

ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU11

First Published: 2022-04-07

Revision History

Date	Revision
Apr 07, 2022	Initial publication

Introduction



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/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html



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.

This 11.5(1)SU11 ReadMe file contains important information about installation procedures and resolved caveats for Cisco Unified Communications Manager release 11.5(1)SU11. This SU can be applied to Cisco Unified Communications Manager and Session Management Edition.



Note Before you install Cisco Unified Communications Manager, Cisco recommends that you review the [Important Notes, on page 6](#) for information about issues that may affect your system.

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 “Hardware” section of the *Upgrade and*

Migration Guide for Cisco Unified Communications Manager and the 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) through 11.5(1)SU10 along with additional changes that are specific to this SU.



Note

You can only install this SU on Cisco Unified Communications Manager Release 8.6x, 9.x, 10.x, 11.0(1x), 11.5(1) through 11.5(1)SU10, or any 11.5(1)ES from 11.5.1.11001-2 to 11.5.1.23165-1. Upgrades from any earlier supported versions require a PCD migration. If upgrading from a version prior to 11.x, make sure you have obtained the appropriate licenses. This SU should not be installed on a Business Edition 3000 server.

For a list of all supported upgrade paths and the supported upgrade method, please see the Compatibility Matrix at:

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



Caution

Please note that if you install an SU it may contain fixes that are not included in the newer Unified CM releases. For example, a fix in the latest 11.5(1)SU, 11.5(1)SU11, may not be included in 12.0(1) because the fix was not available prior to the release of 12.0(1). In this example, an SU or ES on the 12.0(1) branch may be required to retain the same fixes.

New to this Release

For details about the features included in this release, refer to Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 11.5(1) at:

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

The following enhancements were introduced in 11.5(1)SU11:

- **Emergency Calling For National Suicide Prevention Lifeline** In Release 11.5(1)SU11, Unified Communications Manager supports dialing '988' calls, that are 3-digit dialing codes that will be routed to the National Suicide Prevention Lifeline centers. All telecommunications carriers and interconnected voice over Internet Protocol (VoIP) service providers will offer this service to connect with suicide prevention and mental health crisis personnel. This is in support of the FCC mandate of supporting a 3-digit dial code for Suicide Prevention Hotline that comes into effect from July 22, 2022.

For more information, see: <https://www.fcc.gov/suicide-prevention-hotline>

The following enhancements were introduced in 11.5(1)SU10:

- **Redhat 6 Kernel Upgrade** (See the [Upgrade and Migration Guide](#) for important notes regarding Spectre or Meltdown fix and possible performance degradation.)
- **2021a time zone database update**(See the [Upgrade and Migration Guide](#) for important notes regarding the removal of the US/Pacific-New time zone)
- **Apache Struts upgrade from 2.5.22 to 2.5.26**

The following enhancements were introduced in 11.5(1)SU9:

For details on new and changed features, see the [Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5\(1\)SU9](#)

- **UDS Bulk Search by Email** (NOTE: this enhancement also requires support in the Jabber client)
- **Removal of Oracle JRE from JTAPI and IPMA plugins**
- **Upgrade to JDK8**
- **Upgrade to Tomcat9**

The following enhancements were introduced in 11.5(1)SU8:

For details on new and changed features, see the [Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5\(1\)SU8](#)

- **Calendar Integration with Office 365 Support for OAuth 2.0 authentication**
- **Cisco Headset and Finesse Integration for Contact Center**
- **Emergency Call Routing Regulations (Kari's Law)**
- **EM Login Simplification using Headset**
- **Native Phone Migration using IVR and Phone Services**
- **Phone Feature Updates (Mark Your Calls as Spam and Lower Your Voice)**
- **Push Notification Deployment for iOS 13**

The following enhancements were introduced in 11.5(1)SU7:

- **Cisco Headset Management**

For more information on this feature, see the *Cisco Headset 500 Series Administration Guide*:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/Headsets/English/adminguide/n500_b_500-series-ag-new.html

- **Struts framework upgrade**

Apache struts framework was upgraded from 2.3.35 to 2.5.20

The following enhancements were introduced in 11.5(1)SU6:

- **RTMT Updates**

RTMT client no longer includes JRE

The following enhancements were introduced in 11.5(1)SU5:

- **Diversion on Decline for Cisco Webex Hybrid Services**

SIP Trunk Messaging now supports Diversion on Decline for Cisco Webex Hybrid Services.

