



Upgrading Cisco CallManager Release 3.3(2)

Revised: 03/07/2003



Caution

With Cisco CallManager Release 3.3(2), Cisco significantly changed upgrade and installation procedures. You must perform all installation/upgrade procedures exactly as stated in the Cisco CallManager installation/upgrade documentation. Failure to do so causes installation errors, installation failures, and, during upgrades, a total system failure, including a loss of Cisco CallManager data/configuration settings.

Cisco does not provide Cisco CallManager upgrade software via the web for this release.



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

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. The document includes the following topics:

- Frequently Asked Questions about the upgrade
- Pre-/post- upgrade tasks
- Upgrade tasks in the order that is required to complete the upgrade
- Reversion tasks, if you want to go back to the last successful backup and Cisco CallManager release

Use this document in conjunction with the documents that are listed in the [“Locating Related Documentation”](#) section on page 3.

Conventions

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

Using the Cisco IP Telephony Applications Backup Utility, Version 3.5.18 (or later) replaces the document, *Backing Up and Restoring Cisco CallManager Release 3.3*.

Blue Text—To quickly navigate to a section or URL, 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 3.3*

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 Adapter, 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.

- *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, etc.

- 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 navigate to the appropriate documentation.

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 hardware specifications	http://www.cisco.com/warp/public/779/largeent/avid/products/infrastructure.html
<i>Cisco CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
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

Table 1 Quick Reference for URLs (continued)

Related Information and Software	URL and Additional Information
Support patches and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml See the “Procedures for Installing the Cisco CallManager Support Patch (Recommended)” section on page 37. Note The operating system and SQL Server 2000 support patches post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco Integrated Communications System (ICS) 7750	http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm



Note

Additional steps and requirements exist for the Cisco Integrated Communications System (ICS) 7750. If you need Cisco CallManager upgrade information and procedures for the Cisco ICS 7750, refer to the version of the Cisco ICS 7750 documentation that supports this version of Cisco CallManager. Click the URL in [Table 1](#) to navigate to the appropriate documentation.

Upgrading from Cisco CallManager Release 3.2 or 3.1

The following sections apply if you are upgrading from Cisco CallManager Release 3.2 or 3.1.

Contents

This section contains the following topics:

Pre-Upgrade Tasks and Information

- [Locating Related Documentation, page 3](#)
- [Frequently Asked Questions About Upgrading from Cisco CallManager Release 3.2 or 3.1, page 6](#)
 - [From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 3.3\(2\)?, page 6](#)
 - [Which servers, operating system versions, and server configurations does Cisco support for this upgrade?, page 6](#)
 - [What CD-ROMs and information do I need for this upgrade?, page 7](#)
 - [Which server in the cluster do I upgrade first?, page 8](#)
 - [How long does it take to upgrade the publisher database server?, page 11](#)
 - [How does the publisher database server upgrade work?, page 11](#)
 - [How does the subscriber server\(s\) upgrade work?, page 16](#)

- How does a co-resident upgrade work if I have CRS installed with Cisco CallManager?, page 16
- May I remove a drive before I upgrade?, page 17
- May I use Terminal Services to remotely upgrade the server?, page 17
- May I configure a server in the cluster as a Domain Controller?, page 18
- May I perform configuration tasks during the upgrade?, page 18
- Which third-party, Cisco-verified applications may I install on the Cisco CallManager server?, page 18
- Which Cisco IP telephony applications may I install on the Cisco CallManager server?, page 19
- What pre-upgrade tasks should I perform?, page 19
- What post-upgrade tasks should I perform?, page 20
- What additional information should I know before I upgrade?, page 20
- What if I encounter problems during the upgrade?, page 21

Upgrade Tasks

- Procedures for Upgrading the Publisher Database Server (Required), page 22
 - Remove the System From the NT Domain or Microsoft Active Directory Domain and Reboot the Server (Required, If Configured), page 22
 - Disable and Stop Third-Party Cisco-Verified Applications and Reboot the Server (Required), page 23
 - Install and Configure Cisco IP Telephony Applications Server Backup Utility, Version 3.5.18 or Later (Required), page 24
 - Back Up Existing Data (Required), page 26
 - Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring (Strongly Recommended), page 27
 - Install the Operating System By Using Same Server Recovery (Required), page 29
 - Manually Stop Cisco Services and Do Not Reboot the Server, page 31
 - Verify That the MS-SQL Server Service is Running, page 31
 - Install Cisco CallManager (Required), page 31
 - Back Up the Current Database (Required), page 33
- Procedures for Upgrading Subscriber Database Servers (Required), page 34
 - Required Upgrade Tasks for the Publisher Database Server, Table 4 on page 12

Post-Upgrade Tasks

- Procedures for Installing the Cisco CallManager Support Patch (Recommended), page 37
- Enabling Cisco-Verified McAfee Antivirus Services, page 40
- Verifying Services, Patches, and Hotfixes, page 40
- Viewing the Component Versions That Are Installed on the Server, page 41
- Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP), page 41
- Upgrading the Cisco TAPI/TSP for Cisco SoftPhone, page 41
- Using the Cisco CallManager Music On Hold CD-ROM or Download, page 42

Reversion Tasks

- [Reconfiguring If You Did Not Pull a Drive Before the Upgrade](#), page 43
- [Reconfiguring If You Removed a Drive Before the Upgrade](#), page 44
- [Reverting the Hard Drive After Drive Mirroring Completes](#), page 45
- [Reverting Upgraded Cisco IP Telephony Applications After You Revert Cisco CallManager](#), page 46

Upgrade Error Messages

- [Error Messages](#), page 46

Frequently Asked Questions About Upgrading from Cisco CallManager Release 3.2 or 3.1

Review the following questions and corresponding responses before you upgrade from Cisco CallManager Release 3.2 or 3.1.

From which versions of Cisco CallManager can I upgrade to Cisco CallManager Release 3.3(2)?

To verify which versions of Cisco CallManager are compatible for upgrade, refer to the *Cisco CallManager Compatibility Matrix*. See [Table 1](#).

If your server runs Cisco CallManager Release 2.4 or 3.0, you must upgrade every server in the cluster to the latest version of Cisco CallManager Release 3.1 before you can upgrade to a version of Cisco CallManager Release 3.3. For information on upgrading to Cisco CallManager Release 3.1, refer to the latest version of *Upgrading Cisco CallManager Release 3.1*.

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

Cisco supports upgrades to Cisco CallManager Release 3.3(2) on Cisco Media Convergence Servers (MCS), the Cisco ICS 7750, customer-provided IBM xSeries 330/340/342/345 servers, and HP DL320 and DL380 servers that meet Cisco-approved configuration standards.

Cisco supports Cisco-provided operating system version 2000.2.3 or later with Cisco CallManager Release 3.3(2). You must install the operating system via the operating system CD-ROMs that ship with this version of Cisco CallManager. You cannot upgrade to Cisco-provided operating system version 2000.2.3 from a previous version of the operating system.

**Caution**

Before the upgrade, Cisco requires that you remove all servers from the NT Domain or a Microsoft Active Directory Domain. Do not add these servers to a domain until you complete the installation or upgrade procedures on all servers in the cluster.

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.

Before you begin the operating system installation, make sure that you have all drives in the server and verify that the drives are functional. For example, insert two drives for the MCS-7835 and four drives for the MCS-7845-1400. Neglecting to perform these tasks causes the failure of the Cisco CallManager installation to fail and the loss of data/configuration settings from drive-mirroring.

What CD-ROMs and information do I need for this upgrade?

Before you upgrade the publisher database server, locate the following CD-ROMs and information.

CD-ROMS

- Cisco IP Telephony Server Operating System Hardware Detection CD-ROM
- Cisco IP Telephony Server Operating System Installation and Recovery CD-ROM

Cisco requires that you install Cisco-provided operating system version 2000.2.3 or later with this upgrade. You cannot upgrade to Cisco-provided operating system version 2000.2.3 from a previous version of the operating system. This release requires that you perform a Same Server Recovery via CD-ROM.

You use only one of the server-specific Cisco IP Telephony Server Operating System Installation and Recovery CD-ROMs that come in your software kit. During the operating system installation, you receive a prompt to insert the appropriate CD-ROM into the CD-ROM drive.

- Cisco CallManager 3.3 Publisher Upgrade CD-ROM
You use this CD-ROM to start the publisher database server upgrade.
- Cisco CallManager 3.3 Subscriber Upgrade CD-ROM
You use this CD-ROM to start all subscriber server upgrades.
- Cisco CallManager 3.3 Upgrade (Disk 2) and New Installation/Recovery CD-ROM
You use this CD-ROM to complete all Cisco CallManager upgrades.

Passwords

Before the upgrade, obtain the local Administrator account password, the SQL server SA password, and the computer name of the publisher database server.

**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.

**Caution**

For each of the accounts, you must enter the same password on every server in the cluster.

Use the information in [Table 2](#) when you perform the upgrade procedures.

Table 2 Information That Is Needed During the Upgrade

Data	Your Entry
Destination where the MCS.sti 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)	

Which server in the cluster do I upgrade first?



Timesaver

After you finish the entire upgrade of the publisher database server, you can simultaneously install the operating system on all subscriber servers. This task causes call-processing interruptions.

You must perform the Cisco CallManager installation serially.



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.

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

You must upgrade all the servers in the cluster. See [Table 3](#), which describes the upgrade order for the following cluster configurations:

- The Cisco CallManager service runs on the publisher database server (two-server cluster).
- The Cisco CallManager service does not run on the publisher database server.


Table 3 Cluster Upgrade Order

	The Cisco CallManager Service Runs on the Publisher Database Server.	The Cisco CallManager Service Does Not Run on the Publisher Database Server.
Step 1	<p>Upgrade the publisher database server. The “Procedures for Upgrading the Publisher Database Server (Required)” section on page 22 provides the upgrade procedure.</p> <p>When you perform an upgrade, the Cisco CallManager service automatically stops, and the devices that are homed to the publisher database server fail over to the subscriber server.</p>	<p>Upgrade the publisher database server. The “Procedures for Upgrading the Publisher Database Server (Required)” section on page 22 provides the upgrade procedure.</p>
Step 2	<p>Upgrade the subscriber.</p> <p>See the “Procedures for Upgrading Subscriber Database Servers (Required)” section on page 34.</p>	<p>Upgrade the Cisco TFTP server, if it exists separately from the publisher database server.</p> <p>See the “Procedures for Upgrading Subscriber Database Servers (Required)” section on page 34.</p>
Step 3	<p>You completed the Cisco CallManager upgrade. Perform post-upgrade tasks.</p>	<p>Upgrade servers, one server at a time, that have only Cisco CallManager-related services (Music on Hold, Cisco IP Media Streaming Application, etc.) running on them.</p> <p>Make sure that you upgrade only one server at a time.</p> <p>Make sure that the Cisco CallManager service does not run on these servers.</p> <p>See the “Procedures for Upgrading Subscriber Database Servers (Required)” section on page 34.</p>

Table 3 Cluster Upgrade Order (continued)

	The Cisco CallManager Service Runs on the Publisher Database Server.	The Cisco CallManager Service Does Not Run on the Publisher Database Server.
Step 4	Not applicable	<p>Upgrade each secondary server, one server at a time.</p> <p>See the “Procedures for Upgrading Subscriber Database Servers (Required)” section on page 34.</p> <p>About Oversubscribing the Secondary Servers 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).</p> <p>About Registering All Devices to the Same Version of Cisco CallManager 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.</p>

Table 3 Cluster Upgrade Order (continued)

	The Cisco CallManager Service Runs on the Publisher Database Server.	The Cisco CallManager Service Does Not Run on the Publisher Database Server.
Step 5	Not applicable	<p>Upgrade each primary server that has the Cisco CallManager service running on it. Remember to upgrade one server at a time. See the “Procedures for Upgrading Subscriber Database Servers (Required)” section on page 34.</p> <p> 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.</p>
Step 6	Not applicable	<p>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.</p>

How long does it take to upgrade the publisher database server?

To minimize call-processing downtime, Cisco strongly recommends that you perform all upgrade procedures for the Cisco CallManager and all 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 reinstallations, and Cisco-verified application reinstallations.

For the time that it takes to perform specific tasks on the publisher database server, see the [“How does the publisher database server upgrade work?”](#) section on page 11.

For the time that it takes to perform tasks on each subscriber server, see the [“How does the subscriber server\(s\) upgrade work?”](#) section on page 16.

How does the publisher database server upgrade work?

During the upgrade, Cisco requires that you use the Same Server functionality from Cisco-provided operating system version 2000.2.3 to migrate data to this release of Cisco CallManager. To successfully upgrade the publisher database server, you must perform all procedures exactly as stated in this document.



Caution

Before you start the upgrade, make sure that you perform the recommended backup procedures for all co-resident software applications that are installed on the server. 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.

Table 4 includes the entire upgrade process on the publisher database server.

Table 4 Required Upgrade Tasks for the Publisher Database Server

Task	Important Information	Time It Takes To Perform Task
Remove all servers in the cluster from the NT Domain 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 22.	Depends on the size of the cluster
Manually disable all platform agents and Cisco-verified applications (Cisco AVVID Partner 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, and remote management services, ensures that the upgrade does not encounter issues that are associated with these services.	20 minutes
Run the Cisco CallManager HealthCheck Utility.	See the “Run the Cisco CallManager HealthCheck Utility” section on page 24.	1 minute
Manually remove previous versions of the Cisco IP Telephony Applications Backup.	Cisco recommends that you perform this task before you insert the Cisco CallManager Publisher Upgrade CD-ROM. If the backup utility installation detects a previous version of the utility, verify that no backup utility exists under the Add/Remove Programs option in Microsoft Windows. Then, continue the installation, even if an error message states that a previous version is detected.	5 minutes
Manually install the Cisco IP Telephony Applications Server Backup Version 3.5.18 or later.	<p>The Cisco CallManager Publisher Upgrade CD-ROM contains the utility that you must install.</p> <p>About Backup Utility Configuration</p> <p>When the installation prompts you to configure the Cisco IP Telephony Applications Backup Utility, be aware that you must configure the publisher database server as the Backup Server, so data and configuration migration can occur. You cannot uninstall the version of the backup software that installs with this version of Cisco CallManager because this backup utility provides a mandatory component on the publisher database server.</p> <p>About the Network Directory</p> <p>If you choose a network directory as the destination for the backup server, the directory must be shared in Windows 2000. To share a directory, log in on that server, right-click the directory folder icon that you want to share, click Sharing..., click Share this folder, and then click OK.</p>	15 minutes

Table 4 Required Upgrade Tasks for the Publisher Database Server (continued)

Task	Important Information	Time It Takes To Perform Task
<p>Manually back up the data that is on the publisher database server to either a network directory or local tape drive.</p>	<p>Consider the following information before you back up the server:</p> <p>About the Backup Utility Version</p> <p>To back up the data, you must use Cisco IP Telephony Applications Backup Utility, version 3.5.18 or later, with this release of Cisco CallManager</p> <p>About Data Deletion</p> <p>Do not back up the data to a local directory; the operating system installation erases all data that is stored on the local directory.</p> <p>About Temporary Disk Space</p> <p>If the server does not have enough temporary disk space to complete the backup, the backup fails.</p> <p>About Data Preservation</p> <p>Only data that is contained on the publisher database service restores. For example, if Cisco Trivial File Transfer Protocol (TFTP) does not reside on the publisher database server, the restoration at the end of the upgrade erases all customized TFTP information, such as specific phone or gateway loads. If you want to retain this information, you must reconfigure the system, so the loads exist on the publisher database server, or you must manually save this data before the restoration.</p> <p>After the backup, verify that no errors exist. Failure to successfully troubleshoot any problems could cause a total loss of data.</p>	<p>30 to 60 minutes, depending on the size of the Cisco CallManager and Call Detail Record (CDR) database</p>
<p>After you verify that the backup completed successfully, verify that the dbname.ini and backup.ini files exist. Copy the files to the network directory or tape device where the MCS.sti file is stored.</p>	<p>See the “Verify That the dbname.ini and backup.ini Files Exist for the STI_DATA drive; Copy the Files to the Network Directory Where the MCS.sti File Exists (Strongly Recommended)” section on page 27.</p>	

Table 4 Required Upgrade Tasks for the Publisher Database Server (continued)

Task	Important Information	Time It Takes To Perform Task
<p>Using the Cisco-provided operating system CD-ROMs, install operating system version 2000.2.3 or later.</p> <p>You must install Cisco-provided operating system 2000.2.3 or later via the CD-ROMs that ship with Cisco CallManager. You cannot upgrade to Cisco-provided operating system version 2000.2.3 from a previous version of the operating system.</p>	<p>About Removing Drives</p> <p>After you verify that you have a good backup of 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.</p> <p>Before you begin the operating system installation, make sure that you have all drives in the server and verify that the drives are functional. For example, insert two drives for the MCS-7835 and four drives for the MCS-7845-1400.</p> <p>You must also remove additional hard drives from the server. Neglecting to perform these tasks causes the failure of the Cisco CallManager installation and the loss of data/configuration settings from drive mirroring.</p> <p>About Name Resolution</p> <p>After installing the operating system and before installing Cisco CallManager, you must configure name resolution for the backup location.</p> <p>About NT and Microsoft Active Directory Domains</p> <p>Cisco requires that you remove and do not add any servers to the NT Domain or the Microsoft Active Directory Domain until you complete all installation procedures on all servers in the cluster. The installation fails if you do not perform this task.</p> <p>About Data Recovery</p> <p>Make sure that you choose Same Server Recovery during the operating system installation. Choosing this option ensures that the server retains the current network configuration data.</p> <p>About Passwords</p> <p>Make sure that you enter an Administrator password at the end of the operating system installation. If you leave the Administrator password blank, you cannot install Cisco CallManager on the server.</p> <p>Ensure that this password is the same on every server in the cluster.</p> <p>About Operating System Support Patches</p> <p>Cisco strongly recommends that you do not install any operating support patches until you complete the upgrade on every server in the cluster.</p>	<p>45 to 75 minutes, depending on the server type</p>

Table 4 Required Upgrade Tasks for the Publisher Database Server (continued)

Task	Important Information	Time It Takes To Perform Task
<p>Use the Cisco CallManager Upgrade and New Installation/Recovery CD-ROM to install Cisco CallManager.</p>	<p>Microsoft SQL Server 2000, Microsoft SQL Server 2000 Service Pack 2.0, and DC Directory automatically install when you install Cisco CallManager via the CD-ROM.</p> <p>About Configuring Name Resolution on the Backup Location</p> <p>After installing the operating system installation and before installing Cisco CallManager, you must configure name resolution for the backup location.</p> <p>About Data Restoration</p> <p>The CD-ROM that you insert for the Cisco CallManager installation also restores the data that you backed up by using backup utility 3.5.18 or later.</p> <p>The restoration retains all TCP/IP configuration settings, but you lose all NIC settings that you have manually configured; for example, hard-coded Speed/Duplex settings. You must manually configure these settings after you install all servers in the cluster.</p> <p>Only the data that is contained on the publisher database server restores to the destination that you specify.</p> <p>For example, if Cisco TFTP does not reside on the publisher database server, the restoration at the end of the upgrade erases all customized TFTP information, such as specific phone or gateway loads. If you want to retain this information, you must reconfigure the system, so the loads exist on the publisher database server, or you must manually save this data before the restoration. Be aware that the restoration launches automatically.</p> <p>During the restoration, if your location is a network directory, you must click the Browse button and manually highlight the MCS.sti file. Failure to highlight the file causes the upgrade to fail.</p> <p>About Installed Services</p> <p>All services that display in the Service Activation window of Cisco CallManager Serviceability install, but only the services that you configured prior to the upgrade activate after the upgrade completes and the server reboots.</p> <p>If you want to run additional services, you must activate the service on each server in which you want the service to run. You must perform this task by browsing into Cisco CallManager Serviceability from a PC that does not have Cisco CallManager installed. For more information on how to activate services and for service considerations, refer to the <i>Cisco CallManager Serviceability Administration Guide</i>.</p> <p>Cisco CallManager places services in an inactive state until the upgrade completes.</p>	<p>Restoring the Data— up to 70 minutes, depending on the size of the Cisco CallManager and CDR database</p> <p>Installing Cisco CallManager— 45 to 90 minutes</p>

How does the subscriber server(s) upgrade work?

You perform the following procedures to upgrade the subscriber servers:

- Perform pre-upgrade tasks.
- Verify that you removed all servers from the NT or Microsoft Active Directory Domain.
- Run the ServPrep Utility via the Cisco CallManager Subscriber Upgrade CD-ROM.
- Install Cisco-provided operating system version 2000.2.3 by using the Same Server Recovery option.
- Perform a new Cisco CallManager installation.
- Install the Cisco CallManager support patch.

To complete installation tasks on each subscriber server, you should allot 60 to 120 minutes, depending on the server type. Consider the time that it takes to perform pre-/post upgrade tasks.

For procedures, see the [“Procedures for Upgrading Subscriber Database Servers \(Required\)”](#) section on page 34.

How does a co-resident upgrade work if I have CRS installed with Cisco CallManager?

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

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, you have two separate versions of Cisco CallManager running 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; i.e., 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.

To successfully complete the upgrade, Cisco strongly recommends that you manually stop the following services before you install Cisco CallManager on each server.

- ALL Cisco services within the Service Control Panel (services.msc).
- MS-SQL Agent
- DC Directory

- SNMP and its dependencies
- IIS Admin and its dependencies
- Network Time Protocol

**Caution**

Do not reboot the server after you stop the services.

Do not stop the services on every server at the same time. Stop the services on the publisher database server first, perform the upgrade, and then wait for the services to restart before you stop the services on the next server. Remember to perform this process serially.

**Caution**

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

May I remove a drive before I upgrade?

You cannot remove a drive if you have the MCS-7815, MCS-7820, MCS-7822, MCS-7825, or 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. The [“Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring \(Strongly Recommended\)” section on page 27](#) describes how to properly perform this task.

This task may require that you purchase a new drive.

Before you begin the operating system installation, make sure that you have all drives in the server and verify that the drives are functional. For example, insert two drives for the MCS-7835 and four drives for the MCS-7845-1400. Neglecting to perform these tasks causes the failure of the Cisco CallManager installation and the loss of data/configuration settings from drive-mirroring.

May I use Terminal Services to remotely upgrade the server?

Do not use Terminal Services to upgrade to Cisco CallManager Release 3.3(2). 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, see [Table 1](#) 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.

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.

Which third-party, Cisco-verified applications may I install on the Cisco CallManager server?



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.

To review a list of third-party, Cisco-verified applications that you may install on the server, perform the following procedure:

Procedure

- Step 1** Click <http://www.cisco.com/pcgi-bin/ecoa/Search>.
- Step 2** In the Solution pane, click **IP Telephony**.
- Step 3** From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**.
- Step 4** Click **Search**.



