Release Notes for Cisco Unified CallManager Release 5.1(1)

December 11, 2006

These release notes describe the new features and caveats for Cisco Unified CallManager release 5.1(1). 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/univercd/cc/td/doc/product/voice/c_callmg/index.htm

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(1). 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(1) 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:

Cisco Systems

Corporate 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(1) on a Cisco Media Convergence Server (MCS).

You may also install Cisco Unified CallManager on a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

Cisco Unified CallManager 5.1(1) requires a minimum of the following items on the Cisco MCS servers.

- 2 GB of memory
- 72 GB disk drive
- 2 GHz processor

Supported Platforms

To find which servers support the Cisco Unified CallManager 5.1(1) release, please refer to the *Guide to Cisco CallManager Upgrades and Server Migrations* at http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html

Determining the Software Version

To determine the software version of Cisco Unified CallManager, open Cisco Unified CallManager Administration. The following information displays:

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

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.

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 documentation that supports Cisco Unified CallManager Release 5.1(1) comprises existing release 5.0(4) documentation that is listed in the *Cisco Unified CallManager Release 5.1(1) Documentation Guide*, as well as the following new release 5.1(1) documents:

- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- *Release 5.1(1) Release Notes for Cisco Unified CallManager*
- *Upgrading Cisco Unified CallManager, Release 5.1(1)*
- *Installing Cisco Unified CallManager, Release 5.1(1)*
- *Data Migration Assistant Administration Guide, Release 5.1(1)*
- *Cisco Unified Communications Operating System Administration Guide, Release 5.1(1)*
- *Cisco Unified Communications Locale Installer Release Notes for Cisco Unified CallManager, Release 5.1*

The *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)* is a new document that is specific to release 5.1(1)

Limitations and Restrictions

A major deliverable of the Cisco Unified Communications System testing is a recommendation of compatible software releases that have been verified by the test for customers. The recommendations are not exclusive and are in addition to interoperability recommendations for each of the individual voice application or voice infrastructure products.

For a list of Software and Firmware versions of IP telephony components that were tested for interoperability with Cisco Unified CallManager 5.1(1) as part of Unified Communications System Release 5.1(1) testing, see: http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc511/relnotes/rnipt511.htm

For a list of Software and Firmware versions of contact center components that were tested for interoperability with Cisco Unified CallManager 5.1(1) as part of Unified Communications System Release 5.1(1) testing, see: http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc511/relnotes/rnipc511.htm.

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(1). For the most current compatibility combinations and defects that are associated with other Cisco Unified Communications 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(1).

Upgrading from Cisco Unified CallManager Release 5.0(4) to Release 5.1(1)

During the upgrade of Cisco Unified CallManager, the server experiences high disk I/O activity. This can adversely impact call processing. In the worst case, phones that are currently registered with that Cisco Unified CallManager server may failover to their backup server. Cisco strongly recommends that you ensure that all trace levels are set to the default level on all servers in your cluster before you start the upgrade process.

Furthermore, if you have concerns that the upgrade may impact call processing service, Cisco recommends that you perform the upgrade during off-peak hours. If you want to minimize the disruptions to the call processing service, you may choose to stop the Cisco Unified CallManager service on the server before you start the upgrade process.

As always, please follow your standard best practices while performing a Cisco Unified CallManager upgrade.

MTP and Cisco Unified SIP IP Phones

You can configure Cisco Unified CallManager SIP devices (lines and trunks) to always use an MTP. If the configuration parameters are set to not use an MTP (default case), Cisco Unified CallManager will attempt to dynamically allocate an MTP if the DTMF methods for the call are not compatible.

For example, SCCP phones support only out-of-band DTMF, and Cisco Unified SIP IP phones (7905, 7912, 7940, 7960) support RFC2833. Because the DTMF methods are not identical, Cisco Unified CallManager will dynamically allocate an MTP.

If, however, a SCCP phone that supports RFC2833 and out-of-band use, such as Cisco Unified IP Phone 7971, calls a Cisco Unified SIP IP Phone 7940, Cisco Unified CallManager will not allocate an MTP because both phones support RFC2833. Because the same type of DTMF method is supported on each phone, no need exists for an MTP.

Note Cisco Unified CallManager 5.0 and later provides an "MTP Required" checkbox for Cisco Unified SIP IP phones, but you **should not** check this check box for Cisco Unified SIP IP phones.

If you check the “MTP Required” checkbox you may experience problems with Cisco Unified CallManager features such as Shared Line.

When you leave this check box unchecked, Cisco Unified CallManager will still insert MTPs dynamically as needed, so you will experience no benefit from checking the "MTP Required" check box for Cisco Unified SIP IP phones.

Although this configuration option for Cisco Unified SIP IP phones may be removed in a future Cisco Unified CallManager release, Cisco will continue to support it for generic third-party SIP phones.

Rebuilding RAID Drives

A RAID drive may fail and may require manual intervention to rebuild one of the physical drives in a logical pair during normal Cisco Unified CallManager operation.

RAIDed disks, also termed RAID arrays, get arranged in logical pairs. A single logical pair comprises two physical drives. The system keeps the pair of drives in sync with the same data in real time to provide redundancy ultimately for data integrity and assurance. When one physical drive fails to synchronize or begins to experience read or write failures, you may need to rebuild the drive. Many things can cause the failure, but the main concern remains whether the data in a logical drive pair is compromised due to failures in one of the physical drives.

Monitoring software usually detects RAID failures, and failures get reported as a failed drive or a loss of drive redundancy. The procedure for rebuilding a failing drive follows and applies to all Cisco MCS model 7825, 7835, and 7845 servers.

First, check the status of the RAID array by using the CLI **show hardware** command and verify whether the Status field reads Ok or Okay. An example follows:

```
admin:show hardware

HW Platform       : 7835I

Processors      : 1

Type            : Intel(R) Xeon(TM) CPU 3.06GHz

CPU Speed        : 3066

Memory          : 2048 MBytes

Object ID       : 1.3.6.1.4.1.9.1.585

OS Version       : UCOS 2.0.1.0-37

RAID Details      :
```

```
Found 1 IBM ServeRAID controller(s).
Read configuration has been initiated for controller 1...
-------------------------------------------------------------------
Logical drive information
-------------------------------------------------------------------
 Logical drive number 1
         Status of logical drive        : Okay (OKAY)
         RAID level                    : 1
         Size (in MB)                  : 70006
         Write cache status             : Temporary write through (TWT)
         Number of chunks                 : 2
         Stripe-unit size              : 8 KB
         Access blocked                  : No
         Part of array                 : A
Array A stripe order (Channel/SCSI ID)  : 1,0 1,1 Command completed successfully.
```

If the RAID array status field does not read Ok or Okay (for example, shows Degraded or Critical), perform the following steps:

1. Log in to console and enter the CLI command, **utils system shutdown**.

   For information on how to access the console to perform CLI commands, see the *Cisco Unified Communications Operating System Administration Guide*.

2. Power off the server (press power off button).
3. Extract the failed disk drive.
4. Power up the server (press power on button).
   a. If the server is an IBM server (for example, a 7825I, 7835I, or 7845I), the following menu will appear during system reboot:

      ```
      1:ServeRAID-5i Slot 2, Logical drv=1, Firmware=7.12.07, Status=Fail
      1 Drive(s) not responding or found at new location(s)
      Press F2 Detailed information
               F4 Retry the command
               F5 Change the configuration and set the drive(s) defunct
               F10 Continue without changing the configuration
      ```

   b. Press F5
5. After the login prompt appears in the console window, log in and check the status of the RAID array by using the CLI **show hardware** command; the Status field should read Degraded or Critical.
6. Insert the failed disk drive into the original slot; be sure to lock it properly in place.
7. Check the status of the RAID array by using the CLI **show hardware** command; the Status field will read Rebuilding or Critical.
8. After an hour, recheck the status of the RAID array by using the CLI **show hardware** command and verify that the Status field reads Ok or Okay.

If the status does not read Ok or Okay, you may need to replace the physical drive.

Cisco Unified Communications Answer File Generator

Cisco Unified CallManager Release 5.1(1) includes a web application that is called Cisco Unified Communications Answer File Generator that is used to generate answer files for unattended installations of Cisco Unified CallManager Release 5.0(1) and later. Individual answer files get copied to a USB key or a floppy diskette that accompanies the Cisco Unified CallManager DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
- Provides syntactical validation of data entries
- Provides online help and documentation

The following usage requirements apply:

- The web application supports only fresh installs (for example, it does not include upgrades).
- If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.

If a USB key is being used to perform an unattended installation of Cisco Unified CallManager, you may need to reformat the USB key to the FAT32 file system beforehand. You need to reformat especially in the case of USB keys with larger storage capacity (for example, 1 Gigabyte) that are formatted with the FAT file system.

You can use the Windows XP Disk Management Utility to reformat a USB key to the FAT32 file system as follows (you might need to be logged in as an administrator or a member of the Administrators group to perform these tasks):

1. Insert the USB key into a USB slot on the Windows XP PC.
2. Choose **Start** > **Control Panel** > **Administrative Tools** and then double-click Computer Management.
3. Expand the Storage tree and click Disk Management.
4. Right-click the Removable Disk icon and click Format ... . You may be asked whether you are sure that you want to format this partition; click Yes.
5. Click the File System: pull down and select FAT32.
6. Click OK. When prompted to format the volume, click OK again.
7. The Removable Disk icon text should now show the file system format as FAT32.

Using SIP Trunks Between Release 4.x and 5.x Systems

Cisco Unified CallManager Release 5.0 and later and Cisco Unified CallManager Release 4.0 and later support TCP and UDP as Transport Types when they are used with SIP trunks. However, release 4.x uses one TCP connection per SIP call; 5.x supports multiple SIP calls over the same TCP connection (referred to as TCP connection reuse).

The following Cisco products support TCP; however, not all support TCP Reuse (see Table 2 for more information):

- Cisco Unified CallManager Release 4.1 - No TCP Connection Reuse
- Cisco Unified CallManager Release 4.2 - No TCP Connection Reuse
- Cisco Unified CallManager Release 5.0(2) - TCP Connection Reuse
- Cisco Unified CallManager Release 5.0(4) - TCP Connection Reuse
- Cisco Unified CallManager Release 5.1(1) - TCP Connection Reuse
- Cisco IOS 12.3(8)T and above - TCP Reuse
- Cisco IOS 12.3(8)T and below - No TCP Reuse

Table 2 lists the SIP trunk connectivity that is supported between Cisco Unified CallManager Release 4.x and 5.x and the IOS gateway.

Table 2 SIP Trunk Compatibility Matrix

	Cisco Unified CallManager Release 4.x	Cisco Unified CallManager Release 5.x	IOS 12.3(8)T	IOS 12.3(8)T Below
Cisco Unified CallManager Release 4.x	UDP/TCP	UDP only	UDP only	UDP/TCP
Cisco Unified CallManager Release 5.x	UDP only	UDP/TCP	UDP/TCP	UDP only
IOS 12.3(8)T	UDP only	UDP/TCP	UDP/TCP	UDP only
IOS 12.3(8)T Below	UDP/TCP	UDP only	UDP only	UDP/TCP

If a Release 5.x system makes multiple calls over a TCP-based SIP trunk to a 4.x system, the 4.x system will only connect one call. The rest of the calls will not get connected.When using SIP trunks between 4.x and 5.x systems, you must configure both systems to use UDP as the Outgoing Transport Type, so calls between the release 4.x and 5.x systems will connect properly. (See Table 2.)

To configure UDP, use Cisco Unified CallManager Administration.

- For Cisco Unified CallManager Release 5.0 and later that is connecting to a Release 4.x system, choose UDP as the Outgoing Transport Type from the SIP Trunk Security Profile Configuration window.
- For Cisco Unified CallManager Release 4.0 and later that is connecting to a Release 5.x system, choose UDP as the Outgoing Transport Type from the Trunk Configuration window.

For more information about SIP trunks, see the *Cisco Unified CallManager System Guide* and the *Cisco Unified CallManager Administration Guide*.

Configuring SIP Phones With Same Directory Number

Cisco Unified SIP IP Phones 7906, 7911, 7941, 7961, 7970, and 7971 can support multiple lines with the same directory number in different partitions. However, configuring and using other Cisco Unified SIP IP Phones with multiple lines with the same directory number does not get supported.

New and Changed Information for Cisco Unified CallManager Release 5.1(1)

The following sections describe new features and changes that are pertinent to Cisco Unified CallManager, Release 5.1(1) or later. The sections may include configuration tips for the administrator, information about users and where to find more information.

- New and Changed Information for Cisco Unified CallManager Administration, page 9
- New and Changed Information for Cisco Unified Communications Operating System Administration, page 14
- New and Changed Information for Cisco Unified CallManager Features, page 14
- New and Changed Information for Cisco Unified CallManager Applications, page 17
- New and Changed Information for Cisco Unified CallManager Bulk Administration Features, page 18
- New and Changed Information for Cisco Unified CallManager Serviceability, page 20
- New and Changed Information for Third-Party API, page 22
- New and Changed Information for Cisco Unified IP Phones, page 23

New and Changed Information for Cisco Unified CallManager Administration

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

- Cisco Unified CallManager Installation, page 10
- General Administration Enhancements, page 10
- Service Parameter Changes, page 10
- Cisco Unified CallManager Administration Menu Updates, page 11
- Third-Party SIP Phone Enhancements, page 11
- Phone Configuration Enhancements, page 11
- Phone Button Configuration Enhancements, page 11
- License Capabilities Assignment, page 12
- Call Forward Overriding, page 12
- Enterprise Parameter Changes, page 12

- Additional Corporate Directory Support, page 13

Cisco Unified CallManager Installation

Cisco Unified CallManager 5.1 includes the following installation enhancements.

- New network connectivity checking—The installation program checks for network connectivity. If the network is not accessible, you have several options for how to proceed with the installation.
- New hostname and IP assignment during upgrade—The upgrade installation program now allows you to use a different hostname or IP address on the upgraded system.

For more information

- *Installing Cisco Unified CallManager Release 5.1(1)*
- *Upgrading Cisco Unified CallManager Release 5.1(1)*

Data Migration Assistant (DMA) 5.1 includes the following enhancements:

- DMA migrates data for upgrades of Cisco Emergency Responder (CER) 1.3.
- Enhanced interaction between DMA and Cisco Security Agent for Cisco Unified CallManager (CSA) occurs. Depending on the versions of DMA and CSA that you are using, you may possibly leave CSA enabled while DMA runs. In other cases, DMA automatically disables CSA while it is running, and in some cases you must disable CSA manually while you are running DMA.

For more information

- *Data Migration Assistant User Guide Release 5.1(1)*.

General Administration Enhancements

The following requirements apply to Cisco Unified CallManager Administration:

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

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

Service Parameter Changes

Cisco Unified CallManager 5.1 supports the following service parameter changes:

- The TFTP Service Parameter no longer includes the Enable Caching of Configuration Files option.
- Immediate Divert includes the following new service parameters:
  - Use Legacy Immediate Divert
  - Allow QSIG During iDivert
  - Immediate Divert User Response Timer

  See the "Immediate Divert Enhancements" section on page 15 for more information.
- The Cisco Database Layer Monitor service includes a new service parameter, "Send Valid Namespace in AXL Response." See the "New AXL Service Parameter" section on page 23 for more information.

- Cisco Unified CallManager provides a new service parameter, CFA Destination Override, that allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. See the "Call Forward All Override" section on page 16 for more information.
- There are two CallManager service parameters related to the Star50 feature
  - Use Legacy Immediate Divert - This cluster wide service parameter defines whether the legacy iDivert behavior is maintained or the new Star50 behavior is adopted. If the Use Legacy iDivert service parameter is set to True, the user can divert an incoming call only to the user's own voice mailbox.
  - Allow QSIG during iDivert – Immediate Divert diverts calls to voice-messaging systems that can be reached over QSIG, SIP and QSIG-enabled H.323 devices if the cluster wide service parameter is set to True.

Cisco Unified CallManager Administration Menu Updates

The System menu in Cisco Unified CallManager Administration includes the License Capabilities option (**System > Licensing > Capabilities Assignment**).

Third-Party SIP Phone Enhancements

The following enhancements took place to third-party SIP phones in Release 5.1(1).

Third-Party SIP Phone Configuration Enhancements

The Basic and Advanced Third-Party SIP Phone Configuration windows include a check box that is called Require DTMF Reception.

Migrating from Cisco Unified CallManager Release 5.0(1), and Above, to Cisco Unified CallManager Release 5.1(1)

In Cisco Unified CallManager Release 5.1(1) and above, certain characteristics for Basic and Advanced Third-Party SIP Phones changed. These characteristics include changes to the Maximum Number of Calls per Device, Default Maximum Number of Calls per DN, and Default Busy Trigger per DN fields that display on the Directory Number Configuration window in Cisco Unified CallManager Administration. See the *Cisco Unified CallManager New and Changed Information Guide* for more information.

Phone Configuration Enhancements

Use the Phone Configuration window to configure the Cisco TelePresence and the Cisco Unified IP Phone 7906 devices. For more information on Cisco TelePresence and the Cisco Unified IP Phone 7906, see the *Cisco Unified CallManager New and Changed Information Guide*.

Phone Button Configuration Enhancements

Use the Phone Button Configuration window to configure the default phone button template for Cisco TelePresence and Cisco Unified IP Phone 7906 SIP and SCCP. For more information on Cisco TelePresence and the Cisco Unified IP Phone 7906, see the *Cisco Unified CallManager New and Changed Information Guide*.

License Capabilities Assignment

Capabilities Assignment allows system administrators to enable the Cisco Unified Presence Server (CUPS) and Cisco Unified Personal Communicator (CUPC) capabilities for users. You must ensure that licenses for CUPS and CUPC are available.

Make license capabilities assignments to existing users. Before you begin, ensure that users exist on your system by choosing **User Management > End User** and clicking **Find**.

Before you begin configuring the capabilities assignments for users, determine how many CUPS (servers and clients) and CUPC licenses are required for your system by choosing **Licensing > License Unit Calculator**. Acquire the required licenses by using **Licensing > License File Upload**. Verify the total licenses by using **Licensing > License Unit Report**.

Note Cisco Unified CallManager, Release 5.0(4) introduced License Capabilities Assignment.*Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)* fully documents it.

Call Forward Overriding

The behavior of this CallManager feature is configurable via service parameter - CFADestinationOverride. When the feature is enabled on CallManager, it allows the CFA Target to reach the CFA Initiator for important calls. TSP application that monitors the CFA initiator will receive call as normal if the call is initiated from the CFA target.

There is no TSP interface change for this Cisco Unified CallManager feature.

For More Information

- License Capabilities Configuration, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Configuring Non-Cisco SIP IP Phones, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Cisco TFTP, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Immediate Divert, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Cisco Unified IP Phones, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- AXL Programming, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Enterprise Parameter Changes

Cisco Unified CallManager Release 5.1 supports the following enterprise parameter changes:

- Advertise G.722 Codec—This parameter 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 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). For more information, see the "Phone Configuration—Product-Specific Configuration Changes" section on page 13.

Phone Configuration—Product-Specific Configuration Changes

The Product-Specific Configuration area of the Phone Configuration window supports a new parameter, Advertise G.722 Codec. Use this parameter to override the enterprise parameter (see Advertise G.722 Codec in the "Enterprise Parameter Changes" section on page 12) on an individual phone basis.

Use this parameter to override the enterprise parameter (see Advertise G.722 Codec in the "Enterprise Parameter Changes" section on page 1-1) on a per-phone basis

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 is to use the value specified in the enterprise parameter setting.

Table 3 indicates how the phone responds to the configuration options.

Table 3 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 are wideband codecs. For more information on wideband codec, see the "Wideband Codec" section on page 23.

How the Parameters Work With Regions

When you choose a G.711 or G.722 codec in Region Configuration you are choosing the bandwidth utilization. Choosing either of these codecs has the same affect. When you choose either G.711 or G.722, these codecs disallow selecting codecs that have a payload greater than 64kbps, 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 is ignored because G.722, G.711, AAC, and wideband are not allowed.

