Cisco Unified Communications Manager
CSCve31804 COP File

Release Notes Version 1
July 20, 2017

Introduction:

These release notes contain important information about the installation procedures for the COP file for Cisco Unified Communications Manager 11.5(1). This COP file, ***ciscocm.ldap_ssl_certificateNotVerified_fix_v1.3-k3.cop.sgn***, is only designed for and has only been tested with CUCM 11.5(1).

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 makes the required changes to address the following issue:

CSCve31804 - **LDAP Certificate not verified error when saving under LDAP Directory**

Related Documentation:

To view documentation that supports your version Cisco Unified Communications Manager release, go to:
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html

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:

Applying the COP multiple times will not cause any issues; if installed more than once, the installation will exit without making any changes to the system.

Installation Instructions:

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

Apply this COP to all nodes in the cluster.

Applying this update will require a tomcat restart.

***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.ldap_ssl_certificateNotVerified_fix_v1.3-k3.cop.sgn**

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 File System.

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 patches 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:

Remote Server:	Host name or IP address of the remote server from which software will be downloaded.
Remote User:	Name of a user who is configured on the remote server.
Remote Password:	Password that is configured for this user on the remote server.
Download Protocol:	Choose sftp or ftp.

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

Step 10: Choose "**ciscocm.ldap_ssl_certificateNotVerified_fix_v1.3-k3.cop.sgn**" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:

MD5 Hash Value: c5:87:98:b4:88:b1:63:80:6e:c4:aa:19:01:d6:41:98

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

A Warning window displays the selected option.

Step 14: Click Install.

The Install Status window displays and displays the install log.

Step 15: When the installation completes, a Tomcat service restart is required.

Applications which are deployed in Tomcat will be accessible about 10 to 15 mins after the Tomcat service restarts.

Step 16: 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.ldap_ssl_certificateNotVerified_fix_v1.3-k3.cop.sgn