- **Search Telepresence Conference Rooms Via UDS Proxy for LDAP**

UDS Proxy feature is enhanced to support searching of conference rooms represented as Room objects in OpenLDAP Server.

- **Call Recording for SIP or TLS Authenticated calls**

Call recording for authenticated phones while using non secure recorder is allowed.

The following enhancements were introduced in 11.5(1)SU4:

- **HTTPS Proxy for Push Notifications**

TLS connection to the Cloud is now supported.

- **Centralized Deployment for IM and Presence**

Centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters.

The following enhancements were introduced in 11.5(1)SU3:

- **Mixed Mode requires an Encryption License**

This release requires that you have an encryption license installed in order to run Cisco Unified Communications Manager in mixed mode.

- **Push Notifications Enhancements for Cisco Jabber on iPhone and iPad**

With this release, the Push Notifications for Cisco Jabber on iPhone and iPad solution has been enhanced with Voice and Video Call Support; High Availability for IM and Presence; and more.

- **Minimum TLS Version Control**

This release includes the minimum Transport Layer Security (TLS) protocol version configuration support. Use this feature to configure the minimum TLS version to comply with the organization security policies.

- **Enhanced CTL and ITL Phone Trust and Migration**

Provides a common trust anchor and the ability to create a long term trust.

- **Emergency Notifications Paging**

This release comes with a provisioning wizard that allows you to quickly provision and configure advanced notification services.

- **Authenticated Network Time Protocol Support**

With this release, the authenticated Network Time Protocol (NTP) capability for Cisco Unified Communications Manager is supported

- **Cisco Jabber Authentication via OAuth Refresh Logins**

Cisco Jabber clients, as of Jabber Release 11.9, can use OAuth Refresh Logins to authenticate with Cisco Unified Communications Manager and the IM and Presence Service.

- **Compliance to Common Criteria**

With Release 11.5(1) SU3, both Cisco Unified Communications Manager and IM and Presence Service can run in Common Criteria mode. This running mode runs on a FIPS-enabled system, and allows the system to comply with Common Criteria guidelines.

The following enhancements were introduced in 11.5(1)SU2:

- **Cisco Meeting Server Conference Bridge**

Cisco Unified Communications Manager supports the Cisco Meeting Server conference bridge, which supports Ad Hoc, Meet-Me, Conference Now and Rendezvous conferences

- **Cisco Spark Remote Device**

Cisco Spark is supported as a device type for connecting your on-premises environment to Cisco cloud services.

- **MRA Support for Shared Line**

Mobile and Remote Access (MRA) endpoints that register to Cisco Unified Communications Manager via Expressway now support shared lines. To use this feature, you must be connecting to Expressway X8.9.Push Notifications

- **Push Notifications**

With Apple iOS release 11 on Apple iPhone and Apple iPad, you must enable Push Notifications in Cisco Unified Communications Manager to maintain a persistent instant messaging channel to Cisco Jabber on iPhone and iPad. Push Notifications is mandatory for Cisco Jabber on iPhone and iPad. Android and Windows users are unaffected

- **TLS Support for Common Criteria Compliance**

Transport Layer Security (TLS) 1.2 can now be used as a communication protocol for syslog and FileBeat audit logging. This feature enables Cisco Unified Communications Manager and IM and Presence Service to comply with Common Criteria guidelines.

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

- **Enhanced Security Mode implementation.**

Important Notes

Compatibility between collaboration products is detailed at the following link. You must insure your versions are compatible before beginning your upgrade:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html

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.

RedHat 6 Kernel Upgrade



Warning 11.5.1SU10 and higher includes a RedHat 6 Kernel upgrade. The new kernel contains fixes for the Spectre and Meltdown vulnerabilities. See the [Upgrade and Migration Guide](#) for important notes regarding possible performance degradation due to the fixes for these vulnerabilities.

Warning for Upgrades to 12.0(1)



Warning This SU adds support for Extension Mobility Login Simplification using Headset. This feature is not found in CUCM 12.0(1) as that version was released prior to development of this feature. Upgrades from this SU to any 12.0(1) are not allowed and will not be displayed as valid upgrade options. Customers migrating from this SU should choose 12.5(1)SU3 or higher as their target upgrade.

