Cisco Content Security and Control SSM Administrator Guide

Version 6.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8628-02

Cisco Content Security and Control SSM Administrator Guide

CONTENTS

Preface

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introducing the Content Security and Control SSM

This chapter introduces the Content Security and Control Security Services Module (CSC SSM), and includes the following sections:

Overview

Trend Micro InterScan for Cisco CSC SSM (Content Security and Control Security Services Module) provides an all-in-one antivirus and spyware management solution for your network. This guide provides a conceptual explanation of how to manage the CSC SSM, which is resident in your Cisco appliance to do the following:

- Detect and take action on viruses, worms, Trojans, and other threats in your SMTP, POP3, HTTP, and FTP network traffic

Note Traffic utilizing other protocols, such as HTTPS, is not scanned by CSC SSM.

- Block compressed or very large files that exceed specified parameters
- Scan for and remove spyware, adware, and other types of grayware

The above features are available to all customers with the Base License for the CSC SSM software. If you purchased the Plus level of the CSC SSM license in addition to the Base License, you can also:

- Reduce spam and protect against phishing fraud in your SMTP and POP3 traffic
- Set up content filters that enable you to allow or prohibit email traffic containing key words or phrases

- Block URLs that you do not want employees to access, or URLs that are known to have hidden or malicious purposes
- Filter URL traffic according to predefined categories that you allow/disallow, such as adult/mature content, games, chat/instant messaging, or gambling sites

See the "Licensing" section on page 1-11 for more information about the Base License and Plus License.

To start scanning traffic, you need to create one or more service policy rules to send traffic to CSC SSM for scanning. Refer to the ASA 5500 series security appliance documentation for information about how to create service policy rules using th e command line or using ASDM.

With Trend Micro InterScan for Cisco CSC SSM, you do not have to install separate applications for virus protection, spyware blocking, spam detection, or content filtering—all of these functions are available in a single package. Trend Micro InterScan for Cisco CSC SSM provides protection for major traffic protocols—SMTP, HTTP, and FTP, as well as POP3 traffic, to ensure that employees don't accidentally introduce viruses from their personal email accounts. And, the application is easy to maintain.

For information about installing the appliance, see your Cisco documentation. A setup wizard guides you through the installation process.

This guide familiarizes you with the Trend Micro InterScan for Cisco CSC SSM user interface, and describes configuration settings that you may want to fine-tune after installation. This guide does not include a field-by-field description of windows in the user interface. For a description of fields on a specific window, see the CSC SSM online help.

Features and Benefits

Trend Micro InterScan for Cisco CSC SSM helps you manage threats to your network. Table 1-1 provides an overview of the features and benefits:

Table 1-1 Features and Benefits

Features
Scans for traffic containing viruses, and manages infected messages and files
Scans for spam at low to high threshold levels, and allows you to determine how spam is handled
Filters offensive or inappropriate content
Blocks incoming file types that can damage your network
Helps prevent Denial of Service attacks by setting limits on message size
Provides approved senders and blocked senders functionality for file and URL blocking
Filters access to URLs by category
Blocks connections to URLs or FTP sites prohibited by your corporate policies
Benefits
Allied with powerful Cisco firewall protection, Trend Micro InterScan for Cisco CSC SSM secures your network from threats, spam, and unwanted content
Easy to install with a user-friendly setup program
Antivirus, spyware/grayware detection, file blocking, and other protections against security risks in your network traffic is integrated with ASDM

Table 1-1 Features and Benefits (continued)

Features
Allows you to fine-tune configuration of the scanning, anti-spam, and filtering features after installation
Can be configured to automatically update the virus pattern file, scan engine, and spam-detection components when a new version becomes available from Trend Micro
Provides email and syslog notifications to make sure you stay informed of activity
Provides log files that are purged automatically after 30 days
Provides a user-friendly console that includes online help to guide you through tasks
Automatically displays a notification when your license is about to expire

Available Documentation

The documentation for this product assumes that you are a system administrator who is familiar with the basic concepts of managing firewalls and administering a network. It is also assumed that you have privileges to manage the security applications in your network.

Before proceeding, you might also want to read *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*. The *Quick Start Guide* includes documentation for installing the CSC SSM if the appliance you purchased does not have the SSM already installed.

The documentation available for Trend Micro InterScan for Cisco CSC SSM includes the following:

- This document—*Cisco Content Security and Control SSM Administrator Guide*
- Online Help—Two kinds of online help are available:
  - Context-sensitive screen help, which explains how to perform tasks in one window
  - General help, which explains tasks that require action in several windows, or peripheral knowledge needed to complete tasks
- Knowledge Base—An online database of problem-solving and troubleshooting information. Knowledge Base provides the latest information about known product issues. To access the Knowledge Base, visit:

  kb.trendmicro.com/solutions/solutionSearch.asp

Important Terms

Terms are used throughout the documentation and online help that may not be familiar to you, or may be used in an alternate way from what you might expect. A definition of terms is available in the Glossary.

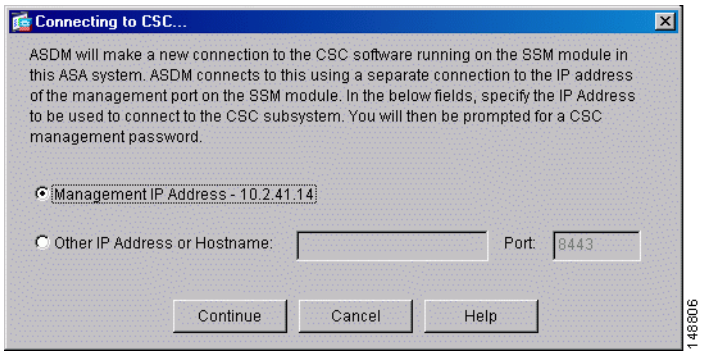
Introducing the ASDM Content Security Tab

The ASDM Home page features a tab called Content Security. The main ASA system home page is the default view. Click the Content Security tab to view a summary of CSC SSM activity.

You are prompted for a connection to the CSC SSM. A dialog box appears, allowing you to choose the IP address that ASDM is aware of, or an alternate. The alternate might be used if you are accessing ASDM through a NAT device, where the IP address of the CSC SSM that is visible from your computer is different from the actual IP address of the CSC SSM management port.

The dialog box appears as follows:

Figure 1-1 Prompt to Connect to CSC SSM



Click **Continue** after choosing the localhost or the alternate. Next, you are prompted to enter your CSC SSM password, configured during installation. Enter the password and click **OK**.

