Cisco TelePresence Content Server Software Release 5.3 and Later Release Notes

Revised: February 7, 2014

These release notes describe the changes and improvements included in the Cisco TelePresence Content Server (Content Server) Software Release 5.3, 5.3.1, and 5.3.2 (Release 5.3.x).

Contents

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

New Hardware and Software Features

Release 5.3.2

Release 5.3.2 is a maintenance release and has no new features. To upgrade to Release 5.3.2, see Upgrading the Content Server Software.

Release 5.3.1

Release 5.3.1 has this new feature: "Optimize for motion" check box in the Content Server User Interface. See Updates to the Administration and User Guide Release 5.3.x for more information.

Release 5.3

Release 5.3 includes these new features and functionality:

Five Additional Recording Ports Option Key

This release introduces a new option key for the second generation Content Server hardware to expand the number of concurrent recorded calls to ten.

- Up to 10 concurrent on-demand recordings on a standalone Content Server.
- Up to 100 concurrent on-demand recordings on a cluster of 10 Content Servers. Mixed capacity Content Servers are allowed in a cluster.

Note The total number of concurrent review calls remains at five regardless of whether the Content Server is optioned for five or ten recording ports.

New Presentation Layout

The new presentation layout is an option for the Joined layout that guarantees a 16:9 aspect ratio media resolution for the resulting media. This new layout offers an event-style presentation layout that focuses on the presentation stream while maintaining a reasonably sized main video stream within a guaranteed 16:9 aspect ratio layout. You can use this layout for streaming from the Content Server web interface, for downloads, and for distribution to other systems.

Content Server Compatibility Matrix

Table 1 lists Cisco Show and Share software versions that are compatible with Content Server software.

Table 1 Cisco Show and Share and Content Server Software Compatibility

Software Version	Show and Share 5.2.1[1]	Show and Share 5.2.2	Show and Share 5.2.3	Show and Share 5.3 and 5.3 Patch 1
Content Server 5.0	Y	Y	N	N
Content Server 5.1	Y	Y	Y	N
Content Server 5.2	N	N	Y	Y
Content Server 5.3.x	N	N	Y	Y

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

Table 2 lists the Cisco MXE 3500 software versions that are compatible with Content Server software.

Table 2 Cisco MXE 3500 and Content Server Software Compatibility

Software Version	MXE 3.2	MXE 3.3
Content Server 5.0	N	N
Content Server 5.1	N	N
Content Server 5.2	Y	Y
Content Server 5.3.x	N	Y

Limitations and Restrictions

Cisco TelePresence Content Server Release 5.3.x does not support Cisco Video Streamer media server configuration capabilities. Although these capabilities are visible on the Content Server User Interface, the underlying infrastructure is currently unsupported.

Open Caveats

Table 3 Open Caveats in Content Server Release 5.3.x

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.

Table 3 Open Caveats in Content Server Release 5.3.x (continued)

Reference ID	Summary
—	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
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.
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.**
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.
CSCtt01659	When HTTPS is used to view Content Server pages, users will not be able to view content in Silverlight and Flash players.
CSCue78942	Content Server failed SIP registrations.
CSCuf56494	Content Server recordings using video + presentation from a TX9000 shows artifacts.
CSCuh76732	Content Server does not record a conference because no RTP is received.
CSCuj22680	Rarely lip sync seen in offline transcoded recordings.
CSCum47953	Grey bar at bottom observed while switching presentation in Content Server SIP Call.
CSCum47420	Grey Playback/Corruption observed with H323 call to/from Content Server.
CSCul89307	Incoming call to Content Server made from TMS/MCU shows garbage call duration value.
CSCuj19103	Windows server and Optimize for Motion are not translated by Language Packs.
CSCul80712	Recordings of lower version do not join when imported to higher version.
CSCul88955	Lip sync issue when two live calls are placed: One is Darwin and the other is WMS/Wowza.
CSCul52342	Content Server Content Engine Service does not restart with specific steps.
CSCul52364	MXE Profiles are accessible without MXE Credential.
CSCul55224	Recording link not being updated with Frontend address.
CSCuh49262	Content Server has an uploading limit of 2 GB.

Resolved Caveats

Resolved Caveats in Release 5.3.2

Table 4 Resolved Caveats in Content Server Release 5.3.2

Reference ID	Summary
CSCud35125	Image ghosting seen in the recording after presenting from Content Server unit.
CSCum04548	In a end to end SIP\H323 call, there is a partial audio loss in one call.
CSCul16401	Audio mixing on running two live streaming calls on Content Server.
CSCud12515	Content Server cannot save and verify front end address if using HTTPS.
CSCuf90480	Content Server needs password recovery procedures documented.

