



Installing Cisco Security Agent for Cisco Customer Response Solutions

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



Note

When Cisco CallManager is installed on the Linux operating system, Cisco CRS and Cisco CallManager cannot reside on the same machine. Use this document to install Cisco Security Agent for Cisco CRS on the Microsoft Windows operating system.

Contents

This document contains information about the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [Before You Begin the Installation, page 3](#)
- [Installing the Cisco Security Agent, page 5](#)
- [Checking the Agent and Policy Versions on the Server, page 6](#)
- [Disabling and Reenabling the Cisco Security Agent Service, page 6](#)
- [Uninstalling the Cisco Security Agent, page 7](#)
- [Upgrading the Cisco Security Agent, page 8](#)
- [Migrating to the Management Center for Cisco Security Agent, page 8](#)
- [Messages, Logs, and Caching, page 9](#)
- [Troubleshooting, page 10](#)
- [Obtaining Additional Information About CSA, page 11](#)



Corporate Headquarters:

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

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

- [Obtaining Related Cisco CRS Documentation, page 12](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 13](#)
- [Cisco Product Security Overview, page 13](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 15](#)

Introduction

The standalone Cisco Security Agent (CSA) provides:

- Intrusion detection and protection for Cisco CRS.
- Defense against previously unknown attacks because CSA does not require signatures, as anti-virus software does.
- Reduced downtime, widespread attack propagation, and clean-up costs.

The Agent is provided free of charge by Cisco Systems for use with Cisco CRS software. The Agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested security rules set (policy). The Agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed. A policy controls access to system resources based on:

- The resources being accessed
- The operation being invoked
- The process invoking the action

This occurs transparently and does not hinder overall system performance.



Caution

Do not view Cisco Security Agent for Cisco CRS as providing complete security for Cisco CRS servers. Rather, view the Agent as an additional line of defense that, when used with other standard defenses such as virus-scanning software and firewalls, provides enhanced security. Cisco Security Agent for Cisco CRS provides enhanced defense for many different Cisco CRS installations and configurations, and thus cannot enforce network access control rules (which block outbound or inbound network traffic) or act as a host-based firewall.

Other security considerations include keeping the operating system updated. The source for many security references is the *IP Telephony Security Operations Guide to Best Practices* found at this location:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e47.html

The standalone Cisco Security Agent uses a static policy that cannot be changed or viewed. However, see the section [Migrating to the Management Center for Cisco Security Agent, page 8](#), for additional information.

Follow the installation instructions in this document to install the standalone Cisco Security Agent on all servers within the CRS cluster, including the CRS Engine, Database, and Voice over IP Monitoring components. Do not install the agent on client machines, such as those running the Cisco Desktop Product Suite or MRCP servers.

**Note**

If Cisco Security Agent has already been installed on a server where both Cisco CallManager and Cisco CRS reside, do not install Cisco Security Agent again on that server. Both products conform to the same Cisco Security Agent policies for the Microsoft Windows operating system. However, if Cisco CallManager has been installed on the Linux operating system, install Cisco CRS on a separate machine running the Microsoft Windows operating system.

System Requirements

- Cisco Customer Response Solutions. Supported Cisco CRS releases are published in the *Cisco CRS Software and Hardware Compatibility Guide*:
http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/crsmatrix.pdf
- Microsoft Windows 2000 Server in English.
- Windows Automatic Update configured so that it does not automatically download updates to the CRS server.

Before You Begin the Installation

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

- The Cisco Security Agent supports any Cisco Media Convergence Server (MCS) or customer-provided, Cisco-approved server where Cisco CRS and Cisco-provided operating system are installed, unless the *Cisco CallManager Compatibility Matrix* indicates otherwise.
- Confirm that the computer you are using to install Cisco Security Agent has up to 20 MB of hard disk space for the download file and the installed files.
- Do not install the agent between the operating system and Cisco CallManager installation.
- Before each Cisco CRS upgrade, you must disable the Cisco Security Agent service. You must also make sure that the service does not get enabled at any time during the Cisco CRS installation. For information on how to disable the service, see the section [Disabling and Reenabling the Cisco Security Agent Service](#), page 6.
- You must disable the Cisco Security Agent service before every operating system or Cisco CRS installation and upgrade, including maintenance release, service release, and support patch installations and upgrades. Ensure that the service does not get enabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade. After installing or upgrading the operating system, Cisco CRS, service release, or support patch, you must enable the Cisco Security Agent Service. When you disable the service, the agent no longer provides intrusion detection for the server.
- Before you install or upgrade the Cisco Security Agent, back up your Cisco CRS data. For more information on how to perform this task, refer to the appropriate version of the Cisco CallManager backup and restore documentation at <http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/bars40/index.htm>.

