Release Notes for Cisco Content Security and Control (CSC) SSM Version 6.6.1125.0

Updated August 2012

Contents

This document provides release information for the Cisco Content Security and Control (CSC) SSM Version 6.6.1125.0 release and includes the following sections:

About the CSC SSM Version 6.6.1125.0 Release

The CSC SSM Version 6.6.1125.0 release applies only to CSC-SSM-10 and CSC-SSM-20. The upgrade installation of CSC SSM 6.6 is only applicable for CSC 6.3.1172.4 using the .pkg file.

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

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

Note Make sure that you manually download and reinstall the Domain Controller Agent on your Windows machines if you are using user/group policies.

See the "Resolved Caveats" section on page 6 for information about the caveats that have been resolved by this release.

Installing the CSC SSM Version 6.6.1125.0 Release

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

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 3.

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/pub/software/portal/select.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 csc6.6.1125.0 .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. To open the Trend Micro InterScan for Cisco CSC SSM interface, click any link except **CSC Setup**, which takes you to the CSC Setup Wizard on the Trend Micro configuration pane.

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 pane.

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 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, then click **Send**.

The CSC SSM software version information appears:

```
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 6.6.1125.0
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:        6.6.1125.0
Data plane Status:   Up
Status:              Up
HTTP Service:        Up
HTTPS 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 6.6.1125.0 release:

- HTTPS Filtering
  - Able to allow or block HTTPS traffic.
  - Supports group-based and user-based HTTPS policies.
  - Includes URL blocking/URL exception list support for HTTPS domains.
- License Renewal Assistant
  - Prominently displays the license status in the dashboard.

  - Proactively notifies the customer about the renewal date (60 days, 30 days, and 1 day in advance, then 14 days after).
  - Provides customers with step-by-step instructions about how to renew licenses, including all necessary information.
- Enhanced File Type Filtering—Identifies and blocks executable files, even those included within compressed files.
- SMTP Content Filtering Global Whitelist
  - Able to define an approved sender that bypasses any SMTP processing.
  - Defines the sender with an exact e-mail address or domain name.
- POP3 Content Filtering Global Whitelist
  - Able to define an approved sender that bypasses any POP3 processing.
  - Defines the sender with an exact e-mail address or domain name.
- IP/User Cache Information Dump—Dumps the IP/user and IP/group mapping information from the cache when a user enables LDAP integration.
- Domain Controller Agent Enhancements
  - Distinguishes machine logon events from other user logon events.
  - Adjusts the remote validation time interval from a central point.
  - Disables the IP user cache purge on the CSC side.
  - Supports Health Monitor and multiple Domain Controller Agents.
  - Improves Domain Controller Agent performance.
  - Shows the IP address of “Not Found” users.
  - Enlarges the debugging log size of the Domain Controller Agent.
  - Enabled “Not Found” IP user cache on the CSC side by default.

This section includes the following topics:

- Software Requirements, page 4
- Known Issues, page 5

Software Requirements

The following lists the CSC versions and the supported ASA and ASDM versions:

- 6.0—End of Sale status
- 6.1 GM—ASA 7.1(2) and ASDM 5.1.4(7)
- 6.2 GM—ASA 7.2(1) and ASDM 5.2(3) and later
- 6.3 GM—ASA 7.2(1), 8.0(2), 8.2(1) and later and ASDM 5.2(1), 6.0(2), 6.2(1) and later
- 6.6 GM—ASA 8.4(2) and ASDM 6.4(2) are required. Earlier versions of ASA and ASDM are not supported on CSC SSM 6.6.

Known Issues

The following table provides a list of known issues and the available workarounds.

Description	Workaround
The Domain Controller Agent has a mechanism to regularly query the remote client registry to validate if the user in cache is still logged into the client machine. The default interval is 140 seconds. However, if the user adds the ShowRun value to the registry of the machine on which the Domain Controller Agent is installed for debugging and troubleshooting, the Domain Controller Agent will try to query the client machine registry within a very short interval.	Modify the ShowRun value to 140 seconds, if necessary.
The DBCS or SBCS account is not supported during configuration of the administrator account in the User Identification Settings pane.	None.
The ID Agent depends on the remote registry to validate remote user information. With some operating systems, for example, Windows 7 and Windows 2008, the remote registry is disabled by default. When the initial ID Agent cache TTL expires, the Domain Controller Agent can no longer identify the user.	Enable the remote registry in all remote machines within the domain. At the same time, modify the firewall rules to allow remote registry access.
File blocking cannot take action on files with the .jar extension.	None.
PowerPoint 2007/2010 was blocked when file blocking for compressed files was enabled and the image file type was selected.	None.

Important Notes

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.

When you change the DNS server using the CSC GUI, the change does not take effect for the Check License Status feature. The workaround is to restart the CSC GUI by entering the following:

```
/opt/trend/isvw/script/ISui restart
```

Caveats

This section describes the known issues and resolved caveats for the CSC SSM Version 6.6.1125.0 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 6
- Resolved Caveats, page 6

Open Caveats

Table 1 lists the open caveats in the CSC SSM Version 6.6.1125.0 release.

Table 1 Open Caveats

ID Number	Caveat Title
CSCtg01139	CSC: Failover configuration requirement needs to be more specific.
CSCtg01153	CSC - DOC: Failover configuration requirement needs to be more specific.
CSCtj35950	Trend Micro CSC crashes unexpectedly.
CSCtj64849	CSC - ID agent crash due to heap memory allocation.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.6.1125.0 release.

Table 2 Resolved Caveats

ID Number	Caveat Title
CSCsh18404	URL filtering function now supports HTTPS.
CSCsi85915	Add white list option for e-mail senders in SMTP/POP3 scanning.
CSCsr20264	Add whitelist option for SMTP content filtering.
CSCsu65006	Need ability to look in the zip file and block only the executable file.
CSCtc41594	Blocking counters to 0 in XML output to ASDM.
CSCtd43464	URL filtering fails CSC 6.3.1172.0 - HTTP Service cycles in loop.
CSCtf23334	No easy way to check the LDAP User > IP and Group > User information.
CSCtf99255	CSC: AD integration does not allow for underscore in domain User ID.
CSCtg06921	CSC: catalina.out file may grow large enough to stop pattern updates.
CSCtg57748	CSC: SysMonitor frequently restarts and goes in a loop.
CSCth28700	CSC Debugging log error for -1.

Table 2 Resolved Caveats (continued)

CSCth65504	CSC: URL blocking form subject to SQL injection.
CSCth65504	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 non-paged kernel memory on host machine.
CSCtj25731	CSC: Unnecessary clm_debug.log messages generated cause low free memory.
CSCtj41993	CSC: Unable to copy new grayware patterns during update.
CSCtj52109	Failed to display CSC security events in content security monitoring.
CSCtl09551	CSC: Period not allowed in domain name for DC credentials in 6.3.1172.4
CSCtl18405	CSC e-mail body becomes attachment when using ellipses in disclaimer.
CSCtl21337	Unable to change administrator e-mail address after applying maintenance release 6.3.1172.4.
CSCtl21378	LogServer process crashes on CSC Module.
CSCtn00051	CSC: User ID-based policy may not work. IDAgent debugs may show normal.
CSCto04050	Virus file using HTTP fails to send first time after CSC card reset.
CSCtq46443	Unable to download file when deferred scanning is enabled.

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 URL:

http://www.cisco.com/en/US/products/ps6823/index.html

For additional ASA documentation, see the following URL:

http://www.cisco.com/en/US/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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.