



Installing Cisco CallManager Release 4.2(1)

Product Key for Cisco CallManager: BTOO VQES CCJU IEBI



Note

The Cisco CallManager product key, which you enter during the operating system installation, allows you to install Cisco CallManager on a server that is dedicated solely to that application. If you want to install Cisco CallManager with Cisco IP Contact Center Express Edition, or Cisco CallManager with Cisco IP Interactive Voice Response on the same server, refer to the Cisco Customer Response Solutions (CRS) installation documentation for the product keys.

This document includes information about installing Cisco CallManager for the first time and reinstalling Cisco CallManager, if necessary.

This document applies if you have one server or many servers in a cluster environment.

Contents

This document contains the following topics:

Locating Documents and Information

- [Locating Related Cisco CallManager Documentation, page 3](#)
- [Important Considerations, page 5](#)
- [Frequently Asked Questions About the Cisco CallManager Installation, page 6](#)
 - [How long does it take to perform the Cisco CallManager installation?, page 6](#)
 - [How does the Cisco CallManager installation work?, page 7](#)
 - [Which servers does Cisco support for this installation?, page 8](#)
 - [May I install other software besides Cisco CallManager on the server?, page 9](#)
 - [May I run a web browser on the server?, page 9](#)
 - [May I add Cisco CallManager servers as members of a Windows domain?, page 10](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [May I configure a server in the cluster as a Domain Controller?](#), page 10
- [May I use Terminal Services, Virtual Network Computing, and Integrated Lights Out to remotely install the application?](#), page 11

Installation Tasks and Information

- [Performing Preinstallation Tasks](#), page 12
- [Installing Cisco CallManager on the Publisher Database Server](#), page 16
- [Installing Cisco CallManager on Subscriber Database Server\(s\)](#), page 19
- [Install the Cisco CallManager Service Release \(when available on cisco.com\)](#), page 26

Postinstallation Tasks and Information

- [Performing Postinstallation Tasks](#), page 21
- [Activating Cisco CallManager Services](#), page 23
- [Configuring the Database](#), page 25
- [Downloading Service Releases and Hotfixes for Ongoing System Management](#), page 25
- [Viewing the Component Versions That Are Installed on the Server](#), page 26
- [Using the Cisco CallManager Music On Hold Disk or Download](#), page 27

Verifying and Re-creating Subscription Connections

- [Verifying and Reinitializing Subscriber Connections](#), page 30

Installation Error Messages

- [Analyzing Error Messages](#), page 31

Documentation Resources and Technical Assistance

- [Obtaining Documentation](#), page 48
- [Obtaining Technical Assistance](#), page 50

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

Conventions

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

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.

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

Locating Related Cisco CallManager Documentation

Cisco strongly recommends that you review the following documents before you perform the Cisco CallManager installation:

- *Release Notes for Cisco CallManager Release 4.2*

This document lists and describes the system requirements, new features, changed information, documentation updates, and open caveats for Cisco CallManager. Cisco provides versions of this document that match the version of the installation document.

- *Installing the Operating System on Cisco IP Telephony Applications Servers*

This document, a companion guide to this installation document, provides information and procedures on installing the operating system on Cisco IP Telephony Applications Servers. This document does not provide Cisco IP telephony application installation procedures. Refer to this document before you install Cisco CallManager, Cisco Personal Assistant, Cisco Conference Connection, or one of the products from the Cisco Customer Response Solutions (CRS) platform.

- *Cisco CallManager Administration Guide* and *Cisco CallManager System Guide*

The *Cisco CallManager Administration Guide* provides step-by-step instructions for configuring, maintaining, and administering the Cisco CallManager voice over IP network.

The *Cisco CallManager System Guide* provides descriptions of the Cisco CallManager system and its components, configuration checklists, and links to associated *Cisco CallManager Administration Guide* procedures.

- *Cisco CallManager Features and Services Guide*

This document describes how to configure features and services for Cisco CallManager, including Cisco Music On Hold, Cisco CallManager Extension Mobility, and so on.

- *The Cisco CallManager Serviceability System Guide* and *Cisco CallManager Serviceability Administration Guide*

This document provides descriptions of Cisco CallManager serviceability and remote serviceability and step-by-step instructions for configuring alarms, traces, and other reporting.

- *Cisco CallManager Bulk Administration Guide*

This document provides information on using the Bulk Administration Tool (BAT) to perform bulk add, update, and delete operations on phones, users, gateways, and ports.

- Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*

This document describes how to install the utility, configure the backup settings, back up Cisco CallManager data, and restore the data.
- Cisco CallManager Security Guide*

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

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

Affected applications may include Cisco Conference Connection, Cisco SoftPhone, Cisco 186 Analog Telephony Adapter, Cisco Personal Assistant, Cisco Response Solutions (CRS), Telephony Application Programming Interface and Java Telephony Application Programming Interface (TAPI/JTAPI) applications, including Cisco-supported 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 installation 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, Cisco Customer Response Applications/Solutions, and Cisco Emergency Responder.
- The appropriate Cisco IP telephony application documentation

Locate the release notes, installation/upgrade, and configuration guides for the applications that you want to integrate with Cisco CallManager.

Table 1 lists URLs for software, product keys, and other related documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
<i>Cisco IP Telephony Operating System, SQL Server, Security Updates</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Operating system installation, Virtual Network Computing (VNC), and Cisco Media Convergence Server (MCS) Network Teaming Driver documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
<i>Cisco CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

Table 1 Quick Reference for URLs (continued)

Related Information and Software	URL
<i>Cisco CallManager Security Guide</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm
Cisco CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco CallManager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Important Considerations

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

- Cisco CallManager requires a minimum of 1 GB of memory on the Cisco CallManager servers. To avoid system problems, such as dropped calls, verify that your servers have a minimum of 1 GB of memory installed. If the installation process detects less than 1 GB memory on the publisher server, the installation aborts. The installation process performs a similar check on the Cisco CallManager subscriber server; it allows the installation to continue if it detects less than the minimum requirement.
- Install the Cisco CallManager software on the publisher server first and then on the subscriber server(s).
- You cannot add a subscriber server to a cluster by installing a previous version of Cisco CallManager and then upgrading the subscriber server to the same version that is running on the publisher server. If you are adding a new subscriber server or replacing a subscriber server on the cluster, you must use the installation CDs with the same Cisco CallManager version that is running on the publisher server.
- Make sure that you are logged in as the administrator on the server before starting the Cisco CallManager installation.
- Install the Cisco CallManager software on one server at a time to ensure that subscriber servers can receive replicate copies of the database from the publisher database server.
- Make sure that the subscriber server that you are installing can connect to the publishing database server during the installation.
- Do not choose cancel after you start the installation. If you choose cancel, you will need to reimage your machine by reinstalling the operating system.
- Because security settings for the Cisco CallManager server are set up by the installation and upgrade script, do not make any adjustments to these predefined settings, or you may experience a significant impact to the functionality of your server.
- When entering passwords for the local Administrator and SA (SQL Server system administrator) accounts, use alphanumeric characters only.
- Enter the same administrator password on all servers in the cluster.

- Install the Cisco CallManager software during off-peak hours or during a maintenance window to avoid impact from call-processing interruptions.
- Do not implement multiple servers in a Cisco CallManager cluster by using a drive that was mirrored or cloned from a single Cisco CallManager server. This results in servers having duplicate Security ID (SID) and impairs Cisco CallManager operations. You must install the Cisco IP telephony operating system and Cisco CallManager software separately on each server by using the Cisco-provided installation disks.
- Do not configure any server in the cluster as a Domain Controller.
- Place the server in a Workgroup before you install the software.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco IP Phones can register with the application when you plug the phones into the network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not use terminal services to install the Cisco CallManager software
- Do not install any Cisco-verified applications until you complete installing Cisco CallManager on every server in the cluster.
- Cisco provides support for a limited set of applications on the servers where Cisco CallManager is installed. If you are uncertain whether a third-party application is supported, do not install it on the server.
- You must disable third-party, Cisco-verified applications on your servers before starting the Cisco CallManager installation.
- Install a security agent to protect your servers against unauthorized intrusion.
- Do not install Cisco Unity on a server where Cisco CallManager is installed.
- Installing or using Netscape Navigator on the Cisco MCS or the Cisco-approved, customer-provided server causes severe performance problems.
- Carefully read the instructions that follow before you proceed with the installation. See [“Performing Preinstallation Tasks” section on page 12](#), [“Performing the Cisco CallManager Release 4.2 Installation” section on page 11](#), and [“Performing Postinstallation Tasks” section on page 21](#)

Frequently Asked Questions About the Cisco CallManager Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you complete the Cisco CallManager installation.

