Release Notes for Cisco Unified CallManager Release 5.1(3)

October 1, 2007

These release notes describe the enhanced capabilities of Cisco Unified CallManager Release 5.1(3) as well as DDTS fixes that ensure software quality.

Note To view the release notes for previous versions of Cisco Unified CallManager, choose the Cisco Unified CallManager version from the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Before you install Cisco Unified CallManager, 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 Cisco Unified CallManager system, you must upgrade to Cisco Unified CallManager 5.1(3). If you ordered and received a server that is preloaded with Cisco Unified CallManager 5.0(4), you can download Cisco Unified CallManager software, version 5.1(3), at Cisco.com.

Cisco recommends that you check Cisco.com for the latest software updates to Cisco Unified CallManager and its applications and download and install the latest updates on your system before the deployment of your Cisco Unified CallManager 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 CallManager, a network business communication system, provides high-quality telephony over IP networks. Cisco Unified CallManager enables the conversion of conventional, proprietary, circuit-switched PBXs to multiservice, open LAN systems.

System Requirements

Make sure that you install and configure Cisco Unified CallManager Release 5.1(3) on a Cisco Media Convergence Server (MCS). To see which MCS servers are compatible with this release, see: http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html.

Note Not all models listed are compatible with this release. Check each model for details.

You may also install Cisco Unified CallManager on a Cisco-approved HP server or a Cisco-approved IBM server . For Cisco-approved HP or IBM configurations, see: http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

Note Not all models listed are compatible this release. Check each model for details.

Tip Cisco recommends that you connect each Cisco Unified CallManager node to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

Supported Platforms

To find which servers support the Cisco Unified CallManager 5.1(3) release, refer to http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

Determining the Software Version

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

- Cisco Unified CallManager System version
- Cisco Unified CallManager Administration version

Upgrading System Software

You can access the latest software upgrades for Cisco Unified CallManager 5.1 on Cisco.com. Table 1 lists the URLs from which you download the software.

Table 1 Download URLs for Software Upgrades

Software	Download URL
Cisco Unified CallManager 5.1	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51
Locale installers	http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtm
Phone firmware	http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto
Cisco Security Agent (CSA)	http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des
Upgrade Assistant	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-utilpage

Related Documentation

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

- *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(2b)*
- *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 CallManager 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 CallManager 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 CallManager releases. If a product does not meet the compatibility testing requirements with Cisco Unified CallManager, you need to wait until a compatible version of the product becomes available before you can upgrade to Cisco Unified CallManager Release 5.1(3). For the most current compatibility combinations and defects that are associated with other Cisco Unified CallManager products, refer to the documentation that is associated with those products.

Important Notes

The following section contains important information that may have been unavailable upon the initial release of documentation for Cisco Unified CallManager Release 5.1(3).

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 CallManager 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 CallManager 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 CallManager certificate to the root certificate trust store in Internet Explorer 7.

JRE must be present to provideall the Java releated browser support for IE6 or IE7.

Procedure

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

Step 2 To access the server, click **Continue to this website (not recommended)**. The Cisco Unified CallManager Administration home page 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 URL 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 CallManager 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 addresses/hostnames for Cisco Unified CallManager, refer to http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094601.shtml.

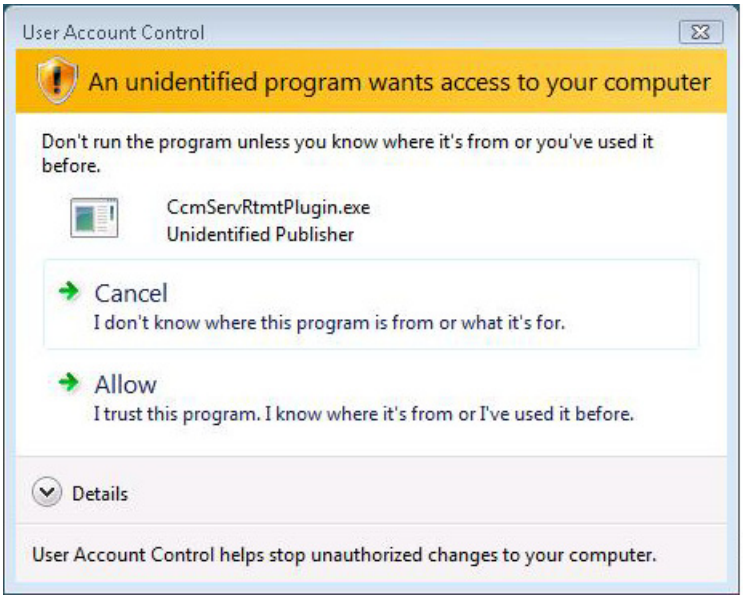
SIP Network/IP Address Field Required for SIP Fallback to SRST Gateway

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 shown in Figure 1 due to a limitation in the InstallAnywhere software. This is a one time popup that displays only when installing RTMT. Select **Allow** to continue.

Figure 1 User Account Control Popup Window



Resolved Caveat 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 are logged in to the local and remote SYSLOG.

Note There are no corresponding alerts for these two authentication alarms.

Resolved Caveat CSCsh58895 Cisco Unified CallManager Cannot Send System or Platform Agent Logs to Remote Syslog Server

Cisco Unified CallManager 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 Cisco Unified CallManager 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 of (A-Z,a-z,0-9,.,-)

- Syslog Severity For Remote Syslog messages - You can select the desired Syslog messages severity for remote syslog server. All the syslog messages with selected or higher severity levels are sent to the remote syslog. If the remote server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

RTMT Requirement When Upgrading Cisco Unified CallManager

If you are running the Cisco Unified Communications Real-Time Monitoring Tool (RTMT) client and monitoring performance counters during a Cisco Unified Communications Manager 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 are displayed 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, press **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. Once you log in again, you may have to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. The only workaround is to log out 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 Cisco Unified CallManager Release 5.1(3)

The following sections contain information that is new or changed for this release of Cisco Unified CallManager.

Installation, Upgrade, and Disaster Recovery

Installation Overview

For 5.1(3), the Cisco Unified Communications Manager installation process includes the following new features:

- Allows you to set the maximum transmission unit (MTU) size
- Enhanced validationto ensure 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(3), enhancements to the installation and upgrade documentation to 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(3) 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

- 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 include a SIP timeout, like a firewall, those timeouts need to be adjusted 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 attempting to connect to another server. Increase this time if you experience connection issues on a slow network. This is a required field, the range is 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 reading data from another server. Increase this time if you experience connection issues on a slow network. This is a required field, the range is 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 Cisco Unified CallManager 5.1(3), 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(3).

A previous 5.x version of the assistant console application works with Cisco Unified CallManager 5.1(3), but if you decide to install the 5.1(3) 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(3), 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 Cisco Unified CallManager 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

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

Windows Vista Support

Cisco Unified CallManager Release 5.1(3) 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 3 on page 19.

Route Patterns, Automated Alternative Routing, and Applications

Cisco Unified CallManager only applies Automated Alternative Routing (AAR) to the endpoints that it controls.hNetwork congestion and bandwidth restrictions can cause tail-end hop-off (TEHO) calls to fail if you configure Cisco Unified CallManager 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 Cisco Unified CallManager TAPI and JTAPI APIs should be aware of this behavior.

AXL Programming

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

Table 2 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(3) 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 Cisco Unified CallManager Release 5.1.

AXL APIs

The following list provides AXL API calls that are new in Cisco Unified CallManager 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 Cisco Unified CallManager.

When this parameter specifies True, Cisco Unified CallManager 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, Cisco Unified CallManager 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 Communications Manager 5.0 release. Cisco recommends that you set this parameter to **True**, so Cisco Unified CallManager sends the valid namespace.

AXL Serviceability Programming

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

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(3).

Web Dialer

The following change to Web Dialer occurred for Cisco Unified CallManager Release 5.1(3):

- **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. Cisco Unified CallManager 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(3). 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 3 lists the supported Java Virtual Machine versions for all the Cisco JTAPI platforms.

Table 3 Supported JVM Versions for Cisco JTAPI

Platform	Release(s)	Cisco Unified CallManager Release 4.x	Cisco Unified CallManager 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 be listed 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(3). 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(3) and all other sub-versions 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 4 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 4 TSP Features (continued)

	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 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 4 TSP Features (continued)

	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 5 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 6 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 7 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 8 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 9 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 10 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 occurred messages in Release 5.1(3)

SIP Line Messaging Guide (Standard)

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

Cisco Unified Communications Manager Data Dictionary

Cisco did not update this document for release 5.1(3). For information about AXL schema changes in this release, see AXL Programming, page 15.

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

Cisco Unified CallManager 5.1(3) adds support the following phones:

- Cisco Unified Wireless IP Phone 7921, page 24
- Cisco Unified IP Phone 7962G and 7942G (SCCP and SIP), page 25
- Cisco Unified IP Phone 7965G and 7945G (SCCP and SIP), page 25
- Cisco Unified IP Phone 7975G (SCCP and SIP), page 25

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 Cisco Unified CallManager Release 5.1(3) 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 Cisco Unified CalManager Release 5.1(3) 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 Cisco Unified CallManager 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 this release.

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 specified by *outfilename*.
- **file** displays information about the file 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 specified by *outfilename*.
- **file** displays information about the file 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 is 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* is the new static IP address for the server.
- *net_mask* is the subnet mask for the server.
- *gateway_ip* is 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 Only use this command option if you cannot restore network connectivity 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 specified by *filename*. These files are stored in the **platform/cli** directory. 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 are displayed 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 gathered by fan probes
- **power-supply** displays information gathered by power supply probes
- **temperatures** displays information gathered by temperature probes

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show iptables

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

The show tech network command is updated as described in this section. 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 specified by *text*. 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 is equivalent 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

The show tech runtime command is updated as described in this section. 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 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

The show tech system command is updated as described in this section. 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 of 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 containing 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* is the report filename that is displayed after the command completes, to get the report.

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**—This command 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. This list can be sorted 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 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 is 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's network connection to the first node in the cluster. 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 cause it 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 are 1 or 2c.
- *community* is the SNMP community string.

- *ip-address* is 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* is 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 sub-sections:

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 47.

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 that call processing can take precedence.

For more information, see Documentation Updates, page 47.

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 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 47.

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 Cisco Unified CallManager 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 alerts.

- ServerDown: This alert gets triggered whenever the active AMC is unable to 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(2a) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

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

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

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/action.do?hdnAction=searchBugs.

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

Table 11 describes possible unexpected behaviors in Cisco Unified CallManager Release 5.1(2a), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 11 to access the online record for that defect, including workarounds.

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

When you open the online record for a defect, you may see data in the "First Fixed-in Version" or "Integrated-in" fields. The information that displays in these fields identifies the list of Cisco Unified 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 Table 11 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "UsingBug Toolkit" section on page 42.

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.

Table 11 Open Caveats as of 9-29-2007

Identifier	Headline
Component: Alert Coll Report	
CSCsk23265	The need exists for an RTMT precanned alert for the NumDevRegExceeded alarm.
CSCsk62515	RTMT hardware failure alert does not gets raised if hard drive fails during startup.
Component: Attendant Console	
CSCsj76444	General SQL failure and Java exception error messages get printed to the upgrade log file.
CSCsk53501	Attendant Console InterServer Race conditions exists when agents get split on publisher server and subscriber server..
Component: AXL	
CSCsk14345	Attempt to remove a Line, CallPickup, CSS, RouteParition, Time Schedule failed.
CSCsk28959	During large scale AXL based phone insertions, the change notify database fills up.
CSCsk41840	getPhone does not always respond with the defaultProfileName after the phone is updated.

Table 11 Open Caveats as of 9-29-2007 (continued)

Component: Backup and Restore (BAR)	
CSCsj31456	RTMT receives a CallProcessingNodeCpuPegging alert during a Disaster Recovery Framework (DRF) backup.
Component: BPS-BAT	
CSCsj03551	Unable to upload user device profiles to BAT tool.
CSCsk06712	BAT VG224 import does not allow domain name over 43 characters.
Component: CAR	
CSCsk34945	Upgrade fails at CAR database migration.
CSCsk17300	User cannot view CDR records by using CAR.
Component: CDP	
CSCsk38849	CDP crashes in malloc call.
CSCsk30772	CDPAgent coredump found on all nodes in a cluster.
Component: CLI	
CSCsk47342	Rebuild status and percentage do not display in **show hardware**.
Component: CTI	
CSCsk29425	Clustering over WAN delay severely slows CTI Change Notification.
CSCsk13169	Extra CPIC occurs when you use CBARGE.
CSCsk13172	Incorrect remote-in-use value for shared line occurs when conference or transfer gets initiated by cbarge or barge.
CSCsi06589	The need exists for verification that nConsultCalls is in range in CCtiApiLineCallJoinRequest.
CSCsk48801	CTIManager does not update partition information when part name is changed.
Component: Call Processing	
CSCsj77506	CAC: Location-based CAC bandwidth does not get released at times.
CSCsk54103	H323: Handle leak with H.323 calls.
CSCsk07661	Huntlist: Hunt group logout impacts HL circular distribution.
CSCsk52316	Huntlist: Basic SCCP calls over SIP trunks do not display Alerting Name.
CSCsg29976	Media Control: Video RSVP call to Cisco Unified Presence Communicator endpoint takes three RSVP resources.
CSCsk18634	Media Control: In a video conference involving two video endpoints and a polycom, the two video endpoints cannot see video from the polycom.
CSCsk40448	QSIG: Callback over QSIG fails if call forward is enabled.
CSCsk53305	QSIG: After maximum hop count is reached the caller gets reorder tone.
CSCsk60495	QSIG: QSIG path replacement attempt causes bandwidth / Cdcc and media leak.
CSCeg64769	QSIG: Cisco Unified CallManager sends erroneous DiveringLegFailed ADPU.
CSCsh97800	SCCP: Call transfer will not complete if the user answers an incoming call before transfer completes.
CSCsj20429	SCCP: Inconsistent port availability exists on SCCP partition.
CSCsh64270	SCCP: Missed calls do not display for conference calls.

Table 11 Open Caveats as of 9-29-2007 (continued)

CSCsj78900	SCCP: Cisco Unified CallManager cannot disconnect a preserved call.
CSCsj13962	SCCP: If a Cisco Unified IP Phone Model 7914 user is on an active call and a call comes in on another line on the 7914, the phone does not ring, it flashes.
CSCsi99786	SCCP: Phone with security enabled reregisters to the subscriber server when the publisher server goes down.
CSCsk23652	Session Initiation Protocol (SIP) Station: Cisco Unified CallManager reports the wrong security status.
CSCsk36982	Session Initiation Protocol (SIP) Station: Phone that is using SIP cannot see a call on shared line if RSVP feature is involved.
CSCsk66471	Session Initiation Protocol (SIP) Trunk: Cisco Unified CallManager hangs in response to reINVITE for passthrough.
CSCsk07094	SS Transfer: Call transfer loop exists on SCCP phone.
CSCsh36576	System: If the "DSCP for Cisco CallManager to Device Interface" enterprise parameter is set higher than CS4 (the default specifies CS3), the signaling packets from Cisco Unified CallManager get tagged with DSCP 000000 instead of the configured DSCP, such as DSCP CS5 101000.
CSCsk27418	System: If trace compression gets enabled, call throughput decreases.
CSCsj20653	System: A large number of phone unregistrations results in critical alarms getting dropped.
Component: Cisco Customer Performance Indicators (CPI)	
CSCsj63325	Application Installation: Subscriber server allowed to switch to 7.0 version when publisher runs 6.0.
CSCsj89934	Application Installation: Reinstalling the subscriber server with a different hostname is succeessful but the server is not functional.
CSCsk56707	Application Installation: Subscriber server upgrade has inconsistent publisher server version requirements.
CSCsk18230	Data Migration Assistant: The need exists for more feedback from DMA when validation fails.
CSCsk21760	Data Migration Assistant: After DMA gets installed, the menu shortcut to launch DMA displays DMAAdmin.
CSCsg92930	Data Migration Assistant: DMA backup screen does not refresh often so the window appears to be white.
CSCsk36026	Data Migration Assistant: Errors and warnings detected in the DMA framework do not get logged in the single error/warning files.
CSCsj49413	Data Migration Assistant: During a DMA backup, a “This page cannot be displayed” message displays.
CSCsk68701	Data Migration Assistant: Exportdb.dll does not register immediately.
CSCsk27561	Operating System: The CLI command “utils core list” may produce a modprobe core file.
CSCsj74466	Operating System: After an installation, the following error displays: init: ID "SD0" respawning too fast: disabled for 5 minutes.
CSCsk26020	Operating System: Servers incorrectly report kernel-based RAID traps.

Table 11 Open Caveats as of 9-29-2007 (continued)

CSCsk18417	Operating System: Fatal errors get displayed in the install log, but no other symptoms exist.
CSCse71209	Operating System: Smart Array 6i v2.68 requires HD firmware update to avoid POST notification.
CSCsf26301	Operating System: Smart Array 5i requires HD firmware update to avoid POST notification.
CSCsk48990	Operating System: The need exists for updated BIOS firmware to support Woodcrest CPU changes for G0 stepping.
CSCsk44741	Operating System: writeCache setting does not get reflected.
CSCsk21776	Operating System: Support G0 stepping CPU for 7835/45 I2/H2/D2 servers.
CSCsk43801	User Interface: Cisco Unified CallManager Administration GUI unavailable after server restart due to a Tomcat deadlock.
CSCsk50402	User Interface: Cisco Unified CallManager does not recognize IP change of LDAP server when hostname gets used.
CSCsk16329	User Interface: CriticalServiceDown alerts get raised after an upgrade and switchover.
CSCsk03132	User Interface: Remove CTL upload from certificate management window and document same.
Component: Cisco Unified CallManager MIB Agent	
CSCsi85520	NO SUCH NAME error returned in SNMP response.
Component: Cisco Unified CallManager User Interface	
CSCsk40837	Voice mail port Find/List and Configuration windows load too slowly.
CSCsk19222	DirSync starts a full sync when the scheduled time is changed.
Component: Database	
CSCsb71648	Migration took over 15 hours.
CSCsk56867	DMA may fail pre-migration in staged upgrade if all servers do not get upgraded.
CSCsk41452	Cisco Unified CallManager cannot access Cisco Unified CallManager Administration or do other tasks.
CSCsg06024	Database engine DDR block causes shutdown of Tomcat server.
CSCsh45042	Informix replication logs get written to the /tmp directory.
CSCsj90196	The need exists to change DRS process so that subscriber rebuild/restore is not required.
CSCsj40566	User cannot easily migrate from 4.x to 5.x if some characters exist in the database.
CSCsk23690	Dbmon core dump occurs on subscriber node.
CSCsk00416	After restarting, the dbmon cored in the subscriber server.
Component: Dialed Number Analyzer	
CSCsk48057	Changing rows per page changes the search option in Trunk Find\List window.
Component: Directory	
CSCsj24600	When the directory export is exporting directory data, no progress indication gets provided to DMA.

Table 11 Open Caveats as of 9-29-2007 (continued)

Component: Documentation	
CSCsj32442	In the upgrade documentation, the need exists for more specific licensing documentation references.
CSCsj34278	Obtaining License File does not apply to upgrade.
Component: Install Product	
CSCsj56299	CDR Analysis and Reporting does not reflect DST changes for New Zealand.
Component: Java Telephony API (JTAPI) Software Development Toolkit (SDK)	
CSCsg03945	CiscoJTAPIClient-linux.bin fails to install.
Component: Media Storage Application	
CSCsk61129	MOH file upload fails due to lack of disk space.
Component: QRT	
CSCsk31721	User cannot when Web Access is disabled.
Component: RISDC	
CSCsk13293	RisDC process leaking memory overtime consuming over 2GB of voice-mail memory usage.
Component: RTMT	
CSCsk60724	RTMT performance counters stale after an upgrade.
CSCsk60648	RTMT alert cannot download trace by using Windows FTP.
CSCsk27462	No RTMT menu item under main menu.
CSCsk58406	User cannot remove user defined alerts if the same counter exists in more than one alert.
Component: Security	
CSCsk11229	CTLClient can bypass initial checks to access subscriber server.
CSCsk33511	CTL client operation fails.
Component: SNMP Research Agents	
CSCsk35666	CdpAgt VM increases continually after crashes, while MIB polling occurs.
CSCsk35585	VM increases for both Cdpd and CdpAgt when cdpd and cdpAgt get restarted and polled multiple times.
Component: Telephony API (TAPI) Software Development Toolkit (SDK)	
CSCsg23468	Latency exists on PlayWave on TSP after client reboot.
CSCsg23990	TSP svchost pegging occurs at 99 percent CPU during TLS connection.
CSCsb64096	TAPI applications stick during RecordWave with Silence after using multiple Wave devices with CTI ports with regression suites.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Unified CallManager Release 5.1(3) documentation suite was released.

Omissions

This section contains information on the following topics:

Incorrect Information for Voice Mail Port Name Field in Help for this Page

The Port Name field allows 1 to 45 characters including letters, numbers, dots, underscores and dashes, followed by -VI and the port number (from 1 to 96).

Barge Phone Display Messages

When a user initiates a barge to a SIP device, the barge initiator phone displays "To Barge <Display name> (Shared Line DN)."

When a user initiates a barge to a SCCP device, the barge initiator phone displays "To Barge <Display name>."

Call Forward All Call Search Space Backward Compatibility Not Documented

The Cisco Extension Mobility chapter in the *Cisco Unified Features and Services Guide* does not provide information on backward compatibility for the Call Forward All calling search space.

This enhancement allows Cisco Unified CallManager Release 4.x customers who are using device mobility and extension mobility to upgrade to Cisco Unified CallManager Release 5.1 without loss of functionality.

The new service parameter (CFA CSS Activation Policy) supports this enhancement. In the Service Parameter Configuration window, this parameter displays in the Clusterwide Parameters (Feature - Forward) section with two options.

- With Configured CSS (default)
- With Activating Device/Line CSS

If you select the **With Configured CSS** option, the Forward All Calling Search Space that is explicitly configured in the Directory Number Configuration window controls the forward all activation and call forwarding. If the Forward All Calling Search Space is set to None, no calling search space gets configured for Forward All. A forward all activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and Secondary Calling Search Space for Forward All occurs during the forward all activation.

If you prefer to use the combination of the Directory Number Calling Search Space and Device Calling Search Space without explicitly configuring a Forward All Calling Search Space, select **With Activating Device/Line CSS** for the CSS Activation Policy. For this option, when Forward All is activated from the phone, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All automatically get populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device.

With this configuration (Calling Search Space Activation Policy set to With Activating Device/Line), if the Forward All Calling Search Space is set to None, when forward all is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space gets used to verify the forward all attempt.

By default, the value of the CFA CSS Activation Policy service parameter set to With Configured CSS.

Roaming

When a device is roaming in the same device mobility group, Cisco Unified CallManager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the CFA CSS gets set to None, and the CFA CSS Activation Policy gets set to With Activating Device/Line CSS; then,

- The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.
- If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS get used as the CFA CSS.
- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.

For more information about configuration options for Call Forward All, see the Directory Number Configuration chapter in the *Cisco Unified CallManager Administration Guide* and the Understanding Directory Numbers chapter in the *Cisco Unified CallManager System Guide*.

CTI Does Not Support Members of Line Groups

The *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* omit the following restriction: If a DN is a member of a line group or hunt list, any device (CTI port, CTI route point, SCCP phone, or SIP phone) that uses that DN should not be associated with a CTI user.

CTI ports and CTI route points may not be associated with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, that DN cannot be associated with either a CTI port (that you configure with the Phone Configuration window) nor with a CTI route point (that you configure with the CTI Route Point Configuration window).

If you configure a DN as part of a line group, you will not be able to associate that DN with a CTI port nor a CTI route point. Conversely, when you configure a CTI port or CTI route point, you will not be able to specify a DN that already belongs to a line group or to a hunt list.

Certificate Documentation Not Provided for Microsoft Internet Explorer 7.0

The *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* do not provide information on importing the certificate for Internet Explorer 7.0. For information on importing the certificate for Internet Explorer 7.0, see the "Internet Explorer 7 Certificate Support" section on page 5.

Documentation Does Not List Correct Browser Support

The *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* do not list all browsers that are supported with Cisco Unified CallManager Administration in 5.1(3). For the current list of supported browsers, see the "General Administration Enhancements" section on page 11.

Documentation Does Not State That Last Name Is Required for LDAP Synchronization

The Cisco Unified CallManager documentation does not include the following information.

When you configure a user in Microsoft Windows Server 2000 and Windows Server 2003 Active Directory (AD), Netscape/iPlanet Directory, Sun ONE Directory Server 5.1, and Sun Java System Directory Server 5.2, ensure that you configure a last name for the user. After you configure LDAP synchronization in Cisco Unified CallManager Administration, users without last names in the corporate directory do not synchronize with the Cisco Unified CallManager database. No error displays in Cisco Unified CallManager Administration, but the log file indicates which users did not synchronize.

Documentation Does Not State the Minimum Requirement for the Perform a Re-sync Every Field

The *Cisco Unified CallManager Administration Guid*e does not state the minimum requirement for the Perform a Re-sync Every field in the LDAP Directory window in Cisco Unified CallManager Administration. Cisco Unified CallManager can synchronize directory information every 6 hours, which is the minimum requirement for the Perform a Re-Sync Every field.

Using the G.722 Codec

The *Cisco Unified CallManager Administration Guide* and the *Cisco Unified CallManager System Guide* do not provide the following information on the G.722 codec.

Cisco Unified CallManager 5.1(3) supports the Advertise G.722 Codec enterprise parameter, which determines whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified CallManager. Codec negotiation involves two steps. First, the phone must advertise the supported codec(s) to Cisco Unified CallManager (not all phones support the same set of codecs). Second, when Cisco Unified CallManager gets the list of supported codecs from all phones that are involved in the call

attempt, it chooses a commonly supported codec based on various factors, including the region pair setting. This parameter only applies to Cisco Unified IP Phone 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE. Valid values specify True (the specified Cisco Unified IP Phones advertise G.722 to Cisco Unified CallManager) or False (the specified Cisco Unified IP Phones do not advertise G.722 to Cisco Unified CallManager).

Note The default for the Advertise G.722 Codec enterprise parameter enables G.722 on all phones in the cluster. The default value of the phone configuration Advertise G.722 Codec Product-Specific parameter uses the value that the enterprise parameter setting specifies.

The Product-Specific Configuration area in the Phone Configuration window supports the parameter, Advertise G.722 Codec. Use this parameter to override the enterprise parameter on an individual phone basis.

Table 12 indicates how the phone responds to the configuration options.

Table 12 How Phone Responds to Configuration Settings

Enterprise Parameter Setting	Phone (Product-Specific) Parameter Setting	Phone Advertises G.722
Advertise G.722 Codec Enabled (True)	Use System Default	Yes
Advertise G.722 Codec Enabled (True)	Enabled	Yes
Advertise G.722 Codec Enabled (True)	Disabled	No
Advertise G.722 Codec Disabled (False)	Use System Default	No
Advertise G.722 Codec Disabled (False)	Enabled	Yes
Advertise G.722 Codec Disabled (False)	Disabled	No

Cisco Unified CallManager supports G.722, which is a wideband codec, as well as a propriety codec simply named Wideband. Both represent wideband codecs. Wideband codecs such as G.722 provide a superior voice experience because wideband frequency response is 200 Hz to 7 kHz compared to narrowband frequency response of 300 Hz to 3.4 kHz. At 64 kbps, the G.722 codec offers conferencing performance and good music quality.

When users use a headset that supports wideband, they experience improved audio sensitivity when the wideband setting on their phones is enabled (it is disabled by default). To access the wideband headset setting on the phone, users choose the **Settings** icon > **User Preferences** > **Audio Preferences** > **Wideband Headset**. Users should check with their system administrator to be sure their phone system is configured to use G.722 or wideband. If the system is not configured for a wideband codec, they may not detect any additional audio sensitivity, even when they are using a wideband headset.

The following Cisco Unified IP Phones (both SCCP and SIP protocols) support the wideband codec G.722 for use with a wideband headset:

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7941G-GE

- Cisco Unified IP Phone 7941G

When you choose a G.711 or G.722 codec in Region Configuration, you are choosing the bandwidth utilization. Choosing either codec produces the same affect. When you choose either G.711 or G.722, these codecs disallow selecting codecs that have a payload greater than 64 kbps, such as the G.722 wideband codec and Advanced Audio Codec (ACC) (when ACC uses more than one channel).

If you choose a region that is lower than G.711 or G.722, the Advertise G.722 Codec enterprise parameter gets ignored because the system does not allow G.722, G.711, AAC, and wideband.

Tip Disregard the following statements in the System Level Configuration chapter in the *Cisco Unified CallManager System Guide* and in the Region Configuration chapter in the *Cisco Unified CallManager System Guide*: "The default audio codec for all calls through Cisco Unified Communications Manager specifies G.711. If you do not plan to use any other audio codec, you do not need to use regions." Because G.711 and G.722 use the same bandwidth, the system may use G.722 unless you choose False for the Advertise G.722 Codec enterprise parameter.

Tip Enabling the Advertise G.722 Codec parameter causes interoperability problems with call park and ad hoc conferences. When you use the enterprise parameter with features such as ad hoc conferencing and call park, change the setting to Disabled and update the device pools for the phones.

When enabled, the service parameter allows Cisco Unified IP Phones (such as 7971, 7970, 7941, 7961) to negotiate and use the G.722 codec when calls are within the same region.

If individual phone control and use of a specific codec type is required (for example, G.711), check the configuration of each phone (by using Phone Configuration) for the parameter Advertise G.722 Codec and change the setting to Disabled. Save and reset the device.

Note If the Advertise G.722 Codec enterprise parameter is set to Enabled, the administrator can override this by using the G.722 Codec Enabled service parameter. This service parameter determines whether Cisco Unified CallManager supports G.722 negotiation for none, some, or all devices. Valid values specify Enabled for All Devices (support G.722 for all devices), Enabled for All Devices Except Recording-Enabled Devices (support G.722 for all devices except those that have call recording enabled), or Disabled (do not support G.722 codec).

Restrictions Not Documented for the User ID Field in the End User Configuration Window

The *Cisco Unified CallManager Administration Guide* does not state that you can enter any character, including alphanumeric and special characters, in the User ID field in the End User Configuration window in Cisco Unified CallManager Administration. No character restrictions exist for this field.

Tip You can modify end user information only if synchronization with an LDAP server is not enabled. If synchronization is enabled, you can view end user data, but you cannot modify it.

CTI Monitored Lines

To calculate the number of CTI monitored lines in a system, use the following formula:

number of pilot point DNs + (number of clients open * number of directory numbers per phone) + (number of parked directory numbers * number of open clients) = CTI Monitored Lines

Shared Line Configuration

The Tips section for Shared Line Appearance in the *Cisco Unified CallManager System Guide* and the Directory Number Configuration chapter in the *Cisco Unified CallManager Administration Guide* requires this addition:

Shared lines always have identical DN settings, except for the field sections in the Directory Number Configuration window that contains the naming convention "on Device SEPXXXXXXXXXXX," which are maintained/mapped to a specific device.

If you add a shared line to a device, the shared DN configuration settings, such as Calling Search Space and Call Forward and Pickup, display. If these DN configuration settings are changed, the new settings apply to all the shared lines.

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 means that the operations are slowed down when IO utilization is in high demand for call processing, so that call processing can take precedence.

When a user makes a request for an on demand operation when the call processing node is running under high IO conditions, the system now displays a warning, giving the user the opportunity to abort the operation. Be aware that the IO rate threshold values that control when the warning displays are configurable with the following new service parameters (CiscoRIS Data Collector Service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The values of these parameters get compared to the system actual CPU and IOWait values. If the goal (the value of the service parameter) is lower than the actual value, the system issues a warning.

For More Information

- Service Parameters Configuration chapter, *Cisco Unified CallManager Administration Guide*

Trace Compression Support

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

- 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.

Use the new enterprise parameter, Trace Compression, to enable or disable trace compression. The default value for this parameter specifies Disabled. For information on setting the values of enterprise parameters, see the Enterprise Parameters Configuration chapter in the *Cisco Unified CallManager Administration Guide*.

You can recognize compressed files by their .gz extension (.gzo if the file is still being written to). To open a compressed file, double click the file name, and the file opens in the log viewer.

For More Information

- Enterprise Parameters Configuration chapter, *Cisco Unified CallManager Administration Guide*

Adding RTMT Performance Counters in Bulk

The *Cisco Unified CallManager Serviceability Administration Guide* omits the following information about adding multiple counters and instances of counters in a single add operation.

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, it was only possible to add them one at a time.

In table format, be aware that all the following methods are now available for selecting counters to view:

- Double click single counter, select single instance from popup window and click **Add**.
- Double click single counter, select multiple instances from popup window and click **Add**.
- Drag single counter, select single instance from popup window and click **Add**.
- Drag single counter, select multiple instances from popup window and click **Add**.
- Select multiple counters, drag on window, select single instance from popup window and click **Add**.
- Select multiple counters, drag on window, select multiple instances from popup window and click **Add**.

In chart format makes the following methods available:

- Double click single counter, select single instance from popup window and click **Add**.
- Drag single counter, select single instance from popup window and click **Add**.

If you attempt to add multiple counters at one time while in chart format, a message displays to indicate that you can only select a single counter or instance while in chart format.

For more information about performance monitoring, see the Configuring and Using Performance Monitoring chapter in the *Cisco Unified CallManager Serviceability Administration Guide*.

Errors

This section contains information on the following topics:

Obtaining a License File

Licensing helps manage Cisco Unified CallManager licenses and enforces the licenses for Cisco Unified CallManager nodes and devices.

The *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* contain incomplete information on obtaining and uploading licenses.

The following sections provide the correct information on obtaining licenses for new Cisco Unified CallManager nodes and/or devices as well as for Cisco Unified CallManager nodes that have been upgraded from various releases.

Note The *Installing Cisco Unified CallManager Release 5.1(3)* and *Upgrading Cisco Unified CallManager Release 5.1(3)* documents also contain the correct licensing procedures.

Note You do not need to obtain new licenses if you are upgrading within a software release train, such as 5.0(1) to 5.1(1).

To obtain and upload a license, see the section that applies to your situation:

New Cisco CallManager Servers and Devices

Use the following procedure to obtain a node license file for new Cisco Unified CallManager servers and to obtain device licenses for new devices that require additional device license units.

Each node in your cluster requires one node license unit. Each device type requires a fixed number of licenses units, depending on the type. For example, Cisco Unified IP Phone 7920 require four license units, and Cisco Unified IP Phone 7970 require five units. If you want licenses for four Cisco Unified IP Phones 7920 and four Cisco Unified IP Phones 7970 phones, you require 36 phone license units.

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary permanent licenses, as described in the following procedure.

Procedure

Step 1 Enter the Product Authorization Key (PAK) that you received with your Cisco Unified CallManager or phone order in the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Click **Submit**.

Step 3 Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified CallManager cluster. You must enter a valid e-mail address as well as the number of nodes and device license units for which you want licenses.

Note For information on calculating the number of device license units that are required for the devices in your system, refer to the "License Unit Calculator" section in the *Cisco Unified CallManager Administration Guide*.

The system sends the license file(s) to you via e-mail by using the E-mail ID that you provided. The format of a license file specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Note One license file may apply to more than one node in your cluster. For information on how to interpret the license file, see the "License File Contents" section of the *Cisco Unified CallManager System Guide*.

Step 4 You must upload the license file to the server with the matching MAC address that you provided in Step 3. See the "Uploading a License file" section on page 57. This server then takes on the functionality of the license manager.

Note You can use the licenses that are specified in the license file only within the cluster on which the license file is uploaded.

Upgrading From Cisco Unified CallManager 4.x Releases

When you upgrade from supported Cisco Unified CallManager Manager 4.x releases, the system calculates the licenses that are required for existing devices and Cisco Unified CallManager nodes and generates an intermediate file (XML file) that contains this information. You use this file to obtain license files that you can upgrade into Cisco Unified CallManager Administration. You receive these licenses free of cost because you are already using these phones for a Cisco Unified CallManager 4.x release.

Use the following procedure to obtain licenses for Cisco Unified CallManager when upgrading from supported 4.x releases.

Note You do not need to obtain new licenses if you are upgrading within a software release train, such as 5.0(1) to 5.1(1).

Procedure

Step 1 After you complete the Cisco Unified CallManager upgrade process, as described in *Upgrading Cisco Unified CallManager*, navigate to Cisco Unified CallManager Administration and choose **System > Licensing > License File Upload**.

The License File Upload window displays.

Step 2 Choose the licugrade_<upgrade version>.lic file from the Existing Files drop-down list and click **View File**. A pop-up window displays that has the license information for existing devices and nodes. Copy this information. To copy the contents on this window, you can use **Ctrl-A** (Select All) and **Ctrl-C** (Copy).

Step 3 Navigate to the License Registration web tool at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=806.

Step 4 Enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified CallManager cluster.

Step 5 In the text box that is provided, paste the license file contents that you copied in Step 2 by using the appropriate keyboard shortcuts, such as **Ctrl-V**.

Step 6 Enter a valid e-mail address and click **Continue**. A license file generates.

The system sends the license file to you via e-mail by using the E-mail address that you provided.

Step 7 You must upload the license file to the server with the matching MAC address that you provided in Step 4. See the "Uploading a License file" section on page 57.

Step 8 You can obtain licenses for new devices that you are adding to the upgraded system, if your system requires additional device license units. For detailed instructions, see the "New Cisco CallManager Servers and Devices" section on page 55.

Uploading a License file

Use the following procedure to upload a license file to the Cisco Unified CallManager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the "Obtaining a License File" section on page 55. The Cisco Unified CallManager server where the license file is loaded takes on the functionality of the license manager.

Note Upload the license file only on the first node of Cisco Unified CallManager cluster.

Procedure

Step 1 Choose **System > License > Upload License File**.

The License File Upload window displays.

Step 2 The Existing License Files drop-down list box displays the license files that are already uploaded to the server.

Note To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.

Step 3 To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4 Browse and choose a license file to upload to the server.

Note The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 5 Click **Upload License File**.

After the upload process completes, the Upload Result file displays.

Step 6 Click **Close**.

Step 7 In the License File Upload window, the status of the uploaded file displays.

Note The license file gets uploaded into the database, only if the version specified in the license file is greater than or equal to the Cisco Unified CallManager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

License File Contents

The *Cisco Unified CallManager System Guide* does not include the following example of a permanent Cisco Unified CallManager node license:

Example 0-1 Permanent CCM_Node licenses

```
# Optional usage agreement, legal language, tracking information
# Some other comments
INCREMENT CCM_NODE cisco 5.0 permanent uncounted \
VENDOR_STRING=<Count>3</Count><OrigMacId>000BCD4EE59D</OrigMacId><LicFileVersion>1.0</LicF
ileVersion> \
 HOSTID=000bcd4ee59d \
 NOTICE="<LicFileID>20050826140539162</LicFileID><LicLineID>1</LicLineID> \
 <PAK></PAK>" SIGN="19B3 4C6C 25AC 6D22 4D75 DE6A 656B 08C5 \
 30E4 16DB 771B 1393 9DC1 DBC4 C5AA 15CC 6E6C B7B8 895A DCBA \
 B40F C551 2625 1C97 F20D 9977 6CFF 3603 081E 6FF2"
```

The preceding license file includes the following information:

- No expiration date for this license exists as indicated by the keyword permanent.
- This license file provides three licenses for the version 5.0 of the feature CCM_NODES.
- The Cisco-specific fieldLicFileID identifies this license file.
- You can add multiple increment lines for same feature in a license file to increase the license count. Ensure that no INCREMENT lines are identical and each of them gets signed independently.

Number of Supported Locations and Regions Increased

The *Cisco Unified CallManager System Guide* and *Cisco Unified CallManager Administration Guide* incorrectly state the number of regions and locations that Cisco Unified CallManager supports.

Cisco Unified CallManager supports up to 1000 locations and up to 2000 regions. The following limitations and restrictions apply:

- Configure as many regions as possible to Use System Default for inter-/intra-region audio codecs and video bandwidth.
- Configure as many locations as possible to Use System Default for the RSVP policy.
- This enhancement requires an MCS 7845H1 or higher server.

Description of Create all new ports like port 1 Button Incorrect

The *Cisco Unified CallManager Administration Guide* describes the Create all new ports like port 1 button incorrectly. When you configure the button, use the following information.

The Create all new ports like port 1 button allows you to create ports 2 through 48 with the same parameters and settings as port 1, only if ports 2 through 48 are not configured.

Message Waiting Configuration Field Descriptions

The descriptions that are provided in the *Cisco Unified CallManager Administration Guide* do not match the allowed values for various fields. The following table contains the revised field descriptions.

Table 13 Message Waiting Configuration Settings

Field Name	Description
Message Waiting Number	Enter the Cisco Message Waiting directory number. Make sure that this number is not used within the Cisco Unified Communications Manager auto-registration range. You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !.
Description	Enter up to 50 characters for a description of the message-waiting directory number. You may use any characters except the following ones: “, <, >, &, %.

Media Resource Group Configuration Field Description

The description that is provided in the *Cisco Unified CallManager Administration Guide* does not match the allowed values for the Description field of the Media Resource Group Configuration window. The following table contains the revised field description.

Table 14 Media Resource Group Configuration Settings

Field	Description
Description	Enter a description for the media resource group. This description can comprise up to 50 characters. Ensure Description does not contain double quotes (“), less than (<), greater than (>), ampersand (&), or the percent sign (%).

Transcoder Configuration Field Description

The description that is provided in the *Cisco Unified CallManager Administration Guide* does not match the details for the Description field of the Transcoder Configuration window. The following table contains the revised field description.

Table 15 Transcoder Configuration Settings

Field	Description
Description	Enter a description (up to 128 characters) or leave blank to generate automatically from the MAC address or device name that you provide.

Application and End User CAPF Profile Configuration Instance ID Setting

The Application and End User CAPF Profile Configuration Settings table in the *Cisco Unified CallManager Security Guide* incorrectly states that the Instance Id field allows these characters: dots (.), dashes(-) and underscore (_). The Instance ID field allows only alphanumeric characters (a-zA-Z0-9).

Incorrect Description for User ID Field End User, Phone, DN, and LA Configuration window

The *Cisco Unified CallManager Administration Guide* incorrectly describes the User ID field that displays in the End User, Phone, DN, and LA Configuration window in Cisco Unified CallManager Administration. When you configure that field, use the following information instead of the information in the administration guide: Enter the end user identification name. Cisco Unified CallManager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , ""

Incorrect Information on How to Install Assistant Console Application

The *Cisco Unified CallManager Features and Services Guide* incorrectly describes how to obtain the assistant console application for Cisco Unified CallManager Assistant. In 5.1(3), the assistant no longer obtains the assistant console application via the URL that is listed in the guide. Instead, the assistant must download the Cisco Unified CallManager Assistant plug-in from Cisco Unified CallManager Administration (choose **Applications** > **Plugins**), as described in the "Cisco Unified CallManager Assistant" section on page 12.

The *Cisco Unified CallManager Features and Services Guide* does not state that the assistant console application supports Windows Vista.

Disregard the entire section, Assistant Console Dialog Options, in the *Cisco Unified CallManager Features and Services Guide*. Instead, use the information in the "Cisco Unified CallManager Assistant" section on page 12.

Incorrect Information for Description Field in the Message Waiting Configuration Window

The *Cisco Unified CallManager Administration Guide* incorrectly states that you can enter up to 30 characters in the Description field in the Message Waiting Configuration window in Cisco Unified CallManager Administration. You can enter up to 50 characters.

Restoring Data to a Subsequent Node

The Restoring Subsequent Cluster Nodes section of the *Disaster Recovery System Administration Guide* incorrectly states that you must restore a subsequent node by restoring it from the same DRS backup file that you used to restore the first node.

Instead, you restore a subsequent node by performing a restore operation on the first node in the cluster. The Restore wizard allows you to select which nodes to restore and prompts you to enter the location of the directory where you backed up your data using DRS. You do not specify a backup file within this directory. DRS automatically obtains the correct backup data to restore the nodes that you selected.

Cisco Unified IP Phone 7902G, 7905G, and 7912G Administration Guide for Cisco Unified CallManager Release 5.0 (SCCP)

The *Cisco Unified IP Phone 7902G, 7905G, and 7912G Administration Guide for Cisco Unified CallManager Release 5.0 (SCCP)* incorrectly documents how an administrator should customize the 7905G and 7912G phones logo. The following sections provide the correct procedure.

Configuring a Custom Background Image

To configure custom background images for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Open a command window and enter the following command:

bmp2logo imageID image.bmp image.logo

where:

- imageID specifies a unique identifier for the new graphic. This identifier must comprise a number from 0 through 4294967296 and must differ from the identifier of the graphic that is currently on the phone.
- image is the base file name of the image that you previously created and saved with the graphics program.

Note The imageID of the image that comes with the phone specifies 1.

For example, if the image identifier is 10 and the base name of your image file is mylogo, enter this command:

bmp2logo 10 mylogo.bmp mylogo.log

Step 2 Copy the image.logo file to the following directory in the TFTP server for the Cisco Unified CallManager:

/

Note Be aware that the file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

Step 3 Add the following line to the Cisco Unified IP Phone profile file:

upgradelogo:imageID,TFTPServerID,image.logo

where:

- imageID specifies the same unique identifier that you specified in Step 1.
- TFTPServerID specifies the IP address of the TFTP server on which the image.logo file gets stored. If the image.logo file is stored on the same TFTP server as the Cisco Unified IP Phone configuration file, replace TFTPServerID with the numeral 0.
- image specifies the base file name of the image file.

  For example, if the image identifier is 10, the converted file is stored on the same TFTP server as the Cisco Unified IP Phone configuration file, and the base name of the converted image file specifies mylogo, add the following line to the configuration file:

  upgradelogo:10,0,mylogo.logo

Note For detailed information about using profile files, see Appendix A, "Additional Configuration Methods and Parameters."

Step 4 Use the cfgfmt.exe tool to generate a binary profile file from the text file.

Step 5 Upload the new binary file that you created to the following directory in the TFTP server for the Cisco Unified CallManager:

/

Note Be aware that the file name and directory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the directory path.

To upload the files, choose **Software Upgrades > Upload TFTP Server File** in Cisco Unified OS Administration. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

You must also copy the customized binary files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you also store backup copies of custom binary files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified CallManager.

Note For detailed information about using profile files, see Appendix A, "Additional Configuration Methods and Parameters."

Step 6 Power cycle the phone.

The new graphic displays when the phone restarts

Incorrect URL for the Cisco Unified CallManager User Option Pages

The Cisco WebDialer chapter in the *Cisco Unified CallManager Features and Services Guide* provides an incorrect URL for the Cisco Unified CallManager User Option Pages. The URL should read

https://<IP address of the Cisco Unified CallManager server>:8443/ccmuser/showhome.do.

Incorrect Information on Configuring Partitions and DNs for JTAPI/TAPI Controlled Devices

Disregard the following note in the Directory Number Configuration chapter in the *Cisco Unified CallManager Administration Guide*: If a JTAPI or TAPI application controls or monitors a device, you should not configure multiple instances of the same DN (with different partitions) on that device.

In fact, if a JTAPI or TAPI application controls a device, you can configure multiple instances of the same DN (with different partitions) on that device.

Default Device Profile Information

The Default Device Profile Configuration chapter of the *Cisco Unified CallManager Administration Guide* incorrectly states that the Default Device Profile can be configured to subscribe to services. Disregard the following text:

- The entire section entitled “Subscribing Services to a Default Device Profile.”
- The portion of the introductory sentence in the “Configuring a New Device Profile” section that lists “subscribed IP phone services” as one of the configurable attributes of the default device profile.

rtmt.log Storage Location

The Trace Collection and Log Central in RTMT chapter of the *Cisco Unified CallManager Serviceability Administration Guide* inaccurately describes the storage location of the rtmt.log file. The correct information follows:

Updating the Trace Configuration Setting for RTMT

To edit trace settings for the Real-Time Monitoring plug-in, choose **Edit > Trace Settings**; then, click the radio button that applies. The system stores the rtmt.log file in the Documents and Settings directory for the user; for example, on a Windows machine, the log gets stored in C:\Documents and Settings\<userid>\.jrtmt\log.

Updates

This section contains updates that have occurred since the release of the Cisco Unified CallManager 5.1(3) documentation. These changes may not appear in the current documentation or the online help for Cisco Unified CallManager:

- Single Sign-On Capability, page 64
- Using Cisco Extension Mobility Description in Cisco Unified IP Phone User Guides, page 64
- Recovering Administrator and Security Passwords, page 64
- Changing a Cisco Unified CallManager Server IP Address, page 65

Single Sign-On Capability

The Application Users and End Users chapter of the *Cisco Unified CallManager System Guide* requires this update for single sign-on capability:

Administrator users in the Standard Unified CM Super Users group can access all administrative applications in the Cisco Unified CallManager Administration navigation menu (Cisco Unified CallManager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting) with a single sign-on to one of the applications.

You set the default Administrator username and password during Cisco Unified CallManager installation. You can change the Administrator password or set up a new Administrator account in the Application User Configuration window in Cisco Unified CallManager Administration.

Using Cisco Extension Mobility Description in Cisco Unified IP Phone User Guides

The following information on extension mobility needs updating in the *Cisco Unified IP Phone Guide* (all phone models).

Cisco Extension Mobility (EM) allows you to temporarily configure a Cisco Unified IP Phone as your own. After you log in to EM, the phone adopts your user profile, including your phone lines, features, established services, and web-based settings. Your system administrator must configure EM for you.

Tips

- EM automatically logs you out after a certain time. Your system administrators establishes this time limit.
- Changes that you make to your EM profile from your User Options web pages take effect immediately if you are logged in to EM on the phone; otherwise, changes take effect the next time that you log in.
- Changes that you make to your EM profile directly on the phone (rather than on your User Options web pages) take effect immediately if you are logged out of EM; otherwise, changes take effect after you log out.
- Local settings that are controlled by the phone do not get maintained in your EM profile.

Recovering Administrator and Security Passwords

This section replaces the section Recovering the Administrator Password in the Log In To Cisco Unified Communications Operating System Administration chapter of the *Cisco Unified Communications Operating System Administration Guide* for releases 5.0(4), 5.1(1), and 6.0(1).

If you lose the administrator password or security password, use the following procedure to reset these passwords.

Note During this procedure, you will be required to remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**

- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

Caution The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Changing a Cisco Unified CallManager Server IP Address

To change the IP address of a Cisco Unified CallManager server, refer to the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094601.shtml

Changes

This section contains changes that have occurred since the release of the Cisco Unified CallManager 5.1(3) documentation. These changes may not appear in the current documentation or the online help for Cisco Unified CallManager:

- IPMA Assistant Console Installation and Windows Vista Support, page 66
- CDR Search Report GUI, page 66
- Devices Associated with the Attendant Console Application User, page 66
- Third Party Certificate Authority Verification, page 67

IPMA Assistant Console Installation and Windows Vista Support

The following changes have been made to IPMA Assistant Console installation to support Windows Vista.

The URL-based installation no longer gets supported by Cisco Unified CallManager Administration and is available only via the Cisco Unified CallManager Administration plugin download page only.

Procedure

Step 1 From the Cisco Unified CallManager plugin page, download CiscoUnifiedCallManagerAssistantConsole.exe.

Step 2 Double-click the .exe file to set up Assistant Console.

Step 3 After the Assistant Console is set up, the IP address of the Cisco Unified CallManager server should be provided to the Assistant Console to connect to the IPMA services.

CDR Search Report GUI

The CDR Search Report GUI windows have been changed to show both the UTC and Local time of the server, including the date and time string (time string format is HH:MM:SS), as in Aug 31, 2007 12:00:00. The default ToDate search criteria got changed to be that of the time of the server in UTC time and the default FromDate got set to be one hour earlier than the ToDate.

Devices Associated with the Attendant Console Application User

The *Cisco Unified CallManager Features and Services Guide* incorrectly states that administrators who are configuring Cisco Unified CallManager Attendant Console must associate devices with the Cisco Unified CallManager Attendant Console ac application user, unless the administrators enable the superprovider feature.

The document should state that administrators must always enable the superprovider feature by associating the ac application user with the user group “Standard CTI Allow Control of All Devices” and must not associate any devices with the Cisco Unified CallManager Attendant Console ac application user.

Caution System instability can occur if you associate devices to the Cisco Unified CallManager Attendant Console application user.

During an upgrade from Cisco Unified CallManager Release 4.x, the system automatically converts the ac application user to a superprovider user and disassociates the devices that were previously associated to the application user.

To enable device security for the Cisco Unified CallManager Attendant Console, configure an ACDeviceAuthenticationUser application user and associate the attendant phones with that user.

Third Party Certificate Authority Verification

The Cisco Unified Communications Operating System Administration Guide, Release 5.1(1) states that Cisco has verified Verisign as a source for third party certificates. This is no longer correct, and Verisign is not a verified CA.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.