Cisco Content Security and Control (CSC) SSM Release Notes Version 6.3.1172.0

June 2009

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.3.1172.0 release. It includes the following sections:

About the CSC SSM Version 6.3.1172.0 Release

The CSC SSM Version 6.3.1172.0 release applies only to CSC-SSM-10 and CSC-SSM-20.

See the "Resolved Caveats" section on page 8 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

Before Installing CSC SSM Version 6.3.1172.0

If you are running CSC SSM Version 6.3.1146.0, perform the following steps:

Step 1 Reimage the CSC with Version 6.3.1172.0; no GUI migration path is available from CSC 6.3. Alternatively, export a configuration backup from a previous 6.3 release, then reimport the updated 6.3 release.

Step 2 Download the csc6.3.1172.0.bin file from the Software Center on Cisco.com.

Step 3 Download the csc6.3.1172.0.bin file to your TFTP server.

Note The TFTP server must support files sizes greater than 60 MB. The .bin files are full binary images that are to be uploaded via a TFTP server. Do not upload .bin files using the CSC Admin Console.

Step 4 Using a terminal application such as Windows HyperTerminal, log on and open a terminal session to the adaptive security appliance console. Then enter the following two commands:

a. `hostname# hw module 1 recover config`

The system response is similar to the following example:

```
Image URL tftp://insidehost/csc6.3.1172.x.bin]:tftp://insidehost/csc6.3.1172.x.bin
Port IP Address [000.000.0.00]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
```

b. `hostname# hw module 1 recover boot`

```
The module in slot 1 will be recovered. This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Step 5 Enter **y** to confirm.

```
Recover issued for module in slot 1
```

Note The recovery process takes at least 10 minutes to finish.

Step 6 To verify that the recovery was successful, enter the following command:

```
hostname# show module 1 details
```

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 6.3.1172.0
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:       6.3.1172.0
```

```
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>
```

Step 7 In a web browser, access ASDM for the adaptive security appliance in which the CSC SSM is installed.

Step 8 In ASDM, verify time settings on the adaptive security appliance. Time setting accuracy is important for logging of security events and for automatic updates of the CSC SSM software.

- If you manually control time settings, verify the clock settings, including the time zone. Choose **Configuration > Device Setup > System Time > Clock**.
- If you are using NTP, verify the NTP configuration. Choose **Configuration > Device Setup > System Time > NTP**.

Step 9 In the ASDM home pane, click the **Content Security** tab.

Step 10 In the Connecting to CSC dialog box, click one of the following radio buttons:

- To connect to the IP address of the management port on the SSM, click **Management IP Address**. ASDM automatically detects the IP address for the SSM in the adaptive security appliance. If this detection fails, you can specify the management IP address manually.
- To connect to an alternate IP address or hostname on the SSM, click **Other IP Address or Hostname**.

Step 11 Enter the port number in the Port field, and then click **Continue**.

Step 12 In the CSC Password dialog box, type your CSC password, and then click **OK**.

Step 13 To complete the configuration, run the CSC Setup Wizard. To access the CSC Setup Wizard, choose **Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup > Launch Setup Wizard**.

The CSC Setup Wizard appears. For assistance with the CSC Setup Wizard, click the **Help** button.

Step 14 Configure service policies to divert the traffic that you want scanned to the CSC SSM. To create a global service policy that diverts traffic for scanning, perform the following steps:

a. Choose **Configuration > Firewall > Service Policy Rules**, and then click **Add**.

The Add Service Policy Rule Wizard screen appears.

b. Click the **Global - applies to all interfaces** option, and then click **Next**.

The Traffic Classification Criteria screen appears.

c. Click the **Create a new traffic class** option, type a name for the traffic class in the adjacent field, check the **Any traffic** check box, and then click **Next**.

The Rule Actions screen appears.

d. Click the **CSC Scan** tab, and then check the **Enable CSC scan for this traffic flow** check box.

e. Choose whether the adaptive security appliance should permit or deny selected traffic to pass if the CSC SSM is unavailable by making the applicable selection in the area labeled: **If CSC card fails, then**.

f. Click **Finish**.

The new service policy appears in the Service Policy Rules pane.

g. Click **Apply**.

The adaptive security appliance begins diverting traffic to the CSC SSM.

Step 15 Uninstall the Domain Controller Agent from the CSC SSM 6.3.1146.0 release package, then install the Domain Controller Agent from the CSC SSM 6.3.1172.0 release package.

Note If the DC Server is running on Windows 2008, you must install the Domain Controller Agent on one of the Windows 2008 machines.

Installing the CSC SSM Version 6.3.1172.0 Release

If you are running the CSC SSM 6.2 release, you must upgrade to CSC Version 6.2.1599.6 before you can install the GUI upgrade package, csc6.3.1172.0.pkg. 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 5.

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 csc6.3.1172.0 .pkg upgrade file from the Software Center on Cisco.com.

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

a. Launch 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 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 6.3.1172.0
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:       6.3.1172.0
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

This section describes the new features for the CSC SSM Version 6.3.1172.0 release.

- Support has been added for AD and LDAP integration with the Windows Domain Controller for policy control of URL filtering and URL blocking for users and groups.
- HTTP processing capacity on active concurrent connections has been doubled.

- Web Reputation technology has been added to protect customers from malicious web threats. This feature requires the Plus License.
- Trend Micro Control Manager 5.0 has been integrated with the CSC SSM to provide ad-hoc queries for user and group reporting.
- CSC syslog format is consistent with the adaptive security appliance syslog format. The source and destination IP information has been added to the ASDM Log Viewer GUI. Syslog message explanations have been added to the *Cisco Content Security and Control (CSC) SSM Administrator Guide*. All syslog messages include predefined syslog priorities and cannot be configured through the GUI.
- The compressed file count limitation in all scan settings has been changed from 400 files to 1000 files to allow CSC to better handle Microsoft Office 2007 files.

Important Notes

ASDM does not display Web Reputation, User Group Policies, or User ID Settings in the Plus License listing on the main page.

When you choose **Configuration > Web**, the Web Reputation link is not available. In addition, URL filtering has two links: one for filtering rules and one for filtering settings; however, both links point to the CSC URL filtering global setting.

CSC 6.3 security event enhancements are not included, such as the new Web Reputation events and user and group identifications.

Also, to access the new features, you must go directly to the CSC UI:

- Web Reputation: Choose **CSC UI > Web (HTTP) > Web Reputation**.
- User Group Policies: Choose **CSC UI > Web (HTTP)> User Group Policies > URL Blocking & Filtering**.
- User ID Settings: Choose **CSC UI > Administration > Device Settings > User ID Settings**.

Caveats

This section describes the known issues and resolved caveats for the CSC SSM Version 6.3.1172.0 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

Table 1 lists the open caveats in the CSC SSM Version 6.3.1172.0 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 occurs when doing FTP i.
CSCsi27604	Intermittent e-mail corruption occurs 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 skipped content for new MIME type for www.unitedstreaming.com.
CSCsr11684	RETR command blocked by CSC-SSM in FTP passive mode.
CSCsu68672	Feature request to support non-IP addresses for ERS-approved IP addresses.
CSCsw27401	CSC memory used 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 is not working reliably.
CSCsy85642	Websense restriction access page does not display.
CSCsz23069	Memory leak exists in the Java process (tomcat).
CSCsz42408	CSC e-mail reputation service typo.

Resolved Caveats

Table 2 lists the resolved caveats in the CSC SSM Version 6.3.1172.0 release.

Table 2 Resolved Caveats

ID Number	Caveat Title
CSCsh27102	CSC GUI allowed clear text to be negotiated as SSL transport cipher.
CSCsj10645	CSC still filters large size messages even if POP3 scanning is disabled.
CSCsj71797	CSC GUI allowed bypass of large e-mails for SMTP/POP3.
CSCsj91182	Was unable to update the virus pattern from the TMCM server.
CSCsk07553	Phishing websites were only categorized without “www.”
CSCsk07581	URL for category reclassification needed to be updated on CSC GUI.
CSCsk08014	CSC locks up and stays in Reload state after upgrading to 6.2.1599.0.
CSCsk17966	Have the option to configure the GUI timeout value.
CSCsk27052	CSC GUI should check the file type for the Product Upgrade upload.
CSCsk39786	Have URL filtering based on the source address.
CSCsk39837	The upgrade process from 6.1.1519 to 6.2.1599 failed sometimes.
CSCsk90093	Enhanced the GUI online help topic about HTTP scanning for unscanned actions and the large file handling feature.
CSCsq56401	CSC could become unresponsive if the route cache reached 262,000 entries.
CSCsr75667	CSC did not scan Office 2007 files correctly.
CSCsr75669	CSC did not block Office 2007 files correctly.
CSCsr95448	CSC GUI timeout was inconsistent.
CSCsu41769	Allow the configuring of URL blocking and filtering based on the client identity.
CSCsu42556	CSC could encounter kernel panic when collecting a data plane capture from the CSC CLI menu.
CSCsv19800	URL filtering exception did not work on search results from http://images.google.com.
CSCsv43913	The “SPAM:” tag was not added to the e-mail subject line when spam e-mail was configured to be deleted.
CSCsw47365	DNS settings that were changed in the CSC Web GUI did not take effect.
CSCsy29814	URL filtering exception caused 100% CPU usage in CSC 6.2.1599.5.
CSCsy32827	Priority order was incorrect after updating the user and group policy.
CSCsy32840	Global URL blocking policy did not work when all user and group policies were deselected.
CSCsz08742	CSC could block the autoupdate function for Adobe products.
CSCsz08744	CSC identified the proxy agent as “IWSS” in the 503 Service Unavailable error message.
CSCsz68344	CSC URL blocking and filtering policies become read-only.

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 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.