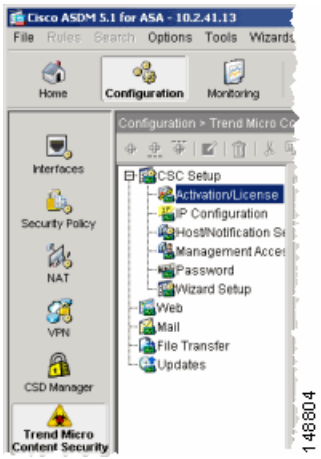
The Content Security tab appears. See Features of the Content Security Tab, page 7-1 for more information.

Configuring Content Security

From the ASDM console, click **Configuration > Trend Micro Content Security** to display the configuration options. These options are:

- CSC Setup—Launch the Setup Wizard to install and configure CSC SSM
- Web—Configure Web scanning, file blocking, URL filtering, and URL blocking
- Mail—Configure scanning, content filtering, and spam prevention for incoming and outgoing SMTP and POP3 mail
- File Transfer—Configure file scanning and blocking
- Updates—Schedule updates for content security scanning components (virus pattern file, scan engine, and so on)

Figure 1-2 Configuration Options on ASDM



The Setup options are described in the *Cisco ASA5500 Adaptive Security Appliance Getting Started Guide*. Also, see the online help for more detailed information about each of these options.

The Web, Mail, File Transfer, and Updates options are described in more detail in other chapters of this *Administrator Guide*:

- Web configuration—see Chapter 4, "Configuring Web (HTTP) and File Transfer (FTP) Traffic"
- Mail configuration—see Chapter 3, "Configuring Mail Traffic (SMTP and POP3)"
- File Transfer configuration—see Chapter 4, "Configuring Web (HTTP) and File Transfer (FTP) Traffic"
- Updates—see Chapter 5, "Managing Updates and Log Queries"

Introducing the CSC SSM Console

After you have successfully installed Trend Micro InterScan for Cisco CSC SSM, and have configured ASA to send traffic to CSC SSM, the virus scanning and detection feature is activated and your network traffic is being scanned using the default settings. Additional features, such as spyware/grayware detection, are not enabled by default and can be configured in the CSC SSM interface.

To enter the CSC SSM interface, click **Configuration > Trend Micro Content Security.** From the Configuration menu (shown in Figure 1-2), select a task. For example, to configure Web scanning, select **Web** from the **Configuration > Trend Micro Content Security** menu. On the right side of the Configuration window (not shown in Figure 1-2) are links to perform the task of interest. For example, clicking the Configure Web Scanning link takes you to the **HTTP Scanning** screen in the CSC SSM interface, where you can configure Web scanning settings.

The first time you log in to the CSC SSM interface, ASDM displays a security certificate, followed by the **Connecting to CSC <link name>** screen. If you leave the CSC SSM interface and then return without logging out of ASDM, only the security certificate displays.

The CSC SSM interface displays in a browser window. The default view in the Trend Micro InterScan for Cisco CSC SSM console is context-sensitive, depending on the link selected. For example:

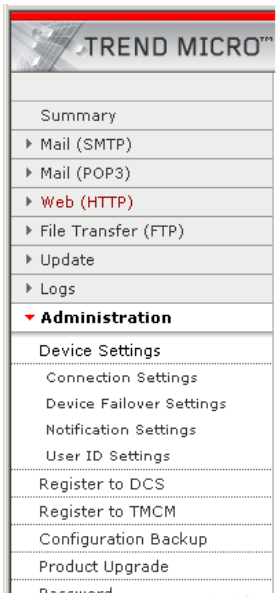
Figure 1-3 HTTP Scanning Window Displays When You Click the Configure Web Scanning Link

To log off, click **Log Off**, which appears in the screen header as shown in Figure 1-3. Then close the browser window.

Navigation Panel

The left pane of the Trend Micro CSC SSM console is the main menu, which also serves as a navigation pane. Click a selection in the navigation pane to open the corresponding window. A selection is compressed when the arrow is pointing right, a selection is expanded when the arrow is pointing down. The corresponding panes do not refresh until you click a selection on the navigation pane.

Figure 1-4 Navigation Pane in the Trend Micro CSC SSM Console



The pathname **Mail (SMTP) > Scanning > Incoming > Action**, indicates the following:

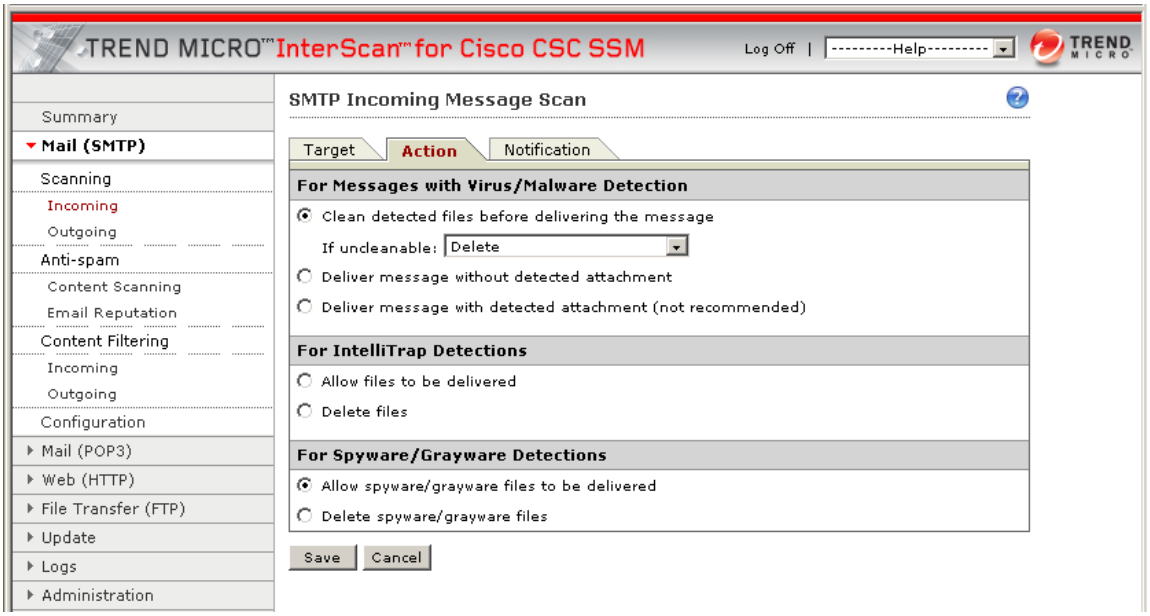
- The main selection in the navigation pane is Mail (SMTP)
- The secondary selection is Scanning
- The tertiary selection is Incoming
- The selected tab on the SMTP Incoming Message Scan screen is the Action tab

Tab Behavior

The interactive screens for your selection display on the right side of the CSC SSM console. Most windows in the user interface have multiple views. For example, the SMTP Incoming Message Scan window has 3 views; Target, Action, and Notification. Switch between views by clicking the appropriate tab for the information to be viewed.The active tab name appears in reddish-brown; inactive tab names appear in black text.