Warning for Upgrades to 12.5(1)



Warning This SU adds support for Extension Mobility Login Simplification using Headset. This feature is not found in CUCM 12.5(1) prior to 12.5.(1)SU3 as those versions were released prior to development of this feature. Upgrades from this SU to any 12.5(1) version earlier than 12.5(1)SU3 are not allowed and will not be displayed as valid upgrade options. Customers migrating from this SU should choose 12.5(1)SU3 or higher as their target upgrade.

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, on page 10](#) of this document to determine the firmware load provided in this SU.

Related Documentation

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

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.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 CM Administration System version: x.x.x

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 and Migration 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 11.5.1.23900-30 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 11.5.1.23900-30 as a patch during the installation.

Release 11.5(1)SU11 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 Restricted and Export Unrestricted Software” section in the **Understanding Upgrades and Migrations** chapter, of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)* referenced above, for a more detailed description.



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

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

Table 1: Restricted ISO Names and Checksum Values

ISO Name:	UCSInstall_UCOS_11.5.1.23900-30.sha512.iso
MD5:	adebc2ecf524d561c412aefb45b45aa8

SHA512:	15c97f4814b438501c91142cd91f7a2bbe42c86b119ccdbd2d2cce6a7a086d3dc36e34c5bb8e835a42f34911ea2398c85973f54f6beaec58ba5027baa658853e
----------------	--

Table 2: UnRestricted ISO Names and Checksum Values

ISO Name:	UCSInstall_UCOS_UNRST_11.5.1.23900-30.sha512.iso
MD5:	4f0b8e83ba027b0ba14b9fd921ddf30e
SHA512:	630109cd49453cb0d661813d2d72fe94de4ced93408ec49a00f401a441d45749158d1ae85c68870517867ea2b8db4c82854bbdc65dff19ef1102c955ee50d77a

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 and Migration 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.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.



Tip For more information about an individual defect, visit the Bug Search Tool (<https://bst.cloudapps.cisco.com/bugsearch>) and use the defect Identifier to access the online record for that defect, including workarounds.

Resolved Caveats

Resolved Caveats for Cisco Unified Communications Manager Release 11.5(1)SU11 describes possible unexpected behaviors in previous Cisco Unified Communications Manager 11.5(1) releases.

Resolved CUCM Caveats in 11.5(1)SU11 (everything fixed in SU11 since SU10)

Known Fixed Release: CCM.011.005(001.23900.030)

[Click Here for the list](#)

Cumulative Resolved CUCM Caveats in 11.5(1) (everything fixed in all SU's since base 11.5(1))

[Click Here for the list](#)

Open Caveats

Open Caveats for Cisco Unified Communications Manager Release 11.5(1)SU11 describes a few of the possible unexpected behaviors still remaining in Cisco Unified Communications Manager Release 11.5(1)SU11.

CUCM Caveats 11.5(1) Complete List

For a complete list of caveats applicable to 11.5(1), use the following Bug Search Tool link:

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=268439621&rls=11.5\(1.1,11.5\(1.2&sb=afr&bt=null](https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=268439621&rls=11.5(1.1,11.5(1.2&sb=afr&bt=null)

To determine the caveats that were open for a specific release, download the results to Excel and use the Known Fixed Release values above to filter out the applicable releases. The Known Fixed Release for base 11.5(1) is 11.5(1.10000.6). Once the filters are applied, additional sorting / filtering can be applied for Bug Severity, Bug Status, and keywords. Here are some examples of how to generate lists for a specific release:

All SU11 Unresolved Caveats: To get a list of caveats that are applicable to 11.5(1) but are not fixed in SU11, use an Advanced Filter in Excel with an AND condition on the Known Fixed Releases column with the following values:

◇*011.005(001.10000.006)*
 ◇*011.005(001.11900.026)*
 ◇*011.005(001.12900.021)*
 ◇*CCM.011.005(001.13900.052)*
 ◇*CCM.011.005(001.13901.003)*
 ◇*CCM.011.005(001.13902.002)*
 ◇*CCM.011.005(001.14900.011)*
 ◇*CCM.011.005(001.15900.018)*
 ◇*CCM.011.005(001.16900.016)*
 ◇*CCM.011.005(001.17900.052)*
 ◇*CCM.011.005(001.18900.097)*
 ◇*CCM.011.005(001.21900.040)*
 ◇*CCM.011.005(001.22900.028)*
 ◇*CCM.011.005(001.23900.030)*

All SU10 Unresolved Caveats: To get a list of caveats that are applicable to 11.5(1) but are not fixed in SU10, use an Advanced Filter in Excel with an AND condition on the Known Fixed Releases column with the following values:

◇*11.5(1.10000.6)*
 ◇*11.5(1.11900.26)*
 ◇*11.5(1.12900.21)*
 ◇*CCM.11.5(1.13900.52)*
 ◇*CCM.11.5(1.13901.3)*
 ◇*CCM.11.5(1.13902.2)*
 ◇*CCM.11.5(1.14900.11)*
 ◇*CCM.11.5(1.15900.18)*
 ◇*CCM.11.5(1.16900.16)*
 ◇*CCM.11.5(1.17900.52)*
 ◇*CCM.11.5(1.18900.97)*
 ◇*CCM.11.5(1.21900.40)*
 ◇*CCM.11.5(1.22900.28)*

All SU9 Unresolved Caveats: To get a list of caveats that are applicable to 11.5(1) but are not fixed in SU9, use an Advanced Filter in Excel with an AND condition on the Known Fixed Releases column with the following values:

◇*11.5(1.10000.6)*
 ◇*11.5(1.11900.26)*

◇*11.5(1.12900.21)*
 ◇*CCM.11.5(1.13900.52)*
 ◇*CCM.11.5(1.13901.3)*
 ◇*CCM.11.5(1.13902.2)*
 ◇*CCM.11.5(1.14900.11)*
 ◇*CCM.11.5(1.15900.18)*
 ◇*CCM.11.5(1.16900.16)*
 ◇*CCM.11.5(1.17900.52)*
 ◇*CCM.11.5(1.18900.97)*
 ◇*CCM.11.5(1.21900.40)*

All SU5 Unresolved Caveats: To get a list of caveats that are applicable to 11.5(1) but are not fixed in SU5, use an Advanced Filter in Excel with an AND condition on the Known Fixed Releases column with the following values:

◇*11.5(1.10000.6)*
 ◇*11.5(1.11900.26)*
 ◇*11.5(1.12900.21)*
 ◇*CCM.11.5(1.13900.52)*
 ◇*CCM.11.5(1.13901.3)*
 ◇*CCM.11.5(1.13902.2)*
 ◇*CCM.11.5(1.14900.11)*
 ◇*CCM.11.5(1.15900.18)*

Security Advisory Caveats: To get a list of caveats that are applicable to Security Advisories or other security related issues, after filtering for a specific release using the examples above, an additional filter for the keyword PSIRT can be applied to the Release Note Enclosure column.

Firmware Versions

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

Phone Firmware

To download phone firmware, follow this procedure:

1. Go to <https://software.cisco.com/download/home>
2. Click on Browse All
3. Click on Collaboration Endpoints
4. Choose the desired Endpoint Type
5. Choose the desired Endpoint Model

Device Packages

To download phone firmware, follow this procedure:

1. Go to <https://software.cisco.com/download/home>
2. Click on Browse All
3. Click on Unified Communications

4. Click on Call Control
5. Click on Unified Communications Manager (CallManager)
6. Choose the desired UCM version
7. Click on the Device Packages link



Note As part of the upgrade process, the current device defaults will be replaced with the values listed below.

