CHAPTER 2

Verifying Initial Setup

This chapter describes how to verify that Trend Micro InterScan for Cisco CSC SSM is operating correctly, and includes the following sections:

- Verifying ASA Clock Setup, page 2-1
- Verifying CSC SSM Activation, page 2-1
- Verifying Scanning, page 2-2
- Testing the Antivirus Feature, page 2-3
- Verifying Component Status, page 2-4
- Viewing the Status LED, page 2-5
- Understanding SSM Management Port Traffic, page 2-6

Verifying ASA Clock Setup

To begin setup verification, you must confirm that the ASA adaptive security appliance clock has been set correctly.

To validate that the clock has been set correctly, perform these steps:

Step 1 Choose **Configuration > Properties**.

Step 2 From the Properties menu, expand the **Device Administration** topic and then click **Clock**.

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

Verifying CSC SSM Activation

Next, you must confirm that the CSC SSM has been activated correctly.

To validate that the CSC SSM has been activated correctly, perform the following steps:

Step 1 If you have physical access to the device, check the status LED on the back of the device. The status LED should be green. If the LED is amber, either solid or blinking, the card is not activated, or service has not started. For more information, see Viewing the Status LED, page 2-5.

Step 2 If you do not have physical access to the device, click the **Content Security** tab in the ASDM (see Figure 1-9 on page 1-11). You should see the device model number, management IP address, version, and other details displayed in the upper left corner. If you do not, contact Cisco TAC for assistance.

Verifying Scanning

Trend Micro InterScan for Cisco CSC SSM starts scanning for viruses and other malware as soon as you configure ASA to divert traffic to the SSM, even before you log on to the CSC SSM console. Scanning runs whether or not you are logged on, and continues to run unless you turn it off manually.

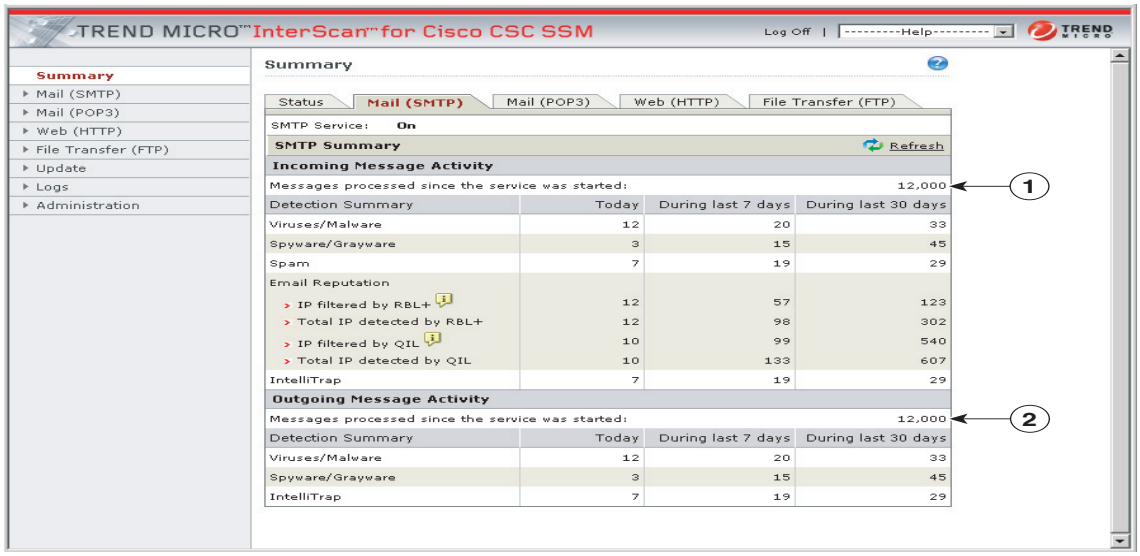
To verify that Trend Micro InterScan for Cisco CSC SSM is scanning your SMTP network traffic, perform the following steps:

Step 1 In ASDM, open the Email Scan pane of the Content Security tab. The Email Scanned Count graph should be incrementing.

Step 2 On the CSC SSM console, click the **Mail (SMTP)** tab on the Summary window and check the Messages processed since the service was started fields in the Incoming Message Activity and Outgoing Message Activity sections of the Summary - Mail (SMTP) window. For an example, see Figure 2-1.

Note You can also verify that packets have been diverted to the CSC SSM from the CLI by entering the **show service-policy csc** command. For more information, see the *Cisco Security Appliance Command Line Configuration Guide*.

Figure 2-1 Verify Scanning on the Summary Window



1	Incoming message activity counter	2	Outgoing message activity counter

The message activity counters increment as traffic passes through your network.

Step 3 Click the **Refresh** link to update the counters.

Note The counters also reset whenever service is restarted.

Step 4 Click the **Mail (POP3)** tab to perform a similar test for POP3 traffic, or view the Email Scanned Count graph in ASDM, which includes counters for POP3 traffic.

Testing the Antivirus Feature

The European Institute for Computer Antivirus Research (EICAR) has developed a harmless test virus that is detected as a real virus by antivirus technology, such as Trend Micro InterScan for Cisco CSC SSM. The test virus is a text file with a .com extension that does not contain any fragments of viral code. Use the test virus to trigger an incident and confirm that e-mail notifications and virus logs work correctly.

To test the antivirus feature, perform the following steps:

Step 1 Open a browser window and go to the following URL:

http://www.eicar.com/anti_virus_test_file.htm

Step 2 Locate the EICAR Download Area shown in Figure 2-2.

Figure 2-2 EICAR Download Area

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

(Note: For the time being we make use of a self-signed certificate. You may be asked by your browser whether you trust this site. Depending on acceptance of this new service we may install a certificate coming from a trusted Certificate Authority at a later point in time.)

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Step 3 Click the **eicar.com** link.

You should receive an immediate notification in your browser that a security event has occurred.

Step 4 On the CSC SSM console, query the virus or malware log file by choosing **Logs > Query** to see the test virus detection recorded in the log.

In addition, a notification has been sent to the administrator e-mail address that you entered during installation on the **Host Configuration** installation window.

If you do not receive an e-mail notification, possible causes may be one of the following:

- The CSC SSM is not activated. Verify that the device has been activated according to the information in Verifying CSC SSM Activation, page 2-1.
- There may be a misconfiguration on the adaptive security appliance. For more information, see Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration, page 8-10.
- The CSC SSM is in a failed state. For example, it is rebooting or a software failure has occurred. If this is the case, the system log message 421007 is generated. Check your system log messages to see whether this error occurred. Before contacting Cisco TAC, see Scanning Not Working Because the CSC SSM Is in a Failed State, page 8-10 for more information.

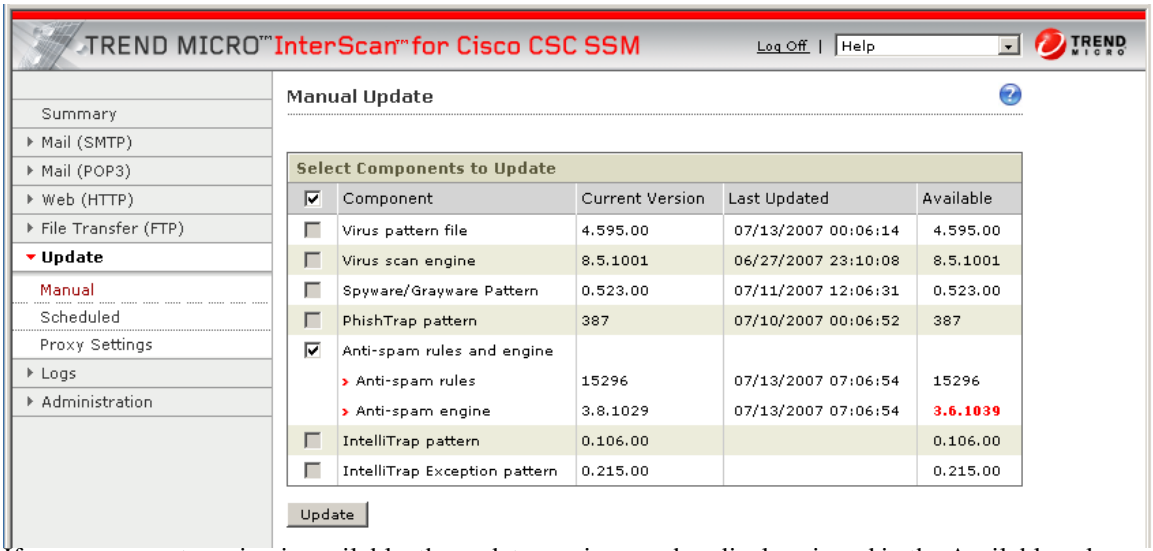
Verifying Component Status

You must confirm that you have the most current antivirus components.

To determine whether you have the most current virus pattern file and scan engine, spyware pattern file, PhishTrap pattern, anti-spam rules, and anti-spam engine, perform the following steps:

Step 1 In the CSC SSM console, click **Update > Manual** to display the Manual Update window, shown in Figure 2-3.

Figure 2-3 Manual Update Window



Step 2 If a more current version is available, the update version number displays in red in the Available column. Choose those components you want to update and click **Update** to download the most recent versions.

