



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.3.1172.3

June 2010

Contents

This document provides release information for the Cisco Content Security and Control (CSC) SSM Version 6.3.1172.3 release and includes the following sections:

- [About the CSC SSM Version 6.3.1172.3 Release, page 1](#)
- [Installing the CSC SSM Version 6.3.1172.3 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 6.3.1172.3 Release

The CSC SSM Version 6.3.1172.3 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 6.3.1172.2 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 4 for information about the caveats that have been resolved by this release.

Installing the CSC SSM Version 6.3.1172.3 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 csc6.3.1172.3.pkg upgrade file from the Software Center on Cisco.com.
- Step 3** Access the Trend Micro CSC SSM console by doing the following:
- Start 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 **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 6.3.1172.3
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:         6.3.1172.3
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

A new configuration item, ActiveQuery, has been added to the IdAgent.ini file. This setting allows the client workstation to be queried directly when the log parsing approach does not work. If the ActiveQuery configuration entry is set to 1, the Domain Controller Agent performs a remote registry query to the client workstation directly for the logged-in user. The default value of ActiveQuery is zero, and behaves the same way as in previous versions.

Caveats

This section describes the known issues and resolved caveats for the CSC SSM Version 6.3.1172.3 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 4](#)

Open Caveats

[Table 1](#) lists the open caveats in the CSC SSM Version 6.3.1172.3 release.

Table 1 *Open Caveats*

ID Number	Caveat Title
CSCsr11684	RETR command blocked by CSC SSM in FTP passive mode.
CSCsw27401	CSC used memory on ASDM is not reported correctly.
CSCsz23069	Memory leak exists in the Java process (tomcat).
CSCtb23415	HTTP traffic freeze occurs with AD integration enabled.
CSCtb66038	Inserting a strange string into an e-mail subject gets garbled through CSC-SSM.
CSCtd43464	URL filtering fails in CSC 6.3.1172.0 - HTTP service cycles go into 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: The catalina.out file may grow large enough to stop pattern updates.
CSCtg57748	CSC: CSC SSM application status frequently restarts and goes into a loop.

Resolved Caveats

[Table 2](#) lists the resolved caveats in the CSC SSM Version 6.3.1172.3 release.

Table 2 *Resolved Caveats*

ID Number	Caveat Title
CSCtb39347	Sometimes the Domain Controller agent cannot find the username or group by IP address.

Table 2 **Resolved Caveats (continued)**

CSCtd78933	The approved sender list scrolls whenever a change is made.
CSCte88539	When the HTTP server closes a connection, CSC returns an HTTP 502 error.
CSCtf17147	The javascript, vbscript, and .jar files are regarded as DOS COM when file blocking is enabled.
CSCtf23288	The LDAP group matching fails if a pre-2000 login name has uppercase characters.
CSCtf25175	HTTP requests are slow to respond with URL filtering enabled.
CSCtf31588	Need to cache the Domain Controller agent not found results to improve performance.
CSCtf33257	If the Domain Controller agent is disabled and then enabled again, CSC still connects to the old Domain Controller agent.
CSCtf39969	CSC: ID Agent does not correctly read the Active Directory Primary Group.
CSCtf40408	Users may not be detected on a PC with multiple IP addresses.
CSCtf66064	CSC: ID Agent delays response to CSC queries, causing significant browsing delays.
CSCth04355	The Active Directory agent is unable to query usernames from the Domain Controller.

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

© 2010 Cisco Systems, Inc.
All rights reserved.