Release Notes for the Cisco Unified Presence Server (CUPS) Release 1.0(2)

August 29, 2006

These release notes describe new documentation and caveats for Cisco Unified Presence Server (CUPS), Release 1.0(2). For more specific information, please see the "New and Changed Information for Cisco Unified Presence Server (CUPS) 1.0(2)" section on page 3, "Documentation Updates" section on page 8 and "Open Caveats" section on page 15.

Contents

These release notes include the following topics:

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

Introduction

The Cisco Unified Presence Server, a critical component for delivering the full value of a Cisco Unified Communications environment, collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. It can also collect information about individual user communications capabilities, such as whether web collaboration or video conferencing is enabled. Using this information, applications such as Cisco Unified Personal Communicator and Cisco Unified CallManager can improve productivity by helping employees connect with colleagues more efficiently through determining the most effective way for collaborative communication.

For More Information

Cisco strongly recommends that you review the following documents before you perform the installation.

- *Cisco Unified Presence Server Administration Guide*
- *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco IP Telephony Disaster Recovery System Administration Guide*
- *Cisco IP Telephony Platform Administration Guide*
- *Cisco Unified CallManager Security Guide*

Table 1 lists URLs for software and additional documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco Unified CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco Unified CallManager Security Guide	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm
Cisco Unified CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco Unified CallManager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

New and Changed Information for Cisco Unified Presence Server (CUPS) 1.0(2)

The following information specifies new and changed information that the CUPS 1.0(2) documentation contains:

Cisco Unified Presence Server Deployment Guide, Release 1.0(2)

This new document contains configuration checklists and procedures for setting up Cisco Unified Presence Server 1.0(2) and integrating it with Cisco Unified CallManager 5.0(4), as well as with the required Microsoft servers and products, including

- Microsoft Office Live Communications Server 2005 with Service Pack 1 (SP1)
- Microsoft Windows Server 2003 Active Directory
- Microsoft Office Communicator 2005

Configuration Troubleshooter

Chapter 7 of the *Cisco Unified Presence Server Administration Guide, Release 1.0(2)*, a new chapter, contains information about the Configuration Troubleshooter that you can use to diagnose configuration issues after the initial configuration of the Cisco Unified Presence Server or whenever you make changes.

The Troubleshooter performs a set of tests on both the Cisco Unified Presence Server cluster and on the Cisco Unified CallManager cluster to validate the Cisco Unified Presence Server configuration.

After the Troubleshooter finishes testing, it reports one of three possible states for each test:

- Test passed
- Test failed
- Test warning, which indicates a possible configuration issue

Note For each test that fails or that results in a warning, the Troubleshooter provides a description of the problem and a possible solution.

Access Configuration Troubleshooter under **System > Troubleshooter**.

Microsoft Office Communicator (MOC) Assignment

Chapter 35 of the *Cisco Unified Presence Service Administration Guide, Release 1.0(2),* a new chapter, contains information about MOC assignment. Because you might have several users with MOC capability in your network, Cisco Unified Presence Server lets you locate specific users on the basis of specific criteria. Use the following procedure to locate users with MOC capability.

Note During your work in a browser session, the cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then open a new browser window, the system retains your Cisco Unified Presence Server search preferences until you modify your search.

From **Application > CTI Gateway > MOC Assignment** you can locate MOH users based on

- User-ID
- Last Name
- Manager
- Department

BAT Considerations

You can use the Bulk Administration Tool to make bulk MOC assignments.

1. After you complete the search based on the appropriate criteria, from the list of records, click the check box for the users that match your search criteria or click **Select All** and click **Bulk Assignment**.
2. On the window that displays, click the Enable MOC check box to enable or disable MOC assignment for the users that you chose.
3. Click **Save**, or to leave the chosen users MOC assignment unchanged, click **Close**.

New Information Displayed in System Status

Use Status to display the Cisco Unified Presence Server System status.

- To view the system status, choose **System > Status**.

  The Unified Presence Server System Status window displays and shows Sync Information and System Information.

