Release Notes for Cisco Unified CallManager Release 5.1(3g)

Updated May 21, 2009

Note You can view release notes for Cisco Unified CM Business Edition at http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html

Note You can view the release notes for previous versions of Cisco Unified CM here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

Before you install Unified CM, Cisco recommends that you review the "Important Notes" section on page 4 for information about issues that may affect your system.

Note To ensure continuous operation and optimal performance of your Unified CM system, you must upgrade to Cisco Unified CM 5.1(3g).

Cisco recommends that you check Cisco.com for the latest software updates to Unified CM and its applications and download and install the latest updates on your system before the deployment of your Unified CM system. For a list of commonly used URLs, see the "Upgrading System Software" section on page 3.

Contents

These release notes discuss the following topics:

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

Introduction

Cisco Unified CM, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

System Requirements

The following sections comprise the system requirements for this release of Unified CM.

Server Support

Make sure that you install and configure Cisco Unified CM Release 5.1(3g) on a Cisco Media Convergence Server (MCS) or a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

To find which MCS are compatible with Cisco Unified CM Release 5.1(3g), refer to the Supported Servers for Cisco Unified CM Releases, go here http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html.

Note Make sure that the matrix shows that your server model supports Unified CM Release 5.1(3g).

Note Be aware that some servers that are listed in the compatibility matrix may require additional hardware support for Unified CM Release 5.1(3g). Make sure that your server meets the minimum hardware requirements, as indicated in the footnotes of the compatibility matrix. Unified CM requires a minimum of 2 GB of memory, 72-GB disk drive, and 2-GHz processor.

Uninterruptible Power Supply

Ensure that you connect each Cisco Unified CM node to an uninterruptible power supply (UPS) to provide backup power and protect your system.

Caution Failure to connect the Cisco Unified Communication Manager nodes to a UPS may result in damage to physical media and require a new installation of Unified CM.

Determining the Software Version

To determine whether you need to upgrade the Cisco Unified CM software that you are using, launch Cisco Unified CM Administration. The following information displays:

- System version
- Administration version

Upgrading System Software

For information about supported Cisco Unified CM upgrades, see the *Cisco Unified Communications Manager Compatibility Matrix* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.

Note You can access the latest software upgrades for Cisco Unified CM 5.1 on Cisco.com.

Related Documentation

The following documentation supports Cisco Unified CM Release 5.1(3x):

- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Serviceability System Guide*
- *Cisco Unified Reporting Administration Guide*
- *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide*
- *Cisco Unified CallManager 5.1(3) Call Detail Records Definitions*
- *Troubleshooting Guide for Cisco Unified CallManager*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Release Notes*
- Adding a Cluster or Single Server for Cisco Unified CallManager Release 5.1(3)
- *Installing Cisco Unified CallManager Release 5.1(3)*
- *Upgrading Cisco Unified CallManager Release 5.1(3)*
- *Data Migration Assistant Administration Guide*
- *Cisco Unified CallManager Documentation Guide for Release 5.1(3)*
- Release Notes for Cisco Unified CallManager Release 5.1(3g)
- Cisco Unified Communications Operating System Administration Guide Release 5.1(1)

Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Cisco Unified CM System testing. The recommendations, which are not exclusive, represent an addition to interoperability recommendations for each individual voice application or voice infrastructure product.

For a list of software and firmware versions of IP telephony components and contact center components that were tested for interoperability with Cisco Unified CM 5.1(x) as part of Cisco Unified Communications System Release 5.1(x) testing, see

http://www.cisco.com/go/unified-techinfo

Note Be aware that the release of Cisco IP telephony products does not always coincide with Cisco Unified CM releases. If a product does not meet the compatibility testing requirements with Cisco Unified CM, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified CM Release 5.1(3). For the most current compatibility combinations and defects that are associated with other Cisco Unified CM products, refer to the documentation that is associated with those products.

Important Notes

Important Notes for Cisco Unified CM 5.1(3g)

Important Notes for Cisco Unified CM Releases 5.1(3, a, b, c, d, e, f).

The following section contains important information that may have been unavailable previously.

Defects That Are Resolved in Cisco Unified CM 5.1(3g)

The following defects are resolved in the 5.1(3g) release of Unified CM.

- CSCsx32236 SCCP port gets closed in response to FD resource exhaustion.
- CSCsz40392 Coredump occurs in sipSafeStrlen.
- CSCsx23689 SIP port gets closed in response to FD resource exhaustion.
- CSCsz24525 md5sum checksum on UCS Install ISO file fails with -c option.
- CSCta94180 H323 performance gets degraded due to port 1720 CSA policy.
- CSCta43460 Critical BIOS update for x306m-8849 / x206m-8485 - 7815/25/I2.
- CSCsz86131 DST: Cisco Unified CM update needed for 2009 W. Australia DST removal.
- CSCsz68252 Install fails due to critical error sd_zoneinfo unrecoverable.
- CSCsz11007 Memory leak causes processes to be killed by OOM Killer.
- CSCsq22534 IPConntrack fills up during TCP flood attack.
- CSCso02681 csadiagnosticszip file creation needs to get added to Unified CM linux builds.

CSCsm60522 ServM Hangs After an Upgrade

After an upgrade, the web admin of the second subscriber server was not accessible.

The release of Cisco Unified CM Release 5.1(3f) resolved this difficulty.

CSCsy25150 Unified CM Does Not Send Daylight Saving Time Updates

Earlier releases of Unified CM 5.1(3) did not send Daylight Savings Time updates to Cisco IP Phones.

For important information about this issue, see the Field Notice at:
http://www.cisco.com/en/US/customer/ts/fn/632/fn63213.html

More DST fixes included in this release:

- CSCsy60141 DNA does not display correct results as per DST changes for MST.
- CSCsm60718 Hardware clock configuration mismatch exists.
- CSCsy70131 TFTP server is not clearing its internal cache properly when it receives a change notification for datetimesetting.

CSCsy17534 Upgrades from Unified CM 5.1(3) to Unified CM 7.1(x) Are Blocked

In previous releases of Unified CM 5.1(3), users could not upgrade to Unified CM 7.1 or higher.

Cisco Unified CM 5.1(3f) resolved this inconsistency.

CSCsx94914 Disable NonRegistered SCCP KeepAlives Service Parameter Forced to False

On systems that were upgraded to an Engineering Special (ES) or Unified CM release that resolves CSCsa67496, when TCP sessions to TCP port 2000 get initiated and then abandoned, the sessions remain in the established state on the server because ccm.exe never closes the session. This causes a TCP connection leak and a memory leak, which results in low virtual memory.

In Cisco Unified CM Release 5.1(3f) and later, the Disable NonRegistered SCCP KeepAlives service parameter gets forced to False so the leaks do not occur.

More Caveats That Are Resolved in Cisco Unified CM 5.1(3x)

In addition to the caveats that are mentioned elsewhere in this document, the following caveats get resolved in this release of Unified CM.

- CSCsk86705 ForwardAll CFA removed from CCMUser window.
- CSCsu93547 Search of CTI route points by dev name returns multiple names for the same dev.
- CSCsu77940 EM logout or other notify gets delayed for up to a minute.
- CSCsr86439 Requirement exists for IDP release note documentation.
- CSCsu63446 "QRT: enhance thread mutex handling in case of http failure" occurs.
- CSCsu78475 SMDI link server does not work properly.
- CSCsa67496 Default value for, Disable Non-Registered SCCP Keepalives service parameter should be changed to "False".
- CSCsw63783 Map disconnect cause 31 to 16 occurs when call is in Active10 state.

- CSCso96280 Core dump and Unified CM CTI service crash.
- CSCsm46064 Problem occurs when Unified CM sends out an invite via tel URI.
- CSCsu38644 Valid SIP message causes CCM process to crash.
- CSCsr20762 Need exists for product name in ISO filename.
- CSCsl21150 Zero file size directory prevents upgrade recognition.
- CSCso75027 TSP buffer overflow causes CTI crash.
- CSCsm80834 Need exists for clusterreset to ignore commented-out lines in sqlhosts.
- CSCsb80753 ExecuteSQLQuery returns error.
- CSCso53771 Unauthenticated access to disaster recovery framework occurs.
- CSCso11097 Upgrade causes a corruption of the RAID controller firmware on an MCS-7845-I2 server.
- CSCsm87181 Utils service stop/start/restart for "A cisco DB" service does not work.
- CSCsm83602 When you modify a phone button template, a large number of change notifys get generated.
- CSCsm78770 Tomcat displays OutOfMemory error.
- CSCsm67799 Need exists for a default alert in RTMT Alert Central for database in blockedDDR.
- CSCsm32426 Cannot repair or reset replication after virtual shared memory runs out.
- CSCsl16967 DRSSticks in Unified CM database backup if a large number of CDR files exist in the preserved folder.
- CSCsl15544 VG248 and VG224 registration errors cause high CPU usage that result in a database block.
- CSCsk99178 Cisco TSP crashes when the application sends multiple LineOpenPhoneOpen.
- CSCsk97288 SRST reference update causes massive change notification storm.
- CSCsk62547 ServM process increases memory use with each backup.
- CSCsk38023 CiscoTSP Wave Driver Vista support
- CSCsk35503 CiscoTSP Windows Vista support
- CSCsk10706 Missing, mismatched and/or corrupted tables exist on subscriber nodes if replication gets broken during a replicate set.
- CSCsk06916 ST cannot allocate memory from the virtual shared memory.
- CSCsj95909 The CTL client plugin does not install or does not work properly on Vista systems.
- CSCsj53293 Remote unauthenticated users can log out any extension mobility (EM) user from a Unified CM server.
- CSCsi70926 TSP seacquire causes intermittent issues.
- CSCsg70952 TSP reports that a phone is not in a CFA state; however, the CFA is configured on the phone.
- CSCsg06024 PMR 84055 Tomcat server down because of database engine DDR block.
- CSCec27300 CiscoTSP restricts the number of characters in a username to a maximum of 30.

