



Installing the Operating System on the Cisco IP Telephony Applications Server

Operating System Version: 2000.4.1b

Use this document as a guide for installing the Cisco-provided Windows 2000 operating system on the Cisco IP Telephony Applications Server. Cisco IP telephony applications that use this operating system include Cisco CallManager, Cisco IP Contact Center Express Edition, Cisco IP Interactive Voice Response, Cisco IP Queue Manager, Cisco Internet Service Node, Cisco Personal Assistant, Cisco Conference Connection, and Cisco Emergency Responder.

What's Changed in Release 2000.4.1b

Because the installation procedure for Cisco IP Telephony Version 2000.4.1b changed, the installation time decreased. This section describes the major changes in Cisco IP Telephony Operating System Version 2000.4.1b.

- The installation sets the following default configurations:
 - Terminal Services is disabled.
 - Community Name is set to public, and Community Rights is set to none.
- Cisco IP Telephony Version 2000.4.1b does not require you to enter a product key during installation.
- Cisco IP Telephony Version 2000.4.1b does not support Same Server Recovery.

Hardware Requirements

Cisco IP Telephony Operating System Version 2000.4.1b supports new installation on the servers that are identified in [Table 1](#).



Note

Cisco-approved, customer-provided servers must meet exact server configurations. See [Table 2 on page 3](#) for references to documents that provide server hardware specifications and part numbers.



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

© 2005 Cisco Systems, Inc. All rights reserved.

**Note**

This operating system does not support servers with only “ECS” appended to the end of the model number.

Table 1 *Supported Hardware Platform*

MCS Servers	Cisco-Approved Servers
MCS-7825-I1-IPC1	IBM x306 3.4GHz server Model 8836-5SU as defined at http://www.cisco.com/go/swonly

Purpose of Document

This document includes information and procedures for the following topics:

- Installing the operating system
- Applying hotfixes, BIOS updates, and service packs

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

Conventions

The following documentation conventions apply to this document:

Blue Text—To quickly navigate to a section or URL, click text that appears in this color.

**Note**

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

**Tip**

Reader, use the information to perform a task. Tips provide helpful information for performing tasks.

**Caution**

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

Related Documentation and Software

Review the following documents before you install the operating system:

- The readme document that posts on the web next to the operating system upgrade
This document provides a list of changes from the last release and additional information about the operating system.
- *Cisco IP Telephony Operating System, SQL Server, and Security Updates*
This document provides information for tracking Cisco-supported operating system, SQL Server, and security files that are available for download from the web.
- The appropriate Cisco IP Telephony application documentation
Locate the release notes, installation/upgrade/backup and restore documents, and configuration guides for the applications that you want to install or upgrade.

As you review this operating system document and perform operating system installation and upgrade procedures, use [Table 2](#), which provides URLs for software and documentation.

Table 2 Quick Reference for Documentation and Software URLs

Related Information and Software	URL
Server hardware specifications	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html (for Cisco MCS) http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html (for Cisco-approved, customer-provided servers)
Related operating system and server documentation, including release notes and <i>Cisco IP Telephony Operating System, SQL Server, Security Updates</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Virtual Network Computing (VNC) documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Operating system upgrade executable/support patches and corresponding readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml Note The operating system and SQL Server support patches post on the voice products operating system cryptographic software page. You can navigate to the site from the voice application (Cisco CallManager, CRS, and so on) software page.
Cisco Security Agent (CSA) and McAfee documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/csa_4_0/index.htm
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm
Cisco Unity documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/index.htm

Table 2 Quick Reference for Documentation and Software URLs (continued)

Related Information and Software	URL
<i>Cisco CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
<i>Using the Cisco Media Convergence Server Network Teaming Driver with Operating System Version 2000.2.7 or later</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/driver

Contents

This document includes the following topics:

- [Important Considerations, page 5](#)

Operating System Installation Tasks and Information

- [Frequently Asked Questions About the Operating System Installation, page 6](#)
 - [What hardware and disks do I receive when I purchase a Cisco MCS or a Cisco IP telephony application?, page 6](#)
 - [Can I install Cisco IP Telephony Server Operating System, Version 2000.4.1b on any MCS server?, page 6](#)
 - [How long does it take to perform the operating system installation?, page 6](#)
 - [Which Cisco IP telephony applications use this Cisco-provided operating system?, page 7](#)
 - [How does the operating system installation work?, page 8](#)
 - [What data must I provide to configure the server?, page 8](#)
 - [Which Cisco-verified, third-party applications may I install on the server?, page 12](#)
 - [Which Cisco IP telephony applications may I install on the same server as Cisco CallManager?, page 13](#)
 - [May I run a web browser on the server?, page 13](#)
 - [What preinstallation tasks should I perform?, page 15](#)
 - [How do I connect the keyboard and mouse to the server?, page 15](#)
 - [What if I encounter problems during the installation?, page 16](#)
 - [Where do I obtain the release notes?, page 16](#)
- [Performing the Operating System Installation, page 16](#)

Operating System Update Tasks and Information (For Upgrades, Service Packs, and Hotfixes)

- [Frequently Asked Questions About Operating System Software Updates, page 22](#)
 - [Why cannot I find the web executable that the Cisco IP telephony application documentation specifies?, page 22](#)
 - [How do I know which version of the operating system runs on my server?, page 22](#)
 - [In what order should I apply the software updates?, page 23](#)

- [Where do I find more information \(release notes/readme\) about the software update?, page 23](#)
- [When should I install the software update?, page 23](#)
- [May I perform configuration tasks during the update?, page 23](#)
- [May I use Terminal Services, VNC, or ILO on this server during an upgrade?, page 23](#)
- [What pre-upgrade tasks should I perform?, page 24](#)
- [What if I encounter problems during the operating system upgrade?, page 25](#)
- [Downloading Operating System Upgrades, Hotfixes, Service Packs, and Additional Software Updates, page 25](#)
- [Downloading Operating System Upgrades, Hotfixes, Service Packs, and Additional Software Updates, page 25](#)
- [Ongoing Server Management, page 26](#)

Additional Information

- [Error Messages, page 26](#)
- [Using the Bug Toolkit, page 28](#)
- [Obtaining Documentation, page 28](#)
- [Documentation Feedback, page 29](#)
- [Obtaining Technical Assistance, page 30](#)
- [Obtaining Additional Publications and Information, page 31](#)

Important Considerations

Before you proceed with the operating system installation, review the following recommendations and information:

- Cisco IP Telephony Operating System Version 2000.4.1b requires a minimum of 2 GB of memory on the server. If the installation process detects less than 2 GB of memory on the server, the installation aborts.
- Install the operating system image on the Cisco CallManager publisher database server first and then on the subscriber server(s).
- Install the same operating system version including the latest operating system service release on all the servers in a cluster.
- Do not configure any server in the cluster as a Windows Domain Controller.
- 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.
- Make sure that you enter the same administrator password on all servers in the cluster.
- Do not attempt to perform any configuration tasks during the installation.
- Install Cisco Security Agent to protect your servers against unauthorized intrusion.
- 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.
- The Ephemeral (Dynamic) port range in Operating System Version 2000.4.1b specifies 49152–65534 instead of the Windows 2000 default of 1024–4999.
- To protect the server from virus attacks during the operating system installation, complete the operating system installation and apply the latest operating system upgrades and service releases before you connect the server to the network.

Installing the Operating System

This section includes information and the procedure for installing the operating system.

Frequently Asked Questions About the Operating System Installation

Review the following questions and responses before you perform the operating system installation.

What hardware and disks do I receive when I purchase a Cisco MCS or a Cisco IP telephony application?

You do not receive a monitor, keyboard, or mouse with any Cisco Media Convergence Server (MCS). During initial startup and configuration of the server, you must supply a monitor, a keyboard, and a mouse.

Before you begin the installation, carefully review the hardware documentation that accompanies your server. Make sure that you have the appropriate hardware before installing the operating system. See [Table 2 on page 3](#) for references to server hardware specifications.



Note

Unless otherwise specified, this document uses base server model numbers. References to the MCS-7825 apply to servers listed in [Table 1](#).

All Cisco MCS and customer-provided servers that meet approved Cisco configuration standards ship with a blank hard drive. When you purchase a Cisco IP telephony application, you use the appropriate disks to install/upgrade the operating system and application:

- Cisco IP Telephony Server Operating System Installation and Recovery Disk
- The disk for the Cisco IP telephony application that you plan to install on the server

Can I install Cisco IP Telephony Server Operating System, Version 2000.4.1b on any MCS server?

No. This installation supports a new installation on only the servers that are listed in [Table 1](#). The hardware detection disk checks your server and will display a message if it detects an unsupported server.

How long does it take to perform the operating system installation?

The entire operating system installation process, excluding preinstallation tasks, takes approximately 20 to 30 minutes per server, depending on your server type.

Which Cisco IP telephony applications use this Cisco-provided operating system?

After you install the Cisco-provided operating system, you install supported Cisco IP telephony applications on a server that is dedicated solely to the single application or a server that supports coresident applications.

See [Table 3 on page 7](#) for more information about the Cisco IP telephony applications that are intended specifically for use with the Cisco-provided operating system:

Table 3 *Approved Server Installations for Cisco IP Telephony Applications*

Cisco IP Telephony Application	Approved Server Installation
Cisco CallManager, Version 3.3 or later	<ul style="list-style-type: none"> • Install on a server that is dedicated to the application. • Install on a server that supports Cisco CallManager and a coresident application.
Cisco IP Contact Center Express Edition, Cisco IP Interactive Voice Response	<ul style="list-style-type: none"> • Install on a server that is dedicated to the application. • Install on a server that supports Cisco CallManager and a coresident application.
Cisco IP Queue Manager	Install on a server that is dedicated to the application
Cisco Internet Service Node	Install on a server that is dedicated to the application
Cisco Personal Assistant	Install on a server that is dedicated to the application.
Cisco Conference Connection	Install on a server that is dedicated to the application.
Cisco Emergency Responder	Install on a server that is dedicated to the application.



Note

Cisco Unity does not use the operating system that is represented in this document. Refer to the Cisco Unity documentation for information on the Cisco Unity operating system. See [Table 2](#).

How does the operating system installation work?

When you begin the installation, you boot the server from the Cisco IP Telephony Server Operating System Installation Disk. After the system boots, the Cisco IP Telephony Applications Server installation utility loads automatically and guides you through the installation process. Cisco IP Telephony Applications Server performs several preinstallation tasks that include preparing your server hard drive and loading server configuration information. (See [“What data must I provide to configure the server?” section on page 8](#) for more information.)

Cisco IP Telephony Applications Server then automatically installs Microsoft Windows 2000 Server, which is intended for use with the Cisco IP telephony applications. This operating system does not fully function for general use.

**Note**

For Cisco-approved, customer-provided IBM x306 servers, you must verify that the servers are running BIOS version 1.34 (or later). If the server does not meet the minimum version, update the version of the BIOS before you begin installing this operating system.

You can create a bootable disk to upgrade the BIOS by running the utility (39r6668.exe) that is found in the IBM folder on the DVD-ROM for IBM servers. Due to a security enhancement to the operating system, you cannot create this utility disk on a Cisco MCS server that is running the Cisco IP Telephony Server Operating System. You must create this disk on a non-MCS server.

What data must I provide to configure the server?

During the installation process, you receive prompts that tell you to enter important configuration information about the server, such as the server name and IP address. You can complete the initial power up more efficiently if you gather all the necessary configuration information before beginning the installation process. The following information applies:

User and Organization Name

Registering the software product that you are installing requires user and organization name. Do not leave the field blank. You can enter underscores, hyphens, numbers, and letters.

Computer Name

Ensure that the computer name comprises a unique network name of 15 characters or less. It may contain alphanumeric characters and hyphens (-) and must begin with an alphabetical character. Make sure that the computer name and workgroup labels follow the rules for ARPANET host names.

**Note**

Although Microsoft allows the use of the underscore character (_) as part of the naming convention, Cisco strongly recommends that you do not use the underscore character in the hostname for this computer. Use of the underscore character can result in lost session variables and cause certain windows and features not to work.

The format for DNS domain names comprises labels that are separated by single dots. Each label consists of 1 to 63 characters with a maximum of 255 characters, including the separating dots, for the entire domain name.

Labels must adhere to the following naming conventions:

- Ensure that computer name starts with a letter.
- Ensure that the computer name ends with a letter or digit.

- Ensure that the interior characters of the computer name contain only letters, digits, and hyphens.
- Ensure the computer name is unique to your network.
- Ensure the computer name is not longer than 15 characters.
- Do not include a space anywhere in the computer name, including leading or trailing spaces. Do not use the following characters and symbols, which are not valid entries in computer names: \ " / [] : | < > + = ; , ?.

Be aware that the labels are case insensitive and must begin and end with a letter or digit character. Do not create domain names that consist solely of digits

**Note**

When you enter a DNS name that includes UTF-8 or underscore character that is not listed in RFC 1123 while modifying the host name, DNS suffix, or creating an Active Directory domain on the DNS server that is provided with this server, a message displays to warn that some DNS server implementations may not support these characters.

**Caution**

Failure to adhere to the described naming convention will result in an inoperable Cisco CallManager system and a complete loss of configuration information and data on a Cisco CallManager publisher server.

**Caution**

The host name (computer name) for a Cisco CallManager server cannot start with a digit. When you choose a host name that begins with a digit, a Cisco CallManager server will not function properly.

**Note**

If you change the computer name after the application installation, you must reinstall the operating system and the application.

Workgroup

This entry specifies the name of the workgroup to which this computer belongs. A workgroup comprises a collection of computers that have the same workgroup name. Ensure that this entry of 15 characters or less follows the same naming conventions as the computer name. A message displays if you attempt to use the same name for the computer name and workgroup name.

**Note**

Cisco strongly recommends that the server belongs to a Workgroup before you install the application. You can change the choice after the installation, but you must place the server in a workgroup again before you upgrade any applications.

Domain Suffix

Always enter the Domain Name System (DNS) domain suffix in the format “mydomain.com” or “mycompany.mydomain.com.” Cisco applications like the Cisco CallManager depend on DNS for IP address to host name and host name to IP address resolution. If your company does not support internet name resolution with a DNS server, enter a fictitious domain suffix such as “mydomain.com” or “mycompany.mydomain.com” during installation and use the same domain suffix when you configure your DNS server.

TCP/IP Properties

Assign an IP address, subnet mask, and default gateway.

**Note**

Cisco recommends that you choose static IP information, which ensures that the server obtains a fixed IP address. With this choice, Cisco IP Phones can register with the application when you plug the phones into the network.

**Caution**

If you choose to use Dynamic Host Configuration Protocol (DHCP), Cisco Technical Assistance Center (TAC) requires that you reserve an IP address for each server in the DHCP server scope. This action prevents the release or reassignment of IP addresses. If you do not reserve IP addresses through the DHCP server scope, the DHCP server may assign a different address to the server if the server is disconnected from, and then reconnected to, the network. To return the server to its original IP address, you must reprogram the IP addresses of the other devices on the network.

You cannot provision the IP Address on this server by using the DHCP server that is provided with this operating system. You must use a separate DHCP server to assign a reserve IP Address to this server. For more information on DHCP and how to configure the DHCP server that is provided with this operating system, press **F1** from the desktop to access the Microsoft Windows 2000 Server online help after you have completed the OS installation.

Domain Name System (DNS)

The Cisco IP Telephony Application that you installed may require you to configure DNS or some type of NetBIOS/IP (NetBIOS over IP) name resolution such as Windows Internet Name Service (WINS). Cisco CallManager requires both DNS and NetBIOS name resolution. You can configure a separate Microsoft WINS server, configure LMHOSTS files on each server, or enable the DNS server that is provided with this operating system. For more information on DNS, WINS, LMHOSTS, and how to enable the DNS server that is provided with this operating system, press **F1** from the desktop to access the Microsoft Windows 2000 Server online help after you have completed the OS installation.

**Note**

Cisco does not recommend using LMHOSTS for name resolution when you have more than 10 nodes on your network.

**Caution**

You must have a name resolution method in place, such as Domain Name System (DNS), Windows Internet Name Server (WINS), or local naming that uses a configured LMHOSTS file. If you use DNS, make sure that the DNS server contains a mapping of the IP address and hostname of the server that you are installing before you begin the installation. If you use local name resolution, ensure that the LMHOSTS file is updated on the existing servers in the cluster before you begin the installation on the subscriber server; then, you must add the same information to the lmhosts file on the new server during installation, as the procedure instructs.

NT Administrator Password

You must enter and confirm an administrator password. Cisco requires a password for security purposes. If you leave the password blank, you cannot install a Cisco IP telephony application on the server.

