Cisco Content Security and Control Version 6.1 Release Notes

May 2006

Contents

This document contains release information for Content Security and Control (CSC) Version 6.1. It includes the following sections:

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.

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

- 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.

New Features in CSC Version 6.1

- **Network Reputation Service (NRS)**—(Was called IP filtering) a real-time blacklist and quick IP lookup technology for identifying spam that frees the MTA from processing the message header during evaluation.
- **Trend Micro Control Manager (TMCM) support**—enables deployment of uniform configurations across multiple installations of CSC SSM.
- **VSAP 8.0**—uses the new virus scan engine.
- **TMASE 3.5**—uses the new anti-spam engine.
- **Spyware Recognition**—enhanced spyware recognition.

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*.

If you are upgrading an activated installation, skip this section.

System Requirements

This section includes the following topics:

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 6.1 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 1.

Table 1 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.

Upgrading from Release 6.0

Install this upgrade only if you are running CSC SSM E/S v6.0 b1349; your existing configuration and registration information will not be changed.

This upgrade is cumulative and contains all the fixes released in previous any patches.

Update the pattern files and scan engine immediately after installing this patch. If this is your first installation of CSC SSM, please allow up to 60 minutes after receiving the Activation Code and activating the Name Reputation Services (NRS) for content filtering to begin.

To upgrade your CSC SSM, follow these steps:

Step 1 Download the csc6.1-b1519.pkg file from the Software Center on Cisco.com. You need to log into Cisco.com to download the software. If you do not have a Cisco.com account, visit the following website to become a registered user:

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

Step 2 Access the Trend Micro CSC SSM console:

a. Launch ASDM.

b. Choose **Configuration > Trend Micro Content Security**.

Step 3 Choose **Administrator > System Patch** from the menu.

Step 4 Click **Browse** and select the .pkg file you downloaded.

Step 5 Click **Install**.

The CSC SSM card automatically reboots after the installation. The reboot can take up to 5 minutes. During the reboot, the scanning services are unavailable. If the CSC SSM console appears to be unresponsive after 5 minutes, log off and then log back on.

Note The upgrade causes the System Patch screen to be renamed Product Upgrade.

Step 6 Click **Summary** to confirm the installed software version.

Step 7 (Optional) Use an Eicar test file to confirm that the upgrade was successful and that the scanning services are configured correctly.

Caveats

This section describes the open and resolved caveats for the CSC 6.1 release. To see more information about an open or resolved caveat, use the Bug Toolkit on Cisco.com. 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

This section contains the following topics:

Open Caveats

Table 2 lists the caveats that are open in Version 6.1.

Table 2 Open Caveats

ID Number	Caveat Title
CSCsd05974	TCP flow dropped due to CSC card failed during SSM stress.
CSCsd17656	The CSC SSM blocks the page with gzip displayed.
CSCsd17794	If FTP-Inspection is disabled in the ASA CLI the FTP-data is not scanned.
CSCsd17818	Yahoo! Finance MarketTracker does not work.
CSCsd17889	Nothing seems to happen when downloading infected file from/to web mail.
CSCsd17954	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011	FTP file blocking will not work when file unscanned due to cfg.
CSCsd18030	Connections may be interrupted during SSM service failure.
CSCsd18044	Connections may be interrupted during the SSM restarting period.
CSCsd18052	Email notification from the CSC SSM is not received.
CSCsd18060	with csc enabled, Large file transfer on HTTP/FTP or Windows Update fail.
CSCse12729	The spyware pattern number may appear to be rolled back.
CSCse12745	NRS feature is not be working on the CSC SSM after registration.
CSCse12755	Some spyware may be detected even if Spyware category is not enabled.
CSCse12767	Fails to convert non-UTF8 Japanese characters to UTF-8.
CSCse12772	Filename may not be properly displayed in the email inline insertion.
CSCse12781	Japanese strings may not be displayed correctly in syslog messages.
CSCse12784	Multi-bytes strings are not allowed on the GUI.
CSCse12786	Original email may break if not encoded in UTF-8.
CSCse12791	Multi-bytes filename may not be displayed correctly.

Closed Caveats

Table 3 lists the caveats that were resolved in Version 6.1.

Table 3 Closed Caveats

ID Number	Caveat Title
CSCsd17646	The CSC SSM cannot block non-standard file extensions such as .xxx.
CSCsd24556	The connection timeout syslog is sent on every SMTP connection.

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.