

# Cisco Unified Communications Manager VMwareTools2016a COP File

Release Notes Version 1  
Apr 19, 2016

## **Introduction:**

These release notes contain important information about the installation procedures for the VMwareTools2016a COP file for Cisco Unified Communications Manager 10.5(2) and 11.0(1). This COP file, *ciscocm.VMwareTools2016a.cop.sgn*, is only designed for and has only been tested with CUCM 10.5(2) and 11.0(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:**

VMware tools upgrade fails due to various Selinux denials and the VM summary tab shows VMware tools **Not Running / Not Installed**. The cop file will update the Selinux Policy files so that VMWare tools upgrade happens properly. This COP file also enables the CLI command “utils vmtools caf-logs delete” which can be used to delete CAF logs which takes up disk space.

The enhancements listed above are already included in Engineering Specials (ES) or Service Update (SU) releases via the following Bug ID:

[CSCux90747](#): VMware Tools 10.0 update fails on CUCM 10.5/11.0 with selinux denials

Consult the **Known Fixed Releases:** field in the [Bug Search](#) tool to determine which ES's and SU's include these fixes.

## **Resolution**

You must follow steps below to install the VMwareTools2016a update.

## **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
- VMware Installation: xxxxx

## **Important Notes:**

The fixes provided in this COP file may not be available in older 10.5(2) and 11.0(1) ES's or SU's. If an ES or SU is installed after this update that does not contain all of the fixes listed above, the COP file will need to be reapplied. Consult the **Known Fixed Releases:** field in the [Bug Search](#) tool to determine which ES's and SU's include these fixes.

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 reboot.

This package will install on the following System Versions:

- 10.5.2.10000-xx or any higher version starting with 10.5.2.xxxxx
- 11.0.1.10000-xx or any higher version starting with 11.0.1.xxxxx

**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.VMwareTools2016a.cop.sgn*

*Step 2:* Copy the upgrade 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 software upgrade, if required.

If the upgrade 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 upgrade file is in the patches directory, you must enter /patches.

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

*Step 8:* Enter the required upgrade 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 upgrade process, click Next.

*Step 10:* Choose "*ciscocm.VMwareTools2016a.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:

9281116652d842c7cde79ea16af39d09

SHA512:

42ef2906f5b2da92dc5c4be924878de96e3cc74f9f7c611dfb28608e95e5aafa4d3c98c95558fa77bbf6642e3

4c43dcaee7b5a6f45c5944a819f3b90b976eeae

*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, click Finish and reboot the server.

*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.VMwareTools2016a.cop

*Step 17:* Run “utils vmtools caf-logs delete” <If you want to delete the CAF logs>