**Tip**

Ensure that you use the same administrator password on all servers in the cluster.

Configuration Data

See [Table 4 on page 11](#) for configuration information that is required for installing the operating system on your server.

- Complete all fields unless otherwise noted.
- Gather this information for each Cisco IP Telephony Applications Server that you are installing in the cluster.
- Make copies of this table and record your entries for each server in a separate table.
- Have the completed lists with you when you begin the installation.

Table 4 Configuration Data for Cisco IP Telephony Application Servers

Configuration Data	Your Entry
User name	
Name of your Organization	
Computer name	
Administrator Password	
Current date, time, and time zone	
TCP/IP properties (required if you choose custom network configuration) <ul style="list-style-type: none"> • IP address • Subnet mask • Default gateway 	
DNS servers (optional) <ul style="list-style-type: none"> • Primary • Secondary DNS domain suffix WINS servers (optional) <ul style="list-style-type: none"> • Primary • Secondary LMHosts file (optional)	If you choose custom network configuration, you must configure at least one name resolution type.
Workgroup	
NT domain (optional)	

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



Caution

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

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

Procedure

- Step 1** Click <http://www.cisco.com/cgi-bin/ecoa/Search>.
- Step 2** Choose the method by which you want to search for applications.



Note

If you choose to search by solution, choose the Search by Solution radio button, choose **IP Communications** from the first drop-down list box, and choose **Operations, Administration & Management (OAM)** from the second drop-down list box.

- Step 3** Click **Search**.



Caution

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

Must I disable Cisco-verified applications?

Except for the first operating system installation, you must disable Cisco Security Agent as well as any third-party, Cisco-verified applications on your servers whenever you perform a reinstallation or upgrade of the operating system.



Caution

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

To disable services, choose **Start > Settings > Control Panel > Administrative Tools > Services**. From the Services window, right-click the service and click **Properties**. Click the drop-down arrow for the Startup-type field and choose **Disabled**. Click **Stop** and then click **OK**.

Disabling and stopping platform agents and services, such as Cisco Security Agent, performance monitoring (for example, NetIQ), antivirus (Cisco-verified McAfee services), and remote management services, ensure that the installation does not encounter issues that are associated with these services

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

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

Unsupported Applications

- The system does not support Cisco Unity on a server that runs this version of the operating system.
- The system does not support the following applications on the same server where Cisco CallManager is installed:
 - Cisco Unity
 - Cisco Conference Connection
 - Cisco Personal Assistant
 - Cisco Emergency Responder
 - Cisco IP Queue Manager
 - Cisco Internet Service Node

Supported Applications

- You can install a compatible version of Cisco IP Contact Center Express Edition or Cisco IP Interactive Voice Response with Cisco CallManager on the same 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).

CSA for Cisco CallManager comprises a standalone agent and security policy that is designed to be used on all servers in the voice cluster. Because the policy that is included with this agent is configured specifically for Cisco CallManager and other Cisco IP telephony applications, you cannot update or view it. You can download the agent from CCO at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.

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

To access information on Cisco Security Agent, see

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm



Caution

If you are uncertain whether a Cisco IP telephony application is supported on the server, do not install it. Before you install the application, always review the application documentation for recommended configurations and installations.

May I run a web browser on the server?

Cisco strongly recommends that you do not run a web browser on the Cisco MCS server or a Cisco-approved, customer-provided server. Cisco approved, customer-provided servers must adhere to exact server configurations. See [Table 2 on page 3](#) for references to documents on server hardware specification.

Running a web browser on the server causes CPU usage to surge. Rather, you should access the server by using a web browser from another computer on the same network.

May I use Terminal Services, VNC, or ILO to install the operating system on this server?

About Terminal Services

Cisco does not support installations or upgrades through Terminal Services.

About Virtual Network Computing

If you want to use Virtual Network Computing (VNC) to remotely install supported applications, see [Table 2](#) to obtain the latest version of the VNC document.



Caution

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

About Integrated Lights Out (ILO)

You can use ILO for remote configuration and monitoring tasks. On Cisco MCS and Cisco-approved, customer-provided servers, Cisco supports the following standard features of ILO:

- Virtual Power to allow full remote control of the server power button
- Remote text console to enable the display and control of remote host server activities such as shutdown and startup

To use ILO, you must obtain the ILO Default Network Settings tag that shipped with your server and perform all necessary startup tasks. Refer to the documentation that accompanies your hardware.

The ILO administrator who accesses the remote server controls all tasks that occur on the server. If an administrator is performing an installation/upgrade directly on the server and ILO administrator tries to access the server, the ILO administrator controls all tasks on the server. These tasks may interrupt the installation or upgrade; to prevent interruptions, notify all users who can access the server about when the upgrade will occur. When an ILO administrator accesses a remote server, the application locks the keyboard and mouse on the remote server where the tasks are occurring.

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

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

What preinstallation tasks should I perform?

For preinstallation tasks that you must complete before you install this operating system, see [Table 5](#).

Table 5 Preinstallation Tasks

	Preinstallation Tasks	Important Notes
Step 1	Carefully review the hardware documentation that accompanies your server. Make sure that you have the appropriate hardware before installing the application.	To review the server hardware specifications, see Table 2 .
Step 2	Connect a monitor, keyboard, and mouse to the server.	See the “ How do I connect the keyboard and mouse to the server? ” section on page 15.
Step 3	Locate Table 4 , which provides specific server configuration information.	See the “ What data must I provide to configure the server? ” section on page 8.
Step 4	For MCS-7825-I1-IPC1 or IBM x306 servers, you must enable Serial ATA Redundant Array of Independent Disks (SATA RAID) and disable hyperthreading prior to installing the operating system.	See the “ How do I enable SATA RAID and disable hyperthreading? ” section on page 16.