Typically the tabs are related and work together. For example, in the following figure, all three tabs are needed to configure virus scanning of incoming SMTP traffic.

Figure 1-5 Tabs Work Together



- **Target**—Allows you to define the scope of activity to be acted upon
- **Action**—Allows you to define the action to be taken when a trigger event has taken place—examples of actions are clean or delete
- **Notification**—Allows you to compose a notification message, as well as define who is notified of the event and the action

For related tabs such as these, clicking **Save** once saves work on all three tabs.

Save Button

The appearance of the **Save** button indicates whether saving is necessary. The **Save** button is unavailable when the window first opens. After you perform tasks on the window, the appearance of the **Save** button changes so the text on the button appears black instead of gray. This is an indication that a **Save** is necessary to validate the work you have done.

Default Values

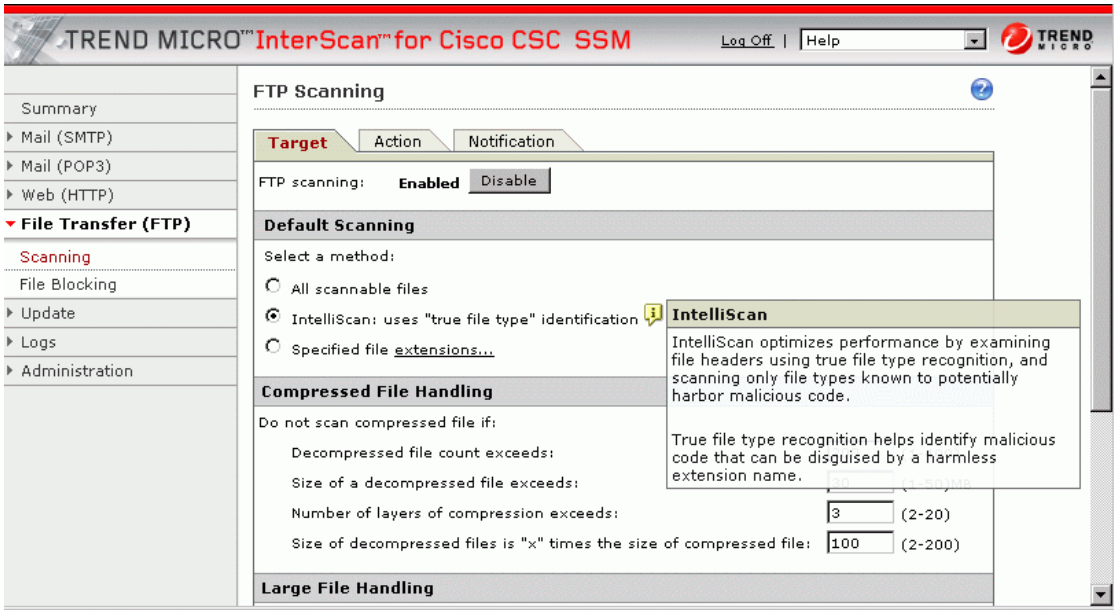
Many windows in the Trend Micro for Cisco CSC SSM user interface include fields that contain default selections. A default selection represents the choice that is best for most users, but you are free to change the default if another choice is better for your environment. Consult the online help for more information about entries in a particular field.

Fields that allow you to compose a notification contain a default message. You can change default notifications by typing over the existing entry.

Tooltip Icons

Some windows in the CSC SSM console contain an information icon called a tooltip. Position your mouse over the tooltip icon to display a popup text box with additional information that helps you make a decision or complete a task. In the following example, mousing over the tooltip icon displays more information about IntelliScan, one of several virus scanning options.

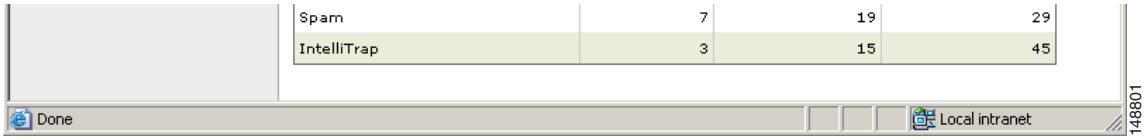
Figure 1-6 Information Icon (Tooltip)



Online Help

There are two types of online help available with Trend Micro InterScan for Cisco CSC SSM. These are general help, and context-sensitive help.

Figure 1-7 General and Context-sensitive Online Help



1	Help drop-down menu	**2**	Help icon

Invoke general help by clicking the Contents and Index tabs from the Help drop-down menu in the Trend Micro InterScan for Cisco CSC SSM banner. A secondary browser window opens, which allows you to view the help contents. Click the plus symbol to expand a help topic.

Figure 1-8 Online Help Contents

Following an introduction, the organization of the online help topics mimics the organization of the left menu in the user interface. Some helpful information about computer viruses is available at the end of the online help contents.

Click the **Index** tab to view the online help index, or click **Search** to search for information using a keyword.

To invoke context-sensitive help, click the window help icon ( ). A secondary browser window appears, which includes information for the window that you are currently viewing in the user interface.

Links in Online Help

The online help contains links, indicated by blue underlined text. Clinking a link either takes you to another help window or displays a popup text box with additional information, such as a definition. Disable popup blocking in your browser to use this feature of the online help.

Most of the documentation in the online help is not repeated in this *Administrator Guide*. Be sure to read the online help for more information about Trend Micro InterScan for Cisco CSC SSM.

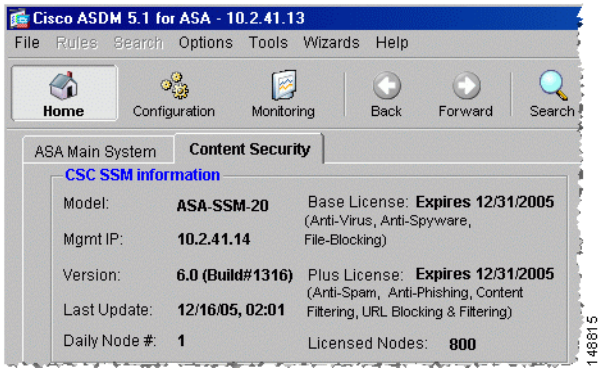
Licensing

As described in the introduction to this chapter, there are two levels of the Trend Micro InterScan for CSC SSM license; the Base License and the Plus License. The Base License provides antivirus, anti-spyware, and file blocking capability. The Plus License adds anti-spam, anti-phishing, content filtering, URL blocking, and URL filtering capability. The Base License is required for Plus license activation.

