CHAPTER 8

Troubleshooting Trend Micro InterScan for Cisco CSC SSM

This chapter describes how to troubleshoot various issues, and includes the following sections:

Troubleshooting Installation

The following describes how to install using the CLI. If problems occur during the installation, see the "What To Do If Installation Fails" section on page 8-3.

To install the CSC SSM via the CLI, perform the following steps.

Step 1 Enter the following command to begin the installation:

```
hostname(config)# hw-module module 1 recover configure
```

Step 2 Output similar to the following appears:

```
Image URL [tftp://171.69.1.129/dqu/csc6.2.xxxx.x.bin]:
Port IP Address [0.0.0.0]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
hostname(config)# hw-module 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]
Recover issued for module in slot 1
hostname(config)#
hostname(config)# debug module-boot
debug module-boot enabled at level 1
```

Step 3 After about a minute, the CSC SSM goes into the ROMMON mode, and prints messages similar to the following:

```
hostname(config)# Slot-1 206> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26
00:13:50 PST 2007
Slot-1 207> domainname@yourdomain.com:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 208> Platform ASA-SSM-AIP-10-K9
Slot-1 209> GigabitEthernet0/0
Slot-1 210> Link is UP
Slot-1 211> MAC Address: 000b.fcf8.01b3
Slot-1 212> ROMMON Variable Settings:
Slot-1 213> ADDRESS=30.0.0.3
Slot-1 214> SERVER=171.69.1.129
Slot-1 215> GATEWAY=30.0.0.254
Slot-1 216> PORT=GigabitEthernet0/0
Slot-1 217> VLAN=untagged
Slot-1 218> IMAGE=dqu/csc6.2.xxxx.x.bin
Slot-1 219> CONFIG=
Slot-1 220> LINKTIMEOUT=20
Slot-1 221> PKTTIMEOUT=2
Slot-1 222> RETRY=20
Slot-1 223> tftp dqu/csc6.2.xxxx.x.bin@171.69.1.129 via 30.0.0.254
```

Step 4 The CSC SSM attempts to connect to the TFTP server to download the image.

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. The .pkg files are used to upgrade image files from the CSC Admin Console, which are then uploaded through a web browser. Do not upload .bin files using the CSC Admin Console.

Step 5 After several seconds, output similar to the following appears:

```
Slot-1 224>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 225>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 226>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 227>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 228>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
. . . [ output omitted ]. . .
Slot-1 400>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 401>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 402>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 403>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 404>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 405> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Slot-1 406> Received 59501255 bytes
```

The TFTP download is complete. Note the number of received bytes, which should be the same size as the CSC SSM image.

Step 6 The ROMMON mode then launches the image.

```
Slot-1 407> Launching TFTP Image...
```

The image is being unpacked and installed.

Step 7 After several minutes, the CSC SSM reboots.

Step 8 Messages similar to the following appear:

```
Slot-1 408> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50 PST 2007
Slot-1 409> morlee@bowmore:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 410> Platform ASA-SSM-AIP-10-K9
Slot-1 411> Launching BootLoader...
```

After a minute or two, the CSC SSM boots up.

Step 9 To verify that the CSC SSM has booted correctly, enter the following command:

```
hostname(config)# show module 1
```

Step 10 Output similar to the following appears:

```
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5520/5530 AIP Security Service Module-10 ASA-SSM-AIP-10-K9  P00000000TT

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 000b.fcf8.01b3 to 000b.fcf8.01b3  1.0          1.0(10)0     CSC SSM 6.2.xxxx.x

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.2.xxxx.x

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Note Look for the two instances of "Up" in the Mod Status table (the last line of the output). The "Down" entry in the Status field of the SSM Application Name table indicates that the card is not yet activated.

What To Do If Installation Fails

Table 8-1 describes what to do if installation fails during the procedure described in the "Troubleshooting Installation" section on page 8-1.

Table 8-1 What to Do If Installation Fails

If installation fails at:	Your action is:
Step 3	**a.** Make sure the TFTP server supports downloading of files larger than 60 MB. **b.** Check the size of the CSC image as it appears on your TFTP server. **c.** Can you perform an MD5 checksum to see whether it matches the checksum published with the image. **d.** Verify the image size that transferred according to the **verbose** output of the adaptive security appliance.
Step 4	**a.** Make sure you set the gateway IP address to 0.0.0.0 if your TFTP server is in the same IP subnet as the CSC SSM. **b.** If there is any router or firewall between the CSC SSM and your TFTP server, make sure these gateways allow TFTP traffic through UDP port 69. Also, verify that routes are set up correctly on these gateways and on the TFTP server. **c.** Verify the image path exists on the TFTP server, and that the directory and file are readable to all users.
Step 6	Verify the total number of bytes downloaded. If the number is different than the size of the CSC SSM image, your TFTP server may not support files that are the size of the image. In this case, try another TFTP server.
Step 7 or Step 9	Download the image again and try to install it again. For more information, see Appendix A, "Preparing to Reimage the Cisco CSC SSM." If the installation is not successful a second time, contact Cisco TAC.

Troubleshooting Activation

Before taking any other action, make sure that the clock is set correctly on the adaptive security appliance. For more information, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the ASDM online help.

Use the **show module**, **show module 1**, and **show module 1 details** commands to verify that the CSC SSM has been activated successfully. If you cannot resolve the problem using the output from these commands, contact Cisco TAC.

Troubleshooting Basic Functions

This section describes issues you may encounter with basic functions, and includes the following topics:

- Cannot Log On, page 8-5
- Recovering a Lost Password, page 8-5
- Summary Status and Log Entries Out of Sync, page 8-6
- Delays in HTTP Connections, page 8-6

- Access to Some Websites Is Slow or Inaccessible, page 8-6
- FTP Download Does Not Work, page 8-7
- Reimaging or Recovery of CSC Module, page 8-8

Note You must configure the syslog server to save the log buffer content to a file, so that it will be available for troubleshooting and debugging purposes.

Cannot Log On

You specified an administrator password when you installed Trend Micro InterScan for Cisco CSC SSM with the Setup Wizard. You must use the password you created during installation to log in, which is not the same password that you use to access ASDM. Passwords are case-sensitive; be sure you have entered the characters correctly.

If you forget your password, it can be recovered. For more information, see Recovering a Lost Password, page 8-5.

Recovering a Lost Password

The two passwords used to manage the CSC SSM are as follows:

- The ASDM/Web interface/CLI password
- The root account password

The default entry for both passwords is “cisco.”

To recover your passwords in case you lose one or more of them, consider the following:

- If you have the ASDM/Web interface/CLI password, but have lost the root account passwords, you can continue to manage the CSC SSM via the web interface.
- Unless you have configured the password-reset policy to “Allowed,” you cannot use the root account in the future. If the password-reset policy is set to “Denied,” recovering these two passwords requires reimaging of the CSC SSM and restoration of the configuration according to the subsequent procedure. For more information, see “Modifying the Password-reset Policy” section on page A-11.

Caution Access the root account only under the supervision of Cisco TAC. Unauthorized modifications made through the root account are not supported and require that the device be reimaged to guarantee correct operation.

- If you have lost all passwords, you must reimage the device and restore the configuration, unless you have configured the password-reset policy to “Allowed.”

To reimage the CSC SSM and recover the configuration, perform the following steps:

Step 1 Reimage the CSC SSM, which restores the factory default settings. Reimaging transfers a factory default software image to the SSM. To transfer an image, see the “Reimaging and Configuring the CSC SSM Using the CLI” section on page A-1.

After reimaging, all passwords are restored to their default value.

Step 2 Reactivate the device and log in using the default password "cisco," and then create a new ASDM password.

Step 3 Use the new ASDM password to access the CSC SSM interface. Choose **Administration > Configuration Backup**.

Step 4 To restore the configuration settings, import the most recent configuration backup.

Step 5 After you have imported the configuration backup, browse through all of the configurations to verify their accuracy.

Summary Status and Log Entries Out of Sync

You may occasionally notice that the counters displayed on the Mail (SMTP), Mail (POP3), Web (HTTP), and File Transfer (FTP) tabs of the Summary window do not synchronize with the statistics displayed in the log reports. In the CSC SSM console, choose **Logs > Query** to access the logs. This mismatch happens because of the following:

- The logs are reset by a reboot that occurs either because of a device error or following the installation of a patch.
- Logs may be purged because of limited memory storage on the SSM.

Delays in HTTP Connections

A delay of approximately 30 seconds can occur if you have URL filtering enabled on the CSC SSM, but the CSC SSM does not have access to the Internet via HTTP. Trend Micro maintains an online database that stores URLs in different categories. The CSC SSM first checks the local URL filtering database. If no entry is located, then the CSC SSM tries to access the URL database when processing an HTTP request from a client. If you cannot grant Internet access to the CSC SSM (either direct or indirect via a proxy), disable URL filtering.

In addition, disabling Deferred Scanning may cause large file transfers to be slow or time out.

Access to Some Websites Is Slow or Inaccessible

There are some websites, such as banks, online shopping sites, or other special purpose servers that require extra backend processing before responding to a client request. The CSC SSM has a non-configurable, 90-second timeout between the client request and the server response to prevent transactions from tying up resources on the CSC SSM for too long. This means that transactions that take a longer time to process will fail. The workaround is to exclude the site from scanning.

For example, for a site on the outside network with the IP address, 100.100.10.10:

```
exempt http traffic to 123.123.10.10
access-list 101 deny tcp any host 123.123.10.10 eq http
catch everything else
access-list 101 permit tcp any eq http
class-map my_csc_class
      match access-list 101
policy-map my_csc_policy
     class my_csc_class
         csc fail-close
service-policy my_csc_policy interface inside
```

This configuration exempts HTTP traffic to 100.100.10.10 from being scanned by the CSC SSM.

Performing a Packet Capture

If there are sites you can access without going through the CSC SSM, but cannot access when traffic is being scanned, report the URL to Cisco TAC. If possible, do a backplane packet capture and send the information to Cisco TAC also.

For example, if the client has an IP address, 1.1.1.1, and the outside website has an IP address, 2.2.2.2:

```
access-list cap_acl permit tcp host 1.1.1.1 host 2.2.2.2
capture cap access-list cap_acl interface inside
```

To perform a packet capture, perform the following steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command:

```
hostname(config)# capture csc_cap interface asa_dataplance buffer 10485760
```

Note The number of bytes in the capture buffer is 10485760. The example is 10 MB.

Step 3 Start the traffic testing.

Step 4 Enter the following command to transfer the captured buffer out of the box:

```
hostname(config)# copy /pcap capture:csc_cap tftp://IP/path
```

Step 5 Enter the following command to stop the capture:

```
hostname(config)# no capture csc_cap interface asa_dataplane
```

Note You can use the last command to reset or clear the buffer between tests, but you must reenter the **capture** command.

FTP Download Does Not Work

If your FTP login works, but you cannot download via FTP, do the following:

- Verify that the inspect ftp setting is enabled on the adaptive security appliance.
- Verify that Deferred Scanning is enabled on the FTP Scanning page.

For more information, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Reimaging or Recovery of CSC Module

During reimaging or recovery of a CSC module, it is possible to type the address of the TFTP server or the file name incorrectly. If this occurs, the CSC module will continuously reboot, attempting the reimaging using the invalid configuration information provided. To stop the reimaging process and correct the configuration, enter the **hw module 1 recover stop** command in the specified configuration mode.

Troubleshooting Scanning Functions

This sections describes issues that you may encounter with scanning for viruses or spam, and includes the following topics:

- Cannot Update the Pattern File, page 8-8
- Spam Not Being Detected, page 8-8
- Cannot Create a Spam Stamp Identifier, page 8-9
- Unacceptable Number of Spam False Positives, page 8-9
- Cannot Accept Any Spam False Positives, page 8-9
- Unacceptable Amount of Spam, page 8-9
- Virus Is Detected but Cannot Be Cleaned, page 8-10
- Virus Scanning Not Working, page 8-10
- Downloading Large Files, page 8-12
- Restart Scanning Service, page 8-13

Cannot Update the Pattern File

If the pattern file is out-of-date and you are unable to update it, the most likely cause is that your Maintenance Agreement has expired. Check the Expiration Date field in the Administration > Product License window. If the date shown is in the past, you cannot update the pattern file until you renew your Maintenance Agreement.

If the pattern file is current, the following may be true:

- The Trend Micro ActiveUpdate server is temporarily down. Try to update the pattern file again in a few minutes.
- Check the network settings and the connectivity of the SSM, including the proxy settings.

Spam Not Being Detected

If the anti-spam feature does not seem to be working, be sure that the following is true:

- You have the Plus License installed and it is current.
- You must have a valid Plus License and the correct DNS settings for the network-based, anti-spam Email Reputation to function correctly.
- You have enabled the feature; the anti-spam option is not enabled by default. For more information, see Enabling SMTP and POP3 Spam Filtering, page 3-8.

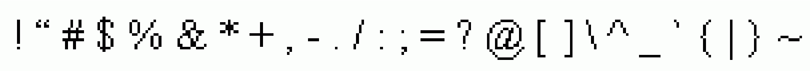
- You have configured the incoming mail domain. The content-based anti-spam scanning is only applied to mail recipients belonging to Incoming Domains. For more information, see Configuring SMTP Settings, page 3-6.

Cannot Create a Spam Stamp Identifier

A spam stamp identifier is a message that appears in the e-mail message subject. For example, for a message titled “Q3 Report,” if the spam stamp identifier is defined as “Spam:,” the message subject would appear as “Spam:Q3 Report.”

If you are having problems creating a spam identifier, make sure you are using only English uppercase and lowercase characters, the digits 0-9, or the set of special characters shown in Figure 8-1.

Figure 8-1 Special Characters for Spam Stamp Identifier



```
! “ # $ % & * + , - . / : ; = ? @ [ ] \ ^ _ ` { | } ~
```

Note If you try to use characters other than those specified, you cannot use the spam identifier for SMTP and POP3 messages.

Unacceptable Number of Spam False Positives

Your spam filtering threshold may be set at a level that is too aggressive for your organization. Assuming you adjusted the threshold to Medium or High, try a lower setting in the threshold fields on the Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam window and the Mail (POP3) > Anti-spam > POP3 Anti-spam windows. Also enable the anti-spam “stamp message” feature on the SMTP Incoming Anti-spam window and the POP3 Anti-spam windows. For more information, see the online help for these two windows.

Also, if users in your network are receiving newsletters through e-mail, this type of message tends to trigger a high number of false positives. Add the e-mail address or domain name to the approved senders list to bypass spam filtering on these messages.

Cannot Accept Any Spam False Positives

Some organizations, such as banks and other financial institutions, cannot risk any message being identified as a false positive. In this case, disable the anti-spam feature for SMTP and POP3.

Unacceptable Amount of Spam

If you receive an unacceptable amount of spam, enable the network-based, anti-spam Email Reputation (ER) setting. Choose **Mail (SMTP) > Anti-spam > Email Reputation**.

If you do not use Email Reputation, you may have set your spam filtering threshold at a level that is too lenient for your organization. Try a higher setting in the threshold fields on the Mail (SMTP) > Anti-spam > Content Scanning/Target window and the Mail (POP3) > Anti-spam/Target.

Virus Is Detected but Cannot Be Cleaned

Not all virus-infected files are cleanable. For example, a password-protected file cannot be scanned or cleaned.

If you think you are infected with a virus that does not respond to cleaning, go to the following URL:

http://subwiz.trendmicro.com/SubWiz/Default.asp

This link takes you to the Trend Micro Submission Wizard, which includes information about what to do, including how to submit your suspected virus to TrendLabs for evaluation.

Virus Scanning Not Working

This section describes why virus scanning may not work, and includes the following topics:

- Scanning Not Working Because of Incorrect Service-Policy Configuration, page 8-10
- Scanning Not Working Because the CSC SSM Is in a Failed State, page 8-10

Ensure that no one has disabled the virus scanning feature on the SMTP Incoming, SMTP Outgoing, POP3, HTTP, and FTP Scanning windows. Also test the virus scanning feature by following the instructions described in the "Testing the Antivirus Feature" section on page 2-3.

Scanning Not Working Because of Incorrect Service-Policy Configuration

Another possible cause is that a file has not been scanned because of an incorrect service-policy configuration. Use the **show service-policy csc** command to configure the SSM to process traffic.

The following example shows how to configure the SSM to process traffic:

```
hostname(config)# show service-policy flow tcp host 192.168.10.10 host 10.69.1.129 eq http
Global policy:
Service-policy: global_policy
    Class-map: trend
        Match: access-lit trend
            Access rule: permit tcp any any eq www
        Action:
            Output flow: csc fail-close
            Input flow set connection timeout tcp 0:05:00
    Class-map: perclient
        Match: access-lit perclient
            Access rule: permit IP any any
            Action:
            Input flow: set connection per-client-max 5 per-client-embryonic-max 2
```

Scanning Not Working Because the CSC SSM Is in a Failed State

If the CSC SSM is in the process of rebooting, or has experienced a software failure, system log message 421007 is generated.

Enter the following command to view the status of the SSM card:

```
hostname(config)# show module 1
```

The output appears in several tables, as shown in the following example. The third table, SSM Application Name, displays status, which is "Down."

```
Mod Card Type                                    Model  Serial No.
--- -------------------------------------------- -----------------------------
1 ASA 5500 Series Security Services Module-10ASA-SSM-10 JAB092400TX

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
 1 0013.c480.ae4c to 0013.c480.ae4c  1.0          1.0(10)0     CSC SSM 6.2.xxxx.x

Mod SSM Application Name           Status           SSM Application Version
--- ---------------------------- ------------------------------------------
 1 CSC SSM                        Down             6.2.xxxx.x

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
 1 Up                 Up
```

The three possible states that could display in the Status field for the third table are as follows:

- Down—A permanent error, such as an invalid activation code was used, licensing has expired, or a file has been corrupted
- Reload—Scanning is restarting, for example, during a pattern file update.
- Up—A normal operating state.

To view the state for each individual process, enter the following command:

```
hostname(config)# show module 1 details
```

Example output similar to the following appears:

```
Getting details from the Service Module, please wait...
    ASA 5500 Series Security Services Module-10
    Model:              ASA-SSM-10
    Hardware version:   1.0
    Serial Number:      JAB092400TX
    Firmware version:   1.0(10)0
    Software version:   CSC SSM 6.2.xxxx.x
    MAC Address Range:  0013.c480.ae4c to 0013.c480.ae4c
    App. name:          CSC SSM
    App. Status:        Down
    App. Status Desc:   CSC SSM scan services are not available
    App. version:       6.2.xxxx.x
    Data plane Status:  Up
    Status:             Up
    HTTP Service:       Down

    Mail Service:       Down

    FTP Service:       Down

    Activated:          No

    Mgmt IP addr:       <not available>

    Mgmt web port:      8443

    Peer IP addr:       <not enabled>
```

The status for the CSC SSM appears in the App. Status field. In the example, the status is “Down.” The possible states for this field are as follows:

- Not Present—The SSM card is not found.
- Init—The SSM card is booting.

- Up—The SSM card is up and running.
- Unresponsive—The SSM card is not responding.
- Reload—The SSM application is reloading recently updated patterns or configuration changes. The traffic is interrupted temporarily with either a "fail-open" or "fail-close." The adaptive security appliance will not perform a failover because this is an administrative reloading.
- Shutting Down—The SSM card is shutting down.
- Down—The SSM card is down and can be safely removed from its slot.
- Recover—The SSM card is being reimaged.

If you have verified your configuration and CSC module status, and viruses are still not found, contact Cisco TAC.

Downloading Large Files

Handling of very large files may be a potential issue for the HTTP and FTP protocols. On the Target tabs of the HTTP Scanning and FTP Scanning windows, you configured large file handling fields, which included a deferred scanning option.

If you did not enable deferred scanning, Trend Micro InterScan for Cisco CSC SSM must receive and scan the entire file before passing the file contents to the requesting user. Depending on the file size, this action could result in the following:

- The file being downloaded, very slowly at first, but more quickly as the download progresses.
- Take longer than the automatic browser timeout period. As a result, the user is unable to receive the file contents at all because the browser times out before the download completes.

If you enabled deferred scanning, part of the content of the large file is delivered without scanning to prevent a timeout from occurring. Subsequent portions of the content are being scanned in the background and are then downloaded if no threat is detected. If a threat is detected, the rest of the file is not downloaded; nevertheless, the unscanned portion of the large file is already stored on the user machine and may introduce a security risk.

Enabling Deferred Scanning

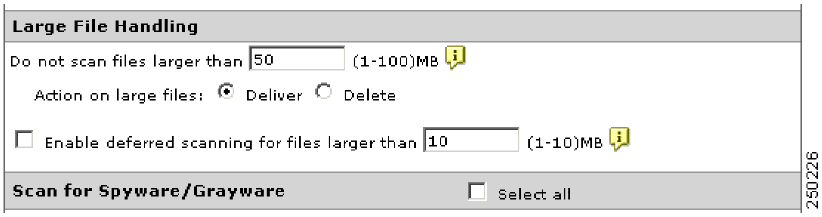
Note If you experience difficulty with Windows updates, you may need to enable deferred scanning and set the size to ten. See the logs for more information.

To enable deferred scanning, perform the following steps:

Step 1 Go to the Web (HTTP) > HTTP scanning tab.

Step 2 In the Large File Handling section, set the "Enable deferred scanning for files larger than" value to 10, as shown in Figure 8-2.

Figure 8-2 Enabling Deferred Scanning



Large File Handling

Do not scan files larger than 50 (1-100)MB

Action on large files: ● Deliver ○ Delete

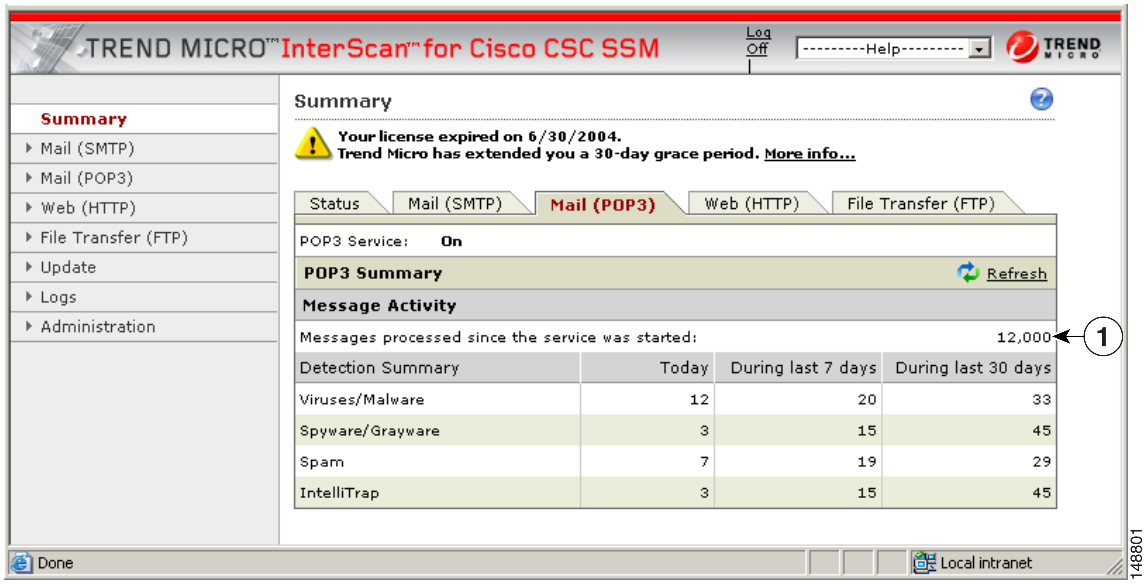
□ Enable deferred scanning for files larger than 10 (1-10)MB

Scan for Spyware/Grayware □ Select all

Restart Scanning Service

In the Message Activity area, the Mail (SMTP and POP3) tabs on the Summary window display a count of messages processed since the service was started. For an example, see Figure 8-3.

Figure 8-3 Messages Processed Counter on the Mail (POP3) Tab of the Summary Window



Summary

Your license expired on 6/30/2004.
Trend Micro has extended you a 30-day grace period. More info...

POP3 Service: On

POP3 Summary

Message Activity

Messages processed since the service was started: 12,000

Detection Summary	Today	During last 7 days	During last 30 days
Viruses/Malware	12	20	33
Spyware/Grayware	3	15	45
Spam	7	19	29
IntelliTrap	3	15	45

1	Message activity counter

Several events can cause these counters to reset to zero:

- A pattern file or scan engine update
- A configuration change
- The application of a patch

The statistics in the Detection Summary area of the window do not reset; these statistics continue to update as trigger events occur.

When the counters reset, it is normal behavior. If, however, you have a continuous zero in the Messages processed fields, e-mail traffic is not being scanned and you should investigate.

Troubleshooting Performance

This section describes issues you may encounter with performance, and includes the following topics:

- CSC SSM Console Timed Out, page 8-14
- Status LED Flashing for Over a Minute, page 8-14
- SSM Cannot Communicate with ASDM, page 8-14
- Logging in Without Going Through ASDM, page 8-14
- CSC SSM Throughput is Significantly Less Than ASA, page 8-15

CSC SSM Console Timed Out

If you leave the CSC SSM console active and no activity is detected for approximately ten minutes, your session times out. Log in again to resume work. Unsaved changes are lost. If you are called away, save your work and log off until you return.

Status LED Flashing for Over a Minute

If the Status LED continues flashing for more than one minute, the scanning service is not available. To resolve this problem, enter the **show module 1 details** command to collect relevant information, and then reboot the system from ASDM.

⚠ **Caution** If the file to be downloaded is larger than the size specified in the Do not scan files larger than field, the file is delivered without scanning and may present a security risk.

SSM Cannot Communicate with ASDM

For information about resetting port access control, see the "Changing the Management Port Console Access Settings" section on page A-17.

Logging in Without Going Through ASDM

If for some reason ASDM is unavailable, you can log directly into the CSC SSM via a web browser. To log in, perform the following steps:

Step 1 Enter the following URL in a browser window:

```
https://{SSM IP addresss}:8443
```

For example:

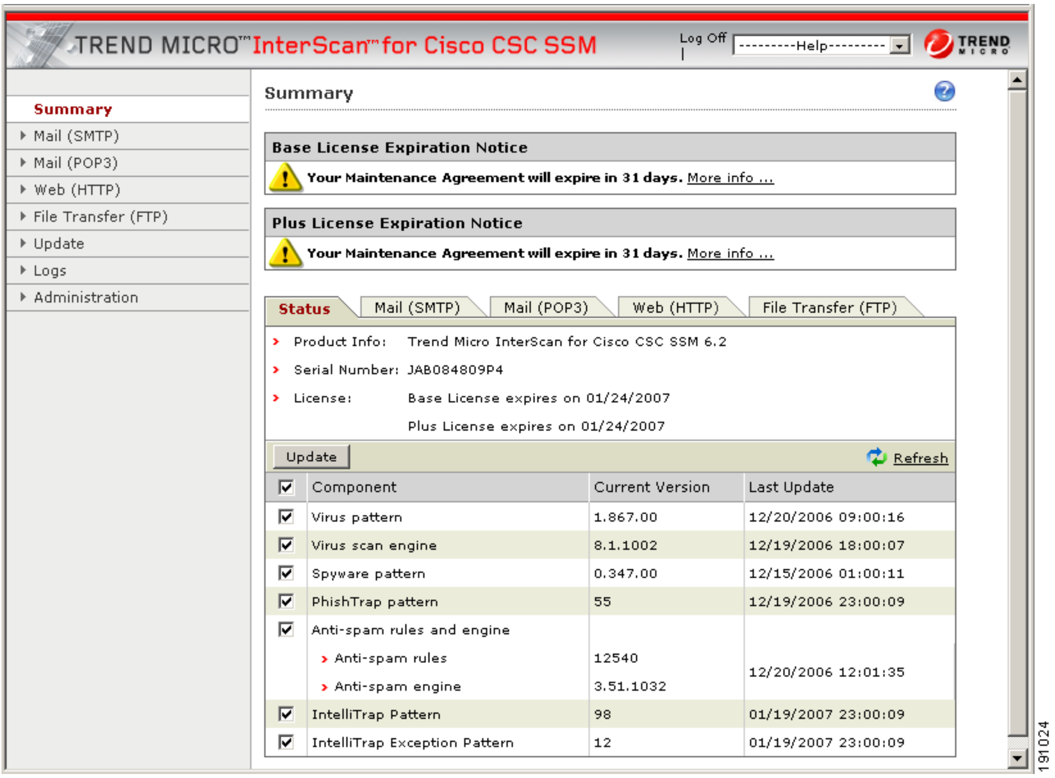
```
https://10.123.123.123:8443/
```

The Logon window appears.

Step 2 Enter the password you created in the Setup Wizard on the Password Configuration installation window and click **Log On**.

The default view of the CSC SSM console is the Status tab on the Summary window, as shown in Figure 8-4.

Figure 8-4 Status Tab of the Summary Screen on the CSC SSM Console



Summary

Base License Expiration Notice

Your Maintenance Agreement will expire in 31 days. More info ...

Plus License Expiration Notice

Your Maintenance Agreement will expire in 31 days. More info ...

- Product Info: Trend Micro InterScan for Cisco CSC SSM 6.2
- Serial Number: JAB084809P4
- License: Base License expires on 01/24/2007
  Plus License expires on 01/24/2007

☑	Component	Current Version	Last Update
☑	Virus pattern	1.867.00	12/20/2006 09:00:16
☑	Virus scan engine	8.1.1002	12/19/2006 18:00:07
☑	Spyware pattern	0.347.00	12/15/2006 01:00:11
☑	PhishTrap pattern	55	12/19/2006 23:00:09
☑	Anti-spam rules and engine		
	› Anti-spam rules	12540	12/20/2006 12:01:35
	› Anti-spam engine	3.51.1032	
☑	IntelliTrap Pattern	98	01/19/2007 23:00:09
☑	IntelliTrap Exception Pattern	12	01/19/2007 23:00:09

CSC SSM Throughput is Significantly Less Than ASA

Restoring files from TCP connections and scanning them is a processor-intensive operation, which involves more overhead than the protocol-conformance checking that is usually done by a security appliance. The workaround is to divert only the connections that need to be scanned to the CSC SSM to mitigate the performance mismatch.

For example, HTTP traffic can be divided into outbound traffic (an inside user is accessing outside websites), inbound traffic (an outside user is accessing inside servers), and intranet traffic (traffic between internal sites or trusted partners). You can configure the CSC SSM to scan only outbound and inbound traffic for viruses, but ignore the intranet traffic.

For more information, see the *Cisco Security Appliance Command Line Configuration Guide.*

Known Issues

The following known issues exist in the CSC SSM:

- The CSC SSM does not scan HTTP proxy traffic nor non-HTTP traffic over port 80.

  Workaround: Do one of the following:

  - Use another port as the proxy service.
  - Use the security appliance modular policyframework to prevent the CSC SSM from scanning the website IP addresses.
  - Deploy a proxy server between the CSC SSM and clients.

- The CSC SSM does not work with certain real-time stock streaming services, such as Yahoo Market Tracker.

  Workaround: Use the security appliance modular policy framework to prevent the CSC SSM from scanning the website IP addresses for stock streaming services.

- Traffic interruptions may occur during configuration or component updates.

  Workaround: Perform configuration updates or scheduled updates during off-hours.

- The CSC SSM does not scan e-mail traffic between Microsoft Exchange servers that use the EXCH50 protocol.

  Workaround: Use the security appliance modular policy framework to prevent the CSC SSM from scanning the Microsoft Exchange servers' IP addresses.

Using Knowledge Base

You can search for more information in the Trend Micro online Knowledge Base, available at the following URL:

http://esupport.trendmicro.com

The Knowledge Base search engine allows you to refine your search, by entering product name, problem category, and keywords. Thousands of solutions are available in the Knowledge Base, and more are added weekly.

Using the Security Information Center

Comprehensive security information is available from the Trend Micro Security Information Center, a free online resource, at the following URL:

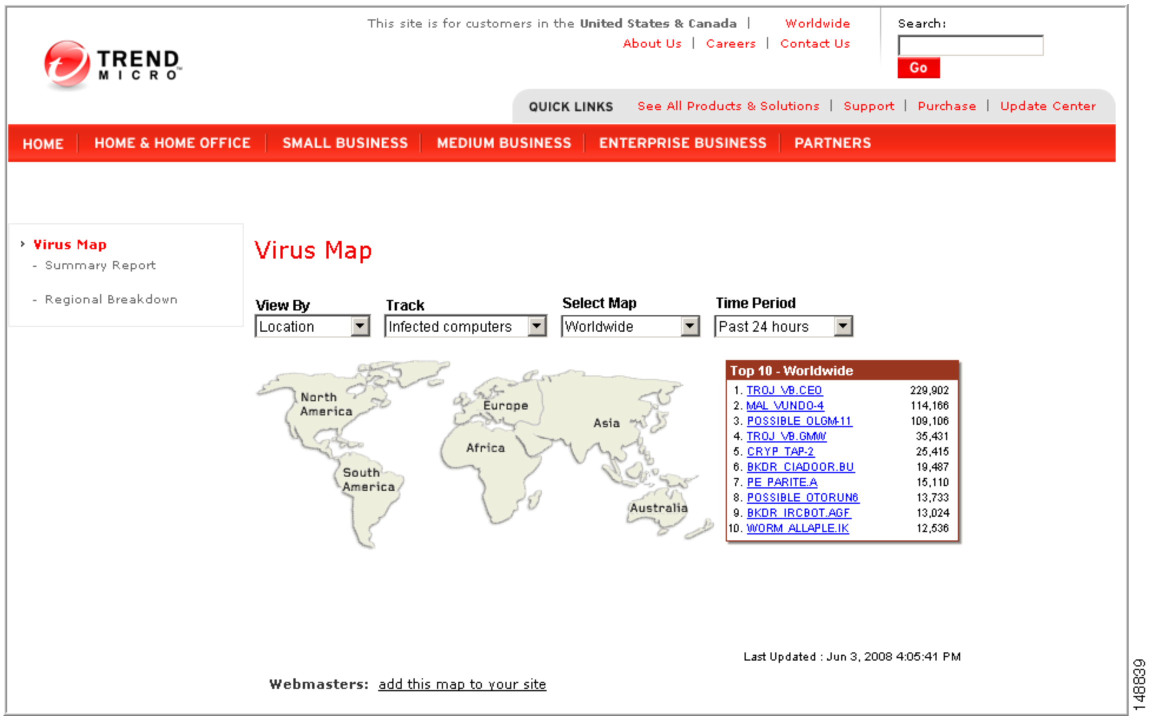
http://trendmicro.com/vinfo/

The Security Information Center provides the following information:

- Virus Encyclopedia—A compilation of knowledge about all known threats, including viruses, worms, Trojans, and others
- Security Advisories—Malware alerts, risk ratings for the most prominent risks, the most current pattern file and scan engine versions, and other helpful information
- Scams and Hoaxes—Information about malware hoaxes, scams such as chain letters or money-based hoaxes, and urban legends

- Joke Programs—A repository of information about known joke programs that are detected by the Trend Micro scan engine
- Spyware and Grayware—Information about the top ten spyware and grayware programs, and a searchable database of these programs
- Phishing Encyclopedia—A list of known phishing scams and a description of the perpetration methods
- Virus Map—A description of threats by location worldwide, shown in Figure 8-5

Figure 8-5 Virus Map


This site is for customers in the United States & Canada | Worldwide
About Us | Careers | Contact Us
Search:
Go
TREND MICRO
QUICK LINKS See All Products & Solutions | Support | Purchase | Update Center
HOME | HOME & HOME OFFICE | SMALL BUSINESS | MEDIUM BUSINESS | ENTERPRISE BUSINESS | PARTNERS
Virus Map
- Summary Report
- Regional Breakdown
Virus Map
North America
Europe
Asia
Africa
South America
Australia
Webmasters: add this map to your site
148839

View By: Location
Track: Infected computers
Select Map: Worldwide
Time Period: Past 24 hours

Top 10 - Worldwide	
1. TROJ_VB.CEO	229,902
2. MAL_VUNDO-4	114,166
3. POSSIBLE_OLGM-11	109,106
4. TROJ_VB.GMW	35,431
5. CRYP_TAP-2	25,415
6. BKDR_CIADOOR.BU	19,487
7. PE_PARITE.A	15,110
8. POSSIBLE_OTORUN6	13,733
9. BKDR_IRCBOT.AGF	13,024
10. WORM_ALLAPLE.IK	12,536

Last Updated : Jun 3, 2008 4:05:41 PM

- Weekly Virus Report—Current news about threats that have appeared in the past week (Subscribe to the Weekly Virus Report to receive a copy automatically each week via e-mail.)
- General virus information, including the following:
  - Virus Primer—An introduction to virus terminology and a description of the virus life cycle
  - Safe Computing Guide—A description of safety guidelines to reduce the risk of infections
  - Risk ratings—A description of how malware and spyware or grayware are classified as Very Low, Low, Medium, or High threats to the global IT community
- White papers—Links to documents that explain security concepts with titles such as *The Real Cost of a Virus Outbreak* or *The Spyware Battle—Privacy vs. Profits*
- Test files—A test file for testing Trend Micro InterScan for Cisco CSC SSM and instructions for performing the test
- Webmaster tools—Free information and tools for webmasters
- TrendLabs—Information about TrendLabs, the ISO 9002-certified virus research and product support center

Understanding the CSC SSM System Log Messages

This section lists the CSC SSM-related system log messages, and includes the following topics:

SSM Application Mismatch [1-105048]

Error Message `%ASA-1-105048: (`*`unit`*`) Mate's service module (`*`application`*`) is different from mine (`*`application`*`)`

Explanation The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

- *unit*—Primary or secondary
- *application*—The name of the application, such as InterScan Security Card

Recommended Action Make sure that both units have identical service modules before trying to reenable failover.

Data Channel Communication Failure [3-323006]

Error Message `%ASA-3-323006: Module in slot `*`slot`*` experienced a data channel communication failure, data channel is DOWN.`

Explanation This message indicates that a data channel communication failure occurred and the system was unable to forward traffic to the SSM. The failure triggers a failover when it occurs on the active adaptive security appliance in a failover pair. It also results in the configured fail-open or fail-closed policy being enforced on traffic that would normally be sent to the SSM. The message is generated whenever a communication problem occurs over the adaptive security appliance dataplane between the system module and the SSM. This communication problem can be caused when the SSM stops, resets, or is removed.

- *slot*—The slot in which the failure occurred

Recommended Action If this is not the result of the SSM reloading or resetting and a corresponding system log message 5-505011 does not appear after the SSM returns to an UP state, reset the module using the **hw-module module 1 reset** command.