What post-installation tasks should I perform?

For post-installation tasks that you must complete before you install the Cisco IP telephony application, see [Table 6 on page 20](#).

How do I connect the keyboard and mouse to the server?

You must supply a monitor and, if necessary, a keyboard and mouse to use during initial startup and configuration of the server.

Plug the mouse and keyboard into the standard mouse and keyboard connectors that are marked on the back of the server. Plug the monitor cable into the monitor connector on the back of the server.



Caution

When installing the operating system on the Cisco MCS, you must use a legacy PS/2 mouse and keyboard. If you use a USB keyboard or mouse, the operating system may not install successfully.



Note

If you connect a MCS server to a Raritan Keyboard/Video/Mouse (KVM) switch, the keyboard and mouse may not work properly. You need a hardware fix for the KVM switch, so contact Raritan directly.

How do I enable SATA RAID and disable hyperthreading?

Before you begin the installation, you must enable SATA RAID and disable hyperthreading on MCS-7825-I1-IPC1 and IBM x306 servers by performing the following steps:

-
- Step 1** To enter the BIOS Configuration and Setup window, power up the server and press F1 during system startup.
 - Step 2** To disable hyperthreading, go to **Advanced Setup > Advanced Processor Options > Hyper Threading Technology** and choose **Disabled**.
 - Step 3** To go back to the main menu, press **ESC**.
 - Step 4** To enable SATA RAID, go to **Devices and I/O Ports > SATA RAID Enable** and choose **Enable**.
 - Step 5** To go back to the main menu, press **ESC**.
 - Step 6** Choose **Save Settings** and press the Enter key.
 - Step 7** Choose Exit Setup and press the Enter key.
-

What if I encounter problems during the installation?

Take the following actions if you encounter problems during the installation,:

1. During the installation, if you receive a message that displays in a dialog box, see the [“Error Messages” section on page 26](#) and perform the recommended corrective action.
2. For New Installations, on the server where the problem occurred, obtain and review the MCSSetup.log log file, which you can access by navigating to the following folder on your server: **C:\Program Files\Common Files\Cisco\Logs**.



Note

Be aware that not all messages that display in the log file are catastrophic. Messages appear in the log file for many reasons. For example, messages show attempts to access a service that Cisco CallManager does not use.

Where do I obtain the release notes?

To obtain the release notes, see [Table 2](#).

Performing the Operating System Installation



Caution

Before the installation, be aware that the process erases the server hard drive and all data and configuration information, if present. If you are reinstalling the operating system and you want to retain the present configuration, be sure to record your previous configuration settings.

**Note**

During the installation, the server reboots several times. Do not power off the server at any time during this process, unless instructed. Any unexpected power interruption during the installation process could prevent proper completion of the configuration and might prevent the operating system from restarting.

Do not connect your server to the network until you install the latest operating system upgrade and apply the appropriate Microsoft hotfixes.

To protect the server from virus attacks during the operating system installation, Cisco recommends that you complete the operating system installation and apply the latest operating system upgrades and service releases before you connect the server to the network.

Installing the Operating System

You will perform the following tasks:

- Insert the installation disk into the drive.
- Click to acknowledge that the installation process erases existing data.
- Read and agree to the terms in the End User License Agreement.
- Enter your user name and name of your organization.
- Enter the computer name and the administrator password.
- Choose the appropriate time zone, date, and time.
- Choose the network setting configuration.
- Join a workgroup, which serves as a requirement for the application installation.

Using the data that you collected in [Table 4](#), complete the following steps to configure each server:

**Note**

The server may reboot multiple times to complete installation of additional drivers and patches. Do not reboot the system manually during this time.

Procedure

- Step 1** Locate the Cisco IP Telephony Server Operating System Installation Disk.
- Step 2** Insert the disk and then power up the server. You must boot from this disk to begin installing the OS.

**Note**

The first time that you start up a new server, you will not see any indication that the startup process is operating normally. The startup on a new server takes longer than on preinstalled servers. You may wait as long as 3 minutes before a video connection occurs.

Do not remove the disk unless the procedure or process prompts you to do so.

- Step 3** If you see the post-startup message about memory upgrades on IBM xSeries servers, perform the following procedure:
- The Post Startup Error(s) window displays a message about memory upgrades. Using the arrow keys, choose **Continue** and then press **Enter**.
 - If the Configuration Error window displays, use the arrows keys to choose **Continue**; then, press **Enter**.
 - The Configuration/Setup Utility window displays a variety of configuration options. Using the arrows keys, choose **Save Settings**. Press **Enter**.
 - The Save Settings window displays a message about saving the current settings. Press **Enter** to continue.
 - The Configuration/Setup Utility window displays. Using the arrows keys, choose **Exit Setup** and then press **Enter**.
 - When the Exit Setup window displays, use the arrow keys to choose **Yes, exit the Setup Utility**. Press **Enter**. The system reboots automatically.
 - On a new server, the IBM BIOS upgrade utility runs; then, the server reboots automatically.
- Step 4** When a message displays that states that all existing configuration and information on the hard drive will be lost, click **OK** to continue the installation.
- Step 5** A message that states that the installation is transferring the operating system image to the server displays. This process takes approximately 15 minutes. You can either click **Okay** or wait 15 seconds for the installation program to clear the message and start transferring the image. The system reboots automatically after the image has been transferred.
- Step 6** The License Agreement window displays. Read through the contents of the agreement. To continue the installation, you must click **I Accept this agreement**; then, click **Next**.
- Step 7** The Personalize Your Software window displays. Enter your name and the name of your company or organization. Click **Next**.
- Step 8** The Computer Name and Administrator Password window displays. Enter the computer name in the computer name field and the administrator password in the administrator password field. Enter the same password in the Confirm Password field. Click **Next**.

