



Cisco TelePresence Content Server Release 5.2 Release Notes

Revised April 18, 2012

Contents

- [Introduction, page 1](#)
- [New Features and Functionality in 5.2, page 2](#)
- [Content Server and Cisco Show and Share Compatibility Matrix, page 5](#)
- [Resolved Caveats, page 5](#)
- [Open Caveats, page 8](#)
- [Upgrading to 5.2, page 9](#)
- [Checking for Updates and Getting Help, page 11](#)
- [Documentation Updates, page 12](#)
- [Related Documentation, page 12](#)
- [Obtaining Documentation and Submitting a Service Request, page 12](#)
- [Getting Information About Accessibility and Cisco Products, page 12](#)

Introduction

These release notes describe the changes and improvements included in the Cisco TelePresence Content Server (Content Server) software version 5.2.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Features and Functionality in 5.2

This release includes the following new features and functionality:

- [Integration with the Cisco Media Experience Engine 3500, page 2](#)
- [Automated creation of personal recording aliases, page 2](#)
- [Improved lookup for access control lists, page 3](#)
- [Ad-hoc recording of a PIN protected MCU conference, page 3](#)
- [Support for a static URL for live streaming of MPEG-4 for Flash content from a Wowza Media Server, page 4](#)
- [PIN protection for watching a recording using a videoconference endpoint, page 4](#)

Integration with the Cisco Media Experience Engine 3500

You can now make a recording with the Content Server and upload it automatically to a Cisco Media Experience Engine 3500 server for further transformation and publishing. The recording will be copied to Media Experience Engine 3500 using FTP on completion of a call and then transformed based on the profile selected in the server configuration.

To enable seamless integration with a Cisco Media Experience Engine 3500 server, a Site Manager needs to set up a media server configuration first. Navigate to **Management > Recording setup > Media server configurations**. Add a Media Experience Engine 3500 Server Configuration and fill out the required FTP and API settings fields. Click the **Get job profiles** button to retrieve a list of spaces and profiles from the Media Experience Engine 3500 server; then, choose the profile space and profile that you want to use.

After saving your Media Experience Engine 3500 server configuration, you can add it to a template.

New Recordings:

To automatically get all your recordings transformed by Cisco Media Experience Engine 3500, you need to use a recording alias with a template that has a distribution output using your Cisco Media Experience Engine 3500 server configuration.

Existing recordings:

Alternatively, to transform an existing recording with Cisco Media Experience Engine 3500, perform the following steps. Navigate to **Manage outputs** for the recording. Select **Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U**. Select **Media Experience Engine 3500** and choose the media server configuration for the Media Experience Engine 3500 server that you want to use.

Automated creation of personal recording aliases

A personal recording alias can now be automatically created for each user with Creator privileges when the user logs in to the Content Server web interface.



Note

This feature is supported only for Content Servers that are registered to an H.323 gatekeeper as gateway.

To enable this feature, a Site Manager needs to select the **Automatically create personal recording aliases for creators** checkbox in Site Settings.

The selected system recording alias settings (with the exception of name, owner, H.323 ID, E.164 alias, SIP URI, SIP display name and email address) will be copied to all newly created personal recording aliases. The name of the newly created alias 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.



Note If a user's user name contains any characters other than alphanumeric characters, dots, hyphens, @ or brackets, this user's automatically generated recording alias will have a blank H.323 ID.

The email address suffix needs to be entered in the form @company.com. Newly created personal recording aliases will use the Creator's user name with this suffix appended at the end to create the email address.

Personal recording aliases can also be created in a bulk operation by using the Content Server's API. AddRecordingAlias and DeleteRecordingAlias functions were added, and ModifyRecordingAlias and GetRecordingAlias functions were made much more complete. Please refer to the [Cisco TelePresence Content Server API Guide](#) for details.

Improved lookup for access control lists

Editors can now add Active Directory users and groups to access control lists for their recordings if those users or groups exist on the LDAP server configured for the Content Server even if users have not logged in to the Content Server and user or group accounts have not yet been added via the Groups and Users page by a Site Manager.

This feature is supported for Content Servers using Domain or LDAP authentication, which have a valid LDAP server configuration in Site Settings.



Note If Guest access is turned on in Site Settings, users and members of groups added to access lists will not be able to log in to the Content Server. A Site Manager needs to add them manually via the Content Server Groups and Users page. Once logged in, they will have access to recordings that Creators have given them access to.

Ad-hoc recording of a PIN protected MCU conference

You can now dial out from the Content Server user interface to make an ad-hoc recording of a PIN protected MCU conference.

Enter the MCU conference number in the Dial number field of the Create Recording page and the numeric PIN in the PIN for MCU conference field. Then, click **Place call**. As the Content Server joins the MCU conference, you will see a message or recording poster confirming the Content Server has joined a password protected MCU conference on an endpoint that has also joined the call.

If you enter an incorrect PIN, the call will not hang up, but you will not see the recording poster or message. The Content Server will be left in the PIN-entry lobby unable to join the conference. You should hang up the call and try again, ensuring you enter the correct PIN.

Support for a static URL for live streaming of MPEG-4 for Flash content from a Wowza Media Server

By default, the stream name for live MPEG-4 for Flash streaming off Wowza Media Server is generated by the Content Server. If the live stream URL needs to be published before streaming starts, Site Managers can now enter a stream name in the Static stream name field on the **Media server configuration: Wowza Media Server for Flash > Live unicast streaming** settings page. The resulting URL is generated and displayed on the page, for example: *rtmp://myWowza/live/mp4:mystream*.

PIN protection for watching a recording using a videoconference endpoint

You can now PIN-protect recordings that are available for watching using a videoconference endpoint.

To add a PIN for all new recordings created with a recording alias, edit your recording alias and enter a PIN in the PIN (optional) field in the Play recording on endpoints section. The PIN must be numeric only and 4 digits long. To PIN protect a single recording, enter a PIN in the Play recording on endpoints section of the Edit recording page and save.

When you dial the playback number of a PIN-protected recording from an endpoint, you will see a visual prompt to enter a PIN using the endpoint remote (or a DTMF keypad when using Movi).

Placeholder dots will indicate how many digits have been entered. When the PIN has been entered successfully, the recording will start playing back immediately.



If the PIN has been entered incorrectly, you will be presented with feedback screen and prompted to re-enter the PIN.



The call will disconnect after three unsuccessful attempts or 30 seconds of inactivity.

Content Server and Cisco Show and Share Compatibility Matrix

Table 1 lists compatible Content Server and Cisco Show and Share versions.

Table 1 *Content Server and Show and Share Compatibility*

Software version	Show and Share 5.2.1 ¹	Show and Share 5.2.2	Show and Share 5.2.3
Content Server 5.0	Y	Y	N
Content Server 5.1	Y	Y	Y
Content Server 5.2	N	N	Y

1. Content Server recordings with Joined and stacked layouts will not be scaled correctly in the Show and Share Release 5.2.1 media player.

Resolved Caveats

The following issues were found in earlier releases and resolved in 5.2.

API

Reference ID	Summary
87357	Added DefaultRecordingAliasID to configuration.xml to expose the default recording alias.

Interoperability

Reference ID	Summary
85587	Fixed an issue where the H.239 content channel would never close when in a call with Polycom MGC-25.

Localization and Internationalization

Reference ID	Summary
72261	Fixed an issue where it was not possible to add a group with special characters \,*,(or) in the name.
85505	Removed a warning message in the Helper log when a custom language pack directory was missing.

Reference ID	Summary
88800	Corrected the wrapping of the Email link in Japanese and French on the View recording page.
89387	Fixed an issue where the Select language link did not appear on the login page if the preferred language in Site Settings was not set to English.