Additional Corporate Directory Support

The DirSync application performs the synchronization of data in the Cisco Unified CallManager database with the customer LDAP directory information. DirSync allows Cisco Unified CallManager to synchronize the data from more corporate directories than with previous releases. DirSync allows synchronization from 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 to the Cisco Unified CallManager database.

User Tips

When directory synchronization is enabled, Cisco Unified CallManager Administration cannot update any user information that is synchronized from the customer Corporate Directory.

For More Information

Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)

New and Changed Information for Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration includes the following enhancements:

- New CLI Commands and Command Options, page 14

New CLI Commands and Command Options

You now have the following new CLI commands and command options are available.

  - show ipsec status
  - show logins
  - show network max_ip_conntrack
  - show open
  - set commandcount
  - set network mtu
  - set network max_ip_conntrack
  - set network pmtud
  - unset network dns options
  - utils core
  - utils dbreplication
  - utils iothrottle
  - utils reset_ui_administrator_password
  - utils sftp
- After uploading a file to the TFTP server, you nust restart the TFTP service to access the file.

For more information

- *Cisco Unified Communications Operating System Administration Guide Release 5.1(1).*

New and Changed Information for Cisco Unified CallManager Features

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

Immediate Divert Enhancements

Legacy iDivert allows diversion of a call to the voice mailbox of the party that invokes the iDivert feature. Enhanced iDivert allows diversion of a call to either the voice mailbox of the party that invokes the iDivert feature or to the voice mailbox of the original called party.

You can divert inbound calls that are in the call offering, call on hold, or call active states. You can divert outbound calls in the call active or call hold states. The diverted party receives the greeting of the voice-messaging system of the party to whom the call gets diverted.

When enhanced iDivert mode is active for incoming calls, the user to whom a call is presented can invoke Immediate Divert to divert the call either to the user’s own voice mailbox or to the voice mailbox of the original called party. After the invoking user presses the iDivert softkey, a screen on the invoking user phone identifies both the original called party and the invoking user. The user selects one of the two names, and the call gets redirected to the voice mailbox of the selected party.

Cisco Unified CallManager Administration Configuration Tips

- Configure appropriate service parameters.
- Configure the iDivert softkey.
- If using hunt lists and line groups, refer to the Limitations and Restrictions section of the Immediate Divert chapter in the *Cisco Unified CallManager New and Changed Information Guide*.
- If using QSIG trunks, refer to the Limitations and Restrictions section of the Immediate Divert chapter in the *Cisco Unified CallManager New and Changed Information Guide.*

Service or Enterprise Parameter Changes

Immediate Divert includes the following new service parameters:

- Use Legacy Immediate Divert
- Allow QSIG During iDivert
- Immediate Divert User Response Timer

User Tips

Users can use iDivert to send an active, ringing, or on-hold call to their voice messaging system. Depending on the type of call and their phone configuration, users can also use iDivert to send the call to the voice-messaging system of another party.

- If a call originally gets sent to the phone of someone else, iDivert allows the user to redirect the call either to their voice messaging system or to the original called party voice messaging system. The system administrator must make this option available.
- If a call gets sent to the user directly (not transferred or forwarded to the user) or if the user phone does not support the described option, using iDivert redirects the call to the voice-messaging syster of the user.

See the Immediate Divert scenarios in the *Cisco Unified CallManager New and Changed Information Guide* for more information about using the enhanced Immediate Divert feature.

Cisco Unified IP Phone Support

- Cisco Unified IP Phone 7906G and 7911G (SCCP and SIP)
- Cisco Unified IP Phone 7961G/GE and 7941G/GE (SCCP and SIP)
- Cisco Unified IP Phone 7970G/7971G-GE (SCCP and SIP
- Cisco Unified IP Phone 7905G and 7912G (SCCP only)
- Cisco Unified IP Phone 7960G and 7940G (SCCP only)

Call Detail Records Considerations

Immediate Divert uses the Immediate Divert code number in the Onbehalf of fields (for example, joinOnbehalfOf and lastRedirectRediectOnBehalfOf) in CDR.

For More Information

- Immediate Divert, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- *Cisco Unified IP Phone User Guide For Your Phone*

Call Forward All Override

The Call Forward All Override feature allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. In other words, when the user to whom calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator), the phone of the initiator rings instead of call forwarding back to the target. The override works whether the CFA target phone number is internal or external.

When the CFA Destination Override service parameter is set to False (the default value), no override occurs. See Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide* for information about configuring service parameters.

Cisco Unified CallManager Administration Configuration Tips

Ensure the CFA Destination Override service parameter is set to True for CFA override to work. The default value specifies False.

Service or Enterprise Parameter Changes

The following new service parameters support Call Forward All Override:

- CFA Destination Override

Cisco Unified IP Phone Support

- 7971G and 7971GE
- 7970G
- 7961G and 7961GE
- 7960G
- 7941G and 7941GE
- 7940G
- 7911G
- 7906G

For More Information

- Understanding Directory Numbers, *Cisco Unified CallManager System Guide*
- Cisco Unified IP Phones, *Cisco Unified CallManager System Guide*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

AAC Voice Codec Support

The Advanced Audio Codec (AAC) feature provides the following capabilities:

- Advanced Audio Codec (AAC) specifies a wideband voice codec that provides improved voice fidelity and equal or better sound quality over older codecs.
- When configuring a region, use the wideband audio codec if you want to configure the AAC for calls between SIP phones. The Cisco Unified IP Phone 7900 series phone supports wideband, a high-quality, high-bandwidth audio codec for IP-phone to IP-phone calls.

Cisco Unified CallManager Administration Configuration Tips

- When configuring a region, use the wideband audio codec if you want to configure the AAC for calls between SIP phones.

CAR/CDR Considerations

- The table of the AAC codec types includes the table of supported codec types.

For More Information

- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Arabic Language (right to left) Support

Cisco Unified CallManager Release 5.1 supports Arabic locales on Cisco Unified CallManager user interfaces and Arabic text on phone screen displays for supported phones.

Cisco Unified IP Phones Supported

- 7906G and 7911G
- 7961G/GE and 7941G/GE
- 7970G/7971G-GE

For More Information

- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide*

New and Changed Information for Cisco Unified CallManager Applications

The following section describes the Cisco Unified CallManager 5.1 applications enhancements:

- Music on Hold, page 18
- DirSync Application Enhancements, page 18

Music on Hold

The Music On Hold feature now supports the new service parameter, Multicast MOH Direction Attribute for SIP.

- The Multicast MOH Direction Attribute for SIP service parameter determines whether Cisco Unified CallManager sets the direction attribute of the Session Description Protocol (SDP) in its multicast Music on Hold (MOH) INVITE message to sendOnly or recvOnly.
- If your deployment uses SIP phone loads 8.4 and earlier for Cisco Unified IP Phone 7940 and 7960, or SIP phone loads 8.1(x) and earlier for Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971, set this parameter to sendOnly. Otherwise, leave this parameter set to the default value, recvOnly.