How long does it take to perform the Cisco CallManager installation?

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes per server, depending on your server type. Before you install Cisco CallManager, consider the size of your cluster.

How does the Cisco CallManager installation work?

Review the following information before you install Cisco CallManager.

Verifying the User Name, Organization Name, and Product Key

Cisco supplies you with a Cisco product key when you purchase a Cisco IP telephony product. The product key, based on a file encryption system, allows you to install only the components that you have purchased, and it prevents other supplied software from being installed for general use. The product key comprises alphabetical letters only.

During the operating system installation, you entered the Cisco CallManager product key. The product key allows you to install Cisco CallManager on a server that is designated for Cisco CallManager only.

During the operating system installation, you registered the software product by entering a user and organization name.

During the Cisco CallManager installation, verify that the correct User Name, Organization Name, and product key display. See the latest version of the operating system documentation for more information.

Entering Passwords

During the Cisco CallManager installation, you must enter a valid password for the following accounts:

- Windows NT Administrator account

If you plan to install Cisco CallManager on the Cisco Media Convergence Server (MCS), you established this password during the operating system installation. If you left the password blank during the operating system installation, or if you enter the wrong password during the Cisco CallManager installation, you cannot install Cisco CallManager on the server.



Tip

Verify that this password is the same on all servers in the cluster. If you change the passwords at any time, you must either log off and log in to the server again, or you must reboot the server and log in to the 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.

- SA (SQL Server system administrator) account
- Directory Manager (DC Directory) account
- Private Password Phrase



Caution

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

Installing the Publisher Database or Subscriber Server

When you install Cisco CallManager, you must determine whether the server will be configured as a publishing database server or a subscriber database server. In a Cisco CallManager distributed system, one server maintains the master, or publisher, database, and all other servers in the cluster maintain

subscriber databases. Subscriber databases provide copies of the master database. During normal operation, all Cisco CallManagers in the cluster read data from and write data to the publisher database. Periodically, Cisco CallManager automatically updates the subscriber databases as needed.

Cisco requires that you first install the publisher database server, so authentication to the database occurs. This decision designates a permanent selection. If you want to reassign the database server type at a later date, you must reinstall Cisco CallManager on the server and choose a different database server type.

**Caution**

If you are configuring a subscriber database server, make sure that the publishing database server for that cluster is installed, connected to the network, and configured properly to work as a distributed system. When configuring a subscriber database server, ensure that the server that you are installing can connect to the publishing database server during the installation. This connection facilitates copying the publisher database from the publisher database server to the local drive on the subscriber server. You must supply the name of the publishing database server and the password for the administrator account on that server. If the publisher server cannot be authenticated during the installation for any reason, the installation will not continue.

You must install one server at a time, or the subscriber servers cannot receive copies of the database from the publisher database server.

Cisco CallManager installs the following software packages:

- Sun Microsystems Java Runtime Environment (JRE)
- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Service Pack 4 (or later)
- DC Directory
- Cisco CallManager

Installing Cisco CallManager Components and Services

The Cisco CallManager installation automatically installs all services that display in the Service Activation window of Cisco CallManager Serviceability. These services install on every server in the cluster. To review a list of installed services, service definitions, and service considerations, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

The Cisco CallManager installation places services in an inactive state until the installation completes. After the installation completes, you must manually activate the service on each server in which you want the service to run. For information on activating services, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Which servers does Cisco support for this installation?

Refer to the *Cisco CallManager Compatibility Matrix* for a list of servers that Cisco CallManager 4.2(1) supports. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

May I install other software besides Cisco CallManager on the server?



Caution

Cisco strongly recommends that you do not install any Cisco-verified applications until you complete the installation on every server in the cluster. If you do not know whether the application is approved for installation, do not install it on the server. Installing unsupported software on the server could cause severe performance problems and call-processing interruptions.

Cisco supports a limited list of applications on the Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server. Consider the following information before you install Cisco CallManager:

- You may install Cisco-verified applications (Cisco Partner Applications), but you must disable and stop these applications before the Cisco CallManager installation and then reboot the server. Disable these applications during installation, restoration, and upgrade procedures.

For more information on supported software, click <http://www.cisco.com/cgi-bin/eco/Search>. In the Solution pane, click **IP Telephony**. From the Solution Category drop-down list box, choose **Operations, Administration, and Maintenance (OAM)**. Click **Search**.

- Installing or using Netscape Navigator on the Cisco MCS or a Cisco-approved, customer-provided server causes severe performance problems. Cisco strongly recommends against installing Netscape Navigator or any other application software on the Cisco MCS or Cisco-approved, customer-provided server.
- Cisco strongly recommends that you install a security agent to protect your servers against unauthorized intrusion. Cisco offers two security agent options: Cisco Security Agent (CSA) for Cisco CallManager and Management Center for Cisco Security Agent (CSA MC). For more information, see the “[Performing Postinstallation Tasks](#)” section on page 21.
- You can install Cisco CallManager and Cisco Customer Response Solutions (CRS) on the same server. Refer to the CRS installation documentation to obtain the coresident installation product key.
- Do not install Cisco Unity on any server where Cisco CallManager is installed.

May I run a web browser on the server?

Cisco strongly recommends that you do not run a web browser on the Cisco MCS or any Cisco-approved, customer-provided server. Running a web browser on the server causes CPU usage to surge.

To access Cisco CallManager Administration, the web-based graphical user interface (GUI) that allows you to perform Cisco CallManager configuration tasks, use a different PC to browse into the Cisco CallManager server that is running Cisco CallManager Administration and log in with administrative privileges.



Tip

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

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

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



Note

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



Note

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

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

- Step 1** Choose **Start > Programs > Administrative Tools > Services**.
- Step 2** Double-click the **Network Time Protocol** service.
- Step 3** In the Startup type field, choose **Disabled**.
- Step 4** Click **Stop**.
- Step 5** Click **OK**.



Caution

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

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

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

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

Cisco strongly recommends that you 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 Cisco CallManager on the server.

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

Do not use Terminal Services or Integrated Lights Out (ILO) to install Cisco CallManager Release 4.2(1). 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. Cisco supports ILO for remote management and configuration tasks only



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 install Cisco CallManager, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm to obtain the latest version of the VNC document.



Caution

If you have installed VNC but do not plan to use it to install Cisco CallManager, disable it to prevent remote access to the server. If you do not disable VNC and a user/administrator accesses the server during the installation, the installation will fail.

What if I encounter problems during the installation?

If you encounter problems during the installation, Cisco recommends that you take the following actions:

1. During the installation if you receive an error message that displays in a dialog box, see the “Analyzing Error Messages” section on page 31 and perform the recommended corrective action.
2. On the server where the problem occurred, obtain and review the log file, ccminst <data/time stamp>.log, from **C:\Program Files\Common Files\Cisco\Logs**.

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.

Performing the Cisco CallManager Release 4.2 Installation

This section contains information about the procedures that are used to complete the Cisco CallManager installation. The section includes the following topics:

- [Performing Preinstallation Tasks, page 12](#)
- [Installing Cisco CallManager on the Publisher Database Server, page 16](#)
- [Installing Cisco CallManager on Subscriber Database Server\(s\), page 19](#)


Performing Preinstallation Tasks

For preinstallation tasks that you must complete before the installation, see [Table 2](#).