Cisco UXL Web Service Added to Service Activation Window

In most Cisco Unified CM releases, the TabSync client in Cisco IP Phone Address Book Synchronizer uses AXL for end-user queries to the Cisco Unified CM database. In Cisco Unified CM 5.1(3x), the TabSync client uses the Cisco UXL Web Service for queries to the Cisco Unified CM database, which ensures that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them.

In the Service Activation window in Cisco Unified CallManager Serviceability (**Tools > Service Activation**), you can activate the Cisco UXL Web Service, which performs the following functions:

- Conducts authentication checks by verifying the end user name and password when an end user logs in to Cisco IP Phone Address Book Synchronizer.
- Conducts a user authorization check by only allowing the user that is currently logged in to Cisco IP Phone Address Book Synchronizer to perform functions such as listing, retrieving, updating, removing, and adding contacts.

Caution You cannot upgrade to a release that does not include this service. Please see the compatibility matrix at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.

Recovery Disk for Cisco Unified CM Release 5.1(3g)

The recovery disk for this release of Unified CM remains

5.1.3.1000-12_recovery.iso

(Cisco Unified CallManager Recovery Disk for 5.1(3) 5.1(3) 01-OCT-2007 209682432)

Important Information About Update or Delete Transaction by Using Custom File in BAT

Do not use the insert or export transaction file or files that are created with bat.xlt for the custom file-based transactions in BAT. Instead, you must create a custom file with the details of the records that need to be updated or deleted. In this custom file, you can enter values for name, description, and user ID based on the search option available on the corresponding custom file-based Find/List page. Make sure that you do not include a header in this file. For example, for **Update Phones > Custom File**, if you select Device Name as the search option, the custom file should contain only device names without the header.

Cisco Unified CM Does Not Support Recovery of Administration or Security Passwords

Cisco Unified CM does not support recovery of administration or security passwords. If you lose these passwords, you must reset the passwords, as described in the *Cisco Unified Communications Operating System Administration Guide*.

The *Cisco Unified Communications Operating System Administration Guide* calls the section, "Recovering the Administrator or Security Passwords," instead of "Resetting the Administrator or Security Passwords." Access the "Recovering the Administrator or Security Passwords" section to reset the passwords.

Clarification for Call Park Configuration

Consider the following information when you configure Call Park:

Because Call Park numbers cannot overlap between Cisco Unified CM servers, ensure that each Cisco Unified CM server has its own unique number range.

Call Park numbers may have an associated partition that restricts access to the Call Park numbers and prevents retrieval of parked calls. If partitions are used to restrict access to Call Park numbers, you must define a unique call park number or range of call park extension numbers for each partition on each Cisco Unified CM in the cluster.

When the end user invokes Call Park, Cisco Unified CM attempts to find an available Call Park number from a Call Park partition that is currently accessible via the calling search space for the party that invoked Call Park.

Viewing Privileges for Roles in Cisco Unified CM Administration

The Role Configuration window in Cisco Unified CM Administration displays the privileges for each standard role. To access the Role Configuration window, find the role by choosing **User Management > Role**; when the Find and List Roles window displays, click **Find**. Click the link for the standard role that you want to view. After the Role Configuration window displays, you can view the privileges in the Resource Access Information pane.

TAPS Name Change in Bulk Administration Tool

Documentation refers to the Tool for Auto-Registered Phone Support (TAPS) as Cisco Unified CallManager Auto-Register Phone Tool in the Online Help for Bulk Administration. All references to 'Cisco Unified CallManager Auto-Register Phone Tool' in the Bulk Administration Tool Online Help should be read as 'Tool for Auto-Registered Phone Support (TAPS)'. This complies with the Bulk Administration user interface.

For More Information

For information on configuring additional features in BAT, refer to the BAT documentation for Cisco Unified CM.

CSCsk86705 ForwardAll CFA Removed from CCMUser Window

The options for the Show Call Forwarding enterprise parameter specified only True and False. The need existed for a third option, Show Only Forward All.

Unified CM Release 5.1(3d) resolved this caveat.

CSCsl71487 Cimserver Memory Leak Fix

RTMT and perfmon counters show that the cimserver process consumes increasing amounts of memory on IBM MCS servers. Over a period of several weeks, cimserver gradually consumes the majority of available virtual memory and eventually causes the server to hang.

Unified CM 5.1(3d) included the fix for this memory leak.

Do Not Log On to the Console During Busy Hours

Because of the CPU resources that are consumed, Cisco does not recommend that you log on to the console during busy hours. If you log on during busy hours, Code Yellow or Code Red alarms may be raised, depending on the tasks that are being performed and the CPU that is utilized to perform those tasks. Cisco recommends that console usage (remote or local) be limited to maintenance or upgrades during Maintenance windows.

(Cisco Unified CallManager Recovery Disk for 5.1(3) 5.1(3) 01-OCT-2007 209682432)

New CLI Command - utils dbreplication clusterreset

This release of Unified CM includes a new CLI command, **utils dbreplication clusterreset** .

This command can be used to debug database replication, but should only be used if **utils dbreplication reset all** has previously been tried and has failed to restart replication on the cluster. This command will tear down and rebuild replication for the entire cluster. After using this command, each sub needs to be rebooted. Also, once the subs have been rebooted, you must go to the pub and issue the CLI command **utils dbreplication reset all**.

Voice Mailbox Mask Interacts with Diversion Header

When a call gets redirected from a DN to a voice-mail server/service that is integrated with Unified CM by using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. This expected behavior occurs because the diversion header gets used by the Unified CM server to choose a mailbox.

CSCso45910 - The Server Will Not Boot to the New Partition.

Prior to this release, after an upgrade, the server would not boot to the new partition.

This release of Unified CM resolves this caveat.

Cisco TSP Vista Support

Cisco TSP supports the Microsoft Vista operating system.

Ensure that the first-time installation of the CiscoTSP and Unified CM TSP Wave driver on a computer that is running the Vista operating system gets performed as a fresh install.

CiscoTSP Limitations on Windows Vista Platform

Always perform the first-time installation of the CiscoTSP and Unified CM TSP Wave Driver on a Vista machine as a fresh install.

- Turn off the Windows firewall if a secure connection to the Unified CM gets used.
- Turn off the Windows firewall if the Unified CM TSP Wave Driver gets used for inbound audio streaming.
- Disable all other devices in the "Sound, video and game controllers" group if the Unified CM TSP Wave Driver gets used for audio streaming.

CSCsm47603 BIOS Upgrade Required

The E6400 processor that IBM includes in their 7825I3 servers does not get supported by the BIOS that is bundled with Cisco Unified CM Release 5.1(3). Because of this, Unified CM Release 5.1(3) downrevs the BIOS to an unsupported version during installation or upgrade. Unfortunately, during startup, the system simply warns the user by displaying a warning message. The customer will not see this message if he is not constantly looking at the terminal. The system allows startup to continue in the unsupported state. The implications of running in this state remain unknown.

This release of Cisco Unified CM resolves this problem.

Australia Summer Time

This year, Australia Summer Time ends on April 6, 2008.

Summer Time begins again at 2:00AM October 5, 2008 (the first Sunday in October) and ends at 2:00AM on April 5, 2009 (the first Sunday in April).

This release of Cisco Unified CM includes the specific dates for the Australia Summer Time changes for this year.

Venezuela Implements New Time Zone

Venezuela implemented a new time zone that is one-half hour behind the previous time zone (GMT-4).

Cisco Unified CM Release 5.1(3a) incorporated this new time zone into Cisco products that are used in Venezuela.

Address Resolution Protocol (ARP) Table Can Fill Up Quickly

Do not install Cisco Unified CM in a large Class A or Class B subnet that contains a large number of devices because the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified CM can have difficulty talking to endpoints and cannot add more phones.

Cisco Unified CallManager Administration Does Not Support Browser Buttons

Cisco Unified CallManager Administration does not support the buttons in your browser. Do not use the browser buttons (for example, the Back button) when you perform configuration tasks.

Internet Explorer 7 Certificate Support

This release supports Internet Explorer 7 web browser for Cisco Unified CallManager Administration. Internet Explorer 7 adds security features that change the way the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified CM server, Internet Explorer 7 flags the Cisco Unified CallManager Administration website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1).

Be sure to import the Cisco Unified CM certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 retains the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified CM certificate to the root certificate trust store in Internet Explorer 7.

Ensure JRE is present to provide all the Java-related browser support for IE6 or IE7.

Procedure

Step 1 Enter the hostname, localhost, or IP address for the Cisco Unified CallManager Administration website. The browser displays a Certificate Error: Navigation Blocked window to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**. The Cisco Unified CallManager Administration displays, and the browser displays the address bar and a Certificate Error status in red.

Step 3 To import the server certificate, click the **Certificate Error** status box to display the status report. Click the **View certificates** link in the report.

Step 4 Verify the certificate details. The Certification Path tab displays, “This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.”

Step 5 Select the General tab in the Certificate window and click **Install Certificate**. The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**. The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**. A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**. The Import Wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.

