Installing Cisco Security Agent for Cisco CallManager

This document provides installation instructions and information about Cisco Security Agent (CSA) for Cisco CallManager. If Cisco CallManager resides on the same server with Cisco Customer Response Solutions (CRS), you can use this document or the *Installing Cisco Security Agent for Cisco Customer Response Solutions* document to install the agent on that coresident server, because both products use identical security policies.

Contents

This document contains information on the following topics:

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

Introduction

Cisco Security Agent provides intrusion detection and prevention for the Cisco CallManager cluster. Cisco Systems provides it free of charge as a standalone security agent for use with servers in the Cisco CallManager voice cluster. The agent provides Windows platform security that is based on a tested security rules set (policy), which has rigorous levels of host intrusion detection and prevention. The agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed.

This process occurs transparently and does not hinder overall system performance.

Note In addition to being specifically tuned for the Cisco CallManager and Cisco CRS software, Cisco Security Agent for Cisco CallManager provides support for many Cisco-approved, third-party applications. The agent also provides security for web and database services. In addition, CSA provides security checks for TCP/IP if you install the Network Shim, which serves as a host-based intrusion detection system. When a later version of the agent becomes available, Cisco strongly recommends that you install the later version.

Cisco strongly recommends that you run this agent in conjunction with the latest Cisco-provided operating system service releases and upgrades. To obtain the Cisco-provided operating system service releases and upgrades, see Table 1.

The standalone Cisco Security Agent uses a static policy that cannot be changed. However, if you want to change the policy for non-CallManager and non-IPCC Express purposes, see the "Migrating to the Management Center for Cisco Security Agents" section on page 9 for more information.

Follow the installation instructions in this document to install CSA on all servers within the voice cluster, including Cisco CallManager, Cisco CRS, Remote Database, voice, and speech servers. Do not install the agent on client machines.

The policy included with Cisco Security Agent for Cisco CallManager provides support for many Cisco-approved, third-party monitoring tools, including the following applications:

- BMC Patrol
- Concord eHealth Monitor
- Diskeeper Server Standard Edition 8.0.478.0
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research Prognosis
- McAfee VirusScan 7.0
- Micromuse Netcool
- NAI Epolicy Agent
- NetIQ Vivinet Manager
- RealVNC
- Symantec Corporate Edition 8.0
- Trend Anti-Virus

- Windows Terminal Services

If you use a third-party software tool that is not Cisco-approved, see the "Migrating to the Management Center for Cisco Security Agents" section on page 9 for more information.

System Requirements

- Cisco CallManager *(*The *Cisco CallManager Compatibility Matrix* includes supported Cisco CallManager releases. To obtain the *Cisco CallManager Compatibility Matrix*, see Table 1)
- Microsoft Windows 2000 Server in English

Before You Begin the Installation

Before you install the Cisco Security Agent for Cisco CallManager, review the following information:

- The Cisco Security Agent supports any Cisco Media Convergence Server (MCS) or customer-provided, Cisco-approved server where Cisco CallManager and Cisco-provided operating system are installed, unless the *Cisco CallManager Compatibility Matrix* indicates otherwise. To obtain the *Cisco CallManager Compatibility Matrix*, see Table 1.
- Install this security agent on every server in the Cisco CallManager cluster, including coresident servers where Cisco CallManager and Cisco Customer Response Solutions/Cisco Customer Response Applications run.
- Install the agent first on the publisher database server and verify that the installation completed successfully; then, install the agent on all subscriber servers serially, that is, on one server at a time.
- Do not install the agent between the operating system and Cisco CallManager installation.
- Before each Cisco CallManager upgrade, you must disable the Cisco Security Agent service by using the procedure that is shown in the "Disabling and Reenabling the Cisco Security Agent Service" section on page 6. You must also ensure that the service does not get reenabled at any time during the Cisco CallManager installation.

Caution You must disable the Cisco Security Agent service before installing, uninstalling, or upgrading any software, including the operating system, Cisco CallManager, maintenance releases, service releases, support patches, and plugins.

You must disable the agent by using the method that is described in the "Disabling and Reenabling the Cisco Security Agent Service" section on page 6. Ensure that the service does not get reenabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade.

After the software installation or upgrade, you must reenable the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

- If you plan to upgrade from Cisco CallManager 3.2(3) to Cisco CallManager 3.3 and you run the agent on the server, you must disable the Cisco Security Agent service before the upgrade. After the upgrade, you must reinstall the Cisco Security Agent on all servers in the cluster because the upgrade to Cisco CallManager 3.3 deletes the agent.