Table 2 *Preinstallation Tasks*

Step	Preinstallation Tasks	Important Notes
Step 1	<p>Plan your system configuration.</p> <p>Determine how many Cisco CallManager servers the cluster will contain, which server will house the publisher database, and where backup tasks will be performed.</p> <p>Determine whether each server will act as a dedicated or coresident server.</p>	See “ Planning your System ” section on page 13
Step 2	<p>This task applies for reinstallation.</p> <p>Configure the server to the state of the original configuration.</p>	If you have hot-swappable drives, make sure that you inserted the appropriate drives into the server and ensure that the drives are functional. Remove any additional hard drives that are in the server.
Step 3	<p>Make sure that you installed the operating system version 2000.4.2sr2 (or later) on all dedicated and coresident servers.</p> <p>Use the Cisco IP Telephony Server Operating System OS/BIOS Upgrade Disk that came with the software kit and upgrade the operating system to version 2000.4.2sr2 or later.</p>	<p>Refer to <i>Installing the Operating System on the Cisco IP Telephony Applications Server</i>. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.</p> <p>Before you perform the upgrade, be sure to read the operating system readme information that is posted on the operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.</p>
Step 4	Download and install the latest Cisco IP Telephony Server Operating System service release (2000.4.2sr2 or later).	<p>The operating system service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.</p> <p>For installation instructions, refer to the file-specific readme document, <i>Cisco IP Telephony Operating System, SQL Server, Security Updates, and Installing the Operating System on the Cisco IP Telephony Applications Server</i>. To obtain the most recent version of these documents, go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.</p>
Step 5	Before you install Cisco CallManager, make sure that you removed all servers from a NT or an Active Directory Domain.	See the “ Removing the Servers from a Domain and Join a Workgroup ” section on page 14.
Step 6	Connect the server(s) to the network.	See the “ Installing Cisco CallManager on the Publisher Database Server ” section on page 16.

Table 2 Preinstallation Tasks (continued)

Step	Preinstallation Tasks	Important Notes
Step 7	If your server supports the Cisco Media Convergence Server Network Teaming Driver, you can install and configure this driver, if you choose to do so.	Refer to the driver documentation by clicking the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Step 8	This step applies if you need to reinstall Cisco CallManager. You must disable and stop all third-party, Cisco-verified, and Cisco-provided, coresident applications that are installed on your server. If you have Cisco-verified applications (Cisco Partner Applications) or platform agents that are installed on the server, you must disable and stop the services.	Cisco strongly recommends that you do not install any Cisco-verified applications until you have completed the installation on every server in the cluster. See “Installing Cisco CallManager on the Publisher Database Server” section on page 16.  Caution Reboot the server after you disable and stop these applications. Do not start the applications until you complete the Cisco CallManager installation on every server in the cluster. Before you start the installation, verify that none of the services is running.
Step 9	Close all web browser windows.	If you have an open browser window, Cisco CallManager will reboot the server after the Sun Microsystems JRE package is installed.
Step 10	Locate specific information that you need to install Cisco CallManager.	See the “Gathering Configuration Information” section on page 15.

Planning your System

You can distribute the call-processing load for your system across multiple Cisco CallManagers as a single cluster. A cluster comprises a set of Cisco CallManagers that share the same database.

At a minimum, you should determine how many Cisco CallManager servers the cluster will contain, which server will house the publisher database, and where backup tasks will be performed. Additional planning should include a strategy for distributing the devices (such as phones or gateways) among the Cisco CallManagers in the cluster to achieve the type of distribution that you want.

Determine whether each server will act as a dedicated or coresident server.

In a Cisco CallManager distributed system, one server maintains the master, or publisher, database, and all other servers in the cluster maintain subscriber databases. Subscriber databases provide copies of the master database. During normal operation, all Cisco CallManagers in the cluster read data from and write data to the publisher database. Periodically, Cisco CallManager automatically updates the subscriber copies of the database from the publisher database.

For more information on planning a Cisco CallManager distributed system, refer to the *Cisco CallManager System Guide*.

If you are installing a dedicated server, locate the Cisco CallManager product key in this document. If you are installing Cisco CallManager on a coresident server, refer to the specific Cisco IP telephony application installation documentation for the coresident product key.

Removing the Servers from a Domain and Join a Workgroup

Perform the following procedure to convert any servers that exist in the NT Domain or Microsoft Active Directory Domain:

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 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.
-

Connecting the Server to the Network

Before you begin the installation, make sure that you connect your server to the network.

The servers in [Table 3](#) contain two network interface cards (NIC), but the Cisco IP telephony application supports only one NIC. When you connect the server to the network, use the NIC connector that is listed in the table because the other NIC is automatically disabled during the installation.



Note

You can implement NIC teaming on servers that support the network teaming driver. For information, refer to the Installing the Cisco Media Convergence Server Network Teaming Driver at http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/driver/hp_team.htm.

Table 3 *Connecting to the Network*

Server	NIC Connector
MCS-7825	Use the lower NIC connector.
MCS-7835 and MCS-7845	Use the NIC 1 connector.
IBM xSeries 330 server	Use the upper NIC connector.

Disabling Third-Party Applications, Antivirus Services, and Security Agents

The following applications/platform agents may interfere with the Cisco CallManager installation:

- Antivirus services
- Intrusion detection services
- NetIQ services

- OEM server agents
- Server management agents
- VOIP monitoring/performance monitoring
- Remote access/remote management agents
- Cisco-provided, coresident applications

About Disabling McAfee Antivirus Services

Before you perform Cisco CallManager installation procedures, you must disable and stop all Cisco-approved McAfee antivirus services. You can enable and start all antivirus services after you complete the procedures.

About Disabling Security Agents

Before you perform Cisco CallManager installation procedures, you must disable and stop all security agents, including Cisco Security Agent for Cisco CallManager. You can enable and start the services after the installation.

For Cisco-Verified, Third-Party Applications

To review a list of Cisco-verified applications that you should disable and stop before the installation, click the following URL: <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**.

Use the following procedure to disable third-party applications, antivirus services, or security agents:

-
- Step 1** Choose **Start > Programs > Administrative Tools > Services**.
 - Step 2** Locate the third-party application, antivirus service, or security agent that you want to stop, right-click Cisco Security Agent, and choose Properties.
 - Step 3** In the Properties window, click the General tab.
 - 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**.
-

Gathering Configuration Information

[Table 4](#) shows the information that is required for installing Cisco CallManager on your server. Complete all fields unless otherwise noted. Gather this information for each Cisco CallManager server that you are installing in the cluster. Make copies of this table and record your entries for each server in a separate table.

Table 4 *Installation Data for Cisco CallManager*

Configuration Data	Your Entry
Workgroup name	
Database server <ul style="list-style-type: none"> • Publisher Server Name • Subscriber(s) Server Name(s) 	
Administrator password (Use the same password on every server in the cluster)	
SA (SQL Server system administrator) password (Use the same password on every server in the cluster)	
Directory Manager (DC Directory) password (Use the same password on every server in the cluster)	
Private Password Phrase for the Cluster (Use the same phrase on every server in the cluster)	



Note

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

Installing Cisco CallManager on the Publisher Database Server

Items Needed: Cisco CallManager Installation, Upgrade, and Recovery Disks 1 and 2

For the publisher database server, the installation takes 45 to 90 minutes, depending on the server type. Use the following procedure to perform the installation.



Note

Critical third-party components that Cisco CallManager requires and installs may require multiple reboots during installation, and you may need to manually restart the installation program and reenter the configuration data.



Caution

Do not remove the Cisco CallManager Installation, Upgrade, and Recovery Disks until the installation procedure directs you to do so.

Procedure

- Step 1** After you install the operating system and log in to the server by using the Administrator account and password, obtain the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 and insert it into the drive.



Note Follow the instructions in the dialog box. On most windows, you can choose **Next** to proceed with the installation. When prompted to enter a password, remember to record your entry.

- Step 2** To acknowledge that you disabled/uninstalled all Cisco-verified applications, click **Yes**.
- Step 3** To confirm that you may be prompted to reboot the server and reenter configuration data multiple times for Cisco CallManager to install critical third-party components, click **OK**.
- Step 4** In the Welcome window, click **Next**.
- Step 5** Accept the Cisco CallManager license agreement by clicking the **I accept the terms in the license agreement** radio button; then, click **Next**.
- Step 6** In the Customer Information window, the User Name and Organization that you entered during the operating system installation automatically display.
- Cisco automatically populates the product (CD) key fields with the product key that you entered during the operating system installation. Click **Next**.
- Step 7** In the Server Type window, the **Publisher** button is chosen; click **Next**.

Cisco requires that you install Cisco CallManager on the publisher database server first, so authentication can occur between the publisher database and subscriber servers.



Note The publisher database server serves as the master database for all servers in the cluster. All servers except the publishing database server maintain subscriber databases, which are copies of the publisher database server. If you are configuring a subscriber database server, make sure that the server that you are installing can connect to the publishing database server before the installation can continue. The installation process necessitates this connection, so the publisher database server can be copied to the local drive on the subscriber server. To make sure that a good connection exists between the servers, issue a ping command from the subscriber server to the publisher database server before you try to authenticate to it. If the ping command is not successful, you must exit the installation program, fix the problem, and begin the installation process again.



