



ReadMe for Cisco Unified Communications Manager Release 12.0(1)SU2

Revision 2

Updated November 21, 2018

Changes in this revision, Revision 2

Added a Warning for a High Severity Caveat that impacts this release.



Warning

This SU release contains a known issue which can cause database replication to fail, only under certain IP address conditions, after upgrading to this release.

Please see the Release-note Enclosure of this CDETS for a detailed description of the conditions that can cause this issue to be seen and the methods to prevent it from being encountered:

[CSCvn30084](#) : Database Replication Failure when IP's have similar values

This ReadMe file discusses the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Version and Description, page 3](#)
- [New to this Release, page 3](#)
- [Important Notes, page 4](#)
- [Related Documentation, page 4](#)
- [Before You Begin, page 4](#)
- [Installation Instructions, page 4](#)
- [Reverting to a Previous Version, page 5](#)
- [Caveats, page 6](#)
- [Obtaining Documentation and Submitting a Service Request, page 15](#)



Americas Headquarters:

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

**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>

**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 4 for information about issues that may affect your system.

Introduction

This 12.0(1)SU2 ReadMe file contains important information about installation procedures and resolved caveats for Cisco Unified Communications Manager release 12.0(1)SU2. This SU can be applied to Cisco Unified Communications Manager and Session Management Edition.

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 IM and Presence Service, Release 12.0(1)* for additional details:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/12_0_1/cucm_b_upgrade-and-migration-guide-1201.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 12.0(1) through 12.0(1)SU1 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.x, 12.0(1) through 12.0(1)SU1 or any 12.0(1)ES from 12.0.1.21001-1 to 12.0.1.22020-1. Upgrades from any earlier supported versions require a PCD migration. Upgrades from 6x through 11x need to be requested via PUT (www.cisco.com/upgrade) to obtain the necessary license.

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-call-manager/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)SU5, 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 additional details about the features included in this release, refer to *Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 12.0(1)* at:

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

The following enhancements were introduced in 12.0(1)SU2:

- **JTAPI Installation Updates for 64-bit Systems**

As of this release, the Oracle Java Runtime Environment is no longer bundled automatically as a part of the JTAPI installation for 64-bit systems. In the case of 64-bit plugins, you must install the latest Java Runtime Environment on your system before you install Cisco Unified JTAPI. Otherwise, your JTAPI installation will fail.

For detailed information on installing and using JTAPI, refer to the Cisco Unified JTAPI Developer Guide for Cisco Unified Communications Manager, Release 12.0(1) at:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html>

The following enhancements were introduced in 12.0(1)SU1:

- **Extension Mobility Roaming Across Clusters**

This release adds the ability for users to roam across multiple clusters and make or receive calls even when the user's home cluster is down.

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.

Related Documentation

To view documentation that supports Cisco Unified CM Release 12.0(x), go to:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-call-manager/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 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 and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)* for detailed information about doing this upgrade:

[Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0\(1\)](#)



Note

Because the 12.0.1.22900-11 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 12.0.1.10000-10 and apply 12.0.1.22900-11 as a patch during the installation.

Release 12.0(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 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 IM and Presence Service, Release 12.0(1)* referenced above, for a more detailed description.

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

- UCSInstall_UCOS_12.0.1.22900-11.sgn.iso

The **MD5** for the Restricted combined download is: 193f578b87107bc955c019455dd408fa

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

```
a4e0097b227032aab85eb7a692ec490106b978f685bb233560b72b3ce1aed85c2bcd3ad8f4f07dd
338c4bbb90f408c5f60c78c8f3932e0da94606345d7e25650
```



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_12.0.1.22900-11.sgn.iso

The **MD5** for the Unrestricted combined download is: dce2e65fe620a3509c544e33a57da701

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

```
707a3300c1efa7278a3216110ec2a3f465bb95418996affbb248ebd295ed5acfa6775b6e45112112
3e6e1bf4b70d26cb093ed285200117c76cc05e4fbab44a25
```

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 12.0(1)* for detailed instructions on “Reverting to a Previous Version.”

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/12_0_1/cucm_b_upgrade-and-migration-guide-1201.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 12.0(1)SU2 describes possible unexpected behaviors in previous Cisco Unified Communications Manager 12.0(1) releases.

