Release Notes for Cisco Media Experience Engine 3500, Release 3.3.x

Revised: October 31, 2013

This document provides information about features, caveats, and software upgrade procedures for Cisco Media Experience Engine 3500 (Cisco MXE 3500) Release 3.3.0, 3.3.1, and 3.3.2 on the Cisco MXE 3500.

Cisco Systems, Inc.
www.cisco.com

Browser Requirements

You must use one of following web browsers to access the Cisco MXE 3500 Web UI:

- Firefox 3 or later (Firefox 3.5 is recommended)
- Internet Explorer 8

New Features

Cisco MXE 3500 Maintenance Release 3.3.2 includes bug fixes and patches. There are no new features.

Cisco MXE 3500 Maintenance Release 3.3.1 includes the following new features:

- Direct upgrade to Release 3.3.1 from Cisco MXE 3500 V2 hardware running Release 3.2, Release 3.2.1, or Release 3.3.
- Upgrade licenses are not required. If you have a Base license, an upgrade license is not required for integrated auto-workflow between Cisco TCS, Cisco MXE 3500, and Cisco Show and Share. If you already have a Graphics license, an upgrade license is not required to use bumpers, trailers, and watermarks.

Cisco MXE 3500 Release 3.3.0 includes the following new features:

- Integrated auto-workflow between Cisco TelePresence Content Server (TCS), Cisco MXE 3500, and Cisco Show and Share.
- Simplified deployment for Cisco MXE 3500 and Cisco Show and Share for transcoding video content.
- New ingest formats for VOD: Flash 9 and 10, WebEx (.arf 2.26 and below) files.
- The Video Conversion Interface is enhanced for ease of use.
- Pulse video analytics for speech and speaker tagging.

Supported Hardware

Cisco MXE 3500 Release 3.3.0 and 3.3.1 runs only on Cisco MXE 3500 Version 2 (V2) hardware.

Cisco MXE 3500 Release 3.3.2 runs on Cisco MXE 3500 V2 and V3 (Cisco MXA UCS M3)hardware.

For more information about migrating to the Cisco MXE 3500 V3 hardware, see the release notes on Cisco.com: *http://www.cisco.com/en/US/products/ps12130/prod_release_notes_list.html*

Supported Hardware Migration

The following Cisco MXE 3500 Release 3.3.x migration paths are supported on Cisco MXE 3500 V3 hardware:

- Cisco MXE 3500 Version 2 (V2) hardware running Release 3.3.2 > Cisco MXE 3500 V3 hardware running Release 3.3.2
- Cisco MXE 3500 Version 2 (V2) hardware running Release 3.3.1 > Cisco MXE 3500 V3 hardware running Release 3.3.2

For more information about migrating to the Cisco MXE 3500 V3 hardware, see the release notes on Cisco.com: *http://www.cisco.com/en/US/products/ps12130/prod_release_notes_list.html*

Upgrading the Software

The following Cisco MXE 3500 Release 3.3.x software upgrade paths are supported on Cisco MXE 3500 V2 hardware:

3.3.1 > 3.3.2

3.3.0 > 3.3.1

3.2.x > 3.3.0

3.1.x > 3.2.x

3.0.x > 3.1.x

To upgrade the software, see these sections:

- Upgrading to Release 3.3.2 from Release 3.3.1, page 3
- Upgrading to Release 3.3.1 from Release 3.3.0, page 4
- Upgrading to Release 3.3.0 from Release 3.2.x, page 4

Before You Begin

- Perform a system backup before upgrading the system software.

  For a clustered deployment, back up both the Resource Manager (RM) appliance and the Resource Nodes (RNs).

  See the Administrative Tasks chapter in the *User Guide for Cisco MXE 3500 Release 3.2* for information on how to backup, restore and upgrade the software.
- You need an account on Cisco.com to access the software download, edelivery, and license websites. If you do not have a Cisco.com account, you can register here: http://www.cisco.com/web/siteassets/account/index.html.
- Software Release 3.3.0 and 3.3.1 runs only on Cisco MXE 3500 V2 hardware. Cisco MXE 3500 Release 3.3.2 runs on Cisco MXE 3500 V2 and V3 hardware.

Upgrading to Release 3.3.2 from Release 3.3.1

The tasks in this section apply only to Cisco MXE 3500 V2 hardware running Release 3.3.1.

To upgrade the software, complete these tasks on the Standalone, or in a clustered deployment, on the Resource Manager (RM) appliance:

- Task 3: Download the New Software Bundle, page 7
- Task 4: Install the New Upgrade Bundle, page 7

In a clustered deployment, perform this task on each Resource Node (RN):

- Task 5: Upgrade Each Resource Node (Only Clustered Deployments), page 8

Upgrading to Release 3.3.1 from Release 3.3.0

The tasks in this section apply only to Cisco MXE 3500 V2 hardware running Release 3.3.0.

To upgrade the software, complete these tasks on the Standalone, or in a clustered deployment, on the Resource Manager (RM) appliance:

- Task 3: Download the New Software Bundle, page 7
- Task 4: Install the New Upgrade Bundle, page 7

In a clustered deployment, perform this task on each Resource Node (RN):

- Task 5: Upgrade Each Resource Node (Only Clustered Deployments), page 8

Upgrading to Release 3.3.0 from Release 3.2.x

The upgrade tasks in this section only apply to Cisco MXE 3500 V2 hardware running Release 3.2.x.

To upgrade the software, complete these tasks on the Standalone, or in a clustered deployment, on the Resource Manager (RM) appliance:

- Task 1: Download and Install Software Patches (Only for Release 3.2.x Upgrade), page 4
- Task 2: Restart the Cisco MXE 3500 (Only for Release 3.2.x Upgrade), page 7
- Task 3: Download the New Software Bundle, page 7
- Task 4: Install the New Upgrade Bundle, page 7

In a clustered deployment, perform this task on each Resource Node (RN):

- Task 5: Upgrade Each Resource Node (Only Clustered Deployments), page 8

Task 1: Download and Install Software Patches (Only for Release 3.2.x Upgrade)

To prepare for the software upgrade, you need to apply software patches to the Linux OS and Windows OS. In a clustered deployment, also apply the software patches to the RM appliance and each RN.

Note The Linux OS software patch is required only on the RM appliance.

Download the Software Patches

Follow these steps to download the software patches:

Step 1 Go to *http://www.cisco.com/cisco/software/type.html?mdfid=282815279&i=rm*.

Step 2 Download the software patches for one of the following releases you are upgrading to:

Cisco MXE 3500 Release 3.3.1

a. Click **Media Experience Engine Patches > Latest Releases >3.3.1**.

b. Download the following software patches to your computer:

- upgrade-bru-3.3.1.mxe, for the Windows OS.
- NCOS-32GB-update-3.3.1.zip, for the Linux OS—Download this software patch only if you have Pulse video analytics.

c. Copy the MD5 checksum displayed in the cart. This is required during installation.

d. Go to Install the Software Patch to Windows OS, page 5.

Cisco MXE 3500 Release 3.3

Download this patch only if you are upgrading to Release 3.3.

a. Click **Media Experience Engine Patches > Latest Releases > 3.3.0**.

b. Download the following software patches to your computer:

- upgrade-bru-3.3.0.mxe, for the Windows OS.

c. Click **Media Experience Engine Patches> Latest Releases >3.3.1**—only if you have Pulse video analytics:

d. Download the following software patch:

- NCOS-32GB-update-3.3.1.zip, for the Linux OS.

e. Go to Install the Software Patch to Windows OS, page 5.

Install the Software Patch to Windows OS

Follow these steps to install the software patch to Windows OS:

Step 1 Login to the Cisco MXE 3500 web UI at **http://*mxe_IP_address*/mxeui/**, where ***mxe_IP_address*** is the hostname or IP address for the Cisco MXE 3500.

Step 2 Under the Tools tab click **Upgrade**. The System Upgrade page appears.