For More Information

- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

DirSync Application Enhancements

The DirSync application performs the synchronization of data in the Cisco Unified CallManager database with the customer LDAP directory information. Cisco Unified CallManager administrators set up the DirSync service by first configuring the LDAP-directory-related Cisco Unified CallManager windows.

This release of Cisco Unified CallManager supports synchronization from more corporate directories than with previous releases. DirSync now allows Cisco Unified CallManager to synchronize the data from the following corporate directories to the Cisco Unified CallManager database:

- Microsoft Windows Server 2000 and Windows Server 2003 Active Directory (AD)
- Netscape/iPlanet Directory
- Sun ONE Directory Server 5.1
- Sun Java System Directory Server 5.2

For More Information

- Understanding the Directory, *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide.*

New and Changed Information for Cisco Unified CallManager Bulk Administration Features

Cisco Unified CallManager Bulk Administration (BAT), a web-based application, performs bulk transactions to the Cisco Unified CallManager database. This section introduces the changes to BAT for Cisco Unified CallManager Release 5.1.

- Updating the Region Matrix, page 19

Updating the Region Matrix

BAT now includes a new Region Matrix menu that allows you to populate or depopulate the region matrix. The region tables define physical locations, whereas the region matrix tables define available bandwidth within (intra) and between (inter) regions.

GUI Changes

Choose **Bulk Administration>Region Matrix>Populate/Depopulate Region Matrix** to update the Region Matrix.

For More Information

- *Cisco Unified CallManager Release 5.1(1) New and Changed Information Guide*

New and Changed Information for Cisco Unified CallManager Security Features

This section introduces the changes to security for Cisco Unified CallManager 5.1.

- CTL Client Modifications, page 19
- TFTP Exclude Digest Credentials Check Box Display, page 19
- Upgrading Cisco Unified IP Phones to Authenticate with LSCs Not MICs, page 20

CTL Client Modifications

You can now secure a Cisco PIX Firewall as part of a secure Cisco Unified CallManager system. To secure a firewall, configure the firewall, which acts as a TLS proxy server, in the CTL client. After the the firewall certificate gets added to the CTL client file, the firewall can inspect packets, detect threats, and perform NAT/Firewall transversal even on Cisco Unified CallManager systems with security enabled.

This release also adds CTL support for a Cisco Unified CallManager supercluster: sixteen call processing servers, one publisher, two TFTP servers, and up to nine media resource servers.

GUI Changes

The following changes to Cisco CTL client apply to secure firewall support:

- To configure a PIX firewall in the CTL client, click the Add Firewall button in the CTL Entries window. After you enter the Hostname or IP Address, Port, Username, Password, and press Next, the CTL client authenticates the proxy server with the username and password before adding its certificate to the CTL file.
- Cisco Unified CallManager Administration uses an etoken to authenticate the TLS connection between the Cisco CTL client and provider before sending the CTL file to the firewall server.
- The Cisco CTL client displays the firewall certificate as a “CCM” certificate

TFTP Exclude Digest Credentials Check Box Display

Only Cisco Unified IP SIP Phone 7905, 7912, 7940, and 7960 display the TFTP Exclude Digest Credentials in Configuration File check box in the phone security profile window. Only these phones fully support this option.

Use this option to exclude digest credentials from the configuration file that is sent to phones after the initial configuration. You may need to uncheck this check box to update the configuration file for changes to digest credentials.

Upgrading Cisco Unified IP Phones to Authenticate with LSCs Not MICs

Cisco supports LSCs to authenticate the TLS connection with Cisco Unified CallManager. Cisco recommends using manufacturer-installed certificates (MICs) for LSC installation only. Because MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.

Cisco recommends upgrading Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971 to use LSCs for TLS connection to Cisco Unified CallManager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues. Some phones that use MICs for TLS connection to Cisco Unified CallManager may not be able to register.

Administrators should remove the following MIC root certificates from the CallManager trust store:
CAP-RTP-001
CAP-RTP-002
Cisco_Manufacturing_CA
Cisco_Root_CA_2048

MIC root certificates that stay in the CAPF trust store get used for certificate upgrades. For information on updating the Cisco Unified CallManager trust store and managing certificates, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.1(1).*

For More Information

- Configuring the Cisco CTL Client, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Configuring Encrypted Phone Configuration Files, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- *Cisco Unified CallManager 5.1 TCP and UDP Port Usage*

New and Changed Information for Cisco Unified CallManager Serviceability

The following serviceability applications include updates for 5.1(1):

- Cisco Unified CallManager Serviceability Administration, page 20
- Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), page 21
- Cisco Unified CallManager Analysis and Reporting (CAR), page 22

Cisco Unified CallManager Serviceability Administration

The Cisco Unified CallManager Serviceability GUI allows you to perform such tasks as configuring trace parameters, configuring alarms, and activating, starting, and stopping services.

GUI Changes

The Cisco Unified CallManager Serviceability GUI contains the following enhancements for 5.1(1):

- The Troubleshooting Trace Setting window, which allows you to choose the services in Cisco Unified CallManager for which you want to set predetermined troubleshooting trace settings, contains the following updates:
  - The Server drop-down list box—Applies the troubleshooting trace settings to the server that you specify.
  - Check All Services check box—Automatically checks all check boxes for the services on the current node that you chose in the Server drop-down list box.
  - Check Selected Services on All Nodes check box—Allows you to check specific service check boxes in the Troubleshooting Trace Settings window. This setting applies for all nodes in the cluster where the service is activated.
  - Check All Services on All Nodes check box—Automatically checks all check boxes for all services for all nodes in the cluster. When you check this check box, the Check All Services and Check Selected Services on All Nodes check boxes automatically get checked.
  - Reset Troubleshooting Traces—Restores the original trace settings for the services on the node that you chose in the Server drop-down list box; also displays as an icon that you can click.
  - Reset Troubleshooting Traces On All Nodes—Restores the original trace settings for the services on all nodes in the cluster.

Serviceability Administration Configuration Tips

Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.

For More Information

- Troubleshooting Trace Settings Configuration, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Trace, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Cisco Unified CallManager Real-Time Monitoring Tool (RTMT)

Cisco Unified CallManager includes the following enhancements for 5.1(1):

- RTMT allows you to zoom in and zoom back out on the monitor of a predefined object. To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. To zoom out and reset the monitor to the initial default view, press the "**R**" key.
- RTMT contains a new counter. The ThreadsBusy counter represents the connector current number of busy/in-use request processing threads.
- The description for the Process Status counter value of 4 changed from traced to stopped.

For More Information

- Real-time Monitoring Configuration, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Performance Objects and Counters, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Cisco Unified CallManager Analysis and Reporting (CAR)

Cisco Unified CallManager Analysis and Reporting (CAR), which is an application that allows you to run reports for Quality of Service (QoS), traffic, billing information, and so on, includes the following enhancements for 5.1(1):

- When a logged-in Cisco Extension Mobility user makes a call, CAR uses the user ID that is configured for the Cisco Extension Mobility user in all reports that display a user ID. When the call is made by a non-Cisco Extension Mobility user (or logged-out Cisco Extension Mobility user) and when the call is made with a device that does not have a configured Owner User ID, CAR uses the default user ID, _unspecifieduser, in the report.
- In all CDR Search reports, the system only displays the oldest 100 records that fall into the time and date range that you configure.

CAR Configuration Tips

When you configure the time range for CDR Search, use Coordinated Universat Time (UTC). Likewise, when you configure the date and time range settings for CDR Search, configure the settings, so the number of CDR results do not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays that you must revise the settings.

For More Information

- CAR Report Results, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- CDR Analysis and Reporting Overview, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- CDR Search Configuration, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

New and Changed Information for Third-Party API

This following sections describe new features and changes that are pertinent to this release of Cisco Unified CallManager and third-party APIs.

- AXL Programming, page 22
- WebDialer Requirements, page 23

AXL Programming

AXL APIs

The following list provides AXL API calls that are new in 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 CallManager 5.0 release. Cisco recommends that you set this parameter to True, so Cisco Unified CallManager sends the valid namespace.

WebDialer Requirements

Cisco Unified CallManager Release 5.1 includes the following change to Cisco Unified CallManager WebDialer:

- WebDialer and Redirector now require HTTPS.

Developers should format Redirector and WebDialer 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)*
- WebDialer API Programmming, *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

New and Changed Information for Cisco Unified IP Phones

The following sections describe the enhancements for Cisco Unified IP Phones:

- Wideband Codec, page 23

Wideband Codec

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 64kbps, 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 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 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

For more information about the administration settings for wideband codecs, see the "Enterprise Parameter Changes" section on page 12 and the "Phone Configuration—Product-Specific Configuration Changes" section on page 13.

Caveats

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

Caveats describe unexpected behavior on a Cisco Unified 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(1) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

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

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

This section includes the following topics:

- Using Bug Toolkit, page 24
- Saving Bug Toolkit Queries, page 26

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

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

To use Bug Toolkit, follow this procedure.

Procedure

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

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

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

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

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

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

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

a. Choose the Cisco Unified CallManager version:

- Choose the major version for the major releases (such as, 5.1, 5.0, 4.1, 4.0).

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information; for example, choosing major version 5.0 and revision version 3 queries for release 5.0(2) caveats.

  A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

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

- To query for all Cisco Unified CallManager caveats for a specified release, choose “All Features” in the left window pane.

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

- To query only for Cisco Unified CallManager-related caveats, choose “ciscocm” and then click **Add**.
- To query only for phone caveats, choose “ciscocm-phone” and then click **Add.**
- To query only for gateway caveats, choose “voice-gateway” and then click **Add**.

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

Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

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

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the **Fixed** check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

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

- You can modify your results by submitting another query and using different criteria.
- You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 26.

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

Saving Bug Toolkit Queries

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

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 24.

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

A new window displays.

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

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

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

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

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

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

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

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

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

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

Open Caveats

Table 4 describes possible unexpected behaviors in Cisco Unified CallManager Release 5.1(1), which are sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 4 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)
- 004.000(000.123) = Cisco Unified CallManager release 4.0(1)
- 004.000(001.008) = Cisco Unified CallManager release 4.0(2)
- 004.001(002.201) = Cisco Unified CallManager release 4.1(3)

Note Because defect status continually changes, be aware that Table 4 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the “Using Bug Toolkit” section on page 24.

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 4 Open Caveats

Identifier	Headline
Component: Alarm Library	
CSCsg98061	cdr-agent core dump
Component: Attendant Console	
CSCsg74177	Attendant Console cannot route calls to a phone in another Cisco Unified CallManager in the same cluster.
CSCsg97024	When you open Attendant Console, call control takes 20-30 seconds to display.
Component: Broadband Provisioning Solutions (BPS) Bulk Administration Tool (BAT)	
CSCsg64288	BAT does not insert users or phones.
Component: Call Processing	
CSCsf27901	CallCoverage: QSIG Disconnect message does not get sent when parties use MeetMe conference and iDivert.
CSCsf31295	CallCoverage: iDivert: When iDivert is used on a Cisco Unified IP 7961 SIP phone, the phone displays the same name for options 1 and 2.
CSCsg20423	CallCoverage: iDivert: When iDivert was placed for a call on hold, phone displays same name for options 1 and 2.
CSCsg57421	Change Notify: When the region configuration is changed to use the system default, audio codec from a specified codec continues to use specified codec after region is reset.
CSCsg89252	After a VPN network outage, the incorrect status gets displayed.
CSCsg31011	H323: Connected Number IE support needs to be in H225 CONNECT message.
CSCsb99980	Media Control: Cisco Unified CallManager inserts Media Termination Points (MTP) for DTMF due to Music on Hold (MOH) connection.
CSCsf13956	Media Control: Cisco Unified CallManager should wait for CLCs before sending TCS after ECS is triggered by SIP.
CSCsg21311	Media Control: SIP video: issue with consult transfer call over SIP Integration Configuration Tool (ICT) and H323 ICT.
CSCsg29976	Media Control: Video RSVP call to Cisco Unified Presence Communicator end point takes three RSVP resources.
CSCsg31775	Media Control: Third party issue: No Remote video exists on SIP polycom.
CSCsg35113	Media Control: Third Party Issue: SIP Cisco Unified Presence Client (CUPC) to SIP Polycom calls - No remote video exists for CUPC.
CSCsg35857	Media Control: Cisco Unified Video Advantage (CUVA) to H.323 via H.323 ICT - Calls disconnect on answer.
CSCsg38154	Media Control: Cisco Unified Video Advantage (CUVA) to H.323 Polycom EP via H.323 Itegration Configuration Tool (ICT) - Calls disconnect on pickup.
CSCsg42281	Media Control: Video H323 to SIP Multipoint Control Unit (MCU) interworking shows one-way video.
CSCsg50860	Media Control: No remote video occurs for the Cisco Unified IP Phone 7985 on SCCP Cisco Unified IP Phone 7985 to H323 calls via SIP ICT.

Table 4 Open Caveats (continued)

CSCsg56183	Media Control: For SIP to GK-controlled H225 trunk call with "BRQ enabled", if H323 device does not send incoming video OLC in time, Cisco Unified CallManager will not send BRQ to GK and just send out outgoing video OLC.
CSCsg59490	Media Control: No remote video occurs on hairpin connections via combinations of H323 and SIP ICTs.
CSCsg64206	Media Control: For CUVA calls of Cisco Unified Presence Communicator over H323 ICT, audio region specifies g711. H.264 gets negotiated initially for the call. After CUVA hold, resume H.263 gets used for the call.
CSCsg64332	Media Control: Video related performance counters do not get updated.
CSCsg71384	Media Control: No remote video occurs on both Cisco Unified Presence Communicator and CUVA.
CSCsg79193	Media Control: CUPC video call does not provide remote video.
CSCsg80611	Media Control: When CUPC calls another CUPC over H.323 ICT for video escalation, the call does not get completed.
CSCsg84039	Media Control: When CUPC calls another CUPC over H.323 ICT for video escalation, the call does not get completed.
CSCsg86643	Media Control: Video escalation request from CUPC gets rejected.
CSCsg97059	Media Control: H323 makes a call to CUVA over SIP ICT, one way video; however CUVA does not see the video.
CSCsg09245	Media Gateway Control Protocol (MGCP): Cisco Unified CallManager-MGCP IB BRI call disconnects with circuit/channel not available cause code.
CSCsg66279	MLPP: Intermittent calls get dropped with dead air from PSTN via MGCP-controlled FXO ports as MGCP gateway sends 516 Wrong Call ID.
CSCsd57244	Q Signaling (QSIG): Call Diversion by reroute does not kick off if not enough bandwidth exists in RSVP Location.
CSCsg05163	Q Signaling (QSIG): Cisco Unified CallManager does not display the MGCP/QSIG User name or the alerting name in the Association Control Service Element.
CSCsg60636	Q Signaling (QSIG): RTMT counters do not work properly for H225 trunk.
CSCsg88249	Resource Reservation Protocol (RSVP) Agent: Set tryPassThru to true if you do not have caps from both parites.
CSCsf25167	Session Initiation Protocol (SIP): SIPT needs PRACK on 18X (early media) to support ring-back tone
CSCsf04195	SCCP: Assistant-on-phone: If the default language is not English, the login does not complete.
CSCsg39825	Session Initiation Protocol (SIP): Cisco Unified CallManager calls to registered SIP phones get immediate reorder DMPidErr message
CSCsg73112	Session Initiation Protocol (SIP): SIP TNP phone may register with Cisco Unified CallManager by using TLS even if the cluster is in nonsecure mode under certain conditions.
CSCsg75127	Session Initiation Protocol (SIP): SIP calls via MGCP-controlled voice gateways may fail under extended load.
CSCsg92831	Incorrect caller ID gets displayed on CUPC after a video call is transferred to CUPC.
CSCsd50352	System: Very slow device reset speed on large clusters degrades performance.

Table 4 Open Caveats (continued)

CSCsg98070	System: When asynchronous logging is enabled, the async thread and router thread wait for each other.
Component: CAR	
CSCsg76135	CAR reports and change notification do not get generated.
Component: Cisco Unified CallManager Assistant	
CSCsg43698	Several issues exist with the Cisco Unified CallManager Assistant softkeys or text messages in the French localization of Cisco Unified CallManager Assistant.
Component: Computer Telephony Integration (CTI)	
CSCsd85136	When the CTIOS server gets cycled, call disappear.
CSCsg27220	Wrong locale information exists in call-forwarding scenarios that are related to unicode.
CSCsg27814	DTMF digits that are entered from Microsoft Office do not get recognized.
CSCsg94671	If a transfer or conference end event is received on a line after the call is cleared, the event will be received with a 0 CI. This will cause the TxEnd or ConfEnd to be sent to all the lines in that device.
Components: Cisco Customer Performance Indicators (CPI) Appinstall	
CSCsf27257	Cisco Unified CallManager installation should not allow hard coding of NIC speed to 1000BaseT.
CSCsg76775	Install fails with certain logic.
Component: Cisco Customer Performance Indicators (CPI) Data Migration Assistant (DMA)	
CSCsg92930	The DMA backup page does not get refreshed automatically so the user has to close the page and reopen it manually to get the page refreshed.
Component: Cisco CustomerPerformance Indicators (CPI) OS	
CSCsg75347	Cisco Unified CallManager sends out a Code Yellow Entry Alarm and Alert and throttles new calls unexpectedly. At the time of this Code Yellow event, CPU seems to spike and spends most time in IOWait state.
CSCsg77021	In Show > Cluster double publisher displays.
CSCsg91146	ST: hpasmd running high CPU.
CSCsg95989	Installation does not get completed on servers with dual CPUs.
Component: Cisco CustomerPerformance Indicators (CPI) Security	
CSCsg80593	MD5 does not get used in phase 2 in IPSEC on Cisco Unified CallManager.
CSCsg82160	The Tomcat web certificate that gets created during installation includes on the hostname, not the fully qualified domain name (FQCN).
Component: Cisco Customer Performance Indicators (CPI)	
CSCse49089	Certificate Management: IPSec validation generates error across clusters if UDP protocol is selected.
CSCsf05359	Certificate Management: Email notification does not get sent for certificates for Cisco Unified CallManager and CAPF.
CSCsf09804	Data Migration Assistant (DMA): Installation fails if not enough hard drive space exists.

Table 4 Open Caveats (continued)

CSCsf24390	Data Migration Assistant (DMA): Error message displays when DMA is installed after deleting a previous version.
CSCsg23117	Data Migration Assistant (DMA): DMA failed to back up.
CSCse43150	Operating System (OS): Uploading core dump and crace files from the real-time monitoring tool causes the system to generate high CPU usage.
CSCse83975	Operating System (OS): Password recovery needs to inform the database of the change.
CSCsg21296	Operating System (OS): IPT platform needs to actively monitor to detect and log duplicate IP addresses.
CSCsg23526	SNMP monitoring of ServeRAID RAID drives fails to report any problems when ServeRAID fails after a Cisco Unified CallManager upgrade.
CSCsg34717	User Interface (UI): User cannot delete remote support account from CLI or from the user interface.
Component: Database	
CSCsb71648	Database migration takes an excessive amount of time when you upgrade from Cisco Unified CallManager, version 4.1(3).
CSCsd63802	Replication state counter stopped on one subscriber after upgrade.
CSCse09426	Need to improve speed of inserting phones into the database exists.
CSCse21733	A ccmAgent core dump occurs upon database shutdown after Cisco Unified CallManager upgrade.
CSCsf05536	Update of statistics needs to continue during error.
CSCsg07605	Disaster recovery system backup makes Cisco Unified CallManager database read only.
CSCsg60389	When the user tries to delete a Route List, the list does not get deleted.
CSCsg70432	CUOS Admin CLI utils: Database replication reset does not start on all nodes.
CSCsg73474	When the user tries to log in to Extension Mobility, the log in fails with an Error 6 Database failure.
CSCsg89319	Extension mobility login fails.
Component: Database Administration	
CSCsg49046	When the Automatic Configuration option is checked on the Cisco Unified CallManager Assistant User Configuration window, submitting the page will fail if the user associated phone has two domain names that are the same, but in different partitions.
CSCsg97738	When an EM user is logged in, another user cannot save any changes in Device > Phone.
CSCsg99466	Phones allow user to subscribe to the same service multiple times.
Component: Java Telephony API (JTAPI) Software Development Toolkit (SDK)	
CSCsg03945	CiscoJTAPIClient-linux.bin fails to install.
Component: Licensing	
CSCse82038	Licensing files that are written to /tmp cause 100 percent disk usage in active partition.

Table 4 Open Caveats (continued)

CSCsg70752	ATA186 should take up 1 DLU; currently, it takes up 2 DLUs.
Component: Rootless	
CSCse65206	Creates wrong VIC when configuring an EVM-HD card on a gateway.
Component: Real-Time Monitoring Tool (RTMT)	
CSCse19328	When any UNC path is selected as the "Look In" location, no subfolders or other files display. Saving log files to the root directory represents the only option.
CSCsg70442	The RTMT Server Process Summary does not show thread information.
Component: Security	
CSCsg99442	Cluster security mode changes to 0 in the enterprise parameter when the user selects "set to default" in enterprise parameter.
Component: Telephony API (TAPI) Software Development Toolkit (SDK)	
CSCsb64096	TAPI application stops during RecordWave with Silence operation.
CSCsg23468	Latency exists on PlayWave on TSP 5.1.1.1 after client reboot.
CSCsg23990	TSP svchost pegging occurs at 99 percent CPU during TLS connection.
Component: TFTP	
CSCsg73432	CTFTP crashes when Cisco Unified CallManager gets configured in secure mode.
CSCsg93169	Call processing and TFTP are using two sets of line numbering mechanisims.
Component: Webdialer Service	
CSCse38991	Need exists to resolve static analysis tasks.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco Unified CallManager release 5.1(1) documentation suite was released.

Omissions

This section provides information that was not included in the Cisco Unified CallManager release 5.1(1) documentation.

- Searching for a Device in RTMT with the Any Status Option, page 32
- Planning Your Software MTP Configuration, page 33
- Ad Hoc Conference Settings Restrictions for SIP Phones, page 33

Searching for a Device in RTMT with the Any Status Option

The Real-time Monitoring Tool chapter of the *Cisco Unified CallManager Serviceability System Guide* does not include the following information.

When you search for a device by choosing the any status option, RTMT does not display a snapshot of the matched device type, but rather it displays data for that device type from the RIS database for all specified Cisco Unified CallManager nodes for a period of time. As a result, you may see multiple entries of a device with multiple status (Registered, Unregistered, etc.) in RTMT. When you see multiple entries of a device, the current status of the device is the entry that has the latest timestamp. You can configure the period of time that information on unregistered or rejected device is kept in the RIS database by configuring the RIS Unused Cisco CallManager Device Store Period service parameter in Cisco RIS Data Collector service in Cisco Unified CallManager Administration. For more information on configuring service parameter, refer to the *Cisco Unified CallManager Administration Guide*.

Planning Your Software MTP Configuration

The following information is missing from the *Cisco Unified CallManager System Guide*, Media Termination Points chapter.

Consider the following information when you are planning your MTP configuration:

- To optimize performance of DTMF signaling, use Cisco IOS release 12.4(11)T or later. This Cisco IOS release supports RFC 2833 DTMF MTP Passthrough of digits.

Ad Hoc Conference Settings Restrictions for SIP Phones

The Conferencing chapter of the *Cisco Unified CallManager System Guide* does not include the following information.

Even though Cisco SIP IP Phones (7911, 7941, 7961, 7970, 7971) can create an ad hoc conference, Cisco SIP IP Phone 7940/60 and third-party SIP phones can only be participants.

The following restrictions apply to all SIP phones when using ad hoc conferencing:

- Cisco Unified CallManager uses “beep” and “beep beep” tones when a new party is added, and when the new party drops from the ad hoc conference, respectively. When a party is added to an ad hoc conference, a user on a SIP Phone may or may not hear the beep; when a participant drops from the ad hoc conference, a user on a SIP Phone may not hear the beep beep. The beeps may not be heard because of the time it takes to re-establish connections for the conference.

Updates

This section provides information that has been updated since the release of the Cisco Unified CallManager release 5.1(1) documentation.

- Name Change, page 33

Name Change

Cisco Unified CallManager Analysis and Reporting Guide, Release 5.0(4), refers to Cisco IP Manager Assistant (IPMA) instead of Cisco Unified CallManager Assistant. For each instance of Cisco IP Manager Assistant (IPMA) in this guide, replace it with Cisco Unified CallManager Assistant. To run reports for Cisco Unified CallManager Assistant in Cisco Unified CallManager Analysis and Reporting (CAR), choose **User Reports > Cisco Unified CallManager Assistant > Manager Call Usage** (or **Assistant Call Usage**). For additional information on running these reports, refer to *Cisco Unified CallManager Analysis and Reporting Guide, Release 5.0(4)*.

Corrections

This section lists corrected information that the current version of the Cisco Unified CallManager documentation may not include:

- Servers That Support Cisco Unified CallManager 5.0(3), page 34
- Cisco Emergency Responder 1.3(1a), page 34

Servers That Support Cisco Unified CallManager 5.0(3)

The document, *Installing Cisco Unified CallManager 5.0(3)* does not provide a complete list of servers that support Cisco Unified CallManager 5.0(3). For a list of servers that support Cisco Unified CallManager 5.0 releases, click the following URL:

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/

Cisco Emergency Responder 1.3(1a)

Cisco Emergency Responder (Cisco ER) 1.3(1a) supports Cisco Unified CallManager 5.0(2) and 5.0(3) in addition to Cisco Unified CallManager 3.3 and Cisco Unified CallManager 4.0, 4.1, and 4.2.

Note Cisco Unified CallManager 5.0(1) does not get supported with Cisco Emergency Responder 1.3(1a)

- Ensure all Cisco ER servers are version 1.3(1a). This allows Cisco ER to support multiple Cisco Unified CallManager 5.0(2) or 5.0(3) clusters. Cisco ER 1.3(1a) will not work with previous versions of Cisco ER.
- Cisco ER 1.3(1a) supports upgrades from Cisco ER 1.2(1), Cisco ER 1.2(2), and Cisco ER 1.2(3).
- Cisco ER 1.3(1a) provides Windows-based support.

Changes

Updated Voice Gateway Model Information

The Understanding Cisco Unified Voice Gateways chapter in the *Cisco Unified CallManager Release 5.1(1) New and Changed Information Guide* contains updated information on the supported voice gateways, protocols, trunk interfaces, and port types.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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

Documentation Feedback

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

Cisco Product Security Overview

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

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

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

- Report security vulnerabilities in Cisco products

- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For nonemergencies—psirt@cisco.com

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

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

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

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

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

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

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Support Website

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

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

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

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

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

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

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