Firmware Versions in this Release

Device type	Load name	Version
3905	3905.9-4-1SR3	9.4 (1SR3.0)
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-9-4-1-3SR3	9.4 (1.3)
6945-SIP	6945-SIP-9-4-1-3SR3	9.4 (1.3)
69xx-SCCP	69xx-SCCP-9-4-1-3SR3	9.4 (1.3)
69xx-SIP	69xx-SIP-9-4-1-3SR3	9.4 (1.3)
7832-sip.14	7832-sip.14-1-1-0001-125.k4	14.1.1 (0001.125)
78xx.14	78xx.14-1-1-0001-136.k4	14.1.1 (0001.136)
7911_7906-sccp	7911_7906-sccp.9-4-2SR3-1	9.4 (2SR3.1)
7911_7906-sip	7911_7906-sip.9-4-2SR3-1	9.4 (2SR3.1)
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)
7921-sccp	7921-sccp.1-4-6-3	1.4 (6.3)
7925-sccp	7925-sccp.1-4-8SR1-5.k3	1.4 (8SR1.5)
7926-sccp	7926-sccp.1-4-8SR1-5.k3	1.4 (8SR1.5)
7931-sccp	7931-sccp.9-4-2SR2-2	9.4 (2SR2.2)
7931-sip	7931-sip.9-4-2SR2-2	9.4 (2SR2.2)
7936-sccp	7936-sccp.3-3-21	3.3 (21.0)
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.9-4-2SR3-1	9.4 (2SR3.1)
7941_7961-sip	7941_7961-sip.9-4-2SR3-1	9.4 (2SR3.1)
7942_7962-sccp	7942_7962-sccp.9-4-2SR3-1	9.4 (2SR3.1)
7942_7962-sip	7942_7962-sip.9-4-2SR3-1	9.4 (2SR3.1)
7945_7965-sccp	7945_7965-sccp.9-4-2SR4	9.4 (2SR4.0)
7945_7965-sip	7945_7965-sip.9-4-2SR4-3	9.4 (2SR4.3)
7970_7971-sccp	7970_7971-sccp.9-4-2SR3-1	9.4 (2SR3.1)
7970_7971-sip	7970_7971-sip.9-4-2SR3-1	9.4 (2SR3.1)
7975-sccp	7975-sccp.9-4-2SR4	9.4 (2SR4.0)
7975-sip	7975-sip.9-4-2SR4	9.4 (2SR4.0)
7985	7985-4-1-7-0-sccp	4.1 (7.0)
8821-sip	8821-sip.11-0-6SR2-4.k4	11.0 (6SR2.4)
8831-sip	8831-sip.10-3-1SR7-2	10.3 (1SR7.2)
8832-sip.14	8832-sip.14-1-1-0001-125.k4	14.1.1 (0001.125)
8845_65-sip.14	8845_65-sip.14-1-1-0001-125.k4	14.1.1 (0001.125)

88xx-sip.14	88xx-sip.14-1-1-0001-125.k4	14.1.1(0001.125)
894x-sccp	894x-sccp.9-4-2SR3-1	9.4(2SR3.1)
894x-sip	894x-sip.9-4-2SR3-1	9.4(2SR3.1)
8961	8961.9-4-2SR4-1.k3	9.4(2SR4.1)
9951	9951.9-4-2SR4-1.k3	9.4(2SR4.1)
9971	9971.9-4-2SR4-1.k3	9.4(2SR4.1)
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)
ATA191.12	ATA191.12-0-1-0405-005	0.1(0405.5)
headset-builtin	headset-builtin.2-3-0101-2.k4	2.3(0101.2)

Unity Connection

 CCM Reference Build: 11.5.1.23900-30

Unity RPMs:

- BuiltRPMsList
- cuc-11.5.1.23900-2161.i386.rpm
- cuc-base-11.5.1.23900-2161.i386.rpm
- cuc-bin-11.5.1.23900-2161.i386.rpm
- cuc-etc-11.5.1.23900-2161.i386.rpm
- cuc-install-11.5.1.23900-2161.i386.rpm
- cuc-jetty-11.5.1.23900-2161.i386.rpm
- cuc-languagepack-enu-11.5.1.23900-2161.i386.rpm
- cuc-lib-ext-11.5.1.23900-2161.i386.rpm
- cuc-lib-jar-11.5.1.23900-2161.i386.rpm
- cuc-lib-so-11.5.1.23900-2161.i386.rpm
- cuc-links-11.5.1.23900-2161.i386.rpm
- cuc-productid-11.5.1.23900-2161.i386.rpm
- cuc-python-11.5.1.23900-2161.i386.rpm
- cuc-python-site-11.5.1.23900-2161.i386.rpm
- cuc-selinux-11.5.1.23900-2161.i386.rpm
- cuc-share-11.5.1.23900-2161.i386.rpm
- 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
- nve-api-6.0.2-14049.i686.rpm
- nve-en-US-Samantha-bet1-6.0.1-13043.i686.rpm
- openssl097a-0.9.7a-9.e15_4.2.i386.rpm

Plug-in Report

-
- cm-ctlc-plugin-6.0.0.1-1.i386.rpm
- cm-taps-plugin-7.0.2.0-1.i386.rpm
- cm-jtapi-plugin-11.5.1.23900-1.i386.rpm
- cm-tsp-plugin-11.5.2.7-0.i386.rpm
- cm-axlsqtoolkit-plugin-1.1.0.0-1.i386.rpm
- cm-rtmt-client-plugin-11.5.0.0-0.i386.rpm

TZDATA file	Version
-----	-----
platform-tzdata-2021c-1.e16.i386.rpm	2021-c

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.