Step 12 After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

Internet Explorer 7 Support

The following applications now support Internet Explorer 7:

- Cisco Unified CallManager Administration
- Cisco Unified CallManager Bulk Administration Tool (BAT)
- Cisco Unified CallManager Serviceability
- Disaster Recovery System (DRS)
- Cisco Unified CallManager Operating System (OS)
- Cisco Unified CallManager CDR Analysis and Reporting (CAR)

New Cisco Unified Reporting Application

The new Cisco Unified Reporting web application, which is accessed at the Cisco Unified CM console, generates reports for troubleshooting or inspecting cluster data.

This convenient tool provides a snapshot of cluster data without requiring multiple steps to get the data. The tool design facilitates gathering data from existing sources, comparing the data, and reporting irregularities.

A report combines data from one or more sources on one or more servers into one output view. For example, you can view a report that shows the *hosts* file for all servers in the cluster.

The application gathers information from the publisher server and each subscriber server. A report provides data for all active cluster nodes that are accessible at the time that the report is generated.

Some reports run checks to identify conditions that could impact cluster operations. Status messages indicate the outcome of every data check that is run.

Only authorized users can access the Cisco Unified Reporting application. By default, this includes administrator users in the Standard Unified CM Super Users group. As an authorized user, you can view reports, generate new reports, or download reports at the graphical user interface (GUI).

Cisco Unified Reporting includes the following capabilities:

- A user interface for generating, archiving, and downloading reports
- Notification message if a report will take excessive time to generate or consume excessive CPU

Refer to the *Cisco Unified Reporting Administration Guide* for more information.

Updating the Hostname or IP Address in the Server Configuration Window

Before you change the hostname or IP address of a server in the Server Configuration window in Cisco Unified CallManager Administration, consider the following information:

- Cisco Unified CallManager Administration does not prevent you from updating the Host Name/IP Address field under any circumstances.
- When you attempt to change the hostname or IP address in the Server Configuration window, the following message displays after you save the configuration: "Changing the host name/IP Address of the server may cause problems with Cisco Unified CallManager. Are you sure that you want to continue?" Before you click OK, make sure that you understand the implications of updating this field; for example, updating this setting incorrectly may cause Cisco Unified CallManager to become inoperable; that is, the database may not work, you may not be able to access Cisco Unified CallManager Administration, and so on. In addition, updating this field without performing other related tasks may cause problems for Cisco Unified CallManager.
- For additional information on changing IP address/hostnames for Cisco Unified CM, refer to *Changing the IP Address and Host Name for Cisco Unified Communications Manager 5.x and 6.x Servers*.

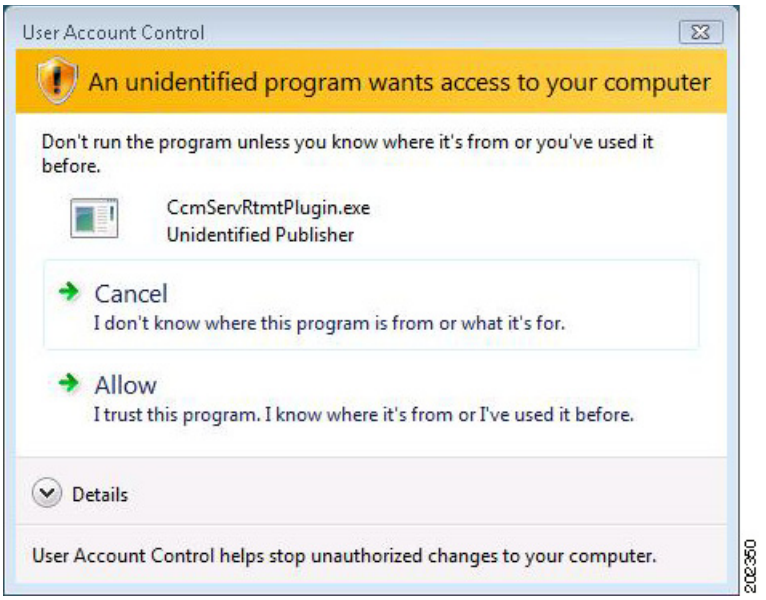
SIP Network/IP Address Field Required for SIP Fallback to SRST Gateway

Although Cisco Unified CallManager Administration does not list the SIP Network/IP Address field as a required setting, you must configure the SIP Network/IP Address field and the SIP Port field in the SRST Reference Configuration window for a SIP device to fall back to the SRST-enabled gateway. For more information on these fields and SRST references, refer to the *Cisco Unified CallManager Administration Guide*.

RTMT on the Microsoft Vista Platform

When you install RTMT on the Microsoft Vista platform, the system displays the User Account Control popup window that is shown in Figure 1 due to a limitation in the InstallAnywhere software. This one-time popup displays only when you are installing RTMT. Select **Allow** to continue.

Figure 1 User Account Control Popup Window



CSCsj22450 Login Failure Does Not Send a Message to the Syslog

This resolved caveats adds the following alarm catalog and two alarms:

LoginAlarmCatalog:

AuthenticationFailed - When a web application login attempt fails

AuthenticationSucceeded - When a web application login attempt succeeds

The alarm events get logged in to the local and remote SYSLOG.

Note No corresponding alerts exist for these two authentication alarms.

CSCsh58895 Unified CM Cannot Send System or Platform Agent Logs to Remote Syslog Server

Unified CM can now send syslog messages to a remote server.

You can configure two new enterprise parameters from **Cisco Unified CallManager Administration > System > Enterprise Parameters**:

- Remote Syslog Server Name - You can enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Note The Unified CM server does not accept Syslog messages from another server.

Remote Syslog Server Name:

  - Maximum length: 255
  - Allowed values: Provide a valid remote syslog server name that comprises (A-Z,a-z,0-9,.,-)
- Syslog Severity For Remote Syslog messages - You can select the desired Syslog messages severity for remote syslog server. The system sends all the syslog messages with selected or higher severity levels to the remote syslog. If the remote server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

RTMT Requirement When Unified CM is Upgraded

If you are running the Cisco Unified Communications Real-Time Monitoring Tool (RTMT) client and monitoring performance counters during an upgrade, the performance counters will not update during and after the upgrade. To continue monitoring performance counters accurately after the upgrade completes, you must either reload the RTMT profile or restart the RTMT client.

iLO Flashing Causes the Login Window to Disappear After Installation or Upgrade

As part of the installation or upgrade processes, the iLO firmware in the servers gets flashed. During the flashing, messages display for the convenience of the user. Because of this, after the installation or upgrade completes, the default login window gets masked by the messages.

To see the login window, click **Enter**.

Serviceability Session Timeout Not Graceful

When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before indicating that the session has timed out and redirecting you to the login window. After you log in again, you may need to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. The only workaround requires you to log out by using the Logout button before making any changes in the user interface if you know that the session has been idle for more than 30 minutes.

New and Changed Information for Unified CM 5.1(3x)

The following section contains information that is new or changed for Unified CM Release 5.1(3x).

- Cisco Unified IP Phones, page 33
- Cisco Unified CallManager Serviceability, page 47
- Operating System CLI Commands, page 35

Disaster Recovery Manual Backup Window

Disaster Recovery System backs up CAR/CDR data automatically when you check the CCM checkbox on the Manual Backup window. The Manual Backup window no longer contains a CAR/CDR checkbox.

New Service Parameters Added to Extension Mobility

Extension Mobility includes four new service parameters. You can find these new parameters at **System > Service Parameters > Cisco Extension Mobility > Advanced.**

- Validate IP Address, page 17
- Trusted List of IPs, page 18
- Allow Proxy, page 18
- Extension Mobility Cache Size, page 18

Validate IP Address

This parameter specifies whether validation of the IP address of the source that is requesting login or logout occurs.

The parameter can take values of true or false.

- If the parameter specifies true, the IP address from which an EM log in or log out request is made gets validated to ensure that it is a trusted IP address.

  Validation Procedure

  - Validation first gets performed against the cache for the device to be logged in or logged out.
  - If the requesting source IP address is not found in cache, the IP address gets checked against the list of trusted IP addresses and hostnames that are specified in the Trusted List of IPs service parameter.
  - If the requesting source IP address is not present in the Trusted List of IPs service parameter, it gets checked against the list of devices that are registered to Unified CM.

  Validation Effect

  - If the IP address of the requesting source is found in the cache or in the list of trusted IP addresses or is a registered device, the device can perform login or logout.
  - If the IP address is not found, the log in or log out attempt gets blocked.
- If the parameter specifies false, the EM log in or log out request does not get validated.

Note Validation of IP addresses may increase the time that is equired to log in or log out a device, but it offers an additional layer of security in the effort to prevent unauthorized log in or log out attempts, especially when used in conjunction with log ins from separate trusted proxy servers for remote devices.

For more information, refer to the design guidelines in the extension mobility documentation.

Trusted List of IPs

This parameter displays as a text box (maximum length - 1024 characters). You can enter strings of trusted IP addresses or hostnames, separated by semicolons, in the text box. IP address ranges and regular expressions do not get supported.

Allow Proxy

Allow Proxy can take values of true or false.

- If the parameter specifies true, the system allows EM log in and log out operations using a web proxy.
- If the parameter specifies false, EM log in and log out requests that come from behind a proxy get rejected.

Note The setting that you select takes effect only if the Validate IP Address parameter specifies true.

Extension Mobility Cache Size

This parameter displays as a text box in which the administrator can configure the size of the device cache that is maintained by extension mobility. The minimum value for this field specifies 1000, and the maximum specifies 20000. The default specifies 10000.

