Cisco TelePresence Content Server Release 5.3 Administration and User Guide

September 2013

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

Text Part Number: OL-25008-01

Cisco TelePresence Content Server Release 5.3 Administration and User Guide

CONTENTS

Preface

Contents

General Description

The Cisco TelePresence Content Server is a network telepresence media recording, archiving, streaming, and sharing solution.

With the Cisco TelePresence Content Server, those in your organization can get their message across regardless of the day, time, devices, or location. Whether delivering a CEO briefing to an entire organization, facilitating corporate training programs, or offering a distance education course, video recordings are a powerful organizational tool. Cisco TelePresence Content Server maximizes the impact, reach, and value of these messages by capturing presentations, streaming them live, and recording them for future distribution.

No longer is your message bound by place and time. Recording and streaming telepresence-generated content enables organizations to communicate to dispersed individuals and scale knowledge—anytime, anywhere. Content can integrate easily into familiar third-party tools, extending the reach and chances that your message will be seen and heard. With the Content Server, existing video conferencing investments are fully leveraged, and your messages are viewed by more people more often.

New in Cisco TelePresence Content Server Release 5.3

- 5 additional recording ports option key
- New presentation layout

New in Release 5.3.1

Content Server Maintenance Release 5.3.1 has no new features.

New functionality includes an “Optimize for motion” check box in the Content Server User Interface Media server configuration settings screen.

For more information about new features and functionality, see the *Cisco TelePresence Content Server Release 5.3.x Release Notes* on 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*, which also lists all new and revised Cisco technical documentation, at:

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

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

CHAPTER 1

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

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.

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.

CHAPTER 2

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 2-1).

Step 6 After updating the settings, click **Save**.

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

Field	Field Description	Usage Guidelines
Recording information		
Name	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 to help users find the recording when they search. If you edit a recording that you did not create, the name could the name of the creator's recording alias and a date/time stamp. The name could also be the type of recording (*OnDemand only* or *Live and OnDemand*) and a date/time stamp.
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.	Optional. This optional setting can help users find the recording when they search.

Table 2-1 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 2-1 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.	You can give viewing access to one of the following: • **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. **Note** After you click **Check access lists** or **Place call**, the users entered have the following formats: – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name 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”).
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 2-1 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**.	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. **Note** After you click **Check access lists** or **Place call**, the users entered have the following formats: – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name 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").
Play recording on endpoints		
Make recording available for playing on endpoints	Check to make the recording available for playback on an endpoint.	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. 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. The recording cannot be played back on an endpoint if it has not been published. See the **Publish recording** setting above for more information. A recording with restricted viewing access and no viewable interface outputs can be played back from an endpoint. Password protection is not applied when a recording is played back from an endpoint unless you add a PIN. **Tip** You can also PIN protect all new recordings created with your personal recording alias (see Edit Recording Aliases).

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 2-2).

Step 5 After updating the settings, click **Save**.

Table 2-2 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.	—

Table 2-2 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.	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. 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: • **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. – **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 2-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
On demand formats	Choose up to three formats: • 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.	• **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.	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**. Beginning in Content Server Release 5.3.1, you can check the **Optimize for motion** check box to optimize the quality of high-motion recordings.

Table 2-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to download for portable devices		
Output layout	Click the layout to use.	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. 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: • **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	Select portable device(s) and whether you want audio and video or audio only: • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible)	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. iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.

Table 2-2 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Outputs to download for general purpose		
Output layout	Click the layout to use.	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. 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: • **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. – **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 2-2 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.	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. 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: • **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. – **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 2-2 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.	The following information is shown for each output: • 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 2-2 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.	The following information is shown for each output: • 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.	The following information is shown for each output: • 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.	The following information is shown for each output: • 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 3-4).

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 3-5).

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

CHAPTER 3

The Management Tab

This chapter explains what users can do in the **Management** tab of the Content Server web UI. To see this tab when you log in, you must have the role of site manager or system administrator.

The **Management** tab in four menus, and each menu has sub-menus:

Diagnostics

- Server Overview, page 3-2
- Cluster Overview, page 3-6 (appears only with a cluster deployment)
- Server Logs, page 3-7
- Transcoding Queue, page 3-8

Recordings

- Edit Recordings, page 3-8
- Import Recordings, page 3-23
- Create Recording, page 3-25

Recording Setup

- Recording Aliases, page 3-30
- Categories, page 3-37
- Templates, page 3-38
- Media Server Configurations, page 3-45
- Call Configurations, page 3-63

Configuration

- Site Settings, page 3-65
- Groups and Users, page 3-80
- Windows Server, page 3-86

Server Overview

To display the **Server overview** page, go to 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, apart from adding 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.

The following information is displayed (Table 3-1):

Table 3-1 Diagnostics > Server Overview

Field	Field Description	Usage Guidelines
System information		
System name	The name for the Content Server that is unique in the cluster.	The System information section is displayed only for Content Servers in a cluster. 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. If the Content Server is in a call when this field changes, it enters **Configuration reload** mode. The change will not take effect until all calls have ended.
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.	The System information section is displayed only for Content Servers in a cluster. 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. If the Content Server is in a call when this field changes, it enters **Configuration reload** mode. The change will not take effect until all calls have ended.
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.	The System information section is displayed only for Content Servers in a cluster. 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. If the Content Server is in a call when this field changes, it enters **Configuration reload** mode. The change will not take effect until all calls have ended.

Table 3-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
Content Server status		
Server mode	The current status of the Content Server.	**Online**: The Content Server can accept calls and transcode outputs. **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**. **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. **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. **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 **Maintenance > Shutdown > Restart**. **Note** Before a shutdown and restart, you must first assign shutdown permission to the domain user on the Content Server that you want to shut down and restart. See the Resolved Caveats section in the *Release Notes for Cisco TelePresence Content Server Release 5.3.x* on Cisco.com for more information (CSCuf16163). **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.
Content Engine status	The current Content Engine service status.	• 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.

Table 3-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
Current calls	A pictorial representation of the number of current calls. • Up to 5 concurrent calls • Up to 10 concurrent calls with the 5 Additional Recording Ports option enabled	• An orange bar represents a call with live streaming outputs. • A brown bar represents a call with on-demand outputs only.
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.	• 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	An arrow in the counter-clockwise direction means that recordings are being transcoded. **No** means that no recordings are being transcoded. 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 complete.
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 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.	—

Table 3-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
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).
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 use 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.	Clicking the **Restart service** button only 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).

For more information about the main features, system requirements, setup, and management of a Content Server cluster, locate documentation for the Cisco TelePresence Content Server on Cisco.com

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.

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.
- **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

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 3-2).

Step 5 After updating the settings, click **Save**.

Table 3-2 Recordings > Edit Recordings: Edit Recording

Field	Field Description	Usage Guidelines
Recording information		
Name	The name of the recording to be displayed in the View Recordings pages.	The default name is the type of recording (*OnDemand only* or *Live and OnDemand*) and a date/time stamp. You can edit this name to help users find the recording when they search.
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.	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 3-2 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.	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.
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.	You can give viewing access to one of the following: • **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. **Note** After you click **Check access lists**, **Place call**, or **Save**, the users entered have the following formats: – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name 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”).

Table 3-2 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 3-2 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**.	Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). • 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: – 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**. 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. **Note** After you click **Check access lists**, **Place call**, or **Save**, the users entered have the following formats: • Local authentication mode: MACHINENAME\user.name • Domain authentication mode: DOMAINNAME (optional)\user.name • LDAP authentication mode: user.name 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”).

Table 3-2 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.	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. 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. The recording cannot be played back on an endpoint if it has not been published. See the **Publish recording** setting above for more information. 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. **Tip** You can also PIN protect all new recordings created with your personal recording alias (see Adding or Editing Recording Aliases).
Export recording		
Export recording	Click **Export record export** to export the recording as a .tcb file. When it appears, click **Download exported recording** link and save the exported .tcb file to an external network location. If necessary, you can also click the **Update exported recording** link to update the previously exported recording.	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. 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. 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.

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.

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 3-3).

Step 5 After updating the settings, click **Save**.

Table 3-3 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.
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 3-3 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.	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. 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: • **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. – **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: • 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.

Table 3-3 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.	• **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.	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**. Beginning in Content Server Release 5.3.1, you can check the **Optimize for motion** check box to optimize the quality of high-motion recordings.
Outputs to download for portable devices		
Output layout	Click the layout to use.	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. 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: • **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 3-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
Portable devices	Select portable device(s) and whether you want audio and video or audio only: • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible)	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. iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.
Outputs to download for general purpose		
Output layout	Click the layout to use.	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. 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: • **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. – **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 3-3 Recordings > Edit Recordings: Manage Outputs (continued)

Field	Field Description	Usage Guidelines
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.	—
Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U		
Output layout	Click the layout to use.	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. 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: • **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. – **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 3-3 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 3-3 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.	The following information is shown for each output: • 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.	The following information is shown for each output: • 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 3-3 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.	The following information is shown for each output: • 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.	The following information is shown for each output: • 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 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 3-2).

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 S3.3.

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 3-4).

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 3-4).

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 3-4 Recordings > Create Recording

Field	Field Description	Usage Guidelines
Create recording		
Recording alias	Select a recording alias for this recording.	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). If others are permitted to watch while recording is in progress, select a recording alias that allows live streaming. 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. You can see whether outputs for your recording are in the queue to be processed by going to **Diagnostics > Transcoding queue.** **Note** *No live resources available* 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.
Template outputs	The outputs that are produced with the selected recording alias.	The Template outputs popup displays the outputs that the template selected for this recording alias produces. This popup includes the following: • 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. If these are not the outputs that you want, select a different recording alias.
Dial number	Enter the number or address of the endpoint that the Content Server should call to make the recording	The number or address can be the following: • 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.
PIN for MCU conference	Enter the PIN for a password protected MCU conference.	The PIN must be numeric only.

Table 3-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
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 (*OnDemand only* or *Live and OnDemand*) 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. These keywords are not displayed to users.	Optional. This optional setting can help users find the recording when they search.