Caution

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

- Step 8** In the Administrator Password / Private password phrase window, do the following:
- Enter the local Windows administrator password.
 - Enter a Private Password Phrase for the cluster; then, reenter it for confirmation.
- The private password phrase contains 1 to 15 characters. This phrase may contain English lower-case letters, English upper-case letters, Westernized Arabic numerals, and the following nonalphanumeric special characters: { } . < > : ? / | \ ` ~ ! @ \$ ^ & * () _ - +.
- Click **Next**.

- Step 9** In the Database passwords window, do the following tasks:
- a. Enter a SQL system administrator (SA) password; then, reenter it for confirmation.
 - b. Enter a Directory Manager password; then, reenter it for confirmation.

Step 10 Now that the Cisco CallManager and other included software are ready to be installed, click **Install**.

Step 11 To reboot the server, click **Yes**.

Step 12 After the server reboots, log in with the Windows Administrator account.

The installation starts. The Cisco CallManager installation takes about 30 to 45 minutes, depending on your server type.



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

Step 13 When prompted, insert Cisco CallManager Installation, Upgrade, and Recovery Disk 2 of 2 and click **OK**.

The installation program continues to install files on your server. Continue to wait while the installation completes.



Note Do not use Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 on another server until you complete the installation process on this server. Before you complete the installation, the installation program prompts you to reinsert Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2.

Step 14 When prompted, insert Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again and click **OK**.

Step 15 When the Cisco CallManager installation completes, click **Finish** to exit the wizard.

The restart server dialog box displays.

Step 16 To restart the server, click **Yes**.



Note You cannot install Cisco CallManager on a subscriber server until you reboot the publisher server.

Step 17 After the server reboots, remove the disk from the drive.

Step 18 Log in to the server by using the Administrator password.

Step 19 If you are installing Cisco CallManager on subscriber server(s), go to [“Installing Cisco CallManager on Subscriber Database Server\(s\)” section on page 19](#). If you are not installing Cisco CallManager on the subscriber server(s), go to [“Performing Postinstallation Tasks” section on page 21](#).

Installing Cisco CallManager on Subscriber Database Server(s)



Note

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



Note

Critical third-party components that Cisco CallManager requires and installs may require multiple reboots during installation, and you may need to manually restart the installation program and reenter the configuration data.

Items Needed: Cisco CallManager Installation, Upgrade, and Recovery Disks 1 and 2

After you install Cisco CallManager on the publisher database server, you install the application on the subscriber database servers. For each subscriber database server, the installation takes 45 to 90 minutes, depending on the server type.



Caution

Perform the installation on one server at a time. This process ensures that the subscriber server(s) can receive a copy of the database from the publisher database server.



Caution

Do not remove the Cisco CallManager Installation, Upgrade, and Recovery Disks until the installation procedure directs you to do so.

Procedure

- Step 1** After you install the operating system and log in to the server by using the Administrator account and password, obtain the Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 and insert it into the drive.
- Step 2** To acknowledge that you disabled/uninstalled all Cisco-verified applications, click **Yes**.
- Step 3** To confirm that you might be prompted to reboot the server and reenter configuration data multiple times for Cisco CallManager to install critical third-party components, click **OK**.
- Step 4** Click **Next** in the Welcome window.
- Step 5** Accept the Cisco CallManager license agreement by clicking the **I accept the terms in the license agreement** radio button; then, click **Next**.
- Step 6** In the Customer Information window, the User Name and Organization that you entered during the operating system installation automatically display.
Cisco automatically populates the product key fields with the product key that you entered during the operating system installation. Click **Next**.



Note The publisher database server functions as the master database for all servers in the cluster. All servers except the publishing database server maintain subscriber databases, which are copies of the publisher database server. If you are configuring a subscriber database server, make sure that the server that you are installing can connect to the publishing database server, so the installation can continue. The installation process necessitates this connection, so the publisher database server can be copied to the local drive on the subscriber server. To make sure a good connection exists between the servers, issue a ping command from the subscriber server to the publisher database server before you try to authenticate to it. In the status of the ping command, verify that the IP address displayed is the IP address of the publisher database server. If the ping command is not successful, you can also try to access the publisher database server from all subscriber servers by choosing **Start > Run**, entering \\<Publisher Server Name>\C\$, and then by clicking **OK**. You do not need to enter a user name and password. Mapping to the drive without entering a user name and password ensures that the passwords on the publisher and subscriber servers match. If the subscriber database server cannot access the publisher server, you must exit the installation program, fix the problem, and begin the installation process again on the subscriber server.

- Step 7** In the Server Type window, perform the following procedure:
- Click the **Subscriber** radio button.
 - Enter the computer name of the publisher database server.



Caution If you enter the IP address or fully qualified DNS of the publisher database server, the installation fails.

- Click **Next**.



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

- Step 8** In the Administrator Password / Private password phrase window, do the following tasks:
- Enter the local Windows administrator password.
 - Enter the Private Password Phrase for the cluster; then, reenter it for confirmation.
 - Click **Next**.
- Step 9** In the Database passwords window, do the following tasks:
- Enter the SQL system administrator (sa) password for the cluster; then, reenter it for confirmation.
 - Click **Next**.
- Step 10** Now that the Cisco CallManager and other included software are ready to be installed, click **Install**.
- Step 11** To reboot the server, click **Yes**.
- Step 12** After the server reboots, log in with the Windows Administrator account.
- The installation starts. The Cisco CallManager installation takes about 30 to 45 minutes, depending on your server type.



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

- Step 13** When prompted, insert Cisco CallManager Installation, Upgrade, and Recovery Disk 2 of 2 and click **OK**.

The installation program continues to install files on your server. Continue to wait while the installation completes.



Note Do not use Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 on another server until you complete the installation process on this server. Before you complete the installation, the installation program prompts you to reinsert Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2.

- Step 14** When prompted, insert Cisco CallManager Installation, Upgrade, and Recovery Disk 1 of 2 again and click **OK**.
- Step 15** When the Cisco CallManager installation completes, click **Finish** to exit the wizard.
- Step 16** To restart the server, Click **Yes**.
- Step 17** After the server reboots, remove the disk from the drive.
- Step 18** Log in by using the Administrator account and password.
- Step 19** After you install Cisco CallManager on all subscriber server(s), go to the [“Performing Postinstallation Tasks” section on page 21](#).
-

Performing Postinstallation Tasks

After installing Cisco CallManager on your server, you must set some configuration parameters for Cisco CallManager and perform other post-installation tasks before you can begin using it. Perform these tasks for each server that you install and complete them before or after the other servers in the cluster are installed.

For post-installation tasks that you must complete after the installation, see [Table 5](#).

Table 5 *Post-Installation Tasks*


Post-Installation Tasks	Important Notes
<p>Activate Cisco CallManager services that you want to run on each server in the cluster.</p> <p> Caution Do not activate Cisco CallManager services in the Microsoft Services window or the Microsoft Computer Management window. You must activate Cisco CallManager services in Cisco CallManager Serviceability.</p>	<p>Refer to the following documents:</p> <ul style="list-style-type: none"> • <i>Cisco CallManager Serviceability Administration Guide</i> • <i>Cisco CallManager Serviceability System Guide</i> <p>See the “Activating Cisco CallManager Services” section on page 23.</p>
<p>Configure DNS.</p>	<p>See the “Configuring DNS” section on page 24.</p>
<p>Configure the database.</p>	<p>See the “Configuring the Database” section on page 25.</p>
<p>To manage your system, install Cisco IP Telephony Backup and Restore (BARS) Version 4.0(9) and configure the backup settings.</p> <p>Remember to back up your Cisco CallManager data daily.</p>	<p>Refer to <i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i>. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm.</p>
<p>To manage your system, install the latest service release and hotfixes that are available on CCO.</p> <p>View the components that are installed on the server.</p>	<p>See the following sections:</p> <ul style="list-style-type: none"> • Downloading Service Releases and Hotfixes for Ongoing System Management, page 25 • Viewing the Component Versions That Are Installed on the Server, page 26
<p>If you want to do so, you can configure the F: drive on the higher end servers with four hard drives (such as the MCS-7845) for trace file collection.</p>	<p>See the <i>Cisco CallManager Serviceability Administration Guide</i>.</p>
<p>Install additional music on hold selections via disk or the web.</p>	<p>See the “Viewing the Component Versions That Are Installed on the Server” section on page 26.</p>
<p>If you want to do so, install and configure Cisco Customer Response Solutions (CRS) on the server.</p>	<p>Refer to the compatible CRS installation documentation.</p>
<p>The locale, English_United_States, installs automatically on the server. To upgrade existing locales or to add new locales to the server, install the Cisco IP Telephony Locale Installer.</p>	<p>Click the following URL to obtain the locale and the installer documentation:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-40</p>
<p>Cisco strongly recommends that you install one of the following security agents to protect your servers against unauthorized intrusion:</p> <ul style="list-style-type: none"> • Cisco Security Agent (CSA) for Cisco CallManager • Management Center for Cisco Security Agent (CSA MC) 	<p>Click the following URL to obtain the security agent documentation:</p> <p>http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmgr/sec_vir/index.htm</p>
<p>If you want to use Norton AntiVirus, install the application and perform post-installation tasks.</p>	<p>Refer to <i>Using Symantec/Norton AntiVirus with Cisco CallManager</i>.</p>

