



Release Notes for Cisco Security Agent for Cisco Unity Bridge, Release 1.1(4)

Published April 14, 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 1.1(4).

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 5](#)
- [Downloading Cisco Security Agent for Cisco Unity Bridge 1.1\(4\), page 6](#)
- [Installing Cisco Security Agent for Cisco Unity Bridge 1.1\(4\), page 7](#)
- [Upgrading to Cisco Security Agent for Cisco Unity Bridge 1.1\(4\), page 8](#)
- [Disabling and Re-enabling the Cisco Security Agent Service, page 8](#)
- [Uninstalling Cisco Security Agent for Cisco Unity Bridge, page 9](#)
- [New and Changed Functionality—Release 1.1\(4\), page 9](#)
- [Caveats, page 10](#)
- [Troubleshooting, page 10](#)
- [Cisco Unity Documentation, page 12](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 13](#)



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

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

- [Cisco Product Security Overview](#), page 13
- [Obtaining Technical Assistance](#), page 14
- [Obtaining Additional Publications and Information](#), page 16

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 agent provides intrusion prevention, malicious mobile code protection, operating system integrity assurance, and audit log consolidation based on a tested set of security rules (policies). It controls system operations by allowing or denying selected system actions before system resources are accessed. This process occurs transparently and does not significantly affect overall system performance.



Caution

Cisco Security Agent for Cisco Unity Bridge should not be viewed as providing complete security for Cisco Unity Bridge servers. Instead, it should be viewed as an additional line of defense that enhances security when used with other defenses such as virus-scanning software and a firewall. Cisco Security Agent for Cisco Unity Bridge is designed to provide enhanced defense for many different Cisco Unity Bridge installations and configurations, and thus cannot enforce network access control rules or act as a host-based firewall.

The agent was created by using CiscoWorks Management Center for Cisco Security Agents and is based on the following Management Center for Cisco Security Agents version 4.0.3, build 736 policies:

- Required Windows System Module
- Common Security Module
- Common Web Server Security Module
- Restrictive MS IIS Module
- Server Module
- User Authentication Auditing Module
- Virus Scanner Module

Cisco Security Agent for Cisco Unity Bridge version 1.1(4) also includes the Unity Bridge Base Group Exceptions policy, which allows normal Bridge operations that the other policies would not allow.

To add, delete, or view policies included in Cisco Security Agent for Cisco Unity Bridge, run CiscoWorks Management Center for Cisco Security Agents, and import the file CiscoUnityBridge-CSA-4.0.3.736-1.1.4.export. The file is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/bridg3d>.

For more information on CiscoWorks Management Center for Cisco Security Agents and on Cisco Security Agent, refer to <http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html>.

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

This section contains procedures for determining the version in use for the following software:

- [Cisco Security Agent, page 4](#)
- [Policy for Cisco Security Agent for Cisco Unity Bridge, page 4](#)

Cisco Security Agent

To Determine the Cisco Security Agent Version in Use

Step 1 Start Regedit.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3 Expand the key
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\CSA Agent\Version.

Step 4 Close Regedit.

Policy for Cisco Security Agent for Cisco Unity Bridge

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

Step 1 Start Regedit.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (Refer to the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3 Expand the key
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\System Info\UnityBridge-CSA Policy\Version.

Step 4 Close Regedit.

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 5](#)
- [Cisco Security Agent Taskbar Icon Available Only for First Windows Logon, page 5](#)
- [Locations in Which Cisco Security Agent Logs Events, page 6](#)

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 virus-scanning 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

Do not stop the Cisco Security Agent service by using the net stop command or the Cisco Security Agent icon in the taskbar. These methods are not supported.



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 8.

Cisco Security Agent Taskbar Icon Available Only for First Windows Logon

If two people log on to Windows on the Bridge server—one at the server and the other by using Windows Terminal Services, or both by using Terminal Services—only the first person to log on will have access to the Cisco Security Agent icon.

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. We recommend that each administrator who logs on to the Cisco Unity server add a shortcut for Securitylog.txt to the Windows desktop. The file is located in the <InstallDirectory>\Cisco\CSAgent\Log directory.</p> <p>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>
CSA Control Panel	To display the CSA Control Panel, double-click the Cisco Security Agent taskbar icon, and click the Messages tab. Only events that have occurred since you logged on to Windows appear in the CSA Control Panel.

Downloading Cisco Security Agent for Cisco Unity Bridge 1.1(4)

To Download Cisco Security Agent for Cisco Unity Bridge 1.1(4)

- 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-4.0.3.736-1.1.4-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 1.1(4)


Note

If you are upgrading Cisco Security Agent for Cisco Unity Bridge to version 1.1(4), see the “[Upgrading to Cisco Security Agent for Cisco Unity Bridge 1.1\(4\)](#)” section on page 8.