Table 3-4 Recordings > Create 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.
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.	You can give viewing access to one of the following: • **Allow access to all users, including guests**: If *A***llow 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. **Note** After you click **Check access lists** or **Place call**, the users entered have the following formats: – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name 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”).
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.

Table 3-4 Recordings > Create Recording (continued)

Field	Field Description	Usage Guidelines
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.
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 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**.	Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). • 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: – 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**. 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. **Note** After you click **Check access lists**, **Place call**, or **Save**, the users entered have the following formats: • Local authentication mode: MACHINENAME\user.name • Domain authentication mode: DOMAINNAME (optional)\user.name • LDAP authentication mode: user.name 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”).
Play recording on endpoints This option only appears on a Content Server that is configured with a Premium Resolution option key.		

Table 3-4 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 3-5).

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 3-5).

Step 4 Click **Save**.

Table 3-5 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**.	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. 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.
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.	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. 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**.
Dialing properties		
H.323 ID	The unique H.323 ID to be dialed to record when using this recording alias.	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. 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.
E.164 alias	The E.164 alias to be dialed when using this recording alias.	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. 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.
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 3-5 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 (*OnDemand only* or *Live and OnDemand*) 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 3-5 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.	You can give viewing access to one of the following: • **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. **Note** After you click **Check access lists**, **Place call**, or **Save** the users entered have the following formats: – Local authentication mode: MACHINENAME\user.name – Domain authentication mode: DOMAINNAME (optional)\user.name – LDAP authentication mode: user.name 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”).

Table 3-5 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 3-5 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 **Open Content Editor**) 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**.	Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). • 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: – 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**. 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. **Note** After you click **Check access lists**, **Place call**, or **Save**, the users entered have the following formats: • Local authentication mode: MACHINENAME\user.name • Domain authentication mode: DOMAINNAME (optional)\user.name • LDAP authentication mode: user.name 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”).

Table 3-5 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 *Name* and, if desired, a *Description*. 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 *Name*, the *Description*, 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 3-6).

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 3-6).

Step 4 Click **Save**.

Table 3-6 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 3-6 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.	—
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.	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: • **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. – **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 3-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
On demand formats	Choose up to three formats: • 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.	• **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	Choose the **Media Server Configurations** for on-demand viewing of the recordings that are created with this template. Formats not selected above are dimmed.	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**. Beginning in Content Server Release 5.3.1, you can check the **Optimize for motion** check box to optimize the quality of high-motion recordings.

Table 3-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Live stream	Click to allow the recording to be streamed while it is in progress.	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. 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. 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.
Outputs to download for portable devices		
Output layout	Click the layout to use.	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: • **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	Select portable device(s) and whether you want audio and video or audio only: • iPod Video • iPod Audio • Zune Video (Microsoft compatible) • Zune Audio (Microsoft compatible)	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. iPod formats are optimized for fifth-generation Apple iPod (and compatible) devices. Zune formats are optimized for first-generation Microsoft Zune (and compatible) devices.

Table 3-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
Outputs to download for general purpose		
Output layout	Click the layout to use.	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: • **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. – **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.

Table 3-6 Recording Setup > Templates: Add or Edit Template (continued)

Field	Field Description	Usage Guidelines
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.		
Output layout	Click the layout to use.	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: • **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. – **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 3-6 Recording Setup > Templates: Add or Edit Template (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. This summary includes information about on-demand and live streaming settings for the template.	The information displayed in the summary is the following: • 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: • 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: • 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: • 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

By default, the Content Server can stream Windows Media live and on demand using the local Windows Media Streaming Server. MPEG-4 for QuickTime and MPEG-4 for Flash can be delivered on demand as a progressive download (HTTP streaming) using the local web server (IIS). Streaming is specified by the two preconfigured media server configurations that cannot be deleted:

- 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.
- Local Windows Media Streaming Server: can be used for streaming Windows Media live and on demand.

External streaming servers for Windows Media, MPEG-4 for QuickTime, and MPEG-4 for Flash can also be used to stream recordings. Site managers set up the streaming server, and then add a Media server configuration to the Content Server that specifies how the Content Server puts the media files on the external streaming server and how the media is streamed. These Media server configurations can then be selected in a template (see **Templates**) or when creating outputs using the **Manage Outputs** page. If this 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

Site managers can add new media server configurations and update existing ones:

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**.

Note 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.

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 set up a media server configuration for a Windows Media streaming server to do live and on-demand streaming. Live streams can be sent to the Windows Media player using either a unicast or a multicast connection. Unicast streaming can be configured for either the local or an external Windows Media streaming server, but multicast streaming can only be configured with the local Windows Media streaming server.

Before You Begin

- Before you start delivering your live content as a multicast stream, ensure that the network is multicast enabled.
- Only viewers with Windows computers can view live Windows Media multicast streams.

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**, 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 3-7).

Step 4 Click **Save**.

Table 3-7 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	Whether the server is to support live multicast streaming. If you check this box, the unicast streaming and on-demand options are unavailable. You cannot create a multicast and on-demand streaming server in the same media server configuration.	In multicast delivery, the server sends only one stream that 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, DNS name of the server, or (local) for multicast streaming.	—
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.	—
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.	—

Table 3-7 Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration

Field	Field Description	Usage Guidelines
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.
Live multicast streaming settings		
Server push point	The HTTP port of the streaming server. The port for the local Content Server's Windows Media streaming server is 8080.	—
Publishing point: Create new using settings 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 an existing publishing point.	The default multicast-enabled publishing point on the Content Server is called TCSmulticastTemplate.
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.	If you do not enter an address, the Content Server uses the first two octets of the IP address that are specified in the destination multicast IP address of the WMS Multicast Data Writer properties of the multicast publishing point, but the Content Server dynamically assigns the last two octets. For example, if 10.0.1.1 is specified at the publishing point, the Content Server can use any address in the 10.0 range for multicast streaming.
Streaming port range start	The first port number in the live streaming port range. Enter an even number between 10000 and 65000.	If you do not enter a port range, the Content Server uses the destination multicast port of the WMS Multicast Data Writer properties of the multicast publishing point.

Table 3-7 Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration

Field	Field Description	Usage Guidelines
TTL	The multicast time to live (TTL) threshold.	This value tells the network how far multicast packets should be allowed to travel across the network. 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. The efficacy of higher values—LAN (TTL=32), WAN (64), Internet (128), Unrestricted (255)—depends on the network configuration. If you do not enter a TTL, the Content Server uses the destination multicast time-to-live (TTL) of the WMS Multicast Data Writer properties of the multicast publishing point.
Publishing point: Use existing Publishing point name	Click to use an existing publishing point on the streaming server. Enter the name of an existing publishing point.	—
Live URL	The live URL is set to http://<local>/tcs/data. **Append filename to URL** is checked, and the option is dimmed in the interface.	—
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.
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.	—

Table 3-7 Recording Setup > Media Server Configurations: Add Windows Media Streaming Server Configuration

Field	Field Description	Usage Guidelines
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. The multicast stream is sent directly from the Content Server.

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 3-8).

Step 4 Click **Save**.

Table 3-8 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.	—
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.	—

Table 3-8 Recording Setup > QuickTime or Darwin Streaming Server Configuration (continued)

Field	Field Description	Usage Guidelines
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.	—
TTL	The multicast time to live (TTL) threshold.	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. The efficacy of higher values—LAN (TTL=32), WAN (64), Internet (128), Unrestricted (255)—depends on the network configuration.
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 QuickTime 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.

Table 3-8 Recording Setup > QuickTime or Darwin 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 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.	—
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 3-9).

Step 4 Click **Save**.

Table 3-9 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.	—
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**.

Table 3-9 Recording Setup > Wowza Media Server for Flash Configuration (continued)

Field	Field Description	Usage Guidelines
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 3-9 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 3-9 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

Note Cisco TelePresence Content Server Release 5.3 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 Table 3-10).

Step 4 Click **Save**.

Table 3-10 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.	—

Table 3-10 Recording Setup > Media Experience Engine 3500 Server Configuration (continued)

Field	Field Description	Usage Guidelines
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 Show and Share setup and support information, go to http://www.cisco.com/en/US/products/ps6682/index.html.

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 3-11).

Step 4 Click **Save**.

Table 3-11 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/macosxserver/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 3-12).

Step 4 Click **Save**.

Table 3-12 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 3-13).

Step 4 Click **Save**.

Table 3-13 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.	—

Table 3-13 Recording Setup > Media Server Configurations: Add iTunes U Server Configuration (continued)

Field	Field Description	Usage Guidelines
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
- 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 3-14).

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 3-14).

Step 4 Click **Save**.

Table 3-14 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		
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.

Table 3-14 Recording Setup > Call Configurations: Add Call Configuration or Edit (continued)

Field	Field Description	Usage Guidelines
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.	The Content Server negotiates the level of encryption with the endpoint. The solution supports media encryption only for the H.323 protocol.
Advertised codecs		
Video codecs	Check the boxes next to the video codecs to be advertised for calls that use this call configuration.	Because of standards compliance, you cannot uncheck H.261. The check box is dimmed.
Audio codec	Check the boxes next to the audio codecs to be advertised for calls that use this call configuration.	Because of standards compliance, you cannot uncheck G.711. 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 3-15 Configuration > Site Settings

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.
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.	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
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 **View all gatekeeper registrations** 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 *Manual*.	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.	—
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 *Terminal* or as a *Gateway*.	If you select Gateway, enter the H.323 gateway prefix and the E.164 gateway prefix. The registration mode for a cluster must be Gateway. 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.