**Note**

Although Microsoft allows the use of the underscore character (_) as part of the naming convention, Cisco strongly recommends that you do not use the underscore character in the hostname for this computer. Use of the underscore character can result in lost session variables and cause certain pages and features not to work.

Ensure that the computer name comprises a unique network name of 15 characters or less. It may contain alphanumeric characters and hyphens (-) and must begin with an alphabetical character. Make sure that the computer name and workgroup labels follow the rules for ARPANET host names. Labels must adhere to the following naming conventions:

- Ensure that computer name starts with a letter.
- Ensure that the computer name ends with a letter or digit
- Ensure that the interior characters of the computer name contains only letters, digits, and hyphens.
- Ensure the computer name is unique to your network.

- Ensure the computer name is not longer than 15 characters.
- Do not include a space anywhere in the computer name, including leading or trailing spaces. Do not use the following characters and symbols, which are not valid entries in computer names: \ " / [] : | < > + = ; , ? .

**Caution**

Failure to adhere to the preceding naming convention will result in an inoperable Cisco CallManager system and a loss of configuration and data on a Cisco CallManager publisher server.

If you leave the password fields blank, you cannot install any Cisco IP telephony applications on the server.

**Note**

Verify the Num Lock status before you enter the password. This task ensures that you enter the appropriate password.

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

**Note**

The installation automatically enables screen-saver password protection. You can disable the screen-saver password protection by unchecking the Password-protected check box on the screen-saver tab on the Display Property Configuration window.

Step 9 The Date and Time Settings window displays. Set the current date and time. Choose the appropriate time zone. Click **Next**.

Step 10 The Networking Settings Window displays. To manually enter network settings on the server, choose **Custom settings**. To enable Dynamic Host Configuration Protocol (DHCP), choose **Typical Settings**. Click **Next**.

On MCS-7825-I1 or IBM 306:

The operating system specifies the network card that is labeled as CT Network Connection as the first Network Interface Card (NIC) and the network card that is labeled as MT Network Connection as the second NIC on the server. The installation program disables the network card that is labeled as MT Network Connection after the first reboot. If you plan to manually enter network settings, configure the network settings on the NIC that is labeled CT Network Connection.

**Note**

The computer may display the second NIC (MT Network Connection) first in Network Setting Configuration. If you incorrectly configure the NIC that is labeled MT Network Connection, the server will boot up as a DHCP client.

Step 11 The Workgroup or Computer Domain windows display. If the server exists in a Domain, Cisco requires that you place the server in a workgroup. To join a workgroup, perform the following procedure:

- Enter a name of the workgroup, for example, WRKGRP. Make sure that you enter a Workgroup name that differs from the Computer Name.
- Click **Next**.

**Note**

If the server exists in a Domain, Cisco requires that you place the server in a Workgroup during installation

- Step 12** Installation proceeds. Upon completion, the computer reboots.
- Step 13** Log in to the server by using the administrative user name and password.
- Step 14** The system checks for network transmission conflicts the first time that the server is started after the operating system is installed and may display a status message. If your server displays a message, click **OK** to clear the message. If you received an error message, correct the network conflict that the installation program detected, clear the System log under Event Viewer, and rerun the utility CheckNICDuplex.exe in the C:\utils folder to ensure that no more network conflicts exist.
- Step 15** Install the operating system on every server in the cluster that uses it.
- Step 16** Refer to the Cisco IP telephony application documentation for additional installation and configuration tasks. See [Table 2](#).

Post-Installation Tasks

See [Table 6](#) for a list of tasks that you should perform after you install the operating system software.

Table 6 *Post-Installation Tasks*

Task	Notes
Verify the operating system version that is installed on the server.	See the “How do I know which version of the operating system runs on my server?” section on page 22.
Verify that you have all hotfixes and support patches installed on the server. If not, download and install the latest OS Service Release that is available on the web.	See Table 2 on page 3 for reference to the readme document for the operating system support software.
If you are planning to install Cisco CallManager Release 3.3(2) or 3.3(3), you should uninstall the non-security Microsoft hotfix 831877 that the OS install includes.	See the “Uninstalling Microsoft Hotfix 831877” section on page 21.
Subscribe to the Cisco CallManager Notification Tool and PSIRT notification tool.	This task enables you to receive e-mail notification whenever new fixes, OS updates, and service releases get released. See the “Applying Additional Security” section on page 21.
Increase the security on your server.	See the “Applying Additional Security” section on page 21
Enable the Cisco Media Convergence Server (MCS) Network Teaming Driver to support the functionality for the failover fault-tolerant network adapters if your hardware supports this.	Refer to <i>Using the Cisco Media Convergence Server Network Teaming Driver with Operating System Version 2000.2.7 or later</i> for a list of supported servers and installation information.
Configure the speed and duplex of your network card to 1000/Full if the hardware on your server and network supports gigabit speed.	Refer to <i>Using the Cisco Media Convergence Server Network Teaming Driver with Operating System Version 2000.2.7 or later</i> .

Uninstalling Microsoft Hotfix 831877

If you are planning to install Cisco CallManager Release 3.3(2) or 3.3(3), you may encounter a problem during installation in which the Cisco CallManager installation program displays a harmless AddAnonymousWebUserAccess message. Click **OK** to continue your installation.

You must uninstall the non-security Microsoft Windows hotfix 831877 that Cisco Win-OS 2000.4.1b and above includes.



Note

Microsoft Windows hotfix 831877 comprises a non-security update that is reapplied whenever you install a Cisco Win-OS service release.

Procedure

-
- Step 1** From the Start menu, choose **Settings > Control Panel**.
The Control Panel window displays.
- Step 2** Double-click the Add/Remove Programs icon.
The Add/Remove Programs window displays.
- Step 3** Scroll down until you locate the Windows 2000 Hotfix 831877 and click the hotfix.
- Step 4** Click Change/Remove.
-

Applying Additional Security

Cisco recommends that you perform the following additional tasks on all servers in a cluster:

- Always apply the latest operating system upgrades and service releases.
- Install a Cisco-verified antivirus program on all servers.
- Cisco strongly recommends that you install Cisco Security Agent to protect your servers against unauthorized intrusion. Refer to the Cisco Security Agent documentation. See [Table 2 on page 3](#)
- If you are planning to install Cisco CallManager, you can install the Cisco CallManager OS Optional Security settings. For more information, refer to the C:\Utils\SecurityTemplates\CCM-OS-OptionalSecurity-Readme.htm document.
- Subscribe to the Cisco CallManager Notification Tool and PSIRT notification tool.

The Cisco CallManager Notification Tool provides automatic e-mail notification of new fixes, OS updates, and service releases that are available for Cisco CallManager and related products, including Cisco CallManager Attendant Console, Cisco IP Manager Assistant (IPMA), and Bulk Administration Tool (BAT). To subscribe, click the following URL and choose **CallManager Cryptographic Software including OS updates** to receive notification when new operating system updates are posted. (Only a registered user of Cisco.com can access this URL.)
<http://www.cisco.com/cgi-bin/Software/Newsbuilder/Builder/VOICE.cgi>

The Cisco PSIRT Advisory Notification Tool provides automatic e-mail notification of all Cisco Security Advisories that the Cisco Product Security Incident Response Team (PSIRT) releases. Security Advisories, which describe security issues that directly impact Cisco products, provide a

set of required actions to repair these products. To subscribe, click the following URL and perform the tasks as directed:

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

Upgrading the Operating System/BIOS and Applying Additional Operating System/BIOS Updates

To obtain the latest BIOS upgrades, operating system hotfixes, service packs, components, and security settings, download and install the latest executable from Cisco.com.

The operating system upgrade updates your system to the latest Cisco-provided operating system version.

Do not perform the operating system upgrade on a server that is already running the same version of the operating system.

Frequently Asked Questions About Operating System Software Updates

Review the following information before you upgrade the operating system.

Why cannot I find the web executable that the Cisco IP telephony application documentation specifies?

If you cannot locate a file on the web, Cisco has removed the file from the web and replaced it with a newer version. Always install the version that is available on the web, unless the readme document states otherwise.

How do I know which version of the operating system runs on my server?

The MCSver.exe program reports the current version of the operating system components. Be aware that Cisco does not report the actual application version through this program. Most of these components, which are 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 changes only if you do a new installation with the Cisco IP Telephony Server Operating System Hardware Detection Disk.

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

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

Procedure

-
- Step 1 On your server, choose **Start > Cisco OS Version** to verify that the operating system image version that you have installed on your server is 2000.4.1b.
 - Step 2 Locate the operating system image version.
-

**Note**

The Cisco OS Version utility named MCSver.exe logs information to C:\Program Files\Common Files\Cisco\Log\MCSver.log. If necessary, you can provide log files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

In what order should I apply the software updates?

Refer to *Cisco IP Telephony Operating System, SQL Server, Security Updates* for more information. See [Table 2](#) to obtain the document.

Where do I find more information (release notes/readme) about the software update?

You can obtain the latest upgrade executable and version-specific readme document from the voice software cryptographic site on the web.

The readme document may be a later version than the executable if information regarding the upgrade is updated. If the readme document is a newer version than the executable, Cisco recommends that you review the updated document for new information regarding the upgrade.

When should I install the software update?

**Caution**

Cisco strongly recommends that you install the software update during off-peak hours or a maintenance window. Installing the software update may cause call-processing interruptions.

May I perform configuration tasks during the update?

**Caution**

Do not attempt to perform any configuration tasks during the installation. Before you update the server, disable all services that allow any administrator to perform remote configuration tasks. For example, disable Terminal Services or VNC, if you do not plan to use it, before the upgrade to prevent an administrator from browsing into the server during the installation.

Notify all users that you are performing an installation, so users do not browse into the server.

Performing configuration tasks during the installation causes an installation failure.

May I use Terminal Services, VNC, or ILO on this server during an upgrade?

About Terminal Services

Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote administration and troubleshooting tasks.

Cisco does not support operating system installations or upgrades through Terminal Services.

**Caution**

Before the installation, 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 installation to fail.

After you perform the installation, you must enable Terminal Services.

About Virtual Network Computing

If you want to use Virtual Network Computing (VNC) to remotely install supported applications, see [Table 2](#) to obtain the latest version of the VNC document.

**Caution**

If you have installed VNC but do not plan to use it to perform the installation, 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.

About ILO

You can use ILO for remote configuration and monitoring tasks. On Cisco MCS and Cisco-approved, customer-provided servers, Cisco does not support ILO for any other purposes, including installation and upgrade tasks.

To use ILO, you must obtain the ILO Default Network Settings tag that shipped with your server and perform all necessary startup tasks. To use this product, refer to the documentation that accompanies your hardware.

The ILO administrator who accesses the remote server controls all tasks that occur on the server. If an administrator is performing an installation/upgrade directly on the server and ILO administrator tries to access the server, the ILO administrator controls all tasks on the server. When an ILO administrator accesses a remote server, the application locks the keyboard and mouse on the remote server where the tasks are occurring. These tasks may interrupt the installation or upgrade; to prevent interruptions, notify all users that can access the server regarding when the upgrade will occur.

What pre-upgrade tasks should I perform?

Perform the following tasks before you upgrade the operating system.

1. Verify the operating system version that is running on your system.
2. Review the readme documentation for the operating system upgrade for specific installation procedures, pre-upgrade and post-upgrade notes, caveats, and compatibility information.
3. Disable all Cisco-verified, third-party applications and reboot the server.
4. Disable Cisco IDS Host Sensor Agents and reboot the server.
5. Verify that you have installed the latest backup utility that is available on the web. Verify that you have a good backup of your data on a network directory or tape device.
6. Verify that you have enough free disk space on the server.

Make sure that you have 1 GB of free disk space before you copy the executable to the server. Delete any unnecessary files. Remove old log files, CDP records, old installation files, and so on.

7. Before you perform the upgrade, close all programs.

8. To avoid impact from call-processing interruptions, upgrade the operating system software during off-peak hours or a maintenance window.
9. Upgrade the operating system image on the Cisco CallManager publisher database server first and then on the subscriber server(s).

What if I encounter problems during the operating system upgrade?

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

1. If you receive a message that displays in a dialog box during the operating system upgrade, see the “[Error Messages](#)” section on page 26 and perform the recommended corrective action.
2. On the server where the upgrade problem occurred, obtain and review the log file, MCSOSupg.log, from C:\Program Files\Common Files\Cisco\Logs.



Note

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

Downloading Operating System Upgrades, Hotfixes, Service Packs, and Additional Software Updates

To install the software update, perform the following procedure:

- Step 1 Perform preinstallation tasks. See the “[What pre-upgrade tasks should I perform?](#)” section on page 24.
- Step 2 Click <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.



Note

To obtain the update from the web, you must have a Cisco Connection Online (CCO) username and password.

- Step 3 Choose **The Application** (for example, Cisco CallManager) > **Download...Cryptographic Software... > Download Cisco 3DES Cryptographic Software under export licensing controls.**
- Step 4 In the window that displays, locate the readme document for the software update.
- Step 5 Review the readme document for specific instructions and caveats.
- Step 6 Download the software update to your hard drive.
- Step 7 Note the location where you save the downloaded file.
- Step 8 Double-click the downloaded file to begin the installation.
- Step 9 Perform the installation on every server where the update is supported, starting with the Cisco CallManager publisher.

Ongoing Server Management

The the IBM Director Agent, an SNMP agent extension, allows you to monitor and manage the specific components of your server, such as CPU, virtual memory, and disk usage. They also monitor server temperature, fan status, power supplies, and NIC information.

On Cisco Media Convergence Servers and approved, customer-provided servers, the drivers upgrade when you insert the Cisco IP Telephony Server Operating System OS Upgrade Disk into the drive or when you upgrade the operating system with the latest OS upgrade software. For information on how to use this disk, refer to the readme documentation.

Error Messages

[Table 7](#) describes error messages that display in dialog boxes and the appropriate corrective actions. If you need to obtain the log files, see the [“What if I encounter problems during the installation?”](#) section on page 16 or the [“What if I encounter problems during the operating system upgrade?”](#) section on page 25.

Table 7 *Error Messages*

Error Message	Corrective Action
This version of the installation program does not support the hardware platform that was detected.	Install the operating system on a supported hardware platform. See Table 1 .
The installation program detected an unsupported version of the system BIOS.	Install BIOS version 1.34 (or later) on the server before you continue the installation.
Installation did not detect the minimum amount of memory (2048 MB) that is required to continue.	Increase the memory on this server to a minimum of 2 GB before you continue the installation.

Table 7 Error Messages (continued)

Error Message	Corrective Action
<p>The specified workgroup name is invalid. Would you like to proceed for now and try joining a workgroup later?</p>	<p>Click No to enter a different workgroup name.</p> <p>Note If you click yes and proceed, you will experience a conflict when you install the Cisco IP Telephony application</p>
<p>The NIC in this server reports that it is connected in half duplex-mode, which indicates a duplex mismatch between the NIC and the switch. Change the NIC speed and duplex settings of this server to match the settings of the switch.</p>	<p>Follow these steps to set the speed and duplex on the server to match the setting on the switch:</p> <ol style="list-style-type: none"> 1. Determine the speed and duplex setting for the switch port that the server is using. 2. Right click My Network Places and click Properties. 3. Right click Local Area Connection and click Properties. 4. Click Configure. 5. Click the Advanced tab. 6. Choose Speed & Duplex, Link Speed & Duplex, or a similar option from the property list. 7. Choose the value that matches the speed and duplex setting of the switch port. <p>Note The MCS-7815I, MCS-7825I, MCS-7835I, MCS-7845I, and Cisco-approved, customer-provided IBM x306, x345, and x346 servers do not provide a setting for 1000 / Full. On these servers, set Auto detect or Auto-negotiate 1000Mbps to connect at gigabit speed. In addition, configure the switch port for Auto.</p> <ol style="list-style-type: none"> 8. To close the Adapter Properties window, click OK. 9. To close the Local Area Connection Properties window and apply the new setting, click OK. 10. Close the Network and Dial-up Connections window.

Using the Bug Toolkit

If you have an account with Cisco.com (Cisco Connection Online), you can use the Bug Toolkit to find caveats for this product.

To use the Bug Toolkit, go to this URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

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/univercd/home/home.htm>

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

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

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

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

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



Note

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 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 TAC 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 TAC 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)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

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

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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>
- *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>
- 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>

CCSP, 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 © 2005, Cisco Systems, Inc. All rights reserved.