming servers extend the scale and capabilities for streaming live and recorded calls; add the ability to live stream MPEG-4 for QuickTime and MPEG-4 for Flash; provide on-demand true streaming of MPEG-4 for QuickTime and MPEG-4 for Flash; and deliver live and on-demand media via the Adobe HTTP Dynamic Streaming protocol.

The last four media servers support distribution outputs, not streaming outputs.



Maintaining the Content Server

This chapter includes the following Content Server maintenance procedures:

- [Backing Up the Content Server, page 9-1](#)
- [Restoring Files, page 9-3](#)
- [Performing a Software Reimage, page 9-5](#)
- [Restoring Files After a Software Reimage, page 9-9](#)
- [Shutting Down and Powering Off the Content Server, page 9-11](#)
- [Securing the Content Server, page 9-12](#)

Backing Up the Content Server

To ensure that you do not lose data, you should back up the Content Server on a regular basis. You should also back up the Content Server before you install a security update, or perform a software reimage. See these sections:

- [Before Backing Up, page 9-2](#)
- [Performing a Manual Backup, page 9-2](#)
- [Configuring a Scheduled Backup, page 9-2](#)

Before Backing Up

You can back up Content Server files to an external USB drive, to a network drive, or to a network share. The backup procedure captures all Content Server data and media files and portal configuration (call configurations, site settings, media servers, templates, recording aliases, etc).

The Content Server backup procedure does not backup the Windows Server 2008, Internet Authentication Service (IAS)/Network Policy Server (NPS), or Windows Media Services (WMS) configurations. If you are experiencing difficulties with the Content Server operating system, you should perform a software reimage to restore the operating system and reconfigure the Windows services. See

the “Performing a Software Reimage” section on page 9-5.

The Content Server backup procedure does not back up media files that are located on a Network Attached Storage (NAS) device or on an external media server. You should back up the media on the external devices at the same time as the Content Server. If you restore from backup, you must restore the media backup taken at the same time as the Content Server backup. Otherwise, you might not be able to play some recordings.

If you are using an external USB drive for a manual or schedule backup, connect the drive to a USB port on the Content Server rear panel. Log in to the Content Server by using Windows Remote Desktop Connection and confirm that the USB hard drive appears under My Computer. Also, make sure that there is sufficient capacity on the USB drive or network drive for the backed-up files.

Performing a Manual Backup

To perform a manual on-demand backup, follow these steps:

-
- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection. Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
 - Step 2** In the Actions menu, click **Backup Once**. The Backup Once Wizard window appears. To create a backup now, click the **Different options** radio button. Click **Next**.
 - Step 3** In the Select Backup Configuration window, click the **Full server** radio button. Click **Next**.
 - Step 4** In the Specify Destination Type window, choose the type of storage (local drive or remote shared folder) for the backup. Click **Next**.
 - Step 5** Specify the USB drive or network location for the backed-up files. Type a name for the backup. Click **Next**.
 - Step 6** In the Confirmation window, click **Backup**. The Backup Progress window displays the backup progress and status details. The backup process takes approximately 10 minutes per 5 GB of data.
 - Step 7** When the backup is complete, click **Close**.
-

Configuring a Scheduled Backup

To configure a scheduled backup, follow these steps:

-
- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection. Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
 - Step 2** In the Actions menu, click **Backup Schedule**. The Backup Schedule Wizard, Getting Started pop up window appears. Click **Next**.
 - Step 3** In the Select Backup Configuration window, click the **Full server** radio button. Click **Next**.
 - Step 4** In the Specify Backup Time window, enter how often and when to run the backup. Click **Next**.
 - Step 5** In the Specify Destination Type window, choose the storage location (local drive or remote shared folder) for the backup. Click **Next**.

If you select a shared folder location, each backup will erase the previous backup and only the latest backup will be available.

- Step 6** Specify the USB drive or network location for the backed-up files. Type a name for the backup. For a remote shared folder location, enter the username and password for scheduling the backup on the network share. Click **Next**.
- Step 7** In the Confirmation window, review your settings for the scheduled backup. Click **Finish**.
The backup process is now scheduled to run according to the schedule that you entered.
-

Restoring Files

You can restore all Content Server files and portal configuration, or specific folders and files. See these sections:

- [Before Restoring, page 9-3](#)
- [Restoring from a Backup, page 9-4](#)

If you want to restore files after performing a software reimage see this section:

- [Restoring Files After a Software Reimage, page 9-9](#)

Before Restoring

Make sure that you are using a backup that was taken from the same Content Server that you are restoring. If you want to restore to a different Content Server, contact your Cisco reseller.

If your media files are located on a NAS or on an external media server, the Content Server restore procedure does not restore those files. You must have a media backup that was taken at the same time as the Content Server backup and you must also restore this media backup. Otherwise, you might not be able to play some recordings.

The Content Server backup procedure captures all Content Server data and media files and portal configuration (call configurations, site settings, media servers, templates, recording aliases, etc). You can restore all Content Server files and portal configuration, or specific folders and files. The [Restoring from a Backup](#) procedure describes how to recover all Content Server files and portal configuration.

The Content Server restore procedure does not restore the original Windows Server 2008, IAS/NPS, or WMS default settings. If you are experiencing difficulties with the Content Server operating system, you should perform a software reimage to restore the operating system and reconfigure the Windows services. See the [“Performing a Software Reimage” section on page 9-5](#). To restore data and media files following a software reimage, see [“Restoring Files After a Software Reimage”](#).

If you are using an external USB drive to restore backed-up files, connect the drive to a USB port on the Content Server rear panel. Log in to the Content Server by using Windows Remote Desktop Connection and confirm that the USB hard drive appears under My Computer.

Restoring from a Backup

To restore the Content Server from a backup, follow these steps:

- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection. Go to **Start > Administrative Tools > Windows Services**. The Windows Services window appears.

- Step 2** In the Services window, **Stop** these services:
- a. SQL Server (Content Server)
 - b. Content Server Content Engine
 - c. Content Server Control Service
 - d. Content Server Helper Tool
 - e. Content Server Offline Transcode Engine
- Step 3** Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
- Step 4** In the Actions menu, click **Recover**. The Recovery Wizard window appears. To select a stored backup, click the **A backup stored on another location** radio button. Click **Next**.
- Step 5** In the Specify Location type window, select the location of the backup file that you want to use for recovery. Click **Next**.
- Step 6** Enter the path of the storage location (local drive or remote shared folder) for the backup file that you want to use to recovery. Click **Next**.
- Step 7** In the Select Backup Date window, choose the backup file date. Click **Next**.
- Step 8** In the Select Recovery Type window, click the **File and Folders** radio button. Click **Next**.
- Step 9** In the Select Items to Recover, select a drive (C: or E:) to recover. To restore all Content Server files, you will need to recover each drive one at a time. Click **Next**.
- Step 10** In the Specific Recovery Options window, enter the recovery destination drive (that you specified in [Step 9](#)) to overwrite. Click the **Overwrite the existing versions with the recovered versions** radio button. Click **Next**.
- Step 11** In the Confirmation window, click **Recover**. The Recovery Progress window displays the recovery progress and status details.
- Step 12** Repeat [Step 4](#) to [Step 11](#) to restore the second Content Server drive. When the recovery of both drives is complete, click **Close**.
- Step 13** Restart the services that you stopped in [Step 2](#).