Table 5 Post-Installation Tasks (continued)

Post-Installation Tasks	Important Notes
If you disabled any third-party application, antivirus services, or security agents prior to installing Cisco CallManager, you must reenab it.	See the “Reenabling Third-Party Applications, Antivirus Services, and Security Agents” section on page 27.
If necessary, you can add a subscriber server to the cluster after the installation.	See the “Adding New Subscriber Servers to the Cluster After the Installation” section on page 28. You cannot add a subscriber server to a cluster by installing a previous version of Cisco CallManager and then upgrading the subscriber server to the same version that is running on the publisher server. If you are adding a new subscriber server or replacing a subscriber server on the cluster, you must use the installation CDs with the same Cisco CallManager version that is running on the publisher server. If you are adding a new server to a secure cluster, refer to the <i>Cisco CallManager Security Guide</i> .
If necessary, you can replace the publisher database server.	See the “Replacing the Publisher Database Server After the Installation” section on page 28.
If you are administering Cisco CallManager servers from a PC that does not have Microsoft Java Machine, you will need to install and configure Sun Microsystems Java Virtual Machine (JVM) on the PC to ensure that Cisco CallManager Administration displays correctly. MSJVM installs by default in all client workstation versions of the current Windows operating systems, except for the following versions: <ul style="list-style-type: none"> Windows XP Professional with SP1 slipstreamed into the installation Windows 2000 Server/Professional with SP4 slipstreamed into the installation 	See the “Requirement for Installation of Java Virtual Machine” section on page 29.

Activating Cisco CallManager Services

Even though all Cisco CallManager services install on each server in the cluster, you must manually activate the services that you want to run on each server in the cluster. To do this, access Cisco CallManager Serviceability by following this procedure:

Procedure

-
- Step 1** Choose **Start > Programs > Cisco CallManager 4.2 > Cisco CallManager 4.2 Administration**.
 - Step 2** From the menu bar, click **Application > Cisco CallManager Serviceability**.
 - Step 3** From the menu bar, click **Tools > Service Activation**.
 - Step 4** Click a server to select it.

- Step 5** Check the Service Names check boxes for the services to be activated.
- Step 6** Click **Update**.

**Caution**

Do not start and stop Cisco CallManager services through the Microsoft Computer Management window or the Microsoft Services window. Starting and stopping Cisco CallManager services through these windows cause problems with the Cisco CallManager database.

You must activate Cisco CallManager services through Cisco CallManager Serviceability. For service recommendations and more information, refer to *Cisco CallManager Serviceability Administration Guide* and *Cisco CallManager Serviceability System Guide*.

Configuring DNS

Cisco strongly recommends that you configure DNS on every server in the cluster where Cisco CallManager is installed. Cisco uses DNS to resolve the server name to an IP address, so servers can interact in the cluster.

**Caution**

When you configure DNS, make sure that you configure and enable the Reverse DNS Lookup function.

The DNS suffix for the connection field must contain the DNS domain information where the server exists as a member.

When multiple DNS domains exist in a single Cisco CallManager cluster or the Backup Network Directory Location exists in a different DNS domain, you must correctly enter the domain information in the Append these DNS suffixes (in order): field. If you need more information on domain naming conventions, refer to *Installing the Operating System on the Cisco IP Telephony Applications Server*. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.

To configure DNS after installing Cisco CallManager, perform the following steps:

Procedure

- Step 1** Choose **Start > Settings > Network and Dial-up Connections**.
- Step 2** Right-click **Local Area Connection** and choose **Properties**.
- Step 3** Choose **Internet Protocol (TCP/IP)**.
- Step 4** Click **Properties**.
- Step 5** Click **Advanced**.
- Step 6** Click the **DNS** tab.
- Step 7** Click the **Add** button that is underneath the DNS server addresses in order of use pane.
- Step 8** In the dialog box, enter the IP address of the DNS server and click **Add**.
- Step 9** Check the **Register the connection's address with DNS** check box, if it is not already checked.

- Step 10** Click **OK**.
- Step 11** Perform this procedure on every server in the cluster that has Cisco CallManager installed.
-

Configuring the Database

After installing Cisco CallManager, you use Cisco CallManager Administration to begin configuring the database. The Cisco CallManager database contains information and parameters that relate to the system as a whole, to connected devices, and to individual users. The following list describes tasks that you must perform in Cisco CallManager Administration or Cisco CallManager Serviceability:

1. In Cisco CallManager Serviceability, activate the services that you want to run on each server in the cluster.
2. Configure system-level settings, such as Cisco CallManager Groups.
3. Design and configure your dialing plan.
4. Configure media resources for conferences, such as music on hold.
5. Install and configure your chosen voice-messaging system.
6. Configure systemwide features, Cisco IP Phone services, Cisco CallManager Extension Mobility, Cisco CallManager Attendant Console, and Cisco IP Manager Assistant.
7. Install and configure the gateways.
8. Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
9. Configure the users.
10. Configure and install the phones; then, associate users with the phones.

For more information about configuring the Cisco CallManager database, refer to the *Cisco CallManager Administration Guide*, the *Cisco CallManager System Guide*, or online help in the Cisco CallManager application.

Downloading Service Releases and Hotfixes for Ongoing System Management

For ongoing management, perform the following tasks:

- Verify that you have installed the latest Microsoft patches and hotfixes ([About Microsoft Patches and Hotfixes, page 25](#)).
- Verify that you have installed the latest Cisco CallManager service release ([Install the Cisco CallManager Service Release \(when available on cisco.com\), page 26](#)).

About Microsoft Patches and Hotfixes

Refer to *Installing the Operating System on the Cisco IP Telephony Applications Server* for more information. To obtain this document, see [Table 1](#).

Install the Cisco CallManager Service Release (when available on cisco.com)

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

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



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

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

Procedure

- Step 1** Click <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.
 - Step 2** Click **Cisco CallManager Version 4.2**.
The Cisco CallManager 4.2 software page displays.
 - Step 3** Locate and download the readme document for the service release.
The readme file provides procedures, caveats, and descriptive information for installing the files.
 - Step 4** Using the readme file as a reference, install the Cisco CallManager service release on every server in the cluster where Cisco CallManager is installed.
 - Step 5** Perform other post-installation tasks.
-

Viewing the Component Versions That Are Installed on the Server

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

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

Choose **Start > Cisco OS Version** to view the operating system image version that you have installed on your server

Installing a Cisco CallManager Security Agent

Cisco offers two security agent options. Both agents control system operations by using policies that allow or deny specific system actions before system resources are accessed.

Cisco Security Agent (CSA) for Cisco CallManager

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

Management Center for Cisco Security Agent (CSA MC)

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

Using the Cisco CallManager Music On Hold Disk or Download

When you install Cisco CallManager on your server, a default music on hold sample automatically installs for customer use. To increase your music on hold selection, you may also install the Cisco CallManager Music On Hold Disk that ships with your Cisco IP Telephony Applications Server, or you may download one of the two following files via the web:

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

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

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

Reenabling Third-Party Applications, Antivirus Services, and Security Agents

Use the following procedure to reenabling third-party applications, antivirus services, or security agents:

-
- Step 1** Choose **Start > Programs > Administrative Tools > Services**.
 - Step 2** Locate the third-party application, antivirus service, or security agent that you want to start, right-click the service, and choose Properties.
 - Step 3** In the Properties window, click the General tab.
 - Step 4** From the Startup type drop-down list box, choose **Automatic**.
 - Step 5** Click **OK**.
 - Step 6** In the Services window, right-click the application or service and click **Start**.
-

Adding New Subscriber Servers to the Cluster After the Installation

If you need to add servers to the cluster, perform the following tasks:



Caution

If you changed any NT Service passwords on the servers in the cluster, you must use the password utility to reset the passwords to the default by using the Admin Utility. The installation fails if you do not perform this task.