  In this release of Cisco Unified Presence Server, the system information includes the following items:

  - Number of end users
  - Number of phone devices
  - Number of licensed Cisco Unified Presence Server end users
  - Number of licensed Cisco Unified Personal Communicator end users
  - Number of assigned Microsoft Office Communicator end users

CTI Gateway Settings

Chapter 34 of the *Cisco Unified Presence Server Administration Guide*, CTI Gateway Settings, a new chapter, describes the use of Computer Telephony Interface (CTI) gateway settings to configure the settings that apply to the CTI gateway.

Configuring CTI Gateway Settings

Follow this procedure to configure the CTI gateway settings.

Procedure

Step 1 Choose **Application > CTI Gateway> Settings**.

The CTI Gateway Settings window displays.

Step 2 Enter the appropriate settings as described in Table 2.

Step 3 To save the data, click the Save icon that displays in the tool bar in the upper, left corner of the window (or click the Save button that displays at the bottom of the window).

Table 2 IP Phone Messenger Configuration Settings

Field	Description
Application Status	From the drop-down list, choose **On** or **Off** to turn the CTI gateway application on or off.
Application Username	This parameter specifies the CTI gateway application user name. **Note** This user name must match the application user name that you configured on the Cisco Unified CallManager cluster.
Application Password	This parameter specifies the CTI gateway application user name. **Note** This password must match the application password that you configured on the Cisco Unified CallManager cluster.
CTI Address	This parameter specifies the IP address or fully qualified domain name of the CTI gateway. **Note** Use Cisco Unified CallManager subscriber nodes and avoid using the primary node IP address.
CTI Address (Failover)	This parameter specifies the IP address or fully qualified domain name of the failover CTI gateway. **Note** Ensure the failover CTI address is not the same as the primary CTI address.
Heartbeat Interval (seconds)	This parameter specifies the value of the heartbeat interval in seconds. Range: 5-20 seconds Default: 8 seconds
Session Timer (seconds)	This parameter specifies the value of the session time in seconds. Range: 1810-2000 seconds Default: 1800 seconds

Alarm Definition Catalog Descriptions

The *Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(2)* includes a Definition Catalog description table as shown in Table 3.

Table 3 Alarm Definition Catalog Descriptions

Field	Description
CiscoUPSConfigAgent	All configuration agent alarms
CiscoUPSPresenceEngine	All presence engine alarms
CiscoUPSSIPProxy	All SIP proxy alarms
CiscoUPSSoap	All Cisco Unified Personal Communicator change notified alarms
CiscoUPSSyncAgent	All sync agent alarms
DBAlarmCatalog	All Cisco database (aupair) alarm definitions

Table 3 Alarm Definition Catalog Descriptions

Field	Description
DRFAlarmsCatalog	All Disaster Recovery Framework alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Cisco CallManager Java Applications alarm definitions **Note** You cannot configure JavaApplications alarms by using the alarm configuration windows. You generally configure these alarms to go to the Event Logs and to generate SNMP traps to integrate with CiscoWorks2000. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
LpmTctCatalog	All Log Partition Monitor Trace Collection Tool alarms
SystemAccessCatalog	All Log Partition Monitor Trace Collection Tool alarms
SystemAccessCatalog	All process and thread monitoring alarms
TFTPAlarmCatalog	All Cisco TFTP alarm definitions

Important Notes

Support for Inbound Caller-Name when Active Directory Stores the Number in E.164

If the MOC user phone numbers are configured in Active Directory in E.164 format, inbound calls will be shown in MOC with the incoming party numbers but no names can be matched by reverse number lookup.

Four-Way Conference Call with SIP Phone Moderator

If you use a SIP phone to host a four-way conference call initiated from the MOC client, the moderator cannot add the fourth participant. If the moderator uses a SCCP device this problem does not occur.

Publisher Server CUPS upgrade

Do not configure anything on the Cisco Unified CallManager publisher server while the CUPS publisher server is being upgraded. If you must configure something, stop the Sync Agent before starting the upgrade and manually start it after the upgrade is completed.

Restarting CUPS delays IPPM services

After a system restart, the IPPM service may not be available for up to 10 minutes while various components in the system initialize.