Performing a Software Reimage

To return a Content Server to the factory-default software, you can perform a software reimage. This procedure clears the server hard drive and then reinstalls the Content Server system software.

You should backup the Content Server before performing a software reimage. See the [“Backing Up the Content Server”](#) section on page 9-1.



Caution

Content Server Release 6.0 software cannot be installed on first- or second-generation Content Server hardware. If you attempt to run the USB media kit 6.0 installer on older hardware it will fail and could cause unrecoverable damage to the Content Server.

The device serial number is on a label located on the top right hand front of the Content Server, and in the web interface (go to **Management > Diagnostics > Server overview**). These are the device serial number formats:

- Third-generation serial number: **49A3xxxx**
- Second-generation serial number: **49A2xxxx**
- First-generation serial number: **49A0xxxx**

You must have administrator privileges to perform a software reimage.

These are the software reimage tasks:

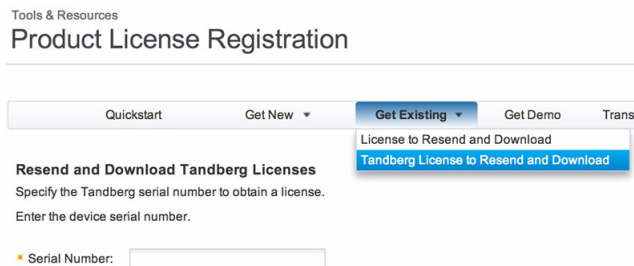
- [Task 1: Clear the hard drive and install the software, page 9-6](#)
- [Task 2: Install the license files, page 9-7](#)
- [Task 3: Configure the basic settings, page 9-8](#)

After you complete the software reimage, see the [“Restoring Files After a Software Reimage”](#) section to restore the data and media files on the Content Server.

Reimage Instructions

You need these items to complete the Content Server software reimage:

- Content Server Release 6.x USB media kit
- USB keyboard, mouse, and VGA monitor
- IP address, subnet mask, and gateway for the Content Server
- Content Server license files
 - Go to cisco.com/go/license and log in. Choose **Get Existing > Tandberg License to Resend and Download**
 - Enter the Content Server serial number in the 49A3xxxx format in the Serial Number field



If you need assistance obtaining the Content Server license files, you can open a case with Cisco TAC: <http://www.cisco.com/cisco/web/support/index.html>

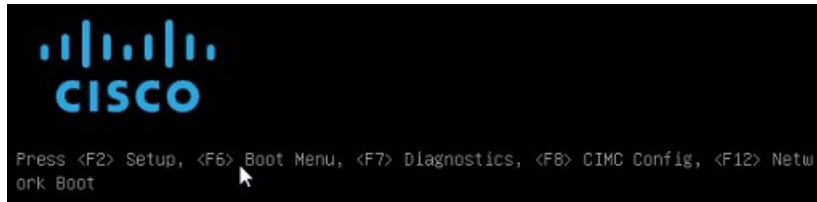
Task 1: Clear the hard drive and install the software

Follow these steps:

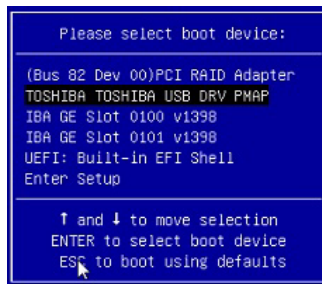
-
- Step 1** Disconnect any external hard drives or USB drives from the Content Server.
 - Step 2** Install the USB drive in a USB port on the Content Server rear panel.
 - Step 3** Use the supplied KVM cable to connect a USB keyboard, mouse, and a VGA monitor to the KVM connector on the Content Server front panel.

Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you do so, the first VGA connector is disabled.

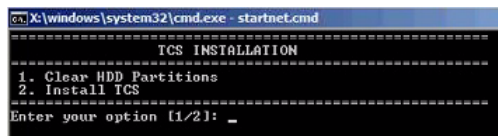
- Step 4** Log in to the Content Server Windows Server Manager. Verify that the USB drive is installed by going to **Start > Computer > Removable Disk (USB drive:)**.
- Step 5** Restart the Content Server. Go to **Start > Log off > Restart > Application Installation (Planned)**.
- Step 6** In the BIOS utility, press **F6** to select the Boot Menu.



- Step 7** When the boot device menu appears, choose **Toshiba USB DRV PMAP** and press **Enter**.



- Step 8** Wait while Windows restarts and boots from the USB drive. The system will cycle through several screens. This could take a few minutes.
- Step 9** When the Content Server Installation menu appears, choose number **1** (Clear HDD Partitions) and press **Enter**.



- Step 10** After clearing the hard drive the Content Server restarts and reboots from the USB drive. When the Content Server Installation menu appears, choose number **2** (Install Content Server) and press **Enter**.
- Step 11** When the installation process is complete, the Content Server restarts. Continue with [Task 2: Install the license files](#).

Task 2: Install the license files

Follow these steps:

- Step 1** Log in to the Content Server Windows Server Manager by using the default password, **Cisco123**.

- Step 2** Go to **Start > Computer > Removable Disk (USB drive) > Tools**. Copy the generic **Licensedata** text file to the Content Server (any folder). The generic license file has these entries that you need to overwrite with your specific license key information:

```
<<Content Server Software Serial No>>
<<Checksum>>
<<Release Key>>
<<R5 Key>>
<<L2 Key>>
```

- Step 3** Obtain your Content Server Checksum and License Release Keys from Cisco.com.

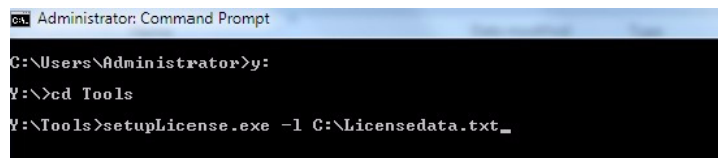
- Step 4** Open the text file that has your specific license key information. Select each data line one at a time, copy, and then overwrite each data line in the generic license file. There should be no extra spaces or lines after you transfer the data to the generic license file.

This example license file shows the Content Server software serial number, the checksum, and three release keys:

```
49A30099
2c:20:23:7a:5f:4a:e1:80:f8:ae:5f:8a:77:a5:25:a7:70:46:4d:19:0d <checksum output truncated>
7892490445634702
114371R5-1-DAB1697D
116381L2-1-6E0429AA
```

- Step 5** Save and close the generic **Licensedata** text file on the Content Server.


