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:

Verify ASA Clock Setup

To begin setup verification, first confirm that the ASA clock has been set correctly. To do so, click **Configuration > Properties**. From the Properties menu, expand the Device Administration topic and click **Clock**. For more information, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Verify CSC SSM Activation

Next, verify that the CSC SSM has been correctly activated. 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 is not started. See View the Status LED, page 2-5 for more information.

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

Verify Scanning

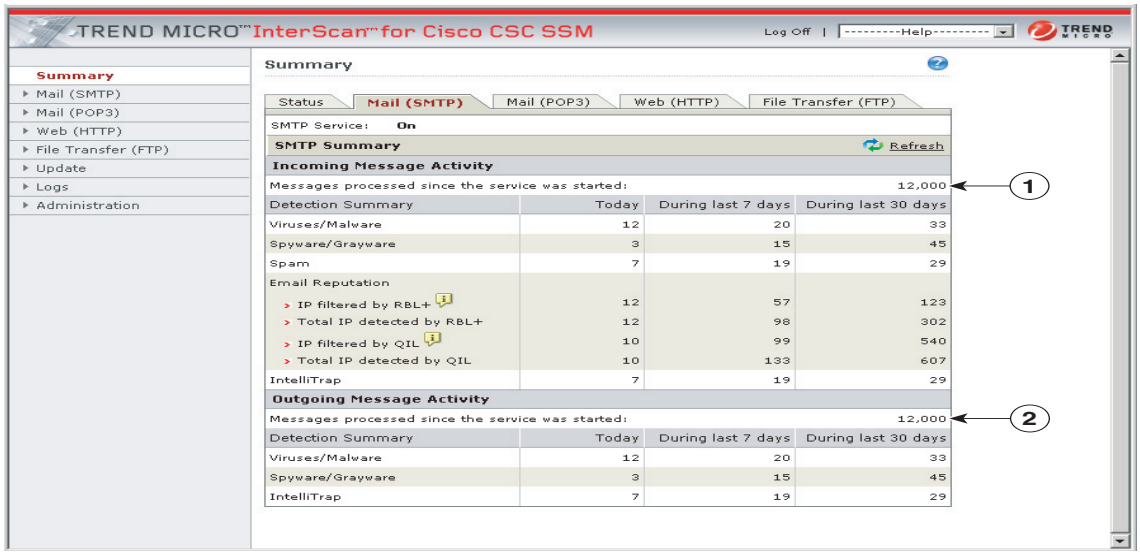
Trend Micro InterScan for Cisco CSC SSM starts scanning for viruses and other malware as soon as you configure ASA to divert traffic to the SSM, even before you log on to the CSC SSM console. Scanning runs whether or not you are logged on, and continues to run unless you manually turn it off.

To verify that Trend Micro InterScan for Cisco CSC SSM is scanning your SMTP network traffic:

- In ASDM, look at the Email Scan pane of the Content Security tab. The Email Scanned Count graph should be incrementing.
- In the CSC SSM console, click the **Mail (SMTP)** tab on the Summary window. Look at 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 are diverted to the CSC SSM from the command-line interface. Use the **show service-policy csc** command. See the *Cisco Security Appliance Command Line Configuration Guide* for more information.

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. Click the Refresh link to update the counters.

Note The counters also reset whenever service is restarted.

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

Test 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 a virus incident and confirm that email notifications and virus logs work properly.

To perform the test, open a browser window and go to the following URL:

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

Scroll down until you see the information box shown in Figure 2-2.

Figure 2-2 EICAR Download Area

Click the eicar.com link. You should get an immediate notification in your browser that a security event has occurred. You should now be able to query the virus/malware log file by navigating in the CSC SSM console to **Logs > Query** to see the test virus detection recorded in the log. Also, a notification is sent to the administrator email address that you chose during installation (on the **Host Configuration** installation window).