Resolved Caveats for Cisco Unified Communications Manager Release 12.0(1)SU2

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

Resolved CUCM Caveats in 12.0(1)SU2

- [CSCvm14042](#) : Evaluation of ciscocm for Struts remote code execution vulnerability August 2018
- [CSCvd70334](#) : Time does not reflect Time Zone configuration from web GUI
- [CSCvk60960](#) : Filebeat 5.6.4 does not work in UC apps 11.5.1 SU5 upgrades
- [CSCve66289](#) : CCMADMIN - Fail to create BAT template in Assistant Configuration Wizard
- [CSCvh05227](#) : User rank apart from default value cause end user field to grayed out for import
- [CSCvh25552](#) : Issue in uploading branding and in first login after branding is enabled
- [CSCvh63683](#) : Owner User ID is not set on CUCM when adding SCCP endpoint via AXL
- [CSCvk54720](#) : DRF Backup history doesn't exists
- [CSCvk58456](#) : DNA broken for Cisco ENCS 5400 ISRV Gw for MGCP protocol
- [CSCvk67927](#) : Checkin CUCA help in Unity Connection 12.0(1) SU2
- [CSCvf24492](#) : Unable to switch version on IMP due to getPeerDeploymentVersionViaSftp function
- [CSCvk01465](#) : CiscoTSP fails to connect to CUCM while switching between networks
- [CSCvk16574](#) : Running BAT jobs results in "cannot allocate memory" failure
- [CSCvk52629](#) : CDRonDemand and CallRecord Service Not Working Even Though Showing STA
- [CSCvk54291](#) : Calls made from dual mode phones to overlapping translation patterns are not wor
- [CSCvk59657](#) : Cisco Unified Communications Manager 11.5 does not remove inactive user group
- [CSCvh03921](#) : CUCM always considers the SIPS URI header if any of the record route headers h
- [CSCvk12357](#) : MRA TLS registration rejected for TCT/BOT since CUCM reuses incorrect certificat
- [CSCvk55821](#) : Removal of bundled OracleJRE from Cisco JTAPI Plugin
- [CSCvf84835](#) : CM Trust certificate missing after upgrade to 12.0.1.10000 7
- [CSCvg47019](#) : Cert sync cause CPU hike/expired certs contradiction with UI and certN logs
- [CSCvh89292](#) : UCM - Device entries missing from RegistrationDynamic table after upgrade
- [CSCvh95867](#) : VG450 is missing in BAT gateway list
- [CSCvh99508](#) : needs UI support for new platform VG400
- [CSCvg04122](#) : TFTP cores on ITLFile rebuild
- [CSCvg10739](#) : Provide an error message and prevent upload of certificates with size greater th
- [CSCvg21257](#) : Cannot enable certificate monitor settings after upgrade
- [CSCvg30223](#) : Call manager 11.5.1su3/12.0 registration fails for 7940/7960 SIP phones
- [CSCvh54605](#) : The CAPF Certificate is not RFC3280 Compliant.
- [CSCvh59516](#) : Unable to upload RSA certificate after upgrade to 11.5 SU3a in FIPS mode
- [CSCvh73320](#) : CAPF Process should not use CallManager Trust MIC Root for issuer verification