- Step 6** Go to **Start > Command Prompt** to run the License Install application. Change the directory to **USB drive > Tools**; and run the **setupLicense.exe -l Licensedata.txt file-path**.



```
Administrator: Command Prompt
C:\Users\Administrator>y:
Y:\>cd Tools
Y:\Tools>setupLicense.exe -l C:\Licensedata.txt_
```

- Step 7** When the setup application is finished, it will display “Successfully read license data from licenseData.txt” and other specific license information.

- Step 8** In the Command Prompt window, enter **restore.bat**.



```
Administrator: Command Prompt
S:\Tools>restore.bat
```

- Step 9** Close the Command Prompt window and restart the Content Server. Go to **Start > Log off > Restart > Application Installation (Planned)**.

- Step 10** Remove the USB drive from the Content Server rear panel. Continue with [Task 3: Configure the basic settings](#).

Note To install additional license keys such as the cluster, premium resolution, or port options, complete the Content Server basic configuration. Navigate to the user interface. Go to **Management > Configuration**. In the Software option area add the license option keys. Click **Restart service** to activate the license keys.

Task 3: Configure the basic settings

After the software reimage, you should reset the administrator password, assign an IP address, set the date and time, and enable Windows Remote Desktop Connection. For more information about the Content Server initial configuration, see the [Cisco TelePresence Content Server Release Quick Start Guide](#) on Cisco.com. Follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Go to Start > Control Panel > User Accounts > Change your Windows password > Change your password . |
| Step 2 | In the Change your password window, enter the current password (Cisco123), the new password, and confirm the new password. Click Change password . Click OK . |
| Step 3 | Go to Start > Control Panel > Network and Internet . From the Network and Sharing Center, click View network status and tasks . |
| Step 4 | In the Connect or disconnect section, click Local Connection . Choose IPv4 from the list. In the IPv4 Properties window, click the Use the following IP address radio button. Enter the Content Server <i>IPv4 address</i> , <i>subnet-mask</i> , and <i>default-gateway</i> . Click OK . |
| Step 5 | In the Server Manager window, click the time and date box in the lower right corner to open the settings window. Or, go to Start > Control Panel > Clock, Language, and Region > Set the time and date . |
| Step 6 | Click Change date and time settings . Update the date, time, and time zone. Click OK . |
| Step 7 | Go to Start > Control Panel > System Security > System > Remote Settings . |
| Step 8 | From the System Properties window Remote tab, select and click a radio button to enable Remote Desktop on the Content Server. Click OK . |
| Step 9 | Restart the server. Go to Start > Log Off > Restart . (Optional) Continue with Restoring Files After a Software Reimage . |
-

You can now disconnect the KVM cable from the Content Server and continue configuring the server by accessing the Content Server user interface and by using Windows Remote Desktop Connection.

Restoring Files After a Software Reimage

After you complete the Content Server software reimage, you should restore the files that you backed up before the reimage. This will restore all Content Server data and media files and portal configuration (call configurations, site settings, media servers, templates, recording aliases, etc). See these sections:

- [Restore Files on a Reimaged Standalone Content Server, page 9-9](#)
- [Restore Files on a Reimaged Content Server with Network Attached Storage, page 9-10](#)
- [Restore Files on a Reimaged Content Server in a Cluster, page 9-10](#)

Restore Files on a Reimaged Standalone Content Server

Follow these step to restore files on the Content Server after completing the “[Performing a Software Reimage](#)” procedure:

-
- Step 1** Log in to the Content Server by using Windows Remote Desktop Connection. Go to **Start > Administrative Tools > Windows Services**. The Windows Services window appears.
- Step 2** In the Services window, stop these services:
- a. SQL Server (Content Server)
 - b. Content Server Content Engine
 - c. Content Server Control Service
 - d. Content Server Helper Tool
 - e. Content Server Offline Transcode Engine
- Step 3** Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
- Step 4** In the Actions menu, click **Recover**. The Recovery Wizard window appears. To choose a stored backup, click the **A backup stored on another location** radio button. Click **Next**.
- Step 5** In the Specify Location type window, choose the location of the backup file that you want to use for recovery. Click **Next**.
- Step 6** Enter the path of the storage location (local drive or remote shared folder) for the backup file that you want to use for recovery. Click **Next**.
- Step 7** In the Select Backup Date window, choose the backup file date. Click **Next**.
- Step 8** In the Select Recovery Type window, click the **File and Folders** radio button. Click **Next**.
- Step 9** In the Select Items to Recover, choose only drive **E:** to recover. Click **Next**.
- Step 10** In the Specific Recovery Options window, enter the recovery destination drive E: to overwrite. Click the **Overwrite the existing versions with the recovered versions** radio button. Click **Next**.
- Step 11** In the Confirmation window, click **Recover**. The Recovery Progress window displays the recovery progress and status details. When the recovery process is finished, click **Close**.
- Step 12** Restart the services that you stopped in [Step 2](#). Restart the Content Server.
-

Restore Files on a Reimaged Content Server with Network Attached Storage

Follow these step to restore files on the Content Server with NAS after completing the [“Performing a Software Reimage”](#) procedure:

-
- Step 1** Add the Content Server to the same domain as the NAS. For more information, see [Chapter 13, “Setting Up External Media Storage.”](#)
- Step 2** Log in to the Content Server by using Windows Remote Desktop Connection.
- Step 3** Run the Content Server Wizard and click **Alternate Storage [NAS] Wizard**. Follow the on-screen instructions to configure the NAS.
- Step 4** Go to **Start > Administrative Tools > Windows Services**. The Windows Services window appears.
- Step 5** In the Services window, stop these services:
- a. SQL Server (Content Server)

- b. Content Server Content Engine
 - c. Content Server Control Service
 - d. Content Server Helper Tool
 - e. Content Server Offline Transcode Engine
 - Step 6** Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
 - Step 7** In the Actions menu, click **Recover**. The Recovery Wizard window appears. To select a stored backup, click the **A backup stored on another location** radio button. Click **Next**.
 - Step 8** In the Specify Location Type window, choose the location of the backup file that you want to use for recovery. Click **Next**.
 - Step 9** Enter the path of the storage location (local drive or remote shared folder) for the backup file that you want to use for recovery. Click **Next**.
 - Step 10** In the Select Backup Date window, choose the backup file date. Click **Next**.
 - Step 11** In the Select Recovery Type window, click the **File and Folders** radio button. Click **Next**.
 - Step 12** In the Select Items to Recover window, select only drive **E:** to recover. Click **Next**.
 - Step 13** In the Specific Recovery Options window, enter the recovery destination drive **E:** to overwrite. Click the **Overwrite the existing versions with the recovered versions** radio button. Click **Next**.
 - Step 14** In the Confirmation window, click **Recover**. The Recovery Progress window displays the recovery progress and status details. When the recovery process is finished, click **Close**.
 - Step 15** Restart the services that you stopped in [Step 5](#). Restart the Content Server.
-