1. Install the operating system on the subscriber server(s) by using the Cisco-provided operating system disks and the operating system documentation.
2. Verify that you configured name resolution, for example, DNS, before you install Cisco CallManager.
3. Install Cisco CallManager on the subscriber server(s) by using the Cisco CallManager Installation, Upgrade, and Recovery Disks 1 and 2.
Make sure that you enter the publisher database server name correctly, so authentication to the publisher database server can occur.
4. Upgrade to the version of Cisco CallManager that currently runs in the cluster.
5. Install the same Cisco CallManager service release and operating system hotfixes/service patch that you have applied to the existing cluster.
6. Reboot all nodes in the cluster.

Replacing the Publisher Database Server After the Installation

To replace an existing or failed server, perform the following steps:

1. Install the operating system and the Cisco CallManager software as if it were a new installation by using the Cisco-provided operating system disks and the operating system documentation.
2. Upgrade to the version of the Cisco CallManager that you want to restore.
3. If necessary, reinstall the Cisco IP telephony applications, plug-ins, and service releases to the version that is compatible with the restored version of Cisco CallManager.
4. To obtain the locales that were used prior to the restoration, reinstall the Cisco IP Telephony Locale Installer.
5. Restore the backup data to the new server and reboot the server.
To restore the data, you must store backup data on tape or on a network directory, not on the local directory of the existing or failed server.
6. Verify that the data was restored to the new server.
7. If you are replacing a server with four drives, Cisco recommends that you set the trace directory path on the server to the default C: drive before you back up your server.
8. If your server has four drives, you can configure the trace drive for trace file collection.

Requirement for Installation of Java Virtual Machine

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

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

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



Note

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

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

If you do not have MSJVM installed on your client machine (or if you receive a message that states that Cisco CallManager cannot detect JVM on the client machine) and you need to perform Cisco CallManager Administration tasks, you must install and configure the Sun Microsystems Java Virtual Machine (JVM) on the client machine. (The Sun JVM is part of the Java 2 Runtime Environment—JRE.) In addition, you must configure the browser security to be Java-enabled. See the [“JRE Installation” section on page 29](#) for information about installing JRE on the client machine.

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



Tip

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

JRE Installation

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



Note

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

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

Procedure

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

The following example shows a zip file name:

`J2RE_Client_1.4.2_08.zip`



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

- Step 2** Right-click the **J2RE_Client_<jre version>.zip** file and click **Copy** to copy the file to your client PC.
- Step 3** Double-click the **J2RE_Client_<jre version>.zip** file to unzip the Sun J2RE installation executable.
- Step 4** Double-click the installation executable file on the client PC.

The following example shows an installation executable file name:

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



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

The JRE software installs in the C:\Program Files\Cisco\Java\JRE\j2re1.4.2_08 directory.

Verifying and Reinitializing Subscriber Connections

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

Verifying the Status of the Subscription

To determine whether the connections between the publisher database server and the subscriber servers within a cluster are broken, wait 35 minutes after you have installed the last subscriber server in the cluster. Then, open SQL Server Enterprise Manager. If a red X icon appears next to the subscription, it 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 2000 > 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 Partner or the Cisco Technical Assistance Center (TAC).

Analyzing Error Messages

This section includes information about resolving error messages and other failures. The section includes the following topics:

- [Installation Messages, page 31](#)
- [Resolving Name Resolution Failures, page 45](#)

Installation Messages

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

Table 6 *Installation Messages*

Message	Reason	Corrective Action
During the installation process, you may be prompted, possibly multiple times, to reboot the server to install a critical component. Follow the instructions in the dialog box: (1) Reboot the server. (2) Log in as the administrator.	This is an informational message only.	Click OK to continue the installation.
You must provide the Computer Name of the publisher server. IP addresses or fully qualified DNS names are not allowed.	You must not enter periods (.) when you enter the publisher database server name.	Reenter the information correctly.
You must provide the publisher server name when installing a subscriber.	This 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 6 *Installation Messages (continued)*

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 that you entered do not match.	This message displays when you enter a password more than one time, but the password that you enter does not match the password on the server.	Enter the same password on all servers in the cluster.
The password that you entered is not valid.	You entered an invalid password.	Enter the correct password.
You must enter a phrase from 1 to 15 characters in length. This phrase may contain English lower-case letters, English upper-case letters, Westernized Arabic numerals, and the following Non-alphanumeric “special characters” { } . < > : ? / \ ` ~ ! @ \$ ^ & * () _ - +	You entered invalid characters for the private password phrase.	Enter valid characters.
The installation has detected pending file operations. You must reboot the server before continuing. The installation will now abort.	Pending file operations are occurring.	Reboot the server and then install Cisco CallManager.
You are not logged on as ‘Administrator’. You must log in by using local Administrator user name and password to install Cisco CallManager.	You did not log in to the server with the local Administrator user name and password.	Log in to the server with the local Administrator user name and password.
You do not have administrator privileges. You must have administrator privileges to install Cisco CallManager.	You do not have administrative privileges.	Log in to the server with an account that has administrative privileges.

Table 6 *Installation Messages (continued)*

Message	Reason	Corrective Action
Windows 2000 Server is not installed. Install Windows 2000 Server before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.4.2sr2 (or later) on all dedicated and coresident servers. Upgrade to 2000.4.2sr2 (or later) and install the latest service release (2000.4.2sr2 or later) before installing Cisco CallManager.
Windows 2000 Service Pack 4 or later is not installed. You must have Windows 2000 Service Pack 4 or later installed before you install Cisco CallManager.	You did not install the appropriate version of the operating system.	Make sure that you installed the operating system version 2000.4.2sr2 (or later) on all dedicated and coresident servers. Upgrade to 2000.4.2sr2 (or later) and install the latest service release (2000.4.2sr2 or later) before installing Cisco CallManager.
You must install CallManager by double clicking CCMSetup.exe.	You tried to install Cisco CallManager by double clicking the msi file that is part of the Cisco CallManager package.	Double-click the CCMSetup.exe.
Cisco CallManager could not install the SUN Microsystems JRE component. Review the Cisco CallManager installation logs to determine cause of failure, take appropriate action. For more information refer, to the Cisco CallManager installation documents.	JRE installation failed.	Obtain and examine the log file.
Cisco CallManager installation has detected JRE version <JREVERSION> installed at <JRELOCATION>. Uninstall this version of JRE from the server and rerun the installation. To continue the installation, you must disable or stop any anti-virus protection, intrusion detection software, and other third-party applications, and then rerun the installation program.	Installation detected a version of JRE that is not compatible or a version that may not have all necessary components installed	Uninstall the current JRE version and rerun the installation program.

Table 6 **Installation Messages (continued)**

Message	Reason	Corrective Action
Cisco CallManager successfully installed Sun JRE and requires the server to be rebooted. To continue the installation, you must disable or stop any anti-virus protection, intrusion detection software, and other third-party applications, and then rerun the installation program.	Cisco CallManager requires the server to be rebooted to continue the installation.	Reboot the server and rerun the installation program.
If you have installed intrusion detection or anti-virus protection software, you must stop and disable these applications from the Services Control console before you continue with the Cisco CallManager installation. All other installed third-party applications must be uninstalled before proceeding with the Cisco CallManager installation. Failure to follow these directives could result in un-recoverable errors. Would you like to proceed?	This message always displays to alert the administrator of the requirements.	If you have Cisco-verified applications (Cisco Partner Applications) or platform agents that are installed on the server, you must disable/uninstall them and stop the services.
Because the <BUILDVERSION> of this Cisco CallManager MSI package is not compatible with the Cisco CallManager setup file (ccmsetup.exe), make sure that you are using the ccmsetup.exe that was distributed with this version of Cisco CallManager. The installation will now abort.	The MSI package is not compatible with the Cisco CallManager setup file.	Use the ccmsetup.exe file that was distributed with this version of Cisco CallManager.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
The installation detected that the server exists in a domain. When a server exists in a domain, authentication between servers may fail, or the non-default domain security policies may be so restrictive that the Cisco CallManager installation cannot build critical NT Accounts during an upgrade. If server is not removed from the domain and added to a workgroup, upgrade errors, upgrade failures, or a total system failure, which includes a loss of data and a complete reinstallation of Cisco CallManager, could result. Would you like to proceed?	The server exists in a domain.	Before you continue the installation, Cisco strongly recommends that you remove all servers in the cluster from the domain.
This release of Cisco CallManager is not supported on this server model. The installation will now abort.	You cannot install this version of Cisco CallManager on this server.	Refer to the <i>Cisco CallManager Compatibility Matrix</i> for a list of servers on which you can install this version of Cisco CallManager. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
The installation program does not have enough disk space on the C drive to complete the installation. The installation program requires that you have 3.0 gigabytes of disk space available on your server. Make at least 3.0 gigabytes of disk space available and restart the installation.	You do not have enough disk space on the C drive of your server to install Cisco CallManager.	Make enough disk space on the C drive and restart the installation.