The System Upgrade page displays information about the previous upgrade (if any) and provides links to display the detailed log messages from the previous upgrade. Information about the previous upgrade is also displayed in the **Help > About** dialog.

Step 3 Paste the MD5 checksum into **MD5 Checksum** field. (If the supplied MD5 checksum does not match the contents of the file, an error message displays and the upgrade terminates.)

Step 4 Click **Browse** to select the software patch file.

Step 5 Click **Upgrade** to begin the upgrade process.

Once an upgrade is initiated, the page will refresh and display the current status of the upgrade operation. An upgrade may take several minutes to complete. During the upgrade do not use or manually refresh the UI.

Step 6 (Optional) Click on Show Logs to view the upgrade details.

Install the Software Patch to Linux OS

Note The Linux OS software patch is required only on the RM appliance.

Follow these steps to install the software patch to the Linux OS:

Step 1 Unzip the software patch (NCOS-32GB-update-3.3.1.zip) to get NCOS-32GB-update-3.3.1.tgz.

Step 2 Copy NCOS-32GB-update-3.3.1.tgz to \\mxe-ip-address\temp, where *mxe-ip-address* is the IP address assigned to the MXE appliance.

Step 3 If an IP address has not be been assigned to ESXi, assign an IP address:

a. Physically console into the Cisco MXE 3500. Or, you can also use the Cisco Integrated Management Controller (CIMC) to access ESXi.

b. Press **F2** and log in as **root**.

c. Select **Configure Management Network**.

d. Select **IP Configuration**.

e. Enter the IP settings, then press **Enter**.

f. Press **Esc** to apply the settings.

g. Press **Esc** to exit ESXi configuration.

Step 4 Transfer the upgrade package to ESXi:

a. From the ESXi console, press **Alt+F1**, then press **enter**.

b. Log in as **admin**. The Cisco MXE 3500 Configuration Menu appears.

c. Select **System Command Prompt**.

d. Enter **scp /mnt/temp/NCOS-32GB-update.tgz admin**@*esxi-ip-address***:/home/admin**, where *esxi-ip-address* is the ESXi IP address.

If an `"RSA key fingerprint ..."` message appears, enter **yes**.

e. Enter **exit** to return to the Cisco MXE 3500 Configuration Menu.

f. Select **Exit System** to exit the Cisco MXE 3500 Configuration Menu.

Step 5 Run the software patch:

a. From the ESXi console, press **Alt+F1** and login as **root**.

b. Enter **cd /home/admin.**

c. Enter **tar -xzvf NCOS-32GB-update-3.3.1.tgz.**

d. Enter **cd NCOS-32GB-update-3.3.1.**

e. Enter **./install.sh.**

The update restarts the Linux OS. It will take a few minutes before the appliance is fully available again.

Step 6 Verify the upgrade:

a. From the ESXi console, press **Alt+F1**.

b. Log in as **admin**. The Cisco MXE 3500 Configuration Menu appears.

c. Select **System Command Prompt**.

d. Enter **more /proc/meminfo | grep MemTotal**

The MemTotal value shows as approximately **32909688 kB**

Task 2: Restart the Cisco MXE 3500 (Only for Release 3.2.x Upgrade)

After completing "Task 1: Download and Install Software Patches (Only for Release 3.2.x Upgrade)", restart the Cisco MXE 3500 from the Cisco MXE Appliance Configuration Menu. To access the Cisco MXE Appliance Configuration Menu, SSH to the *mxe_IP_address* and log in as **admin.**

Task 3: Download the New Software Bundle

Follow these steps to download the upgrade bundle:

Step 1 Go to *http://www.cisco.com/cisco/software/type.html?mdfid=282815279&i=rm*.

Step 2 Download the upgrade package.

- For standalone deployments, **upgrade-rm-3.3.x.mxe**
- For clustered deployments, download the following packages:
  - **upgrade-rm-3.3.x.mxe**
  - **upgrade-rn-3.3.x.zip**

Step 3 Copy the checksum displayed in the cart. The checksum is required for the upgrade.

Step 4 Save the upgrade files to a temporary media, such as a flash drive, or to a network server that you can access from the Cisco MXE 3500.

Task 4: Install the New Upgrade Bundle

Follow these steps to install the upgrade bundle in the standalone or RM appliance:

Step 1 From the Cisco MXE 3500 UI, navigate to **Tools > Upgrade**.

The System Upgrade page displays information about the previous upgrade (if any) and provides links to display the detailed log messages from the previous upgrade. Information about the previous upgrade also displays in the **Help > About** dialog.

Step 2 Paste the checksum into **MD5 Checksum** field. (If the supplied checksum does not match the contents of the file, an error message displays and the upgrade terminates.)

Step 3 Click **Browse** to select the upgrade file.

Step 4 Click **Upgrade** to begin the upgrade process.

Once an upgrade is initiated, the page will refresh and display the current status of the upgrade operation. An upgrade may take several minutes to complete.When the upgrade is complete, the Upgrade Successful message appears.

Note Because the Web UI is being replaced, UI might not reflect the upgrade status. Refresh the UI in the browser to check the status (CSCud72247).

Task 5: Upgrade Each Resource Node (Only Clustered Deployments)

In a clustered deployment, complete the following steps on each RN:

Step 1 Go to *http://www.cisco.com/cisco/software/type.html?mdfid=282815279&i=rm*.

Step 2 Download upgrade-rn-3.3.x.mxe.zip to your computer and extract its contents to \\MXE_IP\temp.

Step 3 Verify that the following files and directory are present:

- upgrade-rn.bat
- upgrade-rn.sh
- bin

Step 4 Upgrade Windows VM.

RDC to *mxe_IP_address*, log in as **admin**, navigate to c:\temp, and run upgrade-rn.bat.

Step 5 Upgrade Linux VM.

a. SSH to *mxe_IP_address*, login as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

b. At the Linux command prompt, enter **su -**, navigate to /mnt/temp and run ./upgrade-rn.sh.

Step 6 Restart the RN from the Cisco MXE Appliance Configuration Menu. To access the Cisco MXE Appliance Configuration Menu, SSH to the *IP_address* of the RN and login as **admin**.

Obtain and Install the Release 3.3 Upgrade License

Use the eDelivery procedure detailed in this section to order the Cisco MXE 3500 Release 3.3 upgrade bundle and receive the PAK, then download the Release 3.3 upgrade license.

Note We strongly recommend to upgrade to Release 3.3.1, which removes the requirement for upgrade licenses.

Release 3.3.0

An upgrade license is required to add bumpers, trailers, and watermarks, and to configure automated workflow from Cisco TelePresence Content Server (TCS) to Cisco MXE 3500 to Cisco Show and Share. If you already have a Graphics license, you must upgrade the license to use bumpers, trailers, and watermarks.

Maintenance Release 3.3.1 and 3.3.2

Upgrade licenses are not required to upgrade to Maintenance Release 3.3.1. and 3.3.2.

If you have a Base license, an upgrade license is not required for integrated auto-workflow between Cisco TCS, Cisco MXE 3500, and Cisco Show and Share.

If you already have a Graphics license, an upgrade license is not required to use bumpers, trailers, and watermarks. If you do not have a Graphics license, obtain and install a Graphics license to use bumpers, trailers, and watermarks. Follow the steps detailed in the “Deploying License Features,” section of the *Administration Guide for Cisco Media Experience Engine 3500 Release 3.3* on Cisco.com to obtain and install a license.