Restore Files on a Reimaged Content Server in a Cluster

Follow these step to restore files on a Content Server in a cluster after completing the [“Performing a Software Reimage”](#) procedure:

- Step 1** Add the Content Server to the same domain as the NAS. For more information, see [Chapter 13, “Setting Up External Media Storage.”](#)
- Step 2** Log in to the Content Server by using Windows Remote Desktop Connection.
- Step 3** Run Content Server Wizard and click the **Cluster Management Wizard**. Follow the on-screen instructions to configure the cluster. For more information, see [Chapter 6, “Creating and Managing a Content Server Cluster.”](#)
- Step 4** Configure the cluster by using the ClusterSettings.xml file. Make sure that the NAS path/external database is the same and is available.
- Step 5** Go to **Start > Administrative Tools > Windows Services**. The Windows Services window appears.
- Step 6** In the Services window, stop these services:
 - a. SQL Server (Content Server)
 - b. Content Server Content Engine
 - c. Content Server Control Service
 - d. Content Server Helper Tool

e. Content Server Offline Transcode Engine

- Step 7** Go to **Start > Administrative Tools > Windows Server Backup**. The Windows Server Backup window appears.
- Step 8** In the Actions menu, click **Recover**. The Recovery Wizard window appears. To select a stored backup, click the **A backup stored on another location** radio button. Click **Next**.
- Step 9** In the Specify Location Type window, choose the location of the backup file that you want to use for recovery. Click **Next**.
- Step 10** Enter the path of the storage location (local drive or remote shared folder) for the backup file that you want to use for recovery. Click **Next**.
- Step 11** In the Select Backup Date window, choose the backup file date. Click **Next**.
- Step 12** In the Select Recovery Type window, click the **File and Folders** radio button. Click **Next**.
- Step 13** In the Select Items to Recover window, select only drive **E:** to recover. Click **Next**.
- Step 14** In the Specific Recovery Options window, enter the recovery destination drive E: to overwrite. Click the **Overwrite the existing versions with the recovered versions** radio button. Click **Next**.
- Step 15** In the Confirmation window, click **Recover**. The Recovery Progress window displays the recovery progress and status details. When the recovery process is finished, click **Close**.
- Step 16** Restart the services that you stopped in [Step 6](#). Restart the Content Server.

Shutting Down and Powering Off the Content Server

The server can run in two power modes:

- Main power mode—Power is supplied to all server components and any operating system on your drives can run.
- Standby power mode—Power is supplied only to the service processor and the cooling fans and it is safe to power off the server from this mode.

You can invoke a graceful shutdown or an hard shutdown by using either of the following methods:

- Use the Cisco Integrated Management Controller (CIMC) management interface. For more information, see the [Cisco TelePresence Content Server Release Quick Start Guide](#) and the [Cisco UCS C220 Server Installation and Service Guide](#) on Cisco.com.
- Use the Power button on the server front panel.

To use the Power button, do the following:

- Step 1** Stop any recording calls that are in progress on the Content Server.
- Step 2** Check the color of the Power Status LED.
- Green—the server is in main power mode and must be shut down before it can be safely powered off.
 - Amber—the server is already in standby mode and can be safely powered off.
- Step 3** Invoke either a graceful shutdown or a hard shutdown:



Caution

To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system.

- Graceful shutdown—Press and release the Power button. The operating system performs a graceful shutdown and the Content Server goes to standby mode, which is indicated by an amber Power Status LED.
- Emergency shutdown—Press and hold the Power button for four seconds to force the main power off and immediately enter standby mode.

Step 4 Disconnect the power cords from the power supplies in the Content Server to completely power off the server.

Securing the Content Server

Antivirus Protection

You can use antivirus protection on the Content Server. If using antivirus software we recommend that you do not scan the **E:** volume or the **C:\program files\Tandberg** directory where the data files are located.

Microsoft Security Patches

You can apply Microsoft security patches to the Content Server. We recommend that you download and install the patches during normal maintenance windows. You can manually install recommended patches from the Microsoft website or use Windows Update.

Content Server security bulletins inform you of patches that we recommend, or not recommend (because of known instability issues with the Content Server application). These bulletins are published if aspects of Microsoft patches are critical to performance or security of the Content Server.

You can access the latest Content Server security bulletins on Cisco.com:

<http://www.cisco.com/c/en/us/support/conferencing/telepresence-content-server/products-field-notices-list.html>

http://www.cisco.com/en/US/products/ps11347/prod_bulletins_list.html

Joining the Content Server to a Domain

The Content Server can be joined to a Microsoft Active Directory Domain in the same way as any Windows Server 2008 server. Domain group policies may be applied to the Content Server.

The Content Server must be joined to a domain to configure external storage or a cluster of Content Servers.

Do not apply any policy that:

- Changes the Administrator account name. If the Administrator account name is changed, the Serial Port/LCD panel password reset tool will not work.
- Restricts the guest group. This will disable the IIS user account. The IIS user account is necessary to provide the web user interface for the Content Server.



Caution

Other group policies might restrict services required for the Content Server to function. We recommended that you test the Content Server after each new group policy is applied before making the Content Server available to users in the production environment.



Port Information

Table 10-1 *Ports Used by the Content Server*

Port	Transport Layer Protocol	Used By	Open on the Content Server Firewall
80	TCP	Content Server web interface (HTTP)	Yes
443	TCP	Content Server web interface using SSL (HTTPS)	Yes
554	TCP, UDP	Windows Media Streaming Server RTSP Protocol	Yes
1718	UDP	Gatekeeper discovery	Yes
1719 ¹	UDP	RAS port	Yes
1722 ¹	UDP	Additional RAS port when in a cluster	Yes
1720 ¹	TCP	Q.931 port	Yes
1721 ¹	TCP, UDP	Additional Q.931 port when in a cluster	Yes
1755	TCP, UDP	Windows Media Streaming Server MMS Protocol	Yes
2090	TCP	Content Server database connection	No
3389	TCP	Remote Desktop Connection Protocol	Yes
8008	TCP	Content Server application communication	No
8080	TCP	Windows Media Streaming Server HTTP Protocol	Yes
8096	TCP	Windows Media Administration Site using SSL	Yes

1. This port is configurable in [Site Settings](#) when in a cluster.

This table does not include any ports used in site settings or manually configured media server configurations for streaming to external streaming servers—for example:

- **Port range** in Advanced H.323 Settings in [Site Settings](#).
- **Network pull port(s)** for Windows Media streaming servers. For more information, see the Windows Media Services help topics.

- **Streaming port range start** specified for unicast streaming on Windows Media streaming server; QuickTime or Darwin streaming servers; Wowza Media Servers for Flash; or multicast streaming in QuickTime or Darwin streaming servers.