If you purchased only the Base License, you may be able to view unlicensed features via the CSC SSM console, but unlicensed features are not functional. You can, however, view online help for an unlicensed feature. You can also purchase the additional functionality offered with the Plus License at a later time.

If you are not sure which level of the license your organization purchased, look at the CSC SSM Information section of the Content Security tab. Your license information is summarized there.

Figure 1-9 Location of License Information on the Content Security Tab



Alternatively, in the CSC SSM console, click **Administration > Product License** to display the Product License window. Scroll to the Plus License section of the window, and check the **Status** field. If this field contains "Activated," you have the Plus License functionality. Otherwise this field indicates "Not Activated."

Windows That Require Plus Licensing

Table 1-2 indicates which windows in the CSC SSM console are functional under the Base License only, and which are functional only when you purchase the additional Plus License.

Table 1-2 Windows Available versus Licenses

Screen Title	Base License	Plus License
Summary > Status/Mail (SMTP)/Mail (POP3)/Web (HTTP)/File Transfer (FTP)	X	
Mail (SMTP) > Scanning > Incoming > Target/Action/Notification	X	

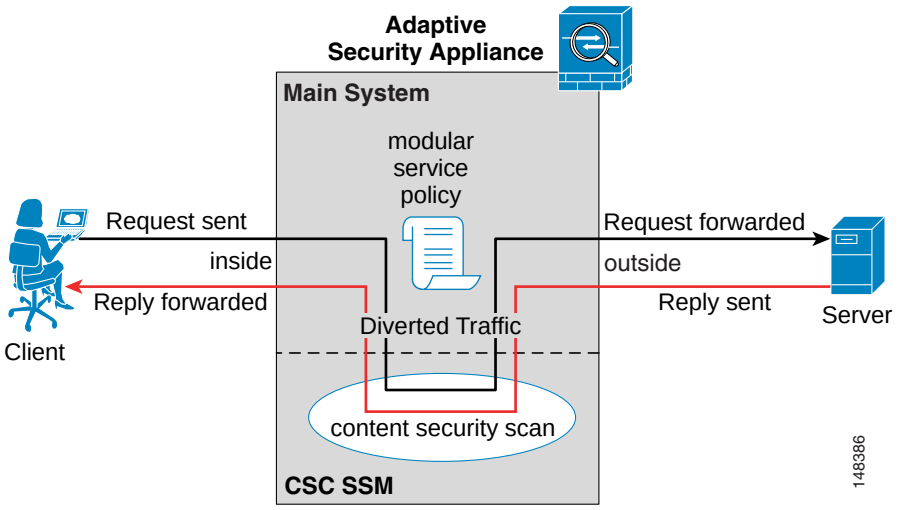
Table 1-2 Windows Available versus Licenses (continued)

Screen Title	Base License	Plus License
Mail (SMTP) > Scanning > Outgoing > Target/Action/Notification	X	
Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam Target/Action		X
Mail (SMTP) > Content Filtering > Incoming > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Content Filtering > Outgoing > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Configuration > Message Filter/Disclaimer/Incoming Mail Domain	X	
Mail (POP3) > Scanning > POP3 Scanning > Target/Action/Notification	X	
Mail (POP3) > Anti-spam > POP3 Anti-spam Target/Action		X
Mail (POP3) > Content Filtering > POP3 Content Filtering Target/Action/Notification		X
Web (HTTP) > Scanning > Target/Webmail Scanning/Action/Notification	X	
Web (HTTP) > File Blocking > Target/Notification	X	
Web (HTTP) > URL Blocking > Via Local List/PhishTrap/Notification		X
Web (HTTP) > URL Filtering > Filtering Rules		X
Web (HTTP) > URL Filtering > Settings > URL Filtering Settings URL Categories/Exceptions/Schedule/Re-classify URL		X
File Transfer (FTP) > Scanning > FTP Scanning Target/Action/Notification	X	
File Transfer (FTP) > File Blocking> Action/Notification	X	
Update > all screens	X	
Logs > all screens	X	
Administration > all screens	X	

Process Flow

Figure 1-10 illustrates the flow of traffic when the CSC SSM is installed in your security appliance. A request is sent from a client workstation to a server. As the request is processed through the security appliance, it is diverted to CSC SSM for content security scanning. If no security risk is detected, the request is forwarded to the server. The reply follows the same pattern in reverse.

Figure 1-10 Process Flow



If a security risk is detected, it can be cleaned or removed, depending on how CSC SSM is configured.

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

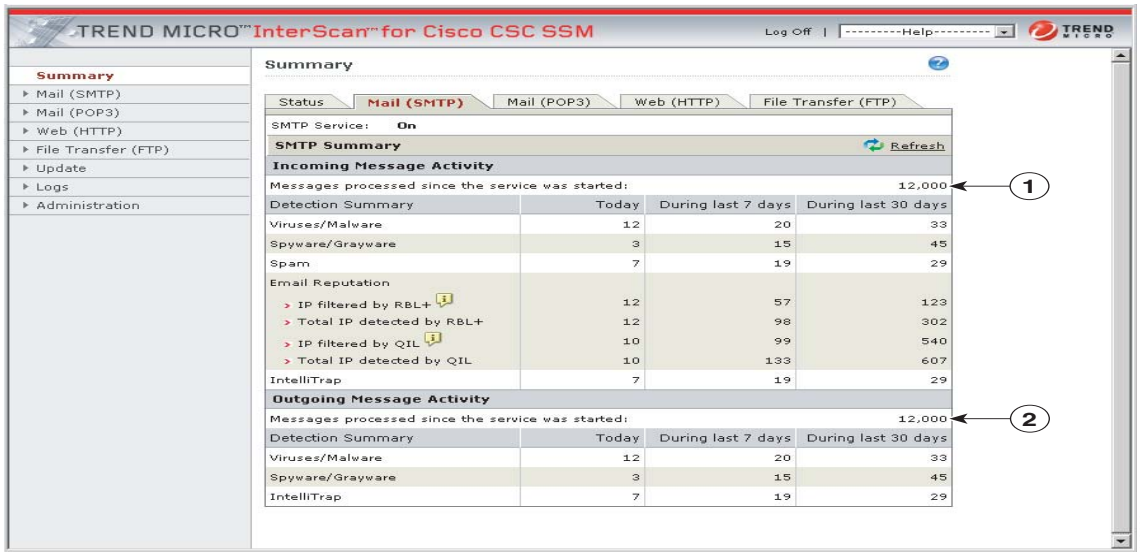
Trend Micro InterScan for Cisco CSC SSM starts scanning for viruses and other malware as soon as you configure ASA to divert traffic to the SSM, even before you log on to the CSC SSM console. Scanning runs whether or not you are logged on, and continues to run unless you manually turn it off.