Note The value you enter takes effect only if the Validate IP Address parameter specifies true.

New Cisco IP Phone Expansion Modules Supported

Cisco Unified CallManager now includes support for the following Cisco Unified IP Phone expansion modules:

- 7915 12-Button Line Expansion Module
- 7915 24-Button Line Expansion Module
- 7916 12-Button Line Expansion Module
- 7916 24-Button Line Expansion Module

Installation, Upgrade, and Disaster Recovery

Installation Overview

For release 5.1(3x), the Cisco Unified CM installation process includes the following new features:

- Process allows you to set the maximum transmission unit (MTU) size
- Enhanced validation ensures that a subsequent node can communicate with the first node

MTU Size Parameter

During installation, you can configure the MTU size parameter. The MTU size represents the largest packet, in bytes, that the host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, 1500 bytes.

Note You can also set the MTU size after installation by using the CLI command, **set network mtu**.

Enhanced Connectivity Validation

To ensure successful installation of a subsequent node, the system validates that the subsequent node can connect with the first node.

If connectivity validation fails, the installation process stops, and the system prompts you to reenter the network configuration information. After you update the network configuration information, you can continue with the installation.

Prior to connectivity validation, from the Network Connectivity Test Configuration window, you can choose whether you want the installation process to continue uninterrupted after a successful validation test or stop and display a successful validation message.

- To pause the installation after the system successfully validates network connectivity, choose **Yes**.
- To continue the installation without a pause, choose **No**.

Enhanced Documentation

For Release 5.1(3x), enhancements to the installation and upgrade documentation cover additional pre- and post-installation tasks, as well as specific steps for adding a new subscriber node to an existing cluster.

The Release 5.1(3x) documentation set also includes a new document that describes the procedures for replacing a cluster or a single server in an existing cluster, *Replacing a Cluster or Single Server for Cisco Unified CallManager Release 5.1(3).*

Disaster Recovery System

DRS now backs up CAR/CDR data automatically. You do not need to select the CAR/CDR feature to back up this data.

Where to Find More Information

For more information, refer to the following documents:

- *Installing Cisco Unified CallManager Release 5.1(3)*
- *Upgrading Cisco Unified CallManager Release 5.1(3)*
- *Replacing a Cluster or Single Server for Cisco Unified CallManager 5.1(3)*
- Disaster Recovery System Administration Guide Release 5.1(3)

Cisco Unified CallManager Administration

This section contains information on the following topic:

General Administration Enhancements

The following requirements apply to Cisco Unified CallManager Administration:

- Microsoft Internet Explorer (IE) 6.0 or 7.0
- Netscape 7.1

Note This release does not support Microsoft IE 5.5 or Netscape 7.0.

Service and Enterprise Parameter Changes

The following parameter changes occur in Unified CM 5.1(3x).

- SIP TCP Unused Connection Timer (new service parameter)—This parameter, which supports the Cisco CallManager service, specifies the time, that is, the interval, in which Cisco Unified CallManager determines whether the TCP connection is still in use. When the timer expires, Cisco Unified CallManager checks for traffic in the preceding block of time, as specified by the value that you configure for the parameter; for example, 20 minutes. If no traffic occurred during that time, Cisco Unified CallManager closes the TCP connection. If traffic occurred, the TCP connection remains open until the timer expires again, at which point Cisco Unified CallManager checks for traffic again.

  For example, if the value for the parameter equals 20 minutes and the timer expires at 3:00, Cisco Unified CallManager examines the time from 2:40 to 3:00. If traffic occurred during that time, the connection remains open until the next examination at 3:20. If no traffic occurred from 3:00 to 3:20, Cisco Unified CallManager closes the TCP connection at or shortly after 3:20. If traffic occurred from 3:00 to 3:20, the TCP connection remains open until Cisco Unified CallManager checks for traffic again at 3:40, and so on.

  After you update this parameter, you must restart the Cisco CallManager service for the changes to take effect.

  For the default, maximum, and minimum values for the parameter, access the parameter in Cisco Unified CallManager Administration and either click the name of the service parameter or click the ? button in the Service Parameter Configuration window.

Note If you have other devices in the path of a call flow that includes a SIP timeout, like a firewall, you need to adjust those timeouts to be slightly longer than two times the value of this parameter.

- Auto select DN on any Partition (new enterprise parameter)—This parameter specifies whether the Directory Number Configuration window automatically selects the first matching DN to populate the window. The default specifies False, which means that the DN/Partition name gets used to populate the DN window. If the parameter is set to True and the DN is changed, the first entry that matches the DN gets used to populate the window.

- Report Socket Connection Timeout and Report Socket Read Timeout (two new enterprise parameters) - These two parameters support the Cisco Unified Reporting application, as follows:
  - The Report Socket Connect Timeout parameter specifies the maximum number of seconds that the application uses when it attempts to connect to another server. Increase this time if you experience connection issues on a slow network. The range for this required field specifies 5 to 120 seconds, and the default value specifies 10 seconds.
  - The Report Socket Read Timeout parameter specifies the maximum number of seconds that the application uses when it reads data from another server. Increase this time if you experience connection issues on a slow network. For this required field, the range specifies 5 to 600 seconds, and the default value specifies 60 seconds.

Refer to New Cisco Unified Reporting Application in the "Important Notes" section on page 4 for a brief description of the application.

Cisco Unified CallManager Applications and Features

The following sections describe the Cisco Unified CallManager 5.1 applications enhancements:

CSCsi80592 MTP Resources Do Not Support Multicast Music on Hold

The following restriction exists for multicast music on hold (MOH) when a media termination point (MTP) is invoked. When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, the caller receives silence instead of music on hold. To avoid this scenario, configure unicast MOH or Tone on Hold instead of multicast MOH

Cisco Unified CallManager Assistant

In Unified CM 5.1(3x), the assistant no longer obtains the assistant console application via a URL that the administrator provides; instead, a plug-in from Cisco Unified CallManager Administration gets downloaded and installed on the assistant PC.

The assistant console application installation supports Netscape 7.1 (or later) and Microsoft Internet Explorer 6.0 (or later). You can install the application on a PC that runs Windows 2000, Windows XP, or Windows Vista [new support for 5.1(3x)].

A previous 5.x version of the assistant console application works with Cisco Unified CallManager 5.1(3x), but if you decide to install the 5.1(3x) plug-in, you must uninstall the previous 5.X version of the assistant console application before you install the plug-in.

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to 5.1(3x), you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

Uninstalling the Assistant Console Application

To uninstall previous versions of the assistant console application, choose **Start> Programs > Cisco Unified CallManager Assistant > Uninstall Assistant Console**.

To uninstall the new plugin-based assistant console application, go to the Control Panel and remove it.

Tip The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified CallManager Assistant.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse into Cisco Unified CallManager Administration and choose **Application > Plugins**.

Step 2 For the Cisco Unified CallManager Assistant plug-in, click the **Download** link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click **Next**.

Step 5 Accept the license agreement and click **Next**.

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click **Next**.

Tip By default, the application installs in C:\Program Files\Cisco\ Unified CallManager Assistant Console.

Step 7 To install the application, click **Next**.

The installation begins.

Step 8 After the installation completes, click **Finish**.

Tip To launch the assistant console, click the desktop icon or choose **Cisco Unified CallManager Assistant > Assistant Console** in the Start...Programs menu.

Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Unified CM server where the Cisco IP Manager Assistant service is activated. The first time that the assistant logs in to the console, the assistant must enter the information in the Cisco Unified CallManager Assistant Server Port and the Cisco Unified CallManager Assistant Server Hostname or IP Address fields.

Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

The Advanced tab in the Cisco Unified CallManager Assistant Settings window allows you to enable trace for the assistant console.

Cisco and Third-Party APIs

These following sections describe new features and changes that are pertinent to Release 5.1(3x) of the Cisco Unified CM APIs and the Cisco extensions to third-party APIs.

Windows Vista Support

Unified CM Release 5.1(3x) adds support for Cisco TAPI and Cisco JTAPI on the Windows Vista platform.

For information about the JVM versions that Cisco JTAPI supports on Windows Vista and other platforms, see Table 2 on page 28.

Route Patterns, Automated Alternative Routing, and Applications

Unified CM only applies Automated Alternative Routing (AAR) to the endpoints that it controls. Network congestion and bandwidth restrictions can cause tail-end hop-off (TEHO) calls to fail if you configure Unified CM to use AAR. To provide failover support for route patterns, you must configure the route lists to take advantage of their built-in redundancy.

Application developers who use the Unified CM TAPI and JTAPI APIs should be aware of this behavior.

AXL Programming

The following table summarizes the AXL schema changes in Release 5.1(3x):

Table 1 AXL Schema Changes

Affected APIs	New and Modified Tags	Change
addPhone updatePhone getPhone	callingSearchSpaceName	Changed type from axl:Name128 to axl:String50 in axl.xsd and axlsoap.xsd
addTranslationalPattern updateTranslationalPattern getTranslationalPattern	callingSearchSpaceName	Changed type from xsd:string to axl:String50 in axl.xsd and axlsoap.xsd
addRouteList updateRouteList getRouteList	callingSearchSpaceName	Changed type from xsd:Name to axl:String50 in axl.xsd and axlsoap.xsd
addHuntList updateHuntList getHuntList	callingSearchSpaceName	Changed type from xsd:Name to axl:String50 in axl.xsd and axlsoap.xsd
addPilotPoint updatePilotPoint getPilotPoint	callingSearchSpaceName	Changed type from axl:UniqueName50 to axl:String50 in axl.xsd and axlsoap.xsd
addPhone updatePhone getPhone	authenticationString	Changed type from axl:Name128 to axl:String50 in axl.xsd and axlsoap.xsd
addPhone updatePhone getPhone	upgradeFinishTime	Changed type from xsd:time to xsd:string
getPhone	dirn	Included minOccurs=0 to XNumPlan in axl.xsd, thereby making it optional

The change in the **callingSearchSpaceName** tag to String50 type affects APIs that inherit from Device. The change also affects add, get, and update APIs of CTIRoutePoint, DevicePool, DeviceProfile, DirectedCallPark, GatewayEndPoint, H323Gateway, H323Phone, H323Trunk, HuntPilot, Line, MGCPEndPoint, PilotPoint, RemoteDestinationProfile, SIPTrunk, VoiceMailPilot, and VoiceMailPort.

