



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.2.1599.6

April 2009

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.2.1599.6 maintenance release. It includes the following sections:

- [About the CSC SSM Version 6.2.1599.6 Release, page 1](#)
- [Installing the CSC SSM Version 6.2.1599.6 Release, page 2](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [New Features, page 3](#)
- [Important Notes, page 3](#)
- [Caveats, page 4](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)

About the CSC SSM Version 6.2.1599.6 Release

The CSC SSM Version 6.2.1599.6 maintenance release applies only to CSC-SSM-10 and CSC-SSM-20 Version 6.2.1599.5.

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



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

Installing the CSC SSM Version 6.2.1599.6 Release

You can install this release if you are running CSC SSM Version 6.2.1599.5. The upgrade will work if the CSC SSM is running Versions 6.2.1599.0 through 6.2.1599.5. 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](#).

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 csc6.2.1599.6 .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
- Through the ASA 5500 series adaptive security appliance CLI
- The CSC SSM Information screen. To access this screen, click the **Content Security** tab on the ASDM Home pane.

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 6.2.1599.6
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:         6.2.1599.6
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

No new features have been added for the CSC SSM Version 6.2.1599.6 maintenance release.

Important Notes



Warning

In the Device Failover Settings screen, the following warning message may appear:

Interscan for CSC SSM could not establish a connection. The software, hardware and patch version on the peer devices much match. Please reconcile the mismatch that was detected and try again.

In addition, the User license, Base license and Plus license must also match to resolve this issue.

Caveats

This section describes the open and resolved caveats for the CSC SSM Version 6.2.1599.6 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 6.2.1599.6 maintenance release.

Table 1 *Open Caveats*

ID Number	Caveat Title
CSCse53604	ASDM is not detecting FTP inspection not enabled scenario.
CSCsh27011	HP UX “tcp_lift_anchor, can't wait” error message appears when doing FTP -i.
CSCsh27102	Admin UI SSL vulnerability appears.
CSCsh40329	TEA CSC module with URL filtering delays or blocks all web traffic.
CSCsh98206	TEA CSC URL filtering, HTTP browsing fails: “page cannot be displayed” error appears.
CSCsh98210	TEA CSC-SSM not passing traffic for several minutes after configuration update.
CSCsi03872	TEA TFTP transfers to/from CSC module are failing.
CSCsi27604	Intermittent e-mail corruption when going through CSC.
CSCsi65720	Secondary DNS server setup is wiped out by session 1 do setup dns command.
CSCsj10645	CSC still filters large size messages even if POP3 scanning is disabled.
CSCsj91181	FTP service may stop under stress conditions.
CSCsj91182	CSC cannot download pattern/engine from TMCM.
CSCsj91183	ConnectWise application does not load when scanned by CSC via HTTP.
CSCsk08014	CSC locks up and stays in Reload state after upgrading to 6.2.1599.0.

Table 1 **Open Caveats (continued)**

CSCsk83986	Additional skip content for new MIME type added for www.unitedstreaming.com.
CSCsr11684	RETR command blocked by CSC-SSM in FTP passive mode.
CSCsr75667	CSC-SSM does not handle Office 2007 files properly.
CSCsr75669	CSC-SSM file blocking does not block Office 2007 files.
CSCsu42556	Module in slot 1 experienced a data channel communication failure.
CSCsu68672	Feature request to support non-IP addresses for ERS -approved IP address.
CSCsv43913	POP3 anti-spam when spam mail is configured to be deleted, Spam: is.
CSCsw27401	CSC used memory on ASDM is not reported correctly.
CSCsw65164	Cannot view videos on websites that are using JW FLV flash player 3.11.
CSCsx31671	CSC file extension blocking not working reliably.
CSCsx33934	HTTP & FTP blocking events on CSC-SSM not displayed in ASDM.
CSCsy29814	URL filtering exemptions cause 100% CPU usage on CSC 6.2.1599.5.
CSCsy85642	Websense restriction access page does not display.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.2.1599.6 maintenance release.

Table 2 **Resolved Caveats**

ID Number	Caveat Title
CSCsq56401	CSC may become unresponsive if the Route Cache reaches 262,000 entries.
CSCsv77805	No e-mail notification is sent to the admin when a scheduled update succeeds or fails.
CSCsx31671	HTTP File Blocking sometimes fail to block as configured.
CSCsx80745	Partial file may be downloaded if blocked by FTP File Blocking.
CSCsy46958	Unable to apply large patch package on CSC GUI.
CSCsy46953	Undeliverable notification e-mails may queue up and affect system operation.

Related Documentation

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

- *Navigating the Cisco ASA 5500 Series Documentation*, 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>
- *Release Notes for Cisco ASDM*, at:
http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html
- *Cisco ASA 5500 Series Hardware Installation 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
- *Release Notes for the Cisco ASA 5500 Series*, 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 ASA 5500 Series Command Reference*, at: http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html
- *Cisco ASA 5500 Series 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

For more information about the CSC SSM, see the following URL:

<http://www.cisco.com/en/US/products/ps6823/index.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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

© 2009 Cisco Systems, Inc.
All rights reserved.