



Release Notes for Cisco TelePresence Recording Server, Release 1.7

Created: September 2010
Updated: August 2, 2011

Contents

- [Introduction, page 1](#)
- [Cisco TelePresence Software Compatibility Matrix, page 2](#)
- [Documentation Errata, page 2](#)
- [New and Changed Information in CTRS Release 1.7.3, page 3](#)
- [New and Changed Information in CTRS Release 1.7.2, page 5](#)
- [New and Changed Information in CTRS Release 1.7.1, page 6](#)
- [New and Changed Information in CTRS Release 1.7.0, page 7](#)
- [Caveats for CTRS Release 1.7.x, page 9](#)
- [New and Changed Information in CTRS Release 1.6.3, page 12](#)
- [New and Changed Information in CTRS Release 1.6.2, page 12](#)
- [New and Changed Information in CTRS Release 1.6.1, page 13](#)
- [Caveats for CTRS Release 1.6.x, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)

Introduction

The Cisco TelePresence Recording Server (CTRS) allows users to do the following:

- Create recordings.
- Store recordings on the CTRS.



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

- Share recordings with others for viewing.
- Make recordings public so that anyone with access to the CTRS can view them.
- Play back recordings on a TelePresence endpoint.
- Play back recordings with a standard browser-based player.
- Download your recordings or public recordings.

CTRS enables users to record in TelePresence Studio Mode. In Studio Mode, users can create team announcements, corporate messages, training modules, video blogs, and other similar recordings.

To record, users must have access to a CTS with CTRS functionality; they control recording through the CTS IP phone interface.

The recordings can be either HD video and audio, or Common Intermediate Format (CIF). All recorded content, including materials that users choose to display on a device that is connected to the VGA input or through a document camera, is shown on the TelePresence monitor from the viewer's perspective. CTRS acts as a viewer endpoint in a TelePresence session and records what it sees.

Users can then share a recording by sending it to a recipient's e-mail address. To play a recording, the recipient must sign in to the CTRS browser-based end-user portal with a corporate username and password (LDAP username and password). If the recipient wants to play a recording on a TelePresence display, he or she must sign in to CTRS through the CTS IP phone user interface with a corporate username and personal identification number (PIN).

The CTRS requires an administrative user, who manages CTRS configuration and maintenance.

Cisco TelePresence Software Compatibility Matrix

For Cisco TelePresence software compatibility information, refer to the information located at the following URL:

http://www.cisco.com/en/US/products/ps8332/products_device_support_tables_list.html

Software Releases and Component Firmware Versions

For the current recommended set of software releases and component firmware versions for the Cisco TelePresence solution, see the information located at the following URL:

http://www.cisco.com/en/US/partner/docs/telepresence/cts_admin/1_7/release/notes/cts_1_7_release_notes.html#wp42142

Documentation Errata

Cisco Show and Share Version

The *Cisco TelePresence Recording Server 1.7 Administration Guide* inadvertently omitted the CTRS versions that are compatible with the Cisco Show and Share software versions. [Table 1](#) provides compatibility information for the CTRS and Cisco Show and Share.

Table 1 CTRS and Cisco Show and Share Version Compatibility

CTRS Versions	Cisco Show and Share Versions
1.7.0 through 1.7.2	5.2.2 and earlier
1.7.3	5.2.2, 5.2.3

Replacing a Hard Disk Drive

This section describes how to replace a hard disk drive in a Cisco MCS-7845-Ix server on which CTRS software is running.



Caution

We do not recommend replacing a hard disk drive while the CTRS is powered on, a process known as hot swapping. Hot swapping a hard disk drive can result in configuration data loss as well as loss of stored videos.

-
- Step 1** Perform a backup of the CTRS configuration data only.
- A backup of the CTRS configuration data may be needed if the scenario described in step 6 occurs. If this scenario occurs, the CTRS configuration data cannot be restored from a backup of the full system data, so make sure to perform a backup of the CTRS configuration data only.
- Step 2** Export the media files (videos) to an archive server.
- Step 3** Power down the CTRS.
- Step 4** Replace the hard disk drive.
- Step 5** Power on the CTRS.
- Step 6** If the CTRS is unresponsive, you must re-install the CTRS software.
- For complete information on how to install the software, see the *Cisco TelePresence Recording Server Administration Guide* at this location:
http://www.cisco.com/en/US/products/ps10341/prod_maintenance_guides_list.html
- Step 7** Restore the configuration data.
- Step 8** Import the archived media files to the CTRS.
-

New and Changed Information in CTRS Release 1.7.3

New Field in Cisco Show and Share Page

The API Version field is now available in the Cisco Show and Share page as shown in [Figure 1](#). This field specifies the Cisco Show and Share version running on your server.

