



ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU1

Revision 3

Updated January 3, 2017

Changes in this revision, Revision 3

Added a new Open Caveat: [CSCva82202](#)

Changes in Revision 2

- Added a new Open Caveat: [CSCvb00248](#)

This ReadMe file discusses the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Version and Description, page 2](#)
- [Important Notes, page 3](#)
- [Firmware Upgrade Issues, page 3](#)
- [Related Documentation, page 3](#)
- [Before You Begin, page 4](#)
- [Installation Instructions, page 4](#)
- [Reverting to a Previous Version, page 5](#)
- [Caveats, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 12](#)



Note

To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL:

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-call-manager/products-release-notes-list.html>



Americas Headquarters:

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

**Note**

Please review all sections in this document pertaining to installation before you install this Service Update (SU). Failure to install this SU as described may result in inconsistent Cisco Unified Communications Manager behavior.

Before you install Cisco Unified Communications Manager, Cisco recommends that you review the “Important Notes” section on page 3 for information about issues that may affect your system.

Introduction

This 11.5(1)SU1 ReadMe file contains important information about installation procedures and resolved caveats for Cisco Unified Communications Manager release 11.5(1)SU1. This SU can be applied to Cisco Unified Communications Manager, Business Edition 6000, Session Management Edition, and Cisco Unity Connection.

System Requirements

The following sections comprise the system requirements for this release.

Server Support

In this release, you cannot install or run Cisco Unified Communications Manager on server hardware; you must run these applications on virtual machines. Please refer to the “Platform requirements” section of the *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* for additional details:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/11_5_1/cucm_b_upgrade-guide-cucm-115.html

Uninterruptible Power Supply

Ensure that you connect each node to an uninterruptible power supply (UPS) to provide backup power and protect your system.

**Caution**

Failure to connect the Cisco Unified Communication Manager nodes to a UPS may result in damage to physical media and require a new installation of Cisco Unified CM.

Version and Description

This SU is a cumulative update that incorporates all of the fixes and changes from Cisco Unified Communications Manager 11.5(1) along with additional changes that are specific to this SU.

**Note**

You can only install this SU on Cisco Unified Communications Manager Release 6.1(4x), 6.1(5x), 7.1(3x), 7.1(5x), 8.0(x), 8.5(1x), 8.6(x), 9.0(x), 9.1(x), 10.0(1), 10.5(x), 11.0(1x), or 11.5(1). This SU will not install over any 11.5(1)ES's. Upgrades from 6x through 10x need to be requested via PUT (www.cisco.com/upgrade) to obtain the necessary license. This SU should not be installed on a Business Edition 3000 server.

See the Compatibility Matrix for further details:

<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-call-manager/products-device-support-tables-list.html>

New to this Release

The following enhancements were introduced in 11.5(1)SU1:

- Enhanced Security Mode implementation.

Important Notes

SUs do not impact system compatibility unless specifically stated.

Cisco provides the following guidance to help you successfully upgrade Cisco Unified Communications Manager software:

- To minimize call-processing interruptions during the upgrade process, register all devices to servers that are running the same version of Cisco Unified Communications Manager software. Make sure that you register all devices to the backup Cisco Unified Communications Manager server or to the primary Cisco Unified Communications Manager server, but not to both the backup and primary servers.

Firmware Upgrade Issues

For all SCCP and SIP firmware upgrades from firmware release versions earlier than 8.3(3) to version 8.5(2)SR1 or greater, you must first upgrade your firmware to version 8.5(2). Once you have upgraded to version 8.5(2), you can upgrade your IP Phone to version 8.5(2)SR1 or later. Refer to the *Firmware Versions in this Release* section of this document to determine the firmware load provided in this SU.

For additional details, Firmware Upgrade Instructions, and Firmware Download locations please see:

SCCP

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/firmware/8_5_2/english/release/notes/7900_852SR1.html#wp57602

SIP

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/firmware/8_5_2/english/release/notes/7900_852SR1.html#wp147343

Related Documentation

To view documentation that supports Cisco Unified CM Release 11.5(x), go to:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/11_5_1/cucm_b_documentation-guide-cucm-imp-1151.html

Before You Begin

Before you upgrade the software version of Cisco Unified Communications Manager, verify your current software version.

