



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.2.1599.3

June 2008

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.2.1599.3 maintenance release. It includes the following sections:

- [About the CSC SSM Version 6.2.1599.3 Release, page 1](#)
- [Installing the CSC SSM Version 6.2.1599.3 Release, page 1](#)
- [Verifying the Installed Version of the CSC SSM Software, page 2](#)
- [Caveats, page 3](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 6](#)

About the CSC SSM Version 6.2.1599.3 Release

The CSC SSM Version 6.2.1599.2 maintenance release applies only to CSC-SSM-10 and CSC-SSM-20 Versions 6.2.1599.0, 6.2.1599.1, and 6.2.1599.2.

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 6.2.1599.3 Release

You can install this release if you are running CSC SSM Version 6.2.1599.0, 6.2.1599.1, or 6.2.1599.2. 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](#).



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

© 2008 Cisco Systems, Inc. All rights reserved.

To upgrade the CSC SSM, perform the following steps:

-
- Step 1** Download the csc6.2.1599.3 .pkg upgrade file from the Software Center on Cisco.com. You need to log into Cisco.com to download the software. If you do not have a Cisco.com account, visit the following website to become a registered user:
- <http://tools.cisco.com/RPF/register/register.do>
- Step 2** Access the Trend Micro CSC SSM console by doing the following:
- Launch ASDM.
 - Choose **Configuration > Trend Micro Content Security**.
 - Click any link on the Trend Micro configuration page to open the Trend Micro InterScan for Cisco CSC SSM interface.
- Step 3** Choose **Administrator > Product Upgrade** from the menu.
- Step 4** Click **Browse** and select the .pkg file you downloaded.
- Step 5** Click **Upload**.
- Step 6** Click **Summary** to confirm the installed software version.
- Step 7** (Optional) Use an Eicar test file to confirm that the upgrade was successful and that the scanning services have been configured correctly. Download the “Anti-Malware Testfile” from <http://www.eicar.org>.
-

For more information, see *Appendix A, “Reimaging and Configuring the CSC SSM Using the CLI,”* in the *Cisco Content Security and Control SSM Administrator Guide*.

Verifying the Installed Version of the CSC SSM Software

The software version appears in the following locations:

- The summary page of the Trend Micro InterScan for Cisco CSC SSM interface.
- Click the **Content Security** tab on the ASDM Home page to open the CSC SSM Information screen.
- Through the ASA 5500 series adaptive security appliance CLI.

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 6.2.1599.3
```

```

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:     6.2.1599.3
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 6.2.1599.3 maintenance release.

- To aid in troubleshooting, CSC log collection records engineering builds that have been installed as part of the revision history.
- You may configure the free memory monitoring threshold. The default value is 20 MB.

Caveats

This section describes the open and resolved caveats for the CSC SSM Version 6.2.1599.3 maintenance release. To view more information about an open or 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 6.2.1599.3 maintenance release.

Table 1 **Open Caveats**

ID Number	Caveat Title
CSCsd17889	Nothing seems to happen when downloading infected file from/to webmail.
CSCsd17954	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011	FTP file blocking will not work when file unscanned due to cfg.
CSCsd18052	E-mail notification from the CSC SSM is not received.
CSCse12729	The spyware pattern number may appear to be rolled back.
CSCse12745	NRS feature is not working on the CSC SSM after registration.
CSCse12755	Some spyware may be detected even if Spyware category is not enabled.
CSCsf05298	Citrix not supported with CSC module.
CSCsf98493	VPN users using proxy have problem browsing via HTTP.
CSCsf98538	White IP List on NRS will disappear from UI.
CSCsh27011	HP UX tcp_lift_anchor, can't wait error message when doing FTP i.
CSCsh27102	Admin UI SSL vulnerability.
CSCsh70101	No error message for invalid URL blocking import file.
CSCsi27604	Intermittent e-mail corruption when going through CSC.
CSCsi40117	100% CPU issue.
CSCsi43395	Do not send disconnect-syslog when HTTP receives RST.
CSCsi65720	Secondary DNS server setup is wiped out by session 1 do setup dns command.
CSCsj10645	CSC still filters large size messages even if disabling POP3 scanning.
CSCsj91181	FTP service may stop under stress condition.
CSCsj91182	CSC cannot download pattern/engine from TMCM.
CSCsj91183	ConnectWise application does not load when scanned by CSC via HTTP.
CSCsj91185	Webmail scanning displays incorrect color when adding new entries.
CSCsk07553	CSC: Phishing websites only categorized without www.
CSCsk07581	CSC: Incorrect URL for submit potential phishing URL to TrendLabs.
CSCsk08014	CSC locks up and stays in Reload state after upgrading to 6.2.1599.0.
CSCsk09801	CSC-SSM Enhancement: block SMTP e-mail with blank subject field.
CSCsk39837	CSC-SSM upgrade from 6.1.1519 to 6.2.1599 via .pkg might fail.
CSCsk83984	CSC: free memory is not correctly calculated/reported.
CSCsk83986	Add additional skip content for new MIME type for www.unitedstreaming.com.
CSCsk90093	Enhance online help for unscanned corrupted files.
CSCsl11398	Add support for FTP APPEND command.
CSCsl33414	CSC: Importing e-mail addresses under white list may fail.
CSCsl44473	CSC: Logging facility settings do not change from local3.

Table 1 **Open Caveats (continued)**

CSCs154663	CSC: Slow e-mail delivery from certain domains.
CSCs154989	CSC module does not delete POP3 spam.
CSCso02432	CSC Blocked Senders Import does not allow dots in user names.
CSCso67276	CSC: Failover may not work with cisco123 encryption key.
CSCso73795	CSC: Module does not take the activation keys provided.
CSCso99926	CM agent restarting.
CSCsq00778	CSC 6.2: accessing windows update; slow access through CSC to services.

Resolved Caveats

[Table 2](#) lists the resolved caveats in the CSC SSM Version 6.2.1599.3 maintenance release.

Table 2 **Resolved Caveats**

ID Number	Caveat Title
CSCsm91133	FTP scanner sometimes does not forward 226 Transfer Complete to the client and causes the FTP session to time out.
CSCsq03282	CSC is misclassifying Microsoft sites.
CSCsq37771	SMTP scanner returns a 5xx code when DATA command returns a non-3xx code.
CSCsq37778	TMCM Agent.ini may be corrupt and cause TMCM services to stop/restart.

Related Documentation

For additional information, see the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco Content Security and Control SSM Administrator Guide*
- *Cisco ASDM Release Notes*
- *Cisco ASA 5500 Series Hardware Maintenance Guide*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco Security Appliance System Log Messages Guide*
- *Open Source Software Licenses for ASA and PIX Security Appliances*

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 “[Obtaining Documentation and Submitting a Service Request](#)” section.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, 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. (0805R)

© 2008 Cisco Systems, Inc.
All rights reserved.