If you are using Cisco CRS, Release 4.5, use the *BARS for Cisco CRS 4.5* document:

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_4_5/english/adm_app/crs451br.pdf

In addition, the *Cisco CRS Installation Guide* provides information about backing up your data.

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_4_5/english/admn_app/crs451ig.pdf

- Before you install or upgrade the Cisco Security Agent, back up all applications that run in the voice cluster. Refer to the appropriate backup documentation for more information.
- Do not use Terminal Services to install or upgrade the Cisco Security Agent. Cisco installs Terminal Services so the Cisco Technical Assistance Center (TAC) 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.



Caution

If you currently run Cisco HIDS Agent (Entercept) on the server, you must uninstall the software from Add/Remove Programs before you install 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, install the Cisco Security Agent during a time when call processing is minimal. The Cisco Security Agent protects the server as soon as you install the software but does not provide complete functionality until you reboot the server.



Caution

Rebooting the server might cause call-processing interruptions. 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 > Uninstall Cisco 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, 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 (C:\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 Customer Response Solutions data to the server for any reason, you must reinstall the agent after you restore the Cisco CRS data.



Tip

If you encounter problems with installing or uninstalling the Cisco Security Agent, see the section [Troubleshooting, page 10](#).

Installing the Cisco Security Agent

Review the section [Before You Begin the Installation, page 3](#), which provides information to help ensure a successful installation.



Note

You must have access to the 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 3DES Cryptographic Software under export licensing control**. On the page that appears, select **CallManager** from the drop-down list of products and click **Submit**. A web form appears; check the appropriate boxes on that form and click **Submit**. A message appears telling you when you can expect to have download access.

To download and install the CSA software, complete the following steps:

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

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



Note

The filename structure is *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 file name *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.

Step 3 Note the location where you save 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 destination where the software will install;



Caution

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

Step 8 Click **Next** to install the Network Shim.



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 Click **Yes**.



Caution

The installation process can affect the performance of Cisco CRS, so it is best to install CSA for CRS and then reboot the server after regular business hours. Rebooting the server might 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** to reboot the server.



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 CRS cluster.

Checking the Agent and Policy Versions on the Server

To determine the agent and policy versions, complete the following steps:

Step 1 Double-click the red flag icon in the system tray area.

Step 2 Choose **Status** to view the Product ID information.

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 CRS server again.

Use “Services” selected from the Microsoft Administrative Tools Control Panel to disable the Cisco Security Agent. It is best to shut down the Cisco Security Agent and then deliberately start it up again.



Caution

It is possible to suspend the Cisco Security Agent using the “net stop csagent” command in a command shell. This method does not actually disable the agent; it merely suspends it. Suspending the agent is not supported 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.

Disabling the CSA

To disable the CSA service, complete the following steps:

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

Step 2 From the Services window, right-click **Cisco Security Agent** and choose Properties.

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

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

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

Step 6 Click **OK**.

**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 Customer Response Solutions.

**Caution**

You must reenable the Cisco Security Agent service after every Cisco CRS installation or upgrade.

Reenabling the CSA

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

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 section [Before You Begin the Installation, page 3](#), which provides information about uninstalling the Cisco Security Agent.

You cannot install one 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, complete the following steps:

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.

Please note that the way in which the version number is reported has changed in CSA 4.5 (file name starting with CiscoCM-CSA-4.5...) as compared to CSA 4.0 (file name starting with CiscoCM-CSA-4.0...). In CSA 4.5, the version number is integrated with the Standalone Agent as described in [Checking the Agent and Policy Versions on the Server, page 6](#). In CSA 4.0, the version is obtained by selecting **Start > Cisco OS Version**. When uninstalling CSA 4.5, the policy version is removed along with the Standalone Agent. When uninstalling CSA 4.0 and selecting **Start > Cisco OS Version**, the old information continues to appear unless you manually delete it by using regedit to remove the entry “CCM-CSA Policy” at HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems, Inc.\System Info\CCM-CSA Policy. If you have never installed a CSA 4.0-based policy, then this does not apply.