System

Reference ID	Summary
84959	The Transcode Engine no longer decodes video for audio only outputs, which reduces the time taken to transcode audio only outputs.
85205	When playing back two recordings joined by the Content Editor on a videoconference endpoint, the correct duration is now displayed when playback is paused.
85323	Corrected an issue where the first two seconds of media were missing from recordings made in firewall traversal calls.
87067	Corrected an issue where trying to edit a user's bandwidth settings changed the logged in Site Manager's bandwidth preferences.
87998	Improved the randomization of recording filenames.
88939	Corrected an issue where a failed transcoding process could cause the offline transcoding engine to get stuck and never move on to the next job.
117121	Administrators setting up the Content Server through the serial interface will now be prompted to change the password from default. The serial port menu will not be available until a new password has been set.
117790, 117791	Resolved an issue where the external management feedback mechanism could block the Content Engine process due to a large delay while attempting to contact an invalid external management system address.
117815	Corrected an issue where the Content Server would not handle a default VCS registration expiry time of 45 seconds.
117952	Due to a 45-character tag limit in Show and Share, keywords sent to a Show and Share media server as part of the distributed media upload are now being truncated at the last space, comma or a semi-colon prior to the 45 character limit. If no delimiters are found, the keyword field will be truncated to 45 characters.
118697	Corrected an issue where calls originating from CUCM registered endpoints to the Content Server would fail due to a problem with matching the incoming SIP URI (containing the IP address of the VCS as the domain name) to the SIP alias on the Content Server.
118749	Resolved a cross site scripting vulnerability in php parameters.
118750	Resolved an issue with directory traversal in file download functionality.

Upgrades and repairs

Reference ID	Summary
114534	<p>Corrected an issue where during an upgrade the installer was reporting that permissions were set incorrectly on media folders (“Full Control” instead of “Write, Delete and Read”) and attempted to repair them, which significantly increased the upgrade time, particularly for clusters.</p> <p>The following changes were made in version 5.2:</p> <ul style="list-style-type: none"> • The installer will now check for “Full Control” when checking permissions. • In upgrade mode, it will report potentially incorrect permissions on media folder directories and print information to the Setup Utility log but will not attempt to configure permissions. • In repair mode, it will report potentially incorrect permissions on media folder directories and print information to the Setup Utility log, as well as attempt to set the correct permissions.
115130	<p>It is now possible to upgrade other Content Servers in cluster if the Content Server that has already been upgraded gets into a call. It is not possible to repair other Content Servers if one of the Content Servers in a cluster gets into a call.</p>

User interface

Reference ID	Summary
54736	Added a confirm dialog to warn users if they are about to delete a category which is used by recordings or recording aliases.
84875	Fixed an issue where the first index in the Flash Player was not clickable.
85508	The Content Editor options dialog on a Mac will now show an informational message that the recording has no available outputs for the Content Editor for recordings which have only Windows Media outputs.
85935	Corrected an issue where an alternate live URL entered in the live unicast streaming settings of a Windows Media server was used for live multicast streaming if a user selected live multicast streaming.
86007	Fixed an issue where clicking on the Flash player while playing an audio only recording did not toggle play and pause.
86008	Corrected an issue with Flash Player where the seek bar was not updated when a user clicked on an index while in paused state.
86461	A link to download the missing Flash plug-in is now displayed when users try to view a Flash recording in Internet Explorer and the Flash plug-in has not been installed.
87774	Double-clicking on a recording in Flash player now toggles full screen.
87825	Fixed an issue where progressive download recordings in Flash player would sometimes not resume after the recording was paused.

Reference ID	Summary
88165	Corrected an issue where pausing a recording streamed off Wowza for Flash media server for the duration of the recording would result in displaying the start play screen in Flash player as if the recording has ended.
89010	Clicking Save on a recording alias page now displays an informational message if a user or group have not been found in LDAP or local users and groups and have been removed from the access list.
114535	Removed the 'unsupported browser' error message from the interface (page header and legacy media player) when users try to access the Content Server using an unsupported browser.
115996	Fixed an issue where recordings with a start time more than 23 days in the future would not be displayed in the interface.

Video

Reference ID	Summary
81657	Corrected an issue where dual video stream was never played back on a videoconference endpoint if H.263 video codec was turned off on the endpoint and the endpoint was not capable of receiving presentation over H.264.
88642	Corrected an issue where, while playing back a joined recording on a videoconference endpoint, pausing during the first recording might result in starting the second recording starting playback earlier than the edited in point.
88643	Reduced the length of the pause between two joined recordings when playing it back on a videoconference endpoint where the edited out point for the first recording is near the beginning of a large file.
87784	Corrected an issue with poor audio playback experience for users watching Content Server recordings from a Movi client.
116064	Corrected an issue where an endpoint might not display the countdown and recording screen if the Content Server could not match its resolution.