Change to axl.xsd for the ringSetting Element

The definition of the ringSetting element changes in Release 5.1(3x) to make this element optional:

```
<xsd:element name="ringSetting" type="axl:XRingSetting" default="Ring" nillable="false"
minOccurs="0"/>
```

Prior to this release, ringSetting comprised a required element:

```
<xsd:element name="ringSetting" type="axl:XRingSetting" default="Ring" nillable="false"/>
```

Documentation Supplement

WSDL AXL and AXIS

By default, AXIS2 creates all the methods and requests in the same stub file, which might be as large as 35 Mb. AXIS1.4 creates individual files for every method, which yields individual files smaller than 2 Mb.

AXIS2 includes the option "-d xmlbeans" to change the binding option, which creates separate files for all methods as with AXIS1.4. For more information, see this URL:

`http://ws.apache.org/axis2/1_1_1/userguide-creatingclients.html.`

Changes in the Initial Version of Release 5.1

The following sections describe the API changes that were introduced in the initial version of Unified CM Release 5.1.

AXL APIs

The following list provides AXL API calls that are new in Unified CM Release 5.1:

- addSIPRealm
- updateSIPRealm
- getSIPRealm
- removeSIPRealm

These APIs add and update credentials (passwordreserve) in siprealm.

New AXL Service Parameter

Cisco Unified CallManager Administration 5.1 release adds a new service parameter, Send Valid Namespace in AXL Response, under the Cisco Database Layer Monitor service. This parameter determines the namespace that gets sent in the AXL response from Unified CM.

When this parameter specifies True, Unified CM sends the valid namespace (that is, http://www.cisco.com/AXL/API/1.0) in the AXL response, so the namespace matches the AXL schema specification.

If the parameter specifies False, Unified CM sends an invalid namespace (that is, http://www.cisco.com/AXL/1.0) in the AXL response, which does not match the AXL schema specification.

The default service parameter value specifies **False** to maintain backward compatibility with the AXL response in the Cisco Unified CM 5.0 release. Cisco recommends that you set this parameter to **True**, so Unified CM sends the valid namespace.

AXL Serviceability Programming

No changes to the AXL Serviceability APIs exist for Release 5.1(3x).

Summary of Changes in Previous Releases

For a summary of changes in previous releases, see the following table:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/devguide/6_0_1/Svc_API_table.html

Documentation Errata

This section corrects some errors in the *Cisco Unified CallManager Developers Guide* for Release 5.0.