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
H.323 gateway prefix	If registered as a gateway, this prefix must be entered before the *H.323 ID* of a Recording alias when calling the Content Server.	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. 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.
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.	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. 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.
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 *Auto* and supply the username and password to be used by the Content Server.
User name	The username to authenticate to the gatekeeper.	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
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.
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**.	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. 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. If you select either **On** or **Auto**, enter the NAT address.
NAT address	The global, external address to a router with NAT support.	In the router, the following ports must be routed to the system IP address: • 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		
Registration status	Displays the status of Content Server registration with the SIP registrar.	Click **View all SIP registrations** to display a page showing all the system and recording alias registration details.
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 3-15 Configuration > Site Settings (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.	—
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).
Server type	Always **Auto**, which supports registering to standard SIP registrars, such as OpenSIPS.	—
Transport	The transport protocol for SIP. The default is *TCP* (Transmission Control Protocol). *UDP* (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		—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
Authentication		
Authentication	Choose the authentication method for the Content Server. If you select either *Domain* or *LDAP* 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.	There are three modes of authentication (for more information, see **Groups and Users**): • *Local*: Only users with valid local accounts added through the **Groups and Users** page can log in. Local groups are not supported. • *Domain*: 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. • *LDAP*: LDAP authentication does not require the Content Server to be added to a domain. Before changing authentication from *Local* to *LDAP*, 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 #page:login&rescue:true to the end of the Content Server URL in the browser.
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.	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
Base DN	The search base that the Content Server uses to search for user records. (DN = Distinguished Name)	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. Base DN examples: • OU=employees,DC=company,DC=com • OU=marketing,OU=employees,DC=company,DC=com 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.
User DN	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: • CN (Common Name) of the special account • OU (Organizational Unit) • DC (Domain Object Class) User DN examples: CN=user_account,OU=employees,DC=company,DC=com CN=user_account,OU=marketing,DC=company,DC=com **Note** DNs can have many more than four parts.	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 *Base DN*.
Password	The password for the account identified above.	—
Password confirm	—	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
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).	• 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.
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.	Only for Content Servers that are registered to an H.323 gatekeeper as a gateway and requires the API to be enabled. **Note** If you have a Content Server cluster, see the "Important Guidelines" section about recording aliases and adding or removing live output from a template in the *Cisco TelePresence Content Server Release Administration and User Guide*. See the "Creating Automatic Personal Recording Aliases" section on page 3-85 for more information about configuring an automatic recording alias. 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.
Recording alias settings to copy	Select the system recording alias to use for all newly created recording aliases.	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. 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.
Email address suffix	Enter the email address suffix 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.

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
Email settings		
Send email when recording finishes	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. 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.	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.	—
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.
Upload language pack	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.	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
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.	The API is designed for integration with the Cisco TelePresence Management Suite (TMS) but can also be used with other management systems. The API is enabled by default and must stay enabled in the following cases: • 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 none of these cases apply, you can disable the API.
User name	The Content Server API username is *admin*.	Username cannot be modified.
Password	The password for accessing the Content Server API.	The default API password is the serial number of the Content Server. 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. Upgrading from Content Server version 4.x to 5.0 does not change the API password. If the 4.x default password (TANDBERG) was never changed: when you upgrade from 4.x to 5.0 and reset the Content Server to factory defaults, the default password is the Content Server serial number.
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.	—

Table 3-15 Configuration > Site Settings (continued)

Field	Field Description	Usage Guidelines
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.
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.

View all gatekeeper registrations

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

Table 3-16 Configuration > Site settings: View all gatekeeper registrations

Field	Field Description	Usage Guidelines
Gatekeeper registration status		
Registered to	The IP address or DNS name of the H.323 gatekeeper that the Content Server is currently registered to.	A green check mark means 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 3-16 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 3-17 Configuration > Site settings: View all SIP registrations

Field	Field Description	Usage Guidelines
SIP registration status		
Status	Whether the registration is active.	A green check mark and the status of 'Active' means that the Content Server has contacted the SIP registrar and can make registrations with it.
System registration		
SIP address	The SIP address (URI) that is registered. This address is set in **Site Settings**.	—
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.

Table 3-17 Configuration > Site settings: View all SIP registrations (continued)

Field	Field Description	Usage Guidelines
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).

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 TCS 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 TCS 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 the authentication mode to LDAP, a you 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 web interface for Windows Server administration on the Content Server) and the local

administrator cannot log in by 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>/tcs/#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 TCS 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. From the **Management** tab, go to **Configuration > Windows server**. Create the accounts in Windows Server administration.

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 3-18).

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 3-18 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. • 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 3-19).

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 3-14).

Step 4 Click **Save**.

Table 3-19 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 3-20 Configuration > Groups and Users: Edit

Field	Field Description	Usage Guidelines
Details		
Name	The name of the user or the Base DN of the group.	—
Role	Whether the group or user has site manager, creator, or viewer privileges.	—

Table 3-20 Configuration > Groups and Users: Edit (continued)

Field	Field Description	Usage Guidelines
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 *TCS_creators* and enter this group into the creator role when adding users and groups. When a member of the *TCS_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@tcs_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 3-80 to configure an LDAP creator group, and enter a unique name such as *TCS_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 in the form *@company.com*.

The creator will receive an email each time that a recording is completed.

Step 6 Click **Save**.

Windows Server

Caution Do not use Remote Desktop in Windows Server Administration from the Content Server web interface to install software upgrades or apply Windows security updates. To do these tasks, access the Content Server through Remote Desktop Connection on your PC. See the "Using Windows Remote Desktop Connection from Your Computer" section on page 3-88 for more information.

Note When you are in the Windows Server Administration interface, you can access Windows help by clicking the ? in the upper right corner.

Using the Content Server Web Interface for Windows Server Administration

Open the Windows Server Administration interface by going to **Management** tab. Then go to **Configuration > Windows server**. You can also access the administration interface by entering the following in an Internet Explorer browser:

https://<Content_Server_IP_address>:8098

Note You must use Internet Explorer (IE) to access the Windows Server Administration interface.

Some IE security settings might prevent the necessary ActiveX controls from running. Without these controls, you cannot access the administration interface or some of its tools. To overcome this issue, add the URL of the Content Server to the trusted sites in your browser. From the browser toolbar, go to **Tools > Internet Options**. Click the **Security** tab, and then click **Trusted sites**. Click **Sites**, and add the Content Server URL.

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 Remote Desktop.

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 In the Content Server interface, from the **Management** tab, go to **Configuration > Windows server**. The server administration window appears.

Step 2 Click **Set Administrator Password**.

Step 3 Enter the current password and new password. Then confirm the new password.

Step 4 Click **OK**.

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 In the Content Server interface, from the **Management** tab, go to **Configuration > Windows server**. The server administration window appears.

Step 2 Click **Maintenance.** Then click **Date/Time**.

Step 3 Update the date, time, and time zone settings.

Step 4 Click **OK**.

Step 5 You must then restart the Content Server.

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 Windows Server Administration interface. To manage local users and groups, do the following:

Step 1 In the Content Server interface, from the **Management** tab, go to **Configuration > Windows server**. The server administration window appears.

Step 2 Click **Users**.

Step 3 Click either **Local Users** or **Local Groups** to manage local accounts for authentication.

Step 4 After entering the account settings, click **OK**.

Note To verify the authentication method that the Content Server uses, go to **Configuration > Site settings** in the Content Server interface.

Using Windows Remote Desktop Connection from Your Computer

To use Windows Remote Desktop Connection from your computer to access the Content Server, 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:

a. In the Remote Desktop Connection dialog box, click **Options**.

b. 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.

CHAPTER 4

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**.

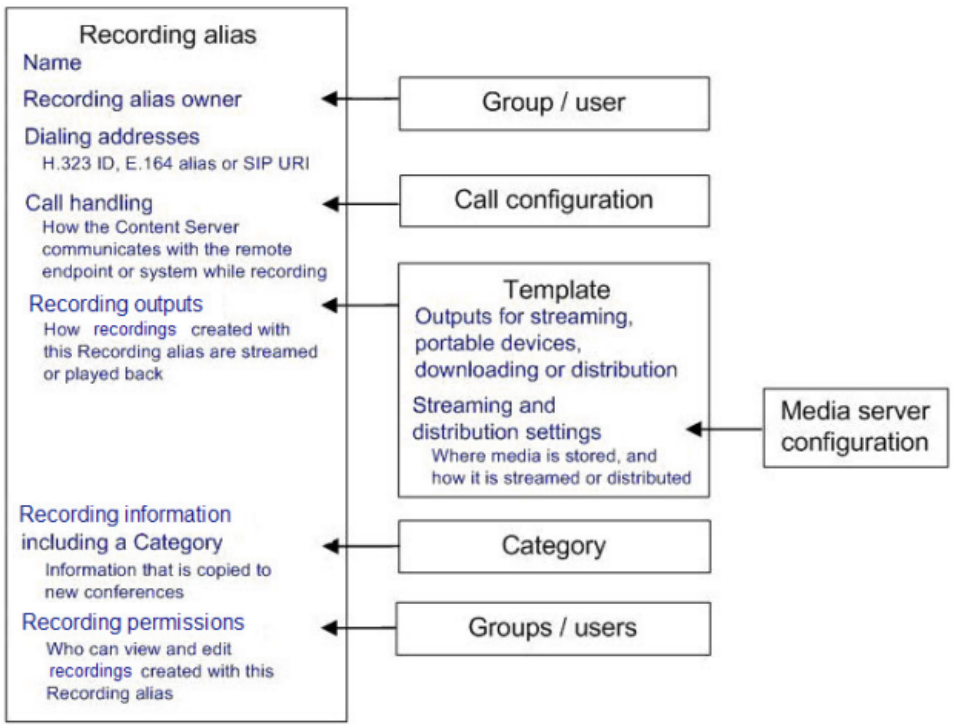
The following are the properties of every recording alias:

- 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 alias.
- 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.



CHAPTER 5

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 though 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

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 3-45 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 3-38 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 Chapter 4, "Understanding Recording Aliases" for information about what is included in a recording alias.)

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.

CHAPTER 6

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 and the NAS must be in the same domain.

For more information about external storage, see the following sections:

Changing the Local Storage Location to Network Attached Storage

Ensure that you have enough time to complete the process of moving media files from the local database to the external storage location. The TCS 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 TCS Wizard to move media from the E: drive to the external storage location does not move any media files that are 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 TCS Wizard to move media between one NAS location and another or from the NAS back to a local Content Server disk drive, these files are not moved, and the TCS Wizard does not delete them 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 7-1 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. Contact your authorized Cisco reseller for details of the recommended security policy settings.

