



# Release Notes for Cisco Security Agent for Cisco Unity Bridge, Release 2.0(2)

---

*Published December 2, 2005*

These release notes provide download, installation, and upgrade instructions, information on new and changed functionality, and caveats for Cisco Security Agent for Cisco Unity Bridge, Release 2.0(2).

Cisco Security Agent for Cisco Unity Bridge software is available on the Cisco Unity Bridge Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/bridg3d>.

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [Requirements and Supported Software, page 3](#)
- [Determining the Software Version, page 4](#)
- [Notes on Using Cisco Security Agent for Cisco Unity Bridge, page 4](#)
- [Downloading Cisco Security Agent for Cisco Unity Bridge 2.0\(2\), page 5](#)
- [Installing Cisco Security Agent for Cisco Unity Bridge 2.0\(2\), page 6](#)
- [Upgrading to Cisco Security Agent for Cisco Unity Bridge 2.0\(2\), page 7](#)
- [Disabling and Re-enabling the Cisco Security Agent Service, page 7](#)
- [Uninstalling Cisco Security Agent for Cisco Unity Bridge, page 8](#)
- [New and Changed Functionality—Release 2.0\(2\), page 8](#)
- [Caveats, page 9](#)
- [Troubleshooting, page 9](#)
- [Cisco Unity Documentation, page 11](#)
- [Obtaining Documentation, page 11](#)
- [Documentation Feedback, page 12](#)



---

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

© 2005 Cisco Systems, Inc. All rights reserved.

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

## Introduction

Cisco Security Agent for Cisco Unity Bridge is a standalone Cisco Security Agent that is provided free of charge by Cisco Systems for use with Cisco Unity Bridge servers that meet the system requirements specified in the “[Requirements and Supported Software](#)” section on page 3.

The standalone Cisco Security Agent (CSA) provides:

- Intrusion detection and prevention for Cisco Unity Bridge software.
- Defense against previously unknown attacks because it does not require signatures, as antivirus software does.
- Reduced downtime, attack propagation, and cleanup costs.

The agent provides Windows platform security (host intrusion detection and prevention) that is based on a tested set of security rules known as a policy. The policy allows or denies specific system actions before system resources are accessed, based on the following criteria:

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

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



### Caution

---

Do not view Cisco Security Agent for Cisco Unity Bridge as providing complete security for a Cisco Unity Bridge server. Instead, view it as an additional line of defense that, when used correctly with other standard defenses such as antivirus software and firewalls, provides enhanced security.

---

The best starting point for references to security and voice products is <http://www.cisco.com/go/ipcsecurity>. We recommend the *IP Telephony Security Operations Guide to Best Practices*.

In addition, refer to the *Cisco Unity Security Guide, Release 4.x*:

- The Domino version of the guide is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/usg/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/dom/index.htm).
- The Exchange version of the guide is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/usg/ex/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/usg/ex/index.htm).

# Requirements and Supported Software

## Software Requirements

- Cisco Unity Bridge version 3.0(1) or later running on the Bridge server.
- Microsoft Windows 2000 Server in English running on the Bridge server. Other language versions are not supported.

**Note**

---

If you install Cisco Security Agent for Cisco Unity Bridge on a server running Windows in Japanese, the display of some non-ASCII characters will be corrupted.

---

## Supported Optional Software

Only the following optional software has been qualified for use on a Bridge server that is running Cisco Security Agent for Cisco Unity Bridge:

- McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 and later.
- VERITAS
  - Backup Exec for Microsoft Windows NT and Windows 2000, version 8.6.
  - NetBackup version 4.5 and later.
- Windows Automatic Update. It must be configured not to automatically download updates to the Bridge server.

## Support Policy for Optional Software

Cisco support policy is that customers can deploy third-party software for backup, monitoring, and security, including modified CSA policies, on the Cisco Unity Bridge server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with the Bridge and Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment between Cisco Unity and the third-party products loaded on the Bridge server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Bridge server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and the Bridge or Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Bridge server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Cisco Unity system.

Before installing any qualified optional service pack on the Bridge server, confirm that the manufacturer of any optional software or hardware that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

# Determining the Software Version

The version of Cisco Security Agent for Cisco Unity Bridge and the version of the policy that the agent was created with are the same. Do the following procedure to determine the version for both the agent and the policy.

## To Determine the Cisco Security Agent for Cisco Unity Bridge Version and Policy Version in Use

---

- Step 1** Double-click the Cisco Security Agent taskbar icon.
  - Step 2** In the tree control on the left of the Cisco Security Agent Panel, click **Status**.
  - Step 3** The version number in the Product ID field applies both to Cisco Security Agent for Cisco Unity Bridge and to the policy that the agent was created with.
- 

## To Determine the Version of the Cisco Security Agent Engine

---

Right-click the Cisco Security Agent taskbar icon, and click **About**.

---

# Notes on Using Cisco Security Agent for Cisco Unity Bridge

The following sections contain information on using Cisco Security Agent for Cisco Unity Bridge:

- [Cisco Security Agent Service Must Be Disabled for Specific Tasks, page 4](#)
- [Locations in Which Cisco Security Agent Logs Events, page 5](#)

## Cisco Security Agent Service Must Be Disabled for Specific Tasks

The Cisco Security Agent service must be disabled and stopped in the following situations:

- Before you install any software on the Bridge server.
- Before you upgrade any software, including Cisco Unity Bridge, on the Bridge server. This also applies to automatic upgrades (for example, installing service packs by using group policy objects or custom scripts). Cisco Security Agent for Cisco Unity Bridge allows supported antivirus applications to automatically download and install upgrades to virus-scanning components.
- Before you add, change, or delete values in the Windows registry.
- Before you change Windows system or boot files.



### Caution

When you disable and stop the Cisco Security Agent service, you must re-enable and start it before it can monitor the Bridge server again.

---

For instructions on disabling and re-enabling the service, see the [“Disabling and Re-enabling the Cisco Security Agent Service” section on page 7](#).

## Locations in Which Cisco Security Agent Logs Events

Cisco Security Agent logs events in the following three locations:

Windows application event log	Events that are generated by Cisco Security Agent have an event source of CSAgent.
Securitylog.txt	<p>Cisco Security Agent logs one event per line. The data in the file is in comma-separated-value format. In general, there should not be many entries in the file, so you should be able to read it in a text editor, for example, Notepad. (You might want to turn off word wrap.) If there are a lot of entries, you can view the data more easily if you copy the file to a computer on which a spreadsheet application is installed, change the file-name extension from .txt to .csv, and open the file in the spreadsheet application.</p> <p>To view the log, double-click the Cisco Security Agent taskbar icon. In the tree control on the left of the Cisco Security Agent Panel, click <b>Messages</b>. Then click <b>View Log</b>. (The log appears in the Program Files\Cisco Systems\CSAgent\Log directory.)</p>
Current messages	To display events that have occurred since you logged on to Windows, double-click the Cisco Security Agent taskbar icon. In the Cisco Security Agent Panel, click <b>Messages</b> .

## Downloading Cisco Security Agent for Cisco Unity Bridge 2.0(2)

### To Download Cisco Security Agent for Cisco Unity Bridge 2.0(2)

- Step 1** Confirm that the computer you are using has up to 20 MB of hard-disk space for the download file and the installed files.
- Step 2** On a computer with a high-speed Internet connection, go to the Cisco Unity Bridge Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/bridg3d>.



**Note** To access the software download page, you must be logged on to Cisco.com as a registered user.

Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unity Bridge, you need to fill out a brief questionnaire. Follow the on-screen prompts.

- Step 3** Click **CiscoUnityBridge-CSA-4.5.1.639-2.0.2-K9.exe**.
- Step 4** Follow the on-screen prompts to complete the download.
- Step 5** If you plan to install Cisco Security Agent for Cisco Unity Bridge from a compact disc, burn the CD.

# Installing Cisco Security Agent for Cisco Unity Bridge 2.0(2)



## Note

If you are upgrading Cisco Security Agent for Cisco Unity Bridge to version 2.0(2), see the “[Upgrading to Cisco Security Agent for Cisco Unity Bridge 2.0\(2\)](#)” section on page 7.

We recommend that you install Cisco Security Agent for Cisco Unity Bridge after regular business hours because the installation will affect Bridge performance. In addition, when the installation completes, you must restart the Bridge server for Cisco Security Agent for Cisco Unity Bridge to start working.



## Caution

Do not install Cisco Security Agent for Cisco Unity Bridge by using Windows Terminal Services, or the installation will fail.

### To Install Cisco Security Agent for Cisco Unity Bridge 2.0(2)

- Step 1** Log on to the Cisco Unity Bridge server by using an account that is a member of the Administrators group or the Local Administrators group.
- Step 2** Confirm that the server has at least 20 MB of hard-disk space available for the download file and the installed files.
- Step 3** If another intrusion-detection application is installed on the Bridge server, uninstall the application before installing Cisco Security Agent for Cisco Unity Bridge. Refer to the applicable documentation.
- Step 4** If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.
- Step 5** If antivirus software is installed on the Bridge server, disable and stop the scanning services:
  - a. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - b. In the right pane, double-click the name of the first virus-scanning service.
  - c. On the General tab, click **Stop** to stop the service immediately.
  - d. In the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
  - e. Click **OK** to close the Properties dialog box.
  - f. Repeat Step **b** through Step **e** for each of the remaining virus-scanning services.
  - g. When the services have been disabled, close the Services MMC.
- Step 6** In Windows Explorer, browse to the directory to which you downloaded the Cisco Security Agent for Cisco Unity Bridge file, and double-click **CiscoUnityBridge-CSA-4.5.1.639-2.0.2-K9.exe**.
- Step 7** Follow the on-screen prompts.



