Cisco Content Security and Control (CSC) SSM Release Notes Version 6.3.1172.4

December 2010

Contents

This document provides release information for the Cisco Content Security and Control (CSC) SSM Version 6.3.1172.4 release and includes the following sections:

About the CSC SSM Version 6.3.1172.4 Release

The CSC SSM Version 6.3.1172.4 release applies only to CSC-SSM-10 and CSC-SSM-20. To install this version, you must have CSC Versions 6.3.1172.0 to 6.3.1172.3 installed.

Caution After this update is installed, the CSC SSM reboots. In addition, you cannot uninstall it; rollback is not supported.

Note Make sure that you manually download and reinstall the Domain Controller agent on your Windows machines if you are using ID-based HTTP user group policies.

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

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 6.3.1172.4 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 csc6.3.1172.4.pkg upgrade file from the Software Center on Cisco.com.

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

a. 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 have 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 in 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 6.3.1172.4
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:       6.3.1172.4
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Mail Service:       Up
FTP Service:       Up
Activated:          Yes
Mgmt IP addr:       10.89.130.341
Mgmt web port:      8443
Peer IP addr:       <not enabled>
```

New Features

The following new features have been added in the CSC 6.3.1172.4 release:

- The Domain Controller Agent debugging log has been improved to record time costs for all tasks. For example, you can record time costs for the following:
  - When a cache check starts
  - The results of a cache check (hit or miss)
  - If missed, to query the agent (for the timestamp)
  - The response received from the agent
- The debugging log levels for the Domain Controller Agent have changed from the following:
  - 0—off
  - 1—on

  to the following:

  - 0—off
  - 1—critical
  - 2— error
  - 3—warning
  - 4—info
  - 5—debug
- The Domain Controller Agent supports different levels of logging. If users want to obtain the most detailed debugging log, they must reset [HKLM\Software\TrendMicro\IdAgent\DebugLevel] to 5 from the default value of 1.

Important Notes

For open caveat CSCtj52109, note the following:

The CSC SSM detected a violation that could not be shown from the ASDM Live Security Events pane. To work around this issue, from the CSC SSM Administration Web Console, choose **Logs > Query > Log Query** to retrieve the violation log immediately.

For new product registration on the Cisco website, there may be a delay of up to one hour for the NRS database to be updated. During this time, the NRS feature will not work on the CSC SSM version 6.1, build 1219.

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

Warning **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 known issues and resolved caveats for the CSC SSM Version 6.3.1172.4 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

Table 1 lists the open caveats in the CSC SSM Version 6.3.1172.4 release.

Table 1 Open Caveats

ID Number	Caveat Title
CSCsr11684	RETR command blocked by CSC-SSM in FTP passive mode.
CSCsw27401	CSC used memory in ASDM is not reported correctly.
CSCsz23069	Memory leak in the java process (tomcat).
CSCtb23415	HTTP traffic freeze with AD integration enabled.
CSCtd43464	URL filtering fails in CSC 6.3.1172.0 - HTTP service cycles in loop.
CSCtf99255	CSC: AD integration does not allow for underscore in domain user ID.
CSCtg01139	CSC: Failover configuration requirement needs to be more specific.
CSCtg01153	CSC- Doc: Failover configuration requirement needs to be more specific.
CSCtg06921	CSC: catalina.out file may grow large enough to stop pattern updates.
CSCtg57748	CSC: SysMonitor frequently restarts and goes into a loop.
CSCth28700	CSC debuglog error for -1.
CSCth65504	CSC: URL blocking form subject to SQL injection.
CSCth68299	CSC: import of 6.2.1599.x cfg with bad character into 6.3.1172.x breaks WRS.
CSCti05907	CSC: Block e-mail with attachments despite GUI setting not to block.
CSCti23136	Trend Micro ID agent leaks nonpaged kernel memory on host machine.
CSCtj25731	CSC: Unnecessary clm_debug.log messages generated cause low free memory.
CSCtj35950	Trend Micro CSC crashes unexpectedly.
CSCtj41993	CSC: Unable to copy new grayware patterns during update.
CSCtj52109	Failed to display CSC security events in content security monitoring. See the "Important Notes" section on page 4.
CSCtj64849	CSC - ID agent crash due to heap memory allocation.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.3.1172.4 release.

Table 2 Resolved Caveats

ID Number	Caveat Title
CSCtb66038	Inserting strange string into Email subject through CSC-SSM.

Table 2 Resolved Caveats (continued)

CSCtf79702	There is no efficient way to troubleshoot the AD integration delay issue from both the CSC and ID Agent perspectives. See the "New Features" section on page 3.
CSCtf99255	CSC does not allow the user domain ID to contain an underscore character.
CSCtg50912 CSCtg50926	CSC services encounter an infinite loop when reloading.
CSCtg57748	The importing of approved or blocked lists would fail without warning or error reporting if the e-mail address contains special characters, such as # ' =- or & (and others).
CSCth28700	CSC will display a very large number for ContentLength when the actual value is -1.
CSCth65504	By submitting a specially crafted URL into the Match section of the Web (HTTP) > URL Blocking > URLs to Block page, hackers can have the webserver make undesirable changes to the SQL table structure that defines the policy of the CSC module.
CSCth68299	When importing an old configuration into the CSC module, it tries to convert the old configuration into the new SQLite DB format. If there is an invalid character in the file (e.g., a single quote), the import would fail.
CSCti05907	E-mail with attachments would be blocked despite a GUI setting of no blocking.
CSCti23136	The Domain Controller Agent leaks non-paged kernel memory on the host machine.

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

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

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.