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 1.1(4)

- 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 Cisco IDS Host Sensor or 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 Cisco IDS Host Sensor or other applicable documentation.
- Step 4** If Windows Automatic Update is configured to automatically download updates from the Microsoft website, disable it.
- Step 5** If virus-scanning 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, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - d. Click **Stop** to stop the service immediately.
 - 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-4.0.3.736-1.1.4-K9.exe**.
- Step 7** Follow the on-screen prompts.


Caution

Do not change any of the default values, or the Cisco Security Agent 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 virus-scanning software is installed on the Bridge server, re-enable and start 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, in the Startup Type list, click **Automatic** to re-enable the service.
 - d. Click **Start** to start the service.
 - 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.

Upgrading to Cisco Security Agent for Cisco Unity Bridge 1.1(4)

Use the task list in this section to upgrade to version 1.1(4) of the Cisco Security Agent for Cisco Unity Bridge. The tasks refer to sections in these release notes.

Upgrade Task List

1. Download the software. See the [“Downloading Cisco Security Agent for Cisco Unity Bridge 1.1\(4\)” section on page 6](#).
2. Disable the Cisco Security Agent service. See the procedure [“To Disable and Stop the Cisco Security Agent Service”](#) in the [“Disabling and Re-enabling the Cisco Security Agent Service” section on page 8](#).
3. Uninstall the previous version. See the [“Uninstalling Cisco Security Agent for Cisco Unity Bridge” section on page 9](#).
4. Install version 1.1(4). See the [“Installing Cisco Security Agent for Cisco Unity Bridge 1.1\(4\)” section on page 7](#). 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 5](#).)



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.



Caution

Do not stop the Cisco Security Agent service by using the net stop command or the Cisco Security Agent icon in the taskbar. These methods are not supported.

To Disable and Stop 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 **Disabled**. This prevents the service from starting when you restart the server.
 - Step 4** Click **Stop** to stop the service immediately.
 - 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** Right-click the **Cisco Security Agent** icon in the Windows taskbar, and click **Suspend Security**.
If the icon does not appear in the taskbar, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the **Cisco Security Agent** service.
 - 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 1.1(4)

This section contains information about new and changed functionality for Cisco Security Agent for Cisco Unity Bridge Release 1.1(4) 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.

Version 1.1(4) Compiled with Cisco Security Agent Version 4.0.3.736

Cisco Security Agent for Cisco Unity Bridge 1.1(4) is compiled with Cisco Security Agent version 4.0.3, build 736.

Caveats

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

If you have an account with Cisco.com, you can use Bug Toolkit to find more information on the caveats in this section, in addition to caveats of any severity for any release. Bug Toolkit is available at the website http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Note that this section contains caveat information for Cisco Security Agent for Cisco Unity Bridge Release 1.1(4), and for Cisco Security Agent versions 4.0.1, build 539 through 4.0.3, build 736 that may affect Cisco Security Agent for Cisco Unity Bridge. For caveat information for earlier versions of Cisco Security Agent for Cisco Unity Bridge, refer to the applicable release notes. 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.

Open Caveats—Release 1.1(4)

There are no open caveats for Cisco Security Agent for Cisco Unity Bridge Release 1.1(4).

Resolved Caveat—Release 1.1(4)

Table 1 Cisco Security Agent for Cisco Unity Bridge Release 1.1(4) Resolved Caveat

Caveat Number	Severity	Component	Description
CSCeg67061	2	csa	Blue screen occurs during a race condition where one thread set a variable to null while that variable was in use by another thread.

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 10](#)
- [Second Attempt to Install Software Fails Without a Warning, page 11](#)

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, <Drive>:\Program Files\Cisco\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** In the Windows taskbar, right-click the **Cisco Security Agent** icon, and click **Suspend Security**.
- Step 2** Do the operation that caused the error message.
- Step 3** In the Windows taskbar, right-click the **Cisco Security Agent** icon, and click **Resume Security**.
- Step 4** Do 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 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, <Drive>:\Program Files\Cisco\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:

1. You tried to install software without first disabling and stopping the Cisco Security Agent service.
2. 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.”
3. You clicked **No**.
4. You disabled and stopped the Cisco Security Agent service.
5. 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** icon.
- Step 2** Click the **Advanced** tab.
- Step 3** Click **Clear**.
- Step 4** Close the Cisco Security Agent Control Panel.

- Step 5** Before you retry installing software on the server, disable the Cisco Security Agent service. See the procedure “[To Disable and Stop the Cisco Security Agent Service](#)” section on page 9.
- Step 6** After you install the software, re-enable the Cisco Security Agent service. See the procedure “[To Re-enable and Start the Cisco Security Agent Service](#)” section on page 9.
-

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.

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

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

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

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID

or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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.