



# Release Notes for Cisco Unified Presence Release 8.6(4)SU1

---

**April 10, 2013**

These release notes describe requirements, restrictions, and caveats for Cisco Unified Presence Release 8.6(4)SU1.



**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](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 14](#)
- [Obtaining Documentation and Submitting a Service Request, 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(4)SU1. 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 the “[Related Documentation](#)” section on 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(4)SU1 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](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](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>.
- 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](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.

- 
- Step 1** Perform the required steps depending on the Internet browser you are using:

**Table 1** *Saving the Certificate to the Trusted Folder*

<b>If you are Using.....</b>	<b>Actions</b>	<b>Troubleshooting Tips</b>
Internet Explorer 6 and 8	<p><b>a.</b> Browse to the application on the Tomcat web server.</p> <p><b>b.</b> Select <b>View Certificate</b> when the Security Alert dialog box displays.</p> <p><b>c.</b> Select <b>Install Certificate</b> in the General pane of the Certificate dialog box.</p> <p><b>d.</b> Select <b>Next</b> in the Certificate Import Wizard dialog box.</p> <p><b>a.</b> Select <b>Place all certificates in the following store.</b></p> <p><b>b.</b> Select <b>Browse</b> adjacent to the Certificate store field.</p> <p><b>c.</b> Browse to <b>Trusted Root Certification Authorities.</b></p> <p><b>d.</b> Select <b>OK.</b></p> <p><b>e.</b> Select <b>Next.</b></p> <p><b>f.</b> Select <b>Finish.</b></p> <p><b>g.</b> Select <b>Yes</b> to install the certificate.</p> <p><b>h.</b> Select <b>OK</b> after you receive a message stating that the import was successful.</p> <p><b>i.</b> Select <b>OK</b> in the lower, right corner of the Certificate dialog box.</p> <p><b>j.</b> Select <b>Yes</b> to trust the certificate, so you do not receive the dialog box again.</p>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• You can verify that the certificate was installed successfully by selecting the Certificate Path tab in the Certificate pane.</li> </ul>

**Table 1** Saving the Certificate to the Trusted Folder (continued)

If you are Using.....	Actions	Troubleshooting Tips
Internet Explorer 7	<p>a. Browse to the application on the Tomcat web server.</p> <p>b. Select <b>Continue to this website (not recommended)</b> option to access the server.</p> <p>c. Select <b>View Certificate</b> when the Security Alert dialog box displays.</p> <p>d. Select <b>Install Certificate</b> in the General pane of the Certificate dialog box.</p> <p>e. Select <b>Next</b> in the Certificate Import Wizard dialog box.</p> <p>f. Select <b>Automatically select the certificate store</b> based on the type of certificate.</p> <p>g. Browse <b>Next</b>.</p> <p>h. Select <b>Finish</b>.</p> <p>i. Select <b>Yes</b> in the Security Warning dialog box.</p> <p>j. Select <b>OK</b> in the Certificate Import Wizard dialog box.</p>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• To verify that the trust store contains the imported certificate, select <b>Tools &gt; Internet Options</b> in the Internet Explorer toolbar and select the Contents tab. Select <b>Certificates</b> and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.</li> <li>• 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.</li> <li>• You can verify that the certificate was installed successfully by selecting the Certification Path tab in the Certificate pane.</li> </ul>
Netscape	<p>a. Browse to the application using Netscape.</p> <p>b. Select one of the following radio buttons:</p> <ul style="list-style-type: none"> <li>• Accept this certificate for this session</li> <li>• Do not accept this certificate and do not connect</li> <li>• Accept this certificate forever (until it expires)</li> <li>• Select <b>OK</b> in the Certificate Authority dialog box.</li> <li>• Select <b>OK</b> in the Security Warning dialog box</li> </ul>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• If you select <b>Do not accept this certificate and do not connect</b>, the application does not open.</li> <li>• To view the certificate credentials before installing the certificate, select <b>Examine Certificate</b>.</li> </ul>

## Installation and Upgrade Notes

- [System Upgrade, page 6](#)
- [The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 8](#)

## System Upgrade

- [Supported Upgrade Paths to Cisco Unified Presence Release 8.6\(4\)SU1, page 7](#)
- [Upgrade from Cisco.com, page 7](#)

## Supported Upgrade Paths to Cisco Unified Presence Release 8.6(4)SU1

Cisco Unified Presence supports the following software upgrade paths to Release 8.6(4)SU1:

**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(4)SU1	<p><b>Before You Begin</b></p> <p>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:  <code>ciscocm.cup.refresh_upgrade_v&lt;latest_version&gt;.cop</code></p> <p>Perform these steps to proceed with the upgrade:</p> <ol style="list-style-type: none"> <li>1. Go to <a href="http://www.cisco.com/upgrade">http://www.cisco.com/upgrade</a>.</li> <li>2. Enter your software contract number.</li> <li>3. Select the CUP&lt;pre-upgrade release&gt;-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.</li> <li>4. Go to <a href="http://www.cisco.com/cisco/software/navigator.html">http://www.cisco.com/cisco/software/navigator.html</a>.</li> <li>5. Navigate to Products &gt; Voice and Unified Communications &gt; Unified Communications Applications &gt; Cisco Unified Presence &gt; Cisco Unified Presence 8.6 &gt; Unified Presence Server Updates.</li> <li>6. Download the complete ISO file: UCSInstall_CUP_8.6.4.11900-1.sgn.iso</li> </ol>



**Note**

Direct upgrades from Cisco Unified Presence Release 7.0(x) and earlier to Release 8.6(4)SU1 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](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(4)SU1 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.

**Related Topics**

- [Supported Upgrade Paths to Cisco Unified Presence Release 8.6\(4\)SU1, page 7](#)
- [The Latest Software Upgrades for Cisco Unified Presence on Cisco.com, page 8](#)

## The 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(4)SU1.

**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:  
`611bdaee7eab20214b7d2326083d4c5f UCSInstall_CUP_8.6.4.11900-1.sgn.iso`
- 

**Troubleshooting Tips**

You can upgrade the ISO image onto a remote server. Copy the ISO (UCSInstall\_CUP\_8.6.4.11900-1.sgn.iso) to your FTP or SFTP server.

**Related Topics**

- [System Upgrade, page 6](#)
- [Upgrade from Cisco.com, page 7](#)

## Additional Installation and Upgrade Considerations

- [Perform Cisco Unified Presence 8.6\(x\) Upgrade Before Cisco Unified Communications Manager 8.6\(x\) Upgrade, page 9](#)
- [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\(4\)SU1 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. Cisco does not support Cisco Unified Presence 8.0(x) servers running with Cisco Unified Communications Manager Release 8.5 or 8.6.

## 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](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 Docwiki here:

[http://docwiki.cisco.com/wiki/License\\_Activation\\_for\\_Cisco\\_UC\\_on\\_UCS](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(4)SU1 Upgrades

Before you upgrade from Cisco Unified Presence Release 8.0(x), 8.5(x), or 8.6(x) to Release 8.6(4)SU1, 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](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(4)SU1 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(4)SU1. 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 Unified Communications mode users per cluster in a High Availability (HA) configuration. 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) can not be used to upgrade to Cisco Unified Presence Release 8.6(4)SU1.

## 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](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](http://www.cisco.com/en/US/products/ps6837/products_licensing_information_listing.html)

## New and Changed Information

No new features have been introduced in Cisco Unified Presence Release 8.6(4)SU1, however, several defects have been resolved. For more information, see [Resolved Caveats, page 12](#).

## Important Notes

The following sections contain information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Release 8.6(4)SU1:

- [CPU Spike Causes Database Connection Failure, page 10](#)

## 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.

## Caveats

- [Using Bug Toolkit, page 11](#)
- [Resolved Caveats, page 12](#)
- [Open Caveats, page 12](#)

## Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain 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 Software Bug Toolkit.

#### Before You Begin

To access Bug Toolkit, you need the following items:

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

**Procedure**

- 
- Step 1** To access the Bug Toolkit, go to <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>.
- 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 Bug ID” field, then select **Go**.
- 

For information about how to search for bugs, create saved searches, and create bug groups, select **Help** on the Bug Toolkit 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 Toolkit (see the [Using Bug Toolkit, page 11](#)).

**Table 3** *Resolved Caveats for Cisco Unified Presence Release 8.6(4)SU1*

Identifier	Severity	Component	Headline
<a href="#">CSCtz67093</a>	3	ctigw	CUPS truncates called party after 20 digits.
<a href="#">CSCua16730</a>	2	esp	Network interfaces may load in wrong order causing proxy routing issues.
<a href="#">CSCua16730</a>	2	esp	SIPD service core dumps in SSL_state
<a href="#">CSCua20741</a>	3	esp	408 error responses in Intradomain Federation at scale
<a href="#">CSCua09717</a>	3	security	DRF fails to backup Subscriber node
<a href="#">CSCua41825</a>	3	vos	Restore of platform component failing in 9.0.0.96000-95 build.
<a href="#">CSCua33621</a>	3	xcp-router	XCP router not orphaned on restart.

## 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(4)SU1*

Identifier	Severity	Component	Headline
<a href="#">CSCtw75780</a>	3	bat	Some imported contacts' presence not showing when max contacts size set.
<a href="#">CSCtx01262</a>	3	config-agent	Config Agent drops all CNs as the ChangeManagerSipdConf queue is full.

**Table 4** Open Caveats for Cisco Unified Presence Release 8.6(4)SU1

Identifier	Severity	Component	Headline
<a href="#">CSCua73880</a>	3	ctigw	CUPS 8.6.4 is causing core dump with RCC.
<a href="#">CSCtz96671</a>	3	cupxcpconfig	Incorrect restart notification for sub
<a href="#">CSCtz38528</a>	3	database-install	L2 upgrade of PUB node in fully provisioned 45k System taking 27hrs
<a href="#">CSCtz88557</a>	3	database	CPU spike causes database connection failure.
<a href="#">CSCty85346</a>	3	database	CLI 'dbreplication forcedatasyncsub' does not work on Cisco Unified Presence.
<a href="#">CSCto77824</a>	3	database	Users have inconsistent presence after Cisco Unified Presence upgrade.
<a href="#">CSCua12285</a>	3	database	Boot up after switch back hanging at 'Starting cupOnL2BootInitd'
<a href="#">CSCtz64227</a>	3	database	Carriage return control characters in db data can cause upgrade failure
<a href="#">CSCtz55120</a>	3	epe	Possible memory leak on soak test run
<a href="#">CSCtz26168</a>	3	epe	Presence Engine core when calendaring enabled on Cisco Unified Presence release 8.6(1)
<a href="#">CSCtz99702</a>	3	epe	Relogin of Jabber causes error impacting presence composition.
<a href="#">CSCtz26163</a>	3	epe	Presence Engine core on startup when calendaring GW is configured
<a href="#">CSCtz83598</a>	3	esp	SIP retransmits result in shared memory exhaustion
<a href="#">CSCtz06790</a>	3	gui-accessibility	When admin locks user on CUCM, user can always access GUI pages with SSO.
<a href="#">CSCty35767</a>	4	gui-accessibility	User in same Groups can not access same webapps with and without SSO
<a href="#">CSCtz83131</a>	3	gui-admin	Incorrect CUCM hostname can cause subscriber install to fail.
<a href="#">CSCtz34968</a>	3	gui-admin	Tomcat hangs after End-User query filter times out.
<a href="#">CSCtr36119</a>	3	gui-troubleshooter	Exchange server status reports false positives.
<a href="#">CSCtz96324</a>	3	gui	Audit user does not have exclusive permission to audit log files.
<a href="#">CSCty29379</a>	3	gui	CUP GUI not working when some services are restarted while SSO enabled.
<a href="#">CSCty82764</a>	3	gui	SSO logout screen not consistent.
<a href="#">CSCtn13881</a>	3	intercluster	ICSA Certs are not sync'ed if an existing peer certs are available
<a href="#">CSCtz62315</a>	3	intercluster	ICSA handling errors for CNs being sent
<a href="#">CSCtz62036</a>	3	intercluster	Can't exchange certs via ICSA between FIPS enabled & FIPS disabled peers
<a href="#">CSCts53870</a>	3	oamagent	Delay in writing pe_cfg.xml upon L2 causes PE to start in bad state.
<a href="#">CSCtz55287</a>	4	security	Text when enable FIPS too CUCM specific
<a href="#">CSCts28606</a>	3	serviceability	"UNKNOWN_ALARM" alerts sent to remote syslog server on router restart
<a href="#">CSCts61745</a>	3	serviceability	Syslog messages dropped when Router debug logging enabled
<a href="#">CSCtt79854</a>	3	serviceability	AlertCentral and CoreDumpFileFound alert properties XML parse error
<a href="#">CSCtz10360</a>	3	serviceability	Server status not reliably retrieved on Cluster Topology page.
<a href="#">CSCtz12616</a>	3	serviceability	Can not delete CUP remote access account.
<a href="#">CSCtz23921</a>	3	serviceability	Pub fails to communicate with subscriber servm when enable/disable HA

**Table 4** *Open Caveats for Cisco Unified Presence Release 8.6(4)SU1*

Identifier	Severity	Component	Headline
<a href="#">CSCtz74208</a>	3	serviceability	SNMP query unable to distinguish between services.
<a href="#">CSCtz23921</a>	3	srm	Publisher fails to communicate with subscriber servm when enable/disable high availability.
<a href="#">CSCtz26078</a>	3	vos	OpenSSH: DSA/DSS connections do not work in FIPS mode
<a href="#">CSCty44483</a>	3	xcp-jabberwerx	JID getting displayed in the top-left corner of chat window
<a href="#">CSCty14182</a>	3	xcp-jsm	XMPP login failures due to bind errors at scale.
<a href="#">CSCts40539</a>	3	xcp-routefabric	8.5 routers in an 8.6 mesh can corrupt routing table

## Documentation Updates

There were no updates made to any documents for Cisco Unified Presence Release 8.6(4)SU1.

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](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.

---

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: [www.cisco.com/go/trademarks](http://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. (1110R)

© 2012 Cisco Systems, Inc. All rights reserved

