



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.2.1599.5

December 2008

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.2.1599.5 maintenance release. It includes the following sections:

- [About the CSC SSM Version 6.2.1599.5 Release, page 1](#)
- [Installing the CSC SSM Version 6.2.1599.5 Release, page 1](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)

About the CSC SSM Version 6.2.1599.5 Release

The CSC SSM Version 6.2.1599.5 maintenance release applies only to CSC-SSM-10 and CSC-SSM-20 Versions 6.2.1599.0 through 6.2.1599.4.

See the [“Resolved Caveats” section on page 5](#) for information about the caveats that have been resolved by this release.

Installing the CSC SSM Version 6.2.1599.5 Release

You can install this release if you are running CSC SSM Version 6.2.1599.0 through 6.2.1599.4. To verify the version of the CSC SSM software installed on the device, see the [“Verifying the Installed Version of the CSC SSM Software” section on page 2](#).



Americas Headquarters:

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

© 2008 Cisco Systems, Inc. All rights reserved.

To upgrade the CSC SSM, perform the following steps:

-
- Step 1** You must log into Cisco.com to download the software, which is available at the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
-  **Note** If you do not have a Cisco.com account, to become a registered user, visit the following website:
<http://tools.cisco.com/RPF/register/register.do>
-
- Step 2** Download the csc6.2.1599.5 .pkg upgrade file from the Software Center on Cisco.com.
- Step 3** Access the Trend Micro CSC SSM console by doing the following:
- Launch ASDM.
 - Choose **Configuration > Trend Micro Content Security**.
 - Click any link on the Trend Micro configuration pane to open the Trend Micro InterScan for Cisco CSC SSM interface.
- Step 4** Choose **Administrator > Product Upgrade** from the menu.
- Step 5** Click **Browse** and select the .pkg file you downloaded.
- Step 6** Click **Upload**.
- Step 7** Click **Summary** to confirm the installed software version.
- Step 8** (Optional) Download the Eicar “Anti-Malware Testfile” from <http://www.eicar.org> to confirm that the upgrade was successful and that the scanning services have been configured correctly. Check the upper right corner of the Home page.
-

For more information, see *Appendix A, “Reimaging and Configuring the CSC SSM Using the CLI,”* in the *Cisco Content Security and Control (CSC) SSM Administrator Guide*.

Verifying the Installed Version of the CSC SSM Software

The software version appears in the following locations:

- The summary pane of the Trend Micro InterScan for Cisco CSC SSM interface.
- Click the **Content Security** tab on the ASDM Home pane to open the CSC SSM Information screen.
- Through the ASA 5500 series adaptive security appliance CLI.

To confirm the version of software, and software components and patches that are installed on the CSC SSM using the CLI, perform the following steps:

-
- Step 1** Open ASDM.
- Step 2** Choose **Tools > Command Line Interface** to display the Command Line Interface dialog box.
- Step 3** In the command line field, enter the **show module 1 details** command, and then click **Send**.

The CSC SSM software version information appears.

```
show module 1 details
```

```

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:                ASA-SSM-20
Hardware version:     1.0
Serial Number:        0
Firmware version:     1.0(10)0
Software version:   CSC SSM 6.2.1599.5
MAC Address Range:    000b.fcf8.012c to 000b.fcf8.012c
App. name:            CSC SSM
App. Status:          Up
App. Status Desc:     CSC SSM scan services are available
App. version:         6.2.1599.5
Data plane Status:    Up
Status:               Up
HTTP Service:         Up
Mail Service:         Up
FTP Service:          Up
Activated:            Yes
Mgmt IP addr:         10.89.130.241
Mgmt web port:        8443
Peer IP addr:         <not enabled>

```

New Features

This section describes the new features for the CSC SSM Version 6.2.1599.5 maintenance release.

- You can import the configuration from different SSM models. Hardware-dependent configurations, such as serial numbers and the number of HTTP scanner processes, should remain unchanged.
- CSC detection logs are purged based on their event time.

Caveats

This section describes the open and resolved caveats for the CSC SSM Version 6.2.1599.5 maintenance release. To view more information about an open or resolved caveat, use the Bug Toolkit on Cisco.com. If you are a registered Cisco.com user, access the 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>

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences, because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling and typographical errors may be corrected.

This section includes the following topics:

- [Open Caveats, page 4](#)
- [Resolved Caveats, page 5](#)

Open Caveats

[Table 1](#) lists the open caveats in the CSC SSM Version 6.2.1599.5 maintenance release.

Table 1 *Open Caveats*

ID Number	Caveat Title
CSCsd17889	Nothing seems to happen when downloading infected file from/to web mail.
CSCsd18052	E-mail notification from the CSC SSM is not received.
CSCse12729	The spyware pattern number may appear to be rolled back.
CSCse12745	NRS feature is not working on the CSC SSM after registration. There may be a one-hour delay for the NRS database to be updated. This only affects new customers for the first hour after the license record has been created.
CSCsf98493	VPN users using proxy have problem browsing via HTTP.
CSCsf98538	WhiteIPList on NRS disappears from UI.
CSCsh27011	HP UX “tcp_lift_anchor, can't wait” error message when using FTP i.
CSCsh27102	Admin UI SSL vulnerability.
CSCsi27604	Intermittent e-mail corruption when going through CSC.
CSCsi40117	100% CPU issue.
CSCsi43395	Do not send disconnect-syslog when HTTP receives RST.
CSCsi65720	Secondary DNS server setup is wiped out by session 1 do setup dns command.
CSCsj10645	CSC still filters large size messages even if disabling POP3 scanning.
CSCsj91181	FTP service may stop under stress condition.
CSCsj91182	CSC cannot download pattern/engine from TMCM.
CSCsj91183	ConnectWise application does not load when scanned by CSC via HTTP.
CSCsk07553	Phishing websites only categorized without -www-.
CSCsk07581	Incorrect URL for submitting potential phishing URL to TrendLabs.
CSCsk08014	CSC locks-up and stays in reload state after upgrading to 6.2.1599.0.
CSCsk83986	Add additional skip content for new MIME type for www.unitedstreaming.
CSCsl11398	Add support for FTP APPEND command.
CSCsq37785	TMCM agent.ini file gets corrupted.
CSCsq56401	CSC may go unresponsive if the route cache reaches 262k.
CSCsr11684	RETR command blocked by CSC-SSM in FTP passive mode.
CSCsr75667	CSC-SSM does not handle Office 2007 files correctly.
CSCsr75669	CSC-SSM file blocking does not block Office 2007 files.
CSCsr95448	GUI timeout inconsistent.
CSCsu42556	Module in slot 1 experienced a data channel communication failure.

Table 1 **Open Caveats (continued)**

CSCsu68672	Feature request to support non-IP address for ERS-approved IP address.
CSCsv19800	HTTP access to results from images.google.com is blocked by URL filter.
CSCsv43913	POP3 anti-spam when spam mail is configured to be deleted.
CSCsv75448	CSC trims FQDN in URL requests.
CSCsv77805	No e-mail notification is sent for scheduled updates.
CSCsw27401	CSC memory used in ASDM is not reported correctly.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.2.1599.5 maintenance release.

Table 2 **Resolved Caveats**

ID Number	Caveat Title
CSCsk83985	Scan server may have a memory leak.
CSCsr66676	HTTP limits file downloads at 2GB.
CSCsr75670	Improve syslog messages to indicate where the syslog originated from, either the HTTP scanner or URL rating server.
CSCsu06743	HTTP file blocking notification GUI does not accept new line.
CSCsu39231	CSC blocks its own URL rating request when .txt files are configured to be blocked in HTTP and when ASA is not configured to skip CSC management traffic.
CSCsu55632	HTTP scanner seems to crash and cause “Page cannot be displayed” errors in browser.
CSCsv75448	CSC rewrites HTTP URI in proxy requests.

Related Documentation

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

- *Documentation Roadmap for the Cisco ASA 5500 Series*, at:
http://www.cisco.com/en/US/products/ps6120/products_documentation_roadmaps_list.html
- *Cisco Content Security and Control (CSC) SSM Administrator Guide*, at:
<http://www.cisco.com/en/US/docs/security/csc/csc62/administration/guide/csc62adm.html>
- *Cisco ASDM Release Notes*, at:
http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html
- *Cisco ASA 5500 Series Hardware Maintenance Guide*, at:
http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*, at:
http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html
- *Cisco ASA 5500 Series Release Notes*, at:
http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html

- *Cisco ASA 5500 Series Configuration Guide Using the CLI*, at:
http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- *Cisco Security Appliance Command Reference*, at:
http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html
- *Cisco Security Appliance System Log Messages*, at:
http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html
- *Open Source Software Licenses for ASA and PIX Security Appliances*, at:
http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

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.

For additional ASA 5500 Series Adaptive Security Appliance documentation, see the following URL and log in with your Cisco.com username and password:

http://www.cisco.com/en/US/partner/products/ps6120/tsd_products_support_series_home.html

This document is to be used in conjunction with the documents listed in the “Obtaining Documentation and Submitting a Service Request” section.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0807R)

© 2008 Cisco Systems, Inc.
All rights reserved.