## Caution

Do not change any of the default values, or Cisco Security Agent for Cisco Unity Bridge may not function properly.

- Step 8** When the installation completes, click **Yes, I Want to Restart My Computer Now**, and click **Finish**.  
Cisco Security Agent for Cisco Unity Bridge begins to work as soon as you restart the Bridge server. You do not need to configure the application.

- Step 9** If antivirus software is installed on the Bridge server, re-enable and start the scanning services:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - In the right pane, double-click the name of the first virus-scanning service.
  - On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
  - Click **Start** to start the service.
  - Click **OK** to close the Properties dialog box.
  - Repeat Step **b** through Step **e** for each of the remaining virus-scanning services.
  - When the services have been disabled, close the Services MMC.

## Upgrading to Cisco Security Agent for Cisco Unity Bridge 2.0(2)

Use the task list in this section to upgrade to version 2.0(2) of the Cisco Security Agent for Cisco Unity Bridge. The tasks refer to sections in these release notes.

### Upgrade Task List

- Download the software. See the [“Downloading Cisco Security Agent for Cisco Unity Bridge 2.0\(2\)” section on page 5](#).
- Stop and disable the Cisco Security Agent service. See the procedure [“To Stop and Disable the Cisco Security Agent Service”](#) in the [“Disabling and Re-enabling the Cisco Security Agent Service” section on page 7](#).
- Uninstall the previous version. See the [“Uninstalling Cisco Security Agent for Cisco Unity Bridge” section on page 8](#).
- Install version 2.0(2). See the [“Installing Cisco Security Agent for Cisco Unity Bridge 2.0\(2\)” section on page 6](#). When the installation is complete, the Cisco Security Agent service is enabled automatically.

## Disabling and Re-enabling the Cisco Security Agent Service

The Cisco Security Agent service must be disabled and stopped before you install or upgrade any software on the Bridge server. (For information on other situations in which you must disable the Cisco Security Agent service, see the [“Cisco Security Agent Service Must Be Disabled for Specific Tasks” section on page 4](#).)



#### Caution

When you disable and stop the Cisco Security Agent service, you must re-enable and start it before it can monitor the Bridge server again.

#### To Stop and Disable the Cisco Security Agent Service

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.

- Step 2 In the right pane, double-click **Cisco Security Agent**.
  - Step 3 On the General tab, click **Stop** to stop the service immediately.
  - Step 4 In the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
  - Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.
  - Step 6 When the service has been disabled, close the Services MMC.
- 

#### To Re-enable and Start the Cisco Security Agent Service

---

- Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2 In the right pane, double-click **Cisco Security Agent**.
  - Step 3 On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
  - Step 4 Click **Start** to start the service.
  - Step 5 Click **OK** to close the Cisco Security Agent Properties dialog box.
  - Step 6 When the service has been re-enabled, close the Services MMC.
- 

## Uninstalling Cisco Security Agent for Cisco Unity Bridge

#### To Uninstall Cisco Security Agent for Cisco Unity Bridge

---

- Step 1 Stop the Cisco Security Agent service:
    - a. On the Windows Start menu, click **Programs > Administrative Tools > Services**.
    - b. In the right pane, double-click **Cisco Security Agent**.
    - c. On the General tab, click **Stop** to stop the service immediately.
    - d. Click **OK** to close the Cisco Security Agent Properties dialog box.
  - Step 2 On the Windows Start menu, click **Programs > Cisco Systems > Uninstall Cisco Security Agent**.
  - Step 3 Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unity Bridge.
  - Step 4 Click **Yes** again to restart the Bridge server.
- 

## New and Changed Functionality—Release 2.0(2)

This section contains information about new and changed functionality for Cisco Security Agent for Cisco Unity Bridge Release 2.0(2) only. Refer to the release notes of the applicable version for information about new and changed functionality in earlier versions of Cisco Security Agent for Cisco Unity Bridge. Release notes for all versions of Cisco Security Agent for Cisco Unity Bridge are available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html).

## Version 2.0(2) Compiled with Cisco Security Agent Version 4.5.1.639

The standalone Cisco Security Agent for Cisco Unity Bridge 2.0(2) is compiled with Cisco Security Agent version 4.5.1, build 639.

## Caveats

This section describes Severity 1, 2, and 3 caveats.