- If you plan to upgrade from Cisco CallManager 3.3(2) to Cisco CallManager 3.3(3) and you run the agent on the server, you must disable the Cisco Security Agent service before the upgrade; however, you do not need to reinstall the agent after the upgrade. Remember to enable the Cisco Security Agent service after the upgrade.
- Before you install or upgrade the agent, back up your Cisco CallManager data. For more information on how to perform this task, refer to the appropriate version of the Cisco CallManager backup documentation. To obtain the Cisco CallManager backup documentation, see Table 1.
- Before you install or upgrade the agent, back up all applications that run in the cluster. Refer to the appropriate backup documentation for more information.
- Do not use Terminal Services to install or upgrade the agent. Cisco installs Terminal Services, so Cisco Technical Assistance Center can perform remote management and configuration tasks. Do not use Integrated Lights Out to install or upgrade the agent.

  If you want to do so, you can use Virtual Network Computing (VNC) to install or upgrade the agent. To obtain VNC documentation, see Table 1.

Caution If you currently run Cisco HIDS Agent (Entercept) on the server, you must uninstall the software from Add/Remove Programs before you install the Cisco Security Agent. If you fail to uninstall the Cisco HIDS Agent before the Cisco Security Agent installation, the installation deletes the TCP stack, and the Cisco Security Agent does not install the firewall component that is necessary for security.

- The agent installation causes a brief spike in CPU usage. To minimize call-processing interruptions, Cisco recommends that you install the agent during a time when call processing is minimal. The agent protects the server as soon as you install the software, but the agent does not provide complete functionality until you reboot the server.

Caution Rebooting the server may cause call-processing interruptions. Cisco recommends that you reboot the server at the end of the business day or during a time when call processing is minimal.

- Before you upgrade the agent or reinstall the agent on the server, you must uninstall the agent and then reinstall the software.

  When you uninstall the agent by using Add/Remove Programs or **Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Security Agent**, a prompt asks whether you want to uninstall the agent. You have limited time to click **Yes** to disable the protection. If you choose **No** or wait to disable the protection, the security mode automatically enables, and the installation aborts.

Caution After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, and the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

- After the installation, you do not need to perform any agent configuration tasks. The software immediately begins to work as designed. Security logs display in the Message tab of the agent GUI, in Microsoft Event Viewer, and in the securitylog.txt file (<InstallDrive>:\Program Files\Cisco\CSAgent\log).
- The Cisco IP Telephony Applications Backup Utility does not back up the log files or text file that the agent generates.

If you need to restore the Cisco CallManager data to the server for any reason, you must reinstall the agent after you restore the Cisco CallManager data.

Tip If you encounter problems with installing or uninstalling the agent, see the "Troubleshooting" section on page 11.

Installing the Cisco Security Agent

Review the "Before You Begin the Installation" section on page 3, which provides information to help ensure a successful installation.

Note You must have access to the Cisco CallManager cryptographic site before you can download the Cisco Security Agent file. If you have not yet applied for download access, go to http://www.cisco.com/kobayashi/sw-center/telephony/crypto/voice-apps/. Click **Apply for Cisco 3DESCryptographic Software under export licensing control**. On the window that appears, choose **CallManager** from the drop-down list of products and click **Submit**. A form displays; check the appropriate check boxes on the form and click **Submit**. A message displays that tells you when you can expect to have download access.

To install the Cisco Security Agent, perform the following procedure:

Procedure

Step 1 From the CallManager server, go to the CallManager & Voice Apps Crypto Software Download site at http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des

Step 2 Choose the latest version of the Cisco CallManager CSA file from the list of files.

Note The filename structure follows the format *CiscoCM-CSA-n.n.n.nnn-n.n.n-K9.exe*, where *n.n.n.nnn-n.n.n* specifies the version of the agent and policy. For example, the filename CiscoCM-CSA-4.0.1.539-1.1.4-K9.exe specifies the agent version 4.0.1.539 and the policy version 1.1.4.

Choose the file with the latest agent version and the latest policy version.

Step 3 Note the location where you saved the downloaded file.

Step 4 Double-click the downloaded file to begin the installation.

Step 5 When the Welcome window displays, click **Next**.

Step 6 To accept the license agreement, click **Yes**.

Step 7 Click **Next** to accept the default location (C:\Program Files\Cisco\CSAgent).

Caution The Cisco CallManager policy rules are directory specific, so the default directory must be used.

Step 8 To install the Network Shim, click N**ext**.

Caution You must install the Network Shim for the agent to have full functionality.

Step 9 The status window displays the options that you chose. To accept the current settings, click **Next**.

