Unified Communications Manager / Unity Connection / Emergency Responder / Unified Communications Manager IM and Presence ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512 COP File

Release Notes Version1
May 12, 2022

Introduction:

These release notes contain important information about the installation procedures for the COP file for Cisco Unified Communications Manager, Unity Connection, Emergency Responder, UCM IM & Presence. This COP file is designed for and tested on Cisco Unified Communication Manager and UCM IM & Presence 11.5, 12.5 and 14 releases. This COP is designed for and tested on Unity Connection and Emergency Responder 12.5, 14 releases.

Note: Before you install this update, Cisco recommends that you review the *Important Notes* section for information about issues that may affect your system.

What this COP file provides:

This COP file contains changes or patches for supporting successful upgrade to latest 14SU2 (containing CiscoSSL7 changes) for a system in FIPS. SHA1 RSA signature is not supported with latest CiscoSSL, which causes issues in some cases when trying to upgrade FIPS enabled systems to 14SU2. See the table below for an explanation of when the COP file is needed. In all cases, the COP file should be installed on the indicated node(s) prior to starting the 14SU2 upgrade.

Upgrade Options which requires COP deployment

	CUCM Only Cluster		CUCM + IMP Cluster	
Direct standard upgrade & Simple Upgrade from 12.5, 14, 14su1 to 14su2	Do not switch version after upgrade	No special handling needed	Do not switch version after upgrade	Install COP on IMP SUB nodes
	Automatic switch version after upgrade	No special handling needed	Automatic switch version after upgrade	Install COP on IMP PUB-SUB nodes
Direct refresh upgrade from 11.5 to 14su2	Do not switch version after upgrade	Install COP on CUCM SUB before upgrade	Do not switch version after upgrade	Install COP on CUCM SUB and IMP SUB
	Automatic switch version after upgrade	No special handling needed	Automatic switch version after upgrade	Install COP on IMP PUB-SUB nodes
Direct standard upgrade from 12.5, 14, 14su1 to 14su2 using PCD in FIPS mode	Do not switch version after upgrade	Install COP on CUCM PUB-SUB nodes	Do not switch version after upgrade	Install COP on CUCM and IMP PUB-SUB nodes
Direct refresh upgrade from 11.5 to 14su2 using PCD in FIPS mode	Use PCD in non FIPS mode and Install COP on CUCM nodes		Use PCD in non FIPS mode and Install COP on CUCM and IMP nodes	
Direct migration to 14 SU2 via PCD migration tasks, with PCD in FIPS mode	Install COP on All nodes of the Cluster		Install COP on All nodes of the Cluster	
Direct migration via Fresh Install with Data Import from 10.5, 11.x, 12.x, 14x to 14su2	No special handling needed		No special handling needed	

Upgrade Options which requires COP deployment

	CUC Cluster		CER Cluster	
Direct standard upgrade & Simple Upgrade from 12.5, 14, 14su1 to 14su2	Do not switch version after upgrade	Install COP on CUC PUB-SUB nodes	Do not switch version after upgrade	No special handling needed
	Automatic switch version after upgrade	NA	Automatic switch version after upgrade	No special handling needed
Direct refresh upgrade from 11.5 to 14su2	Do not switch version after upgrade	NA	Do not switch version after upgrade	No special handling needed
	Automatic switch version after upgrade	No special handling needed	Automatic switch version after upgrade	No special handling needed
Direct standard upgrade from 12.5, 14, 14su1 to 14su2 using PCD in FIPS mode	Do not switch version after upgrade	Install COP on CUC PUB-SUB nodes	Do not switch version after upgrade	No special handling needed
Direct refresh upgrade from 11.5 to 14su2 using PCD in FIPS mode	Use PCD in non FIPS mode		Use PCD in non FIPS mode	
Direct migration to 14 SU2 via PCD migration tasks, with PCD in FIPS mode	NA		NA	
Direct migration via Fresh Install with Data Import from 10.5, 11.x, 12.x, 14x to 14su2	No special handling needed		NA	

Image(s): COP upgrade cases

This COP provides these fix(es):

- CSCwa48315 Subscriber L2 upgrade fail during upgrade to 14SU2 due to unsupported SSH algorithm in FIPS mode

- CSCwa77974 RU upgrade from 11.5 to 14su2 fails in FIPS mode due to CiscoSSL7 upgrade

Determining the Software Versions:

Cisco Unified Communications Manager

You can determine the System Version of the Cisco Unified Communications Manager software that is running on your server by accessing Cisco Unified Operating System Administration Web page.

The following information displays:

- System version: xxxxx

Important Notes:

This COP is applicable for the system in FIPS mode (for mentioned cases in above image). Applying the COP multiple times will not cause any issues; if installed more than once (or) in non-fips, the installation will exit without making any changes to the system.

NOTE:
For Centralized-IM&P cluster deployments, the COP applicability is same as Standard IM&P cluster deployment as mentioned in the table above.

NOTE:
Attempting the COP file install on a system in non-fips (or) on an unsupported product in fips, it will result in the following message being displayed:

Installation of ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512 failed

Copstart script of /common/download/ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop failed

A system reboot is required when the upgrade process completes or is canceled. This will ensure services affected by the upgrade process are functioning properly.

It is unnecessary to reboot if the failure reason is because the fix is already present. Be sure to check the messaging above the reboot message to see the specific reason for the "failure".

Installation Instructions:

As with any installation or upgrade, it is recommended that you apply this update during off peak hours.

No reboot is required as part of the COP file install.

***Caution*: *The updates applied with this COP cannot be uninstalled*.** Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide

From Remote Source:

Step 1: Download, **ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512**

Step 2: Copy the cop file to an ftp or sftp server.

Step 3: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://server-name/cmplatform

Where server-name is the host name or IP address of the admin server.

Step 4: Enter your OS Administrator username and password.

Step 5: Choose Software Upgrades > Install/Upgrade.

Step 6: For the software location source, choose Remote Filesystem.

Step 7: Enter the directory name for the cop file, if required.

If the cop file is located on a Linux or UNIX server, you must enter a forward slash at the beginning of the directory path. For example, if the cop file is in the patch's directory, you must enter /patches.

If the cop file is located on a Windows server, check with your system administrator for the correct directory path.

Step 8: Enter the required cop file information as described in the following table:

Server:	Host name or IP address of the remote server from which software will download.
User Name:	Name of a user configured on the remote server.
User Password:	Password configured for this user on the remote server.
Transfer Protocol:	Choose sftp or ftp.

Step 9: To continue the installation of cop file, click Next.

Step 10: Choose "**ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512**" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename. When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:
(MD5): 17e18aa27034f968ac0e4ea210890ef9

Step 13: After determining that the checksums match, click Next to proceed with the software upgrade.

Step 14: The Installation Status window displays the Status and File Name, Installation log window displays the install logs.

Step 15: Verify Installation Status as Complete.

Step 16: When the installation completes, it will display "Successfully installed ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512 Locale ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop has been installed successfully."

Step 17: Verify the COP file version using this command from the CLI:
　　　　　admin: show version active
　　　　　　Active Master Version: <CUCM_Version>
　　　　　　Active Version Installed Software Options:
　　　　　　ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop