Release Notes for Cisco Unified CallManager Release 5.1(2b)

August 2, 2007

These release notes describe the new features, resolved caveats and open caveats for Cisco Unified CallManager Release 5.1(2b).

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 5.1(2b), 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(2b). 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(2b), 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(2b) on a Cisco Media Convergence Server (MCS) appliance.

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(2b) requires a minimum of the following items on the Cisco MCS appliance:

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

Note 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(2b) 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 documentation that supports Cisco Unified CallManager Release 5.1(2b) comprises existing release 5.0(4) documentation that is listed in the *Cisco Unified CallManager Release 5.1(2) Documentation Guide*, as well as the following release 5.1(x) documents:

- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- *Release Notes for Cisco Unified CallManager Release 5.1(2a)*
- *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*
- *Release Notes for Cisco Unified CallManager Release 5.1(1)*

Limitations and Restrictions

A list of compatible software releases represents a major deliverable of Cisco Unified Communications 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(2b). 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(x).

Important Notes for Cisco Unified CallManager Release 5.1(2b)

- HP NC-Series Broadcom Firmware Updates Available for Supported NICs., page 5
- Additional Servers Supported, page 16
- iLO Firmware on MCS-7825-H1, MCS-7835-H1 and MCS-7845-H1, page 5
- Smart Array 6i Requires HD Firmware Update to Avoid POST Notification, page 5
- Smart Array 5i Requires HD Firmware Update to Avoid POST Notification, page 6
- MCS-7825H2-IPC1 Reboots Randomly, page 6

Important Notes for Cisco Unified CallManager Releases 5.1(1) through 5.1(2a)

- CSCsg97059 SIP and H323 Third-Party Device, page 7
- CSCsc81681 Complex Database Causes Extension Mobility Performance Degradation, page 7
- Disaster Recovery Restore Attempt on a Publisher Node Fails with an Error on the Cisco Unified CallManager Database Component, page 7
- Music On Hold (MOH) Source Files, page 8
- Configuring Fixed Music on Hold by Using the Cisco USB MOH Adaptor, page 8
- Verify Adequate Disk Space Prior to Installation/Upgrade, page 9
- CSCsi52140 Extension Mobility Impacts Upgrades from Cisco Unified CallManager Release 4.1(x) to Cisco Unified CallManager Release 5.1(x) or from Cisco Unified CallManager 5.x to Cisco Unified CallManager Release 6.x, page 9
- Online Help for Cisco Unified CallManager Release 5.1(2x), page 9
- CSCsh58558 BIOS Flash Not Forced, page 9
- CSCsh50712 IBM 7835I2 Server BIOS Flash Files Corrupt, page 9
- CSCsh50685 IBM BIOS MTM Change, page 10
- CSCsh20023 Some Browsers and WinZip, page 10
- CSCsh50754 Do Not Install Cisco Unified CallManager Release 5.1(1) or 5.1(1a) on Hewlett-Packard 7835H2 or 7845H2 Servers, page 11
- Upgrading from Cisco Unified CallManager Release 5.0(4) to Release 5.1(x), page 11
- MTP and Cisco Unified IP Phones That Are Using SIP, page 11
- Rebuilding Failed RAID Drives, page 12

- Cisco Unified Communications Answer File Generator, page 13
- Using SIP Trunks Between Release 4.x and 5.x Systems, page 14
- Configuring Phones That are Running SIP with the Same Directory Number, page 15

HP NC-Series Broadcom Firmware Updates Available for Supported NICs.

The upgrade includes

- iSCSI and UMP firmware upgrade support.
- An IPMI configuration command that allows IPMI to be enabled or disabled from the command line.

You can update firmware manually by downloading and booting from the HP Firmware Maintenance CD version 7.80 (10 May 07) that is located at
http://h18023.www1.hp.com/support/files/server/us/download/27225.html

iLO Firmware on MCS-7825-H1, MCS-7835-H1 and MCS-7845-H1

iLO firmware on MCS-7825H1, MCS-7835H1, and MCS-7845H1platforms may include versions older than version 1.82. The firmware update, version 1.82, contains critical bug fixes and is the minimum version required. The current released version is 1.84.

Workaround

Download the firmware update from the Hewlett-Packard site and apply them manually.

MCS-7825-H1
http://h18023.www1.hp.com/support/files/server/us/family/model/6053.html?submit.y=9&submit.x=11&lang=en&cc=us

MCS-7835-H1 and 7845-H1
http://h18000.www1.hp.com/support/files/server/us/family/model/5561.html?lang=en&cc=us

Smart Array 6i Requires HD Firmware Update to Avoid POST Notification

You should upgrade hard drive models that experience excessive SCSI command timeout . Failure to upgrade may result in the bus down-shifting from Ultra 320 to Ultra 3.

Upgrade following hard disk models to the specified versions:

Table 2 Recommended Firmware Upgrades

Hard Disk Model	Upgrade to
BF018863B8, BF036863B9, BF072863BA	HPB6 B (4 Jan 07
BD146863B3, BD072863B2, BD036863AC, BD03697633	HPB8 B (4 Jan 07
BD14686225, BD07286224, BD03686223, BD07296B44, BD03695CC8	HPB6 E (4 Jan 07)

Table 2 Recommended Firmware Upgrades

Hard Disk Model	Upgrade to
BD009635CB, BD00973623, BD018635CC, BD01873624, BD03663622, BD03673625, BC072638A2	BDCB D (4 Jan 07)
BD01865CC4, BD01875CC7, BD00965CC3, BD00975CC6, BD00415CBC, BD00425CC2	HPB6 D (4 Jan 07)
BD0096349A, BD009734A3, BD0186349B, BD018734A4	3B15 D (4 Jan 07)
BD00962A66, BD00972A69, BD01862A67, BD01872A6A	B008 D (4 Jan 07)
BD00962373 BD00972374 BD01862376 BD01872377 and BC0367237A	BCJG D (4 Jan 07)
BD00912578 and BD01812579	BCJG D (18 Jan 07)
AD01836222, AD00935CCC, AD00435CCB	HPA6 C (16 Jan 07)
AD00933626 and AD01833627 drives version	ADCB D (4 Jan 07)
AD00932372 AD01832375 and AC03632378	ACJG D (4 Jan 07)

Workaround

You can update firmware manually by downloading and booting from the HP Firmware Maintenance CD version 7.80 (10 May 07) that is located at
http://h18023.www1.hp.com/support/files/server/us/download/27225.html

Smart Array 5i Requires HD Firmware Update to Avoid POST Notification

Smart Array 5i version 2.66 recommends updates for some SCSI disk drive models after the Smart Array firmware gets installed.

Workaround

You can download updates and apply them manually. Find information concerning specific hard drive models and the location of firmware updates at
ftp://ftp.compaq.com/pub/softlib2/software1/doc/p1821026293/v33269/266-5i_532.pdf

MCS-7825H2-IPC1 Reboots Randomly

Sporadic reboots of the 7825H2 servers get triggered during long system hangs. ASR functionality autorecovers the servers after 10 minutes of kernel unresponsiveness. Event timing ranges from once every 3 months to once every 3 days.

Workaround

A partial workaround is available with the ciscocm.disable-hpasm.cop.sgn package. Contact Cisco TAC to acquire the workaround.

CSCsg97059 SIP and H323 Third-Party Device

Calls on Cisco Unified CallManager Release 5.x(x) that involve both SIP and H323 third-party device may experience one-way video or no video because of dynamic payload type problems. At this time, no workaround exists.

CSCsc81681 Complex Database Causes Extension Mobility Performance Degradation

Symptom

When you initiate a login from a phone, the database requests a change notify. The phone configuration window changes, and the Extension Mobility login perfmon counter gets updated.

After the RTMT EM perfmon counter and phone configuration window both validate a successful EM login, it can take up to 60 minutes to see the change on the phone.

After you log in, if you see that the phone screen did not change, you can press the service button, and the interface will ask you to log out even though the phone login did not complete.

Cause

The system introduces the EM logins/logouts to Cisco Unified CallManager at a faster rate than it can respond. Cisco Unified CallManager does not reset the phone quickly enough, so the queue to reset the phone backs up when too many change notifications reach the Cisco Unified CallManager.

In the series of events during a login, **phone reset change notify** gets lower priority in the queue of change requests; so the phone reset change notify requests build up a backlog of queued requests. This backlog, in the event of a stress performance test, creates a huge lag time.

Disaster Recovery Restore Attempt on a Publisher Node Fails with an Error on the Cisco Unified CallManager Database Component

When you attempt to restore the publisher node or database to a previously saved version by using DRS and the restore fails, look at the DRS logs on the Cisco Unified CallManager database component. You will see the following information:

> CCMDB Restore failed, installdb failed
>
> 425: Database is currently opened by another user.

Perform the following steps to complete the restoration.

Step 1 Stop the dbmon on all the subscriber servers.

```
admin:utils service list
Requesting service status, please wait...
...
Cisco Database Layer Monitor[STOPPED]
...

admin::59 pts/0    00:00:00 grep dbmon
```

Step 2 After DRF restore on the publisher server completes, restart the dbmon service.

```
admin:utils service list
```

```
Requesting service status, please wait...
...
Cisco Database Layer Monitor[STARTED]
...

admin:
```

Music On Hold (MOH) Source Files

Music audio source files must comprise .wav files in one of the following formats:

- 16-bit PCM (stereo or mono) (16 kHz or 32 kHz or 48 kHz or 8 kHz or 44.1 kHz sample rate)
- 8-bit CCITT g.711 a-law/mu-law (stereo or mono) (8 kHz sample rate)

Configuring Fixed Music on Hold by Using the Cisco USB MOH Adaptor

The fixed music on hold audio source gives you a way to use a custom audio source (that is, radio, mp3 player) as the music on hold audio source.

To do this, ensure each MOH server is provisioned with a Cisco USB MOH adaptor.

Installing the Adaptor

Step 1 Plug the adaptor USB cable into a USB port on the back of the MOH server.

Step 2 Connect an audio source to the adaptor MIC connection by using a patch cable with a mini-plug. Use the MIC connector that is labeled on the adaptor.

Step 3 If the LED on the adaptor is not lit red, press the REC button on the MOH USB adaptor.

