ReadMe for Cisco Unified Presence Release 8.6(5)SU3

March 12, 2014

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(5)SU3.

Note	**To view the Release Notes for previous versions of Cisco Unified Presence, go to the following URL: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html**

Contents

- Introduction, page 2
- System requirements, page 2
- Installation and upgrade notes, page 6
- Additional installation and upgrade considerations, page 8
- Related documentation, page 10
- New and changed information, page 10
- Important notes, page 10
- Caveats, page 11
- Documentation Updates, page 15

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

Introduction

Cisco Unified Presence collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. Cisco Unified Presence can also collect information about individual user communications capabilities, such as whether web collaboration or video conferencing is enabled. Applications such as Cisco Jabber and Cisco Unified Communications Manager use this information to improve productivity amongst employees, that is, to help employees connect with colleagues more efficiently and determine the most effective way for collaborative communication.

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(5)SU3. These release notes are updated for every maintenance release but not for patches or hot fixes.

Before you install Cisco Unified Presence, Cisco recommends that you review, Related Documentation, page 10 for information about the documentation available for Cisco Unified Presence.

System requirements

- Hardware server requirements, page 2
- Server software requirements, page 3
- Supported browsers, page 3

Hardware server requirements

Note	**Cisco Unified Presence Release 8.6(5)SU3 requires 4 GB of RAM, except for the 500 user and Business Edition 6000 OVA deployments, which require 2 GB of RAM.**

The Cisco Unified Presence system is a software product that is loaded onto a hardware server. The hardware server must meet the following requirements:

- One of the following server models:
  - Cisco 7800 Series Media Convergence Server (MCS) listed in the *Hardware and Software Compatibility Information for Cisco Unified Presence*. Go to Cisco.com for the latest information: http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Note	**Cisco Unified Presence does not support MCS-xxxx-I1-IPC1 or MCS-xxxx-H1-IPC1 servers. However, a bridged upgrade is available to customers who need to migrate from any of the discontinued hardware, except for the following servers: MCS-7825-H1-IPC1, MCS-7825-I2-IPC1, MCS-7825-I1-IPC1, MCS-7825-I2-IPC2. For details about the unsupported hardware and the bridged upgrade, see the *Upgrade Guide for Cisco Unified Presence Release 8.6* here: http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html**

  - Cisco-approved, customer-provided third-party server that is the exact equivalent of one of the supported Cisco MCS servers. Go to http://www.cisco.com/go/swonly.
  - Tested Reference Configurations (TRC) for virtualized deployments described on this page: http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#UC_on_UCS_Tested_Reference_Configurations.
  - Cisco Unified Computing System B-series blades or Cisco Unified Computing System C-series

rackmount servers. For information about these Cisco Unified Computing System servers, see the *Hardware and Software Compatibility Information for Cisco Unified Presence Release 8.x here:* http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

- DVD-ROM drive
- Keyboard, mouse, and monitor

Note **Additional server requirements, such as port and IP address requirements, are described in *Port Usage Information for Cisco Unified Presence*.**

The Cisco Unified Presence installer checks for the presence of the DVD-ROM drive, sufficient hard drive and memory sizes, and sufficient CPU type and speed.

Cisco Unified Presence supports bridged upgrades from any of the following servers:

- MCS-7825-H2-IPC1
- MCS-7825-H2-IPC2
- MCS-7835-H1-IPC1
- MCS-7835-I1-IPC1
- MCS-7845-H1-IPC1
- MCS-7845-H2-IPC1 (only if each of the two disks has less than 72GB of storage space, otherwise it is fully supported)
- MCS-7845-I1-IPC1

The bridged upgrade allows you to create a DRS backup on the discontinued hardware. You can then restore the DRS backup on supported hardware after you complete a fresh Cisco Unified Presence installation on the supported hardware. If you attempt an upgrade on discontinued hardware, Cisco Unified Presence displays a warning on the interface and on the CLI, informing you that Cisco Unified Presence only supports the functionality to create a DRS backup on this server.