[CSCvh80924](#) : UCM cloud onboarding https address without port uses port 8080
[CSCvh92050](#) : TFTP Core generated during bulk addition and registration of devices
[CSCvi19143](#) : Show itl verification failed showing wrong error information referring to CTL
[CSCvi23864](#) : Tomcat fails to generate Multi SAN CSR if "\" is used in OU name
[CSCvi31016](#) : Default value of XciscoSyncCall is set to True, triggers LmSyncCallReq even if J
[CSCvi44310](#) : Proxy tftp reaches max serve count and replies back with 503 errors. Phones are
[CSCvi92202](#) : Haproxy unable to bind to CTFTP HTTPS ports(6971 & 6972) when intermediate C
[CSCvj09147](#) : CTL file not copied when running update/reset commands if PUB's IP overlaps SUB
[CSCvj44342](#) : Tftpcache files not deleted for HTTP request in proxy offcluster setup
[CSCvj59087](#) : Jabber signin failing due to haproxy timeout of 3s for tftp port 6972
[CSCvj72951](#) : PCD migration from CUCM 10.5 to 12.0 causing ITLRecovery file permissions issue
[CSCvj77290](#) : Recording is not working for CIPC device if the transport is UDP
[CSCvj82941](#) : Able to download Encrypted config file for EC endpoint over tftp request
[CSCvk24089](#) : High CPU usage on CUCM Publisher server due to carschl process.
[CSCvk39399](#) : CUCM - Define new unreg reason for 8821 battery drain power off
[CSCvg28428](#) : Add QED support for ISR4461 platform
[CSCvg28438](#) : Add QED support for VG450
[CSCvg59092](#) : UDS proxy LDAP Search needs to provide AD's msRTCSIP PrimaryUserAddress c
[CSCvg66920](#) : Meetme Conference allows Multiple Conferences to open with same bridge numbe
[CSCvh04187](#) : Add new QED file to support new platform ENCS 5400
[CSCvh21082](#) : Unable to delete PAB entries with special characters
[CSCvh59027](#) : add UI support for new platform ENCS 5400
[CSCvh77574](#) : Personal Address Book (PAB) Fails When CUCM has Application Dial Rules
[CSCvh80915](#) : UCM cloud onboarding UI doesn't show https for 11.5.1.SU4
[CSCvi15254](#) : CUCM generates traffic to 10.89.68.71 8080
[CSCvi83150](#) : VG400 QED changes for adding new motherboard and NIM module
[CSCvj09023](#) : Handle the "400 Bad Request" for corresponding to "No valid token obtained" erro
[CSCvj39317](#) : VG400 Add QED support for VG400 platforms
[CSCvj55376](#) : UCM as UAS sends 'requires timer' in response to update, is against RFC
[CSCvk14115](#) : Disconnect from application resulting in Call stuck while hold feature is in pro
[CSCvk18260](#) : CUCM - RTMT Monitor User Event not working for files in Syslog Directory
[CSCvk26958](#) : CDR dump file reflects UTC time and not the local time.
[CSCvk31199](#) : Webdialer should implement Content Security Policy and Cache Control
[CSCvk32229](#) : HAProxy 6972 port allows successful TLS connection(for unsuccessful certificate
[CSCuy74098](#) : UDS doesn't support bulk search by number
[CSCvb48082](#) : UDP BAT Export data incorrect, Prints null values in CSV file
[CSCve68054](#) : Warning ignores values for WAP Controller Sync Schedule
[CSCvf46506](#) : After an upgrade or server reboot services do not startup 'Hardware Configuratio
[CSCvf68597](#) : CDR thread not yielding and not able to service any requests
[CSCvg05333](#) : Certificates are not always Synched to Intercluster Peers
[CSCvi72225](#) : CUCM cores while allocating BIB to start the recording to the call
[CSCvj06761](#) : CUCM - Address April 2018 Oracle JDK Critical Patch Vulnerabilities
[CSCvj46946](#) : APNSInitialCallWaitTimer timer expiry is causing core when desk phone unregister
[CSCvj73273](#) : Media identification(mid) line added in SDP answer, when offer did not have grou
[CSCvk15343](#) : Cisco Unified Communications Manager Reflected Cross Site Scripting Vulnerabilit
[CSCvk18745](#) : 12.0(1)su2 upgrade rules to prevent install over ineligible ES's
[CSCut58407](#) : Uploading or deleting certificates CAPF / CallManager / TVS trust may reset phon
[CSCve85731](#) : Cluster manager does not recover after network error causing switch version to f

[CSCvf30614](#) : Feature Group Template incorrectly clears CTI control
[CSCvg04509](#) : Addressing sudoers wild card issue for DB
[CSCvg19946](#) : XCP router crash due to large number of packets in R2R connection write queue b
[CSCvg20109](#) : Serviceability Feature/Network service page spikes CPU from 25 45% on each ses
[CSCvg34985](#) : Cluster Manager config file corrupted after upgrade or reboot
[CSCvg38060](#) : More than one crypto line in SDP response when media inactive
[CSCvg50338](#) : SSO enabling is failing in the systems where the last upgrade done was a cop ins
[CSCvh67024](#) : Incorrect error message for push cloud onboarding https proxy url when proxy cer
[CSCvh69740](#) : PSIRT - RHEL5,6,7,SuSE10,AIX6.1,AIX7.1 All files in/etc/pam.d/ MUST NOT have
[CSCvh99657](#) : Tomcat Utilization shows total memory zero
[CSCvi28666](#) : "dbssso" user is not getting created on the IM&P node at the time of Fresh Instal
[CSCvi36790](#) : SDP Contains fake port in redirected call When MTP inserted due to DTMF mismat
[CSCvi37764](#) : CAPF service crashes while doing BAT to install LSC in some IP Phones
[CSCvi48597](#) : Normal call clearing resulting in MTP leak
[CSCvi49924](#) : Enabling CFA from phone does not follow Calling Search Space Activation Policy
[CSCvi74334](#) : Unable to import common device configuration
[CSCvj01776](#) : RTMT doesn't launch with jre 1.9
[CSCvj25544](#) : New CSDK 4.10UC9W1X1 checkin
[CSCvj43355](#) : CM listening on port 4444
[CSCvj64013](#) : RTMT not collecting all Cisco Smart Licensing logs
[CSCvj72192](#) : SIP Memory Leak When Sending 423 Interval Too Brief Message
[CSCvj76822](#) : Lower rank user able to modify the password for higher ranked user
[CSCvk06392](#) : 11.0(4) SIP loads for 8821 WLAN IP Phones
[CSCvk10562](#) : 10.3(1)SR3 Firmware Checkin for 8831 IP Phone
[CSCvk23306](#) : CCM Core when we do DNS SRV Lookup
[CSCvj23490](#) : Fine tune the ssl sessions to reduce time out and session cache size