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).

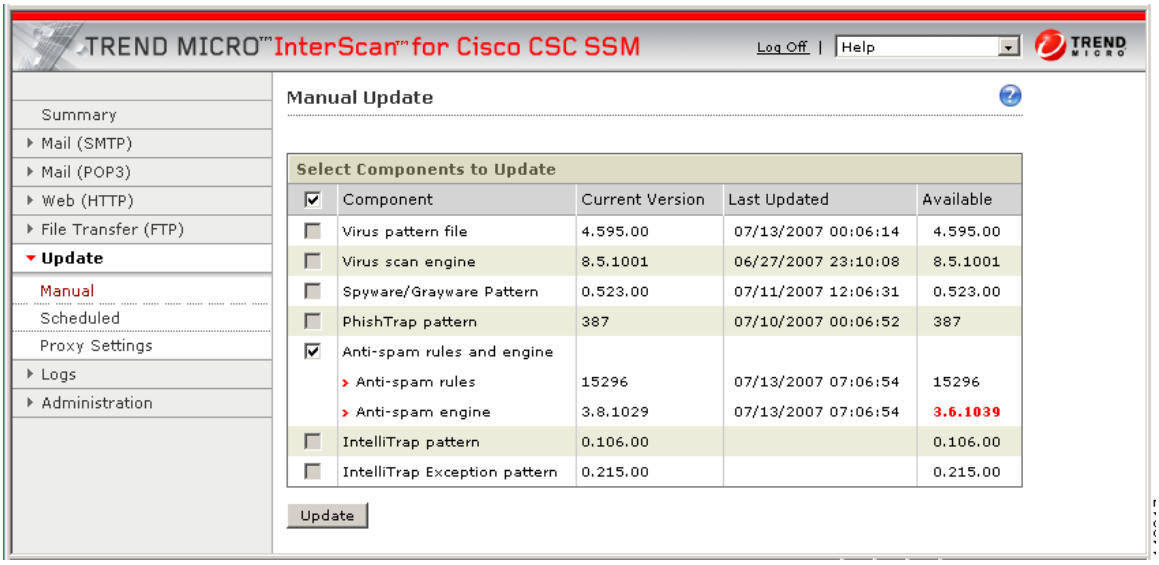
If this does not happen:

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



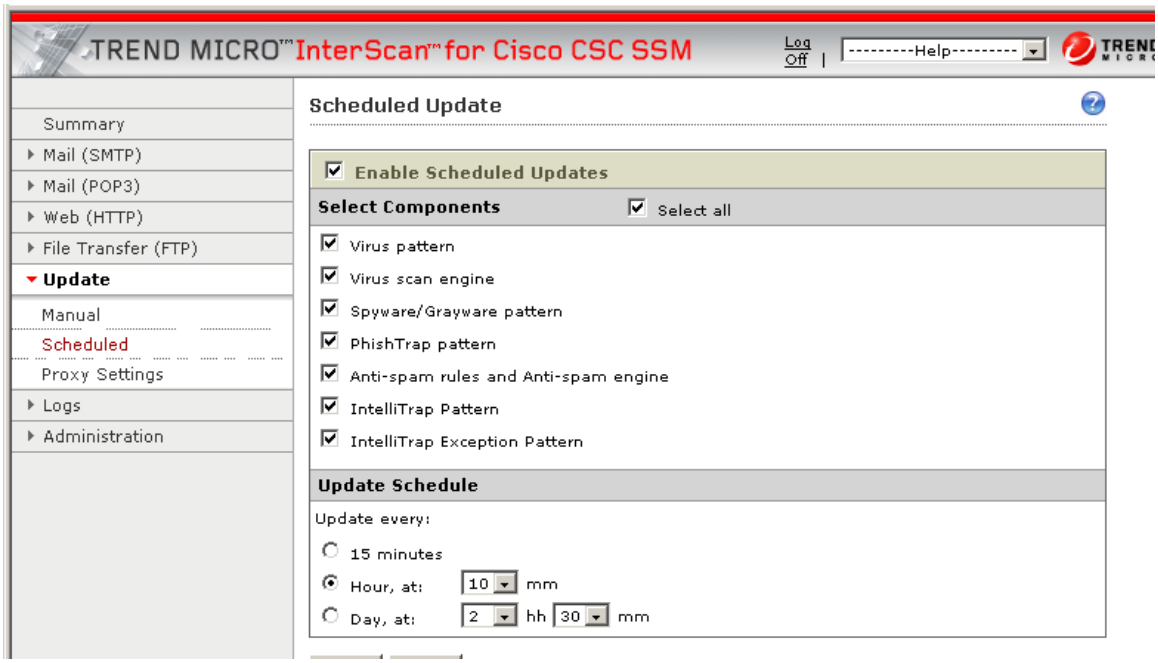
If a more current version is available, the update version number displays in red in the **Available** column. Choose components to be updated and click **Update** to download the most recent version of the selected component.

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

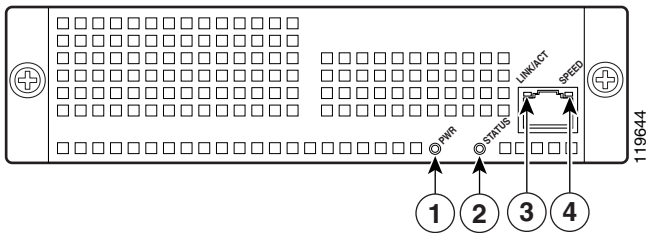


By default, Trend Micro InterScan for Cisco CSC SSM updates components periodically, with an automatic notification after a scheduled update has taken place. You can modify the scheduled update interval to occur more or less frequently.

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

CHAPTER 3

Configuring Mail Traffic (SMTP and POP3)

After installation, assuming you have configured the ASA to send traffic to the SSM, your SMTP and POP3 traffic is being scanned for viruses and other malware such as worms and Trojans. This chapter describes additional configuration required to detect security risks such as spyware or to add an organizational disclaimer to incoming and outgoing messages, and includes the following sections:

Default Mail Scanning Settings

Table 3-1 summarizes the mail configuration settings, and the default values that are in operation after installation.

Table 3-1 Default mail scanning settings

Feature	Default Setting
Mail (SMTP) scanning for incoming and outgoing mail	Enabled using All Scannable Files as the default scanning method
Mail (POP3) scanning	Enabled using All Scannable Files as the default scanning method
Mail (SMTP) and Mail (POP3) scanning message filter (reject messages larger than a specified size)	Enabled to reject messages larger than 20 MB
Mail (SMTP) message rejection (reject messages with recipients higher than a specified number)	Enabled to reject messages addressed to more than 100 recipients

Table 3-1 Default mail scanning settings (continued)

Feature	Default Setting
Mail (SMTP) compressed file handling for incoming and outgoing mail, and Mail (POP3) compressed file handling	Configured to skip scanning of compressed files when: • Decompressed file count is greater than 200 • Decompressed file size exceeds 20 MB • Number of compression layers exceeds 3 • Decompressed/compressed file size ratio is greater than 100/1
Mail (SMTP) incoming and outgoing, and Mail (POP3) action for messages in which malware is detected	Clean the message and/or attachment in which the malware was detected If the message and/or attachment is uncleanable, delete
Mail (SMTP) incoming and outgoing, and Mail (POP3) action for messages in which spyware/grayware is detected	Allow files to be delivered
Mail (SMTP) incoming and outgoing, and Mail (POP3) notification when malware is detected	An inline notification is inserted in the message in which the malware was detected, which states: %VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION%
Password-protected email messages (SMTP and POP3)	Allow files to be delivered without scanning
Compressed files sent via SMTP and POP3 that are not scanned because they exceed specified scanning criteria	Allow files to be delivered

These default settings give you some protection for your email traffic after you install Trend Micro InterScan for Cisco CSC SSM. You may change these settings. Review the online help carefully for more information about these selections before making changes.

There are additional configuration settings that you may want to update post-installation to get the maximum protection for your email traffic. These additional settings are described in the remaining pages of this chapter.

If you purchased the Plus License, which entitles you to receive anti-spam and content-filtering functionality, you must configure these features; they are not operable by default.

Defining Incoming/Outgoing SMTP Mail

When an email message is addressed to multiple recipients, one or more of which is an incoming message (addressed to someone within the same organization with the same domain name) and one of which is outgoing (addressed to someone in a different organization with a different domain name), the incoming rules apply. For example, a message from psmith@example.com is addressed to jdoe@example.com and gwood@example.net.

Assume that incoming SMTP messages are scanned via the "scan all" option, whereas outgoing messages are scanned via IntelliScan. Also assume that spyware/grayware detection is enabled for incoming messages only.

The message from psmith to jdoe and gwood would be treated as an incoming message for both recipients, even though gwood is an "outgoing" recipient.

Enabling SMTP & POP3 Spyware/Grayware Detection

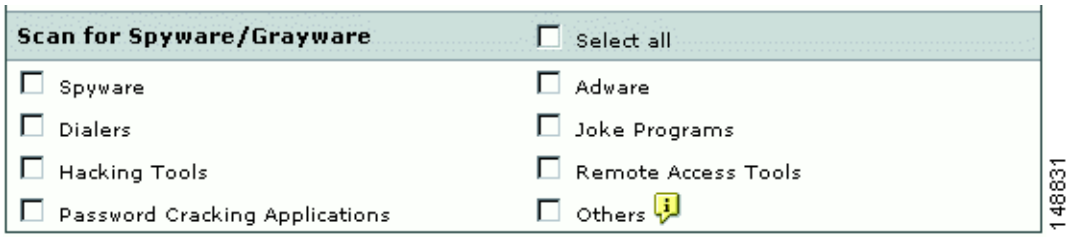
Grayware is a category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

Spyware/grayware detection is *not* enabled by default. To begin detecting spyware and other forms of grayware in your email traffic, configure this feature on the following windows:

- Click the Configure Incoming Scan link on **Configuration > Trend Micro Content Security > Mail** in ASDM to display the **SMTP Incoming Message Scan/Target** window
- Click the Configure Outgoing Scan link on **Configuration > Trend Micro Content Security > Mail** in ASDM to display the **SMTP Outgoing Message Scan/Target** window
- In the CSC SSM console, click **Mail (POP3) > Scanning > POP3 Scanning/Target** to display the **POP3 Scanning/Target** window

In the **Scan for Spyware/Grayware** section of these windows (shown in Figure 3-1), choose the types of grayware you want detected by Trend Micro InterScan for Cisco CSC SSM.

Figure 3-1 Spyware/grayware Scanning Configuration



See the specific online help for the above-mentioned windows to read a description of each of these types of grayware. After you specify the types of grayware to be detected, be sure to click **Save** to enable the new configuration.

Reviewing SMTP & POP3 Notifications

If you are satisfied with the default notification setup, no further action is required. However, you might want to review the notification options and decide whether you want to change the defaults. For example:

- You may want to send a notification to the administrator when a security risk has been detected in an email message (for SMTP, you can also notify the sender and/or recipient)
- You may want to tailor the default text in the notification message to something more appropriate for your organization

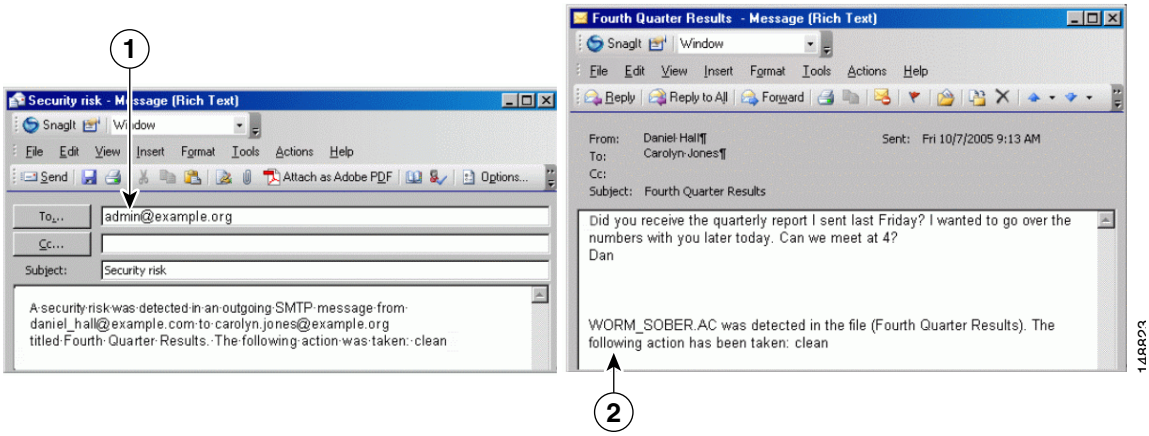
To review and possibly reconfigure email notifications, go to the following windows in the CSC SSM console:

- **Mail (SMTP) > Scanning > Incoming > SMTP Incoming Message Scan/Notification**
- **Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification**
- **Mail (POP3) > Scanning > POP3 Scanning/Notification**

Types of Notifications

There are two types of notifications available in email traffic; email notifications and inline notifications, as shown in Figure 3-2.