Server software requirements

The Cisco Unified Presence server runs on the Cisco Linux-based operating system. This operating system is included with the application.

Related Topic

Installation and upgrade notes, page 6.

Supported browsers

Use Microsoft Internet Explorer version 6.0 or a later release, or Mozilla Firefox version 3.0 or a later release, to access these interfaces: Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Operating System Administration.

Note **Cisco Unified Presence does not currently support Safari or Google Chrome on the Mac OS or Microsoft Windows.**

How to use Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the Apache Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the Internet. HTTPS, which ensures the identity of the server, supports applications, such as Cisco Unified Serviceability. HTTPS also ensures that the user sign-in password is transported securely via the web.

HTTPS for Internet Explorer

The first time you (or a user) access Cisco Unified Presence Administration or other Cisco Unified Presence SSL-enabled virtual directories after a Cisco Unified Presence installation or upgrade, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must respond in one of the following ways:

- By selecting Yes, you select to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application: that is, until you install the certificate in the trusted folder.
- By selecting View Certificate > Install Certificate, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display every time you access the web application.
- By selecting No, you cancel the action. No authorization occurs, and you cannot access the web application. To access the web application, you must select Yes or install the certificate via the View Certificate > Install Certificate option.

Note **The system issues the certificate using the hostname. If you attempt to access a web application using the IP address, the Security Alert dialog box displays, even though you installed the certificate on the client.**

Saving the certificate to the trusted folder

You can save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application. Perform the required steps depending on the Internet browser you are using:

Table 1 Saving the Certificate to the Trusted Folder

If you are using …	Actions	Troubleshooting Tips
Internet Explorer 6 and 8	1. Browse to the application on the Tomcat web server. 2. Select **View Certificate** when the Security Alert dialog box displays. 3. Select **Install Certificate** in the General pane of the Certificate dialog box. 4. Select **Next** in the Certificate Import Wizard dialog box. 5. Select **Place all certificates in the following store.** 6. Select **Browse** adjacent to the Certificate store field 7. Browse to **Trusted Root Certification Authorities**. 8. Select **OK**, **Next**, then **Finish**. 9. Select **Yes** to install the certificate. 10. Select **OK** after you receive a message stating that the import was successful. 11. Select **OK** in the lower, right corner of the Certificate dialog box. 12. Select **Yes** to trust the certificate, so you do not receive the dialog box again.	• After you save the certificate to the trusted folder in Internet Explorer, the next time you browse to the server, ensure that you enter the fully qualified domain name (FQDN) of the server that is associated with the certificate. • You can verify that the certificate was installed successfully by selecting the Certificate Path tab in the Certificate pane
Internet Explorer 7	1. Browse to the application on the Tomcat web server. 2. Select **Continue to this website (not recommended)** option to access the server. 3. Select **View Certificate** when the Security Alert dialog box displays. 4. Select **Install Certificate** in the General pane of the Certificate dialog box. 5. Select **Next** in the Certificate Import Wizard dialog box. 6. Select **Automatically select the certificate store** based on the type of certificate. 7. Select **Next**, then **Finish**. 8. Select **Yes** in the Security Warning dialog box. 9. Select **OK** in the Certificate Import Wizard dialog box.	• After you save the certificate to the trusted folder in Internet Explorer, the next time you browse to the server, ensure that you enter the FQDN of the server that is associated with the certificate. • To verify that the trust store contains the imported certificate, select **Tools > Internet Options** in the Internet Explorer toolbar and select the Contents tab. Select **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list. • After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you re-enter the hostname or IP address or refresh or relaunch the browser. • You can verify that the certificate was installed successfully by selecting the Certification Path tab in the Certificate pane.