Resolved CUCM Caveats since initial release. This SU is based on ES 12.0(1.22020-1)

[CSCvj61995](#) : MXCloseSession stops AgenalInterface and SIPInterface incorrectly, leading to MO
[CSCvj55740](#) : ISR4321 NIM-2BRI - Product Specific Configuration Layout Missing
[CSCvi72752](#) : CUCM does not query all DNS records which are part of a SRV record
[CSCvi54672](#) : IPMA functionality stopped working JTAPI event thread is still blocked by IPMA
[CSCvi45316](#) : BAT cannot insert a null into column
[CSCvi02296](#) : Default ITLFile not served after a BUILD_ALL
[CSCvh87445](#) : CUCM is not sending any response for Re-Invite with T38 lines
[CSCvh61864](#) : Unable to import/export Device pool using BAT in CUCM 12.0.1.10000-10
[CSCvg62701](#) : No way to configure IGMP version for MOH rebroadcast feature
[CSCvg58661](#) : ITL file is regenerated when configuration is saved/modified
[CSCvg08225](#) : Error 400 on clicking "Add to Access Control Group" button in Application User p
[CSCvf87498](#) : CUCM upgrade failure due to Duplicate entry on Universal Device Templates / Univ
[CSCvf21222](#) : CTI Manager core seen at provider initialization if application has a device wit
[CSCvd32919](#) : The region and location remains "Default" and "Hub_None" respectively for Dvor c
[CSCvc99621](#) : ImsReadAdminUserName Procedure returns a User with expired or locked accoun
[CSCuv03102](#) : Add RD via CTI fails when it overlaps with a pattern ending !
[CSCuo03080](#) : Serviceability Remove unnecessary ICSA alarm that shows on RTMT
[CSCvc00859](#) : CUCM - Implement Missing Secure Headers at tomcat level
[CSCvj80956](#) : AXL API requests return 403 forbidden error. WSDL files not readable from URL