Caution

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

Disabling Third-Party, Cisco-Verified Applications (Required)



Caution

To successfully complete installation, upgrade, or restoration procedures, you must disable all Cisco-verified applications/services on every server in the cluster.

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 the installation does not encounter issues that are associated with these services.

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 recommends that you install the Cisco IDS Host Console on a standalone server that is designated for that software. You can install Cisco IDS Host Agents on servers where Cisco CallManager is installed. To access information on Cisco IDS Host Sensor, see [Table 1](#).



Caution

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

What pre-upgrade tasks should I perform?

[Table 5](#) describes pre-upgrade tasks.

Table 5 Pre-Upgrade Tasks

Pre-Upgrade Task	Related Topics
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 3.3(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 8 How does a co-resident upgrade work if I have CRS installed with Cisco CallManager?, page 16
Make sure that you obtain CD-ROMs for the Cisco-provided version 2000.2.3 or later operating system.	Which servers, operating system versions, and server configurations does Cisco support for this upgrade?

Table 5 Pre-Upgrade Tasks (continued)

Pre-Upgrade Task	Related Topics
Make sure that your server configuration supports this upgrade.	Which servers, operating system versions, and server configurations does Cisco support for this upgrade? Note 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.
Review a list of Cisco-verified applications that you must disable before the upgrade.	Disable and Stop Third-Party Cisco-Verified Applications and Reboot the Server (Required), page 23.
Locate information that you must provide during the upgrade.	See Table 2 .
Back up co-resident software applications by referring to the documentation that supports the backup procedure.	How does the publisher database server upgrade work? How does a co-resident upgrade work if I have CRS installed with Cisco CallManager?, page 16

What post-upgrade tasks should I perform?

Do not perform any post-upgrade tasks until you complete the upgrade on all servers in the cluster. See the [“Procedures for Post-Upgrade Tasks”](#) section on [page 38](#) for more information.

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 Service and Enterprise Parameters in Cisco CallManager Administration

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. This rule applies for numeric values only.

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

If you never changed the suggested value, Cisco CallManager automatically updates the value during the Cisco CallManager 3.3 upgrade to match the new suggested value.

During the upgrade, some non-servicewide parameters may change to clusterwide parameters (formerly known as servicewide parameters). For clusterwide parameters, if you configured the same customized value on every server in the cluster, Cisco CallManager does not change the value on any server in the cluster if the value exists between the range of minimum and maximum values. If the customized values are not the same on every server in the cluster, Cisco CallManager automatically updates the value to the suggested value. This rule applies for numeric values only.

About Server Names

Unless otherwise specified in this document, all further references to the MCS-7835 apply to the MCS-7835, which contains a 733-MHz processor, the MCS-7835-1000, which contains a 1-GHz processor, the MCS-7835-1266, which contains a 1.26-GHz processor, and the customer-provided DL380. All further references to the MCS-7825 apply to the MCS-7825, which contains a 800-MHz processor, and the MCS-7825-1133, which contains a 1.2-GHz processor.

About H.323 Intercluster Trunks

A registration problem occurs when multiple Cisco CallManager clusters have the same device name assigned to H.323 intercluster trunks 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 Migrating Cisco CallManager Attendant Console

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*.

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, contact the third-party software vendor directly.

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 [“Installation Error Messages” section on page 46](#) and perform the recommended corrective action.
2. Obtain and review the log file, ccminst <data/time stamp>.log, from C:\Program Files\Common Files\Cisco\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 is not used by Cisco CallManager.

Procedures for Upgrading the Publisher Database Server (Required)

To successfully upgrade the publisher database server, you must perform all procedures exactly as stated in this document. To migrate data and upgrade the publisher database server, perform the following procedures in the indicated order:

1. [Remove the System From the NT Domain or Microsoft Active Directory Domain and Reboot the Server \(Required, If Configured\)](#), page 22
2. [Disable and Stop Third-Party Cisco-Verified Applications and Reboot the Server \(Required\)](#), page 23
3. [Run the Cisco CallManager HealthCheck Utility](#), page 24
4. [Install and Configure Cisco IP Telephony Applications Server Backup Utility, Version 3.5.18 or Later \(Required\)](#), page 24
5. [Back Up Existing Data \(Required\)](#), page 26
6. [Removing a Drive, Inserting a Replacement Drive, and Drive Mirroring \(Strongly Recommended\)](#), page 27
7. [Install the Operating System By Using Same Server Recovery \(Required\)](#), page 29
8. [Manually Stop Cisco Services and Do Not Reboot the Server](#), page 31
9. [Verify That the MS-SQL Server Service is Running](#), page 31
10. [Install Cisco CallManager \(Required\)](#), page 31
11. [Back Up the Current Database \(Required\)](#), page 33

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

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 Applications and Reboot the Server (Required)

To review a list of Cisco-verified applications that Cisco supports and that you should disable before the installation, click <http://www.cisco.com/cgi-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, 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.

If you installed Cisco IDS Sensor Host Agents on the server, locate the corresponding product documentation for procedures on disabling and stopping the services. You must disable and stop the following services:

- intercept Agent
- intercept Watchdog
- intercept Notification Manager
- intercept Server

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; i.e, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.
- 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 Cisco CallManager HealthCheck Utility

Run the Cisco CallManager HealthCheck Utility to verify that your server is in a good state before the upgrade. The readme document that posts next to the utility on the web provides detailed information about the utility. To obtain the utility and the readme 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 3.3**.
The Cisco CallManager 3.3 software page displays.
 - Step 3** Locate and download the readme document.
The readme file provides procedures, caveats, and descriptive information for installing the files.
 - Step 4** Using the readme file as a reference, download and run the utility on every server in the cluster where Cisco CallManager is installed.
-



Tip

You can run the Cisco CallManager HealthCheck Utility at any time. Cisco recommends that you run the utility before and after the upgrade.

Install and Configure Cisco IP Telephony Applications Server Backup Utility, Version 3.5.18 or Later (Required)

Perform the following procedure to remove the existing backup utility, install the new backup utility, and configure the utility:

Procedure

-
- Step 1** If the stiBack service exists on the server, stop the service in the Service Control Manager.
 - Step 2** From the Windows 2000 system tray, right-click the Backup icon and choose **Exit Viewer**.
 - Step 3** Uninstall previous versions of the backup utility by performing the following procedure:
 - a. Choose **Start > Settings > Control Panel**.
 - b. Double-click **Add/Remove Programs**.
 - c. Click **Cisco IP Telephony Applications Backup Utility**.
 - d. Click **Remove**.
 - e. Reboot the server and log in to the server by using the Administrator password.

- Step 4** While the server is running, insert the Cisco CallManager Publisher Upgrade CD-ROM into the CD-ROM drive.
- Step 5** When the Upgrade Warning displays, read the information carefully before starting the upgrade.
- Step 6** Click **Backup Utility** at the bottom of the window.
- Step 7** Click the **Run the program from the current location** radio button and click **Next**.
- Step 8** When a prompt asks you to install the utility, click **Yes**.
- Step 9** If the software detects that a previous version of the backup utility exists on the server, click **Yes** to proceed.

**Note**

Even if you uninstall the previous version of the backup utility, you may receive an error message that the backup utility exists on the server. Continue the backup utility installation.

- Step 10** When the Welcome window displays, click **Next**.
- Step 11** Accept the terms of the license agreement by clicking the **I accept the terms in the license agreement** radio button and click **Next**.
- Step 12** In the Backup Role window, perform the following procedure:
- a. Click the **Backup Server** radio button.
 - b. Click **Next**.
- Step 13** Click the version of Cisco CallManager that is currently running in the cluster; then, click **Next**.
- Step 14** In the Ready to Install the Program window, click **Install**.
- The installation occurs, as indicated in the status bar. Do not click **Cancel**. Continue to wait while the installation completes.
- Step 15** When the installation completes, click **Finish**.
- Step 16** Click **Yes** to restart the server.
- Step 17** Log in to the server by using the local Administrator account and password.
- Step 18** Right-click the backup utility icon in the Windows 2000 system tray; then, choose **Configure Settings**.
- Step 19** When the Backup Utility Configuration window displays, perform the following procedure:
- a. With the CallManager tab open, verify that the publisher database server name displays in the CallManager Targets list.
 - b. To test for CallManager components, click **Verify**.
 - c. When you receive the authentication results in the dialog box, click **OK**.

**Caution**

If you have installed CDR Analysis and Reporting (CAR) on the publisher database server, verify that you have added the publisher database server name (not IP address) to the Cisco CallManager and Cisco CAR target lists. Use the same naming conventions in each list, so the restore utility can restore CAR during the Cisco CallManager database restoration.

- Step 20** Click the **uOne**, **CRA** (Cisco Customer Response Applications), or **CAR** (Cisco CDR Administrative and Reporting Tool) tab and repeat [Step 19](#) to configure the backup for Cisco uOne, CRA, or Cisco CAR.
- Step 21** When the backup setup window displays, click the **Destination** tab.

- Step 22** Configure the destination, the location where the backup utility stores the data. Cisco allows you to choose only one Destination for all stored data.
- To configure a network directory, see [Step 23](#) through [Step 26](#).
- To configure a tape device, see [Step 27](#) through [Step 29](#).



Caution When you configure the destination, do not click the **Local Directory** radio button, or the operating system installation erases all existing data stored on the local directory.

To Configure a Network Directory

If you choose a network directory as the destination for the backup server, the directory must be shared in Windows 2000. To share a directory, log in on that server, right-click the directory folder icon that you want to share, click **Sharing...**, click **Share this folder**, and then click **OK**.

- Step 23** Click the **Network Directory** radio button.
- Step 24** Browse to the location of the directory and click the directory that you want to specify as the location.
- Step 25** Enter a user name and password with administrative privileges and click **Verify**; then, click **OK**.
- Step 26** In the lower, right corner of the window, click **OK**; then, go to [Step 30](#).

To Configure a Tape Device

- Step 27** Click the **Tape Device** radio button.
- Step 28** From the drop-down list box, choose the device that you want to use.
- Step 29** Click **OK**.
- Step 30** When a prompt asks you to save the settings and exit, click **Yes**.
- Step 31** Continue the upgrade by performing the tasks in the “[Back Up Existing Data \(Required\)](#)” section on [page 26](#).
-

Back Up Existing Data (Required)

You must back up the publisher database before you install the operating system. Perform the following procedure:

Procedure

- Step 1** Right-click the Cisco IP Telephony Applications Backup Utility icon in the Windows 2000 system tray and choose **Start backup now**.
- Step 2** Choose the publisher database server in the pane on the left side of the window.
- Step 3** Click **Start backup**.
- Step 4** After the backup completes, verify that the backup completed successfully. The Backup Utility Viewer displays the status of the backup operation by highlighting each task as it occurs. Use the information that is generated in the log window to help identify problems. When the current status returns to “Waiting until <time> on <date>,” the backup is complete. The last line in the log file indicates that the log is closed.

You can obtain the StiBack.log from C:\Program Files\Common Files\Cisco\Logs on the backup server. If you receive the following error messages or other error messages in the log file, the process did not successfully back up the data:

- Cisco CallManager database could not be found on <Server Name>.
- Could not determine APPS version
- Could not find a CCM/ART/CDR SQL database on <Server Name>
- Error finding SQL database
- Error enumerating registry keys on <Server Name>
- Open file request returned Not Enough Space

Step 5 After the backup completes and you verify that no errors occurred, remove the Cisco CallManager Publisher CD-ROM from the CD-ROM drive.



Caution

If you have not backed up co-resident applications on the server, you will lose the data when you perform the operating system installation. Back up these applications now.

Verify That the dbname.ini and backup.ini Files Exist for the STI_DATA drive; Copy the Files to the Network Directory Where the MCS.sti File Exists (Strongly Recommended)



Caution

Cisco strongly recommends that you verify that the dbname.ini and backup.ini files exist on the publisher database server. Cisco IP Telephony Applications Backup Utility, Version 3.5.18 (or later), creates these files during the backup. If these files do not exist, you cannot restore the MCS.sti file.

The files exist in the Recovery directory on the STI_Data drive. Depending on the system, these files exist on the D: or E: drive. For example, the files may exist on the publisher database server in one of the following locations: D:\recover\

After you locate the files, Cisco recommends that you copy the files to the network directory where the MCS.sti file exists.

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

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.



Note

You must always mirror drives in the MCS-7845-1400 in pairs.

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-7845-1400, 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-7845-1400, remove the drives from slot 0 and 2.
 - Step 3** Power on the system.

Cisco MCS

- Step 4** Perform the following procedure for the Cisco MCS (The MCS-7845-1400 requires two spare hard drives):
 - a. To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845-1400, press **F2**.
 - b. This step applies only for the MCS-7830, MCS-7835, or MCS-7845-1400.
When prompted, press **F1** to continue.
 - c. After Windows 2000 finishes booting, insert the replacement hard drive in Slot 0.



Note

On the MCS-7845-1400, 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-7845-1400, 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-7845-1400 only.
After the mirroring process completes in slot 0, insert the next drive into slot 2. The mirror 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 in slot 0.
 - b. Press **F5**.
 - c. Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.
-

Install the Operating System By Using Same Server Recovery (Required)

Before you install the operating system, carefully review [Table 2](#).

Procedure

-
- Step 1** Locate the Cisco IP Telephony Server Operating System Hardware Detection CD-ROM.
 - Step 2** Insert the CD-ROM into the CD-ROM drive and then restart the system immediately. Do not press any keys during the reboot.
 - Step 3** When the Cisco IP Telephony Applications Server QuickBuilder welcome window opens, click **Next**.
 - Step 4** When the Type of Installation window opens, choose **Same Server Recovery**; then, click **Next**.
 - Step 5** A warning message states that the installation erases all data. Click **Next**.
 - Step 6** In the Ready to Install window, click **Next**.
 - Step 7** When the Server Configuration Wizard window displays, click **Next**.



Caution

In the following configuration windows, Cisco CallManager automatically populates the data entry fields.

If the server does not belong to a Workgroup, join a Workgroup during this operating system installation. Joining a Workgroup is a requirement for the Cisco CallManager installation.

Likewise, to successfully complete the upgrade, you must configure DNS or WINS, if you have not already done so.

-
- Step 8** The user name and the name of your organization display in the appropriate fields. The computer name and DNS domain suffix appear. Click **Next**.
 - Step 9** The Join Domain window displays whether the server is in a Workgroup or Domain. If the server exists in a Domain, Cisco requires that you place the server in a Workgroup. To join a Workgroup, perform the following procedure:
 - a. Enter a name of the Workgroup; for example, WRKGRP.
 - b. Click **Next**.
 - Step 10** From the drop-down box, choose the appropriate time zone. Reset the current date and time, if applicable; then, click **Next**.
 - Step 11** If you chose **Use the following IP address** during the original installation, the IP information for the server displays in the next window. If your server was configured for Domain Name System (DNS) or Windows Internet Name Service (WINS), the IP addresses of the primary DNS and WINS servers display. If DNS or WINS was not configured, empty IP addresses fields display. Click **Next**.

- Step 12** If your server was configured with local name resolution, you must update the lmhosts file, so it contains a mapping of the IP address and hostname of each server in the cluster. Perform the following steps to configure the lmhosts file:
- a. In the LMHost window, check the **Check if you want to edit LMHosts file** check box.
 - b. Enter the IP Address and Server Name.
For example:
172.16.0.10 dallascml
 - c. Click **Add Server**.
 - d. Click **Next** to continue.



Note

The Windows 2000 SNMP agent provides security through the use of community names and authentication traps. All SNMP implementations universally accept the default name “public.” Cisco sets the community rights to none for security reasons. If you want to use SNMP with this server, you must configure it.

- Step 13** To ensure security within the Windows 2000 SNMP agent, Cisco recommends that you change the default public community name. Enter a new name; then, click **Next**.
- Step 14** The installation process automatically enables Terminal Services. If you want, you can disable these services; then, click **Next**.
- Step 15** The CD-ROM drive automatically opens. Remove the hardware detection CD-ROM from the CD-ROM drive and insert the server-specific Cisco IP Telephony Server Operating System Installation and Recovery CD-ROM into the CD-ROM drive. The configuration process continues automatically after detection of the appropriate CD-ROM. The server begins an installation and reboot process that takes about 10 minutes to complete.
- Step 16** The CD-ROM drive automatically opens. Remove the operating system CD-ROM; if prompted, press any key to reboot. If you do not receive a prompt, the server reboots automatically.
- Windows 2000 setup begins and takes about 10 minutes to complete. Do not power down the server or press any keys during setup.



Caution

If you receive a message that the configuration file is not found, manually enter the information and continue the installation.

- Step 17** When the dialog box displays, enter an administrative password in the Password field; enter the same password in the Confirm Password field and click **OK**.
- If you leave the password fields blank, you cannot install any Cisco IP telephony applications on the server.



Tip

Make sure that you enter the same password on all servers in the cluster.

- Step 18** Log in to the server by using the local Administrator account and password.
- Step 19** Continue the upgrade by performing the procedure in [“Install Cisco CallManager \(Required\)” section on page 31](#).

**Caution**

After installing the operating system installation and before installing Cisco CallManager, you must configure name resolution for the backup location.

Manually Stop Cisco Services and Do Not Reboot the Server

Manually stop the following services:

- All Cisco services within the Service Control Panel (services.msc).
- MS-SQL Agent
- DC Directory
- SNMP and its dependencies
- IIS Admin and its dependencies
- Network Time Protocol

Verify That the MS-SQL Server Service is Running

Verify that the MS-SQL service is running before you start the Cisco CallManager installation.

Install Cisco CallManager (Required)

Perform the following procedure to install the directory, the database, and Cisco CallManager via CD-ROM. The CD-ROM also prompts you to restore the data that the backup utility stored to a Network Directory or Tape Device.

**Caution**

You may not see any indication that the installation and restoration are progressing. Do not reboot the server unless the installation prompts you to do so. You may not see any activity for up to an hour, depending on the size of your system. Do not remove the CD-ROM until you completely finish the Cisco CallManager installation.

Procedure

- Step 1** After you complete the operating system installation, insert the CD-ROM into the CD-ROM drive. The installation process automatically starts.
- To acknowledge that you disabled/uninstalled Cisco-verified applications, click **Yes**.

**Note**

This extraction may take several minutes. Do not reboot.

- Step 2** The Preparing to Install window displays. Do not click Cancel.
- Step 3** In the Welcome window, click **Next**.
- Step 4** The following message displays: “The Same System Recovery flag was detected. Is this server being configured as a Cisco CallManager Publisher?” Click **Yes**.
- Step 5** Accept the terms of the license agreement by clicking the **I accept the terms in the license agreement** radio button and click **Next**.

- Step 6** In the Customer Information window, the User Name and Organization that you entered during the operating system installation display.
Cisco automatically populates the product key fields with the product key that you entered during the operating system installation. Click **Next**.
- Step 7** In the Setup Type window, click the **Complete** radio button; then, click **Next**.
- Step 8** In the Setup Type window, click the **Publisher** radio button; then, click **Next**.



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.

- Step 9** In the Administrator Password window, enter the Administrator password that you entered during the operating system installation.
- Step 10** In the SQL Password window, perform the following procedure:
- a. Enter the SA (SQL Server system administrator) password.
 - b. Press the **Tab** key.
 - c. To confirm the password, enter the password again; then, click **Next**.
- Step 11** In the Ready to Install the Program, click **Install**.
The status bar indicates the progression of the installation. Continue to wait while the installation completes.
Microsoft SQL Server 2000, Microsoft SQL Server 2000 Service Pack 2.0, and DC Directory install. This process takes 15 to 20 minutes.
- Step 12** To reboot the server, click **Yes**. Do not remove the CD-ROM from the CD-ROM drive.
- Step 13** Log in to the server by using the Administrator password.
- Step 14** The Cisco CallManager installation automatically launches. Continue to wait while the Cisco CallManager installation completes.
- Step 15** The Cisco IP Telephony Applications Restore Utility automatically launches the restoration of the Cisco CallManager data that you stored to a network directory or tape device.
- Step 16** In Step 1 of the restore utility, perform the following procedure:
- a. Choose the location of the data, the place where the data is stored.
If you chose a network directory, you must browse to and manually highlight the MCS.sti file. Failure to highlight the file causes the upgrade to fail.
 - b. Enter a username and password with administrator access rights on the server and then click **Verify**.
 - c. When you receive the authentication results in the dialog box, click **OK**.
 - d. Click **Next**.
- Step 17** In Step 2 of the restore utility, perform the following procedure:
- a. Highlight the CallManager target, which is the server that you want to restore.
 - b. Make sure that the SA password remains blank; then, click **Verify**.
 - c. A dialog box shows that authentication occurred successfully. Click **OK**.
 - d. Click **Next** to continue.
- Step 18** To accept that you will overwrite the target server and lose all existing data if you proceed, click **Yes**.

The utility restores the files to the server where you want the utility to send the files.

- Step 19** The restoration log displays. Verify that no errors exist in the log. If the following error messages or other error messages display in the log file, the process did not successfully restore the data:
- Failed to drop CCM/ART/CDR database from <Server Name>
 - Failed to restore DC Directory
 - Failed to stop DC Directory service
 - Failed to restart DC Directory service
- Step 20** After you verify that no errors exist, click **OK**.
- The Cisco CallManager installation takes approximately 45 to 90 minutes. Although you may see no indication that the installation is progressing, continue to wait while the installation completes.
- Step 21** After the installation completes, click the **Finish** button.
- Step 22** When a prompt asks you to reboot the server, click **Yes**.
- Step 23** After you reboot the server, remove the CD-ROM from the CD-ROM drive.
- Step 24** Log on to the server by using the Administrator password.
- Step 25** Verify that your data and configuration restored to the server.
- Step 26** If the publisher database server is the only server where you plan to install Cisco CallManager, see the [“Procedures for Installing the Cisco CallManager Support Patch \(Recommended\)”](#) section on page 37 to install the Cisco CallManager support patch.
- If you have subscriber servers that you need to install, see the [“Procedures for Upgrading Subscriber Database Servers \(Required\)”](#) section on page 34. Then, install the support patch on all servers in the cluster.

Back Up the Current Database (Required)



Caution

When you back up the entire database on the publisher database server, do not overwrite the data that you backed up before the migration. To retain the backup file, you must archive or rename the existing MCS.sti file before you perform this backup.

For procedures and more information on backing up the database, refer to *Using the Cisco IP Telephony Backup Utility, Version 3.5.18* (or later).

Procedures for Upgrading Subscriber Database Servers (Required)

Table 4 describes how to upgrade the subscriber database servers.

Table 6 Required Upgrade Tasks for the Subscriber Servers



Step	Task	Important Information and Resources
Step 1	Perform pre-upgrade tasks.	See the “ What pre-upgrade tasks should I perform? ” section on page 19.
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 22.
Step 3	Verify that you have disabled and stopped all third-party Cisco-verified applications that run on the server. Make sure that you have rebooted the server.	See the “ Disable and Stop Third-Party Cisco-Verified Applications and Reboot the Server (Required) ” section on page 23.
Step 4	Verify that you have run the Cisco CallManager HealthCheck Utility on every server in the cluster.	See the “ Run the Cisco CallManager HealthCheck Utility ” section on page 24.
Step 5	Run the ServPrep utility.	See the “ Run the ServPrep Utility (Required) ” section on page 35.
Step 6	Manually stop Cisco services, and do not reboot the server.	Manually stop the following services: <ul style="list-style-type: none"> • All Cisco services within the Service Control Panel (services.msc) • MS-SQL Agent, MS-SQL Server, and other SQL dependencies • DC Directory • SNMP and its dependencies • IIS Admin and its dependencies • Network Time Protocol
Step 7	Using the Cisco-provided operating system CD-ROM, install Cisco-provided operating system 2000.2.3 (or later).	 <p>Caution Make sure that you choose Same Server Recovery when you perform the operating system installation. This choice ensures that you save configured data.</p> <hr/> <p>See the “Install the Operating System By Using Same Server Recovery (Required)” section on page 29. Consider the same guidelines for the subscriber servers that you used for the publisher database server.</p>

Table 6 Required Upgrade Tasks for the Subscriber Servers (continued)

Step	Task	Important Information and Resources
Step 8	Start the MS-SQL Server service on the server.	You must start the MS-SQL service before you start the Cisco CallManager upgrade.
Step 9	Perform the Cisco CallManager installation on one server at a time.	Refer to <i>Installing Cisco CallManager Release 3.3(2)</i> . See Table 1 .  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.
Step 10	After each subscriber installation, verify that the subscriber server pulled the subscription from the publisher database server.	See the “Verifying and Reinitializing Subscriber Connections” section on page 36.
Step 11	After you complete the installation on all servers in the cluster, perform post-upgrade tasks.	See the “Procedures for Post-Upgrade Tasks” section on page 38.

Run the ServPrep Utility (Required)

Before you install Cisco CallManager, you must run the ServPrep Utility and install Cisco-provided operating system version 2000.2.3 or later by using the Cisco-provided operating system CD-ROMs.

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 that meet Cisco-approved configuration standards. Do not run this utility on any other servers, including the Cisco ICS 7750 or any other customer-provided servers.

Procedure

- Step 1** Insert the Cisco CallManager Subscriber Upgrade CD-ROM into the CD-ROM drive as soon as you are able to 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.
 - Step 4** See [Table 4](#) to continue the subscriber server installation.
-

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 replicate the database to the subscribers.

Verifying the Status of the Subscription

In the Enterprise Manager, a red X icon next to the subscription indicates that 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 7 > 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).

Procedures for Installing the Cisco CallManager Support Patch (Recommended)

After you install this version of Cisco CallManager on all servers in the cluster, Cisco strongly recommends that you install the latest Cisco CallManager support patch on all servers in the cluster. These support patches provide additional utilities and bug fixes for your system.

Be aware that Cisco CallManager support patches are cumulative. Cisco always rolls these utilities and bug fixes into the next Cisco CallManager release.

**Tip**

Make sure that you install the same version of the support patch on every server in the cluster.

To obtain the latest Cisco CallManager support patch, perform the following procedure:

Procedure

-
- Step 1** Click <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.
 - Step 2** Click **Cisco CallManager Version 3.3**.
The Cisco CallManager 3.3 software page displays.
 - Step 3** Locate and download the readme file for the support patch.
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 support patch on every server in the cluster where Cisco CallManager is installed.
 - Step 5** Perform other post-upgrade tasks.
-

Procedures for Post-Upgrade Tasks

After you complete the upgrade, perform the appropriate tasks as described in [Table 7](#):

Table 7 Post-Upgrade Tasks

Post-Upgrade Task	Related Information and Procedures
<p>Enable all Cisco-verified applications/program agents that you previously disabled on the server.</p> <p>If you have not already done so, set all Cisco-approved McAfee antivirus services to Enable through the Control Panel.</p> <p>If you have Cisco IDS Host Sensor installed on the server, you must enable and start the following services, if you have not already done so:</p> <ul style="list-style-type: none"> • intercept Agent • intercept Watchdog • intercept Notification Manager • intercept Server 	<p>Refer to the following information:</p> <ul style="list-style-type: none"> • The documentation that accompanies your application • Enabling Cisco-Verified McAfee Antivirus Services, page 40 • For information on the Cisco IDS Host Sensor, click the following URL: http://www.cisco.com/warp/public/788/AVVID/ids_host_sensor_cm.html
<p>If you have not already done so, verify that the subscriber servers pulled the copy of the database.</p>	<p>See the “Verifying and Reinitializing Subscriber Connections” section on page 36.</p>
<p>Verify that all services started.</p> <p>Verify that you can make internal calls.</p> <p>Verify that you can place and receive a call across gateways.</p> <p>Verify that all Cisco IP telephony applications that are integrated with Cisco CallManager run properly.</p>	<p>See the “Verifying Services, Patches, and Hotfixes” section on page 40.</p> <p>See the “Viewing the Component Versions That Are Installed on the Server” section on page 41.</p> <p>Refer to the <i>Cisco CallManager Compatibility Matrix</i>, which provides compatibility information and workarounds for applications that are integrated with Cisco CallManager.</p>
<p>After you complete the upgrade on every server in the cluster, you must reinstall Cisco-verified applications that were previously installed on the server.</p>	<p>Refer to the appropriate documentation that accompanies the applications.</p>
<p>If you have CRS and Cisco CallManager installed on the same server, complete the upgrade by referring to the appropriate documentation.</p>	<p>See the “How does a co-resident upgrade work if I have CRS installed with Cisco CallManager?” section on page 16.</p>
<p>Upgrade Cisco TAPI, Cisco JTAPI, Cisco TSP (for the voice-mail system), and the Cisco TSP for Cisco SoftPhone.</p>	<p>See the following sections for more information:</p> <ul style="list-style-type: none"> • Upgrading TAPI, JTAPI, and Cisco Telephony Service Provider (TSP), page 41 • Upgrading the Cisco TAPI/TSP for Cisco SoftPhone, page 41

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Task	Related Information and Procedures
If you need to do so, upgrade the Cisco IP telephony applications that are integrated with your Cisco CallManager system.	Refer to the <i>Cisco CallManager Compatibility Matrix</i> by clicking the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm If the application is compatible with this version of Cisco CallManager, refer to the appropriate Cisco IP telephony application documentation.
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.	Click the following URL to obtain the locale and the installer documentation: http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-33
On the Cisco CallManager NIC and the switch port where the NIC is connected, configure the Speed and Duplex settings to the same value to optimize performance.	Some administrators have found that the 100/Full setting works well.
Review the post-installation tasks section of the Cisco CallManager installation document for additional tasks/requirements that apply to your system; for example, configuring DNS. Review operating system recommendations in the document, <i>Installing the Operating System on the Cisco IP Telephony Application Server</i> .	Refer to <i>Installing Cisco CallManager Release 3.3(2)</i> .
Ongoing System Management Practice Run the Cisco CallManager HealthCheck Utility on every server in the cluster.	See the “ Run the Cisco CallManager HealthCheck Utility ” section on page 24.
Ongoing System Management Practice Back up your Cisco CallManager data.	Refer to <i>Using the Cisco IP Telephony Applications Backup Utility, Version 3.5.18</i> (or later). See Table 1 .
Ongoing System Management Practice Verify the version of hotfixes and service packs that are installed on the server. Download the latest hotfixes, service packs, and Cisco CallManager support patches that are available on the web. This task requires a reboot of the server after you install the files.	Verifying Services, Patches, and Hotfixes, page 40

Enabling Cisco-Verified McAfee Antivirus Services

To enable the Cisco-verified McAfee antivirus services, perform the following tasks:

Procedure

-
- Step 1** After you log in to the server, enable all Cisco-verified McAfee antivirus services through the Control Panel by completing the following procedure:
- a. Choose **Start > Settings > Control Panel > Administrative Tools > Services**.
 - b. From the Services window, right-click one of the antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, or Network Associates Task Manager, and choose **Properties**.
 - c. Verify that the General tab displays in the Properties window.
 - d. From the Startup type drop-down list box, choose **Automatic**.
 - e. Click **OK**.
 - f. In the Services window, right-click the antivirus service and click **Start**.
- Step 2** Perform [Step 1](#) to enable all Cisco-approved McAfee antivirus services; for example, Network Associates Alert Manager, Network Associates McShield, and Network Associates Task Manager.
-

Verifying Services, Patches, and Hotfixes

Perform the following tasks:

- Verify that the appropriate services run on each server in the cluster ([About Services, page 40](#))
- Verify that you have installed the latest Microsoft patches and hotfixes ([About Microsoft Patches and Hotfixes, page 40](#))
- Verify that you have installed the latest Cisco CallManager support patches ([About Cisco CallManager Support Patches, page 40](#))

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*. See [Table 1](#).

About Cisco CallManager Support Patches

See the [“Procedures for Installing the Cisco CallManager Support Patch \(Recommended\)”](#) section on [page 37](#).

Viewing the Component Versions That Are Installed on the Server

The stiver.exe program reports the current version of all installation components, including such components as the operating system, upgrade, and backup and restore utility. 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 CD-ROMs during the initial installation, no longer exist on the system.

The version for OS Image equals your operating system CD-ROM 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 CD-ROM (CD #1).

The version for stiOSUpd.exe equals the version of the operating system upgrade that you last ran either via CD-ROM or via the web. When Cisco updates and releases the Cisco IP Telephony Server Operating System OS/BIOS Upgrade CD-ROM (CD #2), the version of stiOSUpd 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:\sti\stiver
- 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-mail 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 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 `http://<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 plugin.
- Step 4** Follow the prompts in the window to complete the upgrade.
- Step 5** Verify that a basic call works as expected for Cisco SoftPhone.
-

Using the Cisco CallManager Music On Hold CD-ROM 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 CD-ROM.

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 CD-ROM
- ciscocm-MusicOnHoldSampler, which is a small set of files that offers a sample of music that is available on the CD-ROM

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 CD-ROM/file with music on hold. Because of licensing restrictions, you must not distribute the Cisco CallManager Music on Hold CD-ROM/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 Pull a Drive Before the Upgrade

This procedure assumes that you have a good backup file (MCS.sti file) on a tape device or network directory.

Perform the following procedure:

Procedure

-
- Step 1** Perform the following procedure, depending on if 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 200.2.3 or later. You must perform this task by using the Cisco-provided CD-ROMs that shipped with Cisco CallManager Release 3.3(2).
- Step 3** Using the CD-ROMs that originally shipped with Cisco CallManager, reinstall a version of Cisco CallManager 3.0, 3.1, or 3.2 (depends on the original CD-ROMs). Do not install or configure the backup utility that automatically displays during the installation.
- Step 4** Install and configure Cisco IP Telephony Applications Backup Utility 3.5.18 (or later) by using the Cisco CallManager Publisher Upgrade CD-ROM that shipped with Cisco CallManager Release 3.3(2).
- 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 200.2.3 or later. You must perform this task by using the Cisco-provided CD-ROMs that shipped with Cisco CallManager Release 3.3(2).
- Step 8** Using the CD-ROMs that originally shipped with Cisco CallManager, reinstall a version of Cisco CallManager 3.0, 3.1, or 3.2 (depends on the original CD-ROMs). 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 Cisco IP Telephony Applications Backup Utility 3.5.18 or later by using the Cisco CallManager Publisher Upgrade CD-ROM that shipped with Cisco CallManager Release 3.3(2).

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 between 30 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-7845-1400, 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-7845-1400, also slightly pull the drive in Slot 3. Do not completely remove the drives from the server.
- Step 4** Power on the system.

Cisco MCS

- Step 5** Perform the following procedure for all Cisco MCS where you removed a drive:
- To enable interim recovery mode on the MCS-7830, MCS-7835, or MCS-7845-1400, press **F2**.
 - This step applies only for the MCS-7830, MCS-7835, or MCS-7845-1400. When prompted, press **F1** to continue.
 - Push the drive into Slot 1 that was slightly pulled in [Step 3](#).
 - For the MCS-7830, MCS-7835, or MCS-7845-1400, choose **Start > Compaq Systems Tools > Compaq Array Configuration Utility**.
 - Watch the status bar in the lower, right corner to determine when drive mirroring completes.
 - This step applies only for the MCS-7845-1400. After the mirroring process completes in Slot 1, push the drive into Slot 3 that was pulled in [Step 3](#).
 - Verify that the process completed successfully.

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** Using the arrow keys, press **Exit**.
- Step 14** Press **Ctrl + Alt + Del**.
- Step 15** Log in to the server by using the Administrator password.
- Step 16** Push the drive into Slot 1 that was slightly pulled in [Step 3](#).



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 17** Choose **Start > Programs > ServeRaid Manager > ServeRaid Manager**. You can view the progression of the drive mirroring.
 - Step 18** 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. See [Table 1](#) 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 `http://<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** Follow the prompts in the window to complete the installation.
- Step 6** Perform this procedure on all servers where the application is installed.

Error Messages

The following error 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 8 *Installation Error Messages*

Error Message	Reason	Corrective Action
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.

Table 8 *Installation Error Messages (continued)*

Error Message	Reason	Corrective Action
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.
The passwords 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.
You must have intrusion detection, anti-virus protection software, or any third-party applications uninstalled before you continue with the Cisco CallManager installation. Failure to do so could cause 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 (Architecture for Voice, Video and Integrated Data) Partner Applications] or platform agents installed on the server, you must disable/uninstall and stop the services.
Error opening MSI package	Cisco CallManager Setup cannot find the MSI package.	This message displays if the you encounter a media problem; insert the CD-ROM again.
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 CD-ROM from the CD-ROM 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 CD-ROM from the CD-ROM drive.
An unexpected error occurred.	An error occurred during the Cisco CallManager Setup.	Obtain and examine the log file.
An unexpected error occurred while constructing package name.	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.

Table 8 *Installation Error Messages (continued)*

Error Message	Reason	Corrective Action
Unable to connect to <server name>	The installation cannot find the file, Dbname.ini, if the passwords that you enter on the server(s) do not match.	The publisher database server is not available; DNS is not implemented.
Current OS version does not meet minimum requirements. Aborting Cisco CallManager install.	Cisco CallManager Release 3.3(2) requires Cisco-provided operating system version 2000.2.3 or later.	Refer to <i>Cisco IP Telephony Operating System, SQL Server, Security Updates</i> to review which versions are compatible for installation.
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), see Table 1 .
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.
Failure occurred trying to determine if Cisco Directory install succeeded. Aborting Cisco CallManager install.	The DC Directory installation failed.	Obtain and examine the log file.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 web sites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can email your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. 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 monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:
http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:
http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Copyright © 2002. Cisco Systems, Inc.
All rights reserved.