Figure 3-2 Examples of Notifications



1	Email notification	**2**	Inline notification

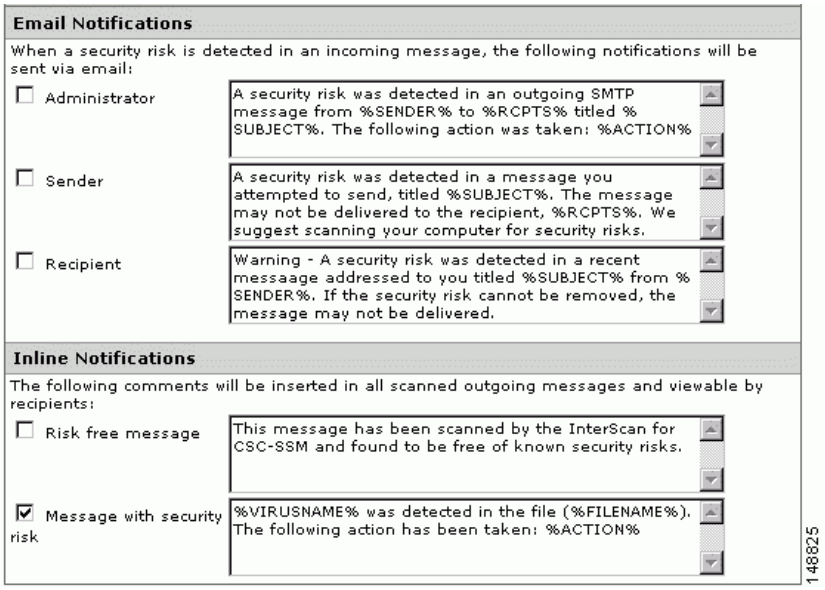
Notifications use variables called tokens to supply information that makes the notification more meaningful. For example, a token called %VIRUSNAME% is replaced with the text WORM_SOBER.AC in the inline notification example on the right.

For more information about tokens, see the online help topic “Using Tokens in Notifications.”

Modifying Notifications

To send a notification to additional recipients, or to change the default text of the notification message that is sent when a trigger event occurs, go to the message scanning notification window to be updated. For example, Figure 3-3 shows the notification fields on the **Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification** window.

Figure 3-3 Configure Notifications for Outgoing SMTP



By default, the only notification is an inline notification to the message recipient, which means neither the sender or the administrator of the originating organization are aware that a security threat was detected and cleaned. To make changes:

- In the **Email Notifications** section of the window, click additional people to receive a notification via email
- In the **Inline Notifications** section of the window, choose whether you want only the risk-free inline notification, the default "risk detected and action taken" message, neither, or both
- To change the text of any of the notifications, highlight the existing text and type your own message in the text box provided; be sure to click **Save** when you are finished

Configuring SMTP Message Filter, Disclaimer, & Incoming Mail Domain

Note These settings apply to SMTP protocol only.

Review the configuration settings available from **Mail (SMTP) > Configuration > SMTP Configuration**. There are four tabs on the **SMTP Configuration** window:

- Message Filter
- Disclaimer
- Incoming Mail Domain
- Advanced Settings

To configure these settings, perform the following steps:

Step 1 On the **Message Filter** tab of the **SMTP Configuration** window, Trend Micro InterScan for Cisco CSC SSM is already configured to reject messages larger than 20 MB and addressed to more than 100 recipients. These settings help protect you from an assault on your network that consumes CPU time while your email server tries to handle huge bogus messages addressed to hundreds of recipients. The default settings are recommended, and if you want to continue to use them, no action is required on this window.

Step 2 On the **Message Filter** tab of the SMTP Configuration window, you may add an organizational disclaimer that appears at the beginning or end of SMTP messages. Click the **Add this disclaimer...** check box to enable this feature, or leave the page as-is if you do not want to use this feature. To customize the disclaimer text, highlight and type over the default message.

Step 3 On the **Incoming Mail** tab of the SMTP Configuration window, you can define additional incoming mail domains for the purpose of:

- scanning for viruses and other threats
- anti-spam
- content-filtering

The **Incoming mail domains** field should already contain the incoming email domain name you entered (on the Host Configuration installation window) during installation. If you have additions, enter the second level domain name only. For example, enter only example.com, not subsidiary domains such as ex1.example.com, ex2.example.com, and so on. If there are no other incoming domains, no further action is needed on this window.

Step 4 The **Advanced Settings** tab of the SMTP Configuration window contains fields that allow you to:

- Set a more aggressive (or permissive) timeout for messages that appear to be from an attacker
- Enable settings that place selected, temporary restrictions on the SMTP traffic. If you suspect you may be under attack, these restrictions make it more difficult for the traffic that has the characteristics of a suspicious message from an attacker to move through system because you have
  - Set a shorter timeout for sending an email (often an email that takes longer to send is part of an intentional attempt to occupy resources)
  - Limited the allowed number of errors triggered, indicative of someone resending a message over and over
  - Limitied the number of times the sender resets the conditions for attempting to send the same email

See the online help for more information.

Step 5 If you made any changes, click **Save** to activate your updated SMTP configuration.

Enabling SMTP & POP3 Spam Filtering

Note This feature requires the Plus License.

The SMTP and POP3 anti-spam feature is disabled by default and must be configured.

Tip Anti-spam is disabled by default whether you purchase the Base and Plus licenses together, or add the Plus license at a later time. You must enable and configure the anti-spam feature to begin using it.

To configure anti-spam functionality:

- Click the Configure Anti-spam link on Configuration > Trend Micro Content Security > Mail in ASDM to display the SMTP Incoming Anti-spam window
- In the CSC SSM console, click **Mail (POP3) > Anti-spam > POP3 Anti-spam** to display the **POP3 Anti-spam** window

To enable anti-spam, perform the following steps:

Step 1 Click **Enable** on the **Target** view of the above windows.

Step 2 Reset the anti-spam threshold to **Medium** or **High** if you do not want to use the default value of **Low**.

Tip You might want to adjust this setting at a later time after you have some experience with blocking spam in your organization. If the threshold is too low, a high incidence of spam occurs. If the threshold is too high, high incidence of false positives (messages identified as spam that are legitimate messages) occurs.

Step 3 Add approved senders in the **Approved Senders** section of the **SMTP Incoming Anti-spam** and **POP3 Anti-spam/Target** windows. Mail from approved senders is always accepted without being evaluated as spam.

Note Approved senders added and saved in either window appear in the other. For example, assume you add robert_li@example.com to the **Approved Senders** list on the **POP3 Anti-spam** window. Now open the **SMTP Incoming Anti-spam** window. The address for robert_li@example.com is already added to the list of **Approved Senders** on the **SMTP Incoming Anti-spam** window as well.

The **Blocked Senders** list is also matched—a blocked sender created on either window appears in both.

Step 4 Add blocked senders in the **Blocked Senders** section of the **SMTP Incoming Anti-spam** and **POP3 Anti-spam/Target** windows. Mail from blocked senders is always rejected. Blocked senders added and saved in either window appear in the other.

Step 5 Configure the action for messages identified as spam on the **SMTP Incoming Anti-spam** and **POP3 Anti-spam/Action** windows. Choices are:

- Stamp the message with a spam identifier, such as “Spam:” and deliver it anyway (The spam identifier acts as a prefix to the message subject, for example, “Spam:Designer luggage at a fraction of the cost!”
- Delete the message

Step 6 Click **Save** to activate anti-spam per your configuration.

Enabling SMTP & POP3 Content Filtering

Note This feature requires the Plus License.

The SMTP and POP3 content filtering feature is disabled by default and must be configured. To configure content filtering functionality, go to the following windows:

- Click the Configure Incoming Filtering link on **Configuration > Trend Micro Content Security > Mail** in ASDM to display the SMTP Incoming Content Filtering/Target window
- Click the Configure Outgoing Filtering link on **Configuration > Trend Micro Content Security > Mail** in ASDM to display the SMTP Outgoing Content Filtering/Target window
- In the CSC SSM console, click **Mail (POP3) > Content Filtering > POP3 Content Filtering/Target** to display the POP3 Content Filtering/Target window

To enable content filtering, perform the following steps:

Step 1 Click **Enable** on the **Target** view of the above windows.

Step 2 Decide whether to use a message size filtering criteria, and if so, set the parameters in the **Message size is** field. For example, if you specify message filtering for messages and attachments greater than 5 MB, messages with attachments less than 5 MB are not filtered. If you do not specify a message size, all messages are filtered, regardless of their size.

Step 3 In the **Message Subject and Body** section of the windows, specify words that if present in the message subject and/or body trigger the content filtering action.

Step 4 In the **Message Attachment** section of the windows, specify characters or words that if present in the attachment name trigger the content filtering action. You can also choose content filtering by file types in this section of the window. For example, if you choose Microsoft Office file types for filtering, attachments created with Microsoft Office tools are filtered for content.

Step 5 Click the **Action** tab of the above listed windows to specify action when content filtering is triggered. For email messages, the choices are:

- Delete messages that violate one of the content filtering policies
- Deliver messages anyway

For attachments, the choices are:

- Allow violating attachments to pass (in which case, do not make any changes in the **For messages that match the attachment criteria** section of the window)
- Delete the attachment and insert an inline notification in the message body

Step 6 Click the **Notification** tab of the above listed window to specify whether a notification is sent to the administrator for a content-filtering violation. (For SMTP, you can also notify the sender and/or recipient.) Change the default text in the notification message box(es) by highlighting and typing over the default message.

Step 7 Click **Save** to activate content filtering per your configuration.

Enabling Network Reputation Services

In addition to filtering spam on the basis of content, CSC SSM provides Network Reputation Services (NRS), which allow you to determine spam based on the reputation of the originating MTA (off-loads the task from the CSC SSM server). With NRS enabled, all inbound SMTP traffic will be checked against the IP databases to see whether the originating IP address is clean or if it has been black-listed for being a known spam vector.

- In the CSC SSM console, click **Mail (SMTP) > Network Reputation Services** to open the Target window.

About RBL+ and QIL

The Realtime Blackhole List (RBL+) is a database that tracks the reputation of some 2 billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and only seldom removed. The Quick IP Lookup (QIL) list is another database for tracking the reputation of IP addresses, but with QIL, IPs are added and removed more frequently (and thus can be considered more current).

When an IP address is found in either database, NRS “marks” the connection and CSC SSM will take the action you have selected for such IPs.

For example, say an MTA has been hijacked or an open relay exploited and used by a 3rd party to deliver spam messages. The system admin may discover the exploit after a few hours or days and correct it, but in the meantime millions of spam messages are being and have been sent by the server. The tainted IP may be added to the QIL database after only a few reports of spam, but then removed once the reports have trailed off (the admin regains control of the MTA). On the other hand, because it takes longer for an IP address to be added to the RBL+, many IPs that are only temporarily problematic (but nonetheless may be responsible for millions of spam) will not be flagged by RBL+. Once added to the RBL+, however, it is harder to remove an IP address from the database -- there is a higher degree of certainty that IPs in the RBL+ are inveterate spam MTAs.

Both services are applied to the message before the message is delivered to your MTA, freeing it from the overhead of processing complex heuristics and analysis while at the same time routing the mail.

To enable and configure NRS filtering, perform the following steps:

Step 1 Click **Enable** on the **Target** view of the above windows.

Step 2 Choose the level of service you want to employ: High or Low. High service level uses both the Realtime Blackhole List (RBL+) and Quick IP Lookup services to check the reputation of the MTA from which the email is received.

Step 3 In the **Approved IP Address** field, add the IP address, or a range of IP addresses, for any machines you want to exempt from the lookup.

Step 4 Click the **Action** tab to make that page active, and then choose the action you want CSC SSM to take on messages found to match an entry in the RBL+ or QIL databases. Actions are described below:

- **Intelligent action** - Spam messages are rejected at the MTA with a brief message
- **Connection closed with no error** - Spam messages are rejected but no message is sent (Note: this may trigger a series of automatic retries on the part of the originating MTA, and can increase traffic volume)

- **Detect, log, then pass** - Spam incidents are logged and then delivered to the intended recipient (other scanning rules will be applied). This action is typically used only for troubleshooting.

CHAPTER 4

Configuring Web (HTTP) and File Transfer (FTP) Traffic

After installation, by default your HTTP and FTP traffic is being scanned for viruses, worms and Trojans. Malware such as spyware and other grayware require a configuration change before they are detected. This chapter describes how to make these configuration updates, and includes the following sections:

Default Web and FTP Scanning Settings

Table 4-1 summarizes the Web and file transfer configuration settings, and the default values