Open Caveats

The following issues currently apply to this version of Content Server.

Reference ID	Summary
—	The Content Server supports only Microsoft Active Directory Server for LDAP and Domain authentication.
—	When configuring LDAP servers in the Authentication section of the Site Settings page, the Content Server cannot accept the root of an Active Directory domain as the base DN. Instead, you must specify an object that resides inside the root. A common root-level object is 'OU=users.' If your users and groups are distributed between multiple root-level objects, specify each of them in separate LDAP servers.

Reference ID	Summary
56699	Internet Explorer security settings may prevent users from accessing the Windows Server administration interface with IE7 or IE8 on Windows XP (Server Pack 3) even if the Content Server has been added to trusted sites in the browser.
63782	It is not possible to register more than 25 SIP aliases on the Content Server.
77297, 77298	QuickTime plug-in v.7.6.6 or higher causes the following issues when playing back MPEG-4 for QuickTime in the viewer: no video displayed in IE/Firefox on PC and Safari/Firefox on Mac when live streaming and garbled audio when viewing on demand with Firefox/IE on a PC. Content Server users are advised not to upgrade their QuickTime plug-in to version 7.6.6 or higher.
81835	When the camera is turned off while reviewing recordings from a E20 endpoint, the review overlay will be missing, and a 'No incoming video' error message will be displayed.
81954	Live Windows Media multicast streams will not be displayed in the Silverlight player in Firefox 3.6.x on a PC.
82218	When HTTPS is used to view Content Server pages, users will not be able to view content in Silverlight and Flash players.
83035	Progressive download of MPEG-4 for Flash recordings from the Local IIS Web Server will not work in IE7 if the file size of the MPEG-4 for Flash output exceeds 2 GB (KB 298618).
84626	Areas of green pixels might be displayed when starting playback and seeking in a Flash video streaming from a Wowza streaming server on some computers. The workaround is to update video drivers and/or turn off hardware acceleration. Visit the Adobe web site to view minimum hardware requirements for SD and HD video playback and video hardware acceleration support: http://www.adobe.com/products/flashplayer/systemreqs/#video
114984	Using the Dial API and assigning the bit rate value to be a non-numeric character allows the call to connect at 128 kbps.

Upgrading to 5.2



Caution

Content Server 5.2 software is only available for second generation Content Server hardware.

Prerequisites and Software Dependencies

Content Server 5.2 software cannot be installed on first generation Content Server hardware. If you attempt to run the 5.2 installer it will fail.

How to tell which Content Server hardware you have:

Figure 1 shows images of the two generations of Content Server hardware referred to in this document.

Figure 1 **Content Server Hardware Editions**

The 5.2 installer will upgrade your Content Server from 5.0 or 5.1 versions only. If your Content Server is at an earlier version, you will need to upgrade to 5.0 first before running the 5.2 installer.

A release key is not required for upgrading to 5.2

**Caution**

You **must** back up your Content Server and turn off anti-virus applications before upgrading. You will need a full backup for restoring to the previous version or in the unlikely event of an upgrade failure. Follow the instructions for backing up and restoring the Content Server in the online help.

**Caution**

If you have installed the Feature Pack for Microsoft SQL Server 2005 or any of its components (which is NOT supported for the Cisco TelePresence Content Server), you must remove the following components prior to upgrading, otherwise the upgrade may fail.

Unsupported components which **MUST** be removed prior to upgrading:


Microsoft SQL Server 2005 Analysis Services 9.0 OLE DB Provider, Microsoft SQL Server 2005 Backward Compatibility Components, Microsoft SQL Server 2005 Command Line Query Utility, Microsoft SQL Server 2005 Data Mining Viewer Controls, Microsoft SQL Server 2005 JDBC Driver, Microsoft SQL Server 2005 Management Objects Collection, Microsoft SQL Server 2005 Compact Edition, Microsoft SQL Server 2005 Notification Services Client Components, Microsoft SQL Server 2005 Upgrade Advisor, Microsoft SQL Server 2005 Reporting Services Add-in for Microsoft SharePoint Technologies, Microsoft SQL Server 2005 Data Mining Add-ins for Microsoft Office 2007.