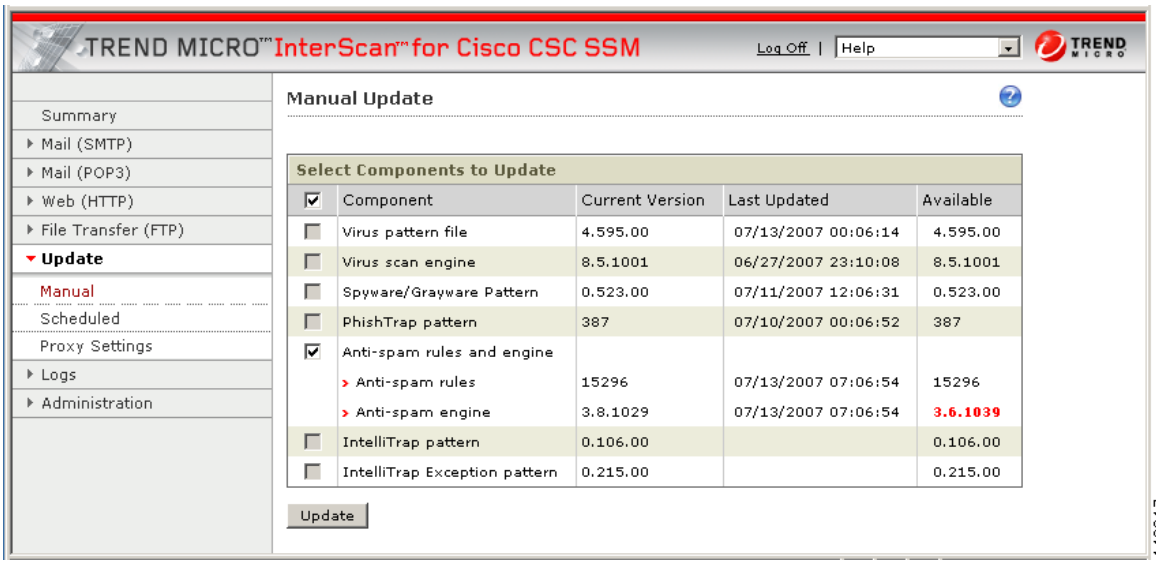
If this does not happen:

1. It is possible that the CSC SSM is not activated. Verify that the device is activated per the information in Verify CSC SSM Activation, page 2-1.
2. There may be a misconfiguration on ASA. See Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration, page 8-10 for more information.
3. CSC SSM is in a failed state, for example, it is in the process of rebooting or a software failure has occurred. If this is the case, a syslog error 421007 is generated. Check your syslog to see if this error is present. Also see Scanning Not Working Because the CSC SSM Is in a Failed State, page 8-10 for more information before contacting Cisco TAC.

Verify Component Status

To find out whether you have the most current virus pattern file and scan engine, spyware pattern file, PhishTrap pattern, anti-spam rules, and anti-spam engine, 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



