Release Notes for the Cisco Unified Presence Server Release 1.0(3)

November 16, 2006

These release notes describe new documentation and caveats for Cisco Unified Presence Server, Release 1.0(3). For more specific information, see the "New and Changed Information for Cisco Unified Presence Server 1.0(3)" section on page 2, Important Information for Cisco Unified Presence Server 1.0(3), page 8, Documentation Updates for Cisco Unified Presence Server 1.0(3), page 8 and "Open Caveats" section on page 21.

Contents

These release notes include the following topics:

CISCO SYSTEMS

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, Release 1.0(3)*

- *Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(3)*

- *Cisco Unified Commications Operating System Administration Guide, Release 1.0(3)*

- *Disaster Recovery System Administration Guide*

Table 1 lists URLs for software and additional documentation.

Table 1   Quick Reference 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 documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
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 1.0(3)

The following information specifies new and changed information that the Cisco Unified Presence Server, Release 1.0(3) documentation contains.

LDAP Buddy

Cisco Unified Presence Server, Release 1.0(3) complies with RFC4479 and RFC4480 for all presence notifications. Cisco Unified Personal Communicator users will now be allowed to add contacts to their buddy list that are non-Cisco Unified Presence Server licensed Cisco Unified CallManager users and LDAP configured. These types of contacts will have directory information available, but will not have presence status.

Installing Cisco Unified Presence Server Release 1.0(3)

The following information specifies new and changed information that the installation guide contains.

- Associated Cisco Unified CallManager Server, page 3
- Performing Pre-Installation Tasks, page 3
- Performing Post-Installation Tasks, page 3

Associated Cisco Unified CallManager Server

Before you proceed with the Cisco Unified Presence Server Installation, consider the following requirements and recommendations.

- Ensure the associated Cisco Unified CallManager server is running software Release 5.1(1) or later.

Performing Pre-Installation Tasks

The pre-installation tasks now include the following task:

Before installing Cisco Unified Presence Server, ensure that you activate the Cisco AXL WebService on the associated Cisco Unified CallManager server. From Cisco Unified CallManager Serviceability window, choose **Tools > Service Activation**.

For More Information

- *Cisco Unified CallManager Serviceability Administration Guide*

Performing Post-Installation Tasks

After installing Cisco Unified Presence Server, you must set some configuration parameters and perform other post-installation tasks before you can begin using it. Perform these tasks for the first server that you install before you install the second Cisco Unified Presence Server node.

The list of post-installation tasks now includes the following task:

Activate the required Cisco Unified Presence Server services, including

- Cisco Enterprise SIP Proxy
- Cisco Enterprise Presence Engine

From the Cisco Unified Presence Server Serviceability window, navigate to **Tools > Service Activation**.

For More Information

- *Cisco Unified Presence Server Administration Guide* and the *Cisco Unified Presence Server Serviceability Administration Guide*.

Cisco Unified Presence Server Administration Guide, Release 1.0(3)

The following information specifies new and changed information that the *Cisco Unified Presence Server Administration Guide* contains.

Introduction

The *Cisco Unified Presence Server Administration Guide* now includes an introductory description..

Configuration Troubleshooter

Chapter 7 of the *Cisco Unified Presence Server Administration Guide, Release 1.0(3)* 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.

Table 2 contains the updated test descriptions that have been added in the *Cisco Unified Presence Server Administration Guide, Release 1.0(3)*.

Table 2   Configuration Troubleshooter Tests

Test Group	Test Description
Sync Agent	Verify that an AXL settings entry exists.
	Verify that the AXL user-id is valid.
	Verify that the publisher address is reachable, then log in and execute a basic query.
	Verify that the Sync Agent synchronized the relevant data (for example, devices, users, and licensing information).
	Verify that the Sync Agent service is running.