You can find the latest caveat information for Cisco Security Agent for Cisco Unity Bridge 2.0(2)—in addition to caveats of any severity for any release—by using Bug Toolkit, an online tool available for customers to query defects according to their own needs. Bug Toolkit is available at [http://www.cisco.com/pegi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/pegi-bin/Support/Bugtool/launch_bugtool.pl).



Note

---

To access Bug Toolkit, you must be logged on to Cisco.com as a registered user.

---

This section contains caveat information for Cisco Security Agent for Cisco Unity Bridge 2.0(2) only. Refer to the release notes of the applicable version for caveat information for earlier versions of Cisco Security Agent for Cisco Unity Bridge. Release notes for all versions of Cisco Security Agent for Cisco Unity Bridge are available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html).

## Open Caveats—Release 2.0(2)

There are no open caveats for Cisco Security Agent for Cisco Unity Bridge Release 2.0(2).

## Resolved Caveats—Release 2.0(2)

There are no resolved caveats for Cisco Security Agent for Cisco Unity Bridge Release 2.0(2).

## Troubleshooting

The following sections contain information on troubleshooting Cisco Security Agent for Cisco Unity Bridge:

- [Problems with the Cisco Unity Bridge or Errors from Cisco Security Agent, page 9](#)
- [Second Attempt to Install Software Fails Without a Warning, page 10](#)

## Problems with the Cisco Unity Bridge or Errors from Cisco Security Agent

Do the procedure in this section if you encounter any of the following problems after installing Cisco Security Agent for Cisco Unity Bridge:

- Problems with the Bridge that cannot otherwise be explained.

- Cisco Security Agent errors in the Windows event log or in the Cisco Security Agent log file, Program Files\Cisco Systems\CSAgent\log\securitylog.txt.
- Cisco Security Agent error messages displayed on the screen.

If you cannot determine the cause of a Cisco Security Agent log entry or error message, contact Cisco TAC.

#### To Troubleshoot Problems with the Bridge or Errors from Cisco Security Agent

---

- Step 1** Stop the Cisco Security Agent service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - In the right pane, double-click **Cisco Security Agent**.
  - On the General tab, click **Stop** to stop the service immediately.
  - Click **OK** to close the Cisco Security Agent Properties dialog box.
- Step 2** Do the operation that caused the error message.
- Step 3** Restart the Cisco Security Agent service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - In the right pane, double-click **Cisco Security Agent**.
  - On the General tab, click **Start** to restart the service.
  - Click **OK** to close the Cisco Security Agent Properties dialog box.
- Step 4** Do the operation that caused the error message.
- Step 5** If the operation completes successfully with the Cisco Security Agent service stopped and continues to fail with the Cisco Security Agent service running, confirm that all of the software running on the Bridge server is listed as supported in the [“Requirements and Supported Software”](#) section on page 3.
- If unsupported software is installed on the server, remove the unsupported software and repeat this procedure.
- Step 6** If you are unable to resolve the problem, contact Cisco TAC and send them the Cisco Security Agent log file, Program Files\Cisco Systems\CSAgent\log\securitylog.txt.
- 

## Second Attempt to Install Software Fails Without a Warning

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

- You tried to install software without first stopping and disabling the Cisco Security Agent service.
- Cisco Security Agent displayed the 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.”
- You clicked **No**.
- You stopped and disabled the Cisco Security Agent service.
- You tried again to install the software, but nothing happened.

When you clicked No in Step 3., your answer was cached in memory. The cache is cleared automatically after an hour. To clear the cache immediately so you can install the software now, do the following procedure.

#### To Clear the Cisco Security Agent Memory Cache So You Can Install Software

---

- Step 1** In the Windows taskbar, double-click the **Cisco Security Agent** taskbar icon.
  - Step 2** In the tree control on the left of the Cisco Security Agent Panel, click **User Query Responses**.
  - Step 3** Click **Clear**.
  - Step 4** Click **OK**.
  - Step 5** Before you retry installing software on the server, stop and disable the Cisco Security Agent service. See the procedure “[To Stop and Disable the Cisco Security Agent Service](#)” section on page 7.
  - Step 6** After you install the software, re-enable and restart the Cisco Security Agent service. See the procedure “[To Re-enable and Start the Cisco Security Agent Service](#)” section on page 8.
- 

## Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/about/aboutdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.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](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

## Ordering Documentation

Beginning June 30, 2005, 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](mailto: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 send comments about Cisco documentation to [bug-doc@cisco.com](mailto: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](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](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](mailto: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.

- Nonemergencies—[psirt@cisco.com](mailto: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 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 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](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.

## 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)—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, 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>

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

© 2005 Cisco Systems, Inc. All rights reserved.