Before You Begin

You must have the following to obtain a license:

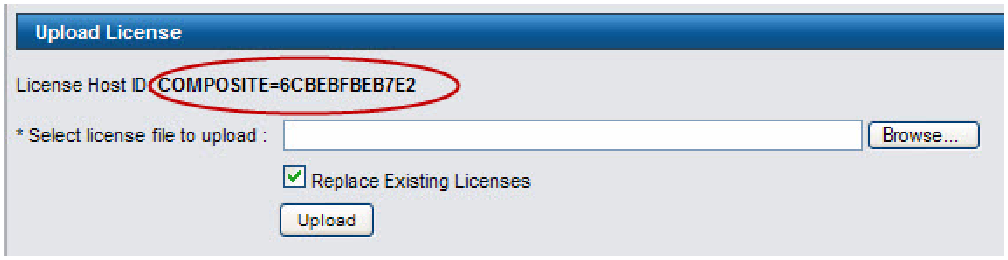
- The Cisco MXE 3500 License Host ID.

Note For clustered deployments, use the same License Host ID for registering the RM and each RN in your installation.

To view the License Host ID,

1. Login to the Cisco MXE 3500 web UI.
2. Under the Tools tab, click **Upload License**.

Figure 1 License Host ID String



License Host ID COMPOSITE=6CBEBFBEB7E2

* Select license file to upload :

☑ Replace Existing Licenses

Obtain the License File

Follow these steps to order and obtain the license file:

Step 1 Order the following eDelivery upgrade licenses for each Cisco MXE 3500.

- L-MXE-PAK= and choose the following options:
- L-MXE-3500-33UPG (Base software upgrade)
- L-MXE-3500-GRLIC (Must already have graphics option)

Step 2 Go to https://edelivery.cisco.com/esd/. Follow the eDelivery process to obtain the Product Authorization Key (PAK).

Step 3 Go to http://www.cisco.com/go/license. Use the PAK and Host ID of the Cisco MXE 3500 to obtain the license file.

Clustered Deployment:

- Complete the license registration of the RM appliance and obtain the license for that registration process. Discard the license file you receive for this registration.

- Register each RN separately. Use the RN PAK and the RM License Host ID for completing registration and obtaining the updated license files one at a time.
- You will use the license file that you receive for the final completed registration process on the RM appliance.

Step 4 Save the final license file to a location that the Cisco MXE 3500 can access during license installation.

Note If the license file is lost, it can take up to one business day to get another copy. The License file is saved during a system back up.

Install the Upgrade License

Follow these steps to install an upgrade license. Install the upgrade license in the standalone or the RM appliance.

Step 1 Log in to the Cisco MXE 3500 web UI.

Step 2 Under the Tools tab, click **Upload License**.

Step 3 Click **Browse** to navigate to and select the license file.

Step 4 Uncheck **Replace Existing Licenses** to add upgrade license to existing license.

Caution If **Replace Existing Licenses** is checked, the existing license is overwritten.

Step 5 Click **Upload** to install the license file on the Cisco MXE 3500.

Troubleshooting Tips

The following sections provides troubleshooting tips and contact information.

- License Files and Registration, page 10
- Upgrade Issues, page 11

License Files and Registration

If you experience problems with the license registration websites or if you have additional questions, for a prompt response, please open a Service Request using the TAC Service Request Tool at:

http://tools.cisco.com/ServiceRequestTool/create/DefineProblem.do.

Please have your valid Cisco ID and password, and the license host ID available. To view the license host ID, login to the Cisco MXE 3500 Web UI. Under the Tools tab, click **Upload License**. See Figure 1.

Alternatively, you may also call one of these numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

You can find a complete list of Cisco TAC contacts at this URL:

http://www.cisco.com/techsupport/contacts

Upgrade Issues

- Web UI Error during upload process.

  Verify that maxRequestLength web.config change has been applied. The maxRequestLength value, 2097151, is set to support 2 GB file uploads.
- Windows or Linux upgrade fails.
  - Examine status.log in c:\mxe\system\winos|ncos
  - Examine bru.log in c:\program files\cisco\media experience engine\logs\BRU
- The Upgrade Release 3.3 or Release 3.3.1 bundle failed to upload.

  Verify that the Cisco MXE 3500 was restarted after the software patch for the Windows OS was applied.
- After the Upgrade bundle is installed, the Cisco MXE 3500 web UI displays the older release version.

  Verify that the Cisco MXE 3500 was restarted after the upgrade bundle was applied.

Licensed Features

Table 1 describes the Cisco MXE 3500 features that require additional licenses.

Table 1 Cisco MXE 3500 Licensed Features

Licensed Feature	Description	PIDs
Resource Manager Resource Node	Enables multiple Cisco MXE 3500 devices to run as a single group with one set of user accounts, job profiles, licensed features, and user interfaces. Enables user-management functionality, such user accounts and roles, profile spaces, and user metadata.	• MXE-3500-33RM-K9 • MXE-3500-33RN-K9
Video Conversion Interface	Enables an easy-to-use interface for end users to do transcoding, post production, and sharing through a portal like Cisco Show and Share.	• MXE-3500-UILIC
Live Streaming (IP Capture)	On the Cisco MXE 3500 V2 hardware, this license enables the appliance to ingest live enterprise TV and IPTV feeds and re-purpose the content so that it can be viewed on a variety of endpoints.	• MXE-3500-LVLIC
Graphics Overlay	On the Cisco MXE 3500 V2 hardware, this license enables the appliance to embed watermark, bumpers, trailers, and text transcripts as text captions.	• MXE-3500-GRLIC

Table 1 Cisco MXE 3500 Licensed Features (continued)

Licensed Feature	Description	PIDs
Speech to Text	Enables the Cisco MXE 3500 to create text transcripts from videos.	• MXE-3500-STLIC
Pulse Video Analytics	Enables keyword tagging and speaker identification and sharing through a portal like Cisco Show and Share.	• MXE-PULSE-200 • MXE-PULSE-400P

For details about obtaining and installing a license file to enable the software for your deployment, see the *Administration Guide for Cisco Media Experience Engine 3500* on Cisco.com.

Important Notes

- Install QuickTime—QuickTime is installed separately because of Apple licensing requirements. It is required for transcoding to and from specific formats.

Note In a clustered deployment, you must install QuickTime on the RM appliance and each RN.

  See the *Administration Guide for Cisco Media Experience Engine 3500* on Cisco.com for instructions on how to install QuickTime.

- In a clustered deployment, use either the IP address or the FQDN instead of the local host in the host settings and the system settings on the Resource Manager appliance. Do not use a combination of the IP address and the domain name.

Limitations and Restrictions

You should review this section before you begin working with the Cisco MXE 3500. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the hardware or software.

- Jobs fail permanently during/after Cisco MXE 3500 restart. Jobs do not auto start.

  The workaround is after the MXE 3500 has been restarted, navigate to the Job status page and manually restart the job using the ‘Reschedule’ option. Please note that the jobs would be available for restart only up to one hour after the system has been restarted. This caveat does not apply to Live jobs. (CSCtr50466)

- Shared folders are not accessible when upgrading from MXE3500 v3.2.1 to MXE350 v3.3.0.

  The workaround is to navigate to Administration->Shared folder access setting page and Click on the **Save** button. This caveat is only applicable if AD is enabled for Shared Folder Access. (CSCtr46855)

- In the Cisco TCS integration with Cisco MXE 3500 with sharing in Cisco Show and Share, a "500 Internal Server error" occurs when a 1+ GB file is uploaded to Cisco Show and Share.

  The workaround is to change the bit rate of the profile used by TCS reduced to limit the size. Please note reducing the bit rate in the profile would reduce the quality of the transcoded file. This caveat is specific to Cisco Show and Share version 5.2.3. (CSCts64703)
- Unable to send UDP multicast MPEG2TS stream from VLC to Cisco MXE 3500.

  There is no workaround. (CSCtq65543)

Caveats

This section includes the following topics:

- Using the Bug Toolkit, page 13
- Open Caveats, page 14
- Resolved Caveats, page 17

Using the Bug Toolkit

Use the Cisco Software Bug Toolkit to search for problems.

Before You Begin

To access Bug Toolkit, you need the following:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use the Cisco Software Bug Toolkit:

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the Search for Bug ID field, then click **Go**.