Step 10 Continue to wait while the installation completes; do not click Cancel.

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

Caution If you want to do so, you can reboot the server at the end of the business day. Rebooting the server may cause call-processing interruptions. The agent protects the server as soon as you install the software, but the agent does not provide complete functionality until you reboot the server.

Step 12 Click **Finish**.

Tip When the installation completes, a red flag displays in the Windows 2000 system tray. You can also verify that the software installed by locating the Cisco Security Agent in the Add/Remove Programs window.

Step 13 Perform this procedure on every server in the cluster.

Checking the Agent and Policy Versions on the Server

To verify the agent and policy versions on the server, locate and run the file **<InstallDrive>:\utils\MCSver.exe**.

Disabling and Reenabling the Cisco Security Agent Service

You must disable the CSA service whenever you want to perform a task that requires the server to be restarted, such as installing, upgrading, or uninstalling software. If you disable the CSA service, you must reenable it before it starts monitoring the Cisco CallManager server again.

Caution You can suspend the CSA by using the "net stop csagent" command in a command shell or the suspend option available by right clicking the CSA icon (red flag in the system tray). However, these methods do not actually disable the agent; they merely suspend it. Cisco does not recommend suspending the agent and does not support suspending the agent because, in the event the installer reboots your machine and continues with installation activity, the reactivated CSA service might interfere with the installation of other software.

Caution You must disable the CSA service using this method before installing, uninstalling, or upgrading any software, including the operating system, Cisco CallManager, maintenance releases, service releases, support patches and plugins. Ensure that the service does not get reenabled at any time during the installation/upgrade. Failure to do so may cause problems with the installation or upgrade.

After installing, upgrading, or uninstalling the software, you must reenable the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

Caution Cisco recommends that you perform the following procedure serially, that is, on one server at a time. After you complete installing, upgrading, or uninstalling the software, you can reenable the service on the server; then, you can disable the service on the next server where you plan to perform the same software operation.

Disabling the CSA

To disable the CSA service, perform the following procedure:

Procedure

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

Step 2 In the Services window, 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**.

Caution In the Services window, verify that the Startup Type of the CSA service is disabled.

Step 7 Close the Services window.

Step 8 Perform this procedure on every server where you plan to install or upgrade Cisco CallManager.

Caution You must reenable the Cisco Security Agent service after installing, upgrading, or uninstalling software. See the "Reenabling the CSA" section on page 7

Reenabling the CSA

To reenable the Cisco Security Agent service after installing, upgrading, or uninstalling software, perform the following procedure:

Procedure

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

Step 2 In the Services window, right-click **Cisco Security Agent** 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 **Apply**.

Step 6 Click **Start**.

Step 7 After the service has started, click **OK**.

Step 8 Close the Services window.

Uninstalling the Cisco Security Agent

Review the "Before You Begin the Installation" section on page 3, which provides information about uninstalling the Cisco Security Agent.

Caution You cannot install the same version of the agent on top of a previously installed version. You must uninstall the agent and then reinstall the software. When you uninstall the agent, a prompt asks whether you want to uninstall the agent. You have limited time to click Yes to disable the protection. If you choose No or wait to disable the protection, the security mode automatically enables

To uninstall the security agent, perform the following procedure:

Procedure

Step 1 Choose **Start > Programs > Cisco Systems > Uninstall Cisco Security Agent**.

Step 2 Click **Yes** or **Yes to All** in response to all questions.

Step 3 Reboot the server.

Caution After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

Note The uninstaller does not remove the registry entries where the policy version is stored. If you want them removed, you must manually delete them.

Upgrading the Cisco Security Agent

Before you upgrade the Cisco Security Agent, perform the following tasks:

1. Uninstall the existing version that is installed on the server.

   See the "Uninstalling the Cisco Security Agent" section on page 8.
2. Install the new version that you plan to run on the server.

See the "Installing the Cisco Security Agent" section on page 5.

Migrating to the Management Center for Cisco Security Agents

The security agent included with Cisco CallManager uses a static policy that cannot be changed or viewed. It is possible to add, change, delete, or view policies if you purchase and install the fully-managed console product, Management Center for Cisco Security Agent (CSA MC). However, any such changed policy is NOT qualified for use with Cisco CRS.

CSA MC contains two components:

- The Management Center installs on a secured server and includes a web server, a configuration database, and a web-based interface. The Management Center allows you to define rules and policies and create agent kits that are then distributed to agents that are installed on other network systems and servers.
- The Cisco Security Agent (the managed agent) installs on all Cisco CallManager servers in the cluster and enforces security policies. The managed agent registers with the Management Center and can receive policy and rule updates. It also sends event log reports back to its Management Center.