Figure 1 Cisco Show and Share Page—API Version Field

System Configuration > Cisco Show and Share as of 12:04:12

CTRS connected to Show and Share tsbu-dt-yv-ss194

Connection Settings

✦ Hostname:

✦ Username:

✦ Password:

Enabled: Yes No

You may contact the Show and Share administrator to create an account.

Preferences

Users will always receive an email if their video does not upload.

Send users an email when their video is successfully uploaded.

Yes No

API Settings

DMM User Name LDAP Attribute:

API Version (same as Show and Share Version):

2109602

For a CTRS running version 1.7.0 through 1.7.2, Cisco Show and Share versions 5.2.2 and earlier are supported. For a CTRS running version 1.7.3, Cisco Show and Share versions 5.2.2 and 5.2.3 are supported.

The default setting of this field is version 5.2.2.

If the Cisco Show and Share server that is connected to the CTRS is running a version other than 5.2.2, you must check the setting of this field and update it as needed.

End-user Portal Tab Enhancements

In CTRS release 1.7.2 and earlier, you could sort Cisco TelePresence Video Portal users in the Configure > Access Management page, End-user Portal tab, by email address only. Starting with CTRS release 1.7.3, you can sort users by their first and last names as well.

Caveats

The following caveat was fixed in CTRS Release 1.7.3:

- CSCtq05603 —Video Portal users sorted by email addr loses order after page update

New and Changed Information in CTRS Release 1.7.2

New Field in Cisco Show and Share Page

The DMM Login User Name Attribute field is now available in the Cisco Show and Share page as shown in [Figure 2](#).

Figure 2 Cisco Show and Share Page—DMM User Name LDAP Attribute Field

The screenshot shows the 'System Configuration > Cisco Show and Share' page. At the top right, it says 'as of 09:18:59'. Below the breadcrumb is a green checkmark icon and the text 'CTRS connected to Show and Share tsbu-dt-yv-ss194'. The main configuration area is divided into three sections: 'Connection Settings', 'Preferences', and 'API Settings'. In the 'Connection Settings' section, there are fields for 'Hostname' (tsbu-dt-yv-ss194), 'Username' (superuser), and 'Password' (masked with dots). Below these is an 'Enabled' section with radio buttons for 'Yes' (selected) and 'No'. A note says 'You may contact the Show and Share administrator to create an account.' with a 'Test Connection' button. The 'Preferences' section has two lines of text: 'Users will always receive an email if their video does not upload.' and 'Send users an email when their video is successfully uploaded.' with radio buttons for 'Yes' (selected) and 'No'. The 'API Settings' section has a field for 'DMM User Name LDAP Attribute' with the value 'sAMAccountName'. At the bottom left are 'Apply' and 'Reset' buttons. On the right edge of the screenshot, the number '209294' is visible vertically.

This field maps to the LDAP attribute specified in the Login User Name field of the Digital Media Manager (DMM), which manages Cisco Show and Share. This mapping ensures that the CTRS associates the correct username to a video while it is being uploaded to the Cisco Show and Share server. If the username is incorrect, the video will not be saved to the correct user account on the Cisco Show and Share server.

The default setting of this field is sAMAccountName, which should work for most organizations.

You need to change the default setting if your organization does not use the values of the LDAP samAccountName attribute as the source for the Cisco Show and Share usernames. Instead, your organization might use the values of another LDAP attribute or have created a customized LDAP attribute.

If one of these scenarios applies to your organization, contact the Show and Share administrator to get the LDAP attribute specified in the Login User Name field of the DMM, then enter the attribute in the DMM Login User Name Attribute field of the Cisco Show and Share page in the CTRS Administrative UI.

