



Cisco Content Security and Control (CSC) SSM Release Notes Version 6.2.1599.0

August 2007

Contents

This document contains release information for the Cisco Content Security and Control (CSC) SSM Version 6.2.1599.0 maintenance release. It includes the following sections:

- [About the CSC SSM Version 6.2.1599.0 Release, page 1](#)
- [Installing the CSC SSM Version 6.2.1599.0 Release, page 3](#)
- [Verifying the Installed Version of the CSC SSM Software, page 3](#)
- [Important Notes, page 4](#)
- [Caveats, page 4](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 10](#)

About the CSC SSM Version 6.2.1599.0 Release

The CSC SSM Version 6.2.1599.0 maintenance release includes the following new features:

- Administrators can configure (that is, add, modify, and delete) an exceptions list to URL filtering. This exceptions list includes the following information: IP addresses, IP address ranges, and subnet masks. Users can import a file of e-mail addresses into this list. In addition, administrators can create separate exceptions lists on client PCs for virus, scanning, anti-spam, or other security-related functions.
- Additional protection against malware has been provided through the use of IntelliTrap pattern files and the IntelliTrap exceptions list. ASDM can also display the status of the IntelliTrap pattern files.
- The serial number of the CSC SSM is provided automatically as part of the registration process.



Americas Headquarters:

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

© 2007 Cisco Systems, Inc. All rights reserved.

- Setup Wizard, which may increase the number of concurrent HTTP connections available.
- ASDM allows administrators to configure which traffic the CSC should scan through the Traffic Flow Selection step of the CSC Setup Wizard.
- Administrators can customize the web page that appears to users for blocked, filtered, infected, or prohibited URLs. Customization includes the company logo and the security policy statement.
- The CSC SSM supports the Damage Cleanup Service (DCS) for cleaning an infected PC. The DCS removes spyware, worms, viruses, Trojan horses, and memory registries on clients and servers. In addition, it repairs system registries and memory. The DCS requires a separate installation of the DCS server.



Note

- -
 - URL filtering supports SOCKS-based proxy servers.
- URL filtering allows bypassing based on client IP addresses.
- URL filtering has added the following new categories:
- Tasteless, Recreation/Hobbies, Entertainment, Arts, Internet Radio and TV, Internet Telephony, Marijuana, Activist Groups, Political/Activist Parties, Infrastructure, Blogs & Web Communications, Photo Searches, Translators (circumvent filtering), Social Networking, Personal Websites, Personal Network Storage/File Download Servers, Peer-to-Peer, Gay/Lesbian/Bisexual, Sport Hunting and Gun Clubs, Sports, Ringtones/Mobile Phone Downloads, (Software) Downloads, Potentially Malicious Software, Spyware, Phishing, Spam, Adware, Virus Accomplice, Disease Vector, Cookies, Dialers, Hacking, Joke Programs, Password Cracking Applications, Remote Access Program, and Made for AdSense sites (MFA).
- URL filtering has removed the following categories: Unrated and Miscellaneous.
- The Network Reputation Service (NRS) has been renamed to the Email Reputation Service (ERS). The ERS portal is accessible through the CSC GUI, which provides detailed reporting and allows customization of the ERS feature.
- Configuration recovery through the CLI after re-imaging has been removed. Make sure you use the .pkg file to upgrade image files through the CSC SSM GUI.
- Detect spam in image files and PDF files. Because the anti-spam engine in this version is a higher version than the one on the Trend Micro Update Server, the updates for the spam engine may display as unsuccessful and in red on the summary page. This is temporary behavior, and will be resolved after the most current TMASE engine has been made available.
- Performance improvements have been made.
- For information about CSC SSM sizing deployment requirements, go to the following URL and log in with your Cisco.com username and password:
- http://www.cisco.com/en/US/customer/products/ps6120/products_white_paper0900aecd805c3cd6.shtml
- 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 6.2.1599.0 Release

You can install this release if you are running CSC SSM version 6.1.x. 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** Download the csc6.2.1599.0.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**.
- Step 3** Choose **Administrator > Product Upgrade** from the menu.
- Step 4** Click **Browse** and select the .pkg file you downloaded.
- Step 5** Click **Install**.
- 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.
-

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



Note

-
- | | |
|---------------|---|
| Step 1 | Content Security |
| Step 2 | Tools > Command Line Interface |
| Step 3 | show module 1 details Send |

```
hostname(config)# 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 6.2.1599.0
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:         6.2.1599.0
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>
    
```

Important Notes

-
-
-

Cisco ASDM Release Notes

Caveats

- **boldface**
-
-

-
-

Open Caveats

Table 1 **Open Caveats**

ID Number	Caveat Title
CSCsd17818	Yahoo! Finance MarketTracker does not work.
CSCsd17889	Nothing seems to happen when downloading infected file from/to web mail.
CSCsd17954	The HTTP proxy connection cannot tunnel through the CSC SSM.
CSCsd18011	FTP file blocking will not work when file not scanned due to cfg.
CSCsd18052	Email 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.
CSCsf26197	CSC software blocks Ameritrade streamer.
CSCsf98493	[HTTP] VPN users using proxy have problem browsing via HTTP.
CSCsf98538	[UI] WhiteIPList on NRS will disappear from UI.
CSCsg52819	CSC module - Import function for user-defined domain lists.
CSCsh18404	CSC module to support https requests in URL filtering.
CSCsh27011	[FTP] HP UX tcp_lift_anchor, can't wait error message when doing FTP i.
CSCsh27102	[Admin UI] SSL vulnerability.
CSCsh39788	After upgrade with *.pkg, URL filtering does not function.
CSCsh53472	CSC module delays HTTP and FTP traffic.
CSCsh58934	SSM Card becomes unresponsive after configuring from ASDM.
CSCsh70101	No error message for invalid URL Blocking import file.
CSCsh80376	Incorrect error message when URL rating lookup times out.
CSCsh97282	Ability to change the CSC SSM default WEB GUI port 8443.
CSCsi27604	Intermittent email 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.
CSCsi66735	CSC SSM does not properly handle partial emails.
CSCsi82300	CSC causes large emails attachments to timeout when downloading via POP3.
CSCsj10645	CSC still filters large size messages even if disabling POP3 scanning.
CSCsj20246	CSC SSM not detecting spyware threats.

Open Caveats (continued)

Cisco/Trend Micro ID Number	Caveat Title

Resolved Caveats

Table 2 Closed Caveats

ID Number	Caveat Title

[illegible]

Table 2 ***Closed Caveats (continued)***

CSCsh14819	Patch history is not displayed properly when upgrading from 6.1p1.
CSCsh15518	Upgrading CSC module may result in no ability to activate module.
CSCsh19934	CSC SSM not passing traffic for several minutes after config update.
CSCsh21113	Scheduled update email notification subject reports incorrect update status.
CSCsh21159	Unable to see streaming video/audio from some sites.
CSCsh23475	CSC module - URL blocking not functional for keywords.
CSCsh27010	POP3 never worked.
CSCsh27014	[HTTP] Asymmetric connection close issue in http proxy.
CSCsh27090	[http] Firefox 2.0 with Fasterfox plug-in has issue opening cisco.com.
CSCsh27092	[HTTP] Codenomicon tool causes CSC CPU to hit 100%.
CSCsh27093	[HTTP] URL Filtering requests sent with incorrect format.
CSCsh27095	[UI] Patch installation does not clean patch history page.
CSCsh27099	[Update] Improve the update feature around notification mail.
CSCsh27103	[HTTP] Streaming media does not work.
CSCsh31484	CSC module on ASA does not show email disclaimer.
CSCsh31982	[HTTP] CSC SSM: Disconnects HTTP sessions from proxy in DMZ.
CSCsh35086	CSC module with URL filtering delays or blocks all web traffic.
CSCsh46886	CSC SSM - SWF files are being treated as executables.
CSCsh50078	CSC URL filtering, HTTP browsing fails: page cannot be displayed error.
CSCsh58065	TFTP transfers to/from CSC module's command line failing.
CSCsh58836	TMCN Agent TMCN Agent sends wrong version information.
CSCsh58901	ASDM Plus license expiration does not disable URL blocking in ASDM.
CSCsh58911	HTTP CSC SSM module CPU pegged at 100%.
CSCsh73881	CSC SSM CPU pegs at 100% when running 6.1(1569).2 image.
CSCsh74915	Trend GUI does not return to login screen after timeout.
CSCsh83148	TCP timestamp unexpectedly set to 0 for flows reordered by the firewall.
CSCsh90870	POP3 Adding deferred scanning to POP3 scanning.
CSCsh96228	POP3 and SMTP corrupt email if CR LF arrives in separate lines.
CSCsh96229	IWSS cannot parse CCM_POST.
CSCsh96231	URL Filtering cannot handle chunked RS response.
CSCsh96235	Incorrect syslog is sent when CSC is unable to connect to URL ratings.
CSCsh96237	Email delays dues to IMSS lacking timeout (current behavior is 120 sec).
CSCsh96238	HTTP does not send syslog on socket timeout.
CSCsi06520	Add support for TLS over FTP.
CSCsi07133	TFTP uploads via CSC module Troubleshooting menu fail.

Table 2 **Closed Caveats (continued)**

CSCsi18226	Failover Unable to establish failover relationship.
CSCsi32093	Issue sending email when recipient list is too large.
CSCsi40116	OCLC Parsing error.
CSCsi43390	Improve Online Help description for Log Query.
CSCsi43391	Service module does not respond under high loads.
CSCsi43393	When SSM log partition is full, IWSS leaks ~isvw/tttt.txt.
CSCsi43397	Include TM agent log into CSC Log Collection.
CSCsi43399	Not able to stream AOL online radio.
CSCsi43791	Command option -dst cache overflow causing CSC to be unable to accept new connections.
CSCsi52793	Allow customer to enable/disable SMTP TLS.
CSCsi52795	Allow un-registering TCM when TCM server is unreachable.
CSCsi52796	SSM License GUI cannot accept new Activation Codes.
CSCsi52797	NRS is not disabled after Plus license expired.
CSCsi52798	Upgrade requires base CSC version 6.1.1569.x.
CSCsi52799	Make core dump enable easier in the header of IS functions.
CSCsi66735	CSC does not handle partial mail properly.
CSCsi83497	Management IP address truncated.
CSCsi83497	IP address for management port may be truncated on ASA CLI for command.
CSCsi89565	ASDM requires at least three characters in email username field.
CSCsj16273	URL categories, Social networking not seen.
CSCsj16273	Social Networking URL category is missing on CSC GUI.
CSCsj19322	CSC: Active Trend GUI session requires reauth every 10 min.
CSCsj19322	CSC GUI times out in 10 minutes, regardless of user activity.
CSCsj33289	CSC memory may be filled up under heavy FTP traffic.
CSCsj46486	Spam subject tagging does not handle QP-encoded subjects properly.
CSCsj64650	SMTP content filtering requires .WILD. entry for wildcards to be enabled.
CSCsj89273	SOCKS-based proxy service is now supported.
CSCsj89274	POP3 scanner does not handle AUTH command properly.
CSCsj89275	Problem accessing email with Entourage.
CSCsj89276	Explain wildcard usage for Content-Filtering in online help.
CSCsj89277	Evaluation Plus license cannot be activated on CSC GUI.
CSCsj91186	Japanese patch record p-6.1-ja-1 is lost after upgrade.

Related Documentation

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

-
-
- *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*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

This document is to be used in conjunction with the documents listed in the “[Obtaining Documentation, Obtaining Support, and Security Guidelines](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

© 2007 Cisco Systems, Inc.
All rights reserved.