Ports for Streaming from the Content Server

Streaming Windows Media from the Content Server uses the following ports:

Table 10-2 *Ports Used for Streaming Windows Media from the Content Server*

Port	Streaming Media Protocol	Firewall Information
554	RTSP	At least one of these ports needs to be open between the Content Server and the Windows Media player. For true (RTSP) streaming, open port 554. See the note below.
8080	HTTP	



Note

The Windows Media player will automatically use protocol rollover if necessary. The default streaming protocol for the Windows Media player is RTSP on port 554. If the player cannot obtain the stream using RTSP (because the port is blocked on a firewall, for example), then it will automatically rollover to MMS. MMS (port 1755) is a deprecated streaming protocol and is not used as a streaming transport for Windows Media Player version 9 and above. The player will then try HTTP on port 80. The Content Server will redirect any requests for Windows Media streams on port 80 to the correct HTTP port used by the Windows Media Streaming Server on the Content Server (port 8080).

Streaming Windows Media from the Content Server to the Silverlight player uses the following port:

Table 10-3 *Port Used for Streaming Windows Media from the Content Server to Silverlight Player*

Port	Streaming Media Protocol	Firewall Information
8080	HTTP	Needs to be open between the Content Server and the Silverlight player.



Note

The Silverlight player will request the stream on port 80 because this is the default HTTP port. The Content Server will redirect any requests for Windows Media streams on port 80 to the correct HTTP port used by the Windows Media Streaming Server on the Content Server (port 8080).

MPEG-4 for QuickTime and MPEG-4 for Flash from Content Server using the default “Local IIS Web Server” media server configuration use the following port:

Table 10-4 *Port Used by MPEG-4 for QuickTime and MPEG-4 for Flash from Content Server using the default “Local IIS Web Server” Media Server Configuration*

Port	Streaming Media Protocol	Firewall Information
80	HTTP	Needs to be open between the Content Server and the player.

Ports for Streaming from External Streaming Servers

The default setup for a Windows Media Streaming Server uses the following ports:

Table 10-5 *Ports Used in the Default Setup for Windows Media Streaming*

Port	Streaming Media Protocol	Firewall Information
554	RTSP	At least one of these ports needs to be open between the Content Server and the Windows Media player. For true (RTSP) streaming, open port 554. See the note below. If using server push in the media server configuration, ensure that the HTTP port is open between the Content Server and the external streaming server.
80	HTTP	



Note

The Windows Media player will automatically use protocol rollover if necessary. The default streaming protocol for the Windows Media player is RTSP on port 554. If the player cannot obtain the stream using RTSP (because the port is blocked on a firewall, for example), then it will automatically rollover to MMS. MMS (port 1755) is a deprecated streaming protocol and is not used as a streaming transport for Windows Media Player version 9 and above. The player will then try HTTP on port 80.

The default setup for a QuickTime or Darwin streaming server uses the following port:

Table 10-6 *Port Used in Default Setup for QuickTime or Darwin Streaming Server*

Port	Streaming Media Protocol	Firewall Information
554	RTSP	Needs to be open between the Content Server, the external streaming server, and the QuickTime player.

The default setup for a Wowza Media Server for Flash uses the following ports:

Table 10-7 *Ports Used in the Default Setup for Wowza Media Server for Flash*

Port	Streaming Media Protocol	Firewall Information
554	RTSP for communication between the Content Server and the Wowza Media Server.	Needs to be open between the Content Server and the Wowza Media Server.
1935	RTMP for communication between the Wowza Media Server and the Flash player.	Needs to be open between the Wowza Media Server and the Flash player.



Premium Resolution

The optional Premium Resolution license enables performance enhancements to the Content Server video-conference bandwidths, frame rates, and recording and streaming resolutions. It also provides the ability to playback recordings from endpoints.

[Table 11-1](#) shows the Premium Resolution performance metrics of recording files for download, recording files for streaming in the Content Server portal, and for streaming live video from an endpoint.

Table 11-1 Premium Resolution Performance Metrics

Function	With Premium Resolution Option	Without Premium Resolution Option
Maximum call speed	4 Mbps	2 Mbps
Maximum recording resolution (for download)	1080p30 or 720p60	w448p30
Live streaming resolution	720p30	w448p30
On-demand web streaming resolution (viewing in the Content Server portal)	720p60	w448p30
Presentation stream recording codec ¹	H.264	H.261 H.263 H.263+
Watching a recording from an endpoint	Yes	No

1. The presentation stream is recorded at the maximum resolution that the endpoint, that is acquiring the presentation stream, is able to encode—up to the maximum resolution settings for each recording.



Note

The Content Server does not record HD resolution if a connected device (endpoint, laptop or PC) shares a presentation in a lower resolution. The recording will be transcoded in the lower resolution regardless of whether or not a Premium Resolution license is installed. (CSCum08630)

Configuring and Using the Premium Resolution Features

To install the Premium Resolution license key, navigate to the Content Server user interface. Go to **Management > Configuration**. In the Software option area add the license option key. Click **Restart service** to activate the license key.

To enable the playback of a recording from an endpoint, navigate to **Management > Recordings > Create recording**. Expand the Full recording information and permissions section. In the Play recordings on endpoints section, click the **Make finished recording available for playing on endpoints** check box. Enter a four-digit PIN (optional) to access the recording.

To enter the playback H.323 gateway prefix or playback E.164 gateway prefix, navigate to **Management > Configuration > Site settings**. In the Gatekeeper settings area, enter the playback H.323 or E.164 gateway prefix.

To enable automatic playback for new recordings created with your personal recording alias, edit your recording alias and select **Make finished recording available for playing on endpoints**.

To play back an existing recording from an endpoint, select **Make recording available for playing on endpoints** in the Play recording on endpoints section of the Edit recording page and save. The playback address for your recording is displayed under the option that you just selected.

For more information about the Premium Resolution option with Content Server clusters, see the Important Guidelines section in the “Creating and Managing a Content Server Cluster” chapter.

Watch Recordings from an Endpoint

You can view Content Server recordings on an endpoint by dialing the playback H.323 ID or E.164 alias of the recording from your endpoint. Playback addresses for recordings are displayed on the Edit recording page and in the email sent from the Content Server when a call has finished.

If you play back your recordings on endpoints that support presentation, you can toggle between layouts. You can pause and resume playback by pressing any Dual-Tone Multi Frequency (DTMF) key.

Playback from endpoints is available only for H.323 and interworking calls, with a maximum of two calls per Content Server.

Pause and Resume from a Cisco IP Video E20 (TE4.0) Endpoint

If you play back your Content Server recording from an E20 endpoint, you will get an in-call soft button option to Pause playback. In Paused mode, a timeline appears with the time elapsed from the beginning of the recording and the total time. Press the Resume soft button to continue viewing the recording. Press the call disconnect button to stop playback when you are done.

Review Recordings from a Cisco IP Video E20 (TE4.0) Endpoint

When you are making a recording on a Content Server from an E20 endpoint, soft buttons in the E20 interface will provide in-call options to stop the recording (Stop) and then either review what you have just recorded (Review), or delete the last take recorded and start a new recording (Redo). You can record as many takes as you want and only the last one will be saved.