[CSCvj79858](#): 12.1(1)SR1 phone loads firmware for 8811/41/51/61/45/65 IP Phones
[CSCvj71574](#): CUCM 12.0.1.21900-7 Security Violation when trying to view BAT sample file
[CSCvj52229](#): mid-call SIP REINVITE with no DN in URI containing IP address wrongly records ho
[CSCvi61573](#): updateLdapDirectory with password results in plaintext password in database
[CSCvi53585](#): Update CAR query to set proper "typeofcall" in Call Split Sceario where "destCa
[CSCvi43802](#): CUCM does not remove the escape character in Conference Now numbers while
[CSCvh81363](#): upgrade space calculation scripts are faulty.
[CSCvh78248](#): Unable to forward calls from Jabber Mobile devices using call manager
[CSCvh59773](#): "Error validating Refresh token" during refreshing access token
[CSCvh21072](#): Tapisrv service crashes due to exception code c0000008 thrown by the TAPI layer
[CSCvh07497](#): Tomcat (and other services) not running after network outage/restore
[CSCvg68875](#): Rapid Memory Leak Results in Core while Processing CcSetupRes Signal
[CSCvg19761](#): Cisco Unified Communications Manager Cross-Frame Scripting Vulnerability
[CSCvg04638](#): For Non-Shared line associated with SparkRD, call on cgpn not cleared when RDD
[CSCvj55205](#): Warning message to be changed for the pop-up coming on clicking 'Remove All
[CSCvj36908](#): New product QED files for Cisco Webex Room 70 Single/Dual G2 and 55 Dual
[CSCvj36358](#): Update displayInstances XML files for new endpoint SW version
[CSCvj35784](#): New product QED files for Cisco Webex Room Kit Pro
[CSCvj15629](#): 2018c DST Updater Cop Failing on Connection 12.0
[CSCvj14115](#): Consultative Transfer with Transcoder failure (on party 2) should try Blind Tran
[CSCvi97350](#): Call Back feature disconnects the call due to missed out SsDataInd whenever '+'
[CSCvi13231](#): Call queuing intermittently stops working on hunt lists
[CSCvh77797](#): Less details in Audit Logs while testing for device association/dissociation wit
[CSCvh66327](#): Disable unused HTTP methods
[CSCvh23223](#): SIPInterface sending out an additional m line in the SDP
[CSCvg75977](#): CCM leak on process SIPStationCdfc caused by process Subscriber
[CSCvg74815](#): Cisco Unified Communications Manager Reflected Cross Site Scripting
[CSCvg32880](#): One-way video occurs and call drops after call transfer even without video bandw
[CSCvg30773](#): 'Ring All Shared Lines' does not work for Spark RD and CMC devices
[CSCvf95640](#): CCM service fails to forward MxOffer to leg B while invoking MTP
[CSCvf88610](#): SIP INVITE Call-Info huntipiloturi parameter is not in ABNF format
[CSCvj00512](#): Cisco Unified Communications Manager Cross-Site Scripting Vulnerability
[CSCvf43317](#): Intermittent Call failure in Hold-resume over SME secure SIP trunk calls
[CSCvj46611](#): add new parameter "enbloc dialing" for 78xx/88xx phones(expect 8821/8831).
[CSCvj22841](#): Phone firmware for 8832/8832NR 12.1.1 release
[CSCvj22837](#): UCM Configuration files for 8832/8832NR 12.1.1 release
[CSCvi33331](#): Increase the name restriction of Spark Remote Device to allow 32 characters
[CSCvh55176](#): After reboot Server is not booting back console stuck with "Probing EDD (edd=off
[CSCvh19809](#): Inconsistent behaviour in the display of original called number in enbloc and di
[CSCvh05469](#): Domain name with multiple dots is not allowing to add the entry
[CSCvf69935](#): getUser fails when end user has many controlled devices
[CSCuq83865](#): RisDC Core on Subscriber node in FIPS mode
[CSCvj01480](#): IP phone firmware v12.1 check in on CUCM branches.
[CSCvj00670](#): RTMT Critical Services pane does not show Critical Services
[CSCvg36295](#): Disable TLS1.0 and TLS1.1 for web access to 78xx & 88xx phones
[CSCvi49528](#): CUCM displays "DNS Unreachable" if DNS response via UDP is larger than 512 byt
[CSCvi21999](#): Call Leak During Blind Transfer / MGCP Disconnect Race Condition
[CSCvi13003](#): Calls Fail due to Malformed Route Header