Note You cannot hear the audio from the MOH USB headphone jack.

Step 4 Repeat Step 1 through Step 3 for each MOH server.

Step 5 From Cisco Unified CallManager Administration, click **Media Resources > Fixed MOH Audio Source**.

The Fixed MOH Audio Source Configuration window displays. The system assigns the Source ID.

Step 6 In the name box, enter a name for the fixed source audio that you recorded.

Step 7 Check the **Enable** check box.

Step 8 Click **Save**.

Step 9 Configure phones to use the MOH audio source that you recorded by putting the Source ID that was assigned in Step 5 on an individual phone or system-wide as a Cisco Unified CallManager service parameter.

Verify Adequate Disk Space Prior to Installation/Upgrade

To avoid problems, you should verify that adequate disk space exists on the common partition prior to initiating an upgrade.

Use the following criteria to determine how much space will be required:

- If this is the first upgrade, you will need three times the size of patch file (for downloading and unpacking) plus the CAR DB (2G).
- If this is a subsequent upgrade, you will need three times the size of patch file (for downloading and unpacking).
- If this is a COP file installation, you will need the size of the COP file plus the size of the unpacked COP file.

Note Performing this manual verification prior to starting an upgrade will keep you from discovering that inadequate space exists to complete the upgrade after you invest the time to download the patch file.

CSCsi52140 Extension Mobility Impacts Upgrades from Cisco Unified CallManager Release 4.1(x) to Cisco Unified CallManager Release 5.1(x) or from Cisco Unified CallManager 5.x to Cisco Unified CallManager Release 6.x

Ensure that users are not logged in to their phones during an upgrade from Cisco Unified CallManager Release 4.1(x) to Cisco Unified CallManager 5.1(x). Phones that users are logged in to during the upgrade will not function properly.

Phones that are at their default profile during an upgrade will function properly

Online Help for Cisco Unified CallManager Release 5.1(2x)

Because these release notes comprise the only updated documentation for Cisco Unified CallManager Release 5.1(2x), the online help version specifies 5.0(4).

CSCsh58558 BIOS Flash Not Forced

Hewlett-Packard servers forced the BIOS flash during a fresh install if the BIOS version on the server did not match the Cisco Unified CallManager image version. Changes ensure that the BIOS does not get flashed when the server has a later (newer) BIOS than exists on the Cisco Unified CallManager release.

CSCsh50712 IBM 7835I2 Server BIOS Flash Files Corrupt

On the Cisco MCS 783512 Unified CallManager appliance, in the case of a fresh software-only installation, if the server that was purchased from IBM has a newer BIOS version than the one that is bundled in Cisco Unified CallManager, the installation will fail.

CSCsh50685 IBM BIOS MTM Change

Be aware that software-only IBM servers (including 7815I2, 7825I2-2800, 7825I2-3400, 7835I1, 7835I2, 7845I1) that were purchased after IBM rolled out their Xcellator ordering process are impacted, and the installation of Cisco Unified CallManager Release 5.1(1) will fail.

Workaround

Upgrade to Cisco Unified CallManager 5.1(1b) or later, or

Manually change MTM strings with help from IBM field support by using these steps:

Step 1 Find the server type and model from the label on the shipping box, or by pressing **F1** to boot into the BIOS setup utility when the system comes up.

Step 2 Use Table 3 to find current MTM of your server and determine how it should be changed.

Step 3 Contact IBM field support to manually change the MTM on your servers. After the IBM field support changes the MTM strings, the system will recognize your server and, Cisco Unified CallManager Release 5.1(x) will support it.

Table 3 MTM Strings to Change on New AC1 Models

Description	Original MTM	Change MTM Back To
7815-I2 x206m, 1yr.	8485AC1	84857AU
MCS-7815-I2, x206m, 3yr	8490AC1	84907AU
MCS-7825-I2-2800, x306m (P920), 1yr	8849AC1	8849G2U 1
MCS-7825-I2-2800, x306m (P920), 3yr	8491AC1	8491G2U
MCS-7825-I2-3400, x306m (P950), 1yr	8849AC1	8849K2U
MCS-7825-I2-3400, x306m (P950), 3yr	8491AC1	8491K2U
MCS-7835-I1, x346 (RoHS), single CPU	8840AC1	88403RU
MCS-7845-I1, x346 (RoHS), dual CPU	8840AC1	88403RU
MCS-7835-I2, x3650, single CPU	7979AC1	79795AU

CSCsh20023 Some Browsers and WinZip

When the Cisco Unified CallManager upgrade patch file is downloaded from cisco.com, some browsers may download files with the extension **tar.gz.sgn** as **tar.gz.gz**.

Workaround

After the patch file is downloaded, rename it with the extension **.gz.sgn** (in place of.gz.gz) and proceed with the install.

CSCsh50754 Do Not Install Cisco Unified CallManager Release 5.1(1) or 5.1(1a) on Hewlett-Packard 7835H2 or 7845H2 Servers

If you install Cisco Unified CallManager Release 5.1(1) or 5.1(1a) on Hewlett-Packard 7835H2 or 7845H2 Windmill server, the server will become nonbootable.

Workaround

Do not install Cisco Unified CallManager Release 5.1(1) or 5.1(1a) on the new servers. You must install Cisco Unified CallManager Release 5.1(1b) or later instead.

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

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 fail over 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, follow standard best practices while you are performing a Cisco Unified CallManager upgrade.

MTP and Cisco Unified IP Phones That Are Using SIP

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 IP Phones (7905, 7912, 7940, 7960) that are using SIP 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 IP Phone 7940 that is using SIP, 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.

Caution Cisco Unified CallManager 5.0 and later provides an "MTP Required" check box for Cisco Unified IP Phones that are using SIP, but you **should not** check this check box for Cisco Unified IP Phones that are using SIP.

If you check the “MTP Required” check box, 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 IP Phones that are using SIP.

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

Rebuilding Failed 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 7825, 7835, and 7845 Unified CallManager Appliances.

Note Disaster Recovery represents the only supported method of backing up and replicating a server configuration. Do not use the method that is documented here to backup or replicate a good mirrored drive. Use t his procedure only to rebuild a failed drive, after the system has already detected that one of the drives failed.

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:

Step 1 Log in to the 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*.

Step 2 Power off the server (press power off button).

Step 3 Extract the failed disk drive.

Step 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 display 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

Step 5 After the login prompt displays 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.

Step 6 Insert the failed disk drive into the original slot; be sure to lock it properly in place.

Step 7 Check the status of the RAID array by using the CLI **show hardware** command; the Status field will read Rebuilding or Critical.

Step 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(2x) 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/index.html

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):

Procedure

Step 1 Insert the USB key into a USB slot on the Windows XP PC.

Step 2 Choose **Start** > **Control Panel** > **Administrative Tools** and then double-click Computer Management.

Step 3 Expand the Storage tree and click Disk Management.

Step 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**.

Step 5 Click the File System: pull down and select **FAT32**.

Step 6 Click **OK**. When prompted to format the volume, click **OK** again.

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

Table 4 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 4.)

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 Phones That are Running SIP with the Same Directory Number

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

New and Changed Information for Cisco Unified CallManager Release 5.1(2b)

The following section contains information about the new features that the Cisco Unified CallManager Release 5.1(2b) contains.

- Additional Servers Supported, page 16
- 2007 Daylight Saving Time Adjustment for New Zealand, page 16

Additional Servers Supported

This release of Cisco Unified CallManager includes support for four additional servers. The servers are MCS-7816H3, MCS-7816I3, MCS-7825H3 and MCS-7825I3.

2007 Daylight Saving Time Adjustment for New Zealand

As announced in New Zealand, beginning this year, daylight saving time (DST) starts on the last Sunday in September and will end on the following first Sunday in April.

Cisco incorporated changes into this release, so the new DST implementation will correctly occur on September 30th, 2007 and will end on April 6th, 2008.

Warning **Any systems that do not get updated will follow the rules set for the previous daylight saving time changes. This means that the system that has not been updated will not modify the clock and will reflect the incorrect time because, on September 30, 2007, the system not will adjust as if DST has taken effect.**

CSCsj72914 Conference Calls Experience Poor Audio Quality

Conference calls that are using the software media resources (MTP, MOH, and CFB) on a Cisco Unified CallManager 5.1(2x) server experience poor audio quality when they traverse a WAN that has QoS implemented.

Because the RTP that is coming from Cisco Unified CallManager has a DSCP of 0x00 these packets can get queued and/or dropped behind other voice signaling and RTP packets at the WAN router. Depending on network conditions for the WAN link this can cause poor audio quality.

Current Condition

The release of Cisco Unified CallManager Release 5.1(2b) resolves this problem.

CSCsj42921 Abbreviated Dialing Does Not Work for Index 43 and Higher

Abbreviated dialing does not work for indexes 43 and higher.

Current Condition

The release of Cisco Unified CallManager Release 5.1(2b) resolves this problem.

New and Changed Information for Cisco Unified CallManager Release 5.1(2a)

The following sections contain information about the caveats that are resolved in the release of Cisco Unified CallManager 5.1(2a)

- CSCsj45679 Data Validation Fails for Lowercase Device Names, page 17
- CSCsj42131 User with Incorrect Primary Extension in Directory Export, page 17
- CSCsj22669 User and User Profile Association Issue in Directory Export, page 17
- CSCsi20684 CSS Call Forward All, page 18
- CSCsi71128 DMA Requires a Long Time to Run, page 18

CSCsj45679 Data Validation Fails for Lowercase Device Names

Caveat

DMA 5.1(2) data validation reports rules compliance errors that are related to device names that contain lowercase characters. If you migrate to Cisco Unified CallManager 5.1(2) despite these error messages, various administrative activities that involve these records and those that use them can fail.

Current Condition

The release of Cisco Unified CallManager Release 5.1(2a) and Data Migration Assistant 5.1(2b) resolves this problem.

CSCsj42131 User with Incorrect Primary Extension in Directory Export

Caveat

After migration from Cisco Unified CallManager Release 4.x to Cisco Unified CallManager Release 5.x, the user gets associated with the wrong primary extension.

Current Condition

The release of Data Migration Assistant 5.1(2b) resolves this problem.