An error exists in the example that shows the PerfmonAddCounter request with two counters and a single-reference accessor. The `SessionHandle` element contains an incorrect value for the `type` attribute. The corrected example follows.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:PerfmonAddCounter
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://schemas.cisco.com/ast/soap/">
      <SessionHandle
xsi:type="ns1:SessionHandleType">b60b683a-24fd-11dc-8000-000000000000</SessionHandle>
      <ArrayOfCounter soapenc:arrayType="ns1:CounterType[2]" xsi:type="soapenc:Array"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        <item xsi:type="ns1:CounterType">
          <Name xsi:type="ns1:CounterNameType">\\sampleserver\Process\Nice</Name>
        </item>
        <item xsi:type="ns1:CounterType">
          <Name xsi:type="ns1:CounterNameType">\\sampleserver\Process\PID</Name>
        </item>
      </ArrayOfCounter>
    </ns1:PerfmonAddCounter>
  </soapenv:Body>
</soapenv:Envelope>
```

An error also exists in the section **Real-Time Information (RisPort) > Selecting Cisco Unified CallManager Real-Time Information > Request Format > SOAP Action and Envelope Information**.
The SOAPAction should be

SOAPAction: http://schemas.cisco.com/ast/soap/action/#RisPort#SelectCmDevice

Extension Mobility API

No changes exist in the Extension Mobility API in Release 5.1(3x).

Web Dialer

The following change to Web Dialer occurred for Unified CM Release 5.1(3x):

- **getProfileSoap**: the list of devices that getProfileSoap returns changed. The list no longer includes unsupported devices.

Documentation Errata

The *Cisco Unified CallManager Release 5.1(1) New and Changed Information Guide* states that the Cisco Unified CallManager Administration directory search page uses the **makeCall** interface. However, beginning with Release 5.0, the directory search page actually uses the **makeCallProxy** interface.

Changes in Release 5.1

The initial 5.1 release of Cisco Unified CallManager included the following change to Cisco Unified CallManager Web Dialer:

- Web Dialer and Redirector now require HTTPS.

Developers should format Redirector and web dialer requests to use HTTPS. Unified CM requires the secured protocol to prevent unauthorized applications from reading user data.

For More Information

- AXL Programming, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Web Dialer API Programming, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Cisco Unified JTAPI Developers Guide

No changes to Cisco Unified JTAPI exists in Release 5.1(3x). As stated previously, beginning with this release, Cisco Unified JTAPI supports the Windows Vista platform.

The following sections supplement the *Cisco Unified CallManager JTAPI Developers Guide*.

Hunt List Targets

The Cisco JTAPI implementation does not support hunt lists. Applications cannot observe an Address, CiscoAddress, or CiscoRouteAddress that is a member of a HuntList LineGroup.

Translation Pattern Support

If a calling party transformation mask is configured for a translation pattern that is applied to a JTAPI application-controlled Address, the application may see extra connections that get created and disconnected when both the calling and called party are observed. A Connection gets created for a transformed calling party instead of the actual calling party, and CiscoCall.getCurrentCallingParty() would return the transformed calling party, when only the called party is observed. In general, JTAPI might not be able to create the appropriate Connection in the Call, and might not be able to provide correct information for currentCalling, currentCalled, calling, called, and lastRedirecting parties.

For example, consider a translation pattern X that is configured with a calling party transformation mask Y and called party transformation mask B. If A calls X, the call goes to B. This scenario follows:

- If the application is observing only B, JTAPI creates a Connection for Y and B, and CiscoCall.getCurrentCallingParty() would return Address Y.
- If the application is observing both A and B, a Connection for A and B gets created, a Connection for Y gets temporarily created and dropped, and CiscoCall.getCurrentCallingParty() would return Address Y.

Other inconsistencies could exist in the calling information if further features get performed on a basic call. Cisco recommends that you not configure a calling party transformation mast for a translation pattern that might get applied to JTAPI application-controlled addresses.

Supported JVM Versions

Table 2 lists the supported Java Virtual Machine versions for all the Cisco JTAPI platforms.

Table 2 Supported JVM Versions for Cisco JTAPI

Platform	Release(s)	Unified CM Release 4.x	Unified CM Releases 5.x and 6.0(1)
Linux	AS 3.0	IBM JVM 1.3.1 IBM JVM 1.4.2 Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.5.0.4 Sun JVM 1.4.2
	Red Hat 7.3	IBM JVM 1.3.1 IBM JVM 1.4.2 Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.5.0.4 Sun JVM 1.4
Solaris	6.2 on SPARC	Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.5.0.4 Sun JVM 1.4.2
Windows	9x	Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.4.2
	2000 NT 4.0+ XP (32-bit) 2003	Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.5.0.4 Sun JVM 1.4.2
	Vista (32bit)	Sun JVM 1.3.1 Sun JVM 1.4.2	Sun JVM 1.5.0.4 Sun JVM 1.4.2

Documentation Errata

Be aware of the following issues in the *Cisco Unified CallManager JTAPI Developers Guide*:

- The reasons fields that are listed for CiscoCallEv should instead appear under CiscoFeatureReason.
- The names of several constants, such as FRAMESIZE_TWENTY_MILLISECOND_PACKET for the CiscoG711MediaCapability interface mislead. These constants do not specify a frame rate (frames-per-packet) value. Instead, they specify the packet rate (frame size). The affected interfaces comprise CiscoG711MediaCapability, CiscoG723MediaCapability, and CiscoGSMMediaCapability. This clarification applies to all the FRAMESIZE_XXX_PACKET constants.

Cisco Unified TAPI Developers Guide

No changes occurred to Cisco Unified TAPI in Release 5.1(3x). As stated previously, beginning with this release, Cisco Unified TAPI supports the Windows Vista platform.

The following sections supplement the *Cisco Unified CallManager TAPI Developers Guide*.

Hunt List Targets

CTI does not support controlled devices as part of Hunt List members. This could result in erroneous behavior for Cisco Unified TAPI applications.

Translation Pattern

TSP does not support the Translation Pattern because it may cause a dangling call in a conference scenario. The application needs to clear the call to remove this dangling call or simply close and reopen the line.

Documentation Supplement: New and Changed Information Summary

The following tables summarize changes in Release 5.1 and earlier. This information applies to Release 5.1(3x) and all respins of Release 5.1. The tables indicate whether a feature was Added (A) or Modified (M) in the indicated release. Modifications and changes that are marked with an asterisk (M*) might impact backward compatibility of TAPI applications.

- TSP Features
- TAPI Line Functions
- TAPI Line Messages
- TAPI Line Structures
- TAPI Phone Functions
- TAPI Phone Messages
- TAPI Phone Structures

Table 3 TSP Features

	Cisco Unified CallManager Releases						
TSP Features	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
CTI Manager and Support for Fault Tolerance	A						
Support for Cisco CallManager Extension Mobility	A						
Support for Multiple CiscoTSP	A						
(Redirect Support for) Blind Transfer				M			
Support for Swap Hold and Setup Transfer with the lineDevSpecific() Function	A						
Support for lineForward()	A						
Support to Reset the Original Called Party upon Redirect with the lineDevSpecific Function	A						
Support to Set the Original Called Party upon Redirect with the lineDevSpecific Function				A			
Support for VG248 Devices	A						
Line In Service or Out of Service	M*						
Support for 7914 Device	A						

Table 3 TSP Features

	Cisco Unified CallManager Releases						
TSP Features	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
Support for Multiple Languages in the CiscoTSP Installation Program and in the CiscoTSP Configuration Dialogs		A					
Support for ATA186 Devices		A					
User Deletion from Directory			M*				
Opening Two Lines on One CTI Port Device			A				
Support for linePark and lineUnpark			A				
Support for Monitoring Call Park Directory Numbers by Using lineOpen			A				
Support for the 7835 Device			A				
Support for the 7905 Device			A				
Support for the 7902 Device			A				
Support for the 7912 Device			A				
Support for the 7970 Device			A				
Support for the 7965 Device			A				
Call Reason Enhancements			M*				
Device Data Passthrough			A				
CiscoTSP Auto Install				A			
Multiple Calls per Line Appearance				A			
Shared Line Appearance				A			
Select Calls				A			
Transfer Changes				M*			
Direct Transfer				A			
Conference Changes				M			
Join				A			
Privacy Release				A			
Barge and cBarge				A			
Dynamic Port Registration				A			
Media Termination at Route Points				A			
QoS Support				A			M
Support for Presentation Indication				A			
Unicode Support						A	
SRTP Support							A
Partition Support							A
SuperProvider Functionality							A
Security (TLS) Support							A

Table 3 TSP Features

	Cisco Unified CallManager Releases						
TSP Features	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
FAC/CMC Support					A		
CTI Port Third-Party Monitoring					A		
Alternate Script Support							A
SIP Features Refer/Replaces							A
SIP URI							A
Change Notification of SuperProvider and CallParkDN Monitoring Flags							A
3XX							A

Table 4 TAPI Line Functions

	Cisco Unified CallManager Releases						
TAPI Line Functions	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
lineAddToConference				M			
lineCompleteTransfer				M			
lineDevSpecific	M			M*	M		M
lineForward	A						
linePark			A				
lineUnpark			A				
lineRedirect					M		
lineBlindTransfer					M		

Table 5 TAPI Line Messages

	Cisco Unified CallManager Releases						
TAPI Line Messages	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
LINE_ADDRESSSTATE	M						
LINE_CALLINFO	M*					M	M
LINE_CALLSTATE				M	M		
LINE_REMOVE	A						
LINE_DEVSPECIFIC					M		M
LINE_CALLDEVSPECIFIC					M		

Table 6 TAPI Line Structures

	Cisco Unified CallManager Releases						
TAPI Line Structures	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
LINEADDRESSCAPS	M			M	M		
LINECALLSTATUS				M	M		
LINEFORWARD	A						
LINEFORWARDLIST	A						
LINEDEVCAPS			M			M	M
LINEDEVSTATUS						M	

Table 7 TAPI Phone Functions

	Cisco Unified CallManager						
TAPI Phone Functions	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**	**5.1**
phoneDevSpecific			A				
PhoneGetStatus			A				
PhoneReqRTPSnapshot							A

Table 8 TAPI Phone Messages

	Cisco Unified CallManager					
TAPI Phone Messages	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**
PHONE_REMOVE	A					

Table 9 TAPI Phone Structures

	Cisco Unified CallManagerCisco Unified CallManager					
TAPI Phone Structures	**3.1**	**3.2**	**3.3**	**4.0**	**4.1**	**5.0**
PHONECAPS						M
PHONESTATUS			A			M

SCCP Messaging Guide

No changes to SCCP messages occurred in Release 5.1(3x)

SIP Line Messaging Guide (Standard)

No changes to SIP line messages occurred in Release 5.1(3x).

Cisco Unified CallManager Data Dictionary

Cisco did not update this document for release 5.1(3x). For information about AXL schema changes in this release, see AXL Programming, page 23.

Cisco Unified Reporting

The Cisco Unified Reporting Administration Guide, a new document, describes how to use the new Cisco Unified Reporting web application. Refer to New Cisco Unified Reporting Application in the "Important Notes" section on page 4 for a brief description of the application.

Cisco Unified IP Phones

Unified CM 5.1(3x) adds support the following phones:

- Cisco Unified Wireless IP Phone 7921, page 33
- Cisco Unified IP Phone 7962G and 7942G (SCCP and SIP), page 34
- Cisco Unified IP Phone 7965G and 7945G (SCCP and SIP), page 34
- Cisco Unified IP Phone 7975G (SCCP and SIP), page 34

Note For additional information on Cisco Unified IP Phones 7900 Series, go to http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Cisco Unified Wireless IP Phone 7921

The Cisco Unified Wireless IP Phone 7921 as a second-generation wireless IP phone extends advanced voice and unified communications capabilities across the enterprise, supporting a host of enhanced calling features, including the following ones:

- IEEE 802.11a, b, and g standards that allow using the phone in the 2.4 GHz or 5 GHz bands
- A large (2-inch) color display
- Dedicated mute and volume keys and a separate Application button that supports Push-to-Talk using Extensible Markup Language (XML)
- Battery with 100 hours standby time or 12 hours talk time
- Wireless security features and voice security features

Where to Find More Information

- *Cisco Unified Wireless IP Phone 7921G Installation Guide*
- *Cisco Unified Wireless IP Phone Guide 7921G for Cisco Unified CallManager 4.1, 4.2, and 5.0 (SCCP)*
- *Cisco Unified Wireless IP Phone 7921G Administration Guide for Cisco Unified CallManager 4.1, 4.2, and 5.0 (SCCP)*
- *Cisco Unified Wireless IP Phone 7921G Accessory Guide*
- *Cisco Unified Wireless IP Phone 7921G Deployment Guide*

Cisco Unified IP Phone 7962G and 7942G (SCCP and SIP)

The system supports Cisco Unified IP Phones 7962G and 7942G for Unified CM Release 5.1(3x) and later. The Cisco Unified IP Phones 7962G and 7942G design meets the needs of businesses with moderate telephone traffic and specific call requirements. The Cisco Unified IP Phones 7962G and 7942G support IEEE 802.3af Power over Ethernet, security, and other calling features. Dedicated hold, redial, and transfer keys facilitate call handling. Illuminated mute and speakerphone keys give a clear indication of speaker status.

Where to Find More Information

- *Cisco Unified IP Phone 7962G Installation Guide*
- *Cisco Unified IP Phone 7942G Installation Guide*
- *Cisco Unified IP Phone 7962G and 7942G Phone Guide*
- *Cisco Unified IP Phone 7962G and 7942G Administration Guide*

Cisco Unified IP Phone 7965G and 7945G (SCCP and SIP)

The system supports Cisco Unified IP Phones 7965G and 7945G on Unified CM Release 5.1(3x) and later. The Cisco Unified IP Phones 7965G and 7945G design meets the needs of businesses with moderate telephone traffic and specific call requirements. The Cisco Unified IP Phones 7965G and 7945G support IEEE 802.3af Power over Ethernet, security, and other calling features. Dedicated hold, redial, and transfer keys facilitate call handling. Illuminated mute and speakerphone keys give a clear indication of speaker status.

Where to Find More Information

- *Cisco Unified IP Phone 7965G Installation Guide*
- *Cisco Unified IP Phone 7945G Installation Guide*
- *Cisco Unified IP Phone 7965G and 7945G Phone Guide*
- *Cisco Unified IP Phone 7965G and 7945G Administration Guide*

Cisco Unified IP Phone 7975G (SCCP and SIP)

The system supports Cisco Unified IP Phone 7975G on Unified CM Release 5.1(3) and later. The Cisco Unified IP Phone 7975G design meets the needs of businesses with moderate telephone traffic and specific call requirements. The Cisco Unified IP Phones 7975G supports IEEE 802.3af Power over Ethernet, security, and other calling features. Dedicated hold, redial, and transfer keys facilitate call handling. Illuminated mute and speakerphone keys give a clear indication of speaker status.

Where to Find More Information

- *Cisco Unified IP Phone 7975G Installation Guide*
- *Cisco Unified IP Phone 7975G Phone Guide*
- *Cisco Unified IP Phone 7975G Administration Guide*

Operating System CLI Commands

This section describes Cisco Unified Communications Operating System CLI commands that are added or updated in Unified CM Release 5.1(3x).

file fragmentation sdi

This command displays file fragmentation information about SDI log files.

Command Syntax

file fragmentation sdi

all *outfilename*

file *filename* {**verbose**}

most fragmented *number*

most recent *number*

Parameters

- **all** records information about all files in the directory in the file that is specified by *outfilename*.
- **file** displays information about the file that is specified by *filename*.
- **most fragmented** displays information about the most fragmented files.
- **most recent** displays information about the most recently logged fragmented file.
- *number* specifies the number of files to list.

Options

- **verbose**—Displays more detailed information

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file fragmentation sdl

This command displays file fragmentation information about SDL log files.

Command Syntax

file fragmentation sdl

all *outfilename*

file *filename* {**verbose**}

most fragmented *number*

most recent *number*

Parameters

- **all** records information about all files in the directory in the file that is specified by *outfilename*.
- **file** displays information about the file that is specified by *filename*.

- **most fragmented** displays information about the most fragmented files.
- **most recent** displays information about the most recently logged fragmented file.
- *number* specifies the number of files to list.

Options

- **verbose**—Displays more detailed information

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

file get

The **file get** command has the new parameters **salog** and **partBsalog**. The **file get** command sends the file to another system by using SFTP.

Command Syntax

file get

salog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

partBsalog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

Parameters

- **salog** specifies the salog log directory.
- **partBsalog** specifies the partBsalog log directory.
- *directory/filename* specifies the path to the file(s) to get. You can use the wildcard character, *, for *filename* as long as it resolves to one file.

Options

- **abstime**—Absolute time period, specified as *hh:mm:MM/DD/YY hh:mm:MM/DD/YY*
- **reltime**—Relative time period, specified as **minutes | hours | days | weeks | months** *value*
- **match**—Match a particular string in the filename, specified as *string value*
- **recurs**—Get all files, including subdirectories

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

file list

The **file list** command has the new parameters **salog** and **partBsalog**. The **file list** command lists the log files in an available log directory.

Command Syntax

file list

salog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

partBsalog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

Parameters

- **salog** specifies the salog log directory.
- **partBsalog** specifies the partBsalog log directory.
- *directory* specifies the path to the directory to list. You can use a wildcard character, *, for *directory* as long as it resolves to one directory.

Options

- **detail**—Long listing with date and time
- **date**—Sort by date
- **size**—Sort by file size
- **reverse**—Reverse sort direction
- **page**—Displays the output one screen at a time

Requirements

Command privilege level: 1 for logs, 0 for TFTP files

Allowed during upgrade: Yes

file view

The **file view** command has a new **system-management-log** parameter. The **file view** command displays the contents of a file.

Command Syntax

file view

system-management-log

Parameters

- **system-management-log** displays the contents of the Integrated Management Logs (IML).

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

set network dhcp

The set network dhcp command gets updated as described in this section. This command configures DHCP on Ethernet interface 0. You cannot configure Ethernet interface 1.

Command Syntax

set network dhcp eth0

enable

disable *node_ip net_mask gateway_ip*

Parameters

- **eth0** specifies Ethernet interface 0.
- **enable** enables DHCP.
- **disable** disables DHCP.
- *node_ip* specifies the new static IP address for the server.
- *net_mask* specifies the subnet mask for the server.
- *gateway_ip* specifies the IP address of the default gateway.

Usage Guidelines

The system asks whether you want to continue to execute this command.

Caution If you continue, this command causes the system to restart. Cisco also recommends that you restart all nodes whenever any IP address gets changed.

Requirements

Command privilege level: 1

Allowed during upgrade: No

set network restore

This command configures the specified Ethernet port to use a specified static IP address.

Caution Use this command option only if you cannot restore network connectivity by using any other **set network** commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After running this command, you must restore your previous network configuration manually.

Caution The server temporarily loses network connectivity when you run this command.

Command Syntax

set network restore eth0 *ip-address network-mask gateway*

Parameters

- **eth0** specifies Ethernet interface 0.
- *ip-address* specifies the IP address.
- *network-mask* specifies the subnet mask.
- *gateway* specifies the IP address of the default gateway.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show ctl

This command displays the contents of the Certificate Trust List (CTL) file on the server. It notifies you if the CTL is not valid.

Command Syntax

show ctl

show diskusage

This command displays information about disk usage on the server.

Command Syntax

show diskusage

activelog {**filename** *filename* | **directory** | **sort**}

common {**filename** *filename* | **directory** | **sort**}

inactivelog {**filename** *filename* | **directory** | **sort**}

install {**filename** *filename* | **directory** | **sort**}

tftp {**filename** *filename* | **directory** | **sort**}

tmp {**filename** *filename* | **directory** | **sort**}

Parameters

- **activelog** displays disk usage information about the activelog directory.
- **common** displays disk usage information about the common directory.
- **inactivelog** displays disk usage information about the inactivelog directory.
- **install** displays disk usage information about the install directory.
- **tftp** displays disk usage information about the tftp directory.
- **tmp** displays disk usage information about the tmp directory.

Options

- **filename** *filename*—Saves the output to a file that is specified by *filename*. The **platform/cli** directory stores these files. To view saved files, use the **file view activelog** command.
- **directory**—Displays just the directory sizes.
- **sort**—Sorts the output based on file size. File sizes display in 1024-byte blocks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show environment

This command displays information about the server hardware.

Command Syntax

show environment

fans

power-supply

temperatures

Parameters

- **fans** displays information that fan probes gather.
- **power-supply** displays information that power supply probes gather.
- **temperatures** displays information that temperature probes gather.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show iptables

Although the **show iptables** command was removed, the **utils firewall list** command now displays similar information.

show memory

This command displays information about the server memory.

Command Syntax

show memory

count

module [**ALL** | *module_number*]

size

Parameters

- **count** displays the number of memory modules on the system.
- **module** displays detailed information about each memory module.
- **size** displays the total amount of memory.

Options

- **ALL**—Displays information about all installed memory modules.
- *module_number*—Specifies which memory module to display. Memory module numbers start at 0.

show network cluster

This command has a new **cluster** parameter.

Command Syntax

show network

cluster

Parameters

- **cluster** displays a list of the nodes in the network cluster.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show tech database

This command has the new parameters **dump** and **session**.

Command Syntax

show tech database

dump

sessions

Parameters

- **dump** creates a CSV file of the entire database.
- **sessions** redirects the session and SQL information of the present session IDs to a file.

show tech network

This section describes the show tech network command updates. This command displays information about the network aspects of the server.

Command Syntax

show tech network

all [**page**] [**search** *text*] [**file** *filename*]

hosts [**page**] [**search** *text*] [**file** *filename*]

interfaces [**page**] [**search** *text*] [**file** *filename*]

resolv [**page**] [**search** *text*] [**file** *filename*]

routes [**page**] [**search** *text*] [**file** *filename*]

sockets {**numeric**}

Parameters

- **all** displays all network tech information.
- **hosts** displays information about hosts configuration.

- **interfaces** displays information about the network interfaces.
- **resolv** displays information about hostname resolution.
- **routes** displays information about network routes.
- **sockets** displays the list of open sockets.

Options

- **page**—Displays one page at a time
- **search** *text*—Searches the output for the string that is specified by *text*. Be aware that the search is case insensitive.
- **file** *filename*—Outputs the information to a file.
- **numeric**—Displays the numerical addresses of the ports instead of determining symbolic hosts. It equates to running the Linux shell command netstat [-n] command.

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech runtime

This section describes the show tech runtime command updates. This command displays runtime aspects of the server.

Command Syntax

show tech runtime

all [**page**] [**file** *filename*]

cpu [**page**] [**file** *filename*]

disk [**page**] [**file** *filename*]

env [**page**] [**file** *filename*]

memory [**page**] [**file** *filename*]

Parameters

- **all** displays all runtime information.
- **cpu** displays CPU usage information at the time that the command is run.
- **disk** displays system disk usage information.
- **env** displays environment variables.
- **memory** displays memory usage information.

Options

- **page**—Displays one page at a time
- **file** *filename*—Outputs the information to a file

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

show tech system

This section describes the show tech system command updates. This command displays system aspects of the server.

Command Syntax

show tech system

all [**page**] [**file** *filename*]

bus [**page**] [**file** *filename*]

hardware [**page**] [**file** *filename*]

host [**page**] [**file** *filename*]

kerenl [**page**] [**file** *filename*]

software [**page**] [**file** *filename*]

tools [**page**] [**file** *filename*]

Parameters

- **all** displays all the system information.
- **bus** displays information about the data buses on the server.
- **hardware** displays information about the server hardware.
- **host** displays information about the server.
- **kerenl modules** lists the installed kernel modules.
- **software** displays information about the installed software versions.
- **tools** displays information about the software tools on the server.

Options