To do that, open Cisco Unified Communications Manager Administration. The following information displays:

- Cisco Unified Communications Manager Administration System version

Installation Instructions



Note

Apply this SU to all of your Cisco Unified Communications Manager servers, beginning with the publisher server and TFTP server.

Refer to the *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* for detailed information about doing this upgrade:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/11_5_1/cucm_b_upgrade-guide-cucm-115.html



Note

Because the 11.5.1.11900-26 build is a non-bootable ISO, it proves useful only for upgrades. You cannot use it for new installations. You may however install with the base version 11.5.1.10000-6 and apply 11.5.1.11900-26 as a patch during the installation.

Release 11.5(x) is available in both restricted (which is the release type that has always been available from Cisco) and unrestricted versions of software to comply with import / export restrictions to various countries. The unrestricted version is available in limited markets. Please refer to the “Export Unrestricted” section in the **Upgrade Planning** chapter, of the *Upgrade Guide for Cisco Unified Communications Manager, Release 11.5(1)* referenced above for a more detailed description.



Caution

For both restricted and unrestricted upgrades from an 8.5(x) or earlier release to a 11.5(x) release, a patch (COP file) must be applied prior to initiating the upgrade. Before you upgrade from compatible versions of Unified CUCM, install the COP file named `ciscocm.refresh_upgrade_v1.5.cop.sgn`. Please refer to the “Refresh Upgrades” section in the **Upgrade overview** chapter at the *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* referenced earlier in this document for detailed installation instructions and download location.

The file names and hash values you will use for this upgrade are:

- UCSInstall_UCOS_11.5.1.11900-26.sgn.iso

The **MD5** for the Restricted combined download is: 18d07c7bc2aa50089211ad6e8fd0f8a5

The **SHA-512** for the Restricted combined download is:

d00af059e4c875612c993cdd49bedc0e04bdaebdf2e130db02d6dc37971d342896d26b02448a5540cd0d4a67e45fec3bc31e0079bed7e3ec1d8ccf066f809d46

**Note**

Once installed, UNRST releases can never be converted or upgraded to releases which support full encryption capabilities

For the Unrestricted version:

- UCSInstall_UCOS_UNRST_11.5.1.11900-26.sgn.iso

The **MD5** for the Unrestricted combined download is: 27ad7a05f044fe21b54ce9e84e2bce78

The **SHA-512** for the Unrestricted combined download is:

c8ce470c0c325445cfaa44f408e602030ff7eeff549c89e3eb495f9e6effc7b7c86434937eeb5157bc
41f2d3f1632201c33817ebaceeee22b7c7a82ed958730f

Reverting to a Previous Version

**Note**

Revert the SU on all servers in the cluster in the same order in which you performed the installation.

Refer to the “Switch to Previous Version” section in the **Upgrade Procedures** chapter at *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* for detailed instructions on “Reverting to a Previous Version.”

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/11_5_1/cucm_b_upgrade-guide-cucm-115/cucm_b_upgrade-guide-cucm-115_chapter_0111.html

Caveats

Caveats describe unexpected behavior on a Cisco Unified Communications server. The following sections contain lists and descriptions of resolved and open caveats in this release.

Resolved Caveats

Resolved Caveats for Cisco Unified Communications Manager Release 11.5(1)SU1 describes possible unexpected behaviors in Cisco Unified Communications Manager Release 11.5(1).

Resolved Caveats for Cisco Unified Communications Manager Release 11.5(1)SU1

The following information comprises unexpected behavior that is addressed by this SU of Cisco Unified Communications Manager.

Resolved CUCM Caveats in 11.5(1)SU1

- [CSCva76688](#) : Change the keyword to "EnhancedSecurityMode" in CLI commands and logs
- [CSCuz34436](#) : Audit Logs not Generated
- [CSCva71953](#) : CallPickup not working for phones sending hostname in INVITE-From header
- [CSCva80503](#) : Online Help terminology update for CUCM 11.5(1)
- [CSCva67977](#) : User with apostrophe in username can't log in to IM&P server