Before you begin, you should obtain the latest version of the following CSA MC documents:

- *Installing Management Center for Cisco Security Agents*
- *Using Management Center for Cisco Security Agents*
- *Release Notes for Management Center for Cisco Security Agents*

You can download these documents at http://www.cisco.com/en/US/customer/products/sw/cscowork/ps5212/prod_technical_documentation.html

In a Cisco CallManager environment, ensure that the Management Center component is installed on a separate, secured server and the managed agent component is installed on all Cisco CallManager servers in the cluster. Make sure that the server that is intended for the Management Center meets the system requirements that are listed in *Installing Management Center for Cisco Security Agents.*

Caution Do not install the Management Center on servers where you have installed Cisco CallManager. If you attempt to do so and the CSA MC installation detects that a version of Microsoft SQL Server runs on the server, the managed console installation automatically aborts.

After you have obtained the CSA MC package and documentation, perform the following procedure:

Procedure

Step 1 On a separate (non-Cisco CallManager) server, download the latest version of the Cisco CallManager policy XML file from the CallManager & Voice Apps Crypto Software Download site at http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des.

Step 2 Note the location where you saved the downloaded file.

Step 3 Uninstall the Cisco Security Agent, if it exists, by following the instructions in the "Uninstalling the Cisco Security Agent" section.

Step 4 Follow the instructions in *Installing Management Center for Cisco Security Agents* for installing the CSA MC.

Step 5 Follow the instructions in *Using Management Center for Cisco Security Agents* for importing the policy file that you downloaded in Step 1.

Step 6 Follow the instructions in *Installing Management Center for Cisco Security Agents* for completing the configuration of the CSA MC

Testing the Cisco Security Agent

In addition to verifying that the Agent is installed, you may want to test the Agent by attacking your own system. If so, go to the "Attack your system" section in the appendix "Evaluating the Cisco Security Agent" in Installing Management Center for Cisco Security Agents 4.0, which can be accessed from http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Messages and Logs

If the Cisco Security Agent has a message for you, the icon in the system tray (the red flag) will wave. To read the message, double-click the icon, then, click the Messages tab.

The messages that display comprise those that were generated when an action either was denied or generated a query. Only the two most recent messages display.

Find the log files in <InstallDrive>:\Program Files\Cisco\CSAgent\log.

- securitylog.txt—This main event log includes logs of rule violations and other relevant events.
- csalog.txt—This file provides Agent startup and shutdown history.
- driver_install.log—This log file provides a record of the driver installation process.
- Cisco Security AgentInstallInfo.txt—This file provides a detailed record of the installation process.

You can view the securitylog.txt file by using Notepad, or, to read the file more easily, you can

1. Copy the file to a computer on which Excel or another spreadsheet is installed.
2. Rename the file to securitylog.csv.
3. Double-click it to view it in the spreadsheet application.

The field names display in the first line of the spreadsheet. You may find it more convenient to see the contents of a spreadsheet cell by clicking on the cell and looking at the contents in the field above the spreadsheet matrix.

For diagnosing problems, the most important fields include DateTime, Severity, Text, and User. Ignore the RawEvent field; it contains essentially the same information the other fields present, but in an unprocessed and difficult to read form.

The order of the severity levels, from least to most severe, follows: Information, Notice, Warning, Error, Alert, Critical, Emergency.

Note Under normal circumstances, you should see very few entries in the log. A flurry of entries that appear at a particular time indicates that something of interest is occurring. You can usually tell from the text describing the events whether this is due to some internal problem (such as someone trying to install software without disabling the Agent) or an external problem (such as an attack on the system that the Agent is detecting and preventing).

Troubleshooting

Review the troubleshooting tips in this section before contacting the Cisco Technical Assistance Center (TAC).

Problems with Installing or Uninstalling the Agent

If you encounter problems with installing or uninstalling the agent, perform the following tasks:

- Verify that you rebooted the server.
- Verify that you did not use Terminal Services to install/upgrade the software.
- Verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Obtain the installation logs from <InstallDrive>:\Program Files\Cisco\CSAgent\log. Inspect the Cisco Security AgentInstallInfo.txt and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log should state that the csanet2k.inf installed. If the Network Shim is not installed, uninstall the agent and then install the agent again.