Netscape	1. Browse to the application using Netscape. 2. Select one of the following radio buttons: • Accept this certificate for this session • Do not accept this certificate and do not connect • Accept this certificate forever (until it expires) • Select **OK** in the Certificate Authority dialog box • Select **OK** in the Security Warning dialog box	• After you save the certificate to the trusted folder in Netscape, the next time you browse to the server, ensure that you enter the FQDN name of the server that is associated with the certificate. • If you select Do not accept this certificate and do not connect, the application does not open. • To view the certificate credentials before installing the certificate, select **Examine Certificate.**

Installation and upgrade notes

- System upgrade, page 6
- Latest software upgrades for Cisco Unified Presence on Cisco.com, page 8

System upgrade

- Supported Upgrade Paths to Cisco Unified Presence Release 8.6(5)SU3, page 6
- Upgrade from Cisco.com, page 7

Supported Upgrade Paths to Cisco Unified Presence Release 8.6(5)SU3

Cisco Unified Presence supports the following software upgrade paths to Release 8.6(5)SU3:

Table 2 Supported Upgrade Paths

Supported Upgrade Paths from Cisco Unified Presence	Installation Instructions
Release 8.0(x), 8.5(x), or 8.6(x) to 8.6(5)SU3	**Before You Begin** Upgrades from 8.0(x) through to 8.6(1) require you to install a COP file on all nodes prior to starting the upgrade. Download the following COP file from Cisco.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop` Perform these steps to proceed with the upgrade: 1. Go to http://www.cisco.com/upgrade. 2. Enter your software contract number. 3. Select the CUP<pre-upgrade release>-8-6-U-K9= option to order. If you do not see this option, contact your Cisco Account Team and/or Reseller to resolve your Contract issue. 4. Go to http://www.cisco.com/cisco/software/navigator.html. 5. Navigate to Products > Voice and Unified Communications > Unified Communications Applications > Cisco Unified Presence > Cisco Unified Presence 8.6 > Unified Presence Server Updates. 6. Download the complete ISO file: UCSInstall_CUP_8.6.5.13900-2.sgn.iso

Note **Direct upgrades from Cisco Unified Presence Release 7.0(x) and earlier to Release 8.6(5)SU3 are not supported. You must first upgrade to an earlier 8.x release of Cisco Unified Presence. For more information about upgrading to Cisco Unified Presence Release 8.x, see the *Upgrade Guide for Cisco Unified Presence*: http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html**

Upgrade from Cisco.com

Cisco does not support downloading major Cisco Unified Presence software releases from Cisco.com, for example, Cisco Unified Presence Release 8.0. From Cisco.com you can download upgrade-only software images that are used to upgrade from a previous major software release to a subsequent software maintenance release or point release of Cisco Unified Presence. For example, you can download Cisco Unified Presence Release 8.0(2) or Cisco Unified Presence Release 8.6(5)SU3 from Cisco.com.

To download this software, go to http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240. You must have an account on Cisco.com to access the Software Center. The images posted at the Software Center require existing installations of Cisco Unified Presence.

Latest software upgrades for Cisco Unified Presence on Cisco.com

Perform the following steps to access the upgrade file for Cisco Unified Presence Release 8.5(x) to 8.6(5)SU3.

Before You Begin

- You can only download point releases of Cisco Unified Presence software from Cisco.com.
- Upgrades from 8.0(x) through to 8.6(1) require you to install a COP file on all nodes prior to starting the upgrade. Download the following COP file from Cico.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`

Procedure

Step 1 Download the UCSInstall files from Cisco Connection Online.

Step 2 Use an md5sum utility to verify that the MD5 sum of the final file is correct:

6e7346043c5d8b41f0fb4ecce8a36a8e UCSInstall_CUP_8.6.5.13900-2.sgn.iso

Troubleshooting Tips

You can upgrade the ISO image onto a remote server. Copy the ISO (UCSInstall_CUP_8.6.5.13900-2.sgn.iso) to your FTP or SFTP server.