Table 2   Configuration Troubleshooter Tests (continued)

Test Group	Test Description
Presence Engine	Verify that the cisco Unified CallManage rPresence Gateway entry exists.
	Verify that the Presence Engine service is running.
	Verify that the Presence Engine OAM Agent service is running.
	Verify that the Presence Engine Database service is running
	Verify that the Cisco Unified CallManager Presence Gateway is valid (check reachability).
	Verify that a valid SIP trunk exists on the Cisco Unified CallManager server.
Proxy Server	Verify that the SIP Prozy service Proxy Domain service parameter
	Verify that the method/event routes exist.
	Verify that the SIP Proxy service is running.
	Verify that the Config Agent service is running.
IPPM **Note** IPPM only gets tested if it is enabled via **Application > IP Phone Messenger > Settings**.	Verify that an IPPM settings entry exists.
	Verify that the IPPM application usernames is valid.
	Verify that the IPPM application password is valid.
	Verify that the Cisco Unified Presence Server IPPM application username and password match the configured Cisco Unified CallManager application username and password.
	Verify that the IPPM service is active..
	Verify that the IPPM service is running.
CTI Gateway **Note** CTI Gateway only gets tested if it is enabledvia **Application > CTI Gateway > Settings**.	Verify that the CTI Gateway Settings entry exists.
	Verify that the CTI Gateway service is active.
	Verify that the Cisco Unified Presence Server application username and password match the currently configured Cisco Unified CallManager application username and password.
	Verify that the CTI Gateway service is running.
	Verify whether any users currently have Microsoft Office Communicator (MOC) assigned.

Transport Listeners

In the Transport Listeners chapter of the *Cisco Unified Presence Server Administration Guide* small changes that relate to the new menu location follow.

To add a transport listener, choose **Cisco Unified Presence Server > Transport Listeners** and click **Add New**.

User-Agent Configuration

The *Cisco Unified Presence Server Administration Guide* includes this new chapter.

You can now use the User-Agent Configuration window to configure the reachability version per Client User-Agent. Setting the reachability version provides backward compatibility with previous versions of Cisco Unified Personal Communicator. By default, reachability version 2, which complies with RFC 4479, gets used for all user-agents that are not specifically configured.

Unity Connection Server Configuration Settings

In the Unity Connection Server chapter of the *Cisco Unified Presence Server Administration Guide* the Protocol Type default in Table 25-1, as corrected, now reads UDP.

CTI Gateway Server Configuration Settings

In the CTI Gateway Server chapter of the *Cisco Unified Presence Server Administration Guide* in the Protocol Type description field in Table 29-1, UDP no longer appears in the list of protocols because UDP is no longer used.

LDAP Server Configuration Settings

In the LDAP Server chapter of the *Cisco Unified Presence Server Administration Guide* the following changes occur:

- In the Port description field in Table 31-1, the default, 389, has been added.
- In the Protocol Type description field in Table 31-1, the default, TCP, has been added.

Proxy Profile Configuration Settings

In the Proxy Profile chapter of the *Cisco Unified Presence Server Administration Guide,* Table 33-1 now includes the Proxy Listener field.

Status

In the Status chapter of the *Cisco Unified Presence Server Administration Guide,* Table 6-3, includes added information that relates to the Find/List columns. Each licensed Cisco Unified Presence Server user displays with additional per-user information, such as their primary extension, associated devices, contact, watchers, Cisco Unified Personal Communicator MOC assignments.

Cisco Unified Presence Server Serviceability Administration Guide

The following information specifies new and changed information that the *Cisco Unified Presence Server Serviceability Administration Guide* contains

- Configuring Trace Parameters, page 7.
- Cisco Unified Presence Server SIP Proxy Service Parameter Trace Filter Settings, page 7

Configuring Trace Parameters

This section describes how to configure trace parameters for Cisco Presence Server services. Several steps unrelated to Cisco Unified Presence Server were removed.

Cisco Unified Presence Server SIP Proxy Service Parameter Trace Filter Settings

When you configure trace parameters for a service that has multiple trace fields, such as the Cisco UPS SIP Proxy service, check the check boxes that display next to the trace fields that you want to enable. For a description of the Cisco UPS SIP Proxy service trace filter setting, see Table 3.

Table 3   **UPS SIP Proxy Service Parameter Trace Filter Settings**

Parameter	Description
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable IPPM Trace	This parameter enables tracing for IP Phone Messenger.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.

For More Information

Cisco Unified Presence Server Interoperability Guide

The following information specifies new and changed information that the *Cisco Unified Presence Server Interoperability Guide Guide* contains.

- Support for RFC4479 and CTI Gateway, page 8
- RFC4480, page 8

Support for RFC4479 and CTI Gateway

Support for RFC4479 and CTI Gateway has been added in this release of Cisco Unified Presence Server.

RFC4480

RFC4480 replaces "draft-ietf-simple-rpid-07" in this release of Cisco Unified Presence Server.

Important Information for Cisco Unified Presence Server 1.0(3)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Server 1.0(3).