[CSCva56740](#) : Main menu missing in SAML Single Sign On Configuration
[CSCuz23871](#) : Invalid remote syslog server delays in logging to valid remote syslog
[CSCux37889](#) : Cisco Unified Communications Manager Apache Struts Vulnerabilities
[CSCva05592](#) : serviceability Connection error thrown when trying to access CUCM SUB from PUB
[CSCuz04727](#) : New APIC EM API Integration (Phase 2)
[CSCva24077](#) : Cannot upload signed certificate to CUCM
[CSCva25596](#) : changing PIN on selfcare showed successful but actually failed
[CSCva28050](#) : [ESM] Contact search auth mode enabled message is shown in IM/P
[CSCva32290](#) : SOAP API selectCmDevice function no longer returns results
[CSCva34863](#) : [ESM] Contact Search auth is showing disabled after migration
[CSCva34890](#) : [ESM] Ccmcip url patterns are not getting added after DB restore
[CSCva43349](#) : Able to create Rank1 user after logging in as Rank2 user
[CSCva43426](#) : Unable to delete lower ranked users from Quick User/Phone Add page
[CSCva47954](#) : [ESM]Misleading securitywarning when FIPS is enabled/disabled in PCD
[CSCva03814](#) : SELinux blocks switch back to old partition after RU failure
[CSCva06831](#) : Need help page text to CUCM Access contorl Group pages for RBAC changes
[CSCva06971](#) : DRS Backup Non Fips algorithms during SFTP Connection in FIPs mode
[CSCva16043](#) : Saml sso does not function after migration
[CSCva26317](#) : SNMP walk returns unsupported security level for v3 user
[CSCva27938](#) : TFTP goes to throttle state when EMCC configured
[CSCva28852](#) : LDAP authentication error due to Null Pointer Exception
[CSCva31517](#) : CONTENT_DIGEST_TAG.len having the wrong value when SHA512 is enabled
[CSCva34874](#) : The cucm mode changes to FiPs from ESM after migration
[CSCva36619](#) : Unable to add a new access control group after logging in as admin user?
[CSCva40071](#) : Sorting of Rank by Name and Description leads to error
[CSCva42803](#) : QED changes adding SHA-512 support for 78xx/88xx phones & Jabber clients
[CSCva42885](#) : End user with Read Only access can create User Rank
[CSCva43327](#) : User rank field shows true or false instead of the ranks
[CSCuz85612](#) : "dbaxlweb" AXL connections are crossing the threshold 100
[CSCva01313](#) : Perfmon counter incorrectly escaped for user with apostrophe in username
[CSCva01767](#) : Remove "TFTP IP Address" and "Server IP Track" TFTP service paramaters
[CSCuz32703](#) : F5185 RBAC changes
[CSCva19546](#) : 'Operation Completes By' code change to maintain backward compatibility
[CSCuy95946](#) : F5185 Audit details for OS admin
[CSCuz40162](#) : CUCM GUI incorrect port numbers in slot 1 of ISR 4451 MGCP gateway
[CSCuz70863](#) : CMUI Link Deprecated Phone Warning to Find/List by Model
[CSCva04753](#) : dtmf test failing in few EO EO scenarios of F4125 SIP DTMF Suite
[CSCva08043](#) : Migration/upgrade failed with Car DB post installation scripts
[CSCva11987](#) : F5185 ESM File perminssion for SNMPD.cnf
[CSCva18439](#) : NGE RSA Cipher Support on JTAPI
[CSCva24151](#) : Regarding the system behaviour issue in PCD system
[CSCva00462](#) : TCP syslog not following RFC
[CSCva04931](#) : Disable User accounts
[CSCuz24801](#) : F5185 - Audit details for DRF
[CSCuz69905](#) : Enable Common Criteria (CC) Mode for UCM and IM/P
[CSCuz85694](#) : UCMUser login failed credentials messaging allows user ID identification
[CSCva02233](#) : Click thru Banner behavior in SSO mode
[CSCva08074](#) : UCM DB update the dbl2j.jar in vob vos to match vob ccm