Upgrade Instructions

The approximate duration of an upgrade is 10–20 minutes.

To upgrade your Content Server to 5.2, do the following:

- Step 1** Log in to the Content Server using Windows Remote Desktop Connection or through the local console.
- Step 2** Transfer the installer and the MD5 file that you downloaded to the Content Server (do not run the installer from a mapped or network drive).
- Step 3** Verify the MD5 hash (checksum) of the installer using the provided MD5 file. Cisco recommends that you verify that the installer has not become corrupted as a result of file transfer, disk error or tampering. Any MD5 program can be used for verifying the installer integrity using the provided MD5 file. You need to follow instructions for the MD5 program you are using.
- Step 4** If the installer passed the MD5 verification, run the installer by double-clicking on it.

- Step 5** Click **Next** when the Next button is available and Install Shield Wizard is ready to begin installation.
- Step 6** At the Content Server prerequisites prompt you need to select the backup option that applies to your Content Server:
- If you select *The Content Server is backed up*, click **Next** to proceed with the installation.
 - If you select *The Content Server is not backed up*, clicking **Next** will display a warning that in case of installation failure there may be no way to recover your data. You may cancel the installation at this point, take a backup of your Content Server and then run the installer again. You may also choose to ignore the warning and proceed with the installation, although this is not recommended.
- Step 7** At the second Content Server prerequisites prompt you need to select the antivirus option that applies to your Content Server:
- If you select *There is no antivirus software installed*, or *The antivirus software is stopped*, click **Next** to proceed with the installation.
 - If you select *The antivirus software is still running*, clicking **Next** will display a warning that this might cause your installation to fail. You may cancel the installation at this point, stop the antivirus software and then run the installer again. You may also choose to ignore the warning and proceed with the installation, although this is not recommended.
- Step 8** At the *Are you sure you wish to continue?* prompt, click **Yes** if you wish to proceed with the upgrade, or **No** if you want to cancel the upgrade.
-
-  **Caution** You must not cancel or interrupt the upgrade process after this point. If you want to revert to the previous version after completing the upgrade to 5.2, you will need to follow the instructions for restoring from backup available in online help.
-
- Step 9** After the installer has configured the Content Server, it will display a message that the upgrade has completed successfully. The installation logs are available in the following locations: **E:\logs\Install** and **E:\logs\SetupUtility**.
-

Checking for Updates and Getting Help

Cisco recommends registering your product at <http://www.tandberg.com/services/video-conferencing-product-registration.jsp> in order to receive notifications about the latest software and security updates. New feature and maintenance releases are published regularly, and we recommend that your Content Server software is always kept up to date.

If you experience any problems when configuring or using your Cisco TelePresence Content Server, consult the online help (available within the UI) for an explanation of how its individual features and settings work. If you cannot find the answer you need, check on the web site at <http://www.tandberg.com/support> to make sure that your product is running the most up-to-date software and for further relevant documentation.

You or your reseller can get help from our support team by raising a case at <http://www.tandberg.com/support/video-conferencing-online-support.jsp>. Make sure you have the following information ready:

- The serial number and product model number of the unit
- The software build number which can be found on the product user interface
- Your contact email address or telephone number

Documentation Updates

This section provides documentation updates for documents available at:

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

Updates to the Administration and User Guide and Online Help

Adding and Editing Call Configurations

The solution supports media encryption only for the H.323 protocol.

Related Documentation

For more information about the Cisco TelePresence Content Server, see these documents:

- *Cisco TelePresence Content Server Release 5.2 Administration and User Guide*
- *Configuring the Cisco TelePresence Content Server for Streaming from a QuickTime Media Server*
- *Configuring the Cisco TelePresence Content Server for Streaming Flash from a Wowza Media Server*
- *Cisco TCS Integration to Cisco Show and Share for Live WMV Streaming*
- *Cisco TelePresence Content Server API Guide*
- *Video on Demand Integration for Cisco TCS to Cisco Show and Share*

All documents are located here:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Getting Information About Accessibility and Cisco Products

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

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

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

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

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

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

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

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

© 2011 Cisco Systems, Inc. All rights reserved.

