CISCO SYSTEMS

Upgrading Cisco CallManager

Release 4.1(3)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
       800 553-NETS (6387)
Fax: 408 526-4100

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

The preface covers these topics:

- Purpose of Document, page vii
- Audience, page viii
- Conventions, page viii
- Locating Related Documentation, page viii
- Obtaining Documentation, page x
- Documentation Feedback, page xi
- Obtaining Technical Assistance, page xi
- Obtaining Additional Publications and Information, page xii

Purpose of Document

This document provides Cisco CallManager upgrade procedures and requirements for the Cisco Media Convergence Server and the customer-provided server that meets approved Cisco configuration standards.

This document contains information on the following topics:

- Preinstallation Information, page 1-1
- Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware), page 2-1
- Performing Post-Upgrade Tasks, page 3-1
- Reverting to the Previous Configuration After an Upgrade Attempt, page 4-1
- Upgrade Messages, page 5-1
- Replacing Servers During the Upgrade, page 6-1

Tip Use this document in conjunction with the documents that are listed in the "Locating Related Documentation" section on page viii.

Audience

The *Upgrading Cisco CallManager* document provides information for network administrators who are responsible for maintaining the Cisco CallManager system. This guide requires knowledge of telephony and IP networking technology.

Conventions

Consider the following documentation conventions as you review this upgrade document:

Unless otherwise specified, base server model numbers will be used in this document. For example references to the MCS-7835 apply to servers including the MCS-7835, the MCS-7835-1000, the MCS-7835-1266, the MCS 7835H-2.4, the MCS-7835I-2.4, MCS-7835H-3.0, MCS-7835I-3.0, the customer-provided DL380, and the customer-provided IBM xSeries 342 and 345.

Blue Text—To quickly navigate to a section or URL from your computer, click text that appears in blue.

Note	Reader, take note. Notes contain helpful suggestions or references to material not covered in the publication.

Caution	Reader, be careful. You may do something that could result in equipment damage or loss of data.

Timesaver	Reader, this tip saves you time as you perform the procedure.

(Required)

This convention indicates that you must perform the procedure. Failing to perform the procedure could cause a total system failure or a loss of data and configuration settings.

(Recommended)

This convention indicates that the procedure is strongly recommended, but not required.

Locating Related Documentation

Cisco strongly recommends that you review the following documents before you upgrade:

- *Release Notes for Cisco CallManager Release 4.1*

  Cisco provides a version of this document that matches the version of the upgrade document. Use this document as a companion guide to the upgrade document.

- *Cisco CallManager Compatibility Matrix*

  To ensure continued functionality with interfacing Cisco IP telephony applications after the Cisco CallManager upgrade, refer to the *Cisco CallManager Compatibility Matrix,* which provides information and workarounds for applications that are integrated with Cisco CallManager.

Affected applications may include Cisco Conference Connection, Cisco SoftPhone, Cisco uOne, Cisco 186 Analog Telephony Adaptor, Cisco Personal Assistant, Cisco Customer Response Solutions (CRS), Telephony Application Programming Interface and Java Telephony Application Programming Interface (TAPI/JTAPI) applications, including Cisco-provided and third-party applications, and Cisco Telephony Service Provider (TSP).

If you use Cisco CallManager and related Cisco IP telephony applications in a call-center environment, review this document before you begin any upgrade procedures.

- Third-party application compatibility information

  Before you upgrade Cisco CallManager, verify that all the Cisco-provided and Cisco-approved applications that run in your network are compatible with this version of Cisco CallManager.

- *Cisco IP Telephony Operating System, SQL Server, Security Updates*

  This document provides information on the latest operating system, SQL Server, and security support updates. Information in this document applies to servers that are running the following Cisco IP telephony applications: Cisco CallManager, Conference Connection, Personal Assistant, and Cisco Customer Response Applications/Solutions, and so on.

- *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide 4.0(1)* (or later)

  This document describes how to install the BARS utility, configure the backup settings, back up Cisco CallManager data, and restore the data/server.

  This document also provides a list of files that the utility backs up. This utility does not back up operating system files, except for Hosts/LMHosts files, if those files exist on the server.

- *Cisco CallManager Security Guide*

  This document provides step-by-step instructions on how to configure and troubleshoot authentication and encryption for Cisco CallManager, Cisco IP Phones, SRST references, and Cisco MGCP gateways.

- The appropriate Cisco IP telephony application documentation

  Locate the release notes, installation/upgrade, and configuration guides for the applications that you have integrated with Cisco CallManager.

Click the URLs in Table 1 to locate the appropriate documentation and related software.

Table 1   Quick Reference for URLs

Related Information and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation (not readme documentation)	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco AVVID Partner Program Compatibility Information	http://www.cisco.com/pcgi-bin/ecoa/Search

Table 1   Quick Reference for URLs (continued)

Related Information and Software	URL and Additional Information
Cisco AVVID Technology Affiliate Program Compatibility Information	http://www.cisco.com/pcgi-bin/ecoa/Search?isAffil=Y
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco CallManager, SQL Server, and operating system service releases, upgrades, and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **Note** The operating system and SQL Server 2000 service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
Cisco CallManager Security Guide	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/a e/index.htm
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

    http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

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

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

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

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

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

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

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

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

Preinstallation Information

This section provides information that you should consider before upgrading a Cisco CallManager server and frequently asked questions (FAQs) regarding the Cisco CallManager 4.1 upgrade.

Important Considerations

Before you proceed with the Cisco CallManager installation or upgrade, consider the following requirements and recommendations:

- Cisco CallManager requires a minimum of 1GB of memory on the Cisco CallManager servers. To avoid system problems, such as dropped calls, verify that your servers have a minimum of 1 GB of memory installed. If the installation process detects less than 1GB memory on the publisher server, the installation aborts. The installation process performs a similar check on the Cisco CallManager subscriber server; it allows the installation to continue if it detects less than the minimum requirement.

- Install the Cisco CallManager software on the publisher server first and then on the subscriber server(s).

- You cannot add a subscriber server to a cluster by installing a previous version of Cisco CallManager and then upgrading the subscriber server to the same version that is running on the publisher server. If you are adding a new subscriber server or replacing a subscriber server on the cluster, you must use the installation CDs with the same Cisco CallManager version that is running on the publisher server.

- Make sure that you are logged in as the administrator on the server before starting the Cisco CallManager installation.

- Install the Cisco CallManager software on one server at a time to ensure that subscriber servers can receive replicate copies of the database from the publisher database server.

- Make sure that the subscriber server that you are installing can connect to the publishing database server during the installation.

- Do not choose cancel after you start the installation. If you choose cancel, you will need to reimage your machine by reinstalling the operating system.

- Because security settings for the Cisco CallManager server are set up by the installation and upgrade script, do not make any adjustments to these predefined settings, or you may experience a significant impact to the functionality of your server.

- When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, use alphanumeric characters only.

- Enter the same administrator password on all servers in the cluster.
- Install the Cisco CallManager software during off-peak hours or during a maintenance window to avoid impact from call-processing interruptions.
- Do not implement multiple servers in a Cisco CallManager cluster by using a drive that was mirrored or cloned from a single Cisco CallManager server. This results in servers having duplicate Security ID (SID) and impairs Cisco CallManager operations. You must install the Cisco IP telephony operating system and Cisco CallManager software separately on each server by using the Cisco-provided installation disks.
- Do not configure any server in the cluster as a Domain Controller.
- Place the server in a Workgroup before you install the software.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco IP Phones can register with the application when you plug the phones into the network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not use terminal services to install the Cisco CallManager software
- Do not install any Cisco-verified applications until you complete installing Cisco CallManager on every server in the cluster.
- Cisco provides support for a limited set of applications on the servers where Cisco CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.
- You must disable third-party, Cisco-verified applications on your servers before starting the Cisco CallManager installation.
- Install a security agent to protect your servers against unauthorized intrusion.
- Do not install Cisco Unity on a server where Cisco CallManager is installed.
- Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.
- Carefully read the instructions that follow before you proceed with the installation. See "Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware)" section on page 2-1 and "Performing Post-Upgrade Tasks" section on page 3-1.

Frequently Asked Questions About Cisco CallManager 4.1 Upgrades

The following frequently asked questions apply for all Cisco CallManager 4.1 upgrades.

From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 4.1(3)?

To verify which versions of Cisco CallManager are compatible for upgrade, refer to the *Cisco CallManager Compatibility Matrix*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

If your server runs a version of Cisco CallManager Release 3.2 or earlier, you must first upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.3 before you can upgrade to a version of Cisco CallManager Release 4.1. For information on upgrading to Cisco CallManager Release 3.3 or 4.0, refer to the appropriate version of the *Upgrading Cisco CallManager* document. You cannot upgrade directly from Cisco CallManager Release 3.2 or earlier to Cisco CallManager Release 4.1.

Before you perform any upgrade procedures, Cisco strongly recommends that you install the latest operating system upgrade/service release, SQL service releases/hotfixes, and Cisco CallManager service release for the versions that currently run in the cluster. Cisco provides the service release and corresponding readme documentation on cisco.com. To obtain these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

⚠
Caution   Cisco recommends that you only upgrade to Cisco CallManager 4.1(3) from a version that is compatible for upgrade to 4.1(3). Versions that are not compatible for upgrade to 4.1(3) may contain features that are not supported in 4.1(3). If you upgrade from an unsupported version, you will not be able to access those features that are not supported in 4.1(3) and you will lose the data that is associated with those features.

Which servers and operating system versions does Cisco support for this upgrade?

For Cisco CallManager Release 4.1(3), Cisco supports the servers listed in the *Cisco CallManager Compatibility Matrix*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.

Cisco recommends that you install Cisco-provided operating system version 2000.2.7 with the latest service release 2000.2.7.sr2 (or later) before you upgrade to Cisco CallManager Release 4.1(3).

For Cisco CallManager 3.3 Upgrades to 4.1(3)

If your server runs Cisco CallManager 3.3 and operating system version 2000.2.3 (or later), you can use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to 2000.2.7sr2 or later. For detailed instructions, refer to "Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware)" section on page 2-1.

For Cisco CallManager 4.0 Upgrades to 4.1(3)

If your server runs Cisco CallManager 4.0, you can use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to 2000.2.7sr2 or later. For detailed instructions, refer to "Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware)" section on page 2-1

Which third-party applications does Cisco support for this upgrade?

The Cisco AVVID Partner Program and Technology Affiliate Program require Interoperability Verification Testing (IVT) for all named AVVID Partners' and Affiliates' applications and products for major releases of Cisco CallManager. If you upgrade to this version of Cisco CallManager before IVT is completed, you may experience performance and compatibility issues with some Cisco-approved, third-party applications that run in your network. Before you upgrade Cisco CallManager, verify that all

the Cisco-provided and Cisco-approved applications that run in your network are compatible with this version of Cisco CallManager. Cisco-provided and Cisco-approved third-party applications include, but are not limited to, Cisco IP Contact Center, Cisco Emergency Responder, IVR, and so on.

Cisco strongly recommends that you do not upgrade to this version of Cisco CallManager until compatibility exists. After the compatible application becomes available, upgrade Cisco CallManager and then the application(s).

To determine if compatibility testing has been completed for a Cisco-approved third-party applications and products, refer to the following URLs.

Cisco AVVID Partner Program

http://www.cisco.com/pcgi-bin/ecoa/Search

Enter the name of the company for which you want to search and then click **Search**.

To see a list of third-party, Cisco-verified applications that may be installed on the server with Cisco CallManager, choose **IP Telephony i**n the Solution pane and then choose **Operations, Administration, and Maintenance (OAM)** in the Solution Category drop-down list box.

Cisco AVVID Technology Affiliate Program

http://www.cisco.com/pcgi-bin/ecoa/Search?isAffil=Y

Enter the name of the company for which you want to search and then click **Search.**

Caution   Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.

Tip   To obtain the latest list of compatible Cisco AVVID applications, refer to the Cisco CallManager Compatibility Matrix at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Caution   Cisco supports a limited list of applications on the servers where Cisco CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.

Which server in the cluster do I upgrade first?

Caution   When you perform the Cisco CallManager portion of the upgrade, you must upgrade one server at a time, so the subscriber servers can pull the replicas of the database from the publisher database server. For the subscriber servers to pull the replicas, the publisher database server must be running, and you must not make any changes on the publisher database server while you are upgrading the subscriber servers. After you complete the upgrade on one server and reboot the server, you can start the upgrade on the next server.

Caution   This document assumes that all servers are functional and running. If the servers are not functional and running, failover will not occur.

You must upgrade all the servers in the cluster. The order varies depending on the cluster configuration.

Cisco CallManager Runs on the Publisher

If the Cisco CallManager service runs on the publisher database server (two-server cluster), upgrade the servers in the following order:

1. Upgrade the publisher database server.

When you perform an upgrade, the Cisco CallManager service automatically stops, and the devices that are homed to the publisher database server failover to the subscriber server.

2. Upgrade the subscriber.

Cisco CallManager Does Not Run on the Publisher

If the Cisco CallManager service does not run on the publisher database server, upgrade the servers in the following order:

1. Upgrade the publisher database server.

2. Upgrade the Cisco TFTP server, if it exists separately from the publisher database server.

3. Upgrade servers, one server at a time, that have only Cisco CallManager-related services (Music on Hold, Cisco IP Media Streaming Application, and so on) running on them.

Make sure that you upgrade only one server at a time.

Make sure that the Cisco CallManager service does not run on these servers.

4. Upgrade each secondary server, one server at a time.

If you choose to oversubscribe the secondary server(s) during the upgrade, Cisco strongly recommends that you have no more than 5,000 devices that are registered to the secondary server during the upgrade and that you oversubscribe the secondary server(s) for no more than a few hours. Cisco strongly recommends that you perform the upgrade during off-peak hours when low call volume occurs (less than 1,000 busy hour call attempts).

If you configured your Cisco CallManager cluster by using approved Cisco configuration standards, which include configuring four primary servers and two secondary servers in the cluster, you can minimize call-processing interruptions if you register all devices to servers that are running the same version of Cisco CallManager during the entire upgrade process; for example, you register all devices to the secondary Cisco CallManager servers or the primary Cisco CallManager servers, but not to both types of servers.

5. Upgrade each primary server that has the Cisco CallManager service running on it. Remember to upgrade one server at a time.

⚠ **Caution** When you upgrade the primary server(s), call-processing interruptions may occur for up to 30 minutes while the devices attempt to obtain the device loads and register to the upgraded version of Cisco CallManager.

6. Upgrade servers that have Cisco IP telephony applications running on them; for example, Cisco Conference Connection or Cisco Emergency Responder. Remember to upgrade one server at a time. Refer to the application documentation for more information.

How does a coresident upgrade work if I have CRS installed with Cisco CallManager?

For information on how to perform the upgrade on a coresident server, refer to the CRS documentation that is compatible with this version of Cisco CallManager.

How long does it take to upgrade the cluster?

To minimize call-processing downtime, Cisco strongly recommends that you perform all upgrade procedures for the Cisco CallManager and all upgrades/reinstallations for Cisco IP telephony applications within a consecutive time period (within one maintenance window).

Before you perform an upgrade, consider the time that it takes to perform pre-/post-upgrade tasks, Cisco IP telephony application upgrades/reinstallations, and Cisco-verified application upgrades/reinstallations.

For the time that it takes to perform specific tasks on the publisher database server, see Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware), page 2-1

Will I experience call-processing interruptions and a loss of services during the upgrade?

Review the following information before you upgrade.

About Minimizing Call-Processing Interruptions

When you upgrade a cluster, two separate versions of Cisco CallManager run in the cluster at the same time. Be aware that the different Cisco CallManager versions that are running in the cluster will not interact and may cause call-processing interruptions to occur.

If you configured your Cisco CallManager cluster by using approved Cisco configuration standards, which include configuring four primary servers and two backup servers in the cluster, you can minimize call-processing interruptions if you register all devices to servers that are running the same version of Cisco CallManager during the entire upgrade process; that is, you register all devices to the backup Cisco CallManager servers or the primary Cisco CallManager servers, but not to both types of servers.

About a Loss of Services

During the upgrade, Cisco CallManager places Cisco CallManager-related services that display in Cisco CallManager Serviceability in an inactive state. After the upgrade completes, migrated services activate and start after the server reboots. To use additional services, you must activate the service on each server on which you want the service to run. For information on activating services, refer to the *Cisco CallManager Serviceability Administration Guide* or to online help in the Cisco CallManager application.

⚠

Caution   Cisco strongly recommends that you perform the upgrade during a single maintenance window to minimize call-processing interruptions.

May I use Terminal Services, Virtual Network Computing, and Integrated Lights Out to remotely upgrade the server?

Do not use Terminal Services or Integrated Lights Out (ILO) to upgrade to Cisco CallManager Release 4.1(3). Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote administration and troubleshooting tasks. Cisco does not support upgrades through Terminal Services.

⚠️
Caution   Before the upgrade, Cisco strongly recommends that you disable Terminal Services and immediately reboot the server to prevent remote access to the server. Accessing the server via Terminal Services may cause the upgrade to fail.

After you upgrade the server, you must enable Terminal Services.

If you want to use Virtual Network Computing (VNC) to remotely upgrade the publisher database server, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm to obtain the latest version of the VNC document.

⚠️
Caution   If you have installed VNC but do not plan to use it to perform the upgrade, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the upgrade, the upgrade will fail.

Do not use Integrated Lights Out (ILO) to perform upgrade or installation tasks. Cisco supports ILO for remote management and configuration tasks only.

May I add Cisco CallManager servers as members of a Windows domain?

Cisco does not recommend adding Cisco CallManager servers as members of a Microsoft Windows domain. However if your system architecture is dependent on servers joining a Windows domain, then you must disable the Network Time Protocol (NTP) software that is installed by Cisco CallManager when you add the server as a member of a domain and use Microsoft time service. You must disable the NTP service on every server in your cluster.

✎
Note   You must install the server as a member of a workgroup during installation of Cisco CallManager.

✎
Note   Do not make any modifications to the installed NTP configuration file (NTP.CONF). Modifications to the NTP.CONF file may result in synchronization problems with CDRs, Traces, Event Logging, and so on. Cisco does not support these modifications.

To disable the Cisco-installed NTP software on a server:

Step 1   Choose **Start > Programs > Administrative Tools > Services**.

Step 2   Double-click the **Network Time Protocol** service.

Step 3   In the Startup type field, choose **Disabled**.

Step 4   Click **Stop**.

Step 5   Click **OK**

⚠

Caution   Every time that you upgrade your server, you must remove the server from the Windows Domain prior to installing the upgrade software.

When you complete your upgrade and you are adding the server to the Windows domain, you must disable the Cisco-installed NTP services again.

If you are joining the server to a Microsoft Windows 4.0 domain, you must also perform an additional procedure for synchronizing time. Refer to *How to Synchronize the Time on a Windows 2000-Based Computer in a Windows NT 4.0 Domain* at http://www.microsoft.com.

May I configure a server in the cluster as a Domain Controller?

Do not configure any server in the cluster as a Domain Controller. If you configure any server in the cluster as a Domain Controller, you cannot upgrade or reinstall Cisco CallManager on the server.

May I perform configuration tasks during the upgrade?

⚠

Caution   Do not attempt to perform any configuration tasks during the upgrade. Before the upgrade begins, disable all services that allow any administrator to perform remote configuration tasks. For example, disable Terminal Services or VNC before the upgrade to prevent an administrator from browsing into the server during the upgrade.

Notify all users that the upgrade is occurring, so users do not browse into the server during the upgrade.

Performing configuration tasks during the upgrade causes an upgrade failure.

May I remove a drive before I upgrade?

⚠

Caution   You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or customer-provided IBM xSeries 330 server.

Removing a Drive and Inserting a Replacement Drive and Drive Mirroring Prior to the Upgrade

The "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 2-12 describes how to properly perform this task.

Removing a Drive and Upgrading With One Drive In the Server

Perform the following procedure if you plan to remove a drive and upgrade with only one hard drive in the server.

Step 1 Power off the publisher database server.

Step 2 For all servers except the MCS-7845, remove the hard drive from Slot 0 and label the drive with the machine name, slot number, and current version of Cisco CallManager.

For the MCS-7845, remove the drives from Slot 0 and Slot 2 and label them with the appropriate information.

Step 3 Power on the system.

Cisco MCS

Step 4 Perform the following procedure for the Cisco MCS (The MCS-7845 requires two spare hard drives):

   a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

> **Note** The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

   b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845. When prompted, press **F1** to continue.

Step 5 Log in to the server by using the Administrator password.

IBM xSeries Server

Step 6 To enable interim recovery mode on the customer-provided IBM xSeries 342 server, press **F5**.

Step 7 Log in to the server by using the Administrator password.

Which Cisco IP telephony applications may I install on the Cisco CallManager server?

Consider the following information before you install other software besides Cisco CallManager on the Cisco MCS or the customer-provided server:

- You can install a compatible version of Cisco Customer Response Solutions (CRS), which you must purchase separately from Cisco CallManager.

- Do not install Cisco Unity, Cisco Conference Connection, Cisco Personal Assistant, or Cisco Emergency Responder on the server where Cisco CallManager is installed.

- Cisco strongly recommends that you install a security agent to protect your servers against unauthorized intrusion. Cisco offers two security agent options: Cisco Security Agent (CSA) for Cisco CallManager and Management Center for Cisco Security Agent (CSA MC).

   CSA for Cisco CallManager designates a standalone agent and security policy that is designed to be used on all servers in the voice cluster. The policy that is included with this agent gets configured specifically for Cisco CallManager and Customer Response Applications (CRA), and you cannot update or view it. You can download the agent from CCO at http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des.

If you want to add, change, delete, or view rules and policies that CSA for Cisco CallManager includes, or if you want to add support for non-Cisco approved, third-party applications, you must purchase and install the fully managed console, CSA MC. CSA MC requires a separate dedicated server to be used as the management center. This management center allows you to create agent kits that are then distributed to agents that are installed on other network systems and servers.

To access information on Cisco Security Agent, see http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm and http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/csa_4_0/index.htm

⚠
Caution   If you are uncertain whether a Cisco IP telephony application is supported on the Cisco CallManager server, do not install it.

What additional information should I know before I upgrade?

This document assumes that all servers in your cluster are currently in an operational state.

About Security and Account Policies

⚠
Caution   If you change any security or account policies from the default, the upgrade may fail. For more information on security and account policies, refer to Microsoft documentation.

About Service and Enterprise Parameters in Cisco CallManager Administration

Cisco CallManager always updates service parameters with non-numeric values to the suggested value.

If your service parameters are set to the suggested value, Cisco CallManager automatically updates the value during the upgrade to match the new suggested value.

If your customized value exists between the range of minimum and maximum values, Cisco CallManager does not change the customized value.

If you configured customized values that are not between the minimum and maximum range of values, the customized value changes during the upgrade to the maximum or minimum value. For example, if the maximum value equals 10 and the value that you configured is 12, Cisco CallManager automatically sets the value to 10.

During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters).

About H.323 Intercluster Trunks

A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to more than one H.323 intercluster trunk in Cisco CallManager Administration. You must assign a unique device name to each H.323 intercluster trunk. Refer to the *Cisco CallManager Administration Guide* for information on the trunk configuration procedure.

About H.323 Gateways

Cisco no longer provides the Run H.225D On Every Node option in Cisco CallManager Administration for H.323 gateways. Before you upgrade, verify that all H.323 dial-peer(s) point to a Cisco CallManager server in the device profile for which they are assigned. If the session target statements in the dial-peer(s) do not point to the appropriate Cisco CallManager server, calls fail.

About the Database

After you upgrade Cisco CallManager, the database name automatically increments; for example, from CCM0300 to CCM0301. Third-party CDR software may have SQL triggers that are hard coded to the original database name. The triggers may point to the previous database name and cause all CDR flat files to write to the BAD directory on the publisher database server. If you need technical assistance with this issue, directly contact the third-party software vendor.

When should I perform post-upgrade tasks?

Do not perform any post-upgrade tasks until you complete the upgrade on all servers in the cluster.

What if I encounter problems during the upgrade?

Cisco recommends that if you encounter problems during the upgrade, take the following actions:

1. During the upgrade if you receive an error message that displays in a dialog box, see the "Upgrade Messages" section on page 5-1 and perform the recommended corrective action.

2. Obtain and review all log files (*.log and *.txt) from the following directories:

   • C:\Program Files\Common Files\Cisco\Logs

   • C:\Program Files\Common Files\Cisco\Directory

   • C:\Install\DBInstall

   • C:\Dcdsrvr\log

Be aware that not all error messages that display in the log file are catastrophic. MSI generates error messages in the log file for many reasons; for example, attempts to access a service that Cisco CallManager does not use.

Upgrading Your Cisco CallManager Server (When You Are Not Replacing Hardware)

You cannot upgrade directly from Cisco CallManager Release 3.2 or earlier to Cisco CallManager Release 4.1. If your server runs a version of Cisco CallManager Release 3.2 or earlier, you must first upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.3 or 4.0 before you can upgrade to a version of Cisco CallManager Release 4.1. For information on upgrading to Cisco CallManager Release 3.3, refer to the latest version of *Upgrading Cisco CallManager Release 3.3*.

✎
Note   If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.1(3) software kit.

If you are upgrading from Cisco CallManager 4.0, you can upgrade by using the disks from the Cisco CallManager 4.1(3) software kit or by using the web download file.

To verify which versions of Cisco CallManager are compatible for upgrade, refer to the *Cisco CallManager Compatibility Matrix*.

You must upgrade Cisco CallManager on the publisher database server and all subscriber servers in the cluster. For the order of the upgrade, see the "Which server in the cluster do I upgrade first?" section on page 1-4.

Before You Begin

Before you start the upgrade, make sure that you perform the following tasks:

	Pre-Upgrade Task	Important Notes
Step 1	Make sure that you run a recommended version of Cisco CallManager on all servers in the cluster.	From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 4.1(3)?, page 1-2
Step 2	Make sure that you understand the order in which you must upgrade the cluster.	Which server in the cluster do I upgrade first?, page 1-4
		How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-6

	Pre-Upgrade Task	**Important Notes**
Step 3	In Cisco CallManager Administration, make sure that you add each server only once on the Server Configuration window (**System > Server**). If you add a server by using the host name and add the same server by using the IP address, Cisco CallManager cannot accurately determine component versions for the server after a Cisco CallManager upgrade. If you have two entries in Cisco CallManager Administration for the same server, delete one of the entries before you upgrade.	Refer to the *Cisco CallManager Administration Guide*.
Step 4	Make sure that your server configuration supports this upgrade.	Which servers and operating system versions does Cisco support for this upgrade?, page 1-3
Step 5	Make sure that you have enough free disk space on each of your servers for the Cisco CallManager upgrade. If you use the Cisco CallManager disks to upgrade, you need 2.0 gigabytes of disk space. If you use the web file to upgrade, you need 3.0 gigabytes of disk space.	
Step 6	If you are using Cisco Unity as your voice-messaging system, configure the voice mail ports in Cisco CallManager to ensure proper migration.	For more information, refer to the *Release Notes for Cisco CallManager*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 7	You must assign a unique device name to each H.323 intercluster trunk. A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to H.323 intercluster trunks in Cisco CallManager Administration.	Refer to the *Cisco CallManager Administration Guide* for information on the trunk configuration procedure.
Step 8	Verify that all H.323 dial-peer(s) point to a Cisco CallManager server in the device profile for which they are assigned. Cisco no longer provides the Run H.225D On Every Node option in Cisco CallManager Administration for H.323 gateways. If the session target statements in the dial-peer(s) do not point to the appropriate Cisco CallManager server, calls fail.	Refer to the *Cisco CallManager Administration Guide* for information on the gateway configuration procedure.

	Pre-Upgrade Task	Important Notes
Step 9	Perform the recommended backup procedures for all coresident software applications that are installed on the server. ⚠ **Caution** Failing to complete a backup causes a loss of data and configuration settings. For information on performing the backup, refer to the documentation that supports the applications. The Cisco IP Telephony Backup and Restore System (BARS) does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	How does a coresident upgrade work if I have CRS installed with Cisco CallManager?, page 1-6
Step 10	Be aware that if you change any security or account policies from the default, the upgrade may fail.	For more information on security and account policies, refer to Microsoft documentation.
Step 11	Understand how Cisco CallManager updates service parameters. **For Service Parameters with Nonnumeric Values** Cisco CallManager always updates service parameters with non-numeric values to the suggested value. **For Service Parameters with Numeric Values** If your service parameters are set to the suggested value, Cisco CallManager automatically updates the value during the upgrade to match the new suggested value. If your customized value exists between the range of minimum and maximum values, Cisco CallManager does not change the customized value. If you configured customized values that are not between the minimum and maximum range of values, the customized value changes during the upgrade to the maximum or minimum value. For example, if the maximum value equals 10 and the value that you configured is 12, Cisco CallManager automatically sets the value to 10. During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters).	For more information on service parameters, refer to the *Cisco CallManager Administration Guide* and the *Cisco CallManager System Guide*.

	Pre-Upgrade Task	Important Notes
Step 12	If you are upgrading a Cisco CallManager 4.0 server and you installed certificates on the phones that are using the Certificate Authority Proxy Function (CAPF) server, you must migrate existing the CAPF data.	Migrating Existing CAPF Data, page 2-4
Step 13	Close all web browser windows.	If you have an open browser window, Cisco CallManager will reboot the server after the Sun Microsystem JRE package has been installed.
Step 14	Verify that all Cisco CallManager Extension Mobility users have logged out of the system prior to the upgrade.	If there are still extension mobility users who are still logged in during the upgrade, they may not be able to use all the features on their phone until they log off and log back in.
Step 15	Before the upgrade, obtain the local Administrator account password, the SQL server SA password, the Private Password Phrase, and the computer name of the publisher database server.	Information That You May Need During the Upgrade, page 2-6
Step 16	Before the upgrade, perform basic connectivity and functional testing of any current Cisco AVVID Partner/Affiliate applications and products in your current (pre-upgrade) environment. Document the tests you perform and the results for use in the post-upgrade procedures.	
Step 17	Obtain and review any required Cisco AVVID Partner/Affiliate versions of software and documentation necessary to support this version of Cisco CallManager.	Which third-party applications does Cisco support for this upgrade?, page 1-3

Migrating Existing CAPF Data

⚠

Caution   Failing to perform the tasks that are described in this section may cause a loss of CAPF data.

Review the following details before you upgrade Cisco CallManager:

- Upgrades from Cisco CallManager 4.0 where CAPF was installed on the Cisco CallManager 4.0 publisher database server—If you performed certificate operations before the upgrade to Cisco CallManager 4.1 and CAPF ran on the publisher database server, the latest operation status migrates to the Cisco CallManager 4.1 database.

- Upgrades from Cisco CallManager where CAPF was installed on a Cisco CallManager 4.0 subscriber server—If you performed certificate operations before the upgrade to Cisco CallManager 4.1 and CAPF ran on a subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade the cluster to Cisco CallManager 4.1.

Copying CAPF 1.0(1) Data from a 4.0 Subscriber Server to the 4.0 Publisher Database Server

⚠️

Caution   If you installed CAPF utility 1.0(1) on a Cisco CallManager 4.0 subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade to Cisco CallManager 4.1. Failing to perform this task causes a loss of CAPF data; for example, you may lose the phone record files in C:\Program Files\Cisco\CAPF\CAPF.phone. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones; CAPF 4.1(1) must reissue the certificates, which are not valid.

To copy the files, perform the following procedure:

Procedure

Step 1   Copy the files in Table 2-1 from the machine where CAPF 1.0 is installed to the publisher database server where Cisco CallManager 4.0 is installed:

Table 2-1   Copy From Server to Server

Files to Copy	From Machine Where CAPF 1.0 Is Installed	To Publisher Database Server Where Cisco CallManager 4.0 Is Installed
*.0	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\Certificates
CAPF.phone	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF
CAPF.cfg files	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF

Step 2   Upgrade every server in the cluster to Cisco CallManager 4.1.

Step 3   After you upgrade the cluster to Cisco CallManager 4.1, upgrade the Cisco CTL client and run it before you use the phones. The Cisco CTL client will copy the CAPF certificate to all the servers in the cluster.

Step 4   Delete the CAPF utility that you used with Cisco CallManager 4.0. See Table 2-1.

Information That You May Need During the Upgrade

Use the information in the following table when you perform the upgrade procedures.

⚠

Caution   When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, enter alphanumeric characters only. The account password must match on every server in the cluster. For each of the accounts, you must enter the same password on every server in the cluster.

The upgrade prompts you for a Private Password Phrase. The upgrade uses the string that you enter to create a unique, encrypted password. You must enter the same phrase on all servers in the cluster.

Table 2-2   Information That You May Need During the Upgrade

Data	Your Entry
Destination where the backup file is stored during the backup	
WorkGroup Name	
Name of your organization	
Computer name of the publisher database server	
Local Administrator account password (same password for all servers in cluster)	
LDAP (DC) Directory Manager password (same password for all servers in cluster)	
SQL Server SA password (same password for all servers in cluster)	
Private Password Phrase for the cluster (same phrase for all servers in cluster)	

Upgrading the Cisco CallManager Publisher Database Server

Review the following upgrade tasks, designated time to perform the task, and the location where you obtain the procedure:

	Task	Procedure	Designated Time
Step 1	Verify that you have performed all pre-upgrade tasks.	See the "Before You Begin" section on page 2-1 and the"Information That You May Need During the Upgrade" section on page 2-6.	Depends on the size of the cluster
Step 2	Remove all servers in the cluster from the NT Domain or the Microsoft Active Directory Domain.	See the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 2-9.	Depends on the size of the cluster
		Tip You can perform this task on all servers in the cluster at the same time.	
Step 3	Manually disable and stop all platform agents, Cisco-verified applications (Cisco AVVID Partner Applications), and Cisco-provided coresident applications that run on the servers in the cluster. Reboot the server.	Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-approved McAfee services), intrusion detection (for example, Cisco Security Agent), and remote management services, ensures that the upgrade does not encounter issues that are associated with these services.	20 minutes
		See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 2-10.	
		Tip You can perform this task on all servers in the cluster at the same time.	
Step 4	Manually install and configure the CIPT Backup and Restore System (BARS), version 4.0(7) (or later).	If you have not already done so, Cisco recommends that you install and configure the backup utility on the publisher database server.	15 minutes
		The CIPT Backup and Restore System (BARS) does not back up any operating system files except Host/LMhost, if these files exist on the server. For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	
Step 5	Using the Backup and Restore System (BARS), version 4.0(7) (or later), manually back up the Cisco CallManager data to either a network directory or tape drive.	For information on backing up your system, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.	30 to 60 minutes, depending on the size of the Cisco CallManager and Call Detail Record (CDR) database
		Tip To significantly improve the speed of the Cisco CallManager upgrade, archive or remove CDRs before backing up your system.	

	Task	Procedure	Designated Time
Step 6	Run the Cisco CallManager Upgrade Assistant Utility on all servers in the cluster. You must perform this task on one server in the cluster at a time, beginning with the publisher database server.	The Cisco CallManager Upgrade Assistant Utility verifies that your server is in a healthy state before the upgrade. Perform this task on one server in the cluster at a time, beginning with the publisher database server. See the "Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)" section on page 2-12.	1 to 20 minutes for the publisher database server; 1 to 5 minutes for the subscriber server
Step 7	If the server supports drive removal, remove a drive from the server to save your data and configuration.	See the "Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)" section on page 2-12.	15 to 60 minutes, depending on the server type
Step 8	Use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to Cisco-provided version 2000.2.7 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. Perform on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.	45 to 75 minutes per server, depending on the server type
Step 9	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-7sr2 or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	15 minutes
Step 10	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page. For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.	5 minutes
Step 11	Verify that you installed Microsoft SQL Server 2000, Service Pack 3a (or later).	For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack. **Tip** Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.	20 minutes

	Task	Procedure	Designated Time
Step 12	Upgrade Cisco CallManager.	If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.1(3) software kit.	45 to 120 minutes per server, depending on the server type
		If you are upgrading from Cisco CallManager 4.0(x), you can upgrade by using the disks from the Cisco CallManager 4.1(3) software kit or by using the web download file.	
		⚠ **Caution** You must perform the Cisco CallManager installation serially; that is, on one server at a time. After you reboot the server and after you verify that the server pulled the subscription from the publisher database server, you can begin the upgrade on the next server.	
		See the "Inserting the Disk or Downloading the Web File" section on page 2-14	
Step 13	Upgrade all of the subscriber servers in the cluster.	See the "Upgrading the Cisco CallManager Subscriber Server(s)" procedure on page 2-17.	Depends on the size of the cluster.
		Note You cannot add a subscriber server to a cluster by installing a previous version of Cisco CallManager and then upgrading the subscriber server to the same version that is running on the publisher server. If you are adding a new subscriber server or replacing a subscriber server on the cluster, you must use the installation CDs with the same Cisco CallManager version that is running on the publisher server.	

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

🔍
Tip   You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

⚠
Caution   When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1   Choose **Start > Settings > Control Panel > System**.

Step 2   Click the **Network Identification** tab.

Step 3   Click the **Properties** button.

Step 4   Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5   Click **OK**.

Step 6   When prompted to do so, reboot the server.

Step 7   Log in to the server by using the Administrator password.

Step 8   Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9   Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip   You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1   Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2   From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, Network Associates Task Manager, or McAfee Framework Service and choose **Properties**.

> ✎
> **Note**   The name of the antivirus service depends on the version of your antivirus software.

Step 3   In the Properties window, verify that the General tab displays.

Step 4   In the Service Status area, click **Stop**.

Step 5   From the Startup type drop-down list box, choose **Disabled**.

Step 6   Click **OK**.

Step 7   Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8   Reboot the server and verify that the services are not running.

> ⚠
> **Caution**   Make sure that the services do not start after the reboot.

> ⚠
> **Caution**   If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Install and Configure CIPT Backup and Restore (BARS) Version 4.0(7) (or Later) (Strongly Recommended)

If you have not already done so, Cisco recommends that you install and configure the backup utility on the publisher database server. The CIPT Backup and Restore System (BARS) does not back up any operating system files except for Host/LMhost, if these files exist on the server.

For a list of files that the utility backs up, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Back Up Existing Data (Strongly Recommended)

For information on backing up your system, refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Run the Cisco CallManager Upgrade Assistant Utility on All Servers in the Cluster (Strongly Recommended)

Tip   You must perform this task on one server in the cluster at a time, beginning with the publisher database server.

The reboot may cause call-processing interruptions.

Item Needed: Web Download of Utility

Run the latest Cisco CallManager Upgrade Assistant Utility to verify that your server is in a healthy state before the upgrade. The document that posts next to the utility on the web provides detailed information about the utility. To obtain the latest version of the utility and the document, perform the following procedure:

Procedure

Step 1   Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2   Click **Cisco CallManager Version 4.1**.

The Cisco CallManager 4.1 software page displays.

Step 3   Locate and download the document.

Step 4   Using the document as a reference, download and run the utility on every server in the cluster where Cisco CallManager is installed.

Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended)

Item Needed: Newly Purchased Hard Drive

You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or the customer-provided IBM xSeries 330 server.

After you verify that you have a good backup of the data, you can remove a drive to save configured data; however, you must insert a replacement drive into the server before you begin the operating system procedures. This task may require that you purchase a new drive.

This process may take between 30 minutes to 60 minutes, depending on the size of the drive.

Perform the following steps to remove a drive, to insert a replacement drive, and to mirror the drives:

Procedure

Step 1   Power off the publisher database server.

Step 2   For all servers except the MCS-7845, remove the hard drive from Slot 0 and label the drive with the machine name, slot number, and current version of Cisco CallManager.

For the MCS-7845, remove the drives from Slot 0 and Slot 2.

Step 3   Power on the system.

Cisco MCS

Step 4   Perform the following procedure for the Cisco MCS (The MCS-7845 requires two spare hard drives.):

    a.   To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

Note   The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

    b.   This step applies only for the MCS-7830, MCS-7835, or MCS-7845.

       When prompted, press **F1** to continue.

    c.   After Windows 2000 finishes booting, insert the replacement hard drive in Slot 0.

Note   On the MCS-7845, do not insert the replacement drive into Slot 2 until the mirror process completes for the drive in Slot 0.

    d.   On the MCS-7830, MCS-7835, or MCS-7845, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**. When the Array Configuration Utility Warning window opens, click **OK**.

    e.   Watch the status bar in the lower, right corner to determine when the mirroring process completes.

    f.   This step applies for the MCS-7845 only.

       After the mirroring process completes in Slot 0, insert the next drive into Slot 2. The mirroring process launches automatically after you insert the drive into Slot 2.

IBM xSeries Server

Step 5   Perform the following procedure for the IBM xSeries server:

    a.   Insert a replacement drive into Slot 0.

    b.   Press **F5**.

    c.   Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.

Upgrade the Operating System to Cisco-Provided Version 2000.2.7 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.7 with the latest service release 2000.2.7sr2 (or later) before you upgrade to Cisco CallManager Release 4.1(3).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-7sr2 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Install Microsoft SQL Server 2000, Service Pack 3a (Required)

For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack.

Tip   Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.

Inserting the Disk or Downloading the Web File

Note   If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.1(3) software kit.

If you are upgrading from Cisco CallManager 4.0(x), you can upgrade by using the disks from the Cisco CallManager 4.1(3) software kit or by using the web download file.

Note   Critical third-party components that are required and installed by Cisco CallManager might require multiple reboots during installation, and you may need to manually restart the installation program and re-enter the configuration data.

Items Needed: Cisco CallManager 4.1(3) Installation and Recovery Disk or Cisco CallManager 4.1(3) web download file

Perform the following procedure:

Procedure

Step 1   If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator password.

Step 2   Choose whether you want to upgrade via disk or the web.

- Using the Disk, Step 3 through Step 4
- Using the Web File, Step 5 through Step 10

Using the Disk

Step 3   Locate the Cisco CallManager 4.1 Installation, Upgrade, and Recovery Disk 1 of 2 and insert it into the drive.

The installation process automatically starts.

> 🔍
> **Tip**   Do not remove the disk until you are directed to do so by procedure.

Step 4   Continue the installation by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Using the Web File

Step 5   Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6   Click **Cisco CallManager Version 4.1**.

Step 7   Download the Cisco CallManager 4.1(3) upgrade file to your hard drive.

Step 8   Note the location where you save the downloaded file.

Step 9   Double-click the downloaded file to begin the installation.

Step 10   A message displays that you run this file for web upgrades only. Click **Yes**.

Step 11   Continue the upgrade by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Upgrading Related Cisco CallManager Services and Detecting the Server (Required)

Continue the upgrade by performing the following procedure.

> ✏️
> **Note**   If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator account.

Procedure

Step 1   To confirm which version of Cisco CallManager you are upgrading from and which version you are upgrading to, click **Yes**.

Step 2   To confirm that you have disabled antivirus and intrusion detection software, click **Yes**.

If you have not installed Microsoft SQL 2000 Service Pack 3a (or a later version), an error message displays. To obtain the service pack and corresponding readme documentation, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

> **Tip**   If you just installed the service pack, you must insert the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again after the service pack installs and the server reboots; continue to wait while the Cisco IP telephony application prepares to install.

Step 3   To confirm that you might be prompted to reboot the server and re-enter configuration data multiple times in order for Cisco CallManager to install critical third-party components, click **OK**.

Step 4   The installation program must update the configuration and restart the server. To proceed with installation, click **OK.**

> **Note**   If you click **Cancel**, Cisco CallManager will not be installed on your server and the installation program will not make any changes to your system.

The server reboots.

Step 5   Log in to the server by using the Administrator account and password.

Step 6   The Preparing to Install window displays while the installation program copies files to your server. This process takes approximately 10 minutes. Do not click Cancel.

Step 7   The Resuming the Installation Wizard window displays. Click **Next**.

Step 8   Enter the administrator password. Click **Next**.

Step 9   Enter the private password phrase for the cluster; confirm the private password phrase, and click **Next**.

Step 10   To begin the installation, click **Install**.

The status window displays. Do not click Cancel.

> **Note**   The progress of the status bar may reset as each software package is being installed and as the installation program configures your machine. You may see the installation program reset the status bar multiple times. Do not reboot the server unless the installation prompts you to do so.

Step 11   If you are using the Cisco CallManager 4.1(3) installation disks, a message displays that indicates that you need to insert the next upgrade disk. Perform the following steps:

   a.   Insert the Cisco CallManager 4.1(3) Installation, Upgrade, and Recovery Disk 2 and click **OK**.

      A message displays that indicates that you need to install the first upgrade disk again.

   b.   Insert the Cisco CallManager 4.1(3) Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**.

Step 12   Click **Finish**.

Step 13   Click **Yes**.

Upgrading the Cisco CallManager Subscriber Server(s)

> **Note**   You cannot add a subscriber server to a cluster by installing a previous version of Cisco CallManager and then upgrading the subscriber server to the same version that is running on the publisher server.   If you are adding a new subscriber server or replacing a subscriber server on the cluster, you must use the installation CDs with the same Cisco CallManager version that is running on the publisher server.

Perform the following tasks to upgrade the subscriber servers.

	Task	Important Information and Resources
Step 1	Perform pre-upgrade tasks.	See the "Before You Begin" section on page 2-1 and the "Information That You May Need During the Upgrade" section on page 2-6.
Step 2	Verify that you removed all servers from the NT or Microsoft Active Directory Domain.	See the "Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)" section on page 2-19.
Step 3	Verify that you have disabled and stopped all third-party, Cisco-verified, and Cisco-provided coresident applications that run on the server. Make sure that you have rebooted the server.	See the "Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)" section on page 2-20.
Step 4	**Optional Task** Run the ServPrep utility.	You can only run the utility via the Cisco CallManager Subscriber Preparation Disk. Cisco does not provide this utility on the web. See the "Run the ServPrep Utility (Optional)" section on page 2-21.
Step 5	Use the operating system upgrade CD-ROM or the operating system upgrade web download to upgrade the operating system to Cisco-provided version 2000.2.7 (or later).	Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml. ⚠ **Caution** If you choose to do so, you can upgrade the operating system on all subscriber servers in the cluster at the same time. This task causes call-processing interruptions.

	Task	Important Information and Resources
Step 6	Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-7sr2 or later). (Required)	The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
		For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.
Step 7	Download and install the latest OS-related security hotfixes, if any. (Recommended)	The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
		For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.
Step 8	Verify that you installed Microsoft SQL Server 2000, Service Pack 3a (or later).	For information on how to verify install the service pack, refer to the readme documentation that accompanies the service pack.
		⚠ **Caution** This task causes call-processing interruptions.

	Task	Important Information and Resources
Step 9	**Task That You Should Perform Serially** Perform the Cisco CallManager upgrade on one server at a time.	⚠️ **Caution** While you are upgrading a subscriber server, do not reboot the publisher server. If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.1(3) software kit. If you are upgrading from Cisco CallManager 4.0(x), you can upgrade by using the disks from the Cisco CallManager 4.1(3) software kit or by using the web download file. ⚠️ **Caution** You must perform the Cisco CallManager installation serially; that is, on one server at a time. After you reboot the server and after you verify that the server pulled the subscription from the publisher database server, you can begin the upgrade on the next server. You use the same Cisco CallManager Installation, Upgrade, and Recovery Disks or web download for the publisher database server and subscriber servers. See the "Inserting the Disk or Downloading the Web File" section on page 2-23
Step 10	After you complete the installation on all servers in the cluster, perform post-upgrade tasks.	See the "Performing Post-Upgrade Tasks" section on page 3-1.

Remove the System from the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured)

🔍
Tip   You can perform this task on all servers in the cluster at the same time.

The reboot causes call-processing interruptions if done at the same time.

⚠️
Caution   When a server exists in a domain during an upgrade, authentication between servers may fail, or the non-default domain security policies may restrict Cisco CallManager from building critical NT accounts. Failing to remove the system from the domain and add it to a work group may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Do not place the servers back into the domain until you have completed the upgrade procedures for every server in the cluster.

Convert any servers that exist in the NT Domain or Microsoft Active Directory Domain by performing the following procedure:

Procedure

Step 1 Choose **Start > Settings > Control Panel > System**.

Step 2 Click the **Network Identification** tab.

Step 3 Click the **Properties** button.

Step 4 Click the **Workgroup** radio button and enter a name, for example, WRKGRP, in the corresponding field.

Step 5 Click **OK**.

Step 6 When prompted to do so, reboot the server.

Step 7 Log in to the server by using the Administrator password.

Step 8 Perform this procedure on every server in the cluster that exists in the NT Domain.

Step 9 Go to the Domain Controller and remove the computer accounts for the Cisco CallManager servers in the cluster.

Disable and Stop Third-Party, Cisco-Verified, and Cisco-Provided Coresident Applications and Reboot the Server (Required)

Tip You must perform this task on all servers in the cluster at the same time.

The reboot may cause call-processing interruptions.

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click http://www.cisco.com/pcgi-bin/ecoa/Search. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

The following platform agents may interfere with the Cisco CallManager installation: antivirus services, intrusion detection services (for example, Cisco Security Agent), OEM server agents, server management agents, VOIP monitoring/performance monitoring, or remote access/remote management agents. Disabling platform agents and services, such as performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), intrusion detection, and remote management services, ensures that you do not encounter issues that are associated with these services.

This document provides procedures for disabling Cisco-verified McAfee antivirus services only. If you need assistance with disabling other services or applications, refer to the corresponding documentation that accompanies the product.

To disable the McAfee antivirus services, perform the following tasks:

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2   From the Services window, right-click one of the antivirus services; that is, Network Associates Alert Manager, Network Associates McShield, Network Associates Task Manager, or McAfee Framework Service and choose **Properties**.

> ✎
> **Note**   The name of the antivirus service depends on the version of your antivirus software.

Step 3   In the Properties window, verify that the General tab displays.

Step 4   In the Service Status area, click **Stop**.

Step 5   From the Startup type drop-down list box, choose **Disabled**.

Step 6   Click **OK**.

Step 7   Perform Step 1 through Step 6 for all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.

Step 8   Reboot the server and verify that the services are not running.

> ⚠
> **Caution**   Make sure that the services do not start after the reboot.

> ⚠
> **Caution**   If Cisco-verified antivirus or intrusion detection software is not currently installed on the server, Cisco strongly recommends that you do not install the software until you complete the entire upgrade/installation of all servers in the cluster.

Run the ServPrep Utility (Optional)

Item Needed: Cisco CallManager Subscriber Upgrade Disk 1

Before you install Cisco CallManager, you must run the ServPrep utility and install Cisco IP Telephony Operating System by using the Cisco-provided operating system disks and upgrade to the latest operating system 2000.2.7sr2 (or later).

The ServPrep utility, which you run on subscriber servers, updates the network configuration by creating the file, STISys.inf, which contains network information. The utility saves TCP/IP settings, but you lose manually configured NIC settings; for example, hard-coded Speed/Duplex settings. After you complete the installation on all servers in the cluster, you must manually configure previous NIC settings.

> ⚠
> **Caution**   This utility supports all Cisco Media Convergence Servers, customer-provided HP DL320 and DL380 servers, and customer-provided IBM xSeries 330, 340, 342, and 345 servers that meet Cisco-approved configuration standards. Do not run this utility on any other servers, including customer-provided servers.

Procedure

Step 1   Insert the Cisco CallManager Subscriber Upgrade Disk 1 into the drive as soon as you can do so.

Step 2   When the Upgrade Warning window displays, carefully read the information and click the **ServPrep Utility** link at the bottom of the window.

Step 3   Run the program from the current location; follow the prompts that display.

Upgrade the Operating System to Cisco-Provided Version 2000.2.7 (or Later) (Required)

Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Perform the upgrade on the publisher database server first; complete the Cisco CallManager upgrade on the publisher database server before you upgrade the operating system on the subscriber servers.

Cisco recommends that you upgrade to install Cisco IP Telephony operating system version 2000.2.7 with the latest service release 2000.2.7sr2 (or later) before you upgrade to Cisco CallManager Release 4.1(3).

Download and Install the Latest Cisco IP Telephony Server Operating System Service Release (Required)

Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-7sr2 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Download and Install the Latest OS-Related Security Hotfixes (If Any) (Recommended)

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Install Microsoft SQL Server 2000, Service Pack 3a (Required)

For information on how to verify and install the service pack, refer to the readme documentation that accompanies the service pack.

Tip Install this service pack on the publisher database server; complete the Cisco CallManager upgrade on the publisher database server before you install this service pack on the subscriber servers.

Inserting the Disk or Downloading the Web File

Note If you are upgrading from Cisco CallManager 3.3, you must use the disks from the Cisco CallManager 4.1(3) software kit.

If you are upgrading from Cisco CallManager 4.0(x), you can upgrade by using the disks from the Cisco CallManager 4.1(3) software kit or by using the web download file.

Note Critical third-party components that are required and installed by Cisco CallManager might require multiple reboots during installation, and you may need to manually restart the installation program and re-enter the configuration data.

Items Needed: Cisco CallManager 4.1(3) Installation and Recovery Disk or Cisco CallManager 4.1(3) web download file

Perform the following procedure:

Procedure

Step 1 If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator password.

Step 2 Choose whether you want to upgrade via disk or the web.

- Using the Disk, Step 3
- Using the Web File, Step 5 through Step 10

Using the Disk

Step 3 Locate the Cisco CallManager 4.1 Installation, Upgrade, and Recovery Disk 1 of 2 and insert it into the drive.

The installation process automatically starts.

Tip Do not remove the disk until you are directed to do so by procedure.

Step 4 Continue the upgrade by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Using the Web File

Step 5 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6 Click **Cisco CallManager Version 4.1**.

Step 7 Download the Cisco CallManager 4.1(3) upgrade file to your hard drive.

Step 8 Note the location where you save the downloaded file.

Step 9 Double-click the downloaded file to begin the installation.

Step 10 A message displays that you run this file for web upgrades only. Click **Yes**.

Step 11 Continue the installation by proceeding to "Upgrading Related Cisco CallManager Services and Detecting the Server (Required)" section.

Upgrading Related Cisco CallManager Services and Detecting the Server (Required)

Continue the upgrade by performing the following procedure:

Note If you did not log in to the server after the operating system upgrade, log in to the server by using the Administrator account.

Procedure

Step 1 To confirm which version of Cisco CallManager you are upgrading from and which version you are upgrading to, click **Yes**.

Step 2 To confirm that you have disabled antivirus and intrusion detection software, click **Yes**.

If you have not installed Microsoft SQL 2000 Service Pack 3a (or a later version), an error message displays. To obtain the service pack and corresponding readme documentation, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Tip If you just installed the service pack, you must insert the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again after the service pack installs and the server reboots; continue to wait while the Cisco IP telephony application prepares to install.

Step 3 To confirm that you might be prompted to reboot the server and re-enter configuration data multiple times in order for Cisco CallManager to install critical third-party components, click **OK**.

Step 4 The installation program must update the configuration and restart the server. To proceed with installation, click **OK.**

Note If you click **Cancel**, Cisco CallManager will not be installed on your server and the installation program will not make any changes to your system.

The server reboots.

Step 5 Log in to the server by using the Administrator account and password.

Step 6 The Preparing to Install window displays while the installation program copies files to your server. This process takes approximately 10 minutes. Do not click Cancel.

Step 7 The Resuming the Installation Wizard window displays. Click **Next**.

Step 8 Enter the administrator password. Click **Next**.

Step 9 Enter the private password phrase for the cluster; confirm the private password phrase, and click **Next**.

Step 10 To begin the installation, click **Install**.

The status window displays. Do not click Cancel.

> **Note** The progress of the status bar may reset as each software package is being installed and as the installation program configures your machine. You may see the installation program reset the status bar multiple times. Do not reboot the server unless the installation prompts you to do so.

Step 11 If you are using the Cisco CallManager 4.1(3) installation disks, a message displays that indicates that you need to insert the next upgrade disk. Perform the following steps:

  a. Insert the Cisco CallManager 4.1(3) Installation, Upgrade, and Recovery Disk 2 and click **OK**.

    A message displays that indicates that you need to install the first upgrade disk again.

  b. Insert the Cisco CallManager 4.1(3) Installation, Upgrade, and Recovery Disk 1 of 2 and click **OK**

Step 12 Click **Finish**.

Step 13 Click **Yes**.

> **Tip** Repeat the procedures in the "Upgrading the Cisco CallManager Subscriber Server(s)" section on page 2-17 on each subscriber server until you have upgraded all the servers in your cluster. After you update all of the servers, perform the appropriate procedures in the "Performing Post-Upgrade Tasks" section on page 3-1.

Performing Post-Upgrade Tasks

After you complete the upgrade, perform the appropriate tasks as described below:

	Post-Upgrade Task	Related Information and Procedures
Step 1	Cisco CallManager installation sets the default recovery setting for Cisco CallManager services to automatically restart the service when a failure is detected. Verify the default failure response of any services that you have previously changed.	See the "Default Recovery Setting" section on page 3-4.
Step 2	Verify that the subscriber servers pulled the copy of the database.	See the "Verifying and Reinitializing Subscriber Connections" section on page 3-5.
Step 3	Verify that all of the appropriate services started. Verify that you can make internal calls. Verify that you can place and receive a call across gateways.	See the "Verifying Services, Patches, and Hotfixes" section on page 3-6. See the "Reassigning Route Lists" section on page 3-7. ⚠ **Caution** If you have third-party software, such as CDR software, integrated with Cisco CallManager and the third-party software does not run as expected after the upgrade, verify that you entered the same SA password on all servers in the cluster.
Step 4	If you have CRS and Cisco CallManager installed on the same server, complete the upgrade by referring to the appropriate documentation.	See the "How does a coresident upgrade work if I have CRS installed with Cisco CallManager?" section on page 1-6.

	Post-Upgrade Task	Related Information and Procedures
Step 5	After you complete the Cisco CallManager upgrade on every server in the cluster, reinstall all Cisco-verified applications and all plug-ins that were previously installed on the server except the Cisco CDR Analysis and Reporting plug-in. For example, if you have integrated your enterprise directory with Cisco CallManager, you must reinstall the Cisco Customer Directory Configuration Plugin on all servers in the cluster after the upgrade, starting with the publisher database server. Reinstalling the plug-in populates your enterprise directory with any additional schema extensions and data entries that Cisco CallManager needs.	Refer to the appropriate documentation that accompanies the applications.
Step 6	Upgrade Cisco TAPI, Cisco JTAPI, Cisco TSP (for the voice-messaging system), and the Cisco TSP for Cisco SoftPhone.	See the following sections for more information: • Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP), page 3-10 • Upgrading the Cisco TAPI/TSP for Cisco SoftPhone, page 3-10
Step 7	If you have CRS or Cisco CallManager Extended Services installed, you must execute the JTAPI update utility to ensure that the JTAPI plug-in is installed properly.	See "Using the JTAPI Update Utility with CRS" section on page 3-10.
Step 8	If you are using Cisco Unity as your voice-messaging system, configure the appropriate settings to ensure proper failover.	For more information, refer to the *Release Notes for Cisco CallManager*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
Step 9	Verify that all Cisco IP telephony applications that are integrated with Cisco CallManager run properly. If you need to do so, upgrade the Cisco IP telephony applications that are integrated with your Cisco CallManager system.	Refer to the *Cisco CallManager Compatibility Matrix* by clicking the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm If the application is compatible with this version of Cisco CallManager, refer to the appropriate Cisco IP telephony application documentation.
Step 10	For your migrated version of Cisco CallManager Attendant Console to work, you must check the Call Park Retrieval Allowed check box for the ac user that you configured in the Global Directory. The attendant console does not initialize if you do not check this check box.	For more information on how to perform this task, refer to the *Cisco CallManager Administration Guide*.

	Post-Upgrade Task	Related Information and Procedures
Step 11	After you upgrade Cisco CallManager, the database name automatically increments; for example, from CCM0300 to CCM0301. Third-party CDR software may have SQL triggers that are hard coded to the original database name. The triggers may point to the previous database name and cause all CDR flat files to write to the BAD directory on the publisher database server.	If you need technical assistance with this issue, directly contact the third-party software vendor.
Step 12	If you want to use Norton AntiVirus, install the application and perform post-installation tasks.	Refer to *Using Symantec/Norton AntiVirus with Cisco CallManager.* Click the following URL to obtain the document: http://wwwin.cisco.com/voice/doc/symantec_antivirus_cm.pdf
Step 13	The locale, English_United_States, installs automatically on the server. To upgrade existing locales or to add additional locales to the server, install the Cisco IP Telephony Locale Installer.	You can obtain locale specific versions of the Cisco IP Telephony Network Locale installer for Cisco CallManager 4.1 when they become available at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml. Refer to the readme file that is posted next to the Cisco IP Telephony Locale Installer software for the complete list of supported languages and localized features. For more information on installing the locale installer, refer to U*sing the Cisco IP Telephony Locale Installer.* **Note** The locale installer has version-specific support for Cisco CallManager releases.
Step 14	You must configure the Network Interface Card (NIC) Speed and Duplex settings of the Cisco CallManager server to match the configuration of the LAN switch port to which the server is connected. Failure to match these settings between the server and switch may cause degraded network performance and unexpected errors to occur. Contact your network administrator or see the Cisco IOS configuration documentation to determine your current settings of the LAN switch port to which the Cisco CallManager NIC is connected.	Some administrators have found that the 100/Full setting works well.
Step 15	Verify the version of hotfixes and service packs that are installed on the server. Download the latest hotfixes, service packs, and Cisco CallManager service release that are available on the web. This task requires a reboot of the server after you install the files. **Tip** Perform this task on an ongoing basis to maintain your system.	Verifying Services, Patches, and Hotfixes, page 3-6 Reassigning Route Lists, page 3-7 **Tip** The service releases may post to the web after the Cisco CallManager upgrade is available.

	Post-Upgrade Task	**Related Information and Procedures**
Step 16	If you are upgrading from Cisco CallManager Release 3.3(x) or 4.0(1) and had more than one primary Cisco CallManager server, you must reassign the route lists to Cisco CallManager groups that you configured if you wish to maintain an optimal load balance.	See the "Reassigning Route Lists" section on page 7.
Step 17	If you are administering Cisco CallManager servers from a PC that does not have Microsoft Java Machine, you will need to install and configure Sun Microsystems Java Virtual Machine (JVM) on the PC to ensure that Cisco CallManager Administration displays correctly. MSJVM installed by default in all client workstation versions of the current Windows operating systems, except for the following versions: • Windows XP Professional with SP1 slipstreamed into the installation • Windows 2000 Server/Professional with SP4 slipstreamed into the installation	See the "Requirement for Installation of Java Virtual Machine" section on page 3-7.
Step 18	Perform basic connectivity and functional testing of any current Cisco AVVID Partner/Affiliate products/applications in your current (post-upgrade) environment. If you find any issues, compare your post-upgrade test results with your documented pre-upgrade test results.	See the "Before You Begin" section on page 2-1

Default Recovery Setting

Cisco CallManager installation sets the default recovery setting on the following services to automatically restart the service when a failure is detected:

- Cisco Serviceability Reporter
- Cisco CallManager
- Cisco CTIManager
- Cisco TFTP
- Cisco Telephone Call Dispatcher
- Cisco Tomcat
- Cisco RIS Data Collector
- Cisco Messaging Interface

Cisco does not recommend changing the recovery setting on a live production system. If you want to change the default failure response of a service, you can set the recovery setting by choosing **Start > Settings > Control Panel > Service**.

Enabling Third-party Applications, Antivirus Services, or Security Agents

After you log in to the server, enable all third-party applications, antivirus services, or security agents through the Control Panel by completing the following procedure:

Procedure

Step 1   Choose **Start > Programs > Administrative Tools > Services.**

Step 2   Locate the third-party application, antivirus service, or security agent that you want to start, right-click the service, and choose Properties.

Step 3   In the Properties window, click the General tab.

Step 4   From the Startup type drop-down list box, choose **Automatic**.

Step 5   Click **OK.**

Step 6   In the Services window, right-click the application or service and click **Start**.

Verifying and Reinitializing Subscriber Connections

If the connections between the publisher database server and the subscribers within a cluster are broken for any reason, you cannot copy the database to the subscribers.

Verifying the Status of the Subscription

To determine whether the connections between the publisher database server and the subscribers within a cluster are broken, wait 35 minutes after you have installed the last subscriber in the cluster. Then, open SQL Server Enterprise Manager. If a red X icon appears next to the subscription, the subscription is broken.

Reinitializing the Subscription/Starting the Replication Snapshot Agent

If you determine that one or more subscription connections are broken, as indicated by the red X icon next to the subscriptions, reinitialize the subscriptions and start the replication snapshot agent on the publisher database server.

Procedure

Step 1   Open SQL Server Enterprise Manager by choosing **Start > Programs > Microsoft SQL Server > Enterprise Manager**.

Step 2   In the following path, choose the name of the publisher database that you are configuring: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Databases/<the publisher database name>Publications.

Step 3   In the main window, right-click the subscription name and choose **Reinitialize all Subscriptions**. Click **Yes** to confirm.

Step 4   In the following path, choose the **Snapshot Agents** folder: Microsoft SQL Servers/SQL Server Group/<this server's hostname>/Replication Monitor/Agents.

Step 5   Right-click the publication name that matches the database name that you are configuring; then, click **Start**.

In rare cases, the reinitialization of the subscriptions may not work. If you determine that the previous procedure did not work as expected, contact the team that provides technical assistance for this product; for example, your Cisco AVVID Partner or the Cisco Technical Assistance Center (TAC).

Verifying Services, Patches, and Hotfixes

Perform the following tasks:

- Verify that the appropriate services run on each server in the cluster (About Services, page 3-6)
- Verify that you have installed the latest Microsoft patches and hotfixes (About Microsoft Patches and Hotfixes, page 3-6)
- Verify that you have installed the latest Cisco CallManager service release (About Cisco CallManager Service Releases, page 3-6)

About Services

Open Cisco CallManager Serviceability and verify that all migrated services are running. To review service activation procedures and service recommendations, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Caution   Do not start and stop services through the Microsoft Computer Management window. Starting and stopping services through the window causes problems with the Cisco CallManager database.

About Microsoft Patches and Hotfixes

Refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

About Cisco CallManager Service Releases

After you install this version of Cisco CallManager on all servers in the cluster, Cisco strongly recommends that you install the latest Cisco CallManager service release on all servers in the cluster. These service releases provide bug fixes for your system.

Be aware that Cisco CallManager service releases are cumulative. Cisco rolls these bug fixes into the next Cisco CallManager release.

Tip   Make sure that you install the same version of the service release on every server in the cluster.

To obtain the latest Cisco CallManager service release, perform the following procedure:

Step 1 Click http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 2 Click **Cisco CallManager Version 4.1**.

The Cisco CallManager 4.1 software page displays.

Step 3 Locate and download the readme file for the service release.

The readme file provides procedures, caveats, and descriptive information for installing the files.

Step 4 Using the readme file as a reference, install the Cisco CallManager service release on every server in the cluster where Cisco CallManager is installed.

Reassigning Route Lists

If you had more than one primary Cisco CallManager server in a cluster and you are upgrading from Cisco CallManager Release 3.3(x) or 4.0(1) to Cisco CallManager 4.1(3), you will need to reassign the route list to the Cisco CallManager group that you configured in Cisco CallManager Administration to maintain optimal load balance. To ensure call processing redundancy, the upgrade program created a Cisco CallManager group containing a primary server and a backup server for every primary Cisco CallManager server in the cluster and then assigned route lists to each Cisco CallManager group using a round robin algorithm. The name format for the created Cisco CallManager group is RLCMG_<primary Cisco Callmanager name>.

Procedure

Step 1 Evaluate the Cisco CallManger group and route list configuration for load balancing and redundancy, as described in the *Cisco CallManager System Guide* and the *Cisco CallManager Network Solutions Design Guide.*

Step 2 Assign the route list(s) to the Cisco CallManger group(s) that you have configured in Cisco CallManager Administration.

Step 3 Delete the migrated CCM group, RLCMG_<primary CM-server-name>.

Requirement for Installation of Java Virtual Machine

The Microsoft Java Virtual Machine (MSJVM) technology allows Java applications to run on Microsoft Windows-based computers. Some versions of Microsoft Internet Explorer (a component of the Windows operating systems) included MSJVM, but Microsoft has discontinued distribution of MSJVM in its software and announced end-of-life support for the product.

MSJVM installed by default in all client workstation versions of the current Windows operating systems, except for the following ones:

- Windows XP Professional with SP1 slipstreamed into the installation
- Windows 2000 Server/Professional with SP4 slipstreamed into the installation

Note   Because the Cisco CallManager Administration windows depend on remote scripts, which depend on the JVM for web interaction, Cisco CallManager requires the use of JVM on the client machine to ensure that the Cisco CallManager Administration display correctly.

If your client machine runs MSJVM, you can continue to use the existing configuration to browse into the Cisco CallManager Administration windows and perform administration tasks.

If you do not have MSJVM installed on your client machine (or if you receive an error message stating that Cisco CallManager cannot detect JVM on the client machine), and you need to perform Cisco CallManager Administration tasks, you must install and configure the Sun Microsystems' Java Virtual Machine (JVM) on the client machine. (The Sun JVM is part of the Java 2 Runtime Environment—JRE.) In addition, you must configure the browser security to be Java-enabled. See the "JRE Installation" section on page 3-8 for information about installing JRE on the client machine.

If you are not sure if MSJVM is installed on the client machine, you can install the Sun J2RE anyway. You would then have two Java Runtime Environments installed and running on your machine.

Tip   If you run two separate JVM products (MSJVM and Sun J2RE) on your client machine, be sure to download and install patches and security updates for each JVM from the appropriate software vendor (Microsoft and Sun).

JRE Installation

As part of the Cisco CallManager installation, the system provides the Sun JRE client software in a zip file that is installed on the Cisco CallManager server.

Note   Windows XP/XP Professional includes a built-in tool that handles zip files. If you use Windows 2000 as your operating system, you must obtain a separate compression utility (such as WinZip) to store and access zip files.

Tip   Be sure you install Cisco IP Telephony operating system version 2000.2.7 with the latest service release 2000.2-7-sr2 (or later) before you upgrade to Cisco CallManager release 4.1(3).

To install the JRE software for the client PC, follow these steps:

Procedure

Step 1   From the Cisco CallManager server, navigate to the **C:\utils\JRE** directory and search for the J2RE_Client_<jre version>.zip file.

The following example shows the zip file name:

J2RE_Client_1.4.2_05.zip

> **Note**   Only the Cisco CallManager Administrator can access the JRE software on the
> Cisco CallManager server; to enable access to other users, copy the J2RE_Client_<jre
> version>.zip file to a server that all users can share.

Step 2   Right-click the **J2RE_Client_<jre version>.zip** file and click **Copy** to copy the file to your client PC.

Step 3   Double-click the **J2RE_Client_<jre version>.zip** file to unzip the Sun J2RE installation executable.

Step 4   Double-click the installation executable file on the client PC.

The following example shows the installation executable file name:

```
j2re-1_4_2_04-windows-i586-p.exe
```

> **Note**   The exact file name of the installation executable file changes with each version as the new
> version number is incorporated into the name.

The JRE software installs in the C:\Program Files\Cisco\Java\JRE directory.

Viewing the Component Versions That Are Installed on the Server

The mcsver.exe program reports the current version of all installation components, including the
operating system. Be aware that Cisco does not report the actual Cisco CallManager version through this
program. Recognize that most of these components, which run from the installation disks during the
initial installation, no longer exist on the system.

The version for OS Image equals your operating system disk version number. The version of OS Image
will change only if you do a new installation with the Cisco IP Telephony Server Operating System
Hardware Detection disk.

The version for stiOSUpg.exe equals the version of the operating system upgrade that you last ran either
via disk or via the web. When Cisco updates and releases the Cisco IP Telephony Server Operating
System OS Upgrade disk (Disk 2), the version of stiOSUpg changes.

Perform the following procedure to view the component versions that are installed on the server:

Procedure

Step 1   Use Windows Explorer to browse to the following folder:

C:\utils\mcsver

Step 2   View the versions of the components that are running on your server.

Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP)

You must upgrade the Telephony Application Programming Interface and Java Telephony Application Programming Interface (TAPI/JTAPI) client software on any application server or client workstation on which TAPI/JTAPI applications are installed. If you do not upgrade the TAPI/JTAPI client, your application will fail to initialize.

The following information applies if you have integrated a Cisco Unity system with Cisco CallManager. TSP makes the voice-mail ports available to Cisco Unity. To ensure that Cisco Unity integrates properly with Cisco CallManager, you may need to upgrade the TSP that is integrated with the voice-messaging system. To ensure that you upgrade to the appropriate TSP release, refer to the *Cisco CallManager Compatibility Matrix*.

Upgrading the Cisco TAPI/TSP for Cisco SoftPhone

Perform the following procedure to upgrade the Cisco SoftPhone TAPI/TSP to the version that is stated in the *Cisco CallManager Compatibility Matrix*.

Procedure

Step 1   From each Cisco Softphone client, browse into server that is running Cisco CallManager Administration and log in with administrative privileges.

> **Tip**   To browse into the server, enter https://<CM-server-name>/CCMAdmin/main.asp, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

Step 2   From the Application menu, choose **Install Plugins**.

Step 3   Click the **Cisco Telephony Service Provider** icon that is associated with the plug-in.

Step 4   To complete the upgrade, follow the prompts in the window.

Step 5   Verify that a basic call works as expected for Cisco SoftPhone.

Using the JTAPI Update Utility with CRS

Cisco Customer Response Solutions (CRS) servers include a JTAPI Update Utility that performs synchronization of the Cisco CallManager Plugin with the CRS server and the Cisco Agent Desktop (CAD). You must run this update tool to ensure successful operation of your CRS server.

If you have CRS or Cisco CallManager Extended Services installed (either coresident with the Cisco CallManager server or on a separate server) and you upgrade and/or install Cisco CallManager, you must take additional action to ensure plug-in synchronization.

Because an upgrade to a Cisco Call Manager server may include an updated JTAPI Plugin component, make sure that you run the JTAPI Update Utility on the CRS server to upgrade the JTAPI client. Running the JTAPI Update Utility on your CRS server, after you upgrade Cisco CallManager, ensures that the JTAPI Plugin gets properly installed.

Note Simply executing the plug-in installer to install the JTAPI Plugin on the CRS server (in lieu of running the JTAPI Update Utility) does not copy the jtapi.jar file to the CRS share folder, which leaves the update in an unfinished state.

For detailed information about the JTAPI Update Utility, refer to the Cisco Customer Response Applications Administrator Guide at http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_5/english/admn_app/apadm35.pdf.

Using the Cisco CallManager Music On Hold Disk or Download

Note This section applies if you have never downloaded the Cisco CallManager Music On Hold files from the web or used the Cisco CallManager Music On Hold disk.

When you initially install Cisco CallManager on your server, a default music on hold audio file sample automatically installs for customer use. To increase your music on hold (MOH) selection, you may download one of the following two files via the web:

- ciscocm-MusicOnHold, which is a set of wav files that provides the entire music selection from the disk
- ciscocm-MusicOnHoldSampler, which is a small set of files that offers a sample of music that is available on the disk

For information on the MOH feature, refer to the latest version of the *Cisco CallManager Administration Guide* and the latest version of the *Cisco CallManager System Guide*.

As a Cisco CallManager user, you can use any disk/file with music on hold. Because of licensing restrictions, you must not distribute the Cisco CallManager Music on Hold disk/files to anyone else, and you must not use the files for any other purpose.

Reverting to the Previous Configuration After an Upgrade Attempt

In the unlikely event of an upgrade failure, or if you prefer an earlier version of Cisco CallManager, perform the following steps to return the Cisco IP Telephony Applications Server to the configuration that was in effect prior to the upgrade.

Reconfiguring If You Did Not Remove a Drive Before the Upgrade

This procedure assumes that you have a good backup file on a tape device or network directory. Refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

Perform the following procedure:

Procedure

Step 1 Perform the following procedure, depending on whether you are reverting the publisher database server or the subscriber server(s):

Publisher Database Server

Step 2 Reinstall the operating system by using Cisco-provided operating system version 2000.2.4 or later.

You must perform this task by using the Cisco-provided disks that shipped with Cisco CallManager server.

Step 3 Using the disks that originally shipped with Cisco CallManager, reinstall Cisco CallManager on your server.

Do not install or configure the backup utility that automatically displays during the installation.

Step 4 If you want to do so, install and configure the Cisco IP Telephony Backup and Restore System (BARS).

Step 5 Perform the necessary upgrade(s) to match the most recent successful backup.

> **Note** To revert to the pre-upgrade configuration, you must restore the version of Cisco CallManager that was in effect when the last successful backup occurred.

Step 6   Restore the data.

Subscriber Server(s)

Step 7   Reinstall the operating system by using Cisco-provided operating system version 2000.2.4 or later.

You must perform this task by using the Cisco-provided disks that shipped with Cisco CallManager server.

Step 8   Using the disks that originally shipped with Cisco CallManager, reinstall a version of Cisco CallManager on your server.

Do not install or configure the backup utility that automatically displays during the installation.

Step 9   If you want to do so, install and configure the Cisco IP Telephony Backup and Restore System (BARS).

You install and configure the backup utility on the subscriber when a Cisco IP telephony application, for example, CRS, exists on the subscriber server.

Reconfiguring If You Removed a Drive Before the Upgrade

This process may take from 15 minutes to 60 minutes, depending on the size of the drive.

Perform the following procedure:

Procedure

Step 1   Shut down the server.

Step 2   Remove the existing hard drive from Slot 0. Insert the hard drive that was removed prior to the upgrade into Slot 0.

> **Note**   On the MCS-7845, perform this additional step. Remove the existing hard drive from Slot 2 and insert the hard drive that you removed prior to the upgrade into Slot 2.

Step 3   Slightly pull the drive in Slot 1; for the MCS-7845, also slightly pull the drive in Slot 3. Do not completely remove the drives from the server.

Step 4   Power on the system.

> **Note**   Step 5 does not apply for MCS-7835I-2.4 and MCS-7835I-3.0 servers.

Cisco MCS

Step 5   Perform the following procedure for all Cisco MCS where you removed a drive:

  a.   To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845, press **F2**.

> **Note**   The MCS-7835H-2.4 (or later) and MCS-7845H-2.4 (or later) default to F2, and the process automatically continues after a 10-second delay.

     b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845. When prompted, press **F1** to continue.

     c. Push the drive that was slightly pulled in Step 3 into Slot 1.

     d. For the MCS-7830, MCS-7835, or MCS-7845, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**.

     e. Watch the status bar in the lower, right corner to determine when drive mirroring completes.

     f. This step applies only for the MCS-7845. After the mirroring process completes in Slot 1, push the drive into Slot 3 that was pulled in Step 3.

     g. Verify that the process completed successfully.

MCS-7835I-2.4 or MCS7835I-3.0 or IBM xSeries Server

Step 6   Press **F5**.

Step 7   Press **Ctrl + I**.

Step 8   Using the arrow keys, choose **Advanced functions**.

Step 9   Using the arrow keys, choose **Copy the configuration from drives to the controller**.

Step 10   Press **Y** for Yes.

          Processing begins.

Step 11   Press any key to continue.

Step 12   Using the arrow keys, press **Exit**.

Step 13   Press **Ctrl + Alt + Del**.

Step 14   Log in to the server by using the Administrator password.

Step 15   Push the drive that was slightly pulled in Step 3 into Slot 1.

> **Note**   Error messages display about the drive state. Proceed with the process. Do not remove the drive.

          This process takes about 35 to 40 minutes, depending on the server.

Step 16   Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.

Step 17   Verify that the process completed successfully.

Reverting the Hard Drive After Drive Mirroring Completes

If you want to revert a hard drive after drive mirroring and you have made changes that affect the domain trust relationship, you must remove the server from the domain and then add it back to the domain. You must have rights to join the server to the domain before you perform this procedure.

Procedure

Step 1   Choose **Start > Settings > Control Panel > System**.

Step 2   Click the **Network Identification** tab.

Step 3   Click the **Properties** button.

Step 4   Click the **Workgroup** radio button and enter **WRKGRP** in the corresponding field.

Step 5   Click **OK**.

Step 6   When prompted to do so, reboot the server.

Step 7   Log in to the server by using the Administrator password.

Step 8   Perform Step 1 through Step 3.

Step 9   Click the **Domain** radio button and enter the domain name for the server.

Step 10 Click **OK**.

Step 11 When prompted to do so, reboot the server.

Reverting Upgraded Cisco IP Telephony Applications After You Revert Cisco CallManager

After you revert the entire cluster to a previous version of Cisco CallManager, you must revert integrated Cisco IP telephony applications. You must revert these integrated applications to the version that is compatible with the reverted Cisco CallManager. To revert the application, perform the following procedure:

Procedure

Step 1   In the *Cisco CallManager Compatibility Matrix,* identify the telephony product and compatible version that matches the cluster reversion. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm to locate this document.

Step 2   From the application server or the client workstation, if applicable, browse into the reverted server that is running Cisco CallManager Administration and log in with administrative privileges.

> **Tip**   To browse into the server, enter https://<CM-server-name>/CCMAdmin/main.asp, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

Step 3   From the Application menu, choose **Install Plugins**.

Step 4   Click the appropriate plugin, as seen in the following list:

- **Cisco Telephony Service Provider** for Cisco SoftPhone

- **Cisco JTAPI** for any application that interfaces with Cisco CallManager by using JTAPI.

Step 5   To complete the installation, Follow the prompts in the window.

Step 6   Perform this procedure on all servers where the application is installed.

C H A P T E R **5**

Upgrade Messages

The following messages may display in dialog boxes (not the log file) during the upgrade. You can obtain and review the log file, ccminst <data/time stamp>.log, from C:\Program Files\Common Files\Cisco\Logs.

Table 5-1   Installation Messages

Message	Reason	Corrective Action
During the installation process, you may be prompted possibly multiple times to reboot the server to install a critical component. Follow the instructions in the dialog box, and (1) Reboot the server. (2) Log in as the administrator. (3) Rerun the installation program. **Note** You may need to re-enter your data in order to resume the installation.	This is an informational message only.	click **OK** to continue the installation.
You must provide the Computer Name of the publisher server. IP addresses or fully qualified DNS names are not allowed.	You must not enter periods (.) when you enter the publisher database server name.	Reenter the information correctly.
You must provide the publisher server name when installing a subscriber.	This error message displays when you install Cisco CallManager on the subscriber server and do not provide the publisher database server name.	Reenter the information correctly.
You have entered an invalid product key. Please re-enter the key.	You entered an invalid product key.	See the Cisco CRS installation documentation to obtain the Cisco CRS product keys. See this document for the Cisco CallManager product key.
You must enter a password.	This message displays when you do not enter a password, but the application requires a password for the installation to occur.	Enter the correct password.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
The passwords that you entered do not match.	This error message displays when you enter a password more than one time, but the password that you enter does not match the password on the server.	Enter the same password on all servers in the cluster.
The password that you entered is not valid.	You entered an invalid password.	Enter the correct password.
You must enter a phrase from 1 to 15 characters in length. This phrase may contain English lower-case letters, English upper-case letters, Westernized Arabic Numerals, and the following Non-alphanumeric "special characters" { } . < > : ? / | \ ` ~ ! @ $ ^ & * ( ) _ - +	You entered invalid characters for the private password phrase.	Enter valid characters.
The installation has detected pending file operations. You must reboot the server before continuing. The installation will now abort.	Pending file operations are occurring.	Reboot the server and then install Cisco CallManager.
You are not logged on as 'Administrator'. You must log in by using local Administrator user name and password to install Cisco CallManager.	You did not log in to the server with the local Administrator user name and password.	Log in to the server with the local Administrator user name and password.
You do not have administrator privileges. You must have administrator privileges to install Cisco CallManager.	You do not have administrative privileges.	Log in to the server with an account that has administrative privileges.
Windows 2000 Server is not installed. Install Windows 2000 Server before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.2.3 (or later) on all dedicated and coresident servers. Upgrade to 2000.2.7 (or later) and install the latest service release (2000-2-7sr2 or later) before installing Cisco CallManager.
Windows 2000 Service Pack 4or later is not installed. You must have Windows 2000 Service Pack 4 or later installed before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.2.3 (or later) on all dedicated and coresident servers. Upgrade to 2000.2.7 (or later) and install the latest service release (2000-2-7sr2 or later) before installing Cisco CallManager.
You must install Cisco CallManager by double clicking CCMSetup.exe.	You tried to install Cisco CallManager by double clicking the msi file that is part of the Cisco CallManager package.	Double-click the CCMSetup.exe.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
Cisco CallManager could not install the SUN Microsystems JRE component. Review the Cisco CallManager installation logs to determine cause of failure, take appropriate action. For more information refer, to the Cisco CallManager installation documents.	JRE installation failed	Obtain and examine the log file.
Cisco CallManager installation has detected JRE version <JREVERSION> installed at <JRELOCATION>. Uninstall this version of JRE from the server and rerun the installation. To continue the installation, you must disable or stop any anti-virus protection, intrusion detection software, and other third-party applications, and then rerun the installation program.	Installation detected a version of JRE that is not compatible or a version that may not have all necessary components installed	Uninstall the current JRE version and rerun the installation program.
Cisco CallManager successfully installed Sun JRE and requires the server to be rebooted. To continue the installation, you must disable or stop any anti-virus protection, intrusion detection software, and other third-party applications, and then rerun the installation program.	Cisco CallManager requires the server to be rebooted to continue the installation.	Reboot the server and rerun the installation program.
You must apply SQL 2000 Service Pack 3 (or later) before proceeding with this installation.	You did not install Microsoft SQL 2000 Service Pack 3.	Install Microsoft SQL 2000 Service Pack 3, and perform the Cisco CallManager upgrade.
The installation program could not detect a valid version of Microsoft SQL 2000. Ensure that the server has a valid Cisco CallManager version before continuing with the upgrade procedure. The installation will now abort.	The installation program did not detect a valid version of Microsoft SQL 2000.	Before attempting another upgrade, you must rebuild the server with a good copy of Cisco CallManager data
If you have installed intrusion detection or antivirus protection software, you must stop and disable these applications from the Services Control console before you continue with the Cisco CallManager installation. All other installed third-party applications must be uninstalled before proceeding with the CallManager installation. Failure to follow these directives could result in un-recoverable errors. Would you like to proceed?	This message always displays to alert the administrator of the requirements.	If you have Cisco-verified applications (Cisco AVVID Partner Applications) or platform agents that are installed on the server, you must disable/uninstall them and stop the services.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
Because the <BUILDVERSION> of this Cisco CallManager MSI package is not compatible with the Cisco CallManager setup file (ccmsetup.exe), make sure that you are using the ccmsetup.exe that was distributed with this version of Cisco CallManager. The installation will now abort.	This message indicates that the MSI package is not compatible with the Cisco CallManager setup file.	Use the ccmsetup.exe file that was distributed with this version of Cisco CallManager.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION>. Direct upgrades from this version of Cisco CallManager are not supported. You must first upgrade to a compatible Cisco CallManager version before upgrading to this version. The installation will now abort.	You tried to upgrade from a version other than Cisco CallManager 3.3 or Cisco CallManager 4.0.	Upgrade to Cisco CallManager 3.3 or Cisco CallManager 4.0 before attempting to upgrade to Cisco CallManager 4.1.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION>. Upgrades from this version of Cisco CallManager require using the Same-Server Recovery method. Please refer to the Upgrading Cisco CallManager Release 4.1(1) documentation for more information. The installation will now abort.	You attempted upgrade directly from Cisco CallManager 3.2 to Cisco CallManager 4.1(1) without following the Same Server Recovery procedures.	You must perform a Same Server Recovery by using the operating system disks that ship with this version of Cisco CallManager to install operating system.
You are attempting to upgrade Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION> by using the web download file. You cannot use the web download file to upgrade from this version of Cisco CallManager directly. You must obtain the upgrade CD-ROM disks from your Cisco account representative to complete this upgrade. The installation will now abort.	You cannot upgrade Cisco CallManager 3.3(x) to 4.1(1) by using the package for web (PFW) download file.	You must use the upgrade CD-ROM disks from the Cisco CallManager 4.1(1)software kit. Contact your Cisco account representative.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
You are attempting a Same System Recovery from an unsupported version of Cisco CallManager. The installation will now abort.	You selected the same server recovery option when you installed the operating system and one of the following conditions exists: • You do not have Cisco CallManager 3.2 installed on the server. • You performed the backup of the Cisco CallManager 3.2 server with the wrong version of the Cisco IP Telephony Applications Backup utility.	Refer to this document for instructions on how to upgrade to Cisco CallManager 4.1(3) from the version of Cisco CallManager installed on your server.
Configuration changes to the Cisco CallManager server do not take effect until you restart your system. Click Yes to restart the computer now or No if you plan to restart the computer later.	This message displays when you make configurational changes to Cisco CallManager during installation.	You do not need to take any corrective action.
Cisco CallManager installation detected a service control file from a previous failed installation. This may have resulted in incorrect service Startup Type settings. Click: "Yes" to continue installing with the current settings, "No" to reset service startup types to the original settings and exit the installation program, or "Cancel" to exit the installation program with no further action.	This message displays when the installation program detects a previous failed installation.	Cisco recommends that you choose Yes and continue installing Cisco CallManager with the current settings.
The installation has detected that the server exists in a domain. When a server exists in a domain, authentication between servers may fail or the non-default domain security policies may be too restrictive for the Cisco CallManager installation to build critical NT Accounts during an upgrade. Failure to remove the server from the domain and add to a workgroup may cause upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager. Would you like to proceed?	The server exists in a domain.	Before you continue the installation, Cisco strongly recommends that you remove all servers in the cluster from the domain.
To proceed, the installation program must update the configuration and restart the server. To continue the installation with these changes and restart the server now, click **OK**. To abort the installation, click **Cancel**.	This is an informational message only.	Cisco recommends that you click **OK** to continue the installation.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
This release of Cisco CallManager is not supported on this server model. The installation will now abort.	You cannot install this version of Cisco CallManager on this server.	Refer to the *Cisco CallManager Compatibility Matrix* for a list of servers on which you can install this version of Cisco CallManager. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
The installation program does not have enough disk space on the C drive to complete the installation. The installation program requires that you have 3.0 gigabytes of disk space available on your server. Make at least 3.0 gigabytes of disk space available and restart the installation. For information, refer to the Upgrading Cisco CallManager guide.	You attempted an upgrade by using the web file from Cisco.com and do not have enough free disk space.	Make 3.0 gigabytes of disk space available and restart the installation program.
The installation program does not have enough disk space on the C drive to complete the installation. The installation program requires that you have 2.0 gigabytes of disk space available on your server. Make at least 2.0 gigabytes of disk space available and restart the installation. For information, refer to the Upgrading Cisco CallManager guide.	You attempted an upgrade by using the CD ROM disks, but you do not have enough free disk space.	Make 2.0 gigabytes of disk space available and restart the installation program.
This version of Cisco CallManager is currently installed.	This message displays when you attempt to install the same version of Cisco CallManager that is currently on the server.	Remove the disk from the drive.
A newer version of this package has already been installed.	This message displays when you attempt to install a previous version of Cisco CallManager after a successful installation of a later version.	Remove the disk from the drive.
Cisco CallManager install did not complete successfully. Review the log file for more information.	The Cisco CallManager installation failed.	Obtain and examine the log file.
Unable to locate MSI package associated with this bootstrapper.	You did not copy all the files that came with the Cisco CallManager installation package to the server.	Copy the complete installation package to the server and rerun the Cisco CallManager installation.
Error opening MSI package	Cisco CallManager Setup cannot find the MSI package.	This message displays if you encounter a media problem; insert the disk again.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
This package has already been installed.	This message displays when you attempt to install the same version of Cisco CallManager again after a successful installation.	Remove the disk from the drive.
An unexpected error occurred.	An error occurred during the Cisco CallManager Setup.	Obtain and examine the log file.
An unexpected error occurred while creating the log directory.	The installation could not create the log file directory.	Verify that security policies on the server are not restrictive.
An unexpected error occurred while constructing package name.	An error occurred during the Cisco CallManager Setup.	Obtain and examine the log file.
The local security policy "Restrict CD-ROM access to locally logged-on user only" is enabled. This setting interferes with the Cisco CallManager installation. Please disable this setting using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation.	The "Restrict CD-ROM access to locally logged-on user only" local security policy is enabled on your server.	Disable this setting by using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation. For more information, see the "Resolving Name Resolution Failures" section on page 5-14.
Failure occurred trying to get DBNAME value from registry. Aborting Cisco CallManager installation.	The installation could not read DBNAME value from registry on the local machine.	Reboot the server and rerun the Cisco CallManager installation.
Failure occurred trying to validate the format of DBNAME value. Aborting Cisco CallManager installation.	The registry contains an invalid format of the DBNAME value. This error only occurs if you have manually modified this value.	Make sure that the DBNAME value is in the format CCM0xxx, where x stands for any digits.
Current OS version does not meet minimum requirements. Aborting Cisco CallManager install. For more information, refer to the Installing the Operating System on the Cisco IP Telephony Applications Server and Upgrading Cisco CallManager documents. The installation will now abort.	Cisco CallManager Release 4.1(1) requires Cisco-provided operating system version 2000.2.7 or later.	Refer to *Cisco Compatibility Matrix* to review which versions are compatible for installation. To access the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
Installing Cisco CallManager using Terminal Services is not allowed. Install will now abort.	Cisco does not support Terminal Services for Cisco CallManager installations, upgrades, or configuration tasks. Cisco Technical Assistance Center (TAC) uses Terminal Services for remote management and troubleshooting tasks.	If you want to use Virtual Network Computing (VNC), obtain the most recent version of the documentation at http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.
Failed to launch <name of executable>, aborting install	The installation attempted to launch the executable, and the launch failed.	Obtain and examine the log file. You may have a media problem.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
Failure occurred during the Cisco Directory installation. Refer to the log file C:\Program Files\Common Files\Cisco\Directory\IntegratedSetup.trc for details. Aborting Cisco CallManager install.	The DC Directory installation failed.	Obtain and examine the log file.
The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications, and restart the installation. For more information, refer to the Upgrading Cisco CallManager document.	The Cisco CallManager installation failed to copy files to your server.	Stop all platform agents and Cisco-verified applications and restart the installation.
Failure occurred during the Cisco CallManager installation. Please look at the Cisco CallManager installation log file for details. Aborting Cisco CallManager installation.	The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications and restart the installation. For more information, refer to the Upgrading Cisco CallManager document.	Obtain and examine the log file.
The password of [X] does not match the password on the publisher [Y]. For details, review the log file [Z].	The username and/or password of the user installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server.	Make sure that you entered the correct publisher server name and that the username and password on the publisher and subscriber match.
Because no network connectivity exists or you entered the incorrect publisher server name, the installation could not verify the password of [X] against the publisher [Y]. For details, review the log file [Z].	During the subscriber server installation, this error occurs if no network connection exists between the subscriber and publisher database servers or you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber server and make sure that you entered the correct publisher database server name.
Either the password of [X] does not match the password on the publisher [Y], or a network connectivity error occurred. For details, review the log file [Z].	One of the following problems occurred: • No network connectivity exists between the publisher database server and the subscriber server. • The username and/or password of the user installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server. • You entered the incorrect publisher database server name.	Do each of the following tasks: • Verify the connection between the publisher database server and subscriber server. • Make sure that you installed Cisco CallManager on the publisher database server and subscriber server using the Administrator username and password. • Make sure that you entered the correct publisher database server name.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
The private password phrase does not match the private password phrase on the publisher [X]. For details, review the log file [Y].	During the subscribe server installation, one of the following problems occurred: • The passwords of the NT service accounts did not match. • You entered the incorrect publisher database server name • You entered a different private password phase on the publisher database server than you did on the subscriber server.	Do each of the following tasks: • Make sure that a trusted connection exists between the subscriber server and the publisher database server. • Make sure that you entered the correct publisher database server. • Make sure you entered the same private password phrase that you entered on the publisher database server.
The installation could not verify the private password phrase on the publisher <server name>, because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	The installation could not verify the private password phrase on the publisher <server name>, because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	During the installation of a subscriber server, the installation program could not verify the private password phrase against the publisher server because of the security settings on either the Publisher or the Subscriber servers. The following list gives the probable causes: • The Publisher or the Subscriber server was in a domain during the installation. • Some local security policy settings on the machine prevented the installation program from performing this operation.
Either the passwords do not match on the publisher [servername], or a network connectivity error occurred.	During the subscriber server installation, one of the following errors occurred: • Network connectivity failed. • You entered a NT service account password that does not match the password on the publisher database server. • You did not enter the correct name of the publisher database server.	Do all of the following tasks: • Verify the connection between the subscriber and publisher database servers. • Make sure that you enter the same NT service account password that you entered on the publisher database server. • Make sure that you enter the correct publisher database server name.
The installation failed to verify the Cisco CallManager version that runs on the publisher database server. Cancel the installation, and review the log file at C:\Program Files\ Common Files\Cisco\Logs\ CCMUIInst.log.	During Subscriber installation, this error occurs if no network connection exists between the subscriber and publisher database servers or you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber database server and make sure that you entered the correct publisher database server name.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
The Cisco CallManager version you are installing on this subscriber does not match the version running on the publisher database server. Cancel the installation and ensure the publisher is upgraded to this Cisco CallManager version before you continue.	You attempted to install a different version of Cisco CallManager on the subscriber database server than you installed on the publisher database server.	Install the same version of Cisco CallManager on the subscriber database server that you installed on the publisher database server.
UMX.dll failed to register. After you complete the installation, review the log file.	UMX.dll failed to register because the process creation failed, the process terminated abnormally, or an error occurred when the system was executing regsvr32.	Verify that you rebooted the server after the installation. Execute a command prompt, enter regsvr32 C:\dcdsrvr\lib\UMX.dll, and press Enter. To verify that you corrected the problem, try to add a new user in Cisco CallManager Administration on this server.
Indexing directory data did not finish. After you complete the installation, review the log file. The log file C:\dcdsrvr\log\DirInstallValidation.log.	The installation could not determine whether the DC Directory completed the indexing of its data.	Continue with installation. At the end of the installation, reboot the server when prompted to do so. After you reboot the server, bring up the services control and wait for DC Directory Server to have a status of *started*. If this is a publisher, database server, you can install Cisco CallManager on the subscriber database servers. If this is a subscriber database server, go to a command window and enter **dcdrepcl trigger all**. Depending on the number of users that are configured in your system, the service may be in the starting state for a long time before changing to a started state.
The Cisco CallManager installation failed to stop <list of services> service(s). Please reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.	The installation program failed to stop the services during installation.	Reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.
The installation encountered an unknown error while trying to resolve the Publisher server name [X]. For more information, review the log file CCMInstUI.log.	The name resolution of the publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 5-14.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
The installation could not resolve the Publisher server name [X] to a valid IP address. Verify that you entered the correct publisher server name, and review the log file CCMInstUI.log for more information.	You entered the wrong publisher server name, or the hosts file has the wrong information.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 5-14.
The installation successfully resolved the Publisher server name [X] to IP address [Y] but could not resolve the IP address back to a host name.	The reverse name resolution of the Cisco CallManager publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 5-14.
The installation successfully resolved the Publisher server name [X] to IP address [Y] and resolved the IP address back to the host name [Z]. The resolved host name does not match the server name that you entered.	The publisher server name that you entered does not match the server name that the installation program retrieved after completing forward and reverse name resolution.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the "Resolving Name Resolution Failures" section on page 5-14.
The installation encountered an unknown error while trying to determine the server type during the upgrade. For more information, review the log file [x].	The registry contains invalid server information.	Obtain and examine the log file.
Because mapped network drives exist on the server, the installation could not verify the password of [x] against the publisher [y]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [z].	The installation could not verify that the password on the subscriber server matches the password on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.
Because mapped network drives exist on the server, the installation could not verify the private password phrase against the publisher [y]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [z].	The installation could not verify that the private password phrase on the subscriber server matches the private password phrase on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
The Cisco CallManager installation detected an unrecoverable error during database migration. You must revert to the original version of Cisco CallManager. For more information, refer to the *Installing the Operating System on the Cisco IP Telephony Applications Server* and *Upgrading Cisco CallManager* documents.	The installation program failed to migrate the Cisco CallManager data.	Revert to the original version of Cisco CallManager by performing the following procedures: • Install the operating system by using the same server recovery method. • Install the version of Cisco CallManager that was running on your server before you attempted to upgrade. • Restore the Cisco CallManager data from the backup file. For more information, see the "Reverting to the Previous Configuration After an Upgrade Attempt" section on page 4-1.
You are upgrading Cisco CallManager <InstalledBUILDVERSION> to version <UpgradeBUILDVERSION> which does NOT support the following features:· • Force Authorization Code and Client Matter Codes· • Call Block for Extension to Extension Transfer If you continue to upgrade, these features will no longer be available, and any associated data will be lost. Do you want to continue the upgrade process?	If you upgrade from 3.3(4) and above to 4.0(2), you will forfeit the listed features.	None. This is an informational message.
The upgrade that you are attempting is not supported. To verify which versions of Cisco CallManager are compatible for upgrade, please refer to the Cisco CallManager Compatibility Matrix on CCO. The installation will now abort.	The version of Cisco CallManager that you are attempting to upgrade from is not supported.	Refer to *Cisco Compatibility Matrix* to review which versions are compatible for installation. To access the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
Cisco CallManager installation failed while installing Microsoft SQL 2000. Review the Cisco CallManager installation logs to determine the cause of failure. Take appropriate action and reinstall both the Cisco IP Telephony Operating System and Cisco CallManager program. For more information refer, to the Cisco CallManager installation documents.	The following items comprise the probable cause: • The target machine probably has a virus. • Cisco Security Agent, antivirus software, or other third-party application was installed and running.	Review the Cisco CallManager installation to determine the cause of failure. Take appropriate action to either remove the virus or disable the specified software and then reinstall both the Cisco IP Telephony Operating System and Cisco CallManager program.

Table 5-1   Installation Messages (continued)

Message	Reason	Corrective Action
Cisco CallManager successfully installed Microsoft SQL 2000 and requires the server to be rebooted. To continue the installation, you must disable or stop any antivirus protection, intrusion detection software, and other third-party software, and then rerun the installation program. When the server reboots, you must rerun the installation program to continue your installation.	Antivirus, intrusion detection, or other third-party application was installed and running	To continue the installation, you must do the following tasks: **a.** Disable or stop any antivirus or intrusion detection software, as well as any other third-party application. **b.** Rerun the installation program. **c.** After the server reboots, rerun the installation program if it does not automatically continue.
Cisco CallManager installation failed while installing Microsoft SQL 2000 SP3A. Review the Cisco CallManager installation logs to determine cause of failure, take appropriate action. Download Microsoft SQL 2000 service pack 3A (or later) from Cisco.com, install it on the server, and rerun the Cisco CallManager installation program. For more information refer, to the Cisco CallManager installation documents.	The following items comprise the probable cause: • The target machine probably has virus. • Cisco Security Agent, antivirus software or other third-party application was installed and running.	Download Microsoft SQL 2000 service pack 3A (or later) from Cisco.com, install the service pack on the server, and then rerun the Cisco CallManager installation program.
Cisco CallManager successfully installed Microsoft SQL 2000 SP3A and requires the server to be rebooted. To continue the installation, you must disable or stop any antivirus protection, intrusion detection software, and other third-party applications, and then rerun the installation program. When the server reboots, you must rerun the installation program to continue your installation. The installation program automatically reboots the server and the installation will continue.	Antivirus, intrusion detection, or other third-party application was installed and running	To continue the installation, you must do the following tasks: **a.** Disable or stop any antivirus or intrusion detection software, as well as any other third-party application. **b.** Rerun the installation program. **c.** After the server reboots, rerun the installation program if it does not automatically continue.
Cisco CallManager could not install the Microsoft MDAC Hotfix MS04-003 at this time. When the installation has finished, please reapply the latest Cisco OS Upgrade Service Release. For more information refer to the Cisco CallManager installation documents.	The hotfix timeout of 1800 seconds expired.	This does not affect the Cisco CallManager installation, but when the installation finishes, reapply the latest Cisco OS Upgrade Service Release.

Message	Reason	Corrective Action
Cisco CallManager could not install the Microsoft SQL 2000 Hotfix MS03-031. When the installation has finished, download the SQL 2000 Hotfix MS03-031 from cisco.com, and manually install it. For more information refer to the Cisco CallManager installation documents.	The Microsoft SQL Hotfix MS03-031 installation failed, possibly because Cisco CSA or an antivirus software was installed and running.	This situation does not affect the Cisco CallManager installation. When the installation finishes, disable Cisco CSA or the antivirus software, download the SQL 2000 Hotfix MS03-031 from cisco.com, and manually install it. You can reenable Cisco CSA and the antivirus software after installing the hotfix. You can download the file SQL2K-MS03-031.exe at http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des
The installation program detected an insufficient amount of memory for this version of Cisco CallManager to function properly on this server. You may continue installing this version on a subscriber server, but you must increase the amount of memory on this server to a minimum of 1 GB after the installation to avoid any system problems.	The server does not meet the minimum memory requirement.	You may continue the installation, but Cisco recommends that you increase the memory on this server to a minimum of 1 GB after the installation to avoid system problems.
The installation program detected an insufficient amount of memory for this version of Cisco CallManager to function properly on this server. Please increase the amount of memory you have on this server to a minimum of 1 GB before you install this version of the program.	The server does not meet the minimum memory requirement.	Increase the memory on this server to a minimum of 1 GB before you install Cisco CallManager.

Resolving Name Resolution Failures

Cisco CallManager requires NetBIOS and IP name resolution. An incorrect WINS (NetBIOS) or DNS (IP) configuration could result in a service outage.

To resolve name resolution failures, consult with your network administrator to confirm NetBIOS and IP name resolution within the entire network, which includes local device IP configurations, local device name resolution (LMHOSTS and HOSTS), network-based name resolution systems (WINS and DNS) and DHCP systems.

Note Cisco recommends that you use either local or network-based name resolution and not both at the same time.

Note If you use local name resolution and you change the IP address of any server, you must update the LMHOSTS and HOSTS files of every affected server within the network accordingly. For the changes to take effect, either reboot each affected server or complete the tasks in Step 4.

Note If you use a network-based name resolution and you change the IP address of any server, you must update the WINS and DNS (including RARP) systems. For the changes to take effect, either reboot each affected server or complete the tasks in Step 4.

Procedure

Step 1 Obtain the IP address, hostname, and DNS suffix of each server in the cluster by using the *ipconfig /all* and *hostname* commands on each server.

Step 2 Populate the hosts files on each server in the cluster with the names and IP addresses of all servers in the cluster. Find the hosts files in c:\winnt\system32\drivers\etc.

The following example illustrates a hosts file where cm1 represents the hostname and mydomain.com represents the default DNS suffix or connection-specific DNS suffix from the ipconfig /all command output.

127.0.0.1 localhost
1.3.5.9 cm1 cm1.mydomain.com
1.2.4.8 cm2 cm2.mydomain.com

Step 3 Populate the lmhosts files on each server in the cluster with the names and IP addresses of all servers in the cluster. Find the lmhosts files in c:\winnt\system32\drivers\etc.

The following example illustrates a lmhosts file where cm1 represents the hostname.

1.3.5.9 cm1 #PRE
1.2.4.8 cm2 #PRE

Step 4 For the changes to take effect, issue the following commands on each server:

ipconfig /flushdns
nbtstat -R

Note Be aware that the letter "R" is case sensitive in the command.

Step 5 Confirm the changes were successfully loaded by performing the following procedures:

a. Examine the output of *nbtstat -c*

The names of all other servers in the cluster should appear with a life of -1. The names appear multiple times.

The following example represents the output of the nbtstat -c command:

Example 5-1   NetBIOS Remote Cache Name Table

Name		Type	Host Address	Life [sec]
CM2	<03>	UNIQUE	1.3.5.9	-1
CM2	<00>	UNIQUE	1.3.5.9	-1

Example 5-1   NetBIOS Remote Cache Name Table

Name		Type	Host Address	Life [sec]
CM2	<20>	UNIQUE	1.3.5.9	-1
CM1	<03>	UNIQUE	1.2.4.8	-1
CM1	<00>	UNIQUE	1.2.4.8	-1
CM1	<20>	UNIQUE	1.2.4.8	-1

b. Examine the output of *ipconfig /displaydns*. You should have at least one forward and one reverse entry for every server in the cluster. The following example contains two forward entries and two reverse entries per server.

Forward Entries

```
cm1.mydomain.com.
-------------------------------------------------------
Record Name . . . . . : cm1.mydomain.com
Record Type . . . . . : 1
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . :
>                1.2.4.8
cm1.
-------------------------------------------------------
Record Name . . . . . : cm1
Record Type . . . . . : 1
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . :
>                1.2.4.8
```

Reverse Entries

```
8.4.2.1.in-addr.arpa.
--------------------------------------------------------
Record Name . . . . . : 8.4.2.1.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
PTR Record  . . . . . :
>                cm1

Record Name . . . . . : 8.4.2.1.in-addr.arpa
Record Type . . . . . : 12
Time To Live  . . . . : 30682708
Data Length . . . . . : 4
Section . . . . . . . : Answer
PTR Record  . . . . . :
cm1.mydomain.com
```

Disabling the Restrict CD-ROM Access to Locally Logged-On User Only Security Policy

If you receive the error message that the local security policy "Restrict CD-ROM access to locally logged-on user only" is enabled, you must disable the setting, reboot the server, and rerun the Cisco CallManager installation. Use the following procedure to disable the security policy.

Procedure

Step 1   To open the Local Security Policy utility, choose **Start > Programs > Administrative Tools > Local Security Policy**.

Step 2   Expand the Local Policies folder in the left pane and choose the Security Options folder.

Step 3   In the right pane, choose the **Restrict CD-ROM access to locally logged-on user only** policy and press **Enter**.

The Local Security Policy dialog box displays.

Step 4   Choose the **Disabled** radio button and click OK.

Step 5   Exit the Local Security Policy utility.

Step 6   Reboot the server.

Step 7   Restart the Cisco CallManager installation.

Replacing Servers During the Upgrade

This document assumes that Cisco CallManager is the only application that runs on the server. This document does not provide procedures for replacing coresident servers where Cisco CallManager, Cisco Customer Response Solutions (CRS), and Cisco-verified, third-party applications are installed on the same server.

By using these procedures, you can replace the publisher database server only, a subscriber server only, multiple subscriber servers, or both the publisher database server and the subscriber server(s) during the upgrade. Unless otherwise indicated in the document, remember to perform all procedures serially; that is, on one server at a time.

⚠

Caution These procedures cause call-processing interruptions. Cisco strongly recommends that you perform this procedure during a maintenance window.   After you perform a backup, do not make any changes to the existing publisher database server. Any changes that you make after a backup will not exist in the new database.

Replacing the Cisco CallManager Publisher Database Server During the Cisco CallManager 4.1(3) Upgrade

Perform the following procedure:

Procedure

Step 1 Perform Step 2 through Step 6 for the existing Cisco CallManager publisher database server.

Performing Tasks on the Existing Cisco CallManager Publisher Database Server (Required)

Step 2 Record all network configuration settings, including the computer name, network card speed and duplex, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plugins, so you can reinstall them after the upgrade. Record the information in Table 6-1

Table 6-1   *Server Configuration Settings*

Server Configuration Settings	Your Entry
Computer Name	
NIC Speed/Duplex settings	
IP Address	
Subnet Mask	
Default Gateway	
DNS Settings	
WINS Settings	
Cisco CallManager services (See Cisco CallManager Serviceability.)	
Coresident applications (Note the application type and version.)	
Cisco verified, third-party applications (Note the application type and version.)	
Plugins from Cisco CallManager Administration	
Other Pertinent Information	

Step 3   If you are replacing a server with four drives, Cisco recommends that you set the trace directory path on the server to the default C: drive. Refer to *Cisco CallManager Serviceability Administration Guide.*

Step 4   Refer to the document, *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*, to perform the following tasks. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

   a.   Install and configure the Cisco IP Telephony Backup and Restore System (BARS) Version 4.0(7) (or later) on the publisher database server; reboot the server.

   b.   Back up the existing Cisco CallManager data.

⚠

Caution   Make sure that you back up the data to a network directory or a local tape device.

After you perform a backup, do not make any changes to the existing publisher database server. Any changes that you make after a backup will not exist in the new database.

Step 5   Copy the HOST and/or LMHOST files from C:\WINNT\SYSTEM32\DRIVERS\ETC to the network directory where the backed-up data is stored. You can perform this task on a floppy drive.

Step 6   Power off the Cisco CallManager publisher database server and disconnect it from the network.

Preparing the New Publisher Database Server

Step 7   Connect the new server to the network and power on the server. By using the Cisco-provided operating system disks, install operating system version 2000.2.4 on the new publisher database server that has no data on it. To obtain the operating system documentation, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.

⚠️

Caution   During the operating system installation, make sure that you choose the New Installation or Server Replacement option. You must enter the exact computer name and network configuration information as the publisher database server that runs Cisco CallManager. Do not check the I am recovering a system from backup check box. Do not join the new publisher database server to a Windows domain. Joining the domain causes the Cisco CallManager installation to fail.

Step 8   Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.7. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 9   Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2.7sr2 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 10   Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 11   Copy the HOST and/or LMHOST files to C:\WINNT\SYSTEM32\DRIVERS\ETC on the new publisher database server; reboot the server.

Step 12   Obtain the document, *Installing Cisco CallManager Release* 4.1(3). Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm to obtain the most recent version.

Step 13   While referencing *Installing Cisco CallManager Release* 4.1(3), perform a Cisco CallManager installation.

Step 14   Restore the backed-up data to the new publisher database server. To obtain the backup and restore utility documentation, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.

🔍

Tip   Verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

Step 15   Use this document, perform a Cisco CallManager 4.1(3) upgrade.

> **Tip**   Verify that the new server behaves as expected. Review and post-upgrade tasks and perform the necessary tasks as you verify. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 3-1.

Replacing the Cisco CallManager Subscriber Server(s) During the Cisco CallManager 4.1(3) Upgrade

You must install Cisco CallManager on subscriber servers serially, that is, on one server at a time.

> **Caution**   If you are replacing the publisher database server and subscriber server(s), make sure that you have replaced the publisher database server first and that the data migrated and services started as expected.
>
> Perform these procedures on a live network with a live publisher database server.

> **Timesaver**   If you choose to do so, you may perform the operating system installation simultaneously on all new servers if the new hardware is not connected to the same network as the current system. Make sure that you install the operating system on a physically isolated network by using the procedures in this document. Installing the operating system in this manner saves you about 1 hour per server when you perform the actual hardware migration to the production network.

> **Tip**   After you install the first subscriber server, verify that the server and application behave as expected. If the server does not behave as expected, power off the live (new) publisher database server and the subscriber server, power on the publisher database server, and rebuild the subscriber server to its original state. If this was a hardware replacement for the subscriber server, restore power to the old subscriber server.
>
> After you install the second subscriber server and verify that it behaves as expected, you may experience call-processing interruptions if you choose to revert the cluster to the original state.

Procedure

Step 1   Record all network configuration settings, including the computer name, network card speed and duplex settings, IP address, subnet mask, gateway, DNS, and WINS for the current system. Record the configuration of the servers in the existing cluster; record all software versions, Cisco CallManager services, coresident applications, and plugins, so you can reinstall them after the upgrade. Use Table 6-1 to record the information.

Step 2   Power off the Cisco CallManager subscriber server and disconnect it from the network.

Step 3   Connect the new server to the network and power on the server.

Step 4   Using the Cisco-provided Operating System disks, install operating system 2000.2.4 (or later) on the new server that has no data on it.

⚠

Caution   During the operating system installation, make sure that you choose the **New Installation or Server Replacement** option.

Do not check the I am recovering a system from backup check box.

Do not join the server to a Windows Domain during the operating system installation. Joining the domain causes the Cisco CallManager installation to fail.

Step 5   Use Cisco IP Telephony Server Operating System OS Upgrade Disk that ships with Cisco CallManager to upgrade the Cisco-provided operating system to version 2000.2.7. Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 6   Download and install the latest Cisco IP Telephony Server Operating System service release (2000-2-7sr2 or later). The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 7   Download and install the latest OS-related security hotfixes, if any.

The operating system related security hotfixes post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.

For installation instructions, refer to the file-specific readme document, *Cisco IP Telephony Operating System, SQL Server, Security Updates,* and *Installing the Operating System on the Cisco IP Telephony Applications Server.* To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Step 8   Using the Cisco CallManager Installation disks, perform a complete subscriber installation on the new server where you installed the operating system.   Refer to the Cisco CallManager installation document for more information. Go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.

🔎

Tip   After you install Cisco CallManager on the server, verify that the new server behaves as expected. Review post-installation and post-upgrade tasks and perform the necessary tasks as you verify. To obtain the Cisco CallManager 4.1(3) installation document for post-installation tasks, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm. To review post-upgrade tasks, see the "Performing Post-Upgrade Tasks" section on page 3-1.

Troubleshooting Hardware Replacements During Upgrades

If the server does not behave as expected, power off the live (new) publisher database server and the subscriber server, if applicable, power on the publisher database server, and rebuild the subscriber server to its original state. If you replaced the subscriber server, restore power to the subscriber server.