When you are finished, press the Save and End soft button or the call disconnect button to end the call. This will save the last recording that you made.

Review recording options are available in calls to recording aliases that have no live streaming outputs. Calls with a live streaming output will only display a Save and End option.

Review recording is available in up to five calls per Content Server.



Understanding Recording Aliases

The Content Server records calls and can produce the resulting recordings in a range of formats and sizes for users to watch or download. Creators of recordings can make recordings available to all or selected users.

To make recordings, creators must use a recording alias. A recording alias defines several properties, including ones related to dialing the Content Server from an endpoint for the recording session; specifying recording outputs; and indicating viewing and editing permissions (see [Recording Alias Properties](#)).

There are two types of recording alias:

- System recording aliases, which can be used by any user in the creator or site manager role.
- Personal recording aliases, which have owners in the creator role. Owners can edit certain parts of their recording aliases: recording settings, default recording information, and default recording permissions.



Note We recommend that site managers create one or more personal recording aliases for each group or user in the creator role. For Content Servers that are registered to a H.323 gatekeeper as gateway, a personal recording alias can be automatically created for each user with Creator privileges when the user logs in to the Content Server web interface (see [Site Settings](#)).

Recording Alias Properties

To create a new recording alias, you must log in as a site manager. Then in the **Management** tab, go to **Recording setup > Recording aliases: Add recording alias**.

The following are the properties of every recording alias:

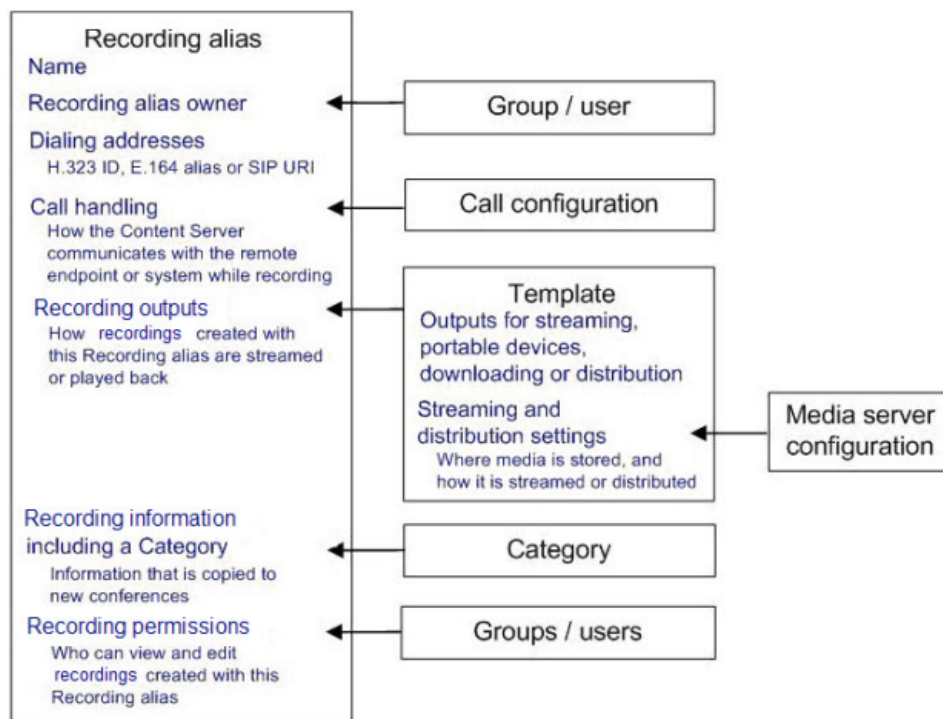
- Name—The recording alias name can be selected when scheduling a recording in TMS. Site managers can also use the name to create recordings from **Recordings > Create Recording**.
- Recording alias owner—The owner must have the creator role. In the site manager role, you must add creators in **Configure > Groups and Users** first. Then in the Add recording alias page, you can choose an owner from the **Personal recording alias owner** drop-down menu if you are creating a personal recording alias. Owners can edit certain parts of their recording aliases.
- Dialing addresses—Dialing is done with an H.323 ID, E.164 alias, or SIP URI, depending on how the gatekeeper and SIP settings are configured in **Configure > Site Settings**. The dialing address is used to call to Content Server and record with this recording alias.

- **Call handling**—These properties determine how the Content Server communicates with remote endpoints or systems while recording (for example, call speeds, call length, and encryption). In the role of site manager, you set call handling properties in call configurations (**Recording setup > Call Configurations**). Then in the Add recording alias page, you can choose an available call configuration from the **Call configuration** drop-down menu.
- **Recording outputs**—These properties determine how a recording is displayed to viewers (for example, format and size). In the site manager role, you set recording outputs in templates (**Recording setup > Templates**). Templates can also contain media server configurations (**Recording setup > Media Server Configurations**). These configurations contain settings for where recording media are stored and how a recording is streamed or distributed. After templates have been created, in the Add recording alias page, you can choose an available template from the **Template** drop-down menu.
- **Recording information including a category**—These properties include ways for viewers to more easily identify recordings that are made with this alias (for example, a description, the recording speaker, and copyright information). These properties are used for every recording that uses this alias, but users with editing permissions can modify many of these properties on a recording-by-recording basis.

A category is a way to group recordings together in the View Recordings list (for example, under “Announcements” or “News”). In addition to the categories that come pre-configured on the Content Server, site administrators can create new categories (**Recording setup > Categories**). In the Add recording alias page, you can choose a category from the **Category** drop-down-list.
- **Recording permissions**—These properties specify who can view and edit recordings that are created with this recording alias. The groups and users that are specified must be added to **Configure > Groups and Users** first.

**Note**

For more information about each specific recording alias setting, see the [Recording Aliases](#) section.





Setting Up External Media Storage

The default storage location for Content Server media files is the E: drive. You also have the option to store files on a Network Attached Storage (NAS) device so that recording capacity is not limited by Content Server disk space. If you set up a NAS device, the Content Server stores recording media to a temporary directory on the Content Server and then automatically stores the media on the NAS. The Content Server streams the media from the NAS.

To ensure that authentication occurs successfully, the Content Server requires external file services to run on the Windows operating system 2003 or later. Cisco recommends using a NAS device that is built on the Windows Storage server and that is also Windows Hardware Quality Lab certified. The file sharing protocol that is used by the Content Server to the NAS is Microsoft SMB.



Note

For best performance, you should dedicate the NAS device to media storage. Running applications such as domain controllers, databases, or external streaming servers on the same device could result in errors.



Note

The Content Server does not support running Windows services such as Active Directory Domain Services (ADDS), DNS server, or file services. You should configure an external server for all Windows-based services.



Note

The Content Server and the NAS must be in the same domain.