Caveats

The following caveat was fixed in CTRS Release 1.7.2:

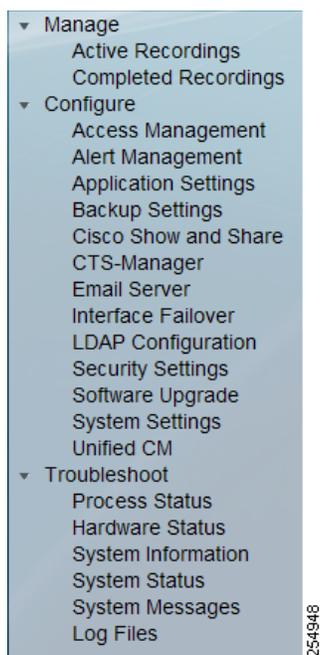
- CSCtn71601—After recording session, rec_audit.log file was not created

New and Changed Information in CTRS Release 1.7.1

Reorganization of Left Navigation in the CTRS Administrative User Interface

The contents of the left navigation in the CTRS administrative user interface have been reorganized as shown in [Figure 3](#).

Figure 3 *Reorganized Left Navigation Contents*



The contents were reorganized for the following reasons:

- To position the most commonly used links at the top of the navigation and the less commonly used links toward the bottom.
- To achieve consistency with the left navigations of other TelePresence administrative user interfaces, for example, the CTMS administrative user interface.

The CTRS 1.7.1 online help content reflects the new organization. However, the content of the *Cisco TelePresence Recording Server Administration Guide* will be reorganized during an upcoming release.

Caveats

The following caveats were fixed in CTRS Release 1.7.1:

- CSCtf01747—CTRS Admin Web UI: Log file filter not working properly
- CSCti29498—CTRS End-User Portal: refresh causes unexpected video deletion
- CSCti30916—No restore files after changing page or number of pages displayed
- CSCti46701—CTRS Admin UI in Firefox & Safari Browsers: diffs with UI in IE browser
- CSCtj09993—User portal displays error message if PIN begins with “0”
- CSCtj13018—CTRS user portal login with username with different case sensitivity
- CSCtj21452—Issue when playing back video recorded by 1.7 CTRS

New and Changed Information in CTRS Release 1.7.0

Support for Cisco Show and Share

If you use Cisco Show and Share for uploading, managing, sharing, and viewing video and audio content in your enterprise network, you can configure a connection between CTRS and your Cisco Show and Share server. You can then use Cisco Show and Share as a video portal for CTRS recordings.

For information about recording, viewing, and sharing CTRS recordings, see Chapter 7, “Creating and Viewing Recordings with the Cisco TelePresence Recording Server” in *Cisco TelePresence System User Guide, Release 1.7*.

Updates to the CTRS Administration Web Interface

The look and feel of the CTRS administration Web interface has been updated to match the look and feel of the CTRS Web user interface.

TIP Support

CTRS release 1.7 supports Telepresence Interoperability Protocol (TIP) version 6.0.

Differences between Enterprise and Commercial Express Versions of CTRS Release 1.7

The Cisco TelePresence Commercial Express product bundle is delivered as a single Cisco MCS server with one or more Cisco TelePresence application DVDs, license keys, and instructions to install the product, including the recommended VMware configuration. During installation, the common infrastructure component within the Cisco applications detects the VMware and identifies it as supported hardware.

Once you have VMware installed on your system, the basic procedure to install CTS-Manager, CTMS, and CTRS are the same. You can install the CTMS and CTRS in any order once you have installed, configured, and set up licensing for CTS-Manager.

The differences between the standard enterprise version of CTRS release 1.7 and the Commercial Express version are as follows:

- The Commercial Express version of CTRS does not create a redundant array of independent disks (RAID) for its media.
- The System Configuration > Application Settings page reflects Commercial Express license information.
- The Commercial Express license permits two simultaneous recording sessions (one to record and one to replay).
- The Commercial Express license permits a maximum of ten simultaneous user sessions on the browser-based video portal. If additional users (beyond the permitted ten) attempt to log in, they see this message: “Maximum number of users are logged in. Please wait and try again.”
- The Remember Me checkbox on the login page of the browser-based video portal is not available in the Commercial Express version.