CSCsj22669 User and User Profile Association Issue in Directory Export

Caveat

Multiple CNN profiles per user exist in the Cisco Unified CallManager Release 4.x directory. After an upgrade to Cisco Unified CallManager 5.1(2), despite a clean DMA run, lost/missing/incorrect login profiles and device associations exist.

Current Condition

The release of Data Migration Assistant 5.1(2b) resolves this problem.

CSCsi20684 CSS Call Forward All

Caveat

DMA fails to validate when invalid contents exist in the CSSForCFA table and one of the following errors is received in the DMA Backup log:

Pre-DMA5.1(2b):

The following directory numbers have invalid CallingSearchSpaces for forward: 61880. Please remove or set these CallingSearchSpaces for these DNs and rerun DMA.

Exportable format of Cisco CallManager databases backed up successfully.

DMA5.1(2b):

Failure: #####>>> Invalid Call Forward All Calling Search Space settings have been detected. The following directory number(s) are involved: [61880]. These DN records, (usually Phone related), must be either corrected or removed and DMA then re-executed. The problem data may have resulted from either residual settings from an older CM version or from an external, adjunct, or third-party CM call forwarding application directly storing into this column. If the affected DN records are obsolete or easily re-entered, they should be deleted via the administration menus. The administrative interface does not provide any means to otherwise correct the problem data. If the problem records can not be deleted, correction will require the use of Enterprise Manager or other SQL access tools. Correction using these direct DB modification tools may require the approval and assistance of Cisco Support. If pursuing record correction, the following SQL query may be helpful to identify problem records that can not be deleted: [SELECT * FROM NumPlan WHERE CSSforCFA IS NOT NULL AND CSSforCFA NOT LIKE '{%']. Additionally, correct settings for the CSSforCFA column include either empty/null or the PKID of a valid CSS in the form '{pkid}:{}'.

modExportDatabase=Failure

Could not complete database processing successfully.

Failed to back up exportable format of Cisco CallManager databases.

Current Condition

The release of Data Migration Assistant 5.1(2b) resolves this problem.

CSCsi71128 DMA Requires a Long Time to Run

Caveat

Upgrading to Cisco Unified CallManager Release 5.x from releases of Cisco Unified CallManager prior to release 4.1(3), DMA execution takes a very long time in the premigration phase. If this occurs, you should wait for completion. A delay in this phase of up to 23 hours for 45,000 devices has occurred.

Current Condition

The release of Data Migration Assistant 5.1(2b) resolves this problem.

New and Changed Information for Cisco Unified CallManager Release 5.1(2)

The following sections describe new features and changes that are pertinent to Cisco Unified CallManager Release 5.1(2). 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 Release 5.1(2) Administration, page 19
- New and Changed Information for Cisco Unified CallManager Serviceability, page 34

New and Changed Information for Cisco Unified CallManager Release 5.1(2) Administration

Cisco Unified CallManager Release 5.1(2) made the following changes:

- AXL Field Enhancement, page 19
- BAT Support for VG224 Gateways, page 19
- Call Forward All Calling Search Space Backward Compatibility, page 33
- Locations and Region Enhancements, page 34

AXL Field Enhancement

Cisco Unified CallManager Release 5.1(2) supports the following new tags that have been added to the AXL APIs:

1. **displayASCII** now exists as a subtag of the tag <lines> in add/update/removePhone APIs.
2. **secondaryCallingSearchSpace** now exists as a subtag of <callForwardAll> in add/update/getLine APIs.
3. **unattendedPort** now exists in:

- add/update/getGatewayEndpoints for the gateway types DigitalAccessT1,DigitalAccessPRI and AnalogAccess
- add/update/getPhone APIs
- add/update/getH323Phone APIs
- add/update/getH323Trunk APIs
- add/update/getSIPTrunk APIs

BAT Support for VG224 Gateways

In the past, using Cisco Unified CallManager Administration to provision analog phones one by one on the VG224 gateway proved very time consuming. Now, you can provision all parameters that can be provisioned from Cisco Unified CallManager Administration through the Bulk Administration Tool (BAT).

This section contains information for

- Creating CSV Data Files for VG224 Gateways, page 20

- Creating a VG224 Gateway Template, page 22
- Field Descriptions for VG224 Gateway Template, page 23
- Adding FXS Ports to a VG224 Gateway Template, page 24
- Field Descriptions for FXS Port Configuration, page 25
- Adding VG224 Gateways to Cisco Unified CallManager, page 29
- Configuration Settings, page 30
- Finding a Gateway Template, page 32

Creating CSV Data Files for VG224 Gateways

Before you create a VG224 gateway template, you must create a CSV data file for the VG224 gateway.

These sections describe how to create the CSV data file.

- Using the BAT Spreadsheet for CSV Data Files for VG224 FXS Gateways and Ports, page 20
- Creating a Text-Based CSV File for VG224 Gateways, page 22
- FXS Trunks CSV File Format for VG224, page 22

Using the BAT Spreadsheet for CSV Data Files for VG224 FXS Gateways and Ports

Use the BAT spreadsheet to create the CSV data file that contains the details, such as domain name, MGCP description, and port identifier, for individual FXS ports.

To create a text-based CSV data file for VG224 gateways, see Creating a Text-Based CSV File for VG224 Gateways, page 22

For more information, see the *Cisco Unified CallManager Bulk Administration Guide 5.0(4).*

Procedure

Step 1 From Cisco Unified CallManager Administration, click **Bulk Administration** > **Upload/Download**.

Step 2 The Find and List Files window displays. Click the **Find** button.

Step 3 The list of files displays. Click the **BAT.xlt** check box and click **Download Selected** button and save the file to your computer.

Step 4 To open the BAT spreadsheet, locate and double-click **BAT.xlt** file.

Step 5 When prompted, click **Enable Macros** to use the spreadsheet capabilities.

Step 6 Click the **VG224** tab.

Step 7 For MGCP, click the **MGCP** radio button and for SCCP, click the **SCCP** radio button.

Step 8 If you choose MGCP, proceed to Step 9. If you choose SCCP, a **Create File Format** button appears in the spreadsheet.

a. Click **Create File Format**; the Field Selection window displays.

b. From the Device Fields box, select the required device fields and click the >> button to move them to the Selected Device Fields box.

c. From the Line Fields box, select the line fields and click the >> button to move them to the Selected Line Fields box.

d. Click the **Up** and **Down** buttons to rearrange the selected fields.

e. You can click the << button to remove any selected fields from the selected fields list.

f. When you are done selecting the required fields, click **Create** to add the selected fields to the VG224 sheet.

Step 9 In each row, provide the information for the following fields:

- **Domain Name**—Enter a name, from 1 to 64 characters, that identifies the gateway. Use the Domain Name System (DNS) host name if it is configured to resolve correctly; otherwise, use the host name as defined on the Cisco MGCP gateway.

  The host name must match exactly the host name that is configured on the Cisco IOS gateway. For example, if the host name is configured on the gateway to resolve to vg224-1 and the IP domain name is not configured, enter the host name in this field (in this case, vg224-1). If the host name is configured on the gateway as vg224-1 and the IP domain name is configured on the gateway as cisco.com, enter vg224-1.cisco.com in this field.
- **Description**—Enter a description of up to 100 characters for the gateway. Use a specific description that helps you locate the gateway.
- **Port Description**—Enter a description for port 1, up to 50 characters. Use a description to help identify the port in a list of ports. This applies to the description field for port 2 through port 4.
- **Port Directory Number**—Enter the directory number, up to 24 numerals and special characters, for this port. This applies to the directory number field for port 2 through port 4.

Note You must use Port 1 Directory Number and Partition fields for FXS ports only. For FXO ports, leave these fields blank.

- **Slot 2—**Enter the slot number that you are trying to configure. For VG224, the slot always equals 2.
- **Subunit—**Enter an integer for the subunit value. For VG224, the subunit always equals 0.
- **Port Number**—Enter an integer for the Port Number.

Step 10 To transfer the data from the BAT Excel spreadsheet into a CSV file, click **Export to BAT Format**.

The system saves the file to C:\XLsDataFiles (or to your choice of another existing folder) as VG224Gateways#timestamp.txt where “timestamp” represents the precise date and time that the file was created.

Tip If you enter a comma in one of the fields, BAT.xlt encloses that field entry in double quotes when you export to BAT format.

If you enter a blank row in the spreadsheet, the system treats the empty row as the end of the file. Data that is entered after a blank line does not get converted to the BAT format.

You must upload the CSV data file to the first node of the Cisco Unified CallManager server, so BAT can access the data input file. For more information, see the “Uploading and Downloading Files” chapter in the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)*.

Note For information on how to read the exported CSV data file, click the link to **View Sample File** in the Insert Gateways window in BAT.

Creating a Text-Based CSV File for VG224 Gateways

Instead of using the BAT spreadsheet for data input to add Cisco VG224 gateways, you can create the comma separated values (CSV) file by using lines of ASCII text with values that are separated by commas.

To create a CSV text file for VG224 gateways, use this procedure.

Procedure

Step 1 Open a text editor (such as Notepad) or any application that allows you to export or create a CSV file.

Step 2 Using a separate line for each gateway, enter the values for each gateway and port that you want to add to Cisco Unified CallManager.

The section FXS Trunks CSV File Format for VG224, page 22, provides descriptions and examples.

Note An error occurs if any blank lines exist in the CSV file. Upload the file to the server that is running the first node database for Cisco Unified CallManager. See the “Uploading a File” section of the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)*.

FXS Trunks CSV File Format for VG224

The following sample format shows the required field length and string types followed by sample of CSV files for a VG224 gateway.

MGCP Domain Name(Mandatory, 1 to 64 characters)**,Description**(Optional, up to 100 characters)**,Slot**(Mandatory, up to 3 numerals), **Subunit** (Mandatory, up to 3 numerals), **Port Number**(Mandatory, up to 3 numerals), **Port Description** Optional, up to 50 characters),**Port Directory Number**(Optional, up to 24 numerals and special characters)

Sample

```
MGCPTest,VG224 Lab Gateway,2,0,0,Port 0,97255576601
MGCPTest,VG224 Lab Gateway,2,0,1,Port 1,97255572001
```

Note You must include comma separators even if a field is blank. Specify the directory number and route partition only if the port type in the VG224 gateway template is POTS.

Example 1

If the Description for a VG224 gateway is blank, use this format:

```
MGCPTest, ,2,0,0,Port 0,97255576601
```

Creating a VG224 Gateway Template

You must create a VG224 template and then add endpoint identifiers for the network modules. You must use a BAT template to configure the following endpoint identifiers.

- Foreign Exchange Station (FXS) ports

Use the following procedure to add a VG224 Gateway template.

Procedure

Step 1 Choose **Bulk Administration** > **Gateways** > **Gateway Template.**

The Find and List Gateway window displays.

Step 2 Click **Add New**. The Add a New Gateway window displays.

Step 3 From the Gateway Type drop-down list box, choose VG224 and click **Next**.

The next Add a New Gateway window displays.

Step 4 From the Protocol drop-down list box, choose MGCP or SCCP and click **Next**.

The Gateway Configuration window displays.

Step 5 Enter values for all the fields. See Creating a VG224 Gateway Template, page 22.

Step 6 Click **Save**. When the insert completes, a new field displays on the pane.

Step 7 In the Subunit 0 field, choose the appropriate type for the subunit field from the drop-down list box.

- VIC-2FXS—Foreign Exchange Station (FXS) voice interface card.

Step 8 Click **Save**. When the Status indicates that the update completed, the endpoint identifiers display as links to the right of the subunit drop-down list boxes.

Step 9 Click an endpoint identifier (for example, 1/0/0) to configure device protocol information and add ports for the installed types of VICs.

For detailed instructions, see the following procedures:

- Adding FXS Ports to a VG224 Gateway Template, page 24

Step 10 To reset the gateway and apply the changes, click **Reset**.

Step 11 Continue configuring endpoint information and ports as needed.

Field Descriptions for VG224 Gateway Template

Table 44-2 provides detailed descriptions for VG200 gateway template configuration settings.

.

Table 5 VG224 Gateway Configuration Settings

Field	Description
Template Name	Enter a name of up to 64 characters that identifies the VG224 gateway template.
Description	Enter a description that clarifies the purpose of the device.

Table 5 VG224 Gateway Configuration Settings (continued)

Field	Description
Cisco Unified CallManager Group	From the drop-down list box, choose a Cisco Unified CallManager redundancy group. A Cisco Unified CallManager redundancy group includes a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager. If the primary Cisco Unified CallManager is not available or fails, the gateway attempts to connect with the next Cisco Unified CallManager in the list and so on.
Configured Slots, VICs, and Endpoints	
Module in Slot 2	For the available slot on the VG224 gateway, choose Analog from the drop-down list box.
Subunit 0	For the available subunit 0 on the VG224 gateway, choose 24FXS as the subunit from the drop-down list box. **Note** Be aware that only Module in Slot 2 and Subunit 0 are available for VG224 gateways.

Adding FXS Ports to a VG224 Gateway Template

You can use Foreign Exchange Station (FXS) ports to connect to any POTS device. Use this procedure to add FXS ports on a VG224 gateway template.

Before You Begin

You must add a VG224 gateway template before configuring ports. See the Creating a VG224 Gateway Template, page 22 for instructions.

Procedure

Step 1 To find the gateway template to which you want to add FXS ports, see Finding a Gateway Template, page 32.

Step 2 From the Gateway Template Configuration window, click the endpoint identifier for the FXS VIC that you want to configure icons.

Step 3 Enter the appropriate **Gateway Information** and **Port Information** settings. See the following sections for details about these fields:

- Field Descriptions for FXS Port Configuration, page 25
- POTS Port Configuration Settings, page 30

Step 4 Click **Save**.

Note After you insert a POTS port, the window refreshes and displays the POTS port information at the bottom of the window. An **Add a new DN** link displays in the Directory Number Information area in the left panel.

Step 5 Click **Add a new DN** to add directory numbers to the POTS port or, if you configured another type of port, go to Step 7.

Note See the Adding or Updating Lines in a BAT Template section of the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)* for information about adding and configuring DNs.

Step 6 To return to the main VG224 Gateway Template Configuration window for the gateway to which you just added the ports, choose **Back to MGCP Configuration** in the Related Links drop-down list box and click **Go**.

Step 7 To reset the gateway and apply the changes, click **Reset**.

Step 8 To add additional FXS ports, repeat Step 2 through Step 6.

Field Descriptions for FXS Port Configuration

Table 6 provides detailed descriptions for FXS port configuration settings.

Table 6 FXS Port Configuration Settings

Field	Description
Device Information	
End-Point Name	For VG224 gateways, this display-only field contains a string that Cisco Unified CallManager generates that uniquely identifies the VG224 analog interface.
Description	Enter a description that clarifies the purpose of the device.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Data/Time Group, Region, and Calling Search Space for auto registration of devices.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

Table 6 FXS Port Configuration Settings (continued)

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and enter a value for Max List Box Items in the Unified CMAdmin Parameters pane.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the location feature does not keep track of the bandwidth that this device consumes.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Table 6 FXS Port Configuration Settings (continued)

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. **Note** Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device pool for the device to determine whether to send Unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device pool of the device matches the terminating phone user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming Unicode characters based on the user locale setting of the device pool of the sending device. If the user locale setting matches the terminating phone user locale, the phone displays the characters.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <*None*>, this device inherits its MLPP domain from the value set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value set for the MLPP Domain Identifier enterprise parameter.
Port Information (POTS)	

Table 6 FXS Port Configuration Settings (continued)

Field	Description
Port Direction	Choose the direction of calls that are passing through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Bothways—Use for inbound and outbound calls (default).
Prefix DN (for FXS ports)	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. The Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Num Digits setting.
Num Digits (for FXS ports)	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that is used to route calls coming into the PRI span. See Prefix DN.
Expected Digits (for FXS ports)	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. **Note** Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
Unattended Port	Check this check box to indicate an unattended port on this device.

Table 6 FXS Port Configuration Settings (continued)

Field	Description
Product-Specific Configuration	
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "**?**" information icon to the right of the **Product Specific Configuration** heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Adding VG224 Gateways to Cisco Unified CallManager

To add Cisco gateways and ports to Cisco Unified CallManager, use this procedure.

Before You Begin

If you want to add a Cisco VG224 gateway, you must have a VG224 gateway template for the trunks or ports and a CSV data file for the VG224 gateway ports. See Creating a VG224 Gateway Template, page 22 and Creating CSV Data Files for VG224 Gateways, page 20.

Procedure

Step 1 Choose **Bulk Administration** > **Gateways** > **Insert Gateways**. The Select the Gateway window displays.

Step 2 Choose type of gateway that you want to insert from the Gateway Type drop-down list box. The Insert Gateway Configuration window displays.

Step 3 In the File Name field drop-down list box, choose the name of the CSV data file that contains the Cisco VG200 gateway information to be added.

Step 4 In the Gateway Template Name field, choose the name of the VG200 or the FXS gateway template that you created for this type of bulk transaction.

Step 5 In the Job Information area, enter the Job description.

Step 6 To insert the gateway immediately, click the Run Immediately radio button or click Run Later to insert at a later time.

Step 7 To create a job for inserting the gateways, click **Submit**.

Step 8 Use the Job Scheduler option in the Bulk Administration main menu to schedule and/or activate this job.

For more information on jobs, see the "Scheduling Jobs" chapter in the *Cisco Unified CallManager Bulk Administration Guide*.

For information on log files, see the "BAT Log Files" section of the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)*.

Configuration Settings

The following sections contain configuration settings for

- POTS Port Configuration Settings, page 30
- Finding a Gateway Template, page 32

POTS Port Configuration Settings

Table 7 describes the POTS port configuration settings.

Table 7 POTS Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose **POTS**.
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the **Beginning Port Number** and **Ending Port Number** fields: • To specify a range of ports, choose appropriate values for **Beginning Port Number** and **Ending Port Number**. • To create a single port, choose the same number in the **Beginning Port Number** and **Ending Port Number** fields. • To add all available ports, choose **All Ports** for both the **Beginning Port Number** and **Ending Port Number** fields.
Port Direction	Choose the direction of calls that pass through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Bothways—Use for inbound and outbound calls (default).
Audio Signal Adjustment into IP Network	This field specifies the gain or loss that is applied to the received audio signal relative to the port application type. **Note** Improper gain setting may cause audio echo. Use caution when you adjust this setting.
Audio Signal Adjustment from IP Network	This field specifies the gain or loss that is applied to the transmitted audio signal relative to the port application type. **Note** Improper gain setting may cause audio echo. Use caution when you adjust this setting.

Table 7 POTS Port Configuration Settings (continued)

Field	Description
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. The Cisco Unified CallManager adds prefix digits after it truncates the number in accordance with the Num Digits setting.
Num Digits	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called.
Expected Digits	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
Call Restart Timer (1000-5000 ms)	Call Restart Timer (1000-5000 ms); ms indicates time in milliseconds.
Offhook Validation Timer (100-1000 ms)	Offhook Validation Timer (100-1000 ms); ms indicates time in milliseconds.
Onhook Validation Timer (100-1000 ms)	Onhook Validation Timer (100-1000 ms); ms indicates time in milliseconds
Hookflash Timer (100-1500ms)	Hookflash Timer (100-1500 ms); ms indicates time in milliseconds.
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. **Note** Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
Product Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "**?**" information icon to the right of the **Product Specific Configuration** heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Finding a Gateway Template

Because you might have several gateway templates, Cisco Unified CallManager lets you locate a specific template on the basis of specific criteria. Use the following procedure to locate templates.

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

Procedure

Step 1 Choose **Bulk Administration > Gateways > Gateway Template**.

The Find and List Gateway window displays.

Step 2 From the first Find Gateways where drop-down list box, choose one of the following criteria:

- Name
- Description
- DN/Route Pattern
- Calling Search Space
- Device Pool
- Route Group Name
- Device Type

Step 3 From the second Find Gateways where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 4 Specify the appropriate search text, if applicable.

Tip To find all gateways that are registered in the database, click **Find** without entering any search text.

Step 5 Choose **Show** from the third drop-down list box to show the end points that are associated with gateways and click **Find**.

A list of discovered templates displays by

- Device Name
- Description
- Device Pool
- Status
- IP Address

Step 6 From the list of records, click the device name that matches your search criteria.

The Gateway Configuration window displays.

Call Forward All Calling Search Space Backward Compatibility

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 Communications Manager 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*.

Locations and Region Enhancements

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.

New and Changed Information for Cisco Unified CallManager Serviceability

Cisco Unified CallManager Release 5.1(2) made the following serviceability change

- DeviceUnregistered Alarm, page 34

DeviceUnregistered Alarm

The release adds new reason codes to the DeviceUnregistered Alarm.

- ReasonCode 14:ConfigurationMismatch. This means that the configuration on the phone does not match the configuration on the Cisco Unified CallManager.
- ReasonCode 15: CallManagerRestart. This means that the system restarted from the Cisco Unified CallManager Administration window (as opposed to "reset" as in ReasonCode 9).
- ReasonCode 16: DuplicateRegistration. This means that Cisco Unified CallManager detected that the same device was registered on two nodes at the same time. When this happens, Cisco Unified CallManager sends a restart request to the phone to force the phone to register with only one Cisco Unified CallManager.

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

The following sections describe new features and changes that are pertinent to Cisco Unified CallManager, Release 5.1(1b) 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 35
- New and Changed Information for Cisco Unified Communications Operating System Administration, page 39
- New and Changed Information for Cisco Unified CallManager Features, page 39
- New and Changed Information for Cisco Unified CallManager Applications, page 43
- New and Changed Information for Cisco Unified CallManager Bulk Administration Features, page 44
- New and Changed Information for Cisco Unified CallManager Serviceability, page 45
- New and Changed Information for Third-Party API, page 47
- New and Changed Information for Cisco Unified IP Phones, page 48

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 35
- General Administration Enhancements, page 35
- Service Parameter Changes, page 36
- Cisco Unified CallManager Administration Menu Updates, page 36
- Third-Party SIP Phone Enhancements, page 36
- Phone Configuration Enhancements, page 37
- Phone Button Configuration Enhancements, page 37
- License Capabilities Assignment, page 37
- Enterprise Parameter Changes, page 37
- Additional Corporate Directory Support, page 38

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, several options exist 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 and 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 (iDivert) includes the following new service parameters:
  - Use Legacy iDivert
  - Allow QSIG During iDivert
  - iDivert User Response Timer

  See the "Immediate Divert Enhancements" section on page 40 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 48 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 41 for more information.
- Two Cisco Unified CallManager service parameters relate to the Enhanced iDivert feature:
  - Use Legacy Immediate Divert - This clusterwide service parameter defines whether the legacy iDivert behavior is maintained or the new Enhanced iDivert behavior is adopted. If the Use Legacy iDivert service parameter is set to True, the user can divert an incoming call only to the voice mailbox of the user.
  - Allow QSIG during iDivert – iDivert diverts calls to voice-messaging systems that can be reached over QSIG, SIP, and QSIG-enabled H.323 devices if the clusterwide 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(1b):.

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(1b)

In Cisco Unified CallManager Release 5.1(1b) 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 that is using 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 and Cisco Unified Personal Communicator capabilities for users. You must ensure that licenses for Cisco Unified Presence and Cisco Unified Personal Communicator 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 Cisco Unified Presence (servers and clients) and Cisco Unified Personal Communicator 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.

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 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 Phones 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 37.

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 37) 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 uses the value that the enterprise parameter setting specifies.

Table 8 indicates how the phone responds to the configuration options.

Table 8 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. For more information on wideband codec, see the "Wideband Codec" section on page 49.

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 codec produces the same effect. When you choose either G.711 or G.722, these codecs disallow selection of codecs that have a payload that is 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 has lower than G.711 or G.722 codec, the Advertise G.722 Codec enterprise parameter gets ignored because the system does not allow G.722, G.711, AAC, and wideband.

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 enhancement:

- New CLI Commands and Command Options, page 39

New CLI Commands and Command Options

You now have the following new CLI commands and command options that 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 fior
  - utils iothrottle
  - utils reset_ui_administrator_password
  - utils sftp
- After uploading a file to the TFTP server, you must 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, page 40
- Call Forward All Override, page 41
- AAC Voice Codec Support, page 42
- Arabic Language (right to left) Support, page 42

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 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

Perform the following steps to configure iDivert.

Step 1 Configure appropriate service parameters.

Step 2 Configure the iDivert softkey.

- If you are 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 you are 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 the voice-messaging system or to the original called party voice-messaging system. The system administrator must make sure that this option is 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 system 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

The following Cisco Unified IP Phones support the immediate divert feature.

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

Call Detail Records Considerations

Immediate divert uses the Immediate Divert code number in the On behalf of fields (for example, join On behalf Of 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 parameter supports Call Forward All Override:

- CFA Destination Override

Cisco Unified IP Phone Support

The following Cisco Unified IP Phones support Call Forward All Override.

- Cisco Unified IP Phone 7971G (SCCP and SIP)
- Cisco Unified IP Phone 7971G-GE (SCCP and SIP)
- Cisco Unified IP Phone 7970G (SCCP and SIP)
- Cisco Unified IP Phone 7961G-GE (SCCP and SIP)

- Cisco Unified IP Phone 7960G (SCCP and SIP)
- Cisco Unified IP Phone 7941G-GE (SCCP and SIP)
- Cisco Unified IP Phone 7940G (SCCP and SIP)
- Cisco Unified IP Phone 7911G (SCCP and SIP)
- Cisco Unified IP Phone 7906G (SCCP and SIP)

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 phones support 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

The following Cisco Unified IP Phones support Arabic language.

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 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 43
- DirSync Application Enhancements, page 43

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 Phones 7940 and 7960, or SIP phone loads 8.1(x) and earlier for Cisco Unified IP Phones 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 44

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 44
- TFTP Exclude Digest Credentials Check Box Display, page 45
- Upgrading Cisco Unified IP Phones to Authenticate with LSCs Not MICs, page 45

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 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 that have security enabled.

This release also adds CTL support for a Cisco Unified CallManager supercluster: sixteen call-processing servers, one publisher server, 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 CTLClient, 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 Phones 7905, 7912, 7940, and 7960 that are using SIP 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 Phones 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 Cisco Unified 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 Cisco Unified CallManager Release 5.1(1b):

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 enhancement for Cisco Unified CallManager Release 5.1(1b):

- 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 Cisco Unified CallManager Release 5.1(1b):

- 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 Cisco Tomcat Connector 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 Cisco Unified CallManager Release 5.1(1b):

- 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 does 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 48

- Web Dialer Requirements, page 48

AXL Programming

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 Release 5.1 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 Cisco Unified CallManager Release 5.0. Cisco recommends that you set this parameter to True, so Cisco Unified CallManager sends the valid namespace.

Web Dialer Requirements

Cisco Unified CallManager Release 5.1 includes 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)*

New and Changed Information for Cisco Unified IP Phones

The following section describes the enhancements for Cisco Unified IP Phones:

- Wideband Codec, page 49

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 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 remains 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, users 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) 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 37 and the "Phone Configuration—Product-Specific Configuration Changes" section on page 37.

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(x) 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 to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

This section includes the following topics:

- Using Bug Toolkit, page 50
- Saving Bug Toolkit Queries, page 50

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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

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

Note If you are looking for information about a specific caveat, enter the ID number in the “Search for bug ID:” field and click **Go**.

Step 2 From the Select Product Category drop-down box, choose “Voice and Unified Communications.”

Step 3 From the Select Product drop-down box, choose “Cisco Unified Communications (CallManager).”

Step 4 In the Software Version, Version drop-down list, choose the major release of Cisco Unified Communications Manager for which you want the caveats (for example, 5.0, 6.0, and so on).

Step 5 Under Advanced Options, choose “Use custom settings for severity, status, and others.”

a. In the information that displays, click (to “uncheck”) the Fixed check box.

b. From the Modified Date drop-down list, choose “Any Time.”

Step 6 Click **Search**.

Note You can save your query for future use. See the “Saving Bug Toolkit Queries” section on page 50.

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 that are 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 50.

Step 2 Click the **Save Search** button that displays at the bottom of the window.

The Save Search Setting window displays.

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

Step 4 In the Place in Group section, you can

- 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.

Step 5 In the Group Notifications Settings section, for Email Updates, 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:

- **No email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Yes, 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.
- **On a schedule**—Click the radio button to choose this option and from the drop-down list, choose how often you want to get updates from the Bug Toolkit.

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

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/en/US/products/hw/phones/ps379/prod_release_notes_list.html.

Open Caveats

Table 9 describes possible unexpected behaviors in Cisco Unified CallManager Release 5.1(2b), which are sorted by component.

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

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

When you open the online record for a defect, you may see data in the “First Fixed-in Version” or “Integrated-in” fields. The information that displays in these fields identifies the list of Cisco Unified 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 9 reflects a snapshot of the defects that were open at the time that 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 50.

Tip Bug Toolkit requires that you have an account with Cisco.com (CDC). 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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

.

Table 9 Open Caveats as of 7-30-2007

Identifier	Headline
Component: Alarm Library	
CSCsj20653	Critical alarms occur when a large number of phones unregister simultaneously.
CSCsj21916	Trace collection alarms do not send remote syslog events.
Component: Alert Coll Report	
CSCsj44019	Because the syslog trap message length limit is 255 characters, some alert messages get truncated and do not include valuable information.
CSCsi89966	User should be warned that the system could become unstable if the switch-version is not complete on a subscriber server after the publisher server has been upgraded.
Component: Attendant Console	
CSCsj76444	General SQL failure and Java exception error messages get printed to the upgrade log file.
CSCsj43639	"Unknown to" displays when a MeetMe call gets transferred to the attendant PC.
Component: AXL	

Table 9 Open Caveats as of 7-30-2007 (continued)

CSCsj71916	AXIS Java Exception occurs.
Component: Backup and Restore (BAR)	
CSCsj31456	RTMT receives a CallProcessingNodeCpuPegging alert during a Disaster Recovery Framework (DRF) backup.
Component: BPS-BAT	
CSCsj74281	In the UDP report that is generated from **Bulk Admin > UDP > Generate UDP report,** the Service URL column remains blank.
CSCsj78157	Last username missing for Cisco Unified Presence update user
CSCsj03551	User cannot upload user device profiles to BAT.
Component: CAR	
CSCsi08316	Critical Service Down alerts occur during upgrade.
CSCsi63705	CAR report results do not display in the correct order.
Component: CDP	
CSCsj38368	CDP message gets sent to destination mac address 00:00:00:00:00:00 about eth1 port. CAM table of switchport that connects to non-primary interface (eth1) contains MAC address of primary interface (eth0) while not being active.
Component: CLI	
CSCsh67199	The CLI command set network NIC does not work properly.
CSCsj64463	From the Arizona time zone, when the user enters the CLI command "show timezone config" the output displays America/Phoenix.
CSCsi70101	You cannot stop or start some platform agents by using the CLI or GUI.
CSCsh80670	User cannot get XML files from CLI.
CSCsi21510	Subscriber installation fails.
CSCsj83200	The need exists for CLI commands to diagnose SNMP monitoring problems on Cisco Unified CallManager.
CSCsi64187	CLI displays incorrectly after linewrap.
Component: CTI	
CSCsi06589	System does not verify that the number of ConsultCalls is in the range of maximum consult calls.
CSCsj67813	EIS messaging to 7920 phones using Cisco Unified CallManager 5.1(2) cause the 7920 to restart with this error: Jun 19 22:55:14 x [call] receive data length(2044) > buffer allocated, abort!
CSCsi85253	Restriction status for open lines gets updated inefficiently by CTI.
CSCsi83873	VG248 registrations cause Cisco Unified CallManager core and CPU spike on publisher server.
Component: Cisco Unified CallManager User Interface	
CSCsj64476	The Cisco Unified CallManager Administration firmware load information report incorrectly states that all 7914 modules are configured for non-default firmware.
CSCsj70201	Hunt-group disappears after values get modified.

Table 9 Open Caveats as of 7-30-2007 (continued)

CSCsi62093	Incorrect EVM-HD subunit number in Cisco Unified CallManager Administration for SCCP analog gateway.
CSCsh18895	Reset function does not work for a full access standard phone administration user.
Component: Call Processing	
CSCsi91401	Database: When you change a phone security profile during a subscriber disconnect, and reconnect later, the phone registration gets rejected.
CSCsg29976	Media Control: Video RSVP call to Cisco Unified Presence Communicator end point takes three RSVP resources.
CSCsi06692	Media Control: MGCP T.38 Fax CallAgent Controlled fails.
CSCsj56172	Media Control: Third party voice messaging system does not recognize DTMF.
CSCsj64738	MLPP: Incorrect call treatment gets applied when an MLPP user calls into a MeetingPlace conference at equal or lower precedence than existing conference attendees. When this occurs, the system denies the call and the user receives a busy signal indicator instead of a BPA announcement.
CSCsh06653	SCCP: A conference call that is initiated by a 24 digit DN displays 'To External' instead of 'To Conference.'
CSCsh64270	SCCP: Missed calls do not display for conference calls.
CSCsi42168	SCCP: Received Calls list on phone does not include conference calls.
CSCsj64657	SCCP: ISDN alerting message does not get sent until the preempted station goes onhook. If this occurs after 4 seconds, a failure occurs on the far end switch and the call does not complete.
CSCsj78900	SCCP: Cisco Unified CallManager cannot disconnect a preserved call.
CSCsj18895	SCCP: When a Cisco Unified IP Phone 7970 communicates with a pre- 6.0 Cisco Unified CallManager release, programmable line keys (PLKs) work as expected but but their labels display "???"
CSCsi49956	Session Initiation Protocol (SIP) Station: When the user transfers a parked call, the call gets put on hold.
CSCsj69298	Session Initiation Protocol (SIP) Station: Cisco Unified CallManager service may restart unexpectedly.
CSCsj15794	Session Initiation Protocol (SIP) Station: Cisco Unified CallManager cannot disconnect a preserved call.
CSCsj63680	Session Initiation Protocol (SIP) Station: When Cisco Unified Personal Communicator attempts to SIP register to Cisco Unified CallManager (for softphone), it fails when the username is entirely numeric (for example 10000).
CSCsj36370	Session Initiation Protocol (SIP) Trunk: FC3725 flow IV fails on Cisco Unified CallManager 5.1 that is using SIP.
CSCsj54212	Session Initiation Protocol (SIP) Trunk: SIP trunk calls fail with the firewall syslog message: Deny TCP (no connection) from [IP]/[Port] to [IP]/5060 flags PSH ACK on interface [Interface Name].
CSCsj73374	Session Initiation Protocol (SIP) Trunk: After a call gets transferred, Cisco Unified CallManager does not respond to an mpserver request.

Table 9 Open Caveats as of 7-30-2007 (continued)

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.
CSCsi32626	System: Calls get rejected due to throttling at a low call rate, not at a higher call rate.
CSCsj76788	System: After a large database gets added, a system may restart during initialization.
Component: Cisco Customer Performance Indicators (CPI)	
CSCsj84265	Appinstall: Network connectivity fails.
CSCsj35209	Appinstall: If you cancel an installation from DVD after the file upload begins, the mount fails.
CSCsi51295	Certificate Management: Tomcat web certificate regeneration fails.
CSCsj04294	Data Migration Assistant: The DMA logs contain errors that indicate files and directories could not be accessed or created.
CSCsj24532	Data Migration Assistant: Provide guidelines on DMA process.
CSCsj24595	Data Migration Assistant: Simplify log file collection.
CSCsi81184	Data Migration Assistant: Installation fails and displays:"Error 1720. There is a problem with this Windows Installer Package. A script required for this install to complete could not be run. Contact your support personnel or package vendor."
CSCsi68776	Data Migration Assistant: The estimated time to complete a backup is not displayed on the DMA window.
CSCsj78789	Data Migration Assistant: DMA validation fails with International Dial plans.
CSCsj02921	Data Migration Assistant: DMA installation fails.
CSCsj24610	Data Migration Assistant: Improve DMA uninstall.
CSCsj49413	Data Migration Assistant: During a DMA backup, a “This page cannot be displayed” message displays.
CSCsf24390	Data Migration Assistant: User tried to install DMA, and an error occurred.
CSCsh05766	Data Migration Assistant: DMA backup status indicates “ready” after the backup instead of “successful” or “failed.”
CSCsd11449	Operating System: BIOS does not get upgraded during an upgrade.
CSCsi30296	Operating System: Disk failures occur in MCS branded servers.
CSCsj74466	Operating System: After an installation, the following error displays: init: ID "SD0" respawning too fast: disabled for 5 minutes.
CSCsj58803	Operating System: For HP NC-Series Broadcom Firmware Updates that are available for supported NICs, see the “Additional Servers Supported” section on page 16
CSCsj49225	Operating system: An install of Cisco Unified CallManager on the subscriber server stops during NTP setup or, for already installed Cisco Unified CallManager nodes, the subscriber server fails to closely track the publisher server time.
CSCsj13054	Operating system: User needs the ability to get the SAR logs by using RTMT and CLI.
CSCsj76935	Operating system: On a kernel panic when netdump is configured, a backtrace gets dumped to the system console for every process in the system. This requires 10-20 minutes and during this time the system is not available.

Table 9 Open Caveats as of 7-30-2007 (continued)

CSCsj77005	Operating system: iLO2 error message on 7845H2 CLI window.
CSCse81663	Operating System: iLO firmware may fall below minimum version that is required. See the "iLO Firmware on MCS-7825-H1, MCS-7835-H1 and MCS-7845-H1" section on page 5
CSCse71209	Operating system: Smart Array 6i v2.68 requires HD firmware update to avoid POST notification. See the "Smart Array 6i Requires HD Firmware Update to Avoid POST Notification" section on page 5
CSCsf26301	Operating system: Smart Array 5i requires HD firmware update to avoid POST notification. See the "Smart Array 5i Requires HD Firmware Update to Avoid POST Notification" section on page 6.
CSCsi11535	Operating system: Subscriber server installation fails due to network conditions.
CSCsi24732	Operating System: IBM temperature sensor MIB does not respond on MCS-7835-I2 and MCS-7845-I2.
CSCsi90211	Operating System: Mirroring caused the screen to freeze and display meaningless text.
CSCsi75567	Operating System: System hangs on server trigger sporadic server reboots. See the "MCS-7825H2-IPC1 Reboots Randomly" section on page 6
CSCsj58962	Operating System: Hard drive models that experience excessive SCSI command timeouts should be upgraded. Failure to upgrade may result in the bus down-shifting from Ultra 320 to Ultra 3. See the "Smart Array 6i Requires HD Firmware Update to Avoid POST Notification" section on page 5
CSCsh54360	Operating System: During startup, Cisco Unified CallManager displays "verifyNetwork = Failed" on the console; but, services that require network functionality operate.
CSCsi02536	Operating System: During an installation of Cisco Unified CallManager, the system displays a BIOS flash failure warning message with options to continue or cancel the installation.
CSCsi74557	Platform API: You can enable DNS only during installation of Cisco Unified CallManager. If DNS is disabled during initial installation, you should reinstall Cisco Unified CallManager.
CSCsi11556	Platform API: Random feature failures occur on Cisco Unified CallManager.
CSCsj86505	Security: The need exists for the ability to restart the cluster manager process when it becomes stuck or unresponsive.
CSCsi88504	Service Manager: CLI cannot restart Tomcat.
CSCsh76059	Tool-kit: DRS does not back up or restore remote SSH keys that are used for TLC or CDR.
CSCsj86327	User Interface: Directory Certificate display shows error.
CSCsj35260	User Interface: SFTP/FTP information displays during upgrade via DVD.
Component: Database	
CSCsb71648	Migration took over 15 hours.
CSCsg06024	Database engine DDR block causes shut down of Tomcat server.
CSCsg90581	DMA upgrade fails.
CSCsh31645	Database replication suspect.

Table 9 Open Caveats as of 7-30-2007 (continued)

CSCsj13610	Cisco Unified CallManager cored after upgrade.
CSCsj40566	User cannot easily migrate from 4.x to 5.x if some characters exist in the database.
CSCsj79811	Database (Informix) does not start after license upload.
CSCsj01673	DMA fails to validate when invalid contents are in the CSSForCFA table.
CSCsj50260	After DMA invokes CAR export routine, no progress information displays on the DMA status window.
CSCse21733	After an upgrade, a ccmAgent core dump occurs when the database is shut down.
CSCsj69397	DMA generates one large installdbw1.log file which causes troubleshooting problems.
CSCsj78261	DMA XML format error.
CSCsh45042	IBM PMR 47825 49R 000 repl logs in /tmp results in not disabled.
CSCsi83076	DMA fails when backslash is used in Informix password.
CSCsi50840	RTMT cannot download Informix RIS traces.
CSCsi79380	When the user restarts the server, the RisDC core file displays.
CSCsj24485	DMA validation fails, and the error messages do not indicate how to fix the problem.
CSCsi35186	Extension mobility logins fail with an Error 6 database failure.
CSCsi41491	Informix creates AF and blocks when SHMTOTAL is reached.
CSCsj64692	After upgrade, the new network service displays inactive.
CSCsi84391	Although the service parameters default gets changes, values remain the same.
Component: Database Administration	
CSCsg96235	Reset function does not work for a full access standard gateway administration user.
CSCsj62771	Wrong partition gets selected when user adds a new line.
Component: Dialed Number Analyser	
CSCsj33867	RTMT reported a CallProcessingNodeCpuPegging alert after an upgrade.
Component: Directory	
CSCsj83255	Migration occurs, but not all users get migrated.
CSCsj82405	After DMA and upgrade, LDAP users in the Cisco Unified CallManager database are missing.
CSCsj24600	When the directory export is exporting directory data, no progress indication gets provided to DMA.
Component: Documentation	
CSCsi16035	Cisco Unified CallManager does not understand (.sgn) files.
CSCsj03460	*Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* do not provide correct information on deleting a server. See the "Deleting a Server" section on page 59
CSCsj31611	Disaster Recovery System documentation does not mention IP/hostname requirement.
CSCsj78966	Customers have questions about the timing of the CDR offload process beyond what is documented.

Table 9 Open Caveats as of 7-30-2007 (continued)

Component: Install Product	
CSCsj56299	CDR Analysis and Reporting does not reflect DST changes for New Zealand
Component: Cisco IP Manager Assistant Service	
CSCsj64228	Cisco IP Manager Assistant line status issues exist.
Component: Java Telephony API (JTAPI) Software Development Toolkit (SDK)	
CSCsg03945	CiscoJTAPIClient-linux.bin fails to install.
Component: QED	
CSCsj61870	Error occurs on Non-IOS T1 PRI Gateway configuration.
Component: RISDC	
CSCsj81077	CallProcessingNodeCPUPegging alerts in RTMT.
Component: Cisco Unified Real Time Monitoring Tool	
CSCsi83330	The permissions for Cisco Unified Real Time Monitoring Tool alert configuration and Cisco Unified Real Time Monitoring Tool profile access do not get properly enforced.
CSCsi80661	Cisco Unified Real Time Monitoring Tool client encounters an error while collecting one specific trace file and aborts trace collection.
CSCsj43460	Cisco Unified Real Time Monitoring Tool : Page Not Yet Implemented occurs on huntlist search.
CSCsj62464	User cannot use Cisco Unified Real Time Monitoring Tool for trace collection
CSCsj77307	RTMT critical services window does not display services.
CSCsj42329	Device search page does not refresh correctly for unregistered devices.
Component: Serv SOAP	
CSCsj72802	SOAP services return incorrect states to Service Manager on status requeue.
Component: Server Web Pages	
CSCsj69249	Successful doServiceActivation includes no return code 0 in ServMResponse.
Component: Syslog	
CSCsj84944	Fresh Install:CiscoSyslogSubA core (cxa_call_unexpected).
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(x) documentation suite was released.

Note Find the only new documentation updates for this release in the "Omissions" section on page 59

- Omissions, page 59
- Errors, page 63
- Updates, page 65
- Changes, page 68

Omissions

This section provides information that the Cisco Unified CallManager Release 5.1(x) documentation does not provide.

Added for Cisco Unified CallManager Release 5.1(2b) Release Notes

Cisco Unified CallManager Release 5.1(2b) Release Notes add the following section.

- Deleting a Server, page 59

Added Previous to Cisco Unified CallManager Release 5.1(2b) Release Notes

The following sections contain omissions that were noted in previous 5.1(x) releases of Cisco Unified CallManager.

- CTI Monitored Lines, page 61
- Call Throttling and the Code Yellow State, page 61
- New Column in the User Options Find and List Directory Entries Window, page 63
- Searching for a Device in Cisco Unified Real Time Monitoring Tool with the Any Status Option, page 63
- Planning Your Software MTP Configuration, page 63
- Ad Hoc Conference Settings Restrictions for SIP Phones, page 63

Deleting a Server

Cisco Unified CallManager Administration Guide and *Cisco Unified CallManager System Guide* do not provide correct information on deleting a server.

In Cisco Unified CallManager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you can delete a subsequent node, in the Find and List Servers window, Cisco Unified CallManager Administration displays the following message: "You are about to permanently delete one or more servers. This action cannot be undone. Continue?" If you click **OK**, the server gets deleted from the Cisco Unified CallManager database and is not available for use.

When you attempt to delete a server from the Server Configuration window, a similar message displays. If you click **OK**, the server gets deleted from the Cisco Unified CallManager database and is not available for use.

Deleting a Server - Important Notes

If you delete a subsequent node (subscriber) from Cisco Unified CallManager Administration be aware of the following information:

Caution Read the following information before you perform the procedure.

Disregard the entire “Deleting a Server” section, in the System-Level Configuration Settings chapter in the *Cisco Unified CallManager System Guide*.

Instead, consider the following information when you delete a server.

- Cisco Unified CallManager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.
- Cisco recommends that you do not delete any node that has Cisco Unified CallManager running on it, especially if the node includes devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified CallManager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified CallManager Administration.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.

To Add the Server Back

Perform the following procedure to add the deleted server back.

Step 1 In Cisco Unified CallManager Administration, add the server, as described in the "Configuring a Server" section (Server Configuration chapter) in the *Cisco Unified CallManager Administration Guide*.

Step 2 After you add the subsequent node to Cisco Unified CallManager Administration, perform an installation on it by using the installation disk that Cisco provided in your software kit.

Note Make sure that the version that you install on the subsequent node matches the version that runs on the first node (publisher) in the cluster.

Caution If the first node in the cluster runs a service release (or engineering special), you must choose the Upgrade During Install option when the installation displays the installation options; before you choose this option, ensure that you can access the service release (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, refer to *Installing Cisco Unified CallManager 5.1*(x).

Step 3 After you install Cisco Unified CallManager, configure the subsequent node, as described in the "Installing Cisco Unified CallManager" section in *Installing Cisco Unified CallManager 5.1(1)*.

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

Call Throttling and the Code Yellow State

Call throttling allows Cisco Unified CallManager to automatically throttle (deny) new call attempts when it determines that various factors, such as heavy call activity, low CPU availability to Cisco Unified CallManager, routing loops, disk I/O limitations, disk fragmentation or other such events, could result in a potential delay to dial tone (the interval users experience from going off hook until they receive dial tone).

This section provides the following information about call throttling:

- Introducing Call Throttling, page 61
- Troubleshooting Call Throttling, page 62
- Related Topics, page 62

Introducing Call Throttling

Call throttling occurs automatically when Cisco Unified CallManager determines such conditions to be present, and the system exits throttling automatically when such conditions are alleviated. You can configure the parameters that are associated with entering and exiting call throttling through several service parameters in Cisco Unified CallManager Administration (**System > Service Parameters**) although Cisco does not advise modification of these parameters unless recommended by Cisco customer support. See the Service Parameters Configuration chapter in the *Cisco Unified CallManager Administration Guide* for information on accessing and configuring service parameters.

Cisco Unified CallManager uses the values that are specified in the call-throttling-related parameters to evaluate the possibility of a delay to dial tone and also to determine when conditions no longer necessitate call throttling. When throttling is necessary to prevent excessive delay to dial tone, Cisco Unified CallManager enters a Code Yellow state, and new call attempts are throttled (denied). You can disable call throttling via the System Throttle Sample Size service parameter, but Cisco does not recommend disabling call throttling. The following list defines several of the call throttling-related service parameters:

- Code Yellow Entry Latency defines the maximum allowable delay, in milliseconds, to handle SDL messages that are sent to Cisco Unified CallManager by the various devices in the system as well as the wealth of internal messages that are received and sent by Cisco Unified CallManager for various activities such as KeepAlives, change notification, and many more types of internal messaging. If the calculated average expected delay is more than the value that is specified in this service parameter, Cisco Unified CallManager enters a Code Yellow state to initiate call throttling and stops accepting new calls.
- Code Yellow Exit Latency Calculation determines the acceptable percentage of Code Yellow Entry Latency to specify exit criteria for leaving the Code Yellow state (Code Yellow exit latency) when Cisco Unified CallManager has initiated call throttling. The basis for the value that you specify in this parameter comprises a formula that uses the value in the Code Yellow Entry Latency parameter, which specifies the delay in milliseconds. To arrive at a percentage, use the following formula: Code Yellow Entry Latency value multiplied by the Code Yellow Exit Latency value. For example:

  Code Yellow Entry Latency service parameter value: 20 msec

Code Yellow Exit Latency service parameter value: 40%

Code Yellow Exit Latency value = 20 X 0.4 = 8 msec, which means Cisco Unified CallManager exits Code Yellow state if the calculated message latency drops to 8 msec or lower.

To get out of the Code Yellow state, Cisco Unfied CallManager ensures that the average expected delay is less than the value of the Code Yellow exit latency.

- Code Yellow Duration specifies the number of minutes that a Cisco Unified CallManager system can remain in a Code Yellow state (call throttling). If this duration is met and the system is still in Code Yellow state, Cisco Unified CallManager enters a Code Red state, which indicates that Cisco Unified CallManager has remained in a Code Yellow state for an extended period and cannot recover. When Cisco Unified CallManager enters a Code Red state, the Cisco CallManager service restarts, which also produces a memory dump that may be helpful for analyzing the failure.
- System Throttle Sample Size indicates the size of the sample, in seconds, that is used to calculate the average expected delay for Cisco Unified CallManager to handle an SDL message. For example, a sample size of 10 means that Cisco Unified CallManager must calculate a non-zero latency value for 10 consecutive seconds before it will calculate the average expected delay and compare it to the value in the CodeYellow Entry Latency parameter. You can disable call throttling via this parameter.

When delay to dial tone is calculated to be over the threshold that is configured in the call-throttling-related service parameters, Cisco Unified CallManager begins rejecting new calls. When call throttling is engaged, a user who attempts a new call will receive reorder tone and, depending on the phone model, may also receive a prompt on the phone display. Call throttling effectively avoids the problem in which a user tries to place a new call, but the length of delay between going off hook and receiving dial tone is excessive enough to cause a reaction in the user (such as complaining to the system administrator or questioning whether the system is down or the phone is broken, for example). Cisco Unified CallManager uses a complex algorithm to constantly monitor the system to anticipate when such latency could occur.

When the delay to dial tone is within the guidelines of the call-throttling-related service parameters, Cisco Unified CallManager ceases throttling calls by exiting the Code Yellow state, and new calls events are again allowed.

Troubleshooting Call Throttling

CCM/SDI and SDL trace files record call throttling events and can provide useful information. Also, you generally will require performance monitoring data for debugging. The Cisco CallManager System Performance object (viewable in the Real-Time Monitoring Tool) includes a counter called ThrottlingSampleActivity, which indicates whether Cisco Unified CallManager has calculated a non-zero value for latency and helps you understand how busy the system is. Frequent non-zero values in this counter could indicate a potential overload condition on the system. To try to circumvent the possibility of a Code Yellow event, consider the possible causes of a system overload, such as heavy call activity, low CPU availability to Cisco Unified CallManager, routing loops, disk I/O limitations, disk fragmentation, or other such events and begin to investigate those possibilities.

Generally, repeated call throttling events require assistance from the Cisco Technical Assistance Center (TAC). TAC will request these trace files for closer examination.

Related Topics

For more information, see the following document:

- Service Parameters Configuration in the *Cisco Unified Communications Manager Administration Guide*

New Column in the User Options Find and List Directory Entries Window

Under Cisco Unified CallManager User Options, the Find and List Directory Entries window contains a new column. This column displays LDAP extension information. The extension number in this column may or may not match the extension number that is shown in the Extension column.

Searching for a Device in Cisco Unified Real Time Monitoring Tool 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, and so on) in RTMT. When you see multiple entries of a device, the current status of the device appears as the entry that has the latest timestamp. You can configure the 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 *Cisco Unified CallManager System Guide*, Media Termination Points chapter, does not include the following information:

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 Unified IP Phones that are using SIP (7911, 7941, 7961, 7970, 7971) can create an ad hoc conference, Cisco Unified IP Phone 7940, Cisco Unified IP Phone 7960, and third-party SIP phones can only be participants.

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

- 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 receive the beep; when a participant drops from the ad hoc conference, a user on a SIP phone may not receive the beep beep. The beeps may not be received because of the time that it takes to reestablish connections for the conference.

Errors

This section provides information about errors that are contained in the Cisco Unified CallManager Release 5.1(x) documentation.

- Alphanumeric Characters Allowed in the Pickup Group Name Field, page 64

Alphanumeric Characters Allowed in the Pickup Group Name Field

The *Cisco Unified Communications Manager Features and Services Guide* incorrectly states that you can enter up to 30 alphanumeric characters in the Pickup Group Name field in the Call Pickup Group Configuration window. The guide should state that you can enter up to 100 characters in the Pickup Group Name field.

Cisco Unified CallManager Features and Services Guide Indicates Support for Disks of Less Than 72GB

The following text, which does not apply, was removed previously from the 5.0(4) Cisco Unified CallManager Administration documentation. The text was left in the 5.1(2) version by mistake. The 5.1(2) version has now been corrected on Cisco.com to remove the text that no longer applies.

URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a0080739bf0.html#wp1093632

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

Part: *Cisco Unified CallManager Features and Services Guide*

Chapter: Music on Hold (Revised 04/30/2007)

Topic: Storing Audio Source Files

Removed information

The following considerations also apply:

- Cisco Unified CallManager supports up to five MOH audio sources on 36- or 40-gigabyte, disk-based systems. Systems with 72- or 80-gigabyte disks support the entire 50 audio streams.
- To increase the number of audio sources that Cisco Unified CallManager supports, install a larger disk during upgrade.

Corrected information

Cisco Unified CallManager, Release 5.0(x) and later, supports hard drives of 72 GB or greater for storing audio source files.

External Route Wizard

Although External Route Wizard is no longer available in Cisco Unified CallManager, the documentation still appears in the *Cisco Unified CallManager System Guide*, in the Understanding Route Plans chapter.

Media Resource Group

The Media Resource Group Configuration and Media Resource Group List Configuration chapters in the *Cisco Unified Communications Administration Guide* imply that any changes to the configuration require that you click the **Reset Devices** button to reset all affected phones. In fact, you need to reset the devices only when you have changed the name of the media resource group or media resource group list.

Survivable Remote Site Configuration

The Survivable Remote Site Configuration chapter in the *Cisco Unified CallManager Administration Guide* presents the configuration fields out of order in the SRST Reference Configuration Settings table. The correct order follows:

- SRST Reference Name
- Port
- IP Address (followed by the remaining fields that are documented in the correct order)

Updates

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

- Changing HostName/IP Address During an Upgrade, page 65
- SNMP Vendor-Specific MIBs, page 65
- Name Change, page 67
- Cisco Extension Mobility, page 67
- CAPF System Interactions and Requirements, page 68

Changing HostName/IP Address During an Upgrade

Upgrading Cisco Unified CallManager Release 5.1(1) states that when you make a DMA backup from a Cisco Unified CallManager Release 4.x system and restore it during a Cisco Unified CallManager Release 5.1(x) installation, you can enter any IP address or hostname for the publisher server and it will overwrite the IP address or hostname in the DMA file.

This functionality includes two restrictions that were not stated in the documentation:

1. You cannot assign an IP address that is already in use in the cluster.
2. You cannot assign a hostname that is already in use in the cluster.

If you attempt to assign an IP address or hostname that is in use in the cluster, the cluster will fail. Correcting this problem requires manual database manipulation.

SNMP Vendor-Specific MIBs

Supported with 5.1(2), the following guides do not contain the correct information on vendor-specific MIBs: *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)* and the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*. When working with SNMP, use the following information about vendor-specific MIBs.

Tip

The following MIB exist on various Cisco MCS, depending on vendor and model number. To query these MIB, you can use the standard MIB browsers that are developed by the hardware vendors; for example, HP Systems Insight Manager (SIM), IBM Director Server+Console, and Dell Open Manage. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 10—Describes supported IBM MIBs
- Table 11—Describes supported HP MIBs
- Table 12—Describes supported Dell MIBs

Table 10 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 11 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events

Table 11 HP MIBs (continued)

MIB	OID	Description
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

Table 12 Dell MIBs

MIB	OID	Description
Supported for browsing and system traps		
MIB-Dell-10892	1.3.6.1.4.1.674.10892.1	Provides hardware component assets/status/events
StorageManagement-MIB	1.3.6.1.4.1.674.10893.1	Provides disk/RAID asset data
MIB-Dell-CM	1.3.6.1.4.1.674.10899	Provides operating system, BIOS, firmware data

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)*.

Cisco Extension Mobility

The following information is supplementary to the information provided in the Cisco Extension Mobility chapter of the *Cisco Unified CallManager Manager Features and Services Guide*:

When subscribing devices to the Extension Mobility IP Phone Service (**Device > Device Settings > Phone Services**), clicking **Update Subscriptions** more than once can result in an error. When there are many phones requiring update, it can take some time for the changes to propagate to all devices.

You must click **Update Subscriptions** only once and wait for this propagation to complete.

CAPF System Interactions and Requirements

This section in the Using the Certificate Authority Proxy Function chapter of the *Cisco Unified Communications Manager Security Guide* requires this new item:

If a secure phone gets moved to another cluster, the Cisco Unified Communications Manager will not trust the LSC certificate the phone sends because it was issued by another CAPF, whose certificate is not in the CTL file. To enable the secure phone to register, delete the existing CTL file by using the "Deleting the CTL File on the Cisco Unified IP Phone" procedure in the *Cisco Unified CallManager Security Guide*. You can then use the Upgrade/Install option to install a new LSC certificate with the new CAPF and reset the phone for the new CTL file (or use the MIC). Use the Delete option in the CAPF section on the Phone configuration page to delete the existing LSC before the phones are moved.

Changes

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

- Recommended Number of Devices in Device Pool, page 68
- Updated Voice Gateway Model Information, page 68
- Number of Login or Logout Operations that Cisco Extension Mobility Supports, page 68

Recommended Number of Devices in Device Pool

The following information from the *Cisco Unified CallManager System Guide*, Redundancy chapter, needs clarification.

You associate devices with a Cisco Unified CallManager group by using device pools. You can assign each device to one device pool and associate each device pool with one Cisco Unified CallManager group. You can combine the groups and device pools in various ways to achieve the desired level of redundancy.

Note A server can exist in a single device pool and can support up to 7500 devices (high-end servers only). See your Cisco representative for information on the types of servers that Cisco Unified CallManager supports.

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.

Number of Login or Logout Operations that Cisco Extension Mobility Supports

The Cisco Unified CallManager Features and Services Guide, Release 5.0(4) (applicable to Release 5.1) does not correctly state the maximum number of login or logout operations that Cisco Extension Mobility supports for Release 5.1(2). The correct restriction follows:

Cisco Extension Mobility supports a maximum of 90 login or logout operations per minute (or 5400 operations per hour). Remember that these operations are sequential, not concurrent. (Some devices may support more login or logout operations per hour).

Note This data was obtained using 7845 3.4 GHz systems.

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.