Additional installation and upgrade considerations

- Perform Cisco Unified Presence 8.6(x) upgrade before Cisco Unified Communications Manager 8.6(x) upgrade, page 8
- Licensing requirements for Release 7.0(x) to 8.6(x) upgrades, page 9
- Software licensing requirements for VMware, page 9
- Recommendations for release 8.0(x), 8.5(x), or 8.6(x) to 8.6(5)SU3 upgrades, page 9
- Platform Manager is not supported , page 10

Perform Cisco Unified Presence 8.6(x) upgrade before Cisco Unified Communications Manager 8.6(x) Upgrade

You must perform the Cisco Unified Presence Release 8.6(x) upgrade *before* you perform the Cisco Unified Communications Manager Release 8.6(x) upgrade.

Licensing requirements for Release 7.0(x) to 8.6(x) upgrades

If you upgrade from Release 7.0(x) to Release 8.6(x), you require a new software version license for *each* Cisco Unified Presence server in your deployment. You must order a separate software version license for each Cisco Unified Presence server. However, you need to upload the license to the first node in a cluster. For information about Cisco Unified Presence licensing modes and requirements, see the Installation Guide for Cisco Unified Presence Release 8.6 here:

http://www.cisco.com/en/US/products/ps637/prod_installation_guides_list.html

Software licensing requirements for VMware

You can run this release of Cisco Unified Presence on a VMware virtual machine deployed on approved Cisco Unified Computing server hardware. For information about supported servers, see *Hardware and Software Compatibility Information for Cisco Unified Presence Release 8.x*. For information about the VMware licensing requirements, see the License Activation for Cisco UC on UCS Doc wiki here: http://docwiki.cisco.com/wiki/License_Activation_for_Cisco_UC_on_UCS

Recommendations for release 8.0(x), 8.5(x), or 8.6(x) to 8.6(5)SU3 upgrades

Before you upgrade from Cisco Unified Presence Release 8.0(x), 8.5(x), or 8.6(x) to Release 8.6(5)SU3, Cisco *strongly advises* that you follow the recommended upgrade procedure in the *Upgrade Guide for Cisco Unified Presence Release 8.6* here:
http://www.cisco.com/en/US/products/ps6837/prod_installation_guides_list.html

Note	**Direct upgrades from Release 7.x and earlier to 8.6(5)SU3 are not supported. You must first upgrade to another 8.x release and then perform a *Refresh Upgrade*. A Refresh Upgrade is significantly different from a Standard Upgrade. For more information, see the *Upgrade Guide for Cisco Unified Presence 8.6***

Important Notes

- Publisher node—upgrade the publisher node and switch the software to the new software release prior to initiating an upgrade and switch version on the Subscriber nodes. If the Cisco Unified Presence Administration GUI is operational on the Publisher node, it is safe to initiate an upgrade and switch version on the Subscriber node. There are special considerations that need to be taken into account when upgrading to Release 8.6(5)SU3. Cisco recommends that you refer to the *Upgrade Guide for Cisco Unified Presence 8.6* before you proceed with upgrading.

Note	**Services on the Publisher will not start until the Subscribers are switched, restarted, and replication is successfully established on that cluster.**

- High Availability User Support—Cisco Unified Presence Release 8.6(x) supports up to 45,000 users per cluster in a High Availability (HA) configuration across 6 nodes and up to 45,000 users per cluster in a non-HA configuration across 3 nodes. If, when you upgrade, you are left with a number of unsupported users, we recommend that you unlicense these surplus users on Cisco Unified Communications Manager before you perform the upgrade.
- Contact List Size—the default maximum value is 200; however you can configure this to a higher value, or configure 0 to set it to unlimited value. After you perform the upgrade, check that the contact

list size for users has not reached the maximum value. If you have a large number of contacts per user, the number of users that a Cisco Unified Presence node supports is reduced.

Platform Manager is Not Supported

Platform Manager (PM) cannot be used to upgrade to Cisco Unified Presence Release 8.6(5)SU3.