Enhancements to the CTRS End-User Video Portal

In addition to various changes that enhance the end-user experience, CTRS release 1.7 includes three important changes to the end-user portal:

- In release 1.7, users can download HD and SD versions of recordings from the CTRS end-user video portal. If a recording includes a presentation, users can download the presentation.
- The CTRS end-user video portal sign-in screen includes a **Remember username** check box. If checked, when users close the browser window without signing out, they do not have to sign in again when they return to the portal.
- End users can share recordings both in e-mail and by uploading to Cisco Show and Share (if their enterprise uses the Cisco Show and Share video portal).

CTRS Full System Data Backup Across Releases

If you perform a full system data backup in CTRS release 1.6 and then upgrade to release 1.7, you cannot restore the full system data files from the backup in release 1.6.

After you upgrade from release 1.6 to 1.7, we recommend that you immediately perform a full system data backup.

Caveats

The following caveats were fixed in CTRS Release 1.7.0:

- CSCtc03471—Skip to the end during playback does not work correctly
- CSCtc77312—Session expiration timer is not reset as expected
- CSCtc88544—HTTP 500 error when server comes up after changing hostname from CLI
- CSCtc95412—Import does not import back the presentation file in a recording

- CSCtc99256—Import interface shows error after exporting
- CSCtd04989—Able to delete admin, but delete should be disabled for default admin user
- CSCtd14343—Phone UI freezes in Review page if pause and stop selected
- CSCtd17697—Playback “Unable to connect” message on phone UI while multiple recordings are starting
- CSCtd17702—Cannot import more than 20 recordings at a time with IE 6

Caveats for CTRS Release 1.7.x

This section includes the following information:

- [CTRS Release 1.7.x Caveat Reference, page 9](#)
- [Caveats for CTRS Release 1.7.0, page 9](#)

CTRS Release 1.7.x Caveat Reference

Table 2 summarizes caveats found in CTRS Release 1.7.x.

Table 2 CTRS Release 1.7.x Caveats and Caveats Corrected Reference

	Software Release	
	1.7.0	
CDETS Number	Found in Release	Corrected in Release
CSCte91618	1.7.0	1.7.0
CSCtf01747	1.7.0	1.7.1
CSCtg05360	1.7.0	None
CSCti29498	1.7.0	1.7.1
CSCti30916	1.7.0	1.7.1
CSCti46701	1.7.0	1.7.1
CSCtj09993	1.7.0	1.7.1
CSCtj21452	1.7.0	1.7.1
CSCtk06701	1.7.0	None
CSCtk08686	1.7.0	None

Caveats for CTRS Release 1.7.0

- CSCte91618—Stopping recording or playback causes phone screen to freeze
Symptom: While making or playing back a recording, the phone screen freezes when a user clicks the stop button.
Conditions: This issue can occur with CTRS 1.6.x and midlet 1-6-0.2S.

Workaround: This issue should resolve if you take one of the following actions:

- Wait for 5 minutes for the timeout at the endpoint (the idle screen is displayed).
 - Stop and restart the midlet services by selecting the services button.
- CSCtf01747—CTRS Admin Web UI: Log file filter not working properly

Symptom: In the Troubleshooting > Log Files page, you used the Web-UI filter to narrow the log files that are displayed, but the page unexpectedly displays no log files.

Conditions: This condition can occur if the CTRS is running software release 1.7.0.

Workaround: Do not use the Web-UI filter. Alternatively, the Log Files page enables you to download selected log files.

- CSCtg05360—CTRS accepted incoming call and recorded session

Symptom: A user dialed the CTRS's access number. The CTRS accepted and recorded the incoming call.

Conditions: This situation can occur if the CTRS is running software version 1.7.0.

Workaround: Users should refrain from dialing the CTRS's access number.

Further Problem Description: In this situation, by default, the CTRS will attempt to record the session. The session will take up a recording session count.

- CSCti29498—CTRS End-User Portal: refresh causes unexpected video deletion

Symptom: In the CTRS End-User Portal video listing page, a user clicked the check box next to a video that they wanted to delete and the Delete button changed to "Delete(1)." The user then clicked the refresh icon and noticed that even though the video was no longer selected, "Delete(1)" remained. The user then clicked the Delete(1) button and noticed that the video was deleted even though it was not selected.

Conditions: This issue can occur if the CTRS is running software version 1.7.0.

Workaround: After selecting a video, do not click the refresh icon. If the refresh icon was clicked, click the My Videos tab to reset the display.