Fresh Installation on a Subscriber Can Result in the Inability to Activate Services on the Subscriber Node from the Publisher Node

Depending on the state of the hardware clock on the system and the time zone, the Tomcat certificate can generate with a timestamp that is invalid (the validity of the certificate represents some number of hours in the future; until this number of hours elapses since the subscriber installation, you cannot start services for this subscriber).

To activate the services

1. Regenerate the Tomcat certificate (the only relevant ones) prior to service activation and after installation completes on the subscriber.
2. Log in to the subscriber platform GUI and choose: **Security > Certificate Mgmt > Delete Regenerate Certificate**.
3. Activate services for the subscriber.

Running a Large BAT Job on Cisco Unified CallManager Can Result in Change Notification Not Working Properly.

If you run a large BAT job, stop the synchronization, so the change notification works properly

Running a Large Synchronization from Cisco Unified CallManager to CUPS Over AXL May Cause Intermittent Timeouts in the NCSClient Connection.

If you run a large synchronization over AXL, stop any provisioning on Cisco Unified CallManager.

Documentation Updates

Updates

End User Capabilities Assignment

Previous *Cisco Unified Presence Server Administration Guide, Release 1.0(2)* documentation releases specified that you could assign end user capabilities as a part of CUPS configuration. This assignment now gets done in Cisco Unified CallManager under **System > Licensing > Capabilities Assignment**.

Omissions

CTI Gateway Settings

When you configure the CTI gateway settings, Cisco recommends that you use Cisco Unified CallManager subscriber nodes and avoid using the Cisco Unified CallManager primary node IP address.

Bulk Administration Tool

In the CUPS Administration window, Bulk Administration Tool (BAT) represents one menu option. That tool allows the CUPS administrator to perform various bulk provisioning tasks. Two types of BAT operations exist for CUPS administrators: set various UPS profiles and enable MOC on end users.

Errors

Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(2)

In Chapter 34 of the *Cisco Unified Presence Service Serviceability Administration Guide, Release 1.0(2)*, CTI Gateway Settings, Table 34-1 specifies a Provider drop-down list. A Provider drop-down list no longer exists in the CTI Gateway Settings window.

Changes

Name Changes

The following list gives name changes that were made in Cisco Unified Presence Server, Release 1.0(2):

- MeetingPlace Server renamed MeetingPlace Express Server.
- MeetingPlace Profile renamed MeetingPlace Express Profile.
- Unity Profile renamed Unity Connection Profile.
- Unity Server renamed Unity Connection Server.
- Presence Engine Backend Gateway renamed CallManager Presence Gateway.

Cisco MeetingPlace Express Server

Cisco MeetingPlace Express Server Configuration Settings

The MeetingPlace Express Server Configuration table includes the following added information:

- The Name parameter field includes the maximum number of characters allowed.
- The Description parameter field includes the maximum number of characters allowed.
- The Port parameter field includes the default port.
- The Protocol Type parameter field includes the default protocol type.
- The Protocol Type parameter field no longer shows TLS as an option.

Table 4 MeetingPlace Express Server Configuration Settings

Field	Description
Name	This parameter specifies the name of the Cisco MeetingPlace Express Server. Maximum characters: 128
Description	This parameter provides a general description of the Cisco MeetingPlace Express server. Maximum Characters: 128
Hostname/IP Address	This parameter specifies the host name or IP Address of the Cisco MeetingPlace Express server.
Port	This parameter specifies the port number that is configured for the Cisco MeetingPlace Express server. Default: 80
Protocol Type	This parameter specifies the protocol to use when contacting the Cisco Unity Connection server. Choose one of the following values: • HTTP • HTTPS Default: HTTP

Cisco MeetingPlace Express Profile Configuration Settings

The MeetingPlace Express Server Configuration Settings table displays the maximum number of characters information in the Name and Description fields as shown in Table 5.

