



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.2.1599.4

September 2008

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.2.1599.4 maintenance release. It includes the following sections:

- [About the CSC SSM Version 6.2.1599.4 Release, page 1](#)
- [Installing the CSC SSM Version 6.2.1599.4 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 6.2.1599.4 Release

The CSC SSM Version 6.2.1599.4 maintenance release applies only to CSC-SSM-10 and CSC-SSM-20 Versions 6.2.1599.0 through 6.2.1599.3.

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 6.2.1599.4 Release

You can install this release if you are running CSC SSM Version 6.2.1599.0 through 6.2.1599.3. 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/cgi-bin/tablebuild.pl/csc>



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 csc6.2.1599.4 .pkg upgrade file from the Software Center on Cisco.com.
- Step 3** Access the Trend Micro CSC SSM console by doing the following:
- a. Launch ASDM.
 - b. Choose **Configuration > Trend Micro Content Security**.
 - c. 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) Use an Eicar test file to confirm that the upgrade was successful and that the scanning services have been configured correctly. Download the “Anti-Malware Testfile” from <http://www.eicar.org>.

For more information, see *Appendix A, “Reimaging and Configuring the CSC SSM Using the CLI,”* in the *Cisco Content Security and Control 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 6.2.1599.4
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:   6.2.1599.4
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 6.2.1599.4 maintenance release.

- You can configure Telnet or SSH access to the CSC SSM management port using the CLI menu.
- You can configure the e-mail disclaimer independently for incoming and outgoing SMTP policy.

Caveats

This section describes the open and resolved caveats for the CSC SSM Version 6.2.1599.4 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 6.2.1599.4 maintenance release.

Table 1 **Open Caveats**

ID Number	Caveat Title
CSCsd17889	Nothing seems to happen when downloading an infected file from or to Webmail.
CSCsd17954	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011	FTP file blocking will not work when a file is unscanned because of the configuration.
CSCsd18052	An e-mail notification from the CSC SSM is not received.
CSCse12729	The spyware pattern number may appear to be rolled back.
CSCse12745	The NRS feature does not work on the CSC SSM after registration.
CSCse12755	Some spyware may be detected even if the Spyware category is not enabled.
CSCse53604	ASDM does not detect the "FTP inspection not enabled" scenario.
CSCse68286	In MPF policy creation, clock setup should be alerted at end of CSC Setup Wizard.
CSCsf05298	Citrix is not supported with the CSC SSM.
CSCsf98493	VPN users using a proxy server have problems browsing via HTTP.
CSCsf98538	The WhiteIPList on NRS will disappear from UI.
CSCsh27011	When using HP UX tcp_lift_anchor, a "can't wait" error message occurs during FTP-i.
CSCsh27102	The admin UI has an SSL vulnerability.
CSCsi27604	Intermittent e-mail corruption occurs when messages go through the CSC SSM.
CSCsi40117	100% CPU usage issue occurred.
CSCsi43395	A disconnect-syslog is not sent when HTTP receives an RST.
CSCsi65720	A secondary DNS server setup is wiped out by the session 1 do setup dns command.
CSCsj10645	The CSC SSM still filters large size messages even if POP3 scanning is disabled.
CSCsj91181	FTP service may stop under stress conditions.
CSCsj91182	The CSC SSM cannot download a pattern file or engine from TMCM.
CSCsj91183	The ConnectWise application does not load when scanned by the CSC SSM via HTTP.
CSCsj91185	Webmail scanning displays an incorrect color when adding new entries.
CSCsk07553	Phishing websites are only categorized without -www-.
CSCsk07581	An incorrect URL was used to submit a potential phishing URL to TrendLabs.
CSCsk08014	The CSC SSM locks up and stays in Reload state after a Version 6.2.1599.0 upgrade.
CSCsk39837	Upgrading from CSC SSM Version 6.1.1519 to 6.2.1599 via the .pkg file might fail.
CSCsk83986	Need to add skip content for new MIME type for www.unitedstreaming.com.
CSCsk90093	Enhance online help for unscanned corrupted files.
CSCsl11398	Add support for the FTP APPEND command.
CSCsl54663	Slow e-mail delivery occurs from certain domains.
CSCsq37785	The TMCM agent.ini file gets corrupted.
CSCsq56401	Trend Micro CSC may become unresponsive if the route cache reaches 262 K.

Table 1 **Open Caveats (continued)**

CSCsr11684	The RETR command is blocked by the CSC SSM in FTP passive mode.
CSCsr56857	Clicking Configuration > Content Security hangs ASDM.
CSCsr66676	HTTP downloads incorrectly stop at 2GB when traffic is diverted to the CSC SSM.
CSCsr72553	Enhance the event logging purging behavior.
CSCsr75667	The CSC SSM does not handle Office 2007 files correctly.
CSCsr75669	CSC SSM file blocking does not block Office 2007 files.
CSCsr75670	Improve syslog messages to indicate where the syslog originated.
CSCsr95448	GUI timeout behavior is inconsistent.
CSCsu06743	HTTP file blocking administration notification GUI does not accept line entries.
CSCsu39231	File blocking of text files may cause the admin e-mail notification to continue.
CSCsu42556	Module in slot 1 experienced a data channel communication failure

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.2.1599.4 maintenance release.

Table 2 **Resolved Caveats**

ID Number	Caveat Title
CSCso67276	Failover cannot be paired up with certain shared keys.
CSCsr87910	Wrong keys are accepted to establish the failover relationship.
CSCsl44473	Syslog facility cannot be changed from local3 on the CSC SSM GUI.
CSCsh70101	No error message is displayed when importing an invalid URL.
CSCsl33414	Unable to import an e-mail address list if any of the e-mail addresses include a period.
CSCsl54989	Unable to delete POP3 spam e-mail messages.
CSCsq00778	Windows Update is slow.
CSCsr72552	The RegServer log is not purged correctly.
CSCsr75666	ActiveUpdate may incorrectly remove a pattern file if the remaining disk space on the flash card is insufficient.
CSCsk83984	The amount of free memory displayed by ASDM may be inaccurate.

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 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/docs/security/asa/asa72/hw/installation/guide/asach3.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 Security Appliance Command Line Configuration Guide*, 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 Guide*, 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, visit the following URL:

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.