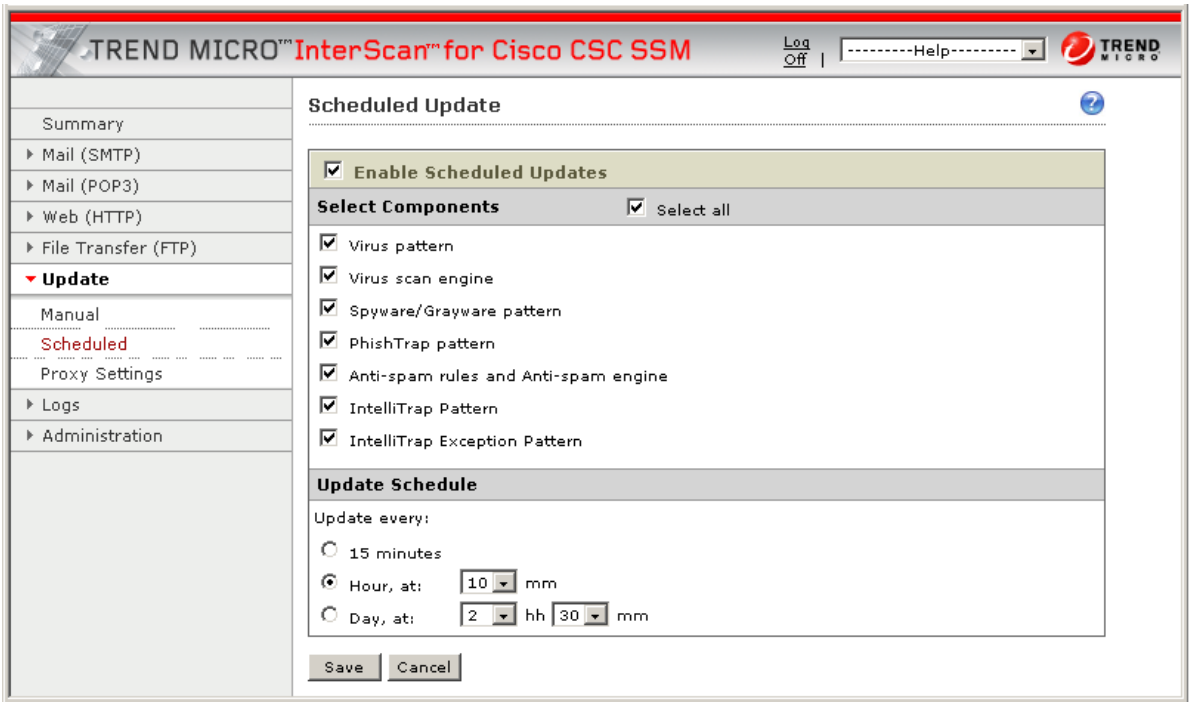
If the current and available versions are the same, and you think a new version is available, or if the Available column is blank, it could mean one of the following:

- The Trend Micro ActiveUpdate server is down.
- A network problem has occurred.

- There are no new components available; everything is current.
- Trend Micro InterScan for Cisco CSC SSM is not configured correctly.

Step 3 To avoid uncertainty, choose **Update > Scheduled** to display the Scheduled Update window, shown in Figure 2-4.

Figure 2-4 Scheduled Update Window

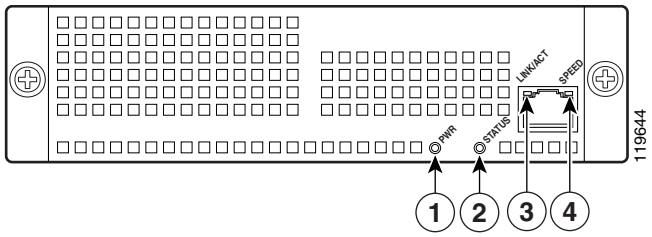


By default, Trend Micro InterScan for Cisco CSC SSM updates components periodically, with an automatic notification after a scheduled update has occurred. You can modify the scheduled update interval.

Viewing the Status LED

On the back of the security appliance, locate the Status LED in the ASA SSM indicators shown in Figure 2-5.

Figure 2-5 ASA SSM Indicators



The Status LED is labeled **2**. The Status LED can be in several different states, which are described in Table 2-1.

Table 2-1 ASA SSM LED Indicators

No.	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green & Amber	Flashing	The SSM is running and activated, but scanning service is down. If the flashing continues for over a minute, either the CSC SSM is loading a new pattern file or scan engine update, or you may need to troubleshoot to locate the problem.
		Green	Solid	The SSM is booted up, but it is not activated.
		Amber	Solid	The SSM has passed power-up diagnostics. This is the typical operational status.
3	LINK/ACT	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Green	100 MB	There is network activity.
		Amber	1000 MB (Gigabit-Ethernet)	There is network activity.

Note The LEDs labeled **1**, **3**, and **4** are not used by the CSC SSM software.

Understanding SSM Management Port Traffic

During installation (on the IP Configuration installation window), you chose an IP address, gateway IP address, and mask IP address for your management interface. The traffic that uses the SSM management port includes the following:

- ActiveUpdate—The communication with the Trend Micro update server, from which Trend Micro InterScan for Cisco CSC SSM downloads new pattern files and scan engine updates.
- URL rating lookups—The downloading of the URL filtering database, which is used if you purchased the Plus License to perform URL blocking and filtering.
- Syslog—Uploading data from Trend Micro InterScan for Cisco CSC SSM to the syslog server(s).
- E-mail notifications—Notifications of trigger events such as virus detection.
- DNS lookup—Resolving the host name used for pattern file updates and looking up the Trend Micro server IP address.
- Cisco ASDM or Trend Micro GUI access—The communication between the Cisco ASDM interface and the Trend Micro InterScan for Cisco CSC SSM interface.