Open Caveats

Table 2 lists the open hardware caveats for Cisco MXE 3500 and includes Severity 2 and Severity 3 caveats.

Because defect status continually changes, this table provides a snapshot of the defects that were open at the time of the release. For an updated list of open defects, access the Bug Toolkit (Step 1, above).

Table 2 Open Caveats for Cisco MXE 3500 Release 3.3.2

Identifier	Headline
CSCud72247	When using Cisco MXE 3500 upgrade bundle via Web UI for an upgrade, the UI appears stuck during step 2. The upgrade can take a several minutes, and the Web UI might not reflect the true upgrade status because the UI is being replaced. The workaround is to refresh the UI in the browser to check the status.
CSCtq01074	Configure Hostname/Domain name does not display current configuration. There is no workaround. The user has to provide the new hostname/DNS without being able to see the existing values on the same screen.
CSCts53583	SUI: Local Account Passwords containing special characters (%&*) could not log in. There is no workaround. Special characters are not allowed for local account passwords for the Video Conversion Interface.
CSCts47520	User entered tags in the Video Conversion Interface are truncated to 45 characters when published to Cisco Show and Share. The workaround is to enter tags within the maximum limit of 45 characters.
CSCts83731	The IP stop trigger option does not work sometimes for live streaming. The workaround is to set pre-filter option to **Optimize for Speed** (Preprocessor profile) and **immediate** (Encoder profile) for live jobs. If “Optimize for Quality” is required, the job can be manually stopped from MXE Web UI Job Status page.
CSCts49348	In the Video Conversion Interface, the Show and Share upload button is available for upload in the Your Results page before transcoding is complete. The workaround is to submit transcoded file to Show and Share from the Job Status page. In the Job Status page, the video can only be published to Cisco Show and Share after transcoding is complete. In case an incomplete file is uploaded to Cisco Show and Share, go to the Show and Share portal and delete the file, then republish the file from Video Conversion interface after transcoding has been completed.
CSCtr57953	In the Video Conversion Interface, upload to Show and Share fails if a combination of IP address and DNS is used in SUI Admin configuration. The workaround is to submit transcoded file to Show and Share from the Job Status page. In the Job Status page, the video can only be published to Cisco Show and Share after transcoding is complete. In case an incomplete file is uploaded to Cisco Show and Share, go to the Show and Share portal and delete the file, then republish the file from Video Conversion interface after transcoding has been completed.

Table 2 Open Caveats for Cisco MXE 3500 Release 3.3.2 (continued)

Identifier	Headline
CSCtr36959	The AD settings need to be saved again after changing the MXE Hostname. After changing the Cisco MXE 3500 hostname and IP Address, AD protected shared folders are not accessible and all jobs fail. The workaround is to navigate to the Shared Folder Access Settings on the Cisco MXE 3500 UI. Click **Save** without changing any configuration.
CSCtx92616	Support VOIP audio type in WebEx .arf transcoding. This file type is not yet supported; there is no workaround.
CSCty29182	WAV encoding goes to pending state. When an .mp3 to .wav transcoding job is submitted, the .wav encoding changes to the pending state. The Health Status Page also displays that the .wav worker is Offline. The workaround is to RDC to the Windows VM and rename: *C:\Program Files\Cisco\Media Experience Engine\bin\WaveEncoder.exe* to *C:\Program Files\Cisco\Media Experience Engine\bin\WavEncoder.exe*

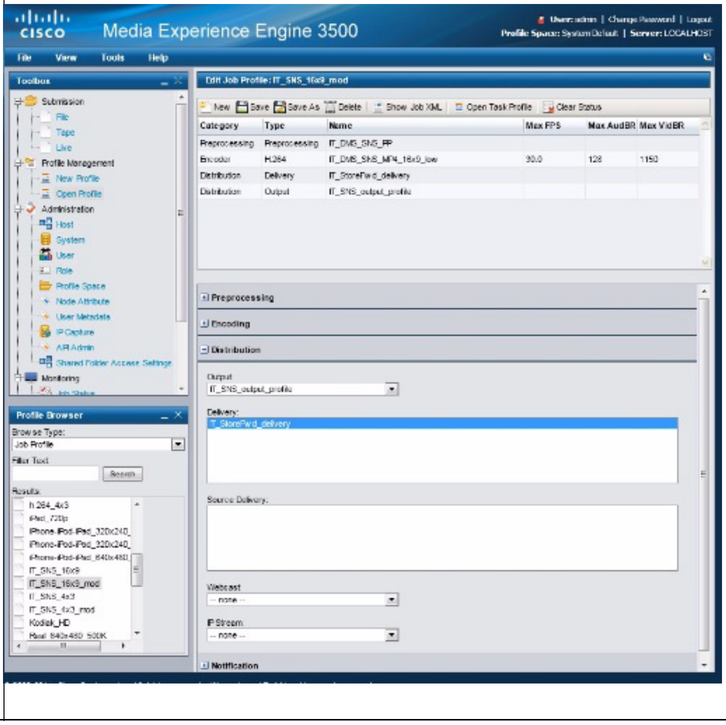
Table 2 Open Caveats for Cisco MXE 3500 Release 3.3.2 (continued)

<table>
<tr><th>Identifier</th><th>Headline</th></tr>
<tr><td>CSCub91160</td><td>
H.264 process stops at around 98% while the job status shows completed. For appliances running software version 3.3.1, MP4 file transcoding jobs show completed while the H.264 process displays as 98% running. This is the workaround:

1. In the Cisco MXE 3500 UI, navigate to **Administration > System Settings**.
2. For the encoder you are using (for example, H.264) change the Output Directory setting.

Note This change affects all H.264 encoders not just one profile. The following steps are required for all H.264 profiles in use.

3. Navigate to **New Profile > Distribution > Delivery**.
    a. In the Common window, enable these check boxes:
    – Profile Enabled
    – Use selected profiles
    b. In the Delivery Formats window, enable the check box for the desired profile (for example, H.264) and select the profiles to deliver. This will pair the delivery profile with a specific encoder. Save the profile.
4. Open the Specific Job Profile and navigate to Distribution. In the Delivery window select that profile that you saved in Step 3. Your job should look like the following screenshot. Save the profile. You should see all output delivered to MXE-RM-IP\output.
5. Repeat these steps for all the job profiles that you use.



Edit Job Profile: IT_SNS_16x9_mod

<table>
<tr><th>Category</th><th>Type</th><th>Name</th><th>Max FPS</th><th>Max AudBR</th><th>Max VidBR</th></tr>
<tr><td>Preprocessing</td><td>Preprocessing</td><td>IT_DMS_SNS_PP</td><td></td><td></td><td></td></tr>
<tr><td>Encoder</td><td>H.264</td><td>IT_DMS_SNS_MP4_16x9_low</td><td>30.0</td><td>128</td><td>1150</td></tr>
<tr><td>Distribution</td><td>Delivery</td><td>IT_StoreFwd_delivery</td><td></td><td></td><td></td></tr>
<tr><td>Distribution</td><td>Output</td><td>IT_SNS_output_profile</td><td></td><td></td><td></td></tr>
</table>

Output: IT_SNS_output_profile
Delivery: IT_StoreFwd_delivery
Source Delivery:
Webcast: -- none --
IP Stream: -- none --

Browse Type: Job Profile
Filter Text:
Results:
h.264_4x3
iPad_720p
iPhone-iPod-iPad_320x240_
iPhone-iPod-iPad_320x240_
iPhone-iPod-iPad_640x480_
IT_SNS_16x9
IT_SNS_16x9_mod
IT_SNS_4x3
IT_SNS_4x3_mod
Kodiak_HD
Real_640x480_500K
</td></tr>
</table>

Table 2 Open Caveats for Cisco MXE 3500 Release 3.3.2 (continued)

Identifier	Headline
CSCuc84385	Large Files from TCS to MXE fails. Large videos that are uploaded from Cisco TCS to Cisco MXE 3500 are not transcoded and are failing with the error "Unable to locate input file" even though the uploaded file is present in the TCS/Shared directory on the MXE 3500. There is no workaround.

Resolved Caveats

- Resolved Caveats in Release 3.3.0, page 17
- Resolved Caveats in Release 3.3.1, page 18
- Resolved Caveats in Release 3.3.2, page 19

Resolved Caveats in Release 3.3.0

Table 3 lists the resolved caveats in Cisco MXE 3500 Release 3.3.0.

Table 3 Resolved Caveats for Cisco MXE 3500 Release 3.3.0

Identifier	Headline
CSCto33154	The Cisco MXE 3500 web UI allows multiple submissions for back up from different instances.
CSCtq49728	When changing the API commands, the current value is not reflected in the UI
CSCtr08420	Upgrade to 3.2.1-2 wipes out API authentication mode used by Cisco Show and Share
CSCtr10170	Sometimes, clicking on the Save button in LDAP and AD settings does not do anything
CSCts41765	VP6f video fails in prefilter.
CSCtr75726	FTP watch folder incorrectly detects file readiness.
CSCts51448	Two instances of multicastout service running on the Linux OS.
CSCua96966	Fix Max Queue Length Report. See patch information in the "MaxQueueLengthSaveReport" section on page 23.
CSCtu37637	Enable live stream output to play on VLC player. See patch information in the "Multicast Checksum Issue" section on page 24.
CSCtx20390	Fix Draft-Processing state issue. See workaround information in the "Draft-Processing State Issue" section on page 30.

Resolved Caveats in Release 3.3.1

Table 4 lists the resolved caveats in Cisco MXE 3500 Maintenance Release 3.3.1.

Table 4 Resolved Caveats for Cisco MXE 3500 Maintenance Release 3.3.1

Identifier	Headline
CSCts78846	Not showing no license error when there is no SUI license.
CSCts83779	ARF to mp4 transcoding creates distorted audio file.
CSCtt12108	White List lookup should use lower case key for acronym.
CSCtt26542	LDAP connection problem in SUI.
CSCtt29764	Change encryption code in casper.
CSCtt30012	Post processing of SSR output based on posterior probability.
CSCtt30249	Prefilter failed when using the "Out Point" AND bumper / trailer options.
CSCtt35883	LMInstaller - simplify installation logic.
CSCtt36036	If customer does not have SUI license, then “Shared Folder Access Settings” option in the MXE UI cannot be selected.
CSCtt45178	Blank audio in webex recordings with muted audio.
CSCtu00963	Sometimes, video is distorted in TCS-MXE-SnS flow with watermark enabled.
CSCtu10471	Automatically Add Entitled License Features.
CSCtu13819	Preview fails in SUI when previewing video-only asset.
CSCtu21635	Fresh Install Sets Incorrect Worker Run Limits.
CSCtu33275	Install Overlay with Speaker Subject on Top.
CSCtu82202	Videos for which thumbnails cannot be generated are being dropped mid-way of analytics flow.
CSCtw56526	Composite ID reset after reboot. See workaround information in the “Composite ID Reset” section on page 22.
CSCtx35225	TCS ftp user password expires. See patch information in the “Login_expiry_patch.tar.gz” section on page 21.
CSCtx92834	ARF transcoding job stuck. See patch information in the “WebExUpgradePatch.zip” section on page 22.
CSCtx96304	Change the threshold for matching speaker names. See patch information in the “Analytics.tar.gz” section on page 27.
CSCty14628	Analytics process goes down intermittently. See patch information in the “Analytics.tar.gz” section on page 27.
CSCty71814	H.264 encoder generates error messages that filled up ecs.log See patch information in the “H264PatchZip” section on page 23.
CSCua96966	Fix Max Queue Length Report. See patch information in the “MaxQueueLengthSaveReport” section on page 23.
CSCtu37637	Enable live stream output to play on VLC player. See patch information in the “Multicast Checksum Issue” section on page 24.
CSCtx20390	Fix Draft-Processing state issue. See workaround information in the “Draft-Processing State Issue” section on page 30.

Table 4 ***Resolved Caveats for Cisco MXE 3500 Maintenance Release 3.3.1 (continued)***

Identifier	Headline
CSCtx99530	Mtagger returns an exception when a video is sent for processing. See patch information in the "Analytics_patch_2.tar.gz" section on page 28.
CSCtz14706	The ssrdb service throws an exception on startup. See patch information in the "Analytics_patch_2.tar.gz" section on page 28.
CSCtz18505	The ssrdb and mtagger services do not come up if the database service is down. See patch information in the "Analytics_patch_2.tar.gz" section on page 28.
CSCtz13241	Mtagger returns a video processing error because of an ssrdb communication failure. See patch information in the "Analytics_patch_2.tar.gz" section on page 28.
CSCtx81886	Speaker names entered for a video are not propagated to future videos. See patch information in the "Analytics_patch_2.tar.gz" section on page 28.
CSCuc84113	Backup script is missing vocabMap. See patch information in the "Backup_filelist" section on page 30.
CSCue26022	Pulse analytics process hangs. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCud11339	Upgrade to 3.3.2 from 3.3.1 deletes the language model. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCud62509	Speaker refresh fails after SSR database restart. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCue25992	Speaker refresh hits solr database query limits. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCtr74486	MXE-3500 R3.2 Incorrect Subnet Mask. See patch information in the "Incorrect Subnet Mask Patch" section on page 24.
CSCud62652	MP4 ingest anomalies. See patch information in the "MP4 Ingest Anomalies Patch" section on page 25.
CSCud67680	Rename command failed in TCS->MXE ftp workflow. See patch information in the "Rename Command Failure Patch" section on page 25.
CSCue93265	Mtagger/ssrLib failed to start because of 4GB limit. See patch information in the "AnalyticsMemoryIssue Patch" section on page 32.
CSCue93280	Memory Mtagger/SSR requires 4GB+ for 1.1GB compressed model. See patch information in the "AnalyticsMemoryIssue Patch" section on page 32.

Resolved Caveats in Release 3.3.2

Table 5 lists the resolved caveats for Cisco MXE 3500 Maintenance Release 3.3.2

Table 5 ***Resolved Caveats for Cisco MXE 3500 Maintenance Release 3.3.2***

Identifier	Headline
CSCtx20390	Increase headerBufferSize for solr jetty.
CSCtz05398	Cisco MXE 3500 generates incorrect in-point.
CSCua96966	Fix Max Queue Length Report.

Table 5 **Resolved Caveats for Cisco MXE 3500 Maintenance Release 3.3.2 (continued)**

Identifier	Headline
CSCty71814	H.264 encoder generates numerous error messages that filled up ecs.log.
CSCtx92834	ARF transcoding job stalled at 0%.
CSCtu55663	TCS joined video is stretched when uploaded to Show and Share with Cisco MXE 3500 transcoding
CSCty14628	Monit: pidfile `/var/run/ssrdb.pid' does not contain a valid pidnumber.
CSCtx96304	SSR - OOB threshold for matching speakers need to be changed.
CSCtx35225	Cisco TCS FTP user password expires.
CSCtu37637	Enable live stream output to play on VLC player.
CSCtw56526	Composite ID reset after reboot.
CSCtx99530	SSR crashes on a video.
CSCtz14706	SSRDb crashed on restart and couldn't come up.
CSCtz13241	Analytics job failed with SSR communication failure message.
CSCtz18505	SSRdb and SSR Client services should always come up.
CSCtx81886	SNS Failed to Update SID Database for Speakers with Apostrophe.
CSCue26022	Pulse analytics process hangs. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCud11339	Upgrade to 3.3.2 from 3.3.1 deletes the language model. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCud62509	Speaker refresh fails after SSR database restart. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCue25992	Speaker refresh hits solr database query limits. See patch information in the "AnalyticsPatches-3.3.x-feb-2013" section on page 31.
CSCtr74486	MXE-3500 R3.2 Incorrect Subnet Mask. See patch information in the "Incorrect Subnet Mask Patch" section on page 24.
CSCud62652	MP4 ingest anomalies. See patch information in the "MP4 Ingest Anomalies Patch" section on page 25.
CSCud67680	Rename command failed in TCS->MXE ftp workflow. See patch information in the "Rename Command Failure Patch" section on page 25.
CSCue93265	Mtagger/ssrLib failed to start because of 4GB limit. See patch information in the "AnalyticsMemoryIssue Patch" section on page 32.
CSCue93280	Memory Mtagger/SSR requires 4GB+ for 1.1GB compressed model. See patch information in the "AnalyticsMemoryIssue Patch" section on page 32.
CSCui19998	MXE-3500 Samba denial of service vulnerability. See patch information in the "Samba Denial of Service Patch" section on page 26.
CSCui48757	MXE - Apache Struts2 command execution vulnerability. See patch information in the "Apache Struts2 Patch" section on page 26.