Resolved Caveats in Release 5.3.1

Table 5 Resolved Caveats in Content Server Release 5.3.1

Reference ID	Summary
CSCuf16163	The Content Server cannot perform a shutdown and reboot from the web User Interface (UI). The workaround is to assign shutdown permission to the domain user on the Content Server that you want to shut down and restart. Follow these steps: 1. With the client machine and the target machine both in the same domain, log in as the domain user to the Content Server UI that you want to shut down and restart. 2. Add *taskshutdown.exe* in the firewall exception of the target machine: a. Navigate to **Control Panel > Windows Firewall**. Click the Exception tab. b. Click **Add Program** and browse to *taskshutdown.exe* from C:\WINDOWS\system32\ServerAppliance\web\Admin\shutdown\support\taskshutdown.exe. 3. Assign shutdown permission to the domain user on the target machine that you want to shutdown and restart: a. Navigate to **Control Panel > Administrative Tools > Local Security Policy > Local Policies > User Rights Assignment**. Double click **<Shut Down the System>** and add the domain user in **<ADD User or Group>**. b. Navigate to **Control Panel > Administrative Tools > Local Security Policy > Local Policies > User Rights Assignment**. Double click **<Force Shut Down the Remote System>** and add the domain user in **<ADD User or Group>**.
CSCuh87539	Users cannot log in to Content Server with a < symbol in their password when using LDAP authentication.
CSCud12515	Content Server Version 5.3 cannot save and verify frontend address if using HTTPS.
CSCuf28109	Live recorded file fails to move from livedata folder to media folder.
CSCud03244	Jerkiness in video is observed in live streaming via a Wowza server.
CSCuf90026	Content Server video with Flash is jerky versus video with WMV which appears normal.
CSCui91596	Content Server drops running calls due to intermittent NAS failures.
CSCua36052	Content Server Version 5.3: OT engine crash when the H263 decoder starts.
CSCua69536	Selecting switched output for live results in Force 16:9 output instead.
CSCub00599	MPEG4 files greater than 4 GB cannot be played.
CSCub04304	Cisco Show and Share MP4 outputs should use keyframe spacing of 4 seconds.
CSCtz98025	Audio stops after various times during recording.
CSCud67695	Content Server sending wrong filename to Cisco MXE during failure conditions.

Table 5 Resolved Caveats in Content Server Release 5.3.1 (continued)

Reference ID	Summary
CSCud86695 CSCub39425	Cannot download recordings from Content Server if the file size is over 2GB; Content Server exporting limit.
CSCty05212 CSCud27370	Audio/video out of sync after ten minutes of a Content Server (mp4f) to Wowza to iPhone configuration; Lip sync observed while using external cameras.

Resolved Caveats in Release 5.3

Table 6 Resolved Caveats in Content Server Release 5.3

Reference ID	Summary
CSCts84156	The Content Server does not load bookmarked pages correctly.
121346	The cluster wizard should check for share permissions early and offer the user the option to opt out of fixing the share permissions instead of re-writing the permissions by default.
121345	The second and subsequent cluster members always checks permissions when running the wizard when updating the NAS location.
CSCts72011	Unable to add a new Content Server to cluster with same system name, H.323 id and E.164 as one that has been removed.
CSCtt01646	Content Server returns the last added recording aliases H.323 id in Q.931 display.
CSCtx47045	Video keeps playing past the edited out point in legacy Windows Media player.
CSCtv07795	Video is corrupt when recorded from Telepresence Server 4.2 (1.5).

Upgrading the Content Server Software

The 5.3.x installer will upgrade your Content Server only from Release 5.3. If your Content Server runs an earlier software version, you should first upgrade to 5.3 before running the Release 5.3.x installer. These are the supported software upgrade paths:

Release 5.2 > 5.3 > 5.3.1 (v5.3 Build 3486)

Release 5.2 > 5.3.x > 5.3.2 (v5.3 Build 5329)

To upgrade the Content Server software, see these sections:

- Guidelines and Prerequisites, page 7
- Software Upgrade Procedure, page 9

Guidelines and Prerequisites

Before you begin, observe these guidelines and prerequisites:

- You must have administrator privileges to perform a software upgrade.
- You should download Release 5.3.2 software from Cisco.com before you begin the upgrade procedure.

- A release key is not required for upgrading to Release 5.3.2.
- Release 5.3.x software cannot be installed on first-generation Content Server hardware. If you attempt to run the 5.3.x installer it will fail.

Caution **Content Server 5.3.x software is only available for second generation Content Server hardware.**

- You can use the Content Server serial number to identify the server hardware version. In the web UI go to **Management > Diagnostics > Server overview**. You can also check the serial number label on the top right front of the Content Server. These are the device serial number formats:
  - First-generation serial number: **49A0***xxxx*
  - Second-generation serial number: **49A2***xxxx*

  Figure 1 shows the first- and second-generation Content Server hardware.

Figure 1 Content Server Hardware Editions

First Generation	Second Generation
	

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 and the *Cisco TelePresence Content Server Administration and User Guide* on Cisco.com.

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 components prior to upgrading or the upgrade may fail.

These unsupported components 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.

