



Cisco Content Security and Control Release Notes Version 6.0(b1349)

February 2006

Contents

This document contains release information for Content Security and Control (CSC) Version 6.0. It includes the following sections:

- [Introduction, page 1](#)
- [Getting Started with CSC SSM, page 3](#)
- [System Requirements, page 3](#)
- [Caveats, page 4](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation, page 5](#)
- [Documentation Feedback, page 6](#)
- [Cisco Product Security Overview, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 9](#)

Introduction

CSC provides an all-in-one malware management solution for your network. The CSC software runs on an SSM that is installed in a compatible Cisco ASA 5500 series adaptive security appliance. The CSC SSM provides the following benefits:

- Detection of and actions to prevent viruses, worms, Trojans, and other threats in your SMTP, POP3, HTTP, and FTP network traffic.



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

© 2006 Cisco Systems, Inc. All rights reserved.



Note Traffic using other protocols, such as HTTPS, is not scanned by CSC.

- Blocking of compressed or very large files that exceed specified parameters.
- Scans for and removal of spyware, adware, and other types of grayware.

The above features are available to all customers with the Base License for CSC. If you purchased the Plus level of the CSC license in addition to the Base License, you also benefit from the following:

- Protection against spam and phishing fraud in your SMTP and POP3 traffic.
- Content filters that enable you to allow or prohibit email traffic containing key words or phrases.
- Blocking of URLs that you do not want employees to access, or URLs that are known to have hidden or malicious purposes.
- Filtering of URL traffic according to predefined categories that you allow/disallow, such as adult/mature content, games, chat/instant messaging, or gambling sites.

With CSC, you do not have to install separate applications for virus protection, spyware blocking, spam detection, or content filtering—all of these functions are available in a single package. CSC provides protection for major traffic protocols—SMTP, HTTP, FTP, and POP3—to ensure that employees do not accidentally introduce viruses from their personal email accounts. And, the application is easy to maintain; after installation and initial configuration, you are unlikely to need to change CSC configuration often.

Features

CSC helps you manage threats to your network. [Table 1](#) provides an overview.

Table 1 *Features and Benefits*

Features
Scans for traffic containing viruses, and manages infected messages or files
Scans for spam at low to high threshold levels, and allows you to determine how spam is handled
Filters offensive or inappropriate content
Blocks incoming file types that can damage your network
Helps prevent DoS (denial of service) attacks by setting limits on message size
Provides approved senders and blocked senders functionality for file and URL blocking
Filters access to URLs by category
Blocks connections to URLs or FTP sites prohibited by your corporate policies
Benefits
Allied with powerful Cisco firewall protection, Trend Micro InterScan for Cisco CSC SSM secures your network from threats, spam, and unwanted content
Easy to install with a user-friendly setup program
Antivirus, spyware/grayware detection, file blocking, and other protections against security risks in your network traffic is integrated with ASDM
Allows you to fine-tune configuration of the scanning, anti-spam, and filtering features after installation

Table 1 **Features and Benefits (continued)**

Features
Can be configured to automatically update the virus pattern file, scan engine, and spam rules and engine, as soon as new versions become available from Trend Micro
Provides email and syslog notifications to make sure you stay informed of activity
Provides log files that are purged automatically after 30 days
Provides a user-friendly console that includes online help to guide you through tasks
Automatically notifies you when your license is about to expire

Getting Started with CSC SSM

Before CSC SSM can scan traffic and protect your network from malware, you must perform several configuration steps. These steps include obtaining one or two activation keys by using the Product Authorization Key (PAK) that you should have received with the CSC SSM.

For detailed configuration steps, including how to obtain activation keys, see the “Configuring the CSC SSM” chapter in the [Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide](#).

System Requirements

This section includes the following topics:

- [Hardware Requirements](#)
- [Client PC Operating System and Browser Requirements](#)

Hardware Requirements

There are two CSC SSM models: CSC SSM 10 and CSC SSM 20. The following adaptive security appliances support both CSC SSM models:

- ASA 5510
- ASA 5520
- ASA 5540



Note

CSC SSM licenses support up to 1000 users while the Cisco ASA 5540 Series appliance can support significantly more users. If you deploy CSC SSM with an ASA 5540 adaptive security appliance, be sure to configure the security appliance to send the CSC SSM only the traffic that should be scanned. For guidance with determining what traffic to scan, see the “Managing AIP SSM and CSC SSM” chapter in the [Cisco Security Appliance Command Line Configuration Guide](#).

Client PC Operating System and Browser Requirements

Client access to CSC is supported with ASDM; therefore, the supported and recommended PC operating systems and browsers for Version 6.0 are identical to those for ASDM Version 5.1 and later. For your convenience, the supported and recommended PC operating systems and browsers for ASDM Version 5.1 are shown in [Table 2](#).

Table 2 *Operating System and Browser Requirements*

	Operating System	Browser	Other Requirements
Windows ¹	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Sun Java ² Plug-in 1.4.2 or 1.5.0 Note HTTP 1.1 —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Netscape 7.1/7.2 with Sun Java Plug-in 1.4.2 or 1.5.0	SSL Encryption Settings —All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2	

1. ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

2. Get Sun Java from java.sun.com

Caveats

This section describes caveats for the 6.0 release.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml

To become a registered cisco.com user, go to the following website:

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

Open Caveats - Release 6.0

[Table 3](#) lists the open caveats for Version 6.0(1).

Table 3 Open Caveats

ID Number	Software Release 6.0(1)	
	Corrected	Caveat Title
CSCsd05974	No	TCP flow dropped due to CSC card failed during SSM stress
CSCsd17646	No	The CSC SSM cannot block non-standard file extensions such as .xxx.
CSCsd17656	No	The CSC SSM blocks the page with gzip displayed.
CSCsd17794	No	If FTP-Inspection is disabled in the ASA CLI the FTP-data is not scanned
CSCsd17818	No	Yahoo! Finance MarketTracker does not work.
CSCsd17889	No	Nothing seems to happen when downloading infected file from/to web mail
CSCsd17954	No	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011	No	FTP file blocking will not work when file unscanned due to cfg
CSCsd18030	No	Connections may be interrupted during SSM service failure
CSCsd18044	No	Connections may be interrupted during the SSM restarting period.
CSCsd18052	No	Email notification from the CSC SSM is not received.
CSCsd18060	No	with csc enabled, Large file transfer on HTTP/FTP or Windows Update fail

Related Documentation

For additional information, see the ASDM online Help or the following documentation found on Cisco.com:

- [Cisco Content Security and Control SSM Administrator Guide](#)
- [Cisco ASDM Release Notes](#)
- [Cisco ASA 5500 Series Hardware Installation Guide](#)
- [Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide](#)
- [Cisco ASA 5500 Series Release Notes](#)
- [Cisco Security Appliance Command Line Configuration Guide](#)
- [Cisco Security Appliance Command Reference](#)

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>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, Networkers, Networking Academy, Network Registrar, 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.