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. This domain account needs to have both administrative rights on the Content Server and permissions over the NAS share.

The TCS Wizard can run under these user accounts:

- A domain administrator account
- The created special domain account—for example, MYDOMAIN\TCSNASUSER
- The local administrator account

Step 4 Configure the NAS (if you have not already done so).

a. Using Windows Remote Desktop Connect, log in to your NAS device.

b. Set up a shared folder.

c. Set permissions on the share to allow the Content Server and the shared account (MYDOMAIN\TCSNASUSER in this example) to have full control over the share. Right-click on the share and click **Sharing and Security**. Then click **Permissions**. Click **Add**.

d. Click **Object Types**. Select **Computers**. Click **OK**.

e. Enter the Content Server server name as it is registered in the domain. Click **Check Names** and **OK**.

f. Enter the shared account name (MYDOMAIN\TCSNASUSER). Click **Check Names** and **OK**.

g. Give the Content Server and the shared account (MYDOMAIN\TCSNASUSER) full control over the share.

h. Click the **Security** tab. Click **Add**. Repeat step d to step g to give the Content Server and MYDOMAIN\TCSNASUSER full control of the NAS share.

Step 5 Using Windows Remote Desktop Connection, log in to the Content Server.

Step 6 Run the TCS 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.

   You can also click **Finish** to exit the wizard without making any changes. If any tests failed, you cannot continue. Check the external NAS configuration and the information that you entered and try again.

Step 9 When the process is complete, click **Finish**. No server restart is necessary. TCS Wizard logs are available in E:\logs\SetupUtility. To check your new media location, go to **Management Settings > Server Overview**.

Reverting the Storage Location to the Default Storage Location

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 Network Attached Storage" section on page 6-1from Step 5 onwards, but select **Return media to local storage** in the wizard.

Changing the Storage Location from One NAS Location to Another

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 Network Attached Storage" section on page 6-1from Step 5 onwards, but select **Move media to a different network location** in the wizard. Enter the new location in which to store media.

Managing the Domain Account Used to Access the NAS

If you want to use another domain account, do the following:

Step 1 Add the new domain account to the Administrators group first. Go to **Start > Administrative Tools > Computer Management**.

Step 2 Go to **System Tools > Local Users and Groups > Groups**.

Step 3 Double-click **Administrators**. Add the new domain account to the administrators group (see Step 3 in the "Changing the Local Storage Location to Network Attached Storage" section on page 6-1).

Step 4 In the TCS wizard, select the NAS wizard. Then use the **Update user account** option to update the Content Server. Follow the on-screen instructions.

Note If the password for the domain account that the Content Server uses to access the NAS share changes, complete only Step 4).

CHAPTER 7

Maintaining the Content Server

This chapter includes the following Content Server maintenance procedures:

Note These procedures contain steps that you must perform on devices that are external to the Content Server. If you need more information about devices that are not Cisco products, consult the documentation for those devices. If you need information about Windows Servers that is not provided here, consult the Microsoft documentation.

Backing Up the Content Server

To ensure that you do not lose data, you should back up the Content Server regularly. You should also back up the Content Server before you upgrade or install a security update. Follow the procedures as described here to prevent issues with future upgrades:

Note If your media files are located on a Network Attached Storage device (NAS) or on an external media server, this backup procedure does not back up those files. Ensure that you back up the media on 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 your Content Server backup; otherwise, you might not be able to play some recordings.

Before Backing Up

You can back up Content Server files to a USB drive or to a network drive.

When performing a manual or scheduled backup, if you use a USB hard drive, you must connect the drive to a USB port on the Content Server. Then log into the Content Server using Windows Remote Desktop Connection to make sure that the USB hard drive appears under My Computer.

Also, make sure that you have enough room on the USB hard drive or network drive for all the files that you want to back up. Check the size of the data for backup by logging in to the Content Server using Windows Remote Desktop Connection. Open My Computer to calculate the amount of C: drive and E: drive space is used.

Performing a Manual Backup

To perform a manual, on-demand backup, follow these steps:

Step 1 Open the backup and restore wizard in one of these ways:

- Log in to Content Server web interface in Internet Explorer. From the **Management** tab, go to **Configuration > Windows server**. In the dialog box that appears, log in with the local administrator password. Then go to **Maintenance > Backup**.

Note Internet Explorer security settings might prevent the necessary Active X scripts from running. With certain browser security settings, you will not be able to access the web interface for Windows Server administration or some of its tools. To overcome this issue, add the URL of the Content Server to the trusted sites in your browser. In Internet Explorer, go to **Tools > Internet Options**. Click the **Security** tab. Click **Trusted sites** and then **Sites**. Add the Content Server URL.

- Log in to the Content Server through Windows Remote Desktop. Go to **Start > All Programs > Accessories > System Tools > Backup**.

Step 2 In the Welcome to the Backup or Restore Wizard dialog box, click **Next**.

Step 3 Click **Back up files and settings**. Click **Next**.

Step 4 In the What to Back Up dialog, click **Let me choose what to back up**. Click **Next**.

Step 5 In the Items to Back Up dialog, expand **My Computer**. Check **Local Disk (C:)**, **Local Disk (E:)**, and **System State**. Click **Next**.

Step 6 In the Backup Type, Destination, and Name dialog, browse to the USB drive or network location that you want to back up to (see the "Before Backing Up" section on page 7-2 for more information). Type a name for the backup. Click **Next**.

Step 7 In the Completing the Backup or Restore Wizard dialog, verify the summary of your choices. Click **Finish**. The backup process takes approximately 10 minutes per 5 GB of data. Progress is displayed, and a detailed report is provided when the backup is complete.

Configuring a Scheduled Backup

To set up a scheduled backup, follow these steps:

Step 1 Open the backup and restore wizard in one of these ways:

- Log in to Content Server web interface in Internet Explorer. From the **Management** tab, go to **Configuration > Windows server**. In the dialog box that appears, log in with the local administrator password. Then go to **Maintenance > Backup**. In the Welcome to the Backup or Restore Wizard dialog box, click **Advanced Mode**.

Note Internet Explorer security settings might prevent the necessary Active X scripts from running. With certain browser security settings, you will not be able to access the web interface for Windows Server administration or some of its tools. To overcome this issue, add the URL of the Content Server to the trusted sites in your browser. In Internet Explorer, go to **Tools > Internet Options**. Click the **Security** tab. Click **Trusted sites** and then **Sites**. Add the Content Server URL.

- Log in to the Content Server through Windows Remote Desktop. Go to **Start > All Programs > Accessories > System Tools > Backup**. In the Welcome dialog box, click **Advanced Mode**.

Step 2 Click the **Schedule Job** tab. Then click **Add Job**. In the next dialog box, click **Next**.

Step 3 In the What to Back Up dialog, click **Let me choose what to back up**. Click **Next**.

Step 4 In the Items to Back Up dialog, expand **My Computer**. Check **Local Disk (C:)**, **Local Disk (E:)**, and **System State**. Click **Next**.

Step 5 In the Backup Type, Destination, and Name dialog, browse to the USB drive or network location that you want to back up to (see the "Before Backing Up" section on page 7-2 for more information). Type a name for the backup. Click **Next**.

Step 6 In the Type of Backup dialog, choose the type of backup from the drop-down list. Then click **Next**.

Step 7 In the How to Back Up dialog, check **Verify data after backup**. Click **Next**.

Step 8 In the Backup Options dialog, click **Append this backup to the existing backups**. Click **Next**.

Step 9 In the When to Backup dialog, click **Later**. Enter a name for the backup. Then click **Set Schedule**. Enter your desired schedule. Click **OK**.

Step 10 Enter an account that has administrative privileges on the Content Server (this could be the local administrator account, or if the Content Server is on a domain, a domain administrator account). Enter the administrator account password and confirm. Click **OK**.

Step 11 In the Completing the Backup or Restore Wizard dialog, verify the summary of your choices. Click **Finish**. The backup process is now scheduled to run according to the schedule you set.

Restoring Files

Note If your media files are located on a Network Attached Storage device (NAS) or on an external media server, this 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.

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.

Restoring from a Backup

To restore the Content Server from a backup, follow these steps:

Step 1 End any recording calls that are in progress.

Step 2 Log in to the Content Server using Windows Remote Desktop Connection.

Step 3 Uninstall the Content Server software:

a. Go to **Start > Control Panel > Add or Remove Programs**.

b. Click **Cisco TelePresence Content Server**. Click **Change**.

c. Select the **Remove** option. Click **Next**.

d. Click **Microsoft SQL Server 2005**. Click **Remove**.

e. In Component selection, select **TCS database engine**. Click **Next**.

f. Select **Microsoft SQL Server VSSWriter**. Click **Remove**.

g. Select **Microsoft SQL Server Setup Support Files**. Click **Remove**.

Step 4 Browse to C:\Windows\Security and look for files called edb*.log. (There is edb.log and at least one more file often called edbtmp.log or edb0000*.log.) Do not delete edb.log, but delete the other files. Not removing these files could result in issues with future upgrades after a restore.

Step 5 Go to **Start > Programs > Accessories > System Tools > Backup** to start the Backup and Restore Wizard.

Step 6 Click **Restore files and settings**. Click **Next**.

Step 7 In the What to Restore dialog, check **Local Disk (C:)**, **Local Disk (E:)** and **System State**. Click **Next**.

Step 8 In the Completing the Backup or Restore Wizard dialog, click **Advanced**.

Step 9 From Where to Restore, leave **Original location** (the default setting). Click **Next** and **OK** to acknowledge the warning.

Step 10 In the How to Restore, select **Replace existing files**. Click **Next**.

Step 11 Leave the default options in Advanced Restore Options. Click **Next**.

Step 12 Verify your choices. Click **Finish**. The restoring process starts, and progress is displayed. When the process is complete, you can display a detailed report by clicking **Report**.

Step 13 Restart the Content Server after the restoring process is successfully completed.

Upgrading the Content Server

We strongly recommend that you check regularly for upgrades to the Content Server software on Cisco.com. To upgrade the Content Server, read the release notes for the software that you are upgrading to. Then follow the upgrade procedure as described here:

- Downloading Content Server Software Releases, page 7-5
- Upgrading the Content Server Software, page 7-5

Note You need a release key to upgrade to another major release train (for example, from release 4.x to 5.x). However, if you upgrade to another release in the same release train, you do not need a release key (for example, from release 5.0 to 5.1). Release keys are available from Cisco.com, and you need your Content Server serial number to get the correct key.

Downloading Content Server Software Releases

Step 1 Log in to the Content Server web interface in the site manager role. From the **Management** tab, go to **Diagnostics > Server overview**.

Step 2 Note the software version that is currently installed.

Step 3 Go to the software download page for the Content Server on Cisco.com. Check for the more recent releases of software.

Step 4 Download the desired installer to a directory on your computer.

Upgrading the Content Server Software

Step 1 Verify that there are no active recording calls or active transcoding sessions.

Step 2 Log in to the Content Server using Windows Remote Desktop Connection.

Step 3 Back up your Content Server (see the Backing Up the Content Server, page 7-1 for more information). Turn off any anti-virus programs.

Step 4 Transfer the installer that you downloaded in Step 4 above to the Content Server. Do not run the installer from a mapped or network drive.

Step 5 If you want, verify the MD5 hash (checksum) of the file.

The unique MD5 file that is provided with the installer can be used to verify that a file has not become corrupted as a result of a faulty file transfer, a disk error, or tampering. With the provided MD5, any MD5 program can be used for verifying the installer.

Step 6 Double-click the executable to run it. Follow the on-screen instructions.

Step 7 If prompted, restart the Content Server. Otherwise, terminate your Windows Remote Desktop Connection session by logging off. Do not choose Shutdown because doing so shuts down the Content Server.

Shutting Down and Restarting the Content Server

You can shut down and restart the Content Engine service by restarting the Content Server. In the web interface for Windows Server administration, go to **Maintenance > Shutdown > Restart**. Before a shutdown and restart, you must first assign shutdown permission to the domain user on the Content Server that you want to shut down and restart. See the Resolved Caveats section in the *Release Notes for Cisco TelePresence Content Server Release 5.3.x* on Cisco.com for more information (CSCuf16163).

You can also use a serial cable to connect a PC to the Content Server serial port to shut down and restart the server. Cisco recommends that you end all calls on the Content Server before you shut down.

Note If calls are in progress when the shutdown occurs, the recorded calls appear in the recordings list but might be unusable. They can be deleted in the normal way.

To restart the Content Server, do the following:

Step 1 Connect the supplied serial cable from the serial port on the back of the Content Server to the serial port on a PC.

Step 2 Start a terminal emulator program on the PC by going to **All Programs > Accessories >Communications > HyperTerminal**. (If HyperTerminal is not installed, download a terminal emulator program from the internet—for example, puTTY.)

Step 3 Open a new connection. Enter a name for the connection.

Step 4 Configure the connection to use the PC serial port as follows:

a. a. Set **Baud rate** to 115200 bps.

b. b. Set **Data bits** to 8.

c. c. Set **Parity** to None.

d. d. Set **Stop bits** to 1.

e. e. Set **Flow control (hardware and software)** to None.

Step 5 Click **OK**.

Step 6 Press **Enter** to display the main menu.

Step 7 Make sure that the Content Server is not recording or transcoding. Then press **Esc** to display Content Server version, IP address, and recording/transcoding status.

Step 8 Use the up or down arrows to navigate to **Commands** and press **Enter** to select.

Step 9 Use the up or down arrows to navigate to **Restart** and press **Enter** to select.

Step 10 Close the terminal emulator session and disconnect the serial cable.

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

To shut down the Content Server using a PC connected to the serial port, do the following:

Step 1 1. Follow steps 1-8 in the previous section.

Step 2 2. Use the up or down arrows to navigate to **Shutdown** and press **Enter**.

Step 3 3. Close the terminal emulator session and disconnect the serial cable.

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

Table 7-1 Terminal Emulator Session Keys

Key	Description
Enter key	Enters Edit mode, confirms an entry.
Esc key	Returns to the previous menu, exits Edit mode without saving.
Up and down arrow keys	Moves between menu items, moves between values in a numerical address and modifies numerical values.

Restoring the Content Server Defaults

You can restore the Content Server to its default settings, partially or fully, usinga PC connected to the Content Server serial port:

- A partial restore (using **ConfigRestore**) deletes all user-created recording aliases, media server configurations, call configurations, and templates. **ConfigRestore** restores the default configuration for the current software release, but does not affect the recordings stored on the server.
- A full restore (using **FullRestore**) deletes all recordings, media files and logs, in addition to deleting all user-created recording aliases, media server configurations, call configurations and templates. **FullRestore** restores the default configuration for the current release. If the data location has been changed to an external storage location (NAS), it also changes the default storage location back to the Content Server. Media files on the NAS are not deleted.

Caution Restoring to defaults (either a partial or full restore) must not be interrupted. Logs of the restore are available in E:\logs\SetupUtility directory.

Important notes:

- Restoring to defaults cleans up the Content Server's database and/or media. It does not revert the Content Server back to the state it was in when delivered (that is, the restore does not affect the operating system in any way).
- A partial restore (**ConfigRestore**) is not available for Content Servers in a cluster.
- A full restore (using **FullRestore**) run on a Content Server which has been clustered will revert that Content Server to a standalone Content Server with the default configuration files for the current software release, and no media. However, the cluster database will still report that this Content Server is part of a cluster: Cisco recommends removing a clustered Content Server from the cluster by running the TCS Wizard before restoring it to its default settings.

To restore default settings, do the following:

Step 1 Connect the supplied serial cable from the serial port on the back of the Content Server to the serial port on a PC.

Step 2 Start a terminal emulator program on the PC by going to **All Programs > Accessories > Communications > HyperTerminal.** (If HyperTerminal is not installed, download a terminal emulator program from the internet—for example, puTTY.)

Step 3 Open a new connection. Enter a name for the connection.

Step 4 Configure the connection to use the PC serial port as follows:

a. Set **Baud rate** to 115200 bps.

b. Set **Data bits** to 8.

c. Set **Parity** to None.

d. Set **Stop bits** to 1.

e. Set **Flow control (hardware and software)** to None.

Step 5 Click **OK**.

Step 6 Press **Enter** to display the main menu.

Step 7 Ensure that the Content Server is not recording or transcoding. Then press **Esc** to display Content Server version, IP address, and recording/transcoding status.

Step 8 Use the up or down arrows to navigate to **Commands** and press **Enter** to select.

Step 9 Use the up or down arrows to navigate to either **FullRestore** or **ConfigRestore** (see "Important Notes" above for more information). Press **Enter**.

Step 10 Close the terminal emulator session and disconnect the serial cable.

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

For terminal emulator session keys, see Table 7-1.

Securing the Content Server

Antivirus Protection

Antivirus protection may be used on the Content Server.

If you use antivirus software on the Content Server, 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

Microsoft security patches may be applied 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 web site or use Windows Update.

Content Server security bulletins inform you of patches either that we recommend highly or that we do not recommend applying because they have been known to cause instability in the Content Server application. These bulletins will be published if aspects of Microsoft patches are critical to performance or security of the Content Server.

Access the latest Content Server security bulletin at 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 2003 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.

CHAPTER 8

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.

CHAPTER 9

Premium Resolution

Additional functionality is available on second-generation Content Server hardware by adding a Premium Resolution key. 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 9-1 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 9-1 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.

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 to 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 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.

CHAPTER 10

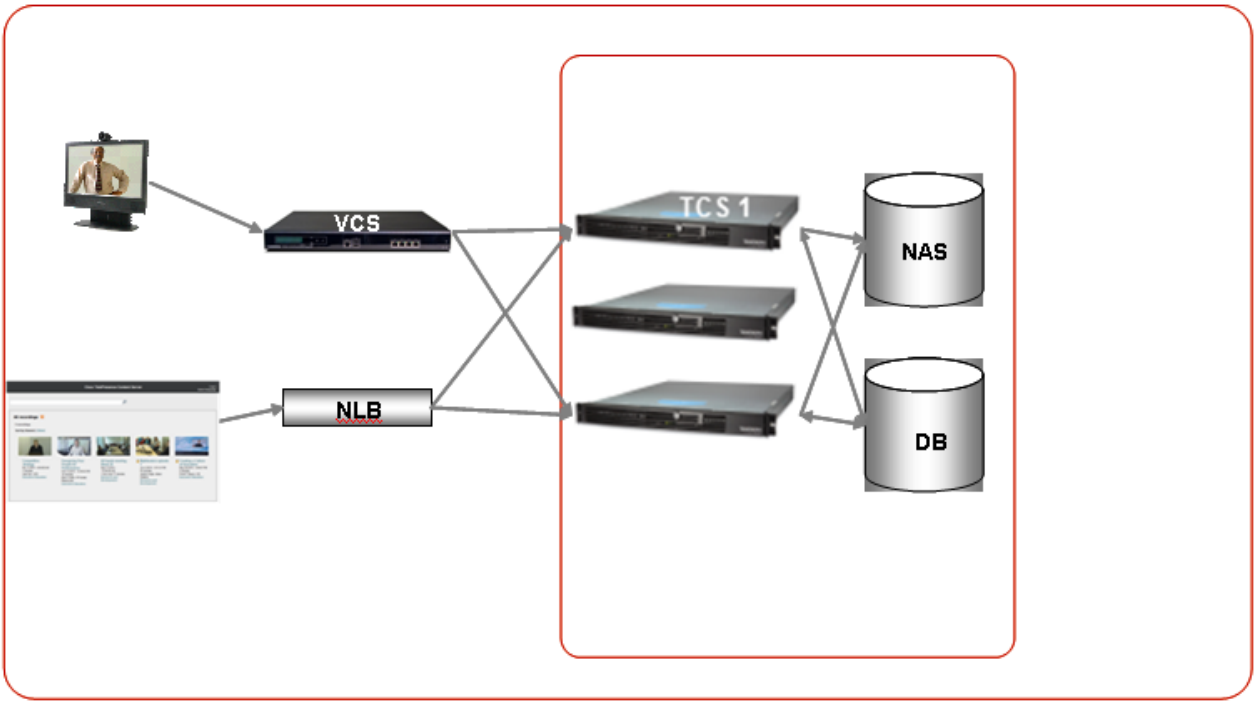
Creating and Managing a Content Server Cluster

This chapter describes the main features, system requirements, setup, and management of a Cisco TelePresence Content Server (TCS) cluster. To a user, a Content Server Cluster behaves exactly as a single Content Server does, but a cluster has a much greater capacity for recording, streaming, and serving the web interface.

Main Features

General Reliability

Multiple Content Servers can be clustered together to increase total recording and playback capacity. In this 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.



Interface Redundancy

The user 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 whole cluster, as well as 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 solution (NLB) ensures that incoming user HTTP requests are spread across the cluster. While multiple solutions are available to handle NLB, the final recommendation in this document includes a hardware solution, Loadbalancer.org.

Inbound H.323 Call Routing

Inbound call load balancing is managed by the VCS (Video Communications Server) that the cluster is registered to. Each Content Server is only 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 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 watched until recording has finished and the offline transcoder has processed the outputs 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 needs two gateway registrations with separate prefixes—one for live transcoded calls and another for non-live (offline transcoded) calls—to ensure 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 that come in on that prefix until it signals that resources are available.

Additionally, for registrations with the VCS, each Content Server needs four system aliases: live and non-live H.323 ID and E.164 system aliases. 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 this 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 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 redundancy of the API functionality and to ensure that the external implementation does not artificially create a controller, it is up to the integrator to build the logic around distributing the API commands among all Content Servers in the cluster to deal with situations such as Content Server unavailability.

Scalable Storage

One Network Attached Storage (NAS) is used for the whole cluster, and 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 API, which provides a special command for dialing out of the cluster as well as cluster status documents to report status and configuration across all nodes. The cluster API commands are fully documented in the Cisco TelePresence Content Server API Guide.

System Requirements

Cisco TelePresence Content Server

- Version 3.3 or higher.
- Each Content Server in the cluster and the NAS must be added to the same Windows Active Directory domain.
- A Cluster Enabled option key is required for each Content Server that is going to be added to a cluster. The option key must be installed before running the TCS wizard so that the clustering option is accessible in the wizard.
- A valid HTTPS security certificate should be obtained from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.). This certificate should then be 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 10-7 for information about database configuration.

Gatekeeper

- VCS X2.1 or higher.

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.

Network Attached Storage (NAS)

- Compatible systems include any NAS device built on the Windows Storage server and which 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 10-10 for information about the required NAS share configuration.

Important Guidelines

- The current solution supports up to 10 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 supports H.323 protocol only. SIP registration and SIP calling is not supported.
- 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.
- The ConfigRestore command (**Main Menu > Commands > Restore Defaults > ConfigRestore**), which available through a serial port connection, is not available when a Content Server is in a cluster.
- The FullRestore command (**Main Menu > Commands > Restore Defaults > FullRestore**), which is available through a serial port connection, restores the Content Server to its original settings, but the command also causes it to lose its cluster settings, while cluster database continues as if the Content Server were still in the cluster. Adding the TCS back to the cluster after running FullRestore is recommended. The Content Server can then be removed from the cluster, if required, using the TCS wizard.
- Adding or removing the live output from a template results in a change of the gateway prefix of recording aliases that use that template.

  Example:

  The live gateway prefix on your cluster is tcscluster.live and the non-live gateway prefix is tcscluster.nonlive.

  A recording alias with an H.323 ID of tcscluster.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 tcscluster.nonlive.myalias@company.com to tcscluster.live.myalias@company.com. Calls to the original alias fail.
- A Premium Resolution Content Server that you add to a non-Premium Resolution cluster behaves like an 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 begins to behave

as 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 9, "Premium Resolution" for more information about Premium Resolution.

See the release notes for a list of other known issues for this release.

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 10-5 before setting up a cluster.

Overview of the Process

Understand Content Server Prerequisites

- Ensure that all the Content Servers that you want to cluster are at version S3.3 or higher. If they are not, upgrade them to at least version S3.3, and check that they have the same build number.
- 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 TCS wizard so that the clustering option is accessible in the wizard.

- Install security certificates from a trusted source, such as a Certificate Authority (COMODO, VeriSign, etc.). This certificate should then be installed 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 through the network load balanced address.

  For more information on installing security certificates, please see the Security Certificate Management section in the TCS Getting Started Guide.
- Ensure 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 10-4).

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 10-7

Step 2 Configure the SQL Server Instance, page 10-8

Step 3 Create a Special User on the SQL Server, page 10-9

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 have to add a new instance to your existing SQL server installation. If Microsoft SQL Server is not already installed, you must install Microsoft SQL Server in order to create the new instance. In both cases, in order to create the instance, you need the Microsoft SQL Server installer available from Microsoft on the installation media (CD or DVD). See the "System Requirements" section on page 10-4 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 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 TCS wizard database connection test fails, and you cannot create a Content Server Cluster with this instance

For more information on installing SQL Server 2005, see Microsoft article in the SQL Server 2005 Books Online:

Preparing to Install SQL Server 2005: http://msdn.microsoft.com/en-us/library/ms143719.aspx

Security Considerations for a SQL Server Installation: http://msdn.microsoft.com/en-us/library/ms144228.aspx

Check Parameters for the System Configuration Checker: http://msdn.microsoft.com/en-us/library/ms143753.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 10-7).

Step 3 Ensure that these parameters are configured as follows:

- **a.** Shared Memory is enabled.
- **b.** Named Pipes are disabled.
- **c.** TCP/IP is enabled.
- **d.** VIA is disabled.

Step 4 Right click **TCP/IP** and click properties. Click the **IP Addresses** tab:

- **a.** For each IP address, set **Enabled** to **No**.
- **b.** Clear all **TCP Dynamic Ports** fields. Delete any zeros that appear in those fields.
- **c.** 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 TCS 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

Before You Begin

This user requires administrative privileges and CREATE TABLE and ALTER TABLE authorization.

Choose any username that you want for this user.

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 10-7).

Step 3 At the Command Utility prompt `1>`, enter the following command to create a user:

```
CREATE LOGIN user_name WITH PASSWORD='strong_password'
```

Then press **Enter**.

Step 4 At the prompt, enter **GO** and press **Enter**.

Step 5 Enter **EXIT** and press **Enter** to exit sqlcmd.

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

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

For more information on using the sqlcmd utility, see the Microsoft article in the SQL Server Books Online: 'sqlcmd Utility."

For more information on creating a user using CREATE LOGIN, see the Microsoft article in the SQL Server Books Online: "CREATE LOGIN (Transact-SQL)."

Configure the NAS

The Content Server cluster uses a share on the NAS as its media storage location. See "System Requirements" section on page 10-4 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 10-10

Step 2 Choose or Create a Domain Account to Access the NAS Share, page 10-10

Step 3 Set up a Share on the NAS, page 10-10

Step 4 Set Permissions and Security Settings on the Share, page 10-11

Manage the Windows Active Directory Domain

All Content Servers in 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 may choose any username you want for this user. In this document, we refer to this user as MYDOMAIN\TCS_NAS_USER. MYDOMAIN\TCS_NAS_USER is used by the Content Server Cluster to access the NAS share.

Note You must enter the username and password for MYDOMAIN\TCS_NAS_USER when you run the TCS wizard.

Set up a Share on the NAS

Step 1 Log on to the NAS using Windows Remote Desktop Connection.

Step 2 Create a folder on the NAS.

Step 3 Make this folder a shared folder.

Note You must enter the path to this share when you run the TCS 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 use the TCS wizard successfully.

Step 1 Right-click the share, and click **Sharing and Security**.

a. Click **Permissions**.

b. Click **Add**.

c. Click **Object Types**.

d. Check the box for Type—**Computers**.

e. Enter all the DNS names of Content Servers that you want to cluster. You used these DNS names when you registered the Content Servers in the domain.

f. Click **Check Names**. Click **OK**.

g. Enter the name of the MYDOMAIN\TCS_NAS_USER account.

h. Click **Check Names**. Click **OK**.

i. Give each of the Content Servers and MYDOMAIN\TCS_NAS_USER full control over the share.

Step 2 Click the **Security** tab.

a. Click **Add**.

b. Click **Object Types**.

c. Check the box for Type—**Computers**.

d. Enter all the DNS names of Content Servers that you want to cluster. You used these DNS names when you registered the Content Servers in the domain.

e. Click **Check Names**. Click **OK**.

f. Enter the name of the MYDOMAIN\TCS_NAS_USER account.

g. Click **Check Names**. Click **OK**.

h. Give each of the Content Servers and MYDOMAIN\TCS_NAS_USER full control over the share in the Security Settings tab.

Create a Content Server Cluster

In order to create a cluster of Content Servers, you must run the TCS wizard from Remote Desktop on one of the Content Servers. Then you must run the TCS wizard on all the remaining Content Servers to add them to the cluster.

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, take these 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 of these Content Servers are added in order to the same cluster, playback aliases are modified for all Content Servers that are added to the cluster after the first server to avoid duplicate aliases. The playback aliases for these servers in the same 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 TCS disk drive and are deleted. If you move media between NAS locations or from the NAS to a local TCS disk drive, the wizard does not move these files, but the wizard does not delete them.

TCS Wizard Options

The TCS wizard that is available as a shortcut from the Remote Desktop of version S3.3 or later Content Servers 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 TCS, you see these options:

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

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

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

User Accounts for the TCS Wizard

The TCS 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 10-10.
- The local default administrator account.

Note Unless explicitly stated otherwise, this document assumes that the TCS wizard is run under a domain administrator account.

Before Running the TCS Wizard

Before you run the TCS wizard to create a new cluster, ensure 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 TCS 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. Ensure 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 TCS_DB_USER).
- The username and password of TCS_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 MYDOMAIN\TCS_NAS_USER domain account.

Create a New 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 **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add the domain account MYDOMAIN\TCS_NAS_USER to the Administrators group on the Content Server.

Step 3 Double click the TCS Wizard icon on the desktop, or open **All Programs > Cisco > Content Server > TCS Wizard**.

Step 4 Click **Next** from the Welcome screen.

Step 5 The wizard displays an overview screen and then runs through its initialization phase. If recordings are in progress on this Content Server, the wizard cannot continue. You can either end the recordings or cancel the wizard. If possible, end the recordings and continue running the wizard.

Step 6 After the wizard finishes its initialization stage, 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 after the wizard process is completed or is cancelled.

Step 7 Click the **Cluster Management Wizard** radio button. Click **Next**.

Step 8 The wizard then verifies cluster prerequisites. Click **Next**.

Step 9 Click the **Create a new cluster** radio button. Click **Next**.

Step 10 Read the informational screen. Click **Next**.

Step 11 At the **Connect to an external SQL Server Database** screen, enter the information for the database instance you have set up:

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

Step 12 Click **Next** in the database configuration informational screen.

Step 13 Enter the username and password of the database user that you created. The TCS uses these user credentials to connect to the database.

Step 14 Click **Next** in the next informational screen.

Step 15 Enter the path for the NAS share that you set up. The path is in this format: *server**share*. Ensure that you enter the NAS server computer name, not the IP address of the NAS.

Step 16 Click **Next** in the next informational screen.

Step 17 In the IIS Anonymous User Account screen, enter the username and password of the domain account that you created. The TCS uses these credentials to access the share on the NAS. An example of a username: MYDOMAIN\TCS_NAS_USER.

Step 18 Click **Next** in the next informational screen.

Step 19 In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for this Content Server. The defaults that are suggested by the wizard are based on the current settings of the standalone TCS. 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. You can change the system name and aliases for this Content Server from the Server Overview page after you successfully set up the cluster.

Step 20 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 TCS is not backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again. Your system will not have changed if you click **Cancel**.

Step 21 The Cluster: Test Result screen displays information about your intended setup. If all tests are successful, click **Configure** to configure the cluster.

You can also click **Finish** to exit 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.

If 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.

Step 22 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. Then click **Save**.

You can also generate the cluster settings file by running this TCS wizard again after you finish creating the cluster (see "Generate a Cluster Settings File" section on page 10-24). You need the cluster settings file if you want to add other Content Servers to this cluster.

Step 23 Click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

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

Note Your cluster cannot make calls until you have registered it to a gatekeeper. See the "Configure Gatekeeper Registration" section on page 10-17.

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 "Understand Content Server Prerequisites" section on page 10-6.
- 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 TCS wizard on any of the Content Servers that are already in the cluster. See the "Generate a Cluster Settings File" section on page 10-24.

Note To understand which configurations and media content from additional Content Servers are added to the cluster, see "The Order of Content Servers Added to the Cluster" section on page 10-12.

After ensuring that additional Content Servers meet the prerequisites, run the TCS 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 Content Server that you want to add to the cluster.

Step 2 Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add the domain account MYDOMAIN\TCS_NAS_USER to the Administrators group on the Content Server.

Step 3 Double-click the TCS Wizard icon on the desktop, or open **All Programs > Cisco > Content Server > TCS Wizard**.

Step 4 Click **Next** in the Welcome screen. The wizard displays an overview screen and then runs through its initialization phase. If recordings are in progress on this Content Server, the wizard cannot continue. You can either end the recordings or cancel the wizard. If possible, end the recordings and continue running the wizard.

Step 5 After the wizard finishes its initialization stage, 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 after the wizard process is completed or is cancelled.

Step 6 Click the **Cluster Management Wizard** radio button. Click **Next**.

Step 7 The wizard then verifies cluster prerequisites. Click **Next**.

Step 8 Click the **Add to an existing cluster** radio button.

Step 9 In the Cluster: Load Cluster Settings File window, browse to the cluster settings file that you copied to the desktop.

Step 10 In the Content Server System Configuration screen, you can change the **System name** and default **Non-Live** and **Live** system aliases for this Content Server. The defaults that are suggested by the wizard are based on the current settings of the standalone TCS. 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. You can change the system name and aliases for this Content Server from the Server Overview page after you add the Content Server to the cluster.

Step 11 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 TCS is not backed up and antivirus software is not stopped, cancel the wizard and complete those actions. Then run the wizard again.

Step 12 The Cluster: Test Result screen displays information about your intended setup and the amount of media to be moved from this Content Server to the media location for the cluster (NAS). If all tests are successful, click **Configure** to configure the Content Server and add it to the cluster.

You can also click **Finish** to exit the wizard without adding the Content Server to the cluster or making any changes. If any of the tests failed, you cannot continue to run the wizard.

If you click Configure, the wizard configures your system and adds the Content Server to the cluster. This process might take some time, depending on the amount of media to be moved to the NAS.

Step 13 Click **Finish** to exit the wizard. The log location for the wizard is displayed on this screen.

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

Configure Gatekeeper Registration

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.

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 your VCS.

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 ensure good load balancing of both types of call across the cluster by the gatekeeper.

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 TCS. 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 system H.323 ID or E.164 alias. Duplications might cause the gatekeeper to reject registration.

If you want to change 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.

Live and Non-Live Prefixes for the Cluster

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 by the gatekeeper. 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 also 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 10-3 for more information.

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's 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. Refer to the TCS Online Help for more information on 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 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 a NLB solution. With an NLB solution, users access the cluster with the Virtual IP address (VIP) that you set up 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 ensure that this process works, you must install a loopback adapter and set its IP to the VIP.

In order to set up network load balancing for a Content Server Cluster, follow these steps:

Step 1 Configure a Load Balancer, page 10-19.

Step 2 Set up a Loopback Adapter on Each TCS in Cluster, page 10-20.

Step 3 Enter the Virtual IP Address of the Cluster (VIP) as the Frontend Address on the TCS, page 10-20.

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 virtual server IP address (VIP) will be accessed by Content Server users. When set up successfully, the load balancer receives a request on the VIP and forwards the request to one of the Content Servers in the cluster.

The VIP in this example setup is 10.10.2.111. In the example, we set up four virtual servers for the cluster, one for each port needed for a TCS 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 set up 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 here). Then enter the VIP that you want to use, followed by the port for this 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 of these virtual servers for each of the ports that you want to load balance. Use different labels each time but the same VIP.

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 into each of the virtual servers you just set up.

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 this TCS, as well as the server IP address, followed by the same port as the one that is used for the virtual server (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. Repeating this procedure, add each additional server in the cluster to each of the virtual servers.

Set up a Loopback Adapter on Each TCS in Cluster

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

Step 1 Log in to the Content Server using Windows Remote Desktop Connection. Run the TCS 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 10-25 for details about updating the load balancer configuration.

Enter the Virtual IP Address of the Cluster (VIP) as the Frontend Address on the TCS

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 TMS use the frontend address.

Managing a Content Server Cluster

This section describes cluster management functionalities that are different from the functionalities of a standalone TCS. This section supplements the Content Server online help.

- Edit Information Common to All Content Servers in Cluster, page 10-23
- Generate a Cluster Settings File, page 10-24
- Update Load Balancer Configuration, page 10-25
- Update Cluster Settings, page 10-25

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 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, Trancoding 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, Trancoding 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 fronted 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 that 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 whole cluster. You can end recording calls on a specific Content Server from the Server overview page for that Content Server.
- Allows you to put a Content Server in maintenance mode. When the Content Server is in maintenance mode, that 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 that Content 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. After 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 some additional information relevant to the cluster, such as:

- 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 will be displayed in red as a warning to the administrator. The administrator should free up space on the NAS. When 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 TCS 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.

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

When all current calls are finished, 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 recording calls manually on the Content Server. Clicking on **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 new calls.

API

The clustering functionality requires that API be enabled. It is not possible to disable the API when Content Servers are clustered. It is important to ensure that the API password is changed from the default at the time of setup.

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 10-16). Cluster settings are in an XML file that contains details of the external database and the TCS_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 using Windows Remote Desktop Connection. Run the TCS 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 on the TCS desktop. Click **Next**.

Step 4 Click **Finish** to exit the wizard.

Update Load Balancer Configuration

If you have changed the virtual IP (VIP) address of the cluster on the load balancer, you need to update it on each Content Server using the TCS wizard.

Step 1 Log in to the Content Server using Windows Remote Desktop Connection. Run the TCS 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 new virtual IP (VIP) address of the cluster that you set up on the load balancer and/or the subnet mask of your network.

Step 5 Click **Next**.

Step 6 Click **Configure** for the wizard to update the loopback adapter. This process might take some time.

Step 7 Click **Finish**.

Step 8 Repeat this procedure for each Content Server in the cluster.

Step 9 In Site settings page, update the frontend address in Site Settings to the new VIP. See "Enter the Virtual IP Address of the Cluster (VIP) as the Frontend Address on the TCS" section on page 10-20 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 TCS 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 using the TCS wizard.

The TCS wizard allows you to:

- Update the Password for MYDOMAIN\TCS_NAS_USER Account, page 10-26
- Change the MYDOMAIN\TCS_NAS_USER Account to Another Domain Account, page 10-26

- Change the Location of the Media Files to a Different NAS Share, page 10-27

Note As an alternative to the procedures described below, you could also remove all Content Servers from the cluster (see "Removing a Content Server from the Cluster" section on page 10-28 for details) and use the TCS NAS wizard on the last Content Server that you 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\TCS_NAS_USER Account

If the password for the account that cluster uses to connect to the NAS—MYDOMAIN\TCS_NAS_USER—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.

The domain administrator needs to set a new password for the account on the domain, and then you must run the TCS wizard on each Content Server in the cluster to update the password:

Step 1 Log in to the Content Server using Windows Remote Desktop Connection as a domain administrator. Run the TCS 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.

You can also click **Finish** to exit the wizard without updating the cluster settings.

Step 6 If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.

Step 7 Click **Finish** to exit the wizard.

Step 8 Repeat the procedure on the other Content Servers in the cluster.

Change the MYDOMAIN\TCS_NAS_USER Account to Another Domain Account

If the account that the cluster uses to connect to the NAS—MYDOMAIN\TCS_NAS_USER—needs to change, get the details of the new domain account from your domain administrator. Then do the following:

Step 1 Add the new account (in this procedure, we refer to the new account as MYDOMAIN\TCS_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 10-11 for details).

Step 2 Log in as a domain administrator to one of the Content Servers in the cluster using Windows Remote Desktop Connection.

Step 3 Go to **Computer Management > System Tools > Local Users and Groups > Groups > Administrators**. Add MYDOMAIN\TCS_NEW_NAS_USER to the Administrators group.

Step 4 Start the TCS 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\TCS_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.

You can also click **Finish** to exit the wizard without updating the cluster settings.

Step 9 If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.

Step 10 Click **Finish** to exit the wizard.

Step 11 Repeat this procedure on the other 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, do the following steps:

Step 1 Set up a new NAS share (see the "Configure the NAS" section on page 10-10 for details). The permissions on this share must allow all Content Servers in the cluster and the MYDOMAIN\TCS_NAS_USER full control of the share. You can continue to use the same MYDOMAIN\TCS_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—in other words, files that are being watched or downloaded by users. Cisco recommends 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 is identical on the new NAS share as on the old NAS share.

Step 4 Log in to a Content Server in the cluster using Windows Remote Desktop Connection. Start the TCS 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.

Step 9 If you click **Configure**, the wizard configures your system and updates settings. This process might take some time.

Step 10 Click **Finish** to exit the wizard.

Step 11 Repeat this procedure on the other Content Servers in the cluster to set the new media location details in IIS.

Removing a Content Server from the Cluster

You can remove one or more Content Servers from the cluster at any time and use them as standalone Content Servers. Run the TCS wizard if you want to remove a Content Server from a cluster.

Note If you are removing Content Servers from a cluster, the order in which you remove them is important.

None of the media or configurations from the cluster are available on Content Servers after you remove them from the cluster. These removed Content Servers become standalone installations with no content or configurations, with the exception of the last Content Server you remove from the cluster. When you run the TCS wizard on the last Content Server remaining in a cluster and click **Remove from cluster**, the last Content Server become a standalone server with media on a NAS. This last Content 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 this 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 using Windows Remote Desktop Connection. Run the TCS 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.

You can also click **Finish** to exit the wizard without removing the Content Server from the cluster. If the external database set up test failed, you cannot remove this Content Server from the cluster.

If you click **Configure**, the wizard configures your system and removes the Content Server from the cluster. This process might take some time.

Step 5 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 this Content Server, but this Content Server is not removed from the load balancer setup. You must remove this Content Server from your load balancer configuration manually. If you do not remove the Content Server from the load balancing configuration, the load balancer continues to try to direct traffic to a Content Server that no longer belongs to the cluster.

Caution If the frontend address in a cluster 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

TMS 12.2 or higher can be used to schedule recording calls on a version 3.3 or higher cluster. Cisco recommends 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.

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 the "Backing Up and Restoring the Content Server Cluster" section on page 10-31). 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 TCS 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 from SQL Server 2005 to SQL Server 2008

Content Server cluster version 3.3 supported only one external Microsoft SQL server version: MSSQL Server 2005. Content Server cluster version 4.0 or later now supports MSSQL Server 2005 or MSSQL Server 2008. When you upgrade your Content Server Cluster from 3.3 to 4.0 or later, you have a choice to upgrade the external SQL server.

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 10-31).

Step 2 Upgrade the cluster by running the S4.0 upgrade installer on each TCS in cluster (see "Upgrading the Cluster to a New Software Version" section on page 10-30).

Step 3 Cisco recommends that you shut down all the Content Servers in a cluster to stop them from communicating with the database while your external SQL server is upgraded.

Shutting down the Content Servers prevents them from trying to access the database while your external SQL server is being upgraded. Putting the Content Servers in maintenance mode alone does not ensure that they stop communicating with the database.

Step 4 Upgrade the instance the cluster uses on the external Microsoft SQL server from MSSQL Server 2005 to MSSQL Server 2008.

Step 5 Power on the Content Servers.

Step 6 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). Cisco also recommends making a test call to the cluster.

Backing Up and Restoring the Content Server Cluster

Cisco recommends that you back up the cluster regularly and also before you upgrade it or install a security update.

It is very important to follow the procedure described here. If you do not follow this procedure, 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:

- The Clustered Content Servers, page 10-31
- The external MS SQL database, page 10-31
- The Media on the NAS/External Streaming Server, page 10-31

The Clustered Content Servers

To back up and restore the Content Servers in a cluster, follow the backup and restoring procedures as described in Chapter 7, “Maintaining the Content Server.”

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.

The 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 Network Attached Storage device (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.

APPENDIX A

Supported Platforms, Browsers, and Plug-ins

Table A-1 Content Server: Platforms, Browsers, and Plug-ins Dependencies

Operating System	Browser	Silverlight	Flash	Windows Media	QuickTime
Windows	Mozilla Firefox 3.6.x and 10	v. 4	v. 10.3 and 11	Windows Media Player 9.x, 10.x, and 11.x	v. 7.0 to 7.6.5
	Internet Explorer 7 and 8	v. 4	v. 10.3 and 11	Windows Media Player 9.x, 10.x, and 11.x	v. 7.0 to 7.6.5
Mac version 10.5 or higher	Mozilla Firefox 3.6.x and 10	v. 4	v. 10.3 and 11	Not supported	v. 7.0 to 7.6.5
	Safari 5 and 5.1.2	v. 4	v. 10.3 and 11	Not supported	v. 7.0 to 7.6.5

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 this URL:

http://port25.technet.com/pages/windows-media-player-firefox-plugin-download.aspx

Note See the *Release Notes for Cisco TelePresence Content Server Release 5.3.x* on Cisco.com for the most current list of supported platforms, browsers, and plug-ins for Content Server Release 5.3.x.

APPENDIX B

Port Information

Table B-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
8098	TCP	Windows Web Administration 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 QuickTime or Darwin streaming servers; Wowza Media Servers for Flash; or multicast streaming in Windows Media streaming servers or QuickTime or Darwin streaming servers.

Ports for Streaming from the Content Server

Streaming Windows Media from the Content Server uses the following ports:

Table B-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 B-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 B-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 B-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 B-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 B-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.

APPENDIX C

License, Copyright, and Trademark Information

Cisco Copyright

Third party licenses information

Amended / expanded copyright notices for third-party software on the TelePresence Content Server systems are listed below:

The non-commercial third party code is distributed in binary form under the terms of open source licenses such as BSD.

In accordance with section (6) of the GNU Lesser General Public License and section 3.6 of the Mozilla Public License, copies of such code will be provided upon request by contacting Cisco. Please contact us by using the Online Support section at www.cisco.com. Please provide USD 10.00 for media and shipping.

License for OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). Copyright © 1998–2005 The OpenSSL Project. All rights reserved.

THE OpenSSL SOFTWARE IS PROVIDED BY THE Open SSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mozilla Public License ("MPL")

Software distributed under the MPL (http://www.mozilla.org/MPL/MPL-1.0.html): MPEG4IP, JS FLV Player.

License for Ogg

Copyright © 2002, Xiph.org Foundation

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Xiph.org Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License for JSON

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, ROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;

OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

```
@category
@package   Services_JSON
@author    Michal Migurski <mike-json@teczno.com>
@author    Matt Knapp <mdknapp[at]gmail[dot]com>
@author    Brett Stimmerman <brettstimmerman[at]gmail[dot]com>
@copyright 2005 Michal Migurski
@license   http://www.opensource.org/licenses/bsd-license.php
@link      http://pear.php.net/pepr/pepr-proposal-show.php?id=198
```

License for Prototype

Prototype is Copyright © 2005-2007 Sam Stephenson (http://conio.net). It is freely distributable under the terms of an MIT-style license (http://dev.rubyonrails.org/browser/spinoffs/prototype/trunk/LICENSE?format=raw).

Copyright © 2005-2007 Sam Stephenson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

License for scriptaculous

script.aculo.us is licensed under the terms of the MIT License (http://www.opensource.org/licenses/mit-license.php).

Copyright © 2005 Thomas Fuchs (http://script.aculo.us, http://mir.aculo.us)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Third party trademark and copyright notices

Portions utilize Microsoft Windows Media Technologies. Copyright © 1999–2002 Microsoft Corporation. All rights reserved.

Wowza Media Server® Disclaimer: Wowza Media Systems, Wowza Media Server and related logos are either registered trademarks or trademarks of Wowza Media Systems, Inc. in the United States and/or other countries.

QuickTime is a trademark of Apple Computer, Inc.

Zune is a trademark of Microsoft Corporation. All rights reserved.

iTunes is a trademark of Apple Inc., registered in the U.S. and other countries.

Podcast Producer is Copyright © 2006-2007 Apple Inc. All Rights Reserved.

Adobe and Flash are registered trademarks of Adobe Systems Incorporated, and may be registered in the United States or in other jurisdictions including internationally.

This product includes PHP software, freely available from http://www.php.net/software/.

Cisco TelePresence Content Server, version 5.2, Copyright 2010-2011, Cisco Systems, Inc. All rights reserved. Certain components of Cisco TelePresence Content Server are licensed under the GNU Lesser Public License (LGPL) Version 2.1. The software code licensed under LGPL Version 2.1 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.1 (http://www.gnu.org/licenses/lgpl-2.1.html). See the User Manual for licensing details.