Software Upgrade Procedure

The approximate duration of an upgrade is 10 to 20 minutes. Follow these steps:

Step 1 Log in to the Content Server as the administrator by using Windows Remote Desktop Connection or through the local console.

Step 2 Transfer the installer and the MD5 file that you downloaded from Cisco.com 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 by using the provided MD5 file. We recommend verifying that the installer is not corrupted due to file transfer, disk error, or tampering. You can use any MD5 program to verify the installer integrity.

Step 4 When the installer passes the MD5 verification, double-click the installer to run the installation wizard.

Step 5 Click **Next** when the Next button is available. The InstallShield Wizard is ready to begin installation.

Step 6 At the Content Server prerequisites prompt, 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** displays a warning that in case of installation failure there may be no way to recover your data. You can cancel the installation at this point, take a backup of your Content Server, and then run the installer again. You can 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, 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** displays a warning that this might cause your installation to fail. You can cancel the installation at this point, stop the antivirus software, and then run the installer again. You can 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** to proceed with the upgrade. Click **No** if you want to cancel the upgrade.

Caution You must not cancel or interrupt the upgrade process after the upgrade begins. If you want to revert to the previous version after completing the upgrade to 5.3.1, follow the instructions in the online help for restoring from backup.

Step 9 After the installer has configured the Content Server, it displays a message that the upgrade has completed successfully.

The installation logs are available in the following locations: **E:\logs\Install** and **E:\logs\SetupUtility**.

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 Release 5.3.x

Recording Download Timeout Increased

The timeout for downloading a recording to the Content Server was increased from a maximum of 20 minutes to maximum of 60 minutes to avoid large-file download failures.

Adding and Editing Call Configurations

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

Windows Media Streaming Server

Live Windows Media multicast streams can be viewed only on Windows computers.

Optimize for motion check box

There is a new “Optimize for motion” check box in the Content Server web user interface (UI). You can use the check box to optimize the quality of high-motion recordings. The option appears in these UI screens:

- **Recordings > Edit recordings: Manage outputs** in the On demand media server configuration settings screen.
- **Recording Setup > Templates: Add or Edit Template** in the On demand media server configuration settings screen.

Supported Platforms, Browsers, and Plug-ins

Table 7 describes the supported platforms, browsers, and plug-ins for Release 5.3.1 software.

Table 7 Supported Platforms, Browsers, and Plug-ins for Release 5.3.1 Software

Operating System	Browsers	Silverlight	Flash	Windows Media Player	QuickTime
Windows	Mozilla Firefox 3.6.x and 21	5.1	11.7	12.0	7.6.6
	Internet Explorer 8	5.1	11.7	12.0	7.6.6
Mac version 10.5 or higher	Mozilla Firefox 3.6.x and 21	5.1	11.7	Not supported	7.6.6
	Safari 6	5.1	11.7	Not supported	7.6.6

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

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

Other required Mozilla Firefox plug-ins:

- Silverlight plug-in 5.1.20125.0
- Shockwave Flash 11.7 r700
- QuickTime plug-in 7.7.3.0

Firefox 21 also requires Shockwave for Director version 12.0.2.122

Updates to the Online Help

Adding and Editing Call Configurations

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

Cisco Video Streamer Server

Note Cisco TelePresence Content Server Release 5.3.x does not support the Cisco Video Streamer media server configuration capabilities.

The following features and functionality that are documented in the Content Server online help for the Cisco Video Streamer are not supported:

- **Recording setup > Media server configuration > Cisco Video Streamer.**
- **Configuration > Site settings > System defaults > MPEG-4 for Flash**—Cisco Video Streamer media server configuration.
- Supported Platforms, Browsers, and Plug-ins—Cisco Video Streamer default Flash player for MPEG-4 for Flash.
- Content Editor—Editing functionality for content hosted on the Cisco Video Streamer.
- Port Information—Ports used in the default setup for communication between the Content Server and Cisco Video Streamer.

Troubleshooting and Technical Support

Cisco recommends registering your product at http://www.cisco.com/cisco/support/notifications.html 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.

Using the server logs to help solve a problem

You can use the server logs to produce debugging information to assist customer support in solving issues. From the **Management** tab, go to **Diagnostics > Server logs** to access the Content Server logs.

Getting more help

If you experience any problems when configuring or using the Content Server, consult the online help for an explanation of how individual features and settings work. Also, see the *Cisco TelePresence Content Server Administration and User Guide* for this release on Cisco.com.

When contacting Cisco for support, make sure that you have this information:

- The serial number and product model number of the server
- The software build number, which can be found on the product user interface
- Your contact email address or telephone number
- A full description of the problem

Related Documentation

- Cisco TelePresence Content Server Documentation

  http://www.cisco.com/en/US/products/ps11347/tsd_products_support_series_home.html
- Cisco Capture Transform Share Documentation

  http://www.cisco.com/en/US/products/ps12130/products_installation_and_configuration_guides_list.html

Information About Accessibility and Cisco Products

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.