Patches and Fixes

For Cisco MXE 3500 Release 3.3, see these topics:

System Patches

Login_expiry_patch.tar.gz

The login_expiry_patch.tar.gz provides a fix to CSCtx35225 by disabling the password expiration for the default FTP accounts. This patch applies to Release 3.3.1.

Step 1 Download **login_expiry_patch.tar.gz** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Copy the patch to \\*mxe-ip-address***\temp**, where *mxe-ip-address* is the IP address assigned to the Cisco MXE 3500 appliance.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

Step 4 At the command prompt, enter **cd /mnt/temp**.

Step 5 Enter **tar -xzvf login_expiry_patch.tar.gz** to get **login_expiry_patch.sh**.

Step 6 Enter **./login_expiry_patch.sh**.

Upon successful completion, `Patch installation successful` is displayed. This message confirms that the patch is applied successfully.

Step 7 Exit command shell and SSH session.

Composite ID Reset

This workaround addresses CSCtw56526, composite ID reset after reboot, and applies to Release 3.3.1.

Step 1 If an IP address has not be been assigned to ESXi, assign an IP address.

For instruction on how to assign an IP to ESXi, see "Step 3If an IP address has not be been assigned to ESXi, assign an IP address:"

Step 2 Change the **.vmx** files.

a. From the ESXi console, press **Alt+F1** and login as **root**.

b. Enter **cd /vmfs/volumes/datastore1/WinOS/**.

c. Edit the WINOS.vmx file. Add the following line: `uuid.action = "keep"`.

d. Save the file in the same location.

e. Enter **cd /vmfs/volumes/datastore1/NCOS/**

f. Edit the NCOS.vmx file. Add the following line: `uuid.action = "keep"`.

g. Save the file in the same location.

Step 3 Log out of ESXi.

WebExUpgradePatch.zip

This patch addresses CSCtx92834 to expand WebEx support to version 2.3.1 and applies to Release 3.3.1.

Note In a clustered deployment, apply this patch to the RM appliance and all RNs.

Step 1 Download **WebExUpgradePatch.zip** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Copy the WebExUpgradePatch.zip file to **\\*mxe-ip-address*\temp**, where *mxe_IP_address* is the IP address assigned to the Cisco MXE 3500 appliance.

Tip If you have Shared Folder Access enabled, you may be prompted for a password. Enter the username as **mxe-user** and the password you created.

Step 3 RDC to the IP_address of the RM or RN appliance you want to apply the patch to.

Step 4 Go to **Start > Run**, and enter \\*mxe-ip-address***temp**. The contents of the \\*mxe-ip-address*\temp folder are displayed.

Step 5 Copy **WebExUpgradePatch.zip** to the desktop.

Step 6 Unzip **WebExUpgradePatch.zip**. The contents are extracted into **WebExUpgradePatch**.

Step 7 Navigate to the WebExUpgradePatch folder and unzip WebEx.zip. The contents are extracted to **WebExUpgradePatch**\WebEx.

Step 8 Navigate to the WebEx folder, and double click on **WebExUpgrade.ba**t.

Step 9 Check status of the upgrade at c:\mxe\system\upgrade\winos\upgrade.log.

Step 10 After the final status displays as `Patch Applied Successfully`, restart the Windows OS for the changes to take effect.

H264PatchZip

This patch addresses CSCty71814 and applies to Release 3.3.1.

Note In a clustered deployment install the patch on the RM and each RN. Use the IP address of the RM appliance when applying the patch to the RNs.

Step 1 Download **H264PatchZip.zip** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Copy the patch to **\\*mxe_ip_address*\media**, where *mxe_ip_address* is the IP address of the RM appliance.

Tip If you have Shared Folder Access enabled, you may be prompted for a password. Enter the username as **mxe-user** and the password you created.

Step 3 RDC to the IP address of the RM or RN appliance you want to apply the patch to.

Step 4 Go to **Start > Run**, and enter **\\*mxe_ip_address*\media**. The contents of the \\mxe_ip_address\media folder are displayed.

Step 5 Copy **H264Patchzip.zip** to the desktop.

Step 6 Unzip **H264Patch.zip**.

Step 7 Navigate to the H264Patch folder, and double click on **H264Patch.bat**.

Step 8 Check the status of the upgrade at **C:\mxe\system\upgrade\winos\upgrade.log**.

MaxQueueLengthSaveReport

This software patch addresses CSCua96966 and applies to Release 3.3.0 and Release 3.3.1.

Note In a clustered deployment install the patch on the RM.

Step 1 Download **MaxQueueLength.zip** and **MaxQueueLengthSaveReport.zip** from **Media Experience Engine Patches > 3.3.0** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 RDC to the IP_address of the RM appliance you want to apply the patch to.

Step 3 Copy **MaxQueueLength.zip** and **MaxQueueLengthSaveReport.zip** to **c:\temp**.

Step 4 Unzip **MaxQueueLength.zip** and **MaxQueueLengthSaveReport.zip**. Two directories are created: MaxQueueLength and MaxQueueLengthSaveReport.

Step 5 Go to **Start > Run** and enter **cd c:\temp\MaxQueueLength**.

Step 6 Enter **run MaxQueueLength.bat** to install the patch.

Step 7 Enter **cd c:\temp\MaxQueueLengthSaveReportPatch**.

Step 8 Enter **run MaxQueueLengthSaveReport.bat** to install the patch.

Multicast Checksum Issue

This patch addresses CSCtu37637 and applies to Release 3.3.0 and Release 3.3.1.

Step 1 Download **MulticastChecksum.tarz** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Copy the patch to \\*mxe-ip-address***temp**, where *mxe-ip-address* is the IP address assigned to the Cisco MXE 3500 appliance.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

Step 4 At the command prompt, enter the following commands in the order shown:

```
cd /mnt/temp
tar -xzvf MulticastChecksum.tarz
cd /opt/cisco/mxe/multicastout/bin/
/sbin/service multicastout stop
mv multicastout multicastout.old
mv /mnt/temp/multicastout  /opt/cisco/mxe/multicastout/bin/
/sbin/service multicastout start
```

Step 5 Exit the command shell and SSH session.

Incorrect Subnet Mask Patch

This patch addresses CSCtr74486 and applies to Release 3.3.1 and Release 3.3.2. This procedure must be repeated on all Cisco MXE 3500 appliances, Resource Manager (RM) and Resource Node (RN).

Step 1 Verify that there are no jobs running on the Cisco MXE 3500.

Step 2 Download **CSCtr74486.zip** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 3 Copy the patch to \\*mxe_ip_address***temp**, where *mxe_ip_address* is the IP address assigned to the Cisco MXE 3500 appliance.

Step 4 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

Step 5 At the command prompt, enter the following commands in the order shown:

```
cd /mnt/temp
```

```
unzip CSCtr74486.zip
cd CSCtr74486
run fix_netmask.sh
```

Step 6 RDC to the Windows VM. Navigate to the **C:\shared\CSCtr74486** directory.