[CSCuz70820](#) : CMUI - Remove deprecated models from list for Add New Phone/Template
[CSCuz84403](#) : Missing web.xml security constraints for contact search after upgrade
[CSCva07788](#) : CUCM 11.5.1 BAT Insert Phones Specific Details failing with syntax error
[CSCuz51426](#) : DST/TZ data upgrade with 2016d
[CSCuz80519](#) : Add new QED for Cisco TelePresence DX70/80
[CSCva00228](#) : Upgrade rules to prevent 11.5(1) Respins from installing over ES's
[CSCva01131](#) : Expired User Accounts status check Jabber SSO Login during ESM
[CSCva05618](#) : 11.5(1)su1 upgrade rules to prevent install over ineligible ES's
[CSCty67386](#) : Tomcat manager returns HTTP 403 instead of 404 error
[CSCuy41450](#) : CUCM - Tomcat Info Disclosure / Session Fixation / CSRF Token Leak Vuls
[CSCuz32703](#) : F5185 RBAC changes
[CSCuz99226](#) : Multiple logs were getting printed in CiscoSyslog regarding file pointer
[CSCuz93144](#) : Directory Number Alias Server cannot be added
[CSCuz74970](#) : Changes to LDAP Directory pages and Directory Sync for RBAC
[CSCuz30245](#) : DB enhancement to support RBAC (ESM US233304)
[CSCuz24801](#) : F5185 Audit details for DRF

Resolved Cisco Unity Connection Caveats in 11.5(1)SU1

[CSCva43404](#) : CiscoSRTP Integration in Unity
[CSCva50077](#) : Handle LDAP User status (Active/Deleted/Disabled) separately
[CSCva51189](#) : Cisco Unity Connection Apache Struts Vulnerabilities Mitigation
[CSCva52271](#) : Tenant Administrator Role not able to access CUCA/REST APIs on 11.5SU1
[CSCva29467](#) : Checkin CUCA help in Unity Connection 11.5(1) SU 1 build
[CSCuz48146](#) : IMS changes - handle exception in case LDAP User table enduser not found
[CSCva06949](#) : Voicemail PIN not working in SRSV mode for end users
[CSCva14718](#) : CUC Jetty stderrout log is growing enormously
[CSCva43819](#) : Authentication Failure coming on Testing UMA ,Video Services and SRSV .
[CSCva45927](#) : Intra dev US246215 Improvements over Bulk edit operation
[CSCva46198](#) : Displayname not updated when firstname or lastname is updated in huron
[CSCva48035](#) : A user with read access to system can read certificate details in CUC
[CSCva50071](#) : TUI Session count is increased two times when login to VVM first time
[CSCva50233](#) : TUI Logon counter got leaked in failsafe scenario and multiple toggle
[CSCva06658](#) : To remove clear text passwords from audit logs
[CSCva38174](#) : Test button is executed by read only Admin.
[CSCva41630](#) : Do not active the inactive user if user is sync with LDAP
[CSCva43819](#) : Authentication Failure coming on Testing UMA ,Video Services and SRSV .
[CSCuz60244](#) : SSO for RTMT not working
[CSCuz96504](#) : SpeechView Activity Report Truncates Phone Extension
[CSCva00511](#) : CUC prim can't access second service control center for password locked
[CSCva02988](#) : REST API enhancement and hardening privileges
[CSCva27428](#) : Inconsistent behaviour when Disabled User login to Inbox & CiscoPCA
[CSCva33782](#) : SHA512 Value is blank in case of export distribution list members
[CSCuz83826](#) : US240425 and US240426 File Integrity support
[CSCva14310](#) : While configuring an LDAP Directory,getting > Internal error, try again
[CSCva20044](#) : Disable Access of System for SIB accounts
[CSCva24276](#) : IMAP session count values are not updated correctly.
[CSCva26182](#) : Incorrect prompt while login from inactive user