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 section [Uninstalling the Cisco Security Agent, page 7](#).
2. Install the new version that you plan to run on the server.
See the section [Installing the Cisco Security Agent, page 5](#).

Migrating to the Management Center for Cisco Security Agent

The security agent included with Cisco CRS 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 installed on other network systems and servers.
- The Cisco Security Agent (the managed agent) installs on all Cisco CRS servers in the voice 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 CRS environment, ensure that the Management Center component is installed on a separate, secured server and that the managed agent component is installed on all Cisco CRS 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*.

Once you have obtained the CSA MC package and documentation, perform the following procedure.

-
- Step 1** On a separate (non-Cisco CRS) server, download the latest version of the Cisco CallManager policy XML file (CiscoCM-CSA-n.n.n.nnn-n.n.nn.export) 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 save the downloaded file.
- Step 3** Uninstall the Cisco Security Agent, if it exists, 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.
-

Messages, Logs, and Caching

This section provides information on how the cache works and discusses event messages and log files.

Event Messages and Log Files

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 following 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 following these steps:

1. Double-click the CSA icon (the red flag in the Windows system tray)
2. Click **Messages** (on the left under Status)
3. Click **View Log** and a pop-up window displays the text of the log file.

You can also use Microsoft Excel to read the file more easily, by following these steps:

1. Copy the file to a computer on which Microsoft Excel is installed.

2. Rename the file to securitylog.csv.
3. Double-click the file to view it in the spreadsheet application.

The field names display in the first line of the spreadsheet. You might 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 these entries are 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).

Understanding How the Cache Works

Cisco Security Agent caches your responses to queries. This is a convenience feature so that you do not have to respond to a pop-up each time you do a repetitive action. The Agent can remember query responses either permanently or temporarily.

The Agent remembers responses to queries permanently based on user input. For example, if a user is queried as to whether an application can talk on the network, and the user responds by selecting **Yes** and clicking **Don't ask again**, the Agent remembers the Yes response permanently and that response appears in the right pane of the window that appears when you double-click the red flag icon and select **Status > User Query Responses** in the left pane.

The Agent remembers responses to queries temporarily if, for example, the user is queried as to whether setup.exe can install software on the system and the user selects **Yes**, but is not given the option of selecting **Don't ask again**. Then the query does not appear when you select **Status > User Query Responses**.

Permanent responses are remembered across reboots. Temporary responses are not remembered across reboots. Also, a query response is tied to the user who responds. On multi-user machines, multiple users may be asked the same question.

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 or uninstall the CSA..
- For installations, verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Verify that the Cisco Security Agent service is not disabled and that its Startup Type value is Automatic.
- Obtain the installation logs from <Install Drive>:\Program Files\Cisco\CSAgent\log. Review the CSAgent-Install.log and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log file should state that the csanet is installed. If the Network Shim is not installed, uninstall the agent and then install the agent again.

Before You Call Cisco TAC

If you cannot identify the problem after reviewing the troubleshooting tips, follow the procedure below before calling the Cisco Technical Assistance Center (TAC):

-
- Step 1** Check the CSA diagnostics by selecting **Start > Programs > Cisco Security Agent > Cisco Security Agent Diagnostics**.
- Step 2** Respond **Yes** when asked if you want to stop the Agent. A command window shows files being copied. When the operation is complete, a message box indicates the location of the csa-diagnostics.zip file.
- Step 3** Click **OK**. The Agent restarts.
- 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 to do so).
- Step 5** Contact the TAC. Be prepared to provide the TAC with the zipped file that you created in Step 3 and the information that you collected in Step 4.
-

Obtaining Additional Information About CSA

For additional information about the Cisco Security Agent, perform the following 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 documentation, go to:
<http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html>

Obtaining Related Cisco CRS Documentation

The latest version of the Cisco CRS documentation can be found at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_4_5/english/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/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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, 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, 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, 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. (0601R)