- CSCti30916—No restore files after changing page or number of pages displayed

Symptom: In the System Configuration > Backup Settings > Backup/Restore page of the CTRS Administration UI, an administrator clicked the Show button to display files available to be restored. After the restore files are displayed, clicking the next page icon or changing the number of files displayed per page then clicking the Go button caused the system to display no files.

Conditions: This issue can occur if the CTRS is running software version 1.7.0.

Workaround: Click the Show button again to redisplay the restore files.

- CSCti46701—CTRS Admin UI in Firefox & Safari Browsers: diffs with UI in IE browser

Symptom: As compared with the CTRS administration UI displayed in an Internet Explorer browser, the UI displayed in an Apple Safari or Mozilla Firefox browser has the following differences:

- In the Troubleshooting > Log Files page, the log file title appears as
<%=logFilesTitle>
- In the Troubleshooting > System Messages page, the calendar button overlaps with the word "on".
- In the Monitoring > Process Status and Monitoring > Hardware Status pages, the automatic refresh feature can cause the HTTP 404 error to display.

Conditions: These difference occur if the CTRS is running software version 1.7.0.

Workaround: None.

- CSCtj09993—User portal displays error message if PIN begins with “0”

Symptom: A PIN cannot begin with “0” (zero). If users enter “0” as the first digit, this popup message appears: “PIN should only contain numerics.”

Conditions: CTRS is running release 1.7.0. Users log in to the user portal to create or change a PIN for recording and viewing videos on CTS endpoints.

Workaround: Advise users not to use “0” as the first digit when they create or change a PIN.

- CSCtj21452—Issue when playing back video recorded by 1.7 CTRS

Symptom: When playing back a video on a TelePresence endpoint, a user might notice video artifacts such as tearing and blockiness.

Conditions: This issue can occur under the following conditions:

1. A video is recorded by a CTRS running software version 1.7.0.
2. The video is exported.
3. The video is imported.
4. The video is played back on a TelePresence endpoint.

Workaround: The following are workarounds to avoid the possibility of seeing artifacts during video playback:

- Steps 1 through 3 under “Conditions” are performed, but instead of playing a video back on a TelePresence endpoint as described in step 4, a user plays back the video in the end-user portal.
- Only steps 1 and 4 under “Conditions” are performed. (The video is not exported and imported.)
- A user can play back a video, which was recorded by a CTRS running pre-1.7.0 software then exported and imported, on a TelePresence endpoint or the end-user portal.



Note

This issue will be fixed in an upcoming CTRS 1.7.x release. Until then, users do not need to be wary of exporting/archiving videos recorded by a 1.7.0 CTRS.

- CSCtk06701—CTRS inadvertently restored with corrupted backup files

Symptom: In the CTRS Administrative UI/Configure > Backup Settings page/Backup/Restore tab, a CTRS administrator selects backup parameters, then clicks the Backup Now button. While waiting for the backup to complete, the admin navigates to another page in the UI, then returns to the Backup/Restore tab and does not notice that the backup failed, which results in corrupted backup files. The admin then inadvertently performs a restoration using the corrupted backup files.

Conditions: This issue can occur with CTRS versions 1.6.0, 1.6.1, 1.6.2, 1.6.3, 1.7.0, and 1.7.1.

Workaround: When performing a backup and restoration, the CTRS admin should carefully check the Backup Status display in the Configure > Backup Settings page/Backup/Restore tab to ensure that the backup was successfully implemented BEFORE performing a restoration.

- CSCtk08686— Restore Now button is clicked before restore data file is selected

Symptom: In the CTRS Administrative UI/Configure > Backup Settings page/Backup and Restore tab, the Restore Now button can be clicked before a CTRS administrator selects a data file to be restored. The ability to click the Restore Now button without specifying a file can result in the CTRS being restored with the wrong data file.

Conditions: This issue can occur with CTRS versions 1.6.0, 1.6.1, 1.6.2, 1.6.3, 1.7.0, and 1.7.1.

Workaround: When restoring the CTRS, the admin should perform these steps in this order:

1. Select the restoration parameters.
 2. Click the Show button.
 3. From the data files that display, select the desired file.
 4. Click the Restore Now button.
- CSCtn71601—After recording session, rec_audit.log file was not created

Symptom: After a Cisco TelePresence Studio Mode recording session, you go to the Troubleshoot > Log Files page in the CTRS Administrative UI and notice that an associated rec_audit.log file has not been created.

Conditions: This issue can occur in CTRS releases 1.7.0 and 1.7.1.

Workaround: None.

- CSCtq05603—Video Portal users sorted by email addr lose order after page update

Symptom: In the Configure > Access Management page, End-user Portal tab, you sort the Cisco TelePresence Video Portal users by email address, then change the number of users displayed on the page or display the next page of users. After the page updates, the ordering of users by email address is lost.

Conditions: This issue can arise in CTRS 1.7.2 and earlier.

Workaround: None.

New and Changed Information in CTRS Release 1.6.3

The following caveats were fixed in CTRS Release 1.6.3:

- CSCtj02672—CTRS: recorded presentation does not play back
- CSCtj21452—Issue when playing back video recorded by 1.7 CTRS

New and Changed Information in CTRS Release 1.6.2

Compatibility Caveat

A compatibility issue exists between a 1.6.2 CTRS and a 1.7.0 CTS endpoint. For example, if you record a presentation on a 1.7.0 CTS endpoint using a 1.6.2 CTRS, the presentation cannot be played back on any endpoint.

This issue was fixed in CTRS release 1.6.3.

Caveats

The following caveats were fixed in CTRS Release 1.6.2:

- CSCtc36852—Previous user's last viewed page still seen when a new user signs in to the end-user portal.
- CSCtc77540—Recording description added from administrative UI is not propagated to end-user portal.
- CSCtd46990—User portal video requires login for every video playback.
- CSCtd64292—If export of a recording fails, the recording cannot be scheduled for deletion.
- CSCte36197—No progress indicator for video downloading during playback.
- CSCte39770—Third-party video portal list no complete on portal.
- CSCte76228—Scheduled video deletion does not send out email notification for weekly schedule.
- CSCtf01683—User portal returns IP address in HTTP host field.
- CSCtf12470—CTRS full system backup fails to back up media files.
- CSCtf17739—CTRS restore does not work; result in database corruption.
- CSCtf88863—Cannot import video files from backup server.

New and Changed Information in CTRS Release 1.6.1

The following caveats were fixed in CTRS Release 1.6.1:

- CSCtc27046—Audio and video do not synchronize after network impairment.
- CSCtc91994—Null/null error and scheduled backup and export are not done if weekly backup and export are selected.
- CSCtd53228—HD version of video is missing the first 15 seconds
- CSCtd68551: When CTRS is on 7845I2 or 7835I2 platform, admin CLI access is denied with lines of java exceptions. Most GUI features are not available.

Caveats for CTRS Release 1.6.x

Caveats were recorded in the following CTRS Release 1.6.x releases:

- [CTRS Release 1.6.x Caveat Reference, page 13](#)
- [Caveats for CTRS Release 1.6.x, page 15](#)

CTRS Release 1.6.x Caveat Reference

[Table 3](#) summarizes caveats found in CTRS Release 1.6.x.

Table 3 CTRS Release 1.6.x Caveats and Caveats Corrected Reference

Software Release		
1.6.0		
CDETS Number	Found in Release	Corrected in Release
CSCtc03471	1.6.0	1.7.0
CSCtc27046	1.6.0	1.6.1
CSCtc29109	1.6.0	None
CSCtc36852	1.6.0	1.6.2
CSCtc71255	1.6.0	1.6.5 (CTS-Manager)
CSCtc77312	1.6.0	1.7.0
CSCtc77540	1.6.0	1.6.2
CSCtc88544	1.6.0	1.7.0
CSCtc91994	1.6.0	1.6.1
CSCtc95412	1.6.0	1.7.0
CSCtc99256	1.6.0	1.7.0
CSCtd04989	1.6.0	1.7.0
CSCtd11516	1.6.0	Unreproducible
CSCtd17697	1.6.0	1.7.0
CSCtd46990	1.6.0	1.6.2
CSCtd53228	1.6.0	1.6.1
CSCtd64292	1.6.0	1.6.2
CSCtd68551	1.6.0	1.6.1
CSCte36197	1.6.0	1.6.2
CSCte76228	1.6.0	1.6.2
CSCtf12680	1.6.0	1.7.0
1.6.1		
CDETS Number	Found in Release	Corrected in Release
CSCte39770	1.6.1	1.6.2
CSCtf01683	1.6.1	1.6.2
1.6.2		
CDETS Number	Found in Release	Corrected in Release
CSCtj02672	1.6.2	1.6.3
1.6.3		
CDETS Number	Found in Release	Corrected in Release
CSCtj73210	1.6.3	None

Caveats for CTRS Release 1.6.x

- CSCtc03471—Skip to the end during playback does not work correctly

Symptom: During playback, if the user skips forward to the end of the recording, the progress bar goes to end and then restarts from beginning of the recording. The recording then plays back for 8 or 9 seconds. Also, the timer above the progress bar does not reflect the time accurately if when skipping quickly without 2 seconds between each skip.

Conditions: This symptom is seen when the user skips forward in a recording.

Workaround: None.
- CSCtc27046—Audio and video do not synchronize after network impairment.

Symptom: Audio/video synchronization issues seen on CTS.

Conditions: If there is severe network impairment to only the audio or video port but not both, the CTS does not always recover from audio/video synchronization issues.

Workaround: Attempt playback when network conditions improve.
- CSCtc29109—Patch file not seen if it contains special characters “[]” in file name

Symptom: Patch file cannot be seen.

Conditions: Usually occurs when downloading the patch file to a destination in which a file of the same name already exists.

Workaround: Rename the file, or delete the duplicate one with “[.]”
- CSCtc36852—Previous user's last viewed page still seen when a new user signs in to the end-user portal

Symptom: Second viewer sees what the first viewer saw after signout.

Conditions: The first viewer signs in to the end-user portal. The first viewer shares one of his/her videos with second viewer. The first viewer then signs out, and the second viewer signs in on the same computer. The second viewer can still see the first viewer's last viewed page.

Workaround: None.
- CSCtc71255—E-mail aliases should not be validated against LDAP servers

Symptom: CTRS uses LDAP library in CTS-Man, which is used to authenticate individual users who want to sign in to CTRS via LDAP. Group aliases should not be validated against LDAP servers.

Conditions: A user tries to share a recording with an e-mail alias.

Workaround: Do not share recordings with e-mail aliases.
- CSCtc77312—Session expiration timer is not reset as expected.

Symptom: The user might not timeout right away when exiting UI. User times out a minute or so later.

Conditions: If the user configures the CTRS to sign out after “five minutes of inactivity” (User Portal User Preferences) but then immediately signs out, the user sees this symptom. [

Workaround: None.

- CSCtc77540—Recording description added from administrative UI is not propagated to end-user portal

Symptom: The user provides a description for a recording, but then the description field says, “No description provided.”

Conditions: The user adds a long title (130 characters) and a short description to a recording. When the user launches the end-user portal, the description field says “No description provided.” The administrative user interface shows both the title and description correctly.

Workaround: None.
- CSCtc88544—HTTP 500 error when server comes up after changing hostname from CLI

Symptom: Admin user interface shows 500 Error.

Conditions: After changing the hostname, this problem occurs intermittently.

Workaround: Reboot the CTRS.
- CSCtc91994—Null/null error and scheduled backup and export are not done if weekly backup and export are selected

Symptom: In System Backup/Restore and Export Media files in the admin user interface, an error message is displayed when the admin schedules a weekly backup/restore or export with multiple weekdays selected or with only Sunday selected. The schedule is not triggered for the weekly setting with multiple weekdays checked or if only Sunday checked.

Conditions: This symptom is seen in Release 1.6.0.

Workaround: Set a daily schedule, or set a weekly schedule with only one weekday selected (but do not select Sunday).
- CSCtc95412—Import does not import back the presentation file in a recording

Symptom: Aux presentation file does not get imported.

Conditions: The user sees this symptom with a recording that has a presentation.

Workaround: Copy the aux presentation file manually to the appropriate folder.
- CSCtc99256—Import interface shows error after exporting

Symptom: Import screen returns error.

Conditions: If there is a filename with more than 10 digits, the user sees this symptom.

Workaround: Do not import this file.
- CSCtd04989—Able to delete admin, but delete should be disabled for default admin user

Symptom: In User Management in the admin user interface, the administrative user can be deleted.

Conditions: This symptom is seen in Release 1.6.0.

Workaround: Do not delete the default administrative user. If other admin users are deleted, sign in as the default admin user and recreate other admin users. If all administrative users are deleted, the admin users are not able to sign in to admin user interface.
- CSCtd11516—CIF public recording seen on IP phone under public recording in corrupted format

Symptom: A corrupted recording title shows in the end-user portal.

Conditions: If a recording in CIF format only is made public, this symptom is seen.

Workaround: Do not make CIF videos public.

- CSCtd14343 (Duplicate of CSCte19618)—Phone UI freezes in Review page if pause and stop selected

Symptom: The user sees a frozen IP phone UI.

Conditions: After recording from an endpoint, the user reviews the recording. When the user pauses and stops multiple times, the progress bar moves as though playback is progressing, but the display is blank. After, the phone UI freezes. The UI unfreezes after the default timeout period has elapsed.

Workaround: Wait for the timeout period to elapse. An idle screen is then displayed. Or stop and start midlet services by selecting the Services button.

- CSCtd17697—Playback “Unable to connect” message on phone UI while multiple recordings are starting

Symptom: The phone UI might show that it is unable to connect.

Conditions: In a scenario in which multiple recordings are being brought up simultaneously (approximately 23), this symptom might be seen.

Workaround: Retry recording or playback.

- CSCtd17702 (duplicate of CSCtf12680)—Cannot import more than 20 recordings at a time with IE 6

Symptom: In the Import Media page in IE 6, the user shows 50 items per page and selects more than 20 recordings. The user then clicks import. A JavaScript error occurs, and the import cannot be executed.

Conditions: This symptom is seen in Release 1.6.0.

Workaround: On the import page, import at most 20 recordings each time in IE 6. Or use IE 7 or IE 8 to import more than 20 recordings.

- CSCtd53228—HD version of video is missing the first 15 seconds

Symptom: HD version missing first 15 seconds, but SD version is fine.

Conditions: Packet loss occurs at the beginning of a recording. A full IDR is not received at the beginning.

Workaround: None

- CSCtd68551—CTRS file system in read-only mode

Symptom: Admin CLI access is denied with lines of java exceptions. Most GUI features are not available.

Conditions: CTRS is on 7845I2 or 7835I2 platform.

Workaround: Power cycle the server.

- CSCtf12680—CTRS Admin UI: Error occurs when importing 20+ files using IE6 browser

Symptom: In the Import Media Files page of the CTRS Administrative UI, you changed the number of recordings displayed per page to 50, selected 20+ recordings, and clicked Import Files. As a result, a Javascript error occurs.

Conditions: This issue can occur under the following conditions:

- You use an Internet Explorer version 6 browser to access the CTRS Administrative UI/Import Media Files page.
- You try to import the files via a CTRS running 1.6.x software.

Workaround: When using an Internet Explorer version 6 browser, select a maximum of 20 recordings to import at one time. To work around this limitation, you can use a version 7 or 8 Internet Explorer browser.

- CSCtj02672—CTRS: recorded presentation does not play back

Symptom: A presentation recorded by a CTRS on a 1.7.0 CTS endpoint could not be played back on a 1.6.2 CTS endpoint.

Conditions: This issue occurred when recording with a CTRS running 1.6.2 software. Currently, a compatibility issue exists between a 1.6.2 CTRS and a 1.7.0 CTS endpoint.

Workaround: If recording a presentation on a 1.7.0 CTS endpoint, use a CTRS running software versions 1.7.0 or 1.6.3.
- CSCtj13018—CTRS user portal login with username with different case sensitivity

Symptom: A user logs into the CTRS end-user portal and expects to see their videos. Instead, they are prompted for a PIN, and no videos display.

Conditions: When the user logged in, they might have specified a username with a different case sensitivity than that recognized by the CTRS end-user portal. For example, instead of specifying “mike,” they specified “Mike.” As a result, the system treats the user as a new user and prompts for a PIN.

Workaround: The next time the user logs in, they should specify the username with the same case sensitive as their Active Directory username.
- CSCtj73210—CTRS: midlet can't list videos if more than 4000 videos in CTRS

Symptom: A user might not be able to view a video through a CTS endpoint.

Conditions: This issue may arise if a user has a high number of recorded videos.

Workaround: Reduce the number of videos so that playback from an endpoint is possible, or access the video from the end-user portal.

Obtaining Documentation and Submitting a Service Request

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)