[CSCuz69703](#) : Limit Logon session per user (VVM VMWS interface)
[CSCuz91830](#) : Struts 1.x Vulnerability Mitigation CPCA
[CSCva15757](#) : Error message is displayed wrong in MediaPlayer
[CSCva19663](#) : Python upgrade for CUC libs
[CSCcuy83478](#) : Auto discovery over LDAPS fails for UMS Test Button
[CSCcuy94244](#) : Audit log configuration webpage for CUC Apps should open correctly
[CSCuz06264](#) : Not able to create SIP certificate in FIPS enabled mode
[CSCuz07421](#) : Users are receiving messages even after their mailbox size exceeds.
[CSCuz20806](#) : Jabber unable to access VoiceMail after Upgrade is performed in SSO Mode
[CSCuz26297](#) : Memory leak in XML parser code, when running the common pin scenario
[CSCuz26312](#) : Drs needs to check db consistency before Database backup
[CSCuz29570](#) : Safari 7 and 9 web & mini inbox not loading properly
[CSCuz34688](#) : DRS backup restore failed due to foreign key constraint violation
[CSCuz38131](#) : Read Only Admin issues in Custom Roles
[CSCuz41304](#) : Not able to download after Record and Play
[CSCuz41827](#) : Search dropdown for suggestions shows "??" for NonEnglish search in SRSV
[CSCuz43509](#) : Switch version of CUC fails when coincides with informix schedule task
[CSCuz43902](#) : US232434 Limit Logon session per user (IMAP)
[CSCuz45577](#) : MediaMaster_Uploaded a file greater than 90 secs.
[CSCuz45606](#) : Speed and Volume functionalities are not working on new media player
[CSCuz45869](#) : The CUCA login page is not Scrollable
[CSCuz45997](#) : Custom role with Read Access unable to view serviceability
[CSCuz47007](#) : Video messaging transfer is inconsistent in case of RNA.
[CSCuz48187](#) : Customer Administrator can bulk edit Partner Administrator from CUCA.
[CSCuz48432](#) : CUC Dates for March alternating greeting listed wrongly via TUI
[CSCuz49368](#) : Media Master Distorted in window's 8.1 on IE11 browser.
[CSCuz50263](#) : Read Only Admin can configure Speech Connect ports
[CSCuz50274](#) : Read Only Admin can Bulk Edit COS, DL and delete Task results
[CSCuz50285](#) : Unauthorize error handling is not proper in HTTPS and Custom Keypad page
[CSCuz50309](#) : Ordering of Privileges List of custom role changes post CUC Upgrade
[CSCuz51310](#) : Greeting recorded on publisher does not sync to subscriber server
[CSCuz55172](#) : CUC - Diginet alternate extensions listing remote partitions
[CSCuz60403](#) : ALL LANG lync integrations Permission denied when uploading logon msg
[CSCuz66350](#) : Disable Access of System for Inactive AD User
[CSCuz67974](#) : Disable Access of System for Inactive local user at CUCA,CPCA,REST,Inbox
[CSCuz67977](#) : Enabling and Disabling of Admin users based on inactivity timeout
[CSCuz69703](#) : Limit Logon session per user (VVM VMWS interface)
[CSCuz75437](#) : Hack count doesn't gets reset on successful login through WEB interfaces
[CSCuz79399](#) : Critical operations happening via REST should be audit logged
[CSCuz79587](#) : [INTDEV]US232230 To generate DB schema docs for CUC 11.5
[CSCuz80965](#) : Not getting Caller Name for Outside caller in "Missed call" notification
[CSCuz83764](#) : Upgrade JDK to 1.7.0_101 for 11.5 Release
[CSCuz84727](#) : Large number of partitions can not be searched
[CSCuz86096](#) : JPN conversations - Duplicate checkbox need to be removed
[CSCuz88605](#) : Activ/De activation of Disable identifier feature through config param
[CSCuz91830](#) : Struts 1.x Vulnerability Mitigation CPCA
[CSCva01582](#) : Enhancement for sprint 163

Open Caveats

Open Caveats for Cisco Unified Communications Manager Release 11.5(1)SU1 describes a few of the possible unexpected behaviors still remaining in Cisco Unified Communications Manager Release 11.5(1)SU1. For a complete list of open caveats please access the bug toolkit located at: https://tools.cisco.com/bugsearch?referring_site=btk



Tip

For more information about an individual defect, click the associated Identifier in the to access the online record for that defect, including workarounds.

Open Caveats

[CSCva84316](#): After upgrade platform CLI admin password removed on pub, unable to ssh

[CSCvb00248](#): CUC/CUCM 11.5(1) does not support passwords longer than 15 characters

[CSCva82202](#): TFTP fails to serve updated signed static files

Firmware / Device Loads

SUs contain firmware loads, however, Cisco recommends that you always download the latest firmware load from the Voice Software Download Center.