Step 7 Double-click the **fix_netmask.bat** file to execute the patch.

Step 8 Exit the command shell and SSH session.

MP4 Ingest Anomalies Patch

This patch addresses CSCud62652 and applies to Release 3.3.1 and Release 3.3.2. This procedure must be repeated on all Cisco MXE 3500 appliances, Resource Manager (RM) and Resource Node (RN).

Step 1 Verify that there are no jobs running on the Cisco MXE 3500.

Step 2 Download **CSCud62652.zip** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 3 Copy the patch to \\*mxe_ip_address***temp**, where *mxe_ip_address* is the IP address assigned to the Cisco MXE 3500 appliance.

Step 4 RDC to the IP address of the RM or RN appliance you want to apply the patch to.

Step 5 Go to **Start > Run**, and enter **\\*mxe_ip_address*\temp**. The contents of the \\mxe_ip_address\temp folder are displayed.

Step 6 Copy **CSCud62652.zip** to the desktop.

Step 7 Unzip **CSCud62652.zip**.

Step 8 Navigate to the PrefilterPatch folder under **CSCud62652**, and double click on **prefilter.bat**.

Rename Command Failure Patch

This patch addresses CSCud67680 and applies to Release 3.3.1 and Release 3.3.2. This procedure must be repeated on all Cisco MXE 3500 appliances, Resource Manager (RM) and Resource Node (RN).

Step 1 Verify that there are no jobs running on the Cisco MXE 3500.

Step 2 Download **CSCud67680.zip** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 3 Copy the patch to \\*mxe_ip_address***temp**, where *mxe_ip_address* is the IP address of the RM appliance.

Step 4 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

Step 5 At the command prompt, enter the following commands in the order shown:

```
cd /mnt/temp
unzip CSCud67680.zip
cd CSCud67680
```

run sh fix_mount_options.sh

Step 6 Exit the command shell and SSH session.

Samba Denial of Service Patch

This patch addresses CSCui19998 and applies to Release 3.3.0, Release 3.3.1, and Release 3.3.2. This procedure must be repeated on all Cisco MXE 3500 appliances, Resource Manager (RM) and Resource Node (RN).

Step 1 Verify that there are no jobs running on the Cisco MXE 3500.

Step 2 Download the patch from Media Experience Engine Patches:
http://software.cisco.com/download/release.html?mdfid=282815279&flowid=29121&softwareid=282988657&release=3.3.2&relind=AVAILABLE&rellifecycle=&reltype=latest

a. For Release 3.3.2, download **CSCui19998_samba-patch_3.3.2.zip**.

b. For Release 3.3.0 and 3.3.1, download **CSCui19998_samba-patch_3.3.1.zip**.

Step 3 Copy the patch to \\mxe_ip_address\temp, where *mxe_ip_address* is the IP address assigned to the Cisco MXE 3500 appliance.

Step 4 SSH to the ip_address of the RM or RN appliance (via putty) and select **System Command Prompt**.

a. Cd to **/mnt/temp**.

b. Run the command unzip **CSCui19998_samba-patch_3.3.2.zip** or **CSCui19998_samba-patch_3.3.1.zip**.

c. Cd to **3.3.2-samba patch** or **3.3.1-samba patch**.

d. Run the command **unzip vulnerability-samba-patch-3.3.2.zip** or **unzip vulnerability-samba-patch-3.3.1.zip**.

e. Cd to **vulnerability-samba-patch**.

f. Run the command **sh vulnerability-samba-patch.sh**.

Step 5 Exit the command shell and SSH session.

Apache Struts2 Patch

This patch addresses CSCui48757 and applies to Release 3.3.0, Release 3.3.1, and Release 3.3.2. This procedure must be repeated on all Cisco MXE 3500 Resource Manager (RM) appliances.

Step 1 Verify that there are no jobs running on the Cisco MXE 3500.

Step 2 Download the **StrutsPatch_CSCui48757.zip** patch from Media Experience Engine Patches:
http://software.cisco.com/download/release.html?mdfid=282815279&flowid=29121&softwareid=282988657&release=3.3.2&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 3 Copy the patch to \\mxe_ip_address\temp, where *mxe_ip_address* is the IP address assigned to the Cisco MXE 3500 RM appliance.

Step 4 SSH to the ip_address of the RM appliance (via putty) and select **System Command Prompt**.

a. Cd to **/mnt/temp**.

b. Run the command **unzip StrutsPatch_CSCui48757**.

c. Cd to **StrutsPatch**.

d. Run **sh UpgradeStruts.sh**.

Step 5 Exit the command shell and SSH session.

Pulse Analytics Patches

Analytics.tar.gz

This patch addresses CSCty14628 and CSCtx96304 for Pulse Video Analytics and applies to Release 3.3.1.

Note In a clustered deployment install the patch on the RM and each RN. Use the IP address of the RM appliance when applying the patch to the RNs.

Step 1 Download **PulseSpeakerRecoThreshAndSSRDB.tar.gz** from **Media Experience Engine Patches > 3.3.1** http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Save the file to a Unix server that the Cisco MXE 3500 can access.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu. The command prompt displays.

Step 4 Enter **cd /tmp** to change directory.

Step 5 Copy the patch by entering **scp** *ip_address***:** *path* where *ip_address: path* is the IP address of the machine and directory path to the patch that you downloaded. You should now see the file **PulseSpeakerRecoThreshAndSSRDB.tar.gz** in the /tmp folder.

Step 6 Enter **su** to enter super user mode.

Step 7 Enter **tar -xvzf PulseSpeakerRecoThreshAndSSRDB.tar.gz** to untar the file. You should see an *analytics* folder in the */tmp* folder.

Step 8 Enter **cd /analytics** to change directory.

Step 9 Enter these commands to stop the following services:

/sbin/service mtagger stop

```
/sbin/service ssrdb stop
```

Step 10 Enter these commands to copy the patch files to the following directories:

```
cp sid.config /opt/system/netsensor/bin/supp/
cp ssrdb /etc/init.d/
```

Step 11 Enter these commands to restart following services:

```
/sbin/service ssrdb start
/sbin/service mtagger start
```

Step 12 Exit command shell and SSH session.

Analytics_patch_2.tar.gz

This patch addresses CSCtx99530, CSCtz14706, CSCtz18505, CSCtz13241, and CSCtx81886 for Pulse Video Analytics and applies to Release 3.3.1.

Note In a clustered deployment install the patch on the RM and each RN. Use the IP address of the RM appliance when applying the patch to the RNs.

Step 1 Download **analytics_patch_2.tar.gz** from
Media Experience Engine Patches > 3.3.1
http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Save the file to a Unix server that the Cisco MXE 3500 can access.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu. The command prompt displays.

Step 4 Enter **cd /tmp** to change directory.

Step 5 Copy the patch by entering **scp** *ip_address***:** *path* where *ip_address: path* is the IP address of the machine and directory path to the patch that you downloaded. You should now see the file analytics_patch_2.tar.gz in the /tmp folder.

Step 6 Enter **su** to enter super user mode.

Step 7 Enter **tar -xvzf analytics_patch_2.tar.gz** to untar the file. You should see an *analytics_patch_2* folder in the */tmp* folder.

Step 8 Enter **cd /analytics_patch_2** to change directory.

Step 9 Enter these commands to stop the following services:

```
/sbin/service mtagger stop
```

Choose **OK** when you see this message on the console:

```
Stopping MediaTagger Service (mtagger):          [  OK  ]
```

```
/sbin/service ssrdb stop
```

Choose **OK** when you see this message on the console:

```
Stopping SpeakerId Repository DB Service (ssrdb):          [  OK  ]
```

Step 10 Enter these commands to copy the patch files to the following directories:

```
cp target/bin/* /opt/cisco/csalt/ssr/bin/
cp target/lib/* /opt/cisco/csalt/ssr/lib/
cp target/lib/* /opt/system/netsensor/lib
```

Step 11 Enter these commands commands to restart following services:

/sbin/service ssrdb start

Choose **OK** when you see this message on the console:

```
Starting SpeakerId Repository DB Service (ssrdb):     [  OK  ]
```

/sbin/service mtagger start

Choose **OK** when you see this message on the console:

```
Starting MediaTagger Service (mtagger):               [  OK  ]
```

Step 12 Exit command shell and SSH session.