Related documentation

The complete Cisco Unified Presence documentation set, with the latest information for Release 8.6(x), is now available here on Cisco.com.

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

To search for documentation on any given release, we recommend that you use the Custom Google search capability introduced in the last release.

For more information, see the *Deployment Guide for Cisco Unified Presence Release 8.6*.

http://www.cisco.com/en/US/products/ps6837/products_licensing_information_listing.html

New and changed information

Several defects have been resolved. For more information, see Resolved caveats , page 12.

Important notes

- CPU Spike Causes Database Connection Failure, page 10
- Certificate Validation, page 11

CPU Spike Causes Database Connection Failure

Problem

The following Cisco Unified Presence interfaces can become inaccessible due to database connectivity problems. When attempting to login to the following applications, the login will appear to hang and will not complete:

- Cisco Unified Presence Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified End User Options

Cause

This condition affects Cisco Unified Presence running on a virtualized environment where the virtual machine (VM) on which Cisco Unified Presence is running has only one CPU. A large CPU spike on the Cisco Unified Presence server can cause the database to become inaccessible. You can verify that you are experiencing this issue by performing the following procedure:

Step 1 From the Cisco Unified Presence CLI, execute the following command to view the database log file: `file view activelog /cm/log/informix/ccm.log`

Step 2 Check the log file for entries similar to the following:

```
listener-thread: err = -25582: oserr = 0: errstr = : Network
connection is broken.
```

Solution

To resolve this issue, add an additional CPU to the VM on which Cisco Unified Presence is running.

Certificate Validation

Problem

When using a Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name.

Cause

Having Cisco Unified Presence server node name different than the sever identity in the certificate presented to Cisco Jabber client, represents identity mismatch.

Solution

To prevent Cisco Jabber from generating certificate warning messages, the FQDN must be used as the Cisco Unified Presence server node name.

Caveats

- Using Bug Search, page 11
- Resolved caveats, page 12
- Open caveats, page 14

Using Bug Search

Known problems (bugs) are graded according to severity level. This ReadMe file contains descriptions of the following:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.
- All customer-found bugs.

You can search for problems by using the Cisco Bug Search tool.

To access Bug Search, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Step 1 To access the Bug Search, go to https://tools.cisco.com/bugsearch?referring_site=btk

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the **Search for:** field, and click **Go**.

For information about how to search for bugs, create saved searches, and create bug groups, select **Help** on the Bug Search page.

Resolved caveats

This section lists caveats that are resolved but that may have been open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity. Because defect status continually changes, be aware that this document reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access the Bug Search Tool.

Table 3 Resolved caveats for Cisco Unified Presence Release 8.6(5)SU3

Identifier	Severity	Component	Headline
CSCuj14419	3	axl	Changing to non english user locale breaks getUser AXL API
CSCug26683	3	axl	ICSA between 10 and 8 fails due to AXL errors
CSCui66810	3	config-agent	CfgAgent writes empty static routes if IMDB ttroute is down
CSCuh86938	3	config-agent	Config Agent core dump occurs if it can't retrieve the nodename
CSCuj69195	3	ctigw	When user clicks on "click to call", sip proxy cores, RCC with MOC
CSCul42879	2	database-ids	IDS uses incorrect index user lookup if intercluster with large clusters
CSCug76766	3	epe	DND is incorrect cascading to a device with a shared line appearance
CSCui67346	3	epe	Presence Engine unable to connect to presence gateway using DNS SRV
CSCtl88055	3	epe	Support "Idle on all devices" feature
CSCud63046	3	epe	XMPP Status shows "On the Phone" while in a meeting:
CSCug66525	3	epe	Presence Engine Roster Cleanup fails if Owner JID contains ':' character
CSCui29999	3	epe	Manual available is not maintained if underlying device status away
CSCui74861	3	epe	Presence Engine Startup is slow
CSCui82748	3	epe	PE PresenceChangeThrottleRate not updated on upgrade from 8.6.2
CSCuj56376	3	epe	User Email address with special characters doesn't work over EWS
CSCuj87713	3	epe	PE stopped trying to re-connect to XCP R2R - incorrect Presence seen
CSCul50741	3	epe	HA - Users don't relogin to the backup node after PE down event on pub
CSCul74225	3	epe	Manual Presence intermittently not composed correctly by Presence Engine
CSCui09967	3	epe	DND stuck state on CUPC for the phone associated

CSCul77560	3	epe	Unsetting DND on Phone clears user/manual DND
CSCum43153	3	epe	Presence doesn't transition from Manual Available to Away when PC locked
CSCum47733	3	epe	Incorrect Composed Presence when setting a Custom Away status
CSCud22574	3	epe	Out of memory on startup due to large number of WinfoEventTable entries
CSCty41459	3	epe-privacy	Error Unblocking a contact containing an apostrophe
CSCug65132	3	esp	SIP Proxy rejects SSLv23 Client Hello messages without looking for TLSv1
CSCul04184	3	esp	SIP Proxy core dump handling large scale SIP based federation traffic
CSCui19679	3	esp	"Cisco SIP Proxy service child process has been stopped" flooding
CSCuj81008	3	esp	Proxy apply direct federation routing (maddr) for non direct fed domains
CSCuj87776	3	esp	SIP Proxy Not returning HTTP 414 on large PWS REST Requests
CSCul30258	3	esp	SIP Proxy cores when invalid RouteEmbedTemplate parameter set
CSCun08416	4	esp	SIP Proxy fails to route IM from userid containing XEP106 characters
CSCuj63038	4	gui	Unknown error on Exchange Server Status page
CSCui22721	3	gui-admin	PE Trouble Shooters Verify SIP Publish results in an internal error
CSCul57798	3	gui-serviceability	XCP router stops if wrong no of connection to DB set in service parameter
CSCts53870	3	oamagent	Delay in writing pe_cfg.xml upon L2 causes PE to start in bad state
CSCuf62906	3	security	IMP 9.0 generates malformed cup-xmpp cert signing request
CSCug18764	3	security	Leaf certificates not able to be uploaded to tomcat-trust
CSCuc39596	3	security	[OpenAM SSO]: OpenAM SSO enable fails with tomcat service not starting
CSCuh19287	3	security	[OpenAM SSO]: Upgrade never completes in GUI, when FIPS and SSO enabled
CSCuf55909	3	security	[OpenAM SSO]: enabling sso from cli fails when users use upn for jabber
CSCui76795	3	security	Stale symbolic links in cert directories prevent DRS backups
CSCul16038	3	security	Tomcat cert with multiple critical extensions set to true not supported
CSCuj83870	3	security	Duplicate SANs in CA signed CUP certs
CSCui03916	4	selinux	SE Linux blocks IBM hardware snmp mib
CSCtz23921	3	serviceability	Pub fails to communicate with subscriber servm when enable/disable HA
CSCum92892	2	vos	IM/P Subscriber Node 'Version Mismatch Error' on switch version attempt.
CSCui14910	3	vos	CUP does not backup and restore the cup cert properly
CSCuj72390	3	vos	DRS backup start time drifts further each day
CSCui53487	2	xcpauth	XCP Authentication service crashes on login
CSCuj65714	2	xcp-router	Jabberd process is causing memory leak on large scale CUP
CSCue84354	2	xcp-router	XCP publish incorrect comp presence for peer, resulting in looping packet
CSCug81385	3	xcp-s2s	XCP S2S issues with email address mapping for Group Chat packets

CSCui96841	3	xcp-s2s	SASL auth requests with an authorization identity set to "="
CSCuc11276	3	xcp-sipgw	SIP Federation Connection Manager core
CSCul32676	4	config-agent	ConfigAgent Core on Shutdown
CSCuf56468	4	epe	"Could not be delivered message" appears although message is received

Open caveats

The caveats in Table 4 describe possible unexpected behavior in the latest Cisco Unified Presence release. These caveats may also be open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity.

