



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 and Submitting a Service Request, page 5](#)

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.



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.



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

© 2006 Cisco Systems, Inc. All rights reserved.

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
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

Table 1 *Features and Benefits (continued)*

Features
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.

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

<http://tools.cisco.com/Support/BugToolKit/>

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.

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

Table 3 Open Caveats (continued)

ID Number	Software Release 6.0(1)	
	Corrected	Caveat Title
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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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.