Phone Firmware

To download phone firmware, follow this procedure:

Step 1 Go <http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240&i=rp>

Step 2 Select **Collaboration Endpoints** in the center column

Step 3 Select **IP Phones** in the right most column

Step 4 Select the desired phone series in the right most column

Step 5 Select the desired phone model in the right most column

Step 6 From the options that display, select the desired software type for your deployment.

Device Packages

Firmware upgrades not explicitly addressed in the Phone Firmware section can be obtained via Dev Packs. To download Dev Packs for this release, follow this procedure:

Step 1 Go <http://www.cisco.com/cisco/software/navigator.html?mdfid=278875240&i=rp>

Step 2 Select **Call Control** in the right most column

Step 3 Select **Unified Communications Manager (CallManager)** in the right most column

Step 4 Select **Unified Communications Manager Version 11.5** in the right most column

Step 5 From the options that display, select **Unified Communications Manager/CallManager Device Packages**

Step 6 From the options that display, select the desired release for your deployment.

Firmware Versions in this Release

Device type	Load name	Version
3905	3905.9-4-1SR2-2	9.4(1SR2.2)
3911_3951-sip	3911_3951-sip.8-1-4a	8.1(4.0)
6608	6608-4.0.0.32-mgcp	4.0(0.32)
6608cfb	6608cfb-4.0.0.03-sccp	4.0(0.3)
6608mtp	6608mtp-4.0.0.06-sccp	4.0(0.6)
6624	6624-4.0.0.13-mgcp	4.0(0.13)
6901-sccp	6901-sccp.9-3-1-SR2-2	9.3(1.0)
6901-sip	6901-sip.9-3-1-SR2-3	9.3(1.0)
6911-sccp	6911-sccp.9-3-1-SR2-3	9.3(1.0)
6911-sip	6911-sip.9-3-1-SR2-4	9.3(1.0)
6945-SCCP	6945-SCCP-9-4-1-3SR2	9.4(1.3)
6945-SIP	6945-SIP-9-4-1-3SR2	9.4(1.3)
69xx-SCCP	69xx-SCCP-9-4-1-3SR2	9.4(1.3)
69xx-SIP	69xx-SIP-9-4-1-3SR2	9.4(1.3)
78xx	78xx.11-5-1-18	11.5(1.18)
7902	7902-8.0.2-sccp	8.0(2.0)
7905	7905-8.0.1.1-sip	8.0(1.1)
7905	7905-8.0.3-sccp	8.0(3.0)
7910	7910-5.0.7.0-sccp	5.0(7.0)
7911_7906-sccp	7911_7906-sccp.9-4-2SR1-1	9.4(2SR1.1)
7911_7906-sip	7911_7906-sip.9-4-2SR1-1	9.4(2SR1.1)
7912	7912-8.0.1.1-sip	8.0(1.1)
7912	7912-8.0.4-sccp	8.0(4.0)
7914-sccp	7914-sccp.5-0-4	5.0(4.0)
7915	7915.1-0-4-2	1.0(4.2)
7916	7916.1-0-4-2	1.0(4.2)
7920-sccp	7920-sccp.3-0-2	3.0(2.0)
7921-sccp	7921-sccp.1-4-6-3	1.4(6.3)
7925-sccp	7925-sccp.1-4-8-4.k3	1.4(8.4)
7926-sccp	7926-sccp.1-4-8-4.k3	1.4(8.4)
7931-sccp	7931-sccp.9-4-2SR1-1	9.4(2SR1.1)
7931-sip	7931-sip.9-4-2SR1-1	9.4(2SR1.1)
7935-sccp	7935-sccp.3-2-19	3.2(19.0)
7936-sccp	7936-sccp.3-3-21	3.3(21.0)
7937	7937-1-4-4-SCCP	1.4(4.0)
7937	7937-1-4-5-7-SCCP	1.4(5.7)
7940-7960	7940-7960-8.12.00-sip	8.12(00.0)
7940-7960-sccp	7940-7960-sccp.8-1-2SR2	8.1(2SR2.0)
7941_7961-sccp	7941_7961-sccp.9-4-2SR1-1	9.4(2SR1.1)
7941_7961-sip	7941_7961-sip.9-4-2SR1-1	9.4(2SR1.1)
7942_7962-sccp	7942_7962-sccp.9-4-2SR1-1	9.4(2SR1.1)
7942_7962-sip	7942_7962-sip.9-4-2SR1-1	9.4(2SR1.1)
7945_7965-sccp	7945_7965-sccp.9-4-2SR1-1	9.4(2SR1.1)

7945_7965-sip	7945_7965-sip.9-4-2SR1-1	9.4(2SR1.1)
7970_7971-sccp	7970_7971-sccp.9-4-2SR1-1	9.4(2SR1.1)
7970_7971-sip	7970_7971-sip.9-4-2SR1-1	9.4(2SR1.1)
7975-sccp	7975-sccp.9-4-2SR1-1	9.4(2SR1.1)
7975-sip	7975-sip.9-4-2SR1-1	9.4(2SR1.1)
7985	7985-4-1-7-0-sccp	4.1(7.0)
8831-sip	8831-sip.10-3-1SR2-2	10.3(1SR2.2)
8845_65-sip	8845_65-sip.11-5-1-18	11.5(1.18)
88xx-sip	88xx-sip.11-5-1-18	11.5(1.18)
894x-sccp	894x-sccp.9-4-2SR2-2	9.4(2SR2.2)
894x-sip	894x-sip.9-4-2SR2-2	9.4(2SR2.2)
8961	8961.9-4-2SR2-2	9.4(2SR2.2)
9951	9951.9-4-2SR2-2	9.4(2SR2.2)
9971	9971.9-4-2SR2-2	9.4(2SR2.2)
ata	ata-3.2.4-sccp	3.2(4.0)
ata187	ata187.9-2-3-1	9.2(3.1)
ata190	ata190.1-2-2-003	1.2(2.3)

Cisco Unity Connection RPMs

CCM Reference Build: 11.5.1.11900-26

Cisco Unity RPMs:

BuiltRPMsList

NRec-10.2.6-14289.x86_64.rpm
 NRec-en-US-10.0.0-10.0.0-12059.i686-linux.rpm
 NSS-6.2.7-14290.i686.rpm
 Nuance-Common-10.2.7-14289.i686.rpm
 Nuance-Common64-10.2.7-14289.x86_64.rpm
 Nuance-NRS64-10.2.7-14289.x86_64.rpm
 Nuance-OAM-10.2.7-14289.i686.rpm
 cuc-11.5.1.11900-1002.i386.rpm
 cuc-base-11.5.1.11900-1002.i386.rpm
 cuc-bin-11.5.1.11900-1002.i386.rpm
 cuc-etc-11.5.1.11900-1002.i386.rpm
 cuc-install-11.5.1.11900-1002.i386.rpm
 cuc-jetty-11.5.1.11900-1002.i386.rpm
 cuc-languagepack-enu-11.5.1.11900-1002.i386.rpm
 cuc-lib-ext-11.5.1.11900-1002.i386.rpm
 cuc-lib-jar-11.5.1.11900-1002.i386.rpm
 cuc-lib-so-11.5.1.11900-1002.i386.rpm
 cuc-links-11.5.1.11900-1002.i386.rpm
 cuc-productid-11.5.1.11900-1002.i386.rpm
 cuc-python-11.5.1.11900-1002.i386.rpm
 cuc-python-site-11.5.1.11900-1002.i386.rpm
 cuc-selinux-11.5.1.11900-1002.i386.rpm
 cuc-share-11.5.1.11900-1002.i386.rpm

nve-api-6.0.2-14049.i686.rpm
 nve-en-US-Samantha-bet1-6.0.1-13043.i686.rpm
 openssl097a-0.9.7a-9.el5_4.2.i386.rpm

Plug-In Report

 cm-rtmt-client-plugin-11.5.0.0-0.i386.rpm
 cm-taps-plugin-7.0.2.0-1.i386.rpm
 cm-axlsqtoolkit-plugin-1.1.0.0-1.i386.rpm
 cm-tsp-plugin-11.5.1.2-0.i386.rpm
 cm-ctlc-plugin-6.0.0.1-1.i386.rpm
 cm-jtapi-plugin-11.5.1.10000-1.i386.rpm

TZDATA file

-----	Version
platform-tzdata-2016d-1.el6.i386.rpm	2016-d

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)

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

© 2016 Cisco Systems, Inc. All rights reserved.