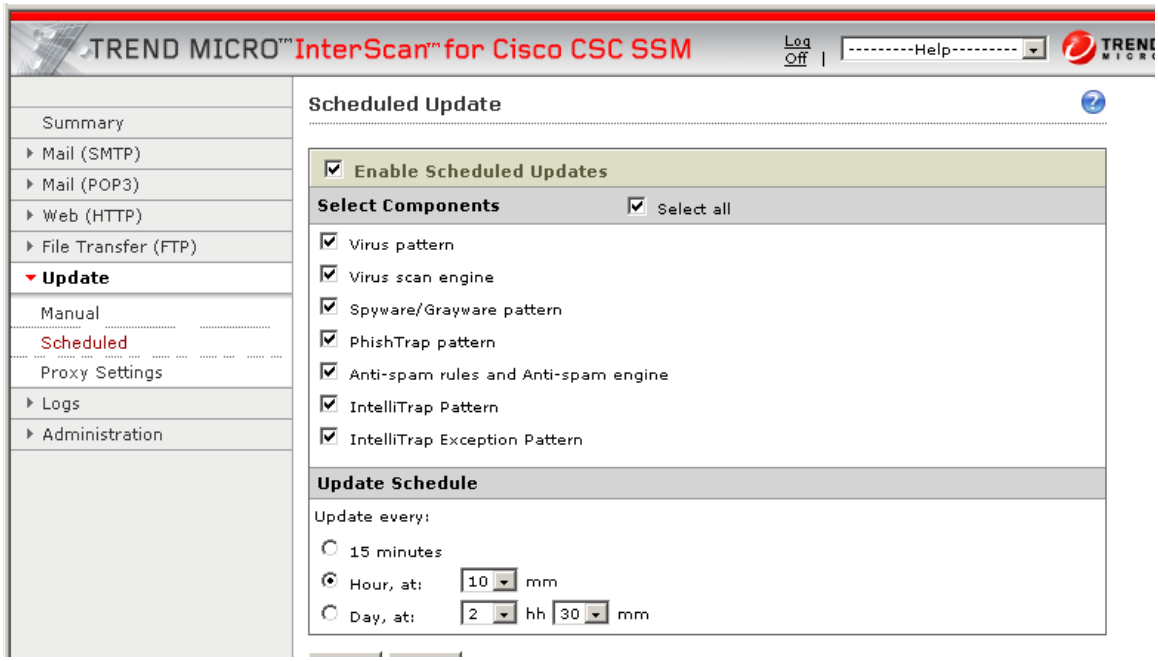
If a more current version is available, the update version number displays in red in the **Available** column. Choose components to be updated and click **Update** to download the most recent version of the selected component.

Tip If the current and available versions are the same, and you suspect there's a new version available, or if the **Available** column is blank, it could mean one of the following:

1. The Trend Micro ActiveUpdate server is down.
2. There's a network problem.
3. There are no new components available; everything really is current.
4. Trend Micro InterScan for Cisco CSC SSM is not configured correctly.

To help avoid the uncertainty, click **Update > Scheduled** to display the Scheduled Update window, shown in Figure 2-4.

Figure 2-4 Scheduled Update Window

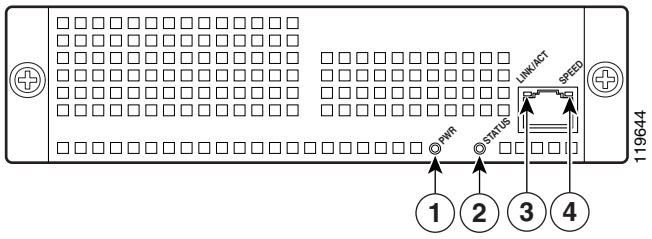


By default, Trend Micro InterScan for Cisco CSC SSM updates components periodically, with an automatic notification after a scheduled update has taken place. You can modify the scheduled update interval to occur more or less frequently.

View the Status LED

On the back of the 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**. There are several states for the **Status** LED, which are described in the following table.

Table 2-1 ASA-SSM Indicators

	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/scan engine update, or you may need to troubleshoot for a problem.
		Green	Solid	The SSM is booted up but it not activated.
		Amber	Solid	The SSM has passed power-up diagnostics. This is the typical operational status.
3	LINK/ACT	Green	Solid	There is 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.

Understand SSM Management Port Traffic

During installation (on the IP Configuration installation window), you chose an IP address, gateway IP, and mask IP for your management interface. Here is a list of traffic that uses the management port:

- **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 utilized if you purchased the Plus License to perform URL blocking and filtering
- **Syslog**—This port is used to upload data from Trend Micro InterScan for Cisco CSC SSM to the syslog server(s)
- **Email notifications**—Notifications of trigger events such as a virus detection are sent via the SSM management port
- **DNS lookup**—The management port is also used for resolving the host name used for pattern file updates and to look up the Trend Micro server IP
- **Cisco ASDM/Trend Micro GUI access**—The management port enables communication between the Cisco ASDM interface and the Trend Micro InterScan for Cisco CSC SSM interface