Table 6 **Installation Messages (continued)**

Message	Reason	Corrective Action
The local security policy “Restrict CD-ROM access to locally logged-on user only” is enabled. This setting interferes with the Cisco CallManager installation. Please disable this setting using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation.	The “Restrict CD-ROM access to locally logged-on user only” local security policy is enabled on your server.	Disable this setting by using the Local Security Policy utility, reboot, and rerun the Cisco CallManager installation. For more information, see the “Disabling the Restrict CD-ROM Access to Locally Logged-On User Only Security Policy” section on page 48.
This package is for upgrades of existing Cisco CallManager installations only.	You attempted to use the Cisco CallManager web download file to install Cisco CallManager.	Use the disks that came with the software kit to install Cisco CallManager
A newer version of Cisco CallManager is already installed.	This message displays when you attempt to install a previous version of Cisco CallManager after a successful installation of a later version.	Remove the disk from the drive.
Cisco CallManager install did not complete successfully. Review the log file for more information.	The Cisco CallManager installation failed.	Obtain and examine the log file.
Unable to locate MSI package associated with this bootstrapper.	You did not copy all the files that came with the Cisco CallManager installation package to the server.	Copy the complete installation package to the server and rerun the Cisco CallManager installation.
Error opening MSI package.	Cisco CallManager Setup cannot find the MSI package.	This message displays if you encounter a media problem; insert the disk again.
This package has already been installed.	This message displays when you attempt to install the same version of Cisco CallManager again after a successful installation.	Remove the disk from the drive.
An unexpected error occurred.	An error occurred during the Cisco CallManager Setup.	Obtain and examine the log file.
An unexpected error occurred while creating the log directory.	The installation could not create the log file directory.	Verify that security policies on the server are not restrictive.
Failure occurred trying to get DBNAME value from registry. Aborting Cisco CallManager installation.	The installation could not read DBNAME value from registry on the local machine.	Reboot the server and rerun the Cisco CallManager installation.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
Failure occurred trying to validate the format of DBNAME value. Aborting Cisco CallManager installation.	The registry contains an invalid format of the DBNAME value. This only occurs if you manually modified this value.	Make sure that the DBNAME value is in the format CCM0xxx, where x stands for any digits.
Current OS version does not meet minimum requirements. This version of CallManager requires the minimum OS version to be <MinOSVersion>. The minimum baseline OS image version is <MinOSBaseVersion>. For more information, refer to the “Installing the Operating System on the Cisco IP Telephony Applications Server and Upgrading Cisco CallManager” documents. The installation will now abort.	This version of Cisco CallManger requires Cisco-provided operating system version 2000.4.2sr2 (or later) and the service release 2000.4.2sr2 (or later.)	Refer to <i>Cisco Compatibility Matrix</i> to review which versions are compatible for installation. To access the document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_allmg/ccmcomp.htm
Installing Cisco CallManager using Terminal Services is not allowed. Install will now abort.	Cisco does not support Terminal Services for Cisco CallManager installations, upgrades, or configuration tasks. Cisco Technical Assistance Center (TAC) uses Terminal Services for remote management and troubleshooting tasks.	If you want to use Virtual Network Computing (VNC), obtain the most recent version of the documentation at http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm .
Failed to launch <name of executable>, aborting install.	The installation attempted to launch the executable, and the launch failed.	Obtain and examine the log file. You may have a media problem.
Failure occurred during the Cisco Directory installation. Refer to the log file C:\Program Files\Common Files\Cisco\Directory\Integrate dSetup.trc for details. Aborting Cisco CallManager install.	The DC Directory installation failed.	Obtain and examine the log file.
Failure occurred during the Cisco CallManager installation. Please look at the Cisco CallManager installation log file for details. Aborting Cisco CallManager installation.	The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications and restart the installation. For more information, refer to the Upgrading Cisco CallManager document	Obtain and examine the log file.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
The Cisco CallManager installation detected an error while copying files. Stop all platform agents and Cisco-verified applications, and restart the installation. For more information, refer to the Upgrading Cisco CallManager document.	The Cisco CallManager installation failed to copy files to your server.	Stop all platform agents and Cisco-verified applications and restart the installation. For more information, see the “Performing Preinstallation Tasks” section on page 12
Either passwords do not match or a network connectivity error occurred.	During the subscriber server installation, one of the following errors occurred: <ul style="list-style-type: none"> • Network connectivity failed. • You entered NT service account password that does not match the password on the publisher database server. • You did not enter the correct name of the publisher database server. 	Do all the following tasks: <ul style="list-style-type: none"> • Verify the connection between the subscriber and publisher database servers. • Make sure that you enter the same NT service account password that you entered on the publisher database server. • Make sure that you enter the correct publisher database server name.
The password of [X] does not match the password on the publisher [servername]. For details, review the log file [Z].	The username and/or password of the user who is installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server.	Make sure that you entered the correct publisher server name and that the username and password on the publisher and subscriber match.
Because no network connectivity exists or you entered the incorrect publisher server name, the installation could not verify the password of [username] against the publisher [servername]. For details, review the log file [X].	During Subscriber installation, this message occurs if no network connection exists between the subscriber and publisher database servers or you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber server and make sure that you entered the correct publisher database server name.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
Either the password of [X] does not match the password on the publisher [Y], or a network connectivity error occurred. For details, review the log file [Z].	<p>One of the following problems occurred:</p> <ul style="list-style-type: none"> No network connectivity exists between the publisher database server and the subscriber server. The username and/or password of the user who is installing Cisco CallManager on the subscriber server does not match the username and/or password on the publisher database server. You entered the incorrect publisher database server name. 	<p>Do each of the following tasks:</p> <ul style="list-style-type: none"> Verify the connection between the publisher database server and subscriber server. Make sure that you installed Cisco CallManager on the publisher database server and subscriber server by using the Administrator username and password. Make sure that you entered the correct publisher database server name.
The private password phrase does not match the private password phrase on the publisher [servername]. For details, review the log file [Y].	<p>During the subscribe server installation, one of the following problems occurred:</p> <ul style="list-style-type: none"> The passwords of the NT service accounts did not match. You entered the incorrect publisher database server name You entered a different private password phrase on the publisher database server than you entered on the subscriber server. 	<p>Do each of the following tasks:</p> <ul style="list-style-type: none"> Make sure that a trusted connection exists between the subscriber server and the publisher database server. Make sure that you entered the correct publisher database server. Make sure that you entered the same private password phrase that you entered on the publisher database server.
The installation failed to verify the Cisco CallManager version that runs on the publisher database server. Cancel the installation, and review the log file at C:\Program Files\Common Files\Cisco\Log\CCMUIInst.log.	During Subscriber installation, this error occurs if no network connection exists between the subscriber and publisher database servers or if you did not enter the correct name of the publisher database server.	Verify the connection between the publisher database server and subscriber database server and make sure that you entered the correct publisher database server name.

Table 6 *Installation Messages (continued)*

Message	Reason	Corrective Action
The Cisco CallManager version that you are installing on this subscriber does not match the version running on the publisher database server. Cancel the installation and ensure the publisher is upgraded to this Cisco CallManager version before you continue.	You attempted to install a different version of Cisco CallManager on the subscriber database server than the version that you installed on the publisher database server.	Install the same version of Cisco CallManager on the subscriber database server that you installed on the publisher database server.
Configuration changes to the Cisco CallManager server do not take effect until you restart your system. Click Yes to restart the computer now or No if you plan to restart the computer later.	This message displays when you make configurational changes to Cisco CallManager during installation.	You do not need to take any corrective action.
Cisco CallManager installation detected a service control file from a previous failed installation. This may have resulted in incorrect service Startup Type settings. Click: "Yes" to continue installing with the current settings, "No" to reset service startup types to the original settings and exit the installation program, or "Cancel" to exit the installation program with no further action.	This message displays when the installation program detects a previous failed installation.	Cisco recommends that you choose Yes and continue installing Cisco CallManager with the current settings.
To proceed, the installation program must update the configuration and restart the server. To continue the installation with these changes and restart the server now, click OK . To abort the installation, click Cancel .	This is an informational message only.	Cisco recommends that you click OK to continue the installation.
UMX.dll failed to register. After you complete the installation, review the log file.	UMX.dll failed to register because the process creation failed, the process terminated abnormally, or an error occurred when regsvr32 was executing.	Verify that you rebooted the server after the installation. Execute a command prompt, enter regsvr32 C:\dcdsrvr\lib\UMX.dll, and press Enter. To verify that you corrected the problem, try to add a new user in Cisco CallManager Administration on this server.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
Indexing directory data did not finish. After you complete the installation, review the log file. C:\dcdsrvr\log\DirInstallValidation.log.	The installation could not determine whether the DC Directory completed the indexing of its data.	Continue with installation. At the end of the installation, reboot the server when prompted to do so. After you reboot the server, bring up the services control and wait for DC Directory Server to have a status of <i>started</i> . If this is a publisher database server, you can install Cisco CallManager on the subscriber database servers. If this is a subscriber database server, go to a command window and enter dcdrepcl trigger all . Depending on the number of users that are configured in your system, the service may be in the starting state for a long time before changing to a started state.
The Cisco CallManager installation failed to stop <list of services> service(s). Please reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.	The installation program failed to stop the services during installation.	Reboot the server, manually stop the service(s), and rerun the Cisco CallManager installation program.
The installation encountered an unknown error while trying to resolve the Publisher server name [X]. For more information, review the log file CCMInstUI.log.	The name resolution of the publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the “Resolving Name Resolution Failures” section on page 45.
The installation could not resolve the Publisher server name [X] to a valid IP address. Verify that you entered the correct publisher server name, and review the log file CCMInstUI.log for more information.	You entered the wrong publisher server name, or the hosts file has the wrong information.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the “Resolving Name Resolution Failures” section on page 45.

Table 6 **Installation Messages (continued)**

Message	Reason	Corrective Action
The installation successfully resolved the Publisher server name [X] to IP address [Y] but could not resolve the IP address back to a host name.	The reverse name resolution of the Cisco CallManager publisher server failed.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the “Resolving Name Resolution Failures” section on page 45.
The installation successfully resolved the Publisher server name [X] to IP address [Y] and resolved the IP address back to the host name [Z]. The resolved host name does not match the server name that you entered.	The publisher server name that you entered does not match the server name that the installation program retrieved after completing forward and reverse name resolution.	Verify that you correctly entered the publisher server name. To verify the hosts file, see the “Resolving Name Resolution Failures” section on page 45.
Because mapped network drives exist on the server, the installation could not verify the password of [username] against the publisher [servername]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [x].	The installation could not verify that the password on the subscriber server matches the password on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.
Because mapped network drives exist on the server, the installation could not verify the private password phrase against the publisher [servername]. Disconnect all the mapped drives, reboot the system, and rerun the installation. For details, review the log file [z].	The installation could not verify that the private password phrase on the subscriber server matches the private password phrase on the publisher database server.	Disconnect all the mapped drives, reboot the system, and rerun the installation.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
The installation could not verify the private password phrase on the publisher <server name>, because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	The installation could not verify the private password phrase on the publisher <server name> because the user does not have permission to access the publisher server over the network. For details, review the log file <log file name>.	<p>During the installation of a subscriber server, the installation program could not verify the private password phrase against the publisher server because of the security settings on either the publisher or the subscriber server.</p> <p>The probable causes include the following:</p> <ul style="list-style-type: none"> • The publisher or the subscriber server was in a domain during the installation. • Some local security policy settings that exist on the machine prevented the installation program from performing this operation.
Cisco CallManager installation failed while installing Microsoft SQL 2000. Review the Cisco CallManager installation logs to determine the cause of failure. Take appropriate action and reinstall both the Cisco IP Telephony Operating System and Cisco CallManager program. For more information refer, to the Cisco CallManager installation documents.	<p>The following items comprise the probable cause:</p> <ul style="list-style-type: none"> • The target machine probably has a virus. • Cisco Security Agent, antivirus software, or other third-party application was installed and running. 	Review the Cisco CallManager installation to determine the cause of failure. Take appropriate action to either remove the virus or disable the specified software and then reinstall both the Cisco IP Telephony Operating System and Cisco CallManager program.
Cisco CallManager successfully installed Microsoft SQL 2000 and requires the server to be rebooted. To continue the installation, you must disable or stop any anti-virus protection, intrusion detection software, and other third-party software, and then rerun the installation program. When the server reboots, you must rerun the installation program to continue your installation.	Antivirus, intrusion detection, or other third-party application was installed and running	<p>To continue the installation, you must do the following tasks:</p> <ol style="list-style-type: none"> Disable or stop any antivirus or intrusion detection software, as well as any other third-party application. Rerun the installation program. After the server reboots, rerun the installation program if it does not automatically continue.

Table 6 Installation Messages (continued)

Message	Reason	Corrective Action
<p>Cisco CallManager installation failed while installing Microsoft SQL 2000 SP4. Review the Cisco CallManager installation logs to determine cause of failure, take appropriate action. Download Microsoft SQL 2000 service pack 4 (or later) from Cisco.com, install it on the server, and rerun the Cisco CallManager installation program. For more information refer, to the Cisco CallManager installation documents.</p>	<p>The following items comprise the probable cause:</p> <ul style="list-style-type: none"> • The target machine probably has virus. • Cisco Security Agent, antivirus software or other third-party application was installed and running. 	<p>Download Microsoft SQL 2000 service pack 4 (or later) from Cisco.com, install the service pack on the server, and then rerun the Cisco CallManager installation program.</p>
<p>Cisco CallManager successfully installed Microsoft SQL 2000 SP3A and requires the server to be rebooted. To continue the installation, you must disable or stop any antivirus protection, intrusion detection software, and other third-party applications, and then rerun the installation program. When the server reboots, you must rerun the installation program to continue your installation. The installation program automatically reboots the server and the installation will continue.</p>	<p>Antivirus, intrusion detection, or other third-party application was installed and running</p>	<p>To continue the installation, you must do the following tasks:</p> <ol style="list-style-type: none"> Disable or stop any antivirus or intrusion detection software, as well as any other third-party application. Rerun the installation program. After the server reboots, rerun the installation program if it does not automatically continue.
<p>Cisco CallManager could not install the Microsoft MDAC Hotfix MS04-003 at this time.</p> <p>When the installation has finished, please reapply the latest Cisco OS Upgrade Service Release.</p> <p>For more information refer to the Cisco CallManager installation documents</p>	<p>The hotfix timeout of 1800 seconds expired.</p>	<p>This does not affect the Cisco CallManager installation, but when the installation finishes, reapply the latest Cisco OS Upgrade Service Release.</p>

Table 6 *Installation Messages (continued)*

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

Resolving Name Resolution Failures

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

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

**Note**

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

**Note**

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

**Note**

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

Procedure

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

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

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

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

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

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

```
1.3.5.9 cm1 #PRE
1.2.4.8 cm2 #PRE
```

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

```
ipconfig /flushdns
nbtstat -R
```

**Note**

Be aware that the letter “R” is case sensitive in the command.

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

- a. Examine the output of *nbtstat -c*

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

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

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

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

Forward Entries

```

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

```

Reverse Entries

```

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

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

```

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

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

Procedure

-
- Step 1 To open the Local Security Policy utility, choose **Start > Programs > Administrative Tools > Local Security Policy**.
 - Step 2 Expand the Local Policies folder in the left pane and choose the Security Options folder.
 - Step 3 In the right pane, choose the **Restrict CD-ROM access to locally logged-on user only** policy and press **Enter**.
The Local Security Policy dialog box displays.
 - Step 4 Choose the **Disabled** radio button and click OK.
 - Step 5 Exit the Local Security Policy utility.
 - Step 6 Reboot the server.
 - Step 7 Restart the Cisco CallManager installation.
-

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

CCOSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Copyright © 2006. Cisco Systems, Inc. All rights reserved