Traffic Dropped Because of CSC Card Failure [3-421001]

Error Message `%ASA-3-421001: TCP|UDP flow from` *`interface_name:ip/port`* `to` *`interface_name:ip/port`* `is dropped because` *`application`* `has failed.`

Explanation A packet was dropped because the CSC SSM application failed. By default, this message is rate limited to one message every ten seconds.

- *interface_name*—The interface name
- *IP_address*—The IP address
- *port*—The port number
- *application*—The CSC SSM application supported in the current release

Recommended Action Immediately investigate the problem with the service module.

Drop ASDP Packet with Invalid Encapsulation [3-421003]

Error Message `%ASA-3-421003: Invalid data plane encapsulation.`

Explanation A packet injected by the service module did not have the correct data plane header. Packets exchanged on data backplane adhere to the ADSP protocol. Any packet that does not have the correct ASDP header is dropped.

Recommended Action Use the **capture name type asp-drop** [**ssm-asdp-invalid-encap**] command to capture the offending packets and contact Cisco TAC.

Traffic Dropped Because of CSC Card Failure [3-421007]

Error Message `%ASA-3-421007: TCP|UDP flow from` *`interface_name:IP_address/port`* `to` *`interface_name:IP_address/port`* `is skipped because` *`application`* `has failed.`

Explanation This message is generated when a flow is skipped because the service module application has failed. By default, this message is rate limited to one message every ten seconds.

- *IP_address*—The IP address
- *port*—The port number
- *interface_name*—The name of the interface on which the policy is applied
- *application*—The CSC SSM application supported in the current release

Recommended Action Immediately investigate the problem with the service module.

Data Channel Communication OK [1-505011]

Error Message `%ASA-1-505011: Module in slot` *`slot`* `data channel communication is UP.`

Explanation This message is generated whenever the data channel communication recovers from a DOWN state. This message indicates that data channel communication is operating normally. It occurs after the data channel communication fails and then recovers.

- *slot*—The slot that has established data channel communication.

Recommended Action If this message was generated as a result of a previous data channel communication failure (system log message 3-323006), check the SSM system log messages to determine the cause of the communication failure.

Application Reloading [1-505013]

Error Message `%ASA-1-505013: Module in slot` *slot*`, application reloading` *application*`, version` *version*

Explanation This message is generated whenever an application on the SSM is reloading. This may occur when an application needs to be restarted after a pattern or software update.

- *slot*—The slot in which the application was reloading.
- *application*—The name of the application reloading.
- *version*—The application version reloading.

Recommended Action If an upgrade was not occurring on the SSM or the application was not intentionally stopped or uninstalled, review the logs from the SSM to determine why the application stopped.

Application Down [1-505014]

Error Message `%ASA-1-505014: Module in slot` *slot*`, application down` *application*`, version` *version*

Explanation This message is generated whenever an application on the SSM is down. This may occur when an application fails to restart after a software upgrade or crash.

- *slot*—The slot in which the application was down.
- *application*—The name of the application down.
- *version*—The application version down.

Recommended Action If an upgrade was not occurring on the SSM or the application was not intentionally stopped or uninstalled, review the logs from the SSM to determine why the application stopped.

Application Up [1-505015]

Error Message `%ASA-1-505015: SSM model Module in slot number, application up application, version version`

Explanation The application running on the SSM in slot *number* is up and running.

- *SSM model*—The SSM model for the device installed in slot *number*.
- *number*—Slot 0 indicates the system main board, and slot 1 indicates the SSM installed in the expansion slot.
- *application*—The application name (string).
- *version*—The application version (string).

Recommended Action None required.

Application Version Changes [3-505016]

Error Message `%ASA-3-505016: Module in slot slot application changed from: application version version to: newapplication version newversion.`

Explanation This message is generated whenever an application version changes, such as after an upgrade. This occurs when a software update for the application on the module is complete.

- *slot*—The slot in which the application was upgraded
- *application*—The name of the application that was upgraded
- *version*—The application version that was upgraded
- *newapplication*—The new application name
- *newversion*—The new application version

Recommended Action Verify that the upgrade was expected and that the new version is correct.

Skip Non-applicable Traffic [6-421002]

Error Message `%ASA-6-421002: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port bypassed application checking because the protocol is not supported.`

Explanation The connection bypassed the service module security checking because the protocol it is using cannot be scanned by the service module. For example, the CSC SSM is not capable of scanning Telnet traffic. If the user configures Telnet traffic to be scanned, the traffic will bypass the scanning service. By default, this message is rate limited to one message every ten seconds.

- *IP_address*—The IP address
- *port*—The port number
- *interface_name*—The name of the interface on which the policy is applied

- *application*—The CSC SSM application supported in the current release

Recommended Action The configuration should be modified to only include protocols that are supported by the service module.

Account Host Toward License Limit [6-421005]

Error Message `%ASA-6-421005:` *`interface_name:IP_address`* `is counted as a user of` *`application`*

Explanation A host has been counted toward the license limit. The specified host was counted as a user of *application*. The total number of users in 24 hours is calculated at midnight for license validation.

- *interface_name*—The interface name
- *IP_address*—The IP address
- *application*—The CSC SSM application supported in the current release

Recommended Action If the overall count exceeds the user license you have purchased, contact Cisco Licensing to upgrade your license.

Daily Node Count [6-421006]

Error Message `%ASA-6-421006: There are` *`number`* `users of` *`application`* `accounted during the past 24 hours.`

Explanation This system log message identifies the total number of users who have used *application* for the past 24 hours. This message is generated every 24 hours to give the total number of hosts that have used services provided by the service module.

- *number*—The number of users counted
- *application*—The CSC SSM application supported in the current release

Recommended Action If the overall count exceeds the user license you have purchased, contact Cisco Licensing to upgrade your license.

Failed to Inject Packet [7-421004]

Error Message `%ASA-7-421004: Failed to inject {TCP|UDP} packet from` *`IP_address/port`* `to` *`IP_address/port`*

Explanation The adaptive security appliance has failed to inject a packet, as instructed by the service module. This could happen if the adaptive security appliance tries to inject a packet into a flow that has already been released or because the adaptive security appliance maintains its connection table independent of the service module.

- *IP_address*—The IP address

- *port*—The port number

Recommended Action If this affects adaptive security appliance performance, contact Cisco TAC.

Connection capacity has been reached

Error Message `The maximum number of connections for` *`protocol`* `has been reached. New connections will be kept in a backlog and may time out.`

Example:

```
The maximum number of connections for HTTP has been reached. New connections will be kept
in a backlog and may time out.
```

Explanation This system log message is generated when the CSC SSM reaches the maximum number of concurrent connections set for a given protocol.

- *protocol*—The protocol involved

Recommended Action Configure the adaptive security appliance to bypass certain traffic from CSC SSM scanning or segment the network to another adaptive security appliance.

Connection capacity has been restored

Error Message `The number of current` *`protocol`* `connections has returned to normal.`

Example:

```
ActiveUpdate: VirusScanEngine/uptodate, VirusPattern/3.189.00, AntiSpamEngine/failed,
GraywarePattern/unlicensed, PhishTrap/187
```

Explanation This system log message is generated when the number of concurrent connections has returned to a range that the CSC SSM can process promptly.

- *protocol*—The protocol involved

Recommended Action None.

CSC has actively disconnected a connection

Error Message `CSCSSM: A` *`protocol`* `session has been disconnected from the client at` *`client_ip`* `to the server at` *`server_ip`* `due to internal error or timeout.`

Example:

```
CSCSSM: A HTTP session has been disconnected from the client at 1.1.1.1 to the server at
2.2.2.2 due to internal error or timeout.
```

Explanation This system log message is generated when a socket timeout is experienced when the CSC SSM proxies a connection, or an internal problem is encountered.

- *protocol*—The protocol involved

- *client_ip*—IP address of the client
- *server_ip*—IP address of the server

Recommended Action None.

CSC SSM status message

Error Message `SysMonitor: INFO: Set CSC SSM Application Status to` *`data_channel_status.`*

Example:

```
SysMonitor: INFO: Set CSC SSM Application Status to UP.
```

Explanation This system log message is generated to indicate the current status of the CSC SSM. When the CSC SSM is healthy, the status is set to UP and traffic can be processed. When the CSC SSM is updating the configuration, or an engine or pattern, the status is set to RELOAD and the adaptive security appliance will perform a fail-open or fail-close. When the CSC SSM is unable to process traffic, the status is set to DOWN and traffic bypasses CSC SSM processing. The adaptive security appliance will perform a fail-open, fail-close, or fail-over according to how it has been configured.

- *data_channel_status*—UP, RELOAD, and DOWN

Recommended Action No action is required for UP and RELOAD status. When the status is DOWN, either restart the services on the CSC SSM or contact Cisco TAC.

Failover service communication failed

Error Message `is-failover-daemon[`*`process_id`*`]:` *`request_type`* `FAILED. Status code` *`code`*`; Status description:` *`text`*

Example:

```
is-failover-daemon[5532]: HEARTBEAT FAILED. Status code 403; Status description:
Connection or request timed out.
```

Explanation This system log message is generated when the failover daemon could not send a heartbeat to its peer to verify network connectivity.

- *process_id*—Process ID of the daemon
- *request_type*—HELLO, HEARTBEAT, SYNCH
- *code*—Status code
- *text*—Status description

Recommended Action If this error occurs while configuring CSC failover, follow the recommended action display in the Device Failover Settings screen of the CSC management console. Otherwise, check all hardware connections between the adaptive security appliances or contact Cisco TAC.

Failover service email could not be sent

Error Message `is-failover-daemon[`*`process_id`*`]: `*`action_type`*` failed notification could not be sent`

Example:

```
is-failover-daemon[5532]: HELLO failed notification could not be sent.
```

Explanation This system log message is generated when the automatic “heartbeat failure” notification e-mailed to the administrator cannot be sent.

- *process_id*—Process ID of the daemon
- *action_type*—HELLO, SYNCH

Recommended Action Restart all services on the CSC SSM, reload the CSC SSM, or contact Cisco TAC.

Failover service encountered an internal error

Error Message `is-failover-daemon[`*`process_id`*`]: Could not create failover sync server socket; Could not open failover sync server socket; Could not create failover request handler thread; Could not create failover sync server thread; Could not create failover sync server; Could not create failover IPC server thread; Could not create failover IPC server; Cannot open IPC sockets; Could not create heartbeat thread`

Example:

```
is-failover-daemon[process_id]: Could not create failover sync server socket
```

Explanation This system log message is generated when the failover service encounters an unrecoverable internal error.

- *process_id*—Process ID of the daemon

A list of possible failover daemon errors follows:

- Could not create a TCP listening socket to accept connections.
- Could not bind the SSM card management port IP address to the TCP listening socket.
- Could not start listening for connections from peers.
- Could not create a thread to service either a heartbeat or synchronization request from a peer.
- Could not create a thread to accept connections from peers.
- Could not create a server object to accept connections and handle requests from peers.
- Could not create a thread to handle IPC requests from the CSC management system.
- Could not create an IPC server object to handle IPC requests from the CSC management system.
- Could not open the IPC FIFOs to receive a request from the CSC management system to send a heartbeat or a synchronization request to the peer.

– Could not create a thread to send periodic heartbeats to a peer.

Recommended Action Restart all services on the CSC SSM, reload the CSC SSM, or contact Cisco TAC.

HTTP URL blocking event

Error Message `is-url-blocking:` *`time|blocked_url|client_ip|blocking_rule`*

Example:

```
is-url-blocking: 2007/01/01 17:10:59|blocked.com/|10.2.3.4|PhishTrap|
```

Explanation This system log message is generated when the CSC SSM detects a URL blocking event in the HTTP scanning.

- *time*—Date and time of the event
- *blocked_url*—The URL that has been blocked
- *client_ip*—IP address of the client
- *blocking_rule*—The rule that has blocked the URL

Recommended Action None.

HTTP URL filtering event

Error Message `is-url-filtering:` *`time|filtered_url|client_ip|url_category`*

Example:

```
is-url-filtering: 2007/01/01 17:10:59|forbidden.com/|10.2.3.4|Company Prohibited Sites|
```

Explanation This system log message is generated when the CSC SSM detects a URL filtering event in the HTTP scanning.

- *time*—Date and time of the event
- *blocked_url*—The URL that has been filtered
- *client_ip*—IP address of the client
- *url_category*—The category of URL blocking or filtering

Recommended Action Adjust the URL filtering setting if you want this URL category to be allowed.

IntelliTrap detection event

Error Message `is-mail-intellitrap: time | malware_name | malware_type | from_address | to_address | email_subject | action_on_the_content | action_on_the_email |`

Example

```
is-mail-intellitrap: 2006/01/01
16:33:01|PKR_TST.A|Packer|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete
|Deliver
```

Explanation This system log message is generated when the CSC SSM detects an IntelliTrap event in the connection. The infected file has been processed or blocked according to the policy setting.

- *time*—Date and time of the event
- *malware_name*—Name of the malware
- *malware_type*—Type of malware
- *from_address*—From address of the e-mail
- *to_address*—To address of the e-mail
- *email_subject*—The subject line text of the e-mail message
- *action_on_the_content*—Action taken on the e-mail content
- *action_on_the_email*—Action taken on the whole e-mail

Recommended Action If the file originated from an internal machine, perform virus scanning on that machine.

License upgrade notice

Error Message `license-upgrade-notice: Your daily node counts (`*`daily_count`*`) has exceeded your licensed seats (`*`seats`*`) by `*`offset`*`. Please upgrade your license.`

Example:

```
License-upgrade-notice: Your daily node counts (300) has exceeded your licensed seats
(100) by 200. Please upgrade your license.
```

Explanation This system log message is generated when CSC SSM detects more nodes connected to the CSC SSM than are specified in the current license. In addition to this message, a notification e-mail is sent to the administrator.

- *daily_count*—The daily node count that has connected to the CSC SSM
- *seats*—The number of seats of the CSC SSM license
- *offset*—The daily count minus the number of seats

Recommended Action Contact Cisco for a license upgrade.

Resource availability of the CSC SSM falls below the desired level

Error Message `SysMonitor: INFO: RESOURCE: *resource_name* free space *current_free_space* K is below *desired_free_space* K`

Example:

```
SysMonitor: INFO: RESOURCE: Compact Flash free space 1234K is below 5120K.
```

Explanation This system log message is generated when one of the storage spaces on the CSC SSM falls below the desired level.

- *resource_name*—The name of the resource:
- – Compact Flash
- – Active Update Temp
- – Scanning TempDir
- – Log
- *current_free_space*—Current free amount of the resource
- *desired_free_space*—Desired free amount of the resource

Recommended Action If the message is sent more than once, contact Cisco TAC.

Resource availability of the CSC SSM has been restored

Error Message `SysMonitor: INFO: RESOURCE: *resource_title* free space is back to normal (more than *desired_free_space* K)`

Example:

```
SysMonitor: INFO: RESOURCE: Compact Flash free space is back to normal (more than 5120K).
```

Explanation This system log message is generated when the CSC SSM has recovered from a previous storage shortage.

- *resource_title*—The name of the resource:
- – Compact Flash
- – Active Update Temp
- – Scanning TempDir
- – Log
- *desired_free_space*—Desired free amount of the resource

Recommended Action None.

Scan service failed

Error Message `SysMonitor: INFO: *service_title* service is DOWN, count = *counter*, restarting`

Example:

```
SysMonitor: INFO: FTP service is DOWN, count = 1, restarting
```

Explanation This system log message is generated when a scan service stops the counter increments for each restart attempt.

Recommended Action If a service goes down, restart all services by accessing the CSC SSM CLI Menu. If the failure persists, reset the CSC SSM or contact Cisco TAC.

Scan service failed to create shared memory

Error Message `ScanServer: (process ID) - CRITICAL: Scan Server unable to create shared memory for IPC. errno = system error`

Example

```
ScanServer: (7418) - CRITICAL: Scan Server unable to create shared memory for IPC. errno =
Not enough space.
```

Explanation This system log message is generated when the CSC SSM scan service cannot create shared memory necessary for scanning.

Recommended Action Restart all services on the CSC SSM or reload the CSC SSM.

Scan service failed to create sockets for scan requests

Error Message `ScanServer: (process ID) - Fatal: Unable to create socket for protocol scan requests.`

Example

```
ScanServer: (7418) - Fatal: Unable to create socket for HTTP scan requests.
```

Explanation This system log is generated when the CSC SSM scan service cannot create domain sockets to accept scan requests from the protocol daemons.

Recommended Action Restart all services on the CSC SSM or reload the CSC SSM.

Scan service failed to create worker threads

Error Message `ScanServer: (process ID) - Fatal: Unable to create worker thread pool for vsapi scans.`

Example

```
ScanServer: (7418) - Fatal: Unable to create worker thread pool for vsapi scans.
```

Explanation This system log is generated when the CSC SSM scan service cannot properly create worker threads for scanning.

Recommended Action Restart the scan service on the CSC SSM or reload the CSC SSM.

Scan service failed to load virus/spyware patterns

Error Message `ScanServer: (process ID) - Unable to update pattern. Error Code = error code`

Example

```
ScanServer: (7418) - Unable to update pattern. Error Code = -8
```

Explanation This system log is generated when the CSC SSM scan service cannot properly load the pattern files necessary for virus and spyware scanning.

Recommended Action Perform a manual update from the CSC SSM console.

Scan service failed to purge old virus/spyware patterns

Error Message `ScanServer: (process ID) - Error: Can't remove old pattern. Unable to do pattern update`

Example

```
ScanServer: (7418) - Error: Can't remove old pattern. Unable to do pattern update
```

Explanation This system log is generated when the CSC SSM scan service cannot properly discard its current set of virus and spyware patterns in order to load a new set of patterns.

Recommended Action Restart the scan service on the CSC SSM.

Scan service recovered

Error Message `SysMonitor: INFO:` *`service_title`* `service is UP.`

Example:

```
SysMonitor: INFO: FTP service is UP.
```

Explanation This system log message is generated when a scan service recovers from a previous failure.

- *service_title*—The name of the service

Recommended Action None.

Scheduled update report

Error Message `ActiveUpdate:` *`component`*`/`*`status component`*`/`*`status`*`.`

Example:

```
ActiveUpdate: VirusScanEngine/uptodate, VirusPattern/3.189.00, AntiSpamEngine/failed,
GraywarePattern/unlicensed, PhishTrap/187
```

Explanation This system log message is generated when a scheduled pattern/engine update occurs.

- *component*—The component that is updated by ActiveUpdate
- *status*—The status or version of the component

Recommended Action If you see consecutive update failures, either troubleshoot the Internet connectivity, the CSC SSM update settings, or contact Cisco TAC.

Service module cannot create FIFO

Error Message `is-service-module[`*`process_id`*`]: Cannot create` *`fifo_name`*`; Cannot open csc` *`subsystem`* `IPC fifos`

Example:

```
is-service-module[5532]: Cannot create /var/run/isvw/servmodfifo.1
```

Explanation This system log message is generated when the system is unable to create FIFOs for IPC with another CSC subsystem.

- *process_id*—Process ID of the service module
- *fifo_name*—Name of the FIFO
- *csc_subsystem*—The name of the CSC subsystem

Recommended Action Restart all services on the CSC SSM, reload the CSC SSM, or contact Cisco TAC.

Service module encountered a problem when communicating with the ASA chassis

Error Message `is-service-module[`*`process_id`*`]: Could not send the node count request to the ASA; Could not get time from the ASA; Could not send the time sync request to the ASA; ASA auto time sync failed on SSM reboot; Management port IP change report to the ASA failed; Management port IP change report failed; Could not increase the process priority`

Example:

```
is-service-module[5532]: Could not send the node count request to the ASA.
```

Explanation This system log message is generated when the Service Module fails to communicate with the adaptive security appliance chassis.

- *process_id*—Process ID

Recommended Action None.

Service module informational report

Error Message `is-service-module[`*`process_id`*`]: Software version: `*`text`*`; Increased process priority to -5; Application name: `*`text`*`; Application version: `*`text`*`; Application state: `*`up/down`*

Example:

```
is-service-module[553]: Software version: CSC SSM 6.2.xxxx.x
```

Explanation This system log message displays the CSC application name, version, and running state during Service Module startup.

- *process_id*—Process ID of the daemon
- *text*—Description of name or version
- *up/dow*n—Service is up or down

Recommended Action None.

Service module internal communication error

Error Message `is-service-module[`*`process_id`*`]: Received unrecognized `*`ipc_operation`*` request; `*`ipc_operation`*` peer closed with no request sent; Bad `*`ipc_operation`*` request from InterScan`

Example:

```
is-service-module[5532]: Received unrecognized time sync request
```

Explanation This system log message is generated when the IPC is unable to communicate with another CSC subsystem.

- *process_id*—Process ID of the service module
- *ipc_operation*—Interprocess communication (IPC) operation

Recommended Action None.

Service module show module 1 details

Error Message `is-service-module[`*`process_id`*`]: Syslog Number and Format: Software version: `*`text`*`; HTTP Service: `*`up/down`*`; Mail Service: `*`up/down`*`; FTP Service: `*`up/down`*`; Activated: `*`Yes/No`*`; Mgmt IP addr: `*`IP_address`*`; Mgmt web port: `*`port`*`; Peer IP addr: `*`ip/not_enabled`*

Example:

```
is-service-module[553]: Software version: CSC SSM 6.2.xxxx.x
```

Explanation This system log message displays the output of the **show module 1 details** command produced by the SSM.

- *process_id*—Process ID of the service module
- *text*—Description of name or version
- *up/dow*n—Service is up or down
- *yes/no*—Yes or No
- *ip_address*—IP address
- *port*—Port number
- *ip/not_enabled*—IP address or not enabled

Recommended Action None.

SMTP/POP3 anti-spam event

Error Message `is-anti-spam: `*`time`*`|`*`from_email_address`*`|`*`to_email_address`*`|`*`email_subject`*`|`*`action_on_the_content`*`|`*`action_on_the_email`*`|`

Example:

```
is-anti-spam: 2007/01/01
19:37:02|fromtester@trendmicro|totester@trendmicro.com|subject|Delete|Deliver|
```

Explanation This system log message is generated when the CSC SSM detects an anti-spam event in the SMTP or POP3 scanning. The spam mail has been processed or blocked according to the policy setting.

- *time*—Date and time of the event
- *from_email_address*—From address of the e-mail
- *to_email_address*—To address of the e-mail

- *email_subject*—The subject line text of the e-mail message
- *action_on_the_content*—Action taken on the e-mail content
- *action_on_the_email*—Action taken on the whole e-mail

Recommended Action If the spam mail is generated from a similar source, you may add this source to the Blocked Sender list to reduce the e-mail volume.

Spyware/Grayware detection event

Error Message `is-`*`mail-malwareCategory`*`:` *`time`*`|`*`malware_name`*`|`*`malware_type`*`|`*`from_address`*`|`*`to_address`*`|`*`email_subject`*`|`*`action_on_the_content`*`|`*`action_on_the_email`*`|`

Example:

```
is-mail-grayware: 2007/01/01 16:33:01|
|Spyware|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete|Deliver|
```

Explanation This system log message is generated when the CSC SSM detects a spyware or grayware event in the connection. The suspicious file has been processed or blocked according to the policy setting. The possible messages generated include the following:

- is-http-grayware
- is-http-virus
- is-ftp-grayware
- is-ftp-virus
- is-mail-grayware
- is-mail-virus

Parameters for this message are the following:

protocol—The protocol being used

malware—Grayware or virus

time—Date and time of the event

malware_name—Name of the malware

malware_type—Type of malware

from_address—From address of the e-mail

email_subject—The subject line text of the e-mail message

to_address—To address of the e-mail.

action_on_the_content—Action taken on the e-mail content.

action_on_the_email—Action taken on the whole e-mail.

Recommended Action If the file originated from an internal machine, perform virus scanning on that machine.

Syslog adaptor starting

Error Message `is-syslog: ISSyslog Adaptor 1.0`

Example:

```
is-syslog: ISSyslog Adaptor 1.0
```

Explanation This system log message is generated when the CSC SSM starts the InterScan Syslog Adaptor.

Recommended Action None.

System monitor started

Error Message `SysMonitor: INFO: SysMonitor started.`

Example:

```
SysMonitor: INFO: SysMonitor started.
```

Explanation This system log message is generated when the system monitor has started.

Recommended Action None.

Time synchronization with the ASA chassis failed

Error Message `is-service-module[`*`process_id`*`]: ASA time sync failed`

Example:

```
is-service-module[5532]: ASA time sync failed.
```

Explanation This system log message is generated when the Service Module is unable to synchronize the SSM system time with the adaptive security appliance system time.

- *process_id*—Process ID of the service module

Recommended Action None required.

Virus detection event

Error Message `is-`*`protocol`*`-virus: `*`time|malware_name|malware_type|from_address|`*
`to_address|email_subject|action_on_the_content|action_on_the_email|`

Example:

```
is-mail-virus: 2007/01/01 16:33:01|
WORM_GREW.A|Virus|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete|Deliver
|
```

Explanation This system log message is generated when the CSC SSM detects a virus event in the connection. The infected file has been processed or blocked according to the policy setting.

- *protocol*—The protocol involved
- *time*—Date and time of the event
- *malware_name*—Name of the malware
- *malware_type*—Type of malware
- *from_address*—From address of the e-mail
- *to_address*—To address of the e-mail
- *email_subject*—The subject line text of the e-mail message
- *action_on_the_content*—Action taken on the e-mail content
- *action_on_the_email*—Action taken on the whole e-mail

Recommended Action If the file originated from an internal machine, perform virus scanning on that machine.

Before Contacting Cisco TAC

Before you contact the Cisco Technical Assistance Center (TAC), check the documentation and online help to see whether it contains the information you need. If you have checked the documentation and the Knowledge Base and still need help, be prepared to give the following information to Cisco TAC:

- Product Activation Code(s)
- Version number of the product
- Version number of the pattern file and scan engine
- Number of users
- Exact text of the error message, if you received one
- Steps to reproduce the problem