



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 3-5](#) (appears only with a cluster deployment)
- [Server Logs, page 3-6](#)
- [Transcoding Queue, page 3-7](#)

Recordings

- [Edit Recordings, page 3-8](#)
- [Import Recordings, page 3-21](#)
- [Create Recording, page 3-23](#)

Recording Setup

- [Recording Aliases, page 3-28](#)
- [Categories, page 3-35](#)
- [Templates, page 3-36](#)
- [Media Server Configurations, page 3-42](#)
- [Call Configurations, page 3-59](#)

Configuration

- [Site Settings, page 3-61](#)
- [Groups and Users, page 3-76](#)
- [Windows Server, page 3-81](#)

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 Configuration > Shutdown > Restart. 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.
Current calls	A pictorial representation of the number of current calls.	- 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.

Table 3-1 Diagnostics > Server Overview (continued)

Field	Field Description	Usage Guidelines
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.	—

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.	—

Table 3-1 *Diagnostics > Server Overview (continued)*

Field	Field Description	Usage Guidelines
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 and the Premium Resolution option key.	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 (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name to help users find the recording when they search.
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.

Table 3-2 **Recordings > Edit Recordings: Edit Recording (continued)**

Field	Field Description	Usage Guidelines
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
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 3-2 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, 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"). Note
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. • 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 .
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. • 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 3-3 *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. • 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 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.

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

Field	Field Description	Usage Guidelines
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.
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 <i>No live resources available</i> is displayed if the Content Server is already streaming the maximum number of live recordings. When you see this message, you can only select recording aliases without live streaming.
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 (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name to help users find the recording when they search. If you leave the name field blank, the default name is the name of the recording alias that you use to record.
Description	Details about the recording.	Optional. This optional setting can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.
Keywords	Keywords that can be used to search for the recording. 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 Allow guest access is selected in Site Settings, this field is displayed. If selected, all users, including guests, can view the recording. • Allow access to all authenticated users: If the <i>Allow guest access</i> box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list or Place call adds all matching groups and users to the list. 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](#)).

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 (<i>OnDemand only</i> or <i>Live and OnDemand</i>) and a date/time stamp. You can edit this name to help users find the recording when they search. If you leave the name field blank, the default name is the name of the recording alias that you use to record.
Description	Details about the recording.	Optional. This optional setting can help users find the recording when they search.
Speaker	Name(s) of the speaker(s) in the recording.	Optional. This optional setting can help users find the recording when they search.
Location	Where the recording took place.	Optional. This optional setting can help users find the recording when they search.
Copyright	Copyright information for the recording.	Optional. This optional setting can help users find the recording when they search.
Keywords	Keywords that can be used to search for the recording. Keywords do not appear in the interface.	Optional. This optional setting can help users find the recording when they search.

Table 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 <i>Allow guest access</i> box is not checked in Site Settings, this field is displayed. If selected, all authenticated (logged in) users can view the recording. • Allow access to only these authenticated groups and users: If selected, then only groups or users entered in the field below can view the recording. Enter all or part of the name or display name of the group or user (either one per line or separated by a semicolon). If only part of a group or username has been entered, clicking Check access list, Place call, or Save adds all matching groups and users to the list. 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”).
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.

Table 3-5 **Recording Setup > Recording Aliases: Add Recording Alias or Edit (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.

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").

Play recording on endpoints

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

Table 3-5 **Recording Setup > Recording Aliases: Add Recording Alias or Edit (continued)**

Field	Field Description	Usage Guidelines
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.
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 3-6 **Recording Setup > Templates: Add or Edit Template (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.	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. • 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 3-6 **Recording Setup > Templates: Add or Edit Template (continued)**

Field	Field Description	Usage Guidelines
On demand sizes	Choose up to two recording sizes based on your user streaming environment and internet connection.	• 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 .
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.

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

Field	Field Description	Usage Guidelines
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.
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. • 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 3-6 **Recording Setup > Templates: Add or Edit Template (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.
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. • 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.



Note

Before you start delivering your live content as a multicast stream, ensure that the network is multicast enabled.

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	Click to use an existing publishing point on the streaming server.	—
Publishing point name	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	Click to use an existing publishing point on the streaming server.	—
Publishing point name	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. An external 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 streaming MPEG-4 for QuickTime 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. 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 only HTTP-based on demand streaming of MPEG-4 for Flash from its local 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. Only the Wowza Media Server for Flash is supported for streaming MPEG-4 for Flash 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. 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.	—

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.

Media Experience Engine 3500 is a product provided by Cisco. For setup and support information, go to <http://www.cisco.com/en/US/products/ps9892/index.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 username to authenticate to the Media Experience Engine 3500 server.	The username 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

Cisco Show and Share is a product provided by Cisco. 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 <i>Cisco TelePresence Content Server and Show and Share Integration Guide</i> 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.
Call options		

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

Field	Field Description	Usage Guidelines
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 <i>Manual</i> .	Manual gatekeeper discovery means that the Content Server registers with one specific gatekeeper, identified by its IP address or fully qualified domain name.
Gatekeeper address	The IP address or DNS name of the gatekeeper.	—
H.323 ID	Other systems can call the Content Server using the H.323 ID if the Content Server is registered to the gatekeeper.	If the Content Server is in a cluster, its H.323 ID is not set here but in the Server Overview page.
E.164 alias	Other systems can call the Content Server using the E.164 alias if the Content Server is registered to the gatekeeper.	If the Content Server is in a cluster, its E.164 alias is not set here but in the Server Overview page.
Registration status	Choose to register the Content Server as a <i>Terminal</i> or as a <i>Gateway</i> .	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 <i>H.323 ID</i> 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 <i>Auto</i> and supply the username and password to be used by the Content Server.
User name	The username to authenticate to the gatekeeper.	—

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 <i>TCP</i> (Transmission Control Protocol). <i>UDP</i> (User Datagram Protocol) can also be used.	—
User name	The username to authenticate to the SIP registrar.	—
Password	The password to authenticate to the SIP registrar.	—
Password confirm		—

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 <i>Domain</i> or <i>LDAP</i> authentication, expand the LDAP server section and enter the details of a Microsoft Active Directory server. To enter details for more than one LDAP server, click Add LDAP server. Currently, only Microsoft Active Directory Server is supported. Clicking Save checks the LDAP server settings because the Content Server attempts to bind to the LDAP server. Changes to this page are not saved if the LDAP server settings are incorrect.	There are three modes of authentication (for more information, see Groups and Users): • <i>Local</i>: Only users with valid local accounts added through the Groups and Users page can log in. Local groups are not supported. • <i>Domain</i>: Users with domain accounts and local users are able to log in. The local administrator account can be used to configure the Content Server, or other local or domain users can be given a site manager role. Domain authentication can only be used if the Content Server has been added to a domain. If you add the Content Server to an existing domain, you need to define a separate security policy for the Content Server. If you do not define a separate security policy, the existing security policies might prevent the Content Server from functioning correctly. The recommended authentication mode for a cluster is domain authentication. • <i>LDAP</i>: LDAP authentication does not require the Content Server to be added to a domain. Before changing authentication from <i>Local</i> to <i>LDAP</i>, the site manager must add at least one LDAP user with the site manager role to the Content Server. To add a site manager, go to Configuration > Groups and users and click Add groups or users. Enter at least one valid username in the site manager role. Under LDAP authentication, local users cannot log in using the standard login method. However, the local administrator can log in by adding <code>#page:login&rescue:true</code> to the end of the Content Server URL in the browser.
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 <i>Base DN</i>.
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. 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 <i>@company.com</i> .	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 <i>admin</i> .	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.

- 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**.

**Note**

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

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.

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 3-83 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.
-