- **page**—Displays one page at a time
- **file** *filename*—Outputs the information to a file

Usage Guidelines

The **file** option saves the information to platform/cli/*filename*.txt. The file name cannot contain the "." character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils create report

This command creates reports about the server in the platform/log directory.

Command Syntax

utils create report

hardware

platform

Parameters

- **hardware** creates a system report that contains disk array, remote console, diagnostic, and environmental data.
- **platform** collects the platform configuration files into a TAR file.

Usage Guidelines

You are prompted to continue after you enter the command.

After creating a report, use the command **file get activelog platform/log/***filename*, where *filename* specifies the report filename that displays after the command completes, to get the report.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils dbreplication clusterreset

This command resets database replication on an entire cluster.

Command Syntax

utils dbreplication clusterreset

Usage Guidelines

Before you run this command, run the command **utils dbreplication stop** first on all subscribers servers, and then on the publisher server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils fior

This command allows you to monitor the I/O on the server. The File I/O Reporting service provides a kernel-based daemon for collecting file I/O per process.

Command Syntax

utils fior

disable

enable

list [**start=***date-time*] [**stop=***date-time*]

start

status

stop

top *number* [**read | write | read-rate | write-rate**] [**start=***date-time*] [**stop=***date-time*]

Options

- **disable**—Prevents the file I/O reporting service from starting automatically when the machine boots. This command does not stop the service without a reboot. Use the **stop** option to stop the service immediately.
- **enable**—Enables the file I/O reporting service to start automatically when the machine boots. This command does not start the service without a reboot. Use the **start** option to start the service immediately.
- **list**—Displays a list of file I/O events, in chronological order, from oldest to newest
- **start**—Starts a previously stopped file I/O reporting service. The service remains in a started state until it is manually stopped or the machine is rebooted.
- **status**—Displays the status of the file I/O reporting service
- **stop**—Stops the file I/O reporting service. The service remains in a stopped state until it is manually started or the machine is rebooted.
- **top**—Displays a list of top processes that create file I/O. You can sort this list by the total number of bytes read, the total number of bytes written, the rate of bytes read, or the rate of bytes written
- **start=**—Specifies a starting date and time
- **stop=**—Specifies a stopping date and time
- *date-time*—Specifies a date and time, in any of the following formats: *H*:*M*, *H*:*M*:*S a*, *H*:*M*, *a*, *H*:*M*:*S Y*-*m*-*d*, *H*:*M*, *Y*-*m*-*d*, *H*:*M*:*S*
- *number*—Specifies how many of the top processes to list
- **[read | write | read-rate | write-rate]**—Specifies the metric that is used to sort the list of top process

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

utils firewall

This command manages the firewall on the node.

Command Syntax

utils firewall

disable {*time*}

enable

list

status

Parameters

- **disable** disables the firewall.
- *time* specifies the duration for which the firewall is disabled, in one of these formats:
  - [0-1440]**m** to specify a duration in minutes.
  - [0-24]**h** to specify a duration in hours.
  - [0-23]**h**[0-60]**m** to specify a duration in hours and minutes.

  If you do not specify a time, the default equals 5 minutes.
- **enable** enables the firewall.
- **list** displays the current firewall configuration.
- **status** displays the status of the firewall.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils network connectivity

This command verifies the node network connection to the first node in the cluster. Be aware that it is only valid on a subsequent node.

Command Syntax

utils network connectivity

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils service

The utils service command has a new **auto-restart** parameter. You can enable auto-restart on a service to cause it to automatically restart.

Command Syntax

utils service

auto-restart {**enable** | **disable** | **show**} *service-name*

Parameters

- **auto-restart** causes a service to automatically restart.

Options

- **enable**- Enables auto-restart
- **disable -** Disables auto-restart
- **show -** Shows the auto-restart status
- *service-name* - Represents the name of the service that you want to stop or start

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils snmp

The **utils snmp** command has the new parameters **get**, **hardware-agents**, and **walk**.

Command Syntax

utils snmp

get *version community ip-address object* [*file*]

hardware-agents [**status** | **restart**]

walk *version community ip-address object* [*file*]

Parameters

- **get** displays the value of the specified SNMP object.
- **hardware-agents status** displays the status of the hardware agents on the server.
- **hardware-agents restart** restarts the hardware agents on the server.
- **walk** walks the SNMP MIB, starting with the specified SNMP object.
- *version* specifies the SNMP version. Possible values include 1 or 2c.
- *community* specifies the SNMP community string.
- *ip-address* specifies the IP address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IP address of another node in the cluster to run the command on that node.
- *object* specifies the SNMP Object ID (OID) to get.
- *file* specifies a file in which to save the command output.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Cisco Unified CallManager Serviceability

This section contains the following subsections:

- Supported Operating Systems, page 50

Adding RTMT Performance Counters in Bulk

On the RTMT Perfmon Monitoring pane, in table format only (not in chart format), you can now select multiple counters and multiple instances of counters and add them all with a single click. Prior to this enhancement, you could add them only one at a time.

For more information, see Documentation Updates, page 52.

RTMT Database Summary with Database Replication Information

The RTMT database summary predefined monitoring object now includes the following information:

- Replicates created
- Replication status

Start Counter(s) Logging in the Menu Bar

Prior to this release, the RTMT Performance Monitoring window included a Start Counter(s) Logging menu item for each tab, but not at the RTMT top menu bar level. Now, this menu item consistently remains available.

RTMT Trace and Log Central Disk IO and CPU Throttling

RTMT now supports the throttling of critical Trace and Log Central operations and jobs, whether they are running on demand, scheduled, or automatic. The throttling effect slows down the operations when IO utilization is in high demand for call processing, so call processing can take precedence.

For more information, see Documentation Updates, page 52.

Trace Compression Support

This feature enables the ROS (Recoverable Outstream) library to support the compressed output of tracefiles. The files get compressed as they are being generated. The following benefits of tracefile compression apply:

- Reduces the capacity that is required to store tracefiles
- Reduces the disk head movement, which results in significantly improved call load. The CPU virtually never gets blocked due to tracefile demands.

For more information, see Documentation Updates, page 52.

RTMT Critical Services

Cisco Unified CallManager Real-Time Monitoring Tool (RTMT) provides new states for the critical services that display in RTMT. The Critical Services monitoring category (choose **Monitor > Server > Critical Services** or click the **Server** button and **Critical Services** icon) provides the name of the critical service, the status (whether the service is starting, up, stopping, down, stopped by the administrator, not activated, or in an unknown state), and the elapsed time during which the services have existed in a particular state for a particular Unified CM node. For a specific description of each state, review the following information:

- starting (new state)—The service currently experiences starting, as indicated in the Critical Services pane and in Control Center in Cisco Unified CallManager Serviceability.
- up—The service currently runs as indicated in the Critical Services pane and in Control Center in Cisco Unified CallManager Serviceability.
- stopping (new state)—The service currently remains in stop state, as indicated in the Critical Services pane and in Control Center in Cisco Unified CallManager Serviceability.
- down—The service stopped running unexpectedly; that is, you did not perform a task that stopped the service. The Critical Services pane indicates that the service is down.

Tip The CriticalServiceDown alert gets generated when the service status equals down (not for other states).

- stopped by Admin (new state)—You performed a task that intentionally stopped the service; for example, the service stopped because you backed up or restored Cisco Unified CallManager, performed an upgrade, stopped the service in Cisco Unified CallManager Serviceability or the Command Line Interface (CLI), and so on. The Critical Services pane indicates the status.
- not activated—The service does not currently exist in activated state as indicated in the Critical Services pane and in Service Activation in Cisco Unified CallManager Serviceability.
- unknown state—The system cannot determine the state of the service, as indicated in the Critical Services pane.

Preconfigured Alerts

The Preconfigured Alerts chapter of the *Cisco Unified CallManager Serviceability Guide* contains the following new preconfigured alerts:

- ServerDown: This alert gets triggered whenever the active AMC cannot talk to a remote host.
- HardwareFailure: This alert gets triggered whenever a corresponding HardwareFailure alarm/event occurs.
- SDLLinkOutOfService: This alert gets triggered whenever a corresponding "SDLLinkOOS alarm/event occurs.
- SyslogStringMatchFound
- SyslogSeverityMatchFound
- DBReplicationFailure: This alert gets triggered whenever the corresponding perfmon counter "replication status" has values other than 0 (init) and 2 (success).
- SystemVersionMismatched: This alert gets triggered whenever a mismatch exists in system version.

RTMT Services, Servlets and Service Parameters

The list of RTMT Services, Servlets, and Service Parameters now includes RisDC.

Supported Operating Systems

The list of supported operating systems now includes Windows Vista.

For More Information

- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*

Caveats

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

Caveats describe unexpected behavior on a Cisco Unified CallManager 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 CallManager Release 5.1(3x) 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://tools.cisco.com/Support/BugToolKit.

UsingBug Toolkit

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

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

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 Acccess the Bug Toolkit, http://tools.cisco.com/Support/BugToolKit.

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

Step 3 If you are looking for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field, and click **Go**.

Tip Click **Help** on the Bug Toolkit page for information about how to search for bugs, create saved searches, create bug groups, and so on.

Open Caveats

For more information about an individual defect, click the associated Identifier in the "Open Caveats as of September 10, 2009" section on page 52 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 CallManager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified CallManager 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; however, the version information that displays for the Cisco Unified CallManager maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco Unified CallManager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 003.003(003.144) = Cisco CallManager Release 3.3(4)
- 005.000(000.123) = Cisco Unified CallManager Release 5.0(1)
- 005.000(001.008) = Cisco Unified CallManager Release 5.0(2)
- 005.001(002.201) = Cisco Unified CallManager Release 5.1(3)

Note Because defect status continually changes, be aware that the "Open Caveats as of September 10, 2009" section on page 52 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 "UsingBug Toolkit" section on page 50.

Tip 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.

Open Caveats as of September 10, 2009

The following list contains information about unexpected behaviors that might occur in Unified CM 5.1(3x):

Table 10 Open Caveats for CM Release 5.1(3)

Identifier	Headline
CSCsg23990	TSP svchost pegs 99% CPU during TLS connection.
CSCta29539	Default net-snmp logrotate configuration causes weekly agent restart .
CSCtb42207	Intermitent H323 calls drop when MTP gets invoked.

Documentation Updates

Updates to Cisco Unified Communications Manager 5.1(3) Documentation provides information about omissions, errors, or updates for the documentation that supports Cisco Unified Communications Manager 5.1(3x).To obtain this document, go to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/5_1_3/cucm-doc_updates-513.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
