



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.3.1172.1

September 2009

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.3.1172.1 release. It includes the following sections:

- [About the CSC SSM Version 6.3.1172.1 Release, page 1](#)
- [Installing the CSC SSM Version 6.3.1172.1 Release, page 2](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [New Features, page 3](#)
- [Caveats, page 3](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)

About the CSC SSM Version 6.3.1172.1 Release

The CSC SSM Version 6.3.1172.1 release applies only to CSC-SSM-10 and CSC-SSM-20.

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 6.3.1172.1 Release

If you are running the CSC SSM 6.3 release, your current license and configuration will be preserved during the upgrade.

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 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 csc6.3.1172.1 .pkg upgrade file from the Software Center on Cisco.com.

Step 3 Access the Trend Micro CSC SSM console by doing the following:

- a. Start 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 **Administration > Product Upgrade** from the menu.

Step 5 Click **Browse** and select the .pkg file that 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 B, “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 6.3.1172.1
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:         6.3.1172.1
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

Content filtering criteria for blocked e-mail messages have been added to web console log query results.

Caveats

This section describes the known issues and resolved caveats for the CSC SSM Version 6.3.1172.1 release. To view more information about a 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 6.3.1172.1 release.

Table 1 **Open Caveats**

ID Number	Caveat Title
CSCsh27011	[FTP] HP UX tcp_lift_anchor, can't wait error message when doing FTP i.
CSCsi27604	Intermittent e-mail corruption when going through CSC.
CSCsi65720	Secondary DNS server setup is wiped out by session 1 do setup dns command.
CSCsj91181	FTP service may stop under stress conditions.
CSCsj91183	ConnectWise application does not load when scanned by CSC via HTTP.
CSCsk83986	Add additional skip content for new MIME type for www.unitedstreaming.com.
CSCsr11684	RETR command blocked by CSC-SSM in FTP passive mode.
CSCsw27401	CSC used memory on ASDM is not reported correctly.
CSCsw65164	Can't view videos on websites that are using JW FLV flash player 3.11.
CSCsz23069	Memory leak in the java process (tomcat).
CSCta22307	HTTP/FTP services do not start after importing configuration 10 times.
CSCta99320	Upgrade to CSC 6.3.1172.pkg may fail.
CSCtb23415	HTTP traffic freeze with AD integration enabled.
CSCtb39347	CSC: LDAP user ID based policy may not work as expected.
CSCtb64854	CSC high CPU IWSS performance degraded.
CSCtb66038	Inserting strange string into e-mail subject through CSC-SSM.
CSCtb66040	HTTP file blocking - Some SWF and CSS files are blocked as executable.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.3.1172.1 release.

Table 2 **Resolved Caveats**

ID Number	Caveat Title
CSCsr20290	Add more detail to logs that indicate e-mail dropped due to content.
CSCta22816	Web UI login cannot recognize plus character in a password.
CSCta32382	Mail scanner does not abort on client socket timeout.
CSCta58382	HTTP Service fails if HTTP logging is enabled at the debugging level.
CSCtb19528	CSC-SSM user group policy does not handle apostrophes correctly.
CSCtb45797	After upgrading from 6.2 to 6.3, the TCM agent version was showing version 3.5.
CSCtb45798	After upgrading from 6.2 to 6.3, TCM GUI shows the wrong versions of pattern updates.
CSCtb53210	The exported CSV file for URL Filtering/Blocking or FTP File Blocking does not contain the source and destination IP addresses.
CSCtb53149	The User ID field is left blank when some global policies have been applied and the URL Filtering/Blocking logs have been generated.

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/products/ps6823/tsd_products_support_model_home.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 URLs:

- <http://www.cisco.com/en/US/products/ps6823/index.html>
- <http://www.cisco.com/go/cscssm>

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 using 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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

© 2009 Cisco Systems, Inc.
All rights reserved.