Table 4 Open caveats for Cisco Unified Presence Release 8.6(5)SU3

Identifier	Severity	Component	Headline
CSCua84174	4	axl	AXL toolkit downloaded from GUI is corrupted
CSCui51099	4	bat	Contact with multiple groups intermittently not BAT imported correctly
CSCul32654	4	config-agent	Copyfrompeer for TTLOGIN & TTREG broken after node boot up
CSCty85346	3	database	CLI 'dbreplication forcedatasyncsub' doesn't work on CUP
CSCtz88557	4	database	CPU spike causes database connection failure
CSCun31368	3	database-imdb	IMDB Replication is broken when node boots up after being powered down.
CSCum02939	3	epe	CUCM device remains stuck in DND despite clearing DND from Jabber
CSCtu42689	4	esp	Phone presence not shown in CUPC when CUPS hostname starts a number
CSCul84488	4	esp	SIP Proxy treating ARC subscribes as federated requests
CSCue72366	4	gui	CUPS Troubleshooter page showed error message for SIP Publish Model
CSCuc44918	4	gui	No notice that XCP Router needs to be restarted after parameter changes.
CSCui45774	4	gui	Use email address only with inter-domain federation
CSCuj28830	4	gui-admin	Web Admin Pg - need notification warning when logging not set to default
CSCui88619	5	gui-admin	CUPS External Database Verification Error when using special password.
CSCuc26300	4	gui-serviceability	Changing Node name halts access XCP Config Manager restart
CSCuf04522	4	gui-serviceability	guiRework on msg in changing Federation Routing CUP FQDN
CSCuh36248	5	gui-troubleshooter	Presence Gateway error with DNS SRV configuration in Troubleshooter
CSCuh72980	4	install	SUB installation fails - unable to obtain CUCM PUB info
CSCuj28749	4	licensing	IM&P counts a User Template as a licensed user.
CSCug09157	3	security	OpenAM SSO: intermittent http 500, 403, bad cert error when sso enabled.

CSCty97447	3	security	[OpenAM SSO] j2ee policy agent debug logs can grow too large.
CSCty29379	4	security	CUP GUI not working when some services are restarted while SSO enabled
CSCuj97487	4	security	Misleading exception in logs during upload of signed tomcat certificate
CSCui86000	4	serviceability	Excessive logging can cause performance issues and system outages
CSCuj83919	4	serviceability	Misleading/Confusing Alert message for service not activated
CSCuh89979	4	serviceability	Slow Tomcat responses when using RTMT
CSCuj25912	4	srm	IM&P server does not restart services
CSCuh60802	4	sync-agent	CUPS Sync Agent - duplicate value for a record with unique key
CSCue11001	4	sync-agent	Synchronization process with CM can't be completed
CSCum84645	3	vos	CUPS DRS Issue:DRS backup option missing some components
CSCuh42251	4	vos	CUPS primary install wizard asks for NTP but doesn't use it
CSCum76745	3	xcp-jsm	Existing temp-presence sub not affected by changes to privacy list
CSCui09350	3	xcp-jsm	Jabber iphone, custom status text lost when place in background
CSCtz23657	4	xcp-jsm	No warning when trying to IM inter-cluster user while failover occurring
CSCug49106	4	xcp-router	Federated contacts deleted when federation enabled but XMPP fed cm off
CSCub53720	4	xcp-sipgw	Core dump on sip federartion manager. Caused a reboot of the service.
CSCuc44918	4	gui	No notice that XCP Router needs to be restarted after parameter changes.

Documentation Updates

For the latest versions of all Cisco Unified Presence documentation, go to http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Obtaining documentation and submitting a service request

For information about 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.