To configure NAS, see these sections:

- [Changing the Local Storage Location to NAS, page 13-1](#)
- [Reverting NAS Storage Location to the Default, page 13-3](#)
- [Changing NAS Storage to New Location, page 13-3](#)
- [Managing the Domain Account for NAS Access, page 13-4](#)

Changing the Local Storage Location to NAS

Ensure that you have enough time to complete the process of moving media files from the local database to the external storage location. The Content Server Wizard copies all media files that are referenced by the Content Server database from the E: drive to the NAS device. This operation can take several minutes, depending on the quantity of media to be moved.

**Caution**

Using the Content Server Wizard to move media from the E: drive to the external storage location does not move media files not associated with the Content Server database. These files include orphaned temporary files not used in any recording; .tcb import or export files; and files that are placed in the data folder by users. These files are not moved and are deleted.

However, if you use the Content Server Wizard to move media from one NAS location and to another, or from the NAS back to a local Content Server disk drive, these files are not moved. The Content Server Wizard does not delete the files from the NAS.

To change the media storage location from the default E: drive to a NAS device, do the following:

-
- Step 1** Back up the Content Server. See [“Backing Up the Content Server”](#) section on page 9-1 for more information about backup.
- Step 2** Add the Content Server to the same domain as the NAS. If you add the Content Server to an existing domain, you need to define a separate security policy for the Content Server; otherwise, the existing security policies might prevent the server from functioning correctly.
- Step 3** Choose or create an account in the domain that IIS (the Microsoft Internet Information Server) on the Content Server will use to access the share on the NAS device. This domain account needs to have both administrative rights on the Content Server and permissions over the NAS share.
- The Content Server Wizard can run under these user accounts:
- A domain administrator account
 - The created special domain account—for example, MYDOMAIN\Content Server_NAS_USER
 - The local administrator account
- Step 4** Configure the NAS (if you have not already done so).
- a. Log in to the NAS device by using Windows Remote Desktop Connection.
 - b. Set up a shared folder. Right-click the shared folder and select **Properties**. Select the Sharing tab. Click **Share**.
 - c. In the File Sharing window, select a name and click **Share**; or type a name, click **Add** and then click **Share**. In the Sharing tab, Advanced Sharing section, click **Advanced Sharing**.
 - d. Click **Permissions**. In the Select Users, Computers, Service Accounts, or Groups window, enter the Content Server name as it is registered in the domain. Click **OK**.
 - e. In the Share Permission window, give the Content Server and the shared account full permission:
 - Select the Content Server and click **Allow** in the Full Control, Change, and Read check boxes.
 - Select the shared account name (MYDOMAIN\Content Server_NAS_USER) and click **Allow** in the Full Control, Change, and Read check boxes.
 Click **OK**.
 - f. In the Advanced Sharing window, click **Apply** to apply the configuration. Click **OK** to exit the window.
 - g. Click the **Security** tab. Click **Edit**. Add the Content Server and the shared account name (MYDOMAIN\Content Server_NAS_USER).
 - h. In the Security Permission window, give the Content Server and the shared account full permission:
 - Click **Allow** in all check boxes for the Content Server and the MYDOMAIN\Content Server_NAS_USER.

- i. In the Advanced Sharing window, click **Apply** to apply the configuration. Click **OK** to exit the window.
 - j. Click **Apply** in the Security tab window. Click **Close** to close the Properties window.
- Step 5** Log in to the Content Server by using Windows Remote Desktop Connection.
- Step 6** Run the Content Server Wizard.
- Step 7** Click **Alternate Storage [NAS] Wizard**.
- If there are live calls, the wizard prompts you to end all calls. It also puts the Content Server in idle mode so that no new calls or transcoding jobs are accepted while the wizard is running. The wizard must complete (or be cancelled) in order to return the Content Server to normal operation (online mode).
- Step 8** Follow the on-screen instructions:
- a. Enter the remote server information for the new NAS location in this format:
`\\server_name\share_name\`. The server name must be entered as the DNS name, not as an IP address.
 - b. At the Content Server Checks step, confirm that the Content Server is backed up and that anti-virus software has been stopped. If you have not backed up or stopped the anti-virus software, cancel the wizard and complete those actions. Then run the wizard again. If you click **Cancel**, your system will not change.
 - c. The NAS Test Result step displays information about your intended setup. If all the tests are successful, click **Configure** to configure the Content Server and move existing media files from the E: drive to the NAS. Moving files might take several minutes depending on how many media files have to be moved.
 - d. When the process is complete, click **Finish**. No server restart is necessary. Content Server Wizard logs are available in E:\logs\SetupUtility. To check your new media location, go to **Management Settings > Server Overview**.
-

Reverting NAS Storage Location to the Default

You cannot complete the reversion process if the total size of the media files on the NAS is larger than the space available on the E: drive. Check the data folder size on the NAS. If you want to proceed but find that the files on your NAS exceed the E: drive space, delete some files in the Content Server web interface first.

Follow the steps in the “[Changing the Local Storage Location to NAS](#)” section beginning with [Step 5](#), and select **Return media to local storage** in the wizard.

Changing NAS Storage to New Location

You cannot complete this process if the total size of the media files on the original NAS location is larger than the space available on the destination drive. Check the data folder size on the NAS. If you find that the files on your NAS exceed the destination drive space, delete some files first.

Follow the steps in the “[Changing the Local Storage Location to NAS](#)” section beginning with [Step 5](#), and select **Move media to a different network location** in the wizard. Enter the new location in which to store the media.

Managing the Domain Account for NAS Access

If you want to use another domain account, do the following:

-
- Step 1** Log in to the Content Server as a domain administrator by using Windows Remote Desktop Connection.
 - Step 2** Go to **Start > Control Panel > User Accounts > Manage User Accounts**. Add the new domain account to the Administrators group on the Content Server (see [Step 3](#) in the “[Changing the Local Storage Location to NAS](#)” section).
 - Step 3** In the Content Server Wizard, select the NAS Wizard. Then use the **Update user account** option to update the Content Server. Follow the on-screen instructions.



Note Complete only Step 3 if the Content Server domain account password used to access the NAS share changes.



Using Cisco TMS with the Content Server

Cisco recommends that you use the Cisco TelePresence Management System (TMS) for scheduled calls that you want to record with the Content Server. The TMS is aware of Content Server capabilities so that resource conflicts are resolved at the time of the scheduling. TMS 12.2 or higher can be used to schedule recording calls on a version 3.3 or higher Content Server.

There is no guarantee that ad hoc recording calls (unscheduled calls) can connect. Successful connection depends on the number and type of other recording calls that are active when users make their calls. We recommend that a Content Server that is managed by TMS should not be used for ad hoc recording calls.

Configuring the Content Server for Use by TMS

You only need to perform this procedure once for each Content Server that you add to TMS. To add the Content Server to TMS, do the following:

Step 1 In the Content Server administrative web interface, enable the Content Server API:

- a. From the Management tab, go to **Configuration > Site settings**.
- b. In the API section, check **API enabled**.



Note If you have not already, change the API password from the default to a strong password.

Step 2 Staying in the Content Server administrative web interface, configure the Content Server:



Note If you use a group-owned recording alias (AD or LDAP), users will not be able to choose the recording alias in the TMS interface.

- If the Content Server is registered to a gatekeeper in gateway mode, users scheduling a call in TMS 11.8 and above can choose from a range of system recording aliases and their personal recording aliases. No further special configuration is necessary on the Content Server for standalone Content servers.

If the Content Server is part of a cluster, ensure that the frontend address in Site settings is set to the network load balanced address for the cluster; otherwise, links to recordings that are generated by TMS might not work.

- If the Content Server is registered to a gatekeeper in terminal mode, only system aliases and dedicated personal recording aliases (with the owner set to api-admin) are available for recording. On the Content Server, do the following:
 - a. From the **Management** tab, go to **Configuration > Groups and users**. Add a user with a site manager role and with the username api-admin.
 - b. Create a personal recording alias—for example, with the name TMS Alias—and set the owner to api-admin.
 - c. Create two live and three non-live dedicated TMS-only recording aliases. Only those aliases are available to TMS for scheduling.
- Step 3** Add the Content Server (or Content Server cluster) to TMS. For more information, read the TMS online help.
-

Using TMS to Schedule Recording Sessions

To use TMS to schedule recording sessions on the Content Server, do the following:

-
- Step 1** In the TMS web interface, go to **Booking > New Conference**.
- Step 2** In the advanced settings section, choose a recording alias.
- Step 3** Save the scheduled session. TMS will provide a link to view the recording.
-

For more information, see the TMS online help.



The View Recordings Tab

This chapter explains what users can see and do in the **View Recordings** tab of the Content Server web UI.

From the **View Recordings** tab, you can watch a recording in the Content Server web interface, download an output of the recording for viewing on a device, or email a link to the recording to someone else.

- [Watching a Recording in the Content Server Web Interface](#)
- [Watching a Downloaded Output on Your Computer](#)
- [Watching a Downloaded Recording on a Portable Device](#)
- [Sending a Link to the Recording to Others](#)

Watching a Recording in the Content Server Web Interface

To play the recording in a player in Content Server web interface, do the following:

-
- | | |
|---------------|---|
| Step 1 | In a web browser, enter the URL of the Content Server. |
| Step 2 | If guest access is enabled, you see a list of recordings that guest users have permission to see. Guest users do not have to log in to play some or all of these recordings. If guest access is not enabled, you must log in (enter a username and password) to see a list of recordings. |
| Step 3 | Locate the recording that you want to view. |
| Step 4 | Click the thumbnail or the name of the recording. |
| Step 5 | Click the play button in the center of the recording. |
-

By default, the Content Server displays the recording at the best quality for your connection, but you can also choose an internet speed. Under the recording, click the **Set bandwidth preferences** tab. Uncheck the **Automatically determine internet speed** box. Then choose a speed from the **Internet speed** drop-down menu. If you choose a recording playback size that is too big for your internet speed, you might still be able to watch the recording, but it might occasionally stop playing and buffer.

Availability of a Player in the Content Server Web Interface

The availability of a player depends on the following:

- Streaming outputs—Whether or not the recording has outputs that are suitable for playing in a player. If no streaming outputs are available, you cannot play it in a player. The recording creator or those with editing permissions can change the outputs settings from the recording's [Manage Outputs](#) page.
- Format and player type—The format of the recording outputs (Windows Media, MPEG-4 for QuickTime, or MPEG-4 for Flash) and whether or not the correct player is installed on your computer.
 - Depending on the template that the creator used for the recording, you might have two sizes per format to choose from. For example, the creator might have given you the option to play back MPEG-4 for Flash at 800 kbps 796 x 448 or 250 kbps 426 x 240. If a different size recording is available, you see an icon in the time line of the Silverlight or Flash player. Clicking the icon plays the movie in another size.
 - To check the status of players, click the **Other formats** tab. Click **Show player information**. Then click the **Check** button for a player to run a status check for that player.

**Note**

PC users can view outputs in the following formats: Windows Media, MPEG-4 for QuickTime, and MPEG-4 for Flash. Silverlight player plays Windows Media movies. Mac users can view outputs in the following formats: Windows Media with the Silverlight plug-in, MPEG-4 for QuickTime, and MPEG-4 for Flash.

Watching a Downloaded Output on Your Computer

If a recording has downloadable outputs, you can download the outputs to your computer. If you have limited access to the Internet, downloading might be a better option than streaming in a player. After you save a recording on your computer, you can watch it as often as you want.

**Note**

If the download time exceeds 20 minutes, the download will fail.

Recording creators can use a recording alias that uses a template that specifies the creation of downloadable outputs. Or after the recording is created, site managers, creators, or those with editing permissions can add outputs by clicking [Manage Outputs](#) for the recording. If you required an output that is currently not available for the recording, contact the recording creator or the Content Server site manager.

To download an output of the recording, do the following:

- Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.
- Step 2** Under the recording, click the **Download** tab. If a recording does not have downloadable outputs, you will not see the **Download** tab.
- Step 3** Click the link for recording output that you want to download. A window for file download appears.
- Step 4** Click **Save File**, and put the recording where you want it on your computer.
- Step 5** You can double click the downloaded file for playback.

The recording is played back in the appropriate viewer for its format (in the program that is the default to play that type of media file on your computer). For example, if you have set up QuickTime to play .mp4 files and you download an MPEG-4 for Flash file, QuickTime plays the downloaded file.

Watching a Downloaded Recording on a Portable Device

If a recording has downloadable outputs that are suitable for portable devices, you can download the recording and watch it on your iPod or Microsoft Zune device. You need to use a computer as an intermediary device and then load the recording on the portable device as you would any other file. After the recording has been loaded on the device, you can watch it as often as you like.

Recording creators can use a recording alias that uses a template that specifies the creation of downloadable outputs. Or after the recording is created, site managers, creators, or those with editing permissions can add outputs by clicking [Manage Outputs](#) for the recording. If you required an output that is currently not available for the recording, contact the recording creator or the Content Server site manager.

To download an output of the recording, do the following:

-
- Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.
 - Step 2** Under the recording, click the **Download** tab. If a recording does not have downloadable outputs, you will not see the **Download** tab.
 - Step 3** Click the link for recording output that you want to download. A window for file download appears.
 - Step 4** Click **Save File**, and put the recording where you want it on your computer.
 - Step 5** From your computer, load the recording on to your portable device for playback.
-

Sending a Link to the Recording to Others

You can send a link to the recording to another viewer in email.

To share an email link, do the following:

-
- Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.
 - Step 2** Under the recording, click the **Share** tab.
 - Step 3** Click **Email link**. The link appears in your default email application.



Note Although you can watch the recording, the person to whom you send the email might not have the correct permissions to watch it. Contact the recording creator or the Content Server site manager for help with viewer permissions.