- Cisco Unified Presence Server Update/Export Information, page 8

Cisco Unified Presence Server Update/Export Information

The Cisco Unified CallManager Bulk Administration Tool (BAT) Guide for Release 5.1(1) now includes procedures for updating and exporting Cisco Unified Presence Server users.

Documentation Updates for Cisco Unified Presence Server 1.0(3)

This section provides documentation changes that were unavailable when the Cisco Unified Presence Server 1.0(3) documentation suite was released.

- Cisco Unified Presence Server Documentation Guide for Release 1.0(3), page 8

Cisco Unified Presence Server Documentation Guide for Release 1.0(3)

- Troubleshooting Guide for Cisco Unified Presence Server, Release 1.0(3), page 8

Troubleshooting Guide for Cisco Unified Presence Server, Release 1.0(3)

The *Cisco Unified Presence Server Documentation Guide for Release 1.0(3)* lists the *Troubleshooting Guide for Cisco Unified Presence Server, Release 1.0(3)* as part of the documentation suite. The Troubleshooting Guide is not available for 1.0(3).

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

The following information specifies new and changed information that the Cisco Unified Presence Server 1.0(2) documentation contains:

- Cisco Unified Presence Server Deployment Guide, Release 1.0(2), page 9
- Configuration Troubleshooter, page 9

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

Bulk Assignment Considerations

You can use Bulk Assignment 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 4.

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 4   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 5.

Table 5 *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
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 for Cisco Unified Presence Server 1.0(2)

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified Presence Server 1.0(2).

- Support for Inbound Caller-Name When Active Directory Stores the Number in E.164, page 13
- Four-Way Conference Call with SIP Phone Moderator, page 13
- Publisher Server Cisco Unified Presence Server Upgrade, page 13
- Restarting Cisco Unified Presence Server Delays IPPM Services, page 13
- Fresh Installation on a Subscriber Can Result in the Inability to Activate Services on the Subscriber Node from the Publisher Node, page 13
- Running a Large BAT Job on Cisco Unified CallManager Can Result in Change Notification Not Working Properly., page 13
- Running a Large Synchronization from Cisco Unified CallManager to Cisco Unified Presence Server Over AXL May Cause Intermittent Timeouts in the NCSClient Connection., page 14

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 display 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 callthat is 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 Cisco Unified Presence Server Upgrade

Do not configure anything on the Cisco Unified CallManager publisher server while the Cisco Unified Presence Server 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 completes.

Restarting Cisco Unified Presence Server 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 Cisco Unified Presence Server 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 for Cisco Unified Presence Server 1.0(2)

This section provides documentation changes that were unavailable when the Cisco Unified Presence Server 1.0(2) documentation suite was released.

Updates

This section provides documentation updates that were unavailable when the Cisco Unified Presence Server 1.0(2) documentation suite was released.

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 Cisco Unified Presence Server configuration. This assignment now gets done in Cisco Unified CallManager under **System > Licensing > Capabilities Assignment**.

Omissions

This section provides documentation omissions that were left out of the Cisco Unified Presence Server 1.0(2) documentation suite

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

Errors

This section provides documentation errors that were in the Cisco Unified Presence Server 1.0(2) documentation suite.

- Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(2), page 15

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

This section provides documentation changes that were unavailable when the Cisco Unified Presence Server 1.0(2) documentation suite was released.

- Name Changes, page 15
- Cisco MeetingPlace Express Server, page 16
- Cisco MeetingPlace Express Profile Configuration Settings, page 16
- Unity Connection Profile Configuration Settings, page 17
- Unity Connection Host Configuration Settings, page 18
- Presence Gateway Configuration Settings, page 18
- Scheduling Jobs, page 18
- Cisco Unified Presence Server Serviceability Administration Guide, Release 1.0(2), page 19

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 that are allowed.
- The Description parameter field includes the maximum number of characters that are 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 6   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 you are 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 7.

Table 7   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 8.

Table 8   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 changed. It now includes a Name field and default information in the Port and Protocol Type fields as shown in Table 9.

Table 9   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.
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 10   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 Cisco Unified Presence Server

Throughout the document, text now notes or deletes information that does not apply to Cisco Unified Presence Server.

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, page 19
- Saving Bug Toolkit Queries, page 20

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 20.

> **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 19.

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 11 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 11 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 11 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 .