Backup_filelist

This patch addresses CSCuc84113 for Pulse Video Analytics and applies to Release 3.3.1.

Note In a clustered deployment, install the patch on only the RM.

Step 1 Download **backup_filelist** from
Media Experience Engine Patches > 3.3.1
http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Save the file to a Unix server that the Cisco MXE 3500 can access.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu. The command prompt displays.

Step 4 Copy backup_filelist to the scripts folder:

cp backup_filelist /opt/mgmt/scripts

Step 5 Exit command shell and SSH session.

Step 6 Run a backup.

Draft-Processing State Issue

This workaround addresses CSCtx20390 for Pulse Video Analytics: Rarely, videos uploaded to Cisco Show and Share remain in the Draft-Processing state and do not complete processing. It applies to Release 3.1 and Release 3.3.1.

Step 1 SSH to *mxe_IP_address*, login as **root**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu.

Step 2 At the command prompt, open **jetty.xml** with a text editor, such as vi:

vi /opt/cisco/search/etc/jetty.xml

Step 3 Find the following text (line#48):

```
<Call name="addConnector">
  <Arg>
    <New class="org.mortbay.jetty.nio.SelectChannelConnector">
```

```
      <Set name="maxIdleTime">30000</Set>
      <Set name="Acceptors">2</Set>
      <Set name="confidentialPort">8443</Set>
    </New>
  </Arg>
</Call>
```

Step 4 Add the **headerBufferSize parameter** as shown:

```
<Call name="addConnector">
  <Arg>
    <New class="org.mortbay.jetty.nio.SelectChannelConnector">
      <Set name="maxIdleTime">30000</Set>
      <Set name="Acceptors">2</Set>
      <Set name="confidentialPort">8443</Set>
   <Set name="headerBufferSize">20000</Set>
    </New>
  </Arg>
</Call>
```

Step 5 Save the file.

Step 6 Enter **/sbin/service search restart** to restart the search service.

Step 7 Exit the command shell and SSH session.

AnalyticsPatches-3.3.x-feb-2013

This patch applies to CSCue26022, CSCud11339, CSCud62509, CSCue25992 and to Release 3.3.2 and Release 3.3.1.

Note You must install this patch again if you upgrade to Release 3.3.2 from 3.3.1.

Note In a clustered deployment, install the patch on only the RM.

Before You Upgrade to Release 3.3.2

If you have (1) applied this patch to Release 3.3.1 and are upgrading to Release 3.3.2 or (2) have upgraded from Release 3.3.0 to 3.3.1, complete these steps before you begin:

1. SSH to the Linux VM and enter **sbin/service analytics stop** to stop the analytics service.
2. Check if **/db/data/postmaster.pid** and, if so, remove it if it.
3. Enter **/sbin/service analytics start** to restart the analytics service.

To apply this patch to Release 3.3.2 or 3.3.1:

Step 1 Download **analyticsPatches-3.3.x-feb-2013** from
Media Experience Engine Patches > 3.3.X
http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Save the file to a Unix server that the Cisco MXE 3500 can access.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu. The command prompt displays.

Step 4 Enter **cd /tmp** to change directory.

Step 5 Copy the patch by entering **scp** *ip_address***:** *path* where *ip_address: path* is the IP address of the machine and directory path to the patch that you downloaded. You should now see the file **analyticsPatches-3.3.x-feb-2013** in the /tmp folder.

Step 6 Enter **tar xzvf analyticsPatches-3.3.x-feb-2013** to untar the file. You should see an *analyticsPatches-3.3.x-feb-2013* folder in the */tmp* folder.

Step 7 Enter **cd analyticsPatches-3.3.x-feb-2013** to change directory.

Step 8 Enter this command to apply the patch:

```
sh ./patchAnalytics.sh
```

Step 9 Exit command shell and SSH session.

AnalyticsMemoryIssue Patch

This patch applies to CSCue93265 and CSCue93280 and to Release 3.3.2 and Release 3.3.1.

Note You must install this patch again if you upgrade to Release 3.3.2 from 3.3.1.

Note In a clustered deployment, install the patch on only the RM.

Step 1 Download **analyticsMemoryIssue.tar.gz** from
Media Experience Engine Patches > 3.3.X
http://www.cisco.com/cisco/software/type.html?mdfid=282815279&flowid=29121.

Step 2 Save the file to a Unix server that the Cisco MXE 3500 can access.

Step 3 SSH to *mxe_IP_address*, log in as **admin**, and select System Command Prompt from the Cisco MXE Appliance Configuration Menu. The command prompt displays.

Step 4 Enter **cd /tmp** to change directory.

Step 5 Copy the patch by entering **scp** *ip_address***:** *path* where *ip_address: path* is the IP address of the machine and directory path to the patch that you downloaded. You should now see the file **analyticsMemoryIssue.tar.gz** in the /tmp folder.

Step 6 Enter **tar -xvzf analyticsMemoryIssue.tar.gz** to untar the file. You should see an *analyticsMemoryIssue* folder in the */tmp* folder.

Step 7 Enter **cd analyticsMemoryIssue** to change directory.

Step 8 Enter these commands to stop the following services:

```
/sbin/service mtagger stop
Stopping MediaTagger Service (mtagger):                  [  OK  ]
/sbin/service ssrdb stop
Stopping SpeakerId Repository DB Service (ssrdb):                 [  OK  ]
```

Step 9 Enter these commands to copy the patch files to the following directories:

```
cp target/bin/* /opt/cisco/csalt/ssr/bin/
    cp: overwrite `/opt/cisco/csalt/ssr/bin/SSRCollect'? y
    cp: overwrite `/opt/cisco/csalt/ssr/bin/SSRCollect_filebased'? y
    cp: overwrite `/opt/cisco/csalt/ssr/bin/SSRConnect'? y
cp target/lib/* /opt/cisco/csalt/ssr/lib/
cp target/lib/* /opt/system/netsensor/lib
```

Step 10 Enter these commands commands to restart following services:

```
/sbin/service ssrdb start
Starting SpeakerId Repository DB Service (ssrdb):          [  OK  ]
/sbin/service mtagger start
Starting MediaTagger Service (mtagger):                  [  OK  ]
```

Step 11 Exit command shell and SSH session.

Documentation Updates

This is the documentation update for Release 3.3:

Quick Start Hardware Installation Guide for Cisco Media Experience Engine 3500 (Release 3.3) "Powering and Configuring the Cisco MXE 3500" Section

Added the following note between Step 3 and Step 4:

Step 3: Press **Alt+F1** and then press **Enter.**

Note Wait a few minutes while the system boots. You will get a login prompt when the system is ready.

Step 4: Log in with the following default credentials:

- User Name: **admin**
- Password: **change_it**

Related Documentation

For a list of available Cisco MXE 3500 documentation, see the *Guide to Documentation for Cisco Media Experience Engine 3500* at the following URL:

http://www.cisco.com/en/US/products/ps9892/products_documentation_roadmaps_list.html

Getting Information About Accessibility and Cisco Products

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

Providing Documentation Feedback

To provide feedback on this Cisco MXE 3500 document, or to report an error or omission, you can use the online, Embedded Feedback form that appears on the left side of the screen at the following URL:

http://www.cisco.com/en/US/docs/video/mxe/3500/sw/3_x/release/note/mxe3500rn_33.html

Alternatively, you can send feedback to mxe-doc@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.

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