Table 5 Cisco MeetingPlace Express Profile Configuration Settings

Field	Description
Name	This parameter specifies the name of the Cisco MeetingPlace Express profile. Maximum characters: 128
Description Primary MeetingPlace	This parameter provides a general description of the Cisco MeetingPlace Express profile. Maximum characters: 128
Express Server	This parameter specifies the primary Cisco MeetingPlace Express server. From the drop-down list, you can choose from the Cisco MeetingPlace Express servers that you have already defined on the system.
Backup MeetingPlace Express Server	This parameter specifies the backup Cisco MeetingPlace Express server. From the drop-down list, you can choose from the Cisco MeetingPlace Express servers that you have already defined on the system. You can specify two backup Cisco MeetingPlace Express servers.

Unity Connection Profile Configuration Settings

The Unity Connection Profile Configuration Settings table displays the maximum number of characters information in the Name and Description fields as shown in Table 6.

Table 6 Unity Connection Profile Configuration Settings

Field	Description
Name	This parameter specifies the name of the Cisco Unity Connection Profile. Maximum characters: 128
Description	This parameter provides a general description of the Cisco Unity Profile. Maximum characters: 128
Voice Messaging Pilot	This parameter specifies the voice-messaging pilot that is associated with this Cisco Unity Connection profile. You can also choose No Voice Mail from the drop-down list.
Primary Unity Connection Server	This parameter specifies the primary Cisco Unity Connection server.From the drop-down list, you can choose from the Cisco Unity Connection servers that you already defined on the system.
Backup Unity Connection Server	This parameter specifies the backup Cisco Unity Connection server. From the drop-down list, you can choose from the Cisco Unity Connection servers that you already defined on the system. You can specify two backup Cisco Unity Connection servers.

Unity Connection Host Configuration Settings

The Unity Host Configuration window has changed. It now includes a Name field and default information in the Port and Protocol Type fields as shown in Table 7.

Table 7 Unity Connection Host Configuration Settings

Field	Description
Name	This parameter specifies the name of the Cisco Unity Connection host. Maximum characters: 128
Description	This parameter provides a general description of the Cisco Unity Connection server.
Hostname/IP Address	This parameter specifies the host name or IP Address of the Cisco Unity Connection server.

Table 7 Unity Connection Host Configuration Settings

Field	Description
Port	This parameter specifies the port number that is configured for the Cisco Unity Connection server. Default: 143
Protocol Type	This parameter specifies the protocol to use when you are contacting the Cisco Unity Connection server. Choose one of the following values: • TCP • UDP • TLS Default: TCP

Presence Gateway Configuration Settings

Only two configuration settings exist in this release: Description and CallManager Presence Gateway.

Table 8 Presence Gateway Configuration Settings

Field	Description
Description	This parameter specifies the description of the presence gateway. Maximum characters: 255
CallManager PresenceGateway	This parameter specifies the fully qualified domain name or the IP address of the associated Cisco Unified CallManager server.

Scheduling Jobs

In the Finding a Job section of the *Cisco Unified Presence Server Administration Guide*, a new sentence appears in Step 8, to specify what you will see in the Job Configuration window:

You can view the status and the summary result of the job that you selected.

Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(2)

Noted or Deleted Information Not Applicable to CUPS

Throughout the document, information that does not apply to CUPS was either noted or deleted.

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of Severity level 1, 2, and 3.

Caveats describe unexpected behavior on a Cisco Unified Presence server. Severity 1 caveats represent the most serious caveats, Severity 2 caveats represent less serious caveats, and Severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Unified Presence Server 1.0(2) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section includes the following topics:

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

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

To use Bug Toolkit, follow this procedure.

Procedure

Step 1 To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.

Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco Unified Presence Server, go to the "Search for bugs in other Cisco software and hardware products" section and enter Cisco Unified Presence Server in the Product Name field. Alternatively, you can scroll through the product name list and click Cisco Unified Presence Server.

Step 4 Click **Next**. The Cisco Unified Presence Server search window displays.

Step 5 Choose the version and filters to query for caveats. You can choose any or all of the available options:

a. Choose the version to query.

b. Choose the Features or Components to query; make your selection from the "Available" list and click Add to place your selection in the "Limit search to" list.

- To query for all Cisco Unified Presence Server caveats, choose “All Features” in the left window pane.

Note The default value specifies “All Features” and includes all the items in the left window pane.

c. Enter keywords to search for a caveat title and description, if desired.

d. Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the **Fixed** check box for resolved caveats; check the **Open** check box for caveats that are not yet resolved.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.
- You can save your query for future use. See the “Saving Bug Toolkit Queries” section on page 14.

Note For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the “Using Bug Toolkit” section on page 13.

Step 2 In the search result window, click the **This Search Criteria** button that displays at the bottom of the window.

A new window displays.

Step 3 In the Name of saved search field, enter a name for the saved search.

Step 4 Under My Bug Groups, use one of the following options to save your defects in a bug group:

- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
- Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.

Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

Step 5 Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
  - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
  - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
- **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

For complete Cisco Unified IP Phone firmware release note information, refer to the applicable firmware release notes for your specific model IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/.

Open Caveats

Table 9 describes possible unexpected behaviors, which are sorted by component, in Cisco Unified Presence Server 1.0(2).

Note For more information about an individual defect, click the associated Identifier in Table 9 to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the "First Fixed-in Version" or "Integrated-in" fields. The information that displays in these fields identifies the list of Cisco Unified Presence interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Presence Server releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1.

Because defect status continually changes, be aware that Table 9 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "Using Bug Toolkit" section on page 13.

Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

.

Table 9 Open Caveats

Identifier	Headline
Component: CTI Gateway	
CSCsf17355	Support for inbound caller-name when Active Directory stores number in E.164.
Component: Database	
CSCse47551	Presence changes do not display.
CSCse80428	User cannot remove a downed subscriber ctigw node.
CSCsf07326	During high IPPM IM load, performance monitoring reports that the database has an high IO wait time.
Component: EPE	
CSCsf08033	In the Presence Engine logs, an error that indicates that a problem occurred in resolving the hostname prints out. The Presence Engine fails to initiate the autorecovery procedure.
Component: ESP	
CSCsd78497	Large TCP message does not print fully when StateMachine is used.
CSCsd78525	TCP debug does not print.
CSCsd94525	TCP debug messages do not follow serviceability formatting.
CSCse76600	Proxy server stops handling any TCP or TLS traffic, crashes and generates core file.
Component: GUI	
CSCse60410	Users cannot display all available CTI gateway profiles in CUPS administration.
CSCse70207	The CUPS export page is not accessible from Cisco Unified CallManager Administrator GUI.
CSCse86824	The CUPS end-user windows do not get localized properly.
Component: Install	
CSCse55244	During the startup of CUPS after installation, some "unresolved symbol" messages display on the console for the ipvmsapp process.
Component: IPPM	
CSCse74751	If the default method/event routing configurations get overwritten, IPPM login may not properly publish status or subscribe to buddies, which leaves the user unviewed by others and unable to see status of others.
Component: Serviceability	
CSCse57458	Remove extraneous SYSAPPL-MIB services from CUPS SNMP.
Component: SOAP Interface	
CSCse16839	CUPS keeps the unencrypted LDAP server login password in its database.
Component: Sync-agent	
CSCse58839	During initial database synchronization phase, user cannot activate the presence engine or proxy for a few hours.

Table 9 Open Caveats

Identifier	Headline
Component: VOS	
CSCsd52374	SNMP agent fails to recognize drive failure on new Cisco MCS 7825 Cisco Unified CallManager appliance server with serial ATA drives.
CSCse16130	During an upgrade of the CUPS image, some syslog warning messages print to the console window.
CSCse65392	VOS virtual memory leak occurred during a five day load test.
CSCse72226	The number of file descriptors that were being used kept growing on a five-day run.
CSCsf07358	High I/O wait CPU gets observed in "common" partition of the disk during IM state change stress test.

Troubleshooting

For troubleshooting information, refer to the *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)*. This document provides troubleshooting procedures for Cisco Unified CallManager systems. The *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)* provides guidance for network administrators who are responsible for managing the Cisco Unified CallManager system, for enterprise managers, and for employees. This document does not cover every possible trouble event that might occur on a Cisco Unified CallManager system but instead focuses on those events that are frequently seen by the Cisco Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have.PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non emergencies.

- For Non emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation" section.