[CSCvh20757](#) : Incorrect File Permissions for Ipsec.xml File Following PCD Migration
[CSCvg75502](#) : MIB2 service is not in running state post upgrade
[CSCvg56395](#) : Calls not presented to the phones in a line group
[CSCvf73771](#) : Cannot set "None" for Device and Line configuration using BAT.
[CSCvf63462](#) : CUCM Fails To Get SSO Status
[CSCvd80012](#) : Outgoing Invite from CUCM doesn't send the application IX CUCM Version 10.5
[CSCvi53400](#) : CUCM AXL addPhone NullPointerException
[CSCvi15924](#) : BAT Validate import file doesn't check for trailing spaces in CSV file.
[CSCvi12584](#) : SIP Trunk duration. Mismatch between Time In Full Service and Time Up/Down cou
[CSCvh86595](#) : Data not propagated to all nodes during network flapping.
[CSCvh67638](#) : DST/TZ data upgrade with 2018c
[CSCvh17818](#) : Incorrect File Permissions for Prefs.xml File Following PCD Migration
[CSCvg06692](#) : After PCD Migration Incorrect File permissions impacts trace collection, CDP and
[CSCvf63806](#) : After PCD Migration Incorrect File permissions impacts SFTP operations
[CSCva22660](#) : CUCMChange the TFTP request path to /Desktops/240x320x24 for wallpaper ima
[CSCvi40743](#) : Phone FW for 792x 1.4(8)SR1-5 release
[CSCvi35945](#) : Copy button on the device config page does not work.
[CSCvi08335](#) : Getting blank page when performing copy operation at Phone page
[CSCvh89673](#) : Jabber does call-forward-all to junk values even with NONE CSS in call forward s
[CSCvh83796](#) : CUCM Core when race condition hit during transfer operation
[CSCvh79219](#) : CA controlled NTE DTMF not negotiated correctly between SIP and MGCP
[CSCvh69630](#) : MGCP Interface does not close channel if it receives MXFarEndOfferNeeded and if
[CSCvh62145](#) : CLI - utils create report platform should not download platformConfig.xml
[CSCvh61049](#) : ISC BIND Remote Denial of Service Vulnerability
[CSCvh58783](#) : Add MR2 English Locale to CUCM
[CSCvh48379](#) : CCM cored while trying to update the storePathHeader
[CSCvh27333](#) : Path replacement doesn't work for CFA/CFB/CFUR through a SIP Trunk
[CSCvh03836](#) : LPM does not have correct permissions to delete files when HWM is hit
[CSCvg74810](#) : Cisco Unified Communications Manager SQL Injection Vulnerability
[CSCvg24314](#) : ECC Profile URL Does not Contain Port causing core
[CSCvg05789](#) : Core in SIPStationInit Due to Memory Corruption
[CSCvf22116](#) : Cisco Unified Communications Manager LDAP Information Disclosure Vulnerability
[CSCvf10487](#) : SNR destination cannot receive calls if we have Path header
[CSCvh95267](#) : BAT - Update phones is not working for CSF, TAB, TCT and BOT devices
[CSCvh48571](#) : Failed to save device/cucm/RemoteDestination. Error, code-1
[CSCvg94144](#) : DBL out of shared virtual memory when running BPS jobs
[CSCvg50439](#) : CCM service cores due to duplicate device register signal in a LineControl
[CSCvh61524](#) : CUCM generating incorrect Call duration for transfer Scenario
[CSCvh55509](#) : 8821Add default English-US dictionary into CUCM for IP-Phone 8821 for SR6
[CSCvh13881](#) : Recording fails intermittently once conference starts
[CSCvg54414](#) : CUCM - QSIG Route Optimisation intermittently fails in transfer scenarios
[CSCvg31320](#) : JTAPI client to include support for RHEL 7
[CSCvf71339](#) : IPVMS should preserve tx and rx for one-way media
[CSCvf57448](#) : Unable to configure ILS if remote clusters are previously configured in Cluster
[CSCvf20218](#) : Cisco Unified Communications Manager HTTP interface Information Disclosure Vul
[CSCvf08417](#) : BIB Recording failed due to Software-Based MTP OutOfResource
[CSCvh61031](#) : Access to the requested resource has been denied.
[CSCvh05981](#) : ICSA needs to log alarms for successful and failed Peer Sync events

[CSCvg75966](#) : Thread synchronization issues in QBEHelper results in CEF core
[CSCvg63773](#) : Burn the new QuoVadis certificate to cucm iso
[CSCvg25974](#) : Disable 3DES- CBC Ciphers in SSHD
[CSCvf81559](#) : IVR service parameter update missing
[CSCvf79013](#) : Learned Directory URIs missing from CUCM after upgrade
[CSCvf66225](#) : 80-bit-encrypted MOH and Announcement (IPVMS)
[CSCvf61908](#) : Disable the 3DES Cipher Suites Support in TVS
[CSCvf61901](#) : Disable 3DES Cipher Suites Support in CAPF
[CSCvf47039](#) : Password can be seen in plain text in log files when UI password is changed using
[CSCvg89116](#) : Cisco Unified Communications Manager and Cisco Unified Presence Cross-Site S
[CSCvf53884](#) : TVS thread handling re-architecture
[CSCvd10872](#) : Multiple Cisco Products Disk Utilization Denial of Service Vulnerability
[CSCvh55099](#) : 11.0(3)SR6 SIP loads for 8821 WLAN IP Phones
[CSCvh23527](#) : UCM Memory Leak With SCCP Devices and Location Based Services
[CSCvh03320](#) : Licensing "TelePresence Room" getting "Unmapped Exception String index out of
[CSCve73171](#) : HCMF Vulnerable version of python in use
[CSCvd72245](#) : Evaluation of ciscocm for NTP March 2017
[CSCti42583](#) : BAT.xlt needs to be supported on 32-bit Office 2010
[CSCvh17135](#) : Gateway has been blocked and redirecting to the security.jsp
[CSCvf30437](#) : CUCM not forwarding name in the remote party-ID.
[CSCvd54314](#) : CUCM does not properly handle SIP Update w/SDP and 183 W/SDP glare
[CSCvg68784](#) : Call pickup stops working intermittently - Stale CIs stuck in pickup table
[CSCvg43550](#) : ARC application reporting OOS events for Cisco IP phone extentions; phones need
[CSCvc96618](#) : 2016g DST Updater Cop Failing on Connection
[CSCvg87841](#) : 12.0(1) QED for Cisco ATA 191 device
[CSCvg87838](#) : 12.0(1) SIP load for Cisco ATA 191 device
[CSCvg81698](#) : On CCM UI the Spark room kit registration status shows as None
[CSCvg79738](#) : RU from 9.x to 12.5 fails in smartlicensing export
[CSCvg66406](#) : Migration from 12.0/12.0su1 to higher versions using PCD does not migrate smart
[CSCvg38675](#) : CCM Cores in mutex_lock Operation
[CSCvg33717](#) : Scheduled Date Time jumps forwards or backwards depending on timezone offset
[CSCvf95828](#) : Struts upgrade to 2.3.34
[CSCvf84642](#) : CUCM affected by Apache Tomcat vulnerabilities
[CSCvf66549](#) : Rename or Import Contacts - Custom File Job is InComplete even if the file has a
[CSCvf02916](#) : IX5000 Telepresence endpoint - add enable for proximity from client apps
[CSCve59587](#) : Cannot Set SSH Password In Common Phone Profile
[CSCvd54701](#) : India DoDIntercluster Mobility
[CSCuu57031](#) : sensitive info seen in URL
[CSCvg80340](#) : Unity Connection Help for This Page not loading for "Edit Call Input Handler" af
[CSCvg48503](#) : Unable to Change User Rank for LDAP Imported Users
[CSCvg38255](#) : MTP resource leak due to MXTimeout
[CSCvg20603](#) : Application user password appearing in logs
[CSCvg19311](#) : MVA for disabling mobility is not working when enable MVA service parameter is s
[CSCvg04920](#) : RU or PCD Migration to 12.x Causes GUI/DB Errors On Existing Device Updates
[CSCvf99804](#) : ARC application prints out "error" message while calling SIP busy destination
[CSCvf77305](#) : RTMT 12.0 not launching windows error 2 occurred while loading the Java VM
[CSCvf70124](#) : Presence user assignment changes are not logged in Audit logs
[CSCvf36328](#) : CUCMAddress July Oracle Critical Patch Vulnerabilities

[CSCve51537](#) : AMC Failover Collector does not work when Primary Collector is not reachable
[CSCvg51264](#) : Cisco Unified Communications Manager Cross Site Scripting Vulnerability
[CSCva27502](#) : Password is logged in logs during execution of Admin CLI
[CSCvg57582](#) : Unable to enable IGMP protocol for Rebroadcast External Multicast Source feature
[CSCvf70585](#) : Large ITL File Size Increase after Unified Communications Manager 12.0 Upgrade
[CSCvf79346](#) : Cisco Unified Communications Manager Cross Site Scripting Vulnerability
[CSCvf56538](#) : CTI monitoring DevName must be upper case
[CSCvg45484](#) : Check in firmware release 12-0-1SR1 for phone models 88xx/8845_65
[CSCvg29297](#) : Add device enablers for Cisco Spark Room 70 Dual and Cisco Spark Room 70 Sin
[CSCvg22923](#) : CUCM unauthorized access vulnerability
[CSCve82179](#) : A call on a random extension would get rejected up as user busy.
[CSCvg33688](#) : CUCM cores are generated post RU upgrade
[CSCvg10268](#) : Normalization Scrip to pass through header "x-att-loop" sent by AT&T
[CSCvf72935](#) : CUCM is presenting a NULL_SHA cipher for phones over MRA
[CSCvf39052](#) : CTI messages carry \ escape character when the hunt pilot member is configured a
[CSCvf36322](#) : CUCMOS Updates for Sudo, Glibc, Libtiff, Coreutils, GnuTLS, OpenSSH, Bash
[CSCvf36286](#) : CUCMOS Updates for Bind, NSS, MySQL, Jasper
[CSCvf88802](#) : CUCM cores when Jabber tries to register through APNS feature
[CSCvf78696](#) : BATIn Update Phones page, the search box gets empty after hitting "Find"
[CSCvf73537](#) : Call Manager sending unescaped # causing MRA Phones to Unregister
[CSCvf36682](#) : Cisco Unified Communications Manager SQL Injection Vulnerability
[CSCvf69887](#) : CUCM 10.5.2+ SW MTP not advertising RTCP Pass Through (PT) even though it c
[CSCvf96778](#) : CTI based SSO fails when defining CUCM sever as IP address in CCMAdmin//S
[CSCvf94485](#) : phone firmware for 7832 12.0.1 release
[CSCvf94416](#) : Phone firmware for 8832/8832NR 12.0.1 release
[CSCvf89436](#) : 11.0(3)SR4 QED files for 8821 WLAN IP phones
[CSCvf88162](#) : 11.0(3)SR4 SIP loads for 8821 WLAN IP Phones
[CSCvf87066](#) : Check in firmware release 12-0-1-11 for phone models 78xx/88xx/8845_65
[CSCvf01557](#) : CHS+KORCCMADMINStrings shows up in English with locale in Lincense Manag
[CSCvf69143](#) : incoming calls from MGCP gateway do not match the most specific pattern
[CSCvf65311](#) : Upgrade rules to prevent 12.0(1) Respins from installing over ES's
[CSCvf57440](#) : No push is sent to devices during rapid link OOS and link ISV between nodes
[CSCvf51739](#) : Wallpaper files replacement for 88xx phone

Open Caveats

Open Caveats for Cisco Unified Communications Manager Release 12.(1)SU2 describes a few of the possible unexpected behaviors still remaining in Cisco Unified Communications Manager Release 12.0(1)SU2. For a complete list of open caveats please access the bug toolkit located at:
https://bst.cloudapps.cisco.com/bugsearch/?referring_site=btk

When using the bug toolkit, the Known Fixed Releases values for 12.0(1) SU's are as follows:

12.0(1)SU2 = CCM.12.0(1.22900.11)
 12.0(1)SU1 = CCM.12.0(1.21900.7)

**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

[CSCvn30084](#) : Database Replication Failure when IP's have similar vlaues

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 12.0** 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-9-4-1-3SR3	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	7832-sip.12-1-1-12.k3	12.1(1.12)
78xx	78xx.12-1-1-12.k3	12.1(1.12)
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)
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	7937-1-4-4-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.9-4-2SR3-1	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.9-4-2SR3-1	9.4(2SR3.1)
7945_7965-sip	7945_7965-sip.9-4-2SR3-1	9.4(2SR3.1)
7975-sccp	7975-sccp.9-4-2SR3-1	9.4(2SR3.1)
7975-sip	7975-sip.9-4-2SR3-1	9.4(2SR3.1)
7985	7985-4-1-7-0-sccp	4.1(7.0)
8821-sip	8821-sip.11-0-4-14.k3	11.0(4.14)
8831-sip	8831-sip.10-3-1SR3-5	10.3(1SR3.5)
8832-sip	8832-sip.12-1-1-23.k3	12.1(1.23)
8845_65-sip	8845_65-sip.12-1-1SR1-4.k3	12.1(1SR1.4)
88xx-sip	88xx-sip.12-1-1SR1-4.k3	12.1(1SR1.4)
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	ata191.12-0-1-29	12.0(1.29)

Plug-In Report

```
-----
cm-rtmt-client-plugin-12.0.0.0-0.i386.rpm
cm-taps-plugin-7.0.2.0-1.i386.rpm
cm-axlsqltoolkit-plugin-1.1.0.0-1.i386.rpm
cm-tsp-plugin-12.0.1.2-0.i386.rpm
cm-ctlc-plugin-6.0.0.1-1.i386.rpm
cm-jtapi-plugin-12.0.1.22900-1.i386.rpm
```

TZDATA file

-----	Version
platform-tzdata-2018c-1.el6.i386.rpm	2018-c
platform-tzdata-2018c-1.el6.noarch.rpm	2018-c

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.

© 2018 Cisco Systems, Inc. All rights reserved.