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 11   Open Caveats

Identifier	Headline
Component: CTI Gateway	
CSCsf01493	Cisco Unified Presence Server cores with ClearConnection Req missing Mandatory fields (Call-ID)
CSCsf02799	The CTI Gateway should wait until CTI provider open completed event to start sending.
CSCsf17355	Support for inbound caller-name when AD stores number in E.164
CSCsg13548	Unable to exercise CTI Control with Loadbalancer & Cisco Unified Presence Server TLS Enabled
CSCsg28116	Need Timer or Limit in the No. of Rings for Shared Line/Ext.Mobility
CSCsg44501	Do No Distrub Feature Support on Cisco Unified Presence Server.
Component: Database	
CSCsg07326	During high IPPM IM load, performance monitoring reports that the DB has an high IO wait time.
CSCsg32653	Debug flags for the Cisco Unified SIP Proxy Server in versions 1.0.1 and 1.0.2 do not get carried over during an upgrade to 1.0.3.
CSCsg56941	A dbmon core appeared on the subscriber node in the DB library code.
CSCsg69733	Multiple application crashed in subscriber Cisco Unified Presence Server node
Component: EPE	
CSCse88298	Second presence engine in the cluster fails to start.
CSCse89362	The presence engine on the second node of a cluster fails to start.
CSCse97453	The presence engine fails to start after a power outage or after a machine was rebooted without a graceful shutdown.
CSCsg20180	The presence engine fails to start after a machine reboot.
CSCsg45909	Presence engine core dump occurred; it may have happened under load when the Cisco Unified CallManager was rebooted.

Table 11 **Open Caveats (continued)**

Identifier	Headline
Component: ESP	
CSCsd78497	When ESP state machine debugs are enabled, any SIP message that is larger than 8192 bytes (8K) will get truncated in the trace file. The output includes only the first 8K of the message.
CSCsf21086	Shared memory size did not get set by processor type.
CSCsf98634	Some presence users do not receive presence information.
Component: GUI	
CSCse60410	User cannot see all available CTI gateway profiles for a user.
CSCse96284	Troubleshooter page remains blank when first node is down.
CSCsg18760	The end user and administrator can enter the exact same predefined message that is to be displayed in IPPM.
CSCsg28677	If a broadcast is attempted from the Cisco Unified Presence Server admin or end-user broadcast page after the page has timed out, then an Exception is seen.
CSCsg70400	Cisco Unified Presence Server Cisco Unified CallManager Gateway page should not allow users to add more than one entry
Component: Install	
CSCse55244	During the startup of Cisco Unified Presence Server after installation, some "unresolved symbol" messages display on the console for the ipvmsapp process.
CSCsg18964	In dual-node Cisco Unified Presence Server cluster, if an IPPM status is changed from a phone registered to Cisco Unified Presence Server publisher node, the status change does not get reflected in watchers that are registered to the second Cisco Unified Presence Server node.
Component: IPPM	
CSCsg66185	IPPM cores
Component: Phone	
CSCsg60735	If Japanese local is selected for the 7940 series phone, it causes an XML parse error.
Component: Serviceability	
CSCsd94525	ESP TCP debug messages that the proxy generates by the proxy do not follow the same formatting scheme as other debug messages. Although the messages are quite readable they do not use the same timestamp format and do not have the same postamble following the log message as other debug and log messages generated by the proxy.
Component: SOAP Interface	
CSCse38370	When publisher Cisco Unified Presence Server goes down, Cisco Unified Presence Ccommunicator cannot log in because the Cisco Unified Presence Server database is read only at the subscriber.
Component: Sync-agent	

Table 11   Open Caveats (continued)

Identifier	Headline
CSCse58839	During initial database synchronization phase, user cannot activate the presence engine or proxy for a few hours.
Component: VOS	
CSCsd52374	SNMP agent fails to recognize drive failure on new Cisco MCS 7825 Cisco Unified CallManager appliance server with serial ATA drives.
CSCse65392	During an upgrade of the Cisco Unified Presence Server image, some syslog warning messages get printed to the console window.
CSCse72226	The number of file descriptors are used kept growing on a five-day run.
CSCsf07358	High I/O wait CPU occurred in "common" partition of the disk during IM state change stress test.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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 nonemergencies.

- For nonemergencies — 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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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/en/US/support/index.html

Access to all tools on the Cisco Support 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   Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip   **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- 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 channel product 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

- *Internet Protocol Journal* is s a quarterly journal published by Cisco 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, 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 where networking professionals 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

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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