Problems Running Cisco CallManager or CSA Errors

Perform the procedure in this section if you encounter any of the following problems after installing Cisco Security Agent for Cisco CallManager:

- Problems with Cisco CallManager that cannot otherwise be explained
- CSA errors in the Windows event log or in the CSA log file (<InstallDrive>:\Program Files\Cisco\CSAgent\log\securitylog.txt)
- CSA error messages that display on the screen

If you cannot determine the cause of a CSA log entry or error message, contact Cisco TAC. However, before doing so, refer to the "Before You Call TAC" section on page 12.

To troubleshoot problems with Cisco CallManager or errors from Cisco Security Agent, perform the following procedure:

Procedure

Step 1 In the Windows task bar, right-click the Cisco Security Agent icon (the red flag in the Windows system tray), and click **Suspend security**.

Step 2 Perform the operation that caused the error message.

Step 3 In the Windows task bar, right-click the Cisco Security Agent icon and click **Resume security**.

Step 4 Perform the operation that caused the error message.

Step 5 If the operation completes successfully with the Cisco Security Agent suspended and continues to fail with the Cisco Security Agent enabled, confirm that all of the software applications that are running on the Cisco CallManager server are supported third-party applications that are shown in the "Introduction" section on page 2.

If unsupported software is installed on the server, remove the unsupported software and repeat this procedure.

If you cannot resolve the problem, refer to the "Before You Call TAC" section on page 12.

Second Attempt to Install Software Fails Without a Warning

Cisco Security Agent caches your responses to queries for 1 hour. This convenience feature means that you do not have to respond to a popup each time that you do a repetitive action; however, in certain situations, this feature may have undesirable results.

In the following case, an attempt to install software will fail without a warning:

1. You try to install software without first stopping and disabling the Cisco Security Agent service. Cisco Security Agent displays the following message:

   Cisco Security Agent: A problem was detected, press one of the action buttons below. Are you installing/uninstalling software? If not, this operation is suspicious.

2. You click **No**. (This action causes the problem when running the install the next time—see below.)
3. You stop and disable the Cisco Security Agent service.
4. You attempt to install the software a second time, but nothing happens.

When you clicked **No** in step 2 above, the system cached your answer in memory. The system clears the cache automatically after an hour.

To clear the cache immediately, so you can install the software now, perform the following procedure:

Procedure

Step 1 Reenable the service, as described in the section Reenabling the CSA, page 7.

Step 2 In the Windows task bar, double-click the Cisco Security Agent icon in the Windows system tray (the red flag).

Step 3 Click the **Advanced** tab.

Step 4 Click **Clear**.

Step 5 Close the Cisco Security Agent Control Panel.

Note Before you retry installing the software on the server, disable the Cisco Security Agent service. After you install the software, reenable the Cisco Security Agent service. See the "Disabling and Reenabling the Cisco Security Agent Service" section on page 6.

Before You Call TAC

If you cannot identify the problem after reviewing the troubleshooting tips, follow the procedure below before calling Cisco TAC:

Procedure

Step 1 In <InstallDrive>:\Program Files\Cisco\CSAgent\bin, double-click csainfo.bat. This will collect useful hardware and software data.

Step 2 csainfo will ask whether you want to stop the Agent. Click **Yes**. The file csainfo.log gets created.

Step 3 Zip up the <InstallDrive>:\Program Files\Cisco\CSAgent\ directory (which includes csainfo.log and securitylog.txt).

Step 4 Determine the version of your CSA engine and of your CSA policy (the section Checking the Agent and Policy Versions on the Server, page 6, describes the method for doing this).

Step 5 Contact TAC. Be prepared to provide them with the zipped file that you created in Step 3 and the information that you collected in Step 4.

Obtaining Additional Information About the Cisco Security Agent

For additional information on the Cisco Security Agent, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- In the Windows 2000 system tray, right-click the flag and choose **Open Control Panel**; go to Step 2.
- Choose **Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent**; go to Step 2.

Step 2 In the upper, right corner of the window, click the **?** icon.

The Cisco Security Agent documentation displays.

Tip To obtain the Cisco Security Agent 4.0 documentation, click the following URL:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Obtaining Related Cisco CallManager Documentation

Click the URLs in Table 1 to navigate to related Cisco CallManager documentation.

Table 1 Quick Reference for URLs

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

Table 1 Quick Reference for URLs (Continued)

Related Information and Software	URL and Additional Information
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco CallManager, SQL Server, and operating system service releases, upgrades, and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **Note** The operating system and SQL Server 2000 service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco Integrated Communications System (ICS) 7750	http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm
Cisco Emergency Responder	http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/index.htm

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation 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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

You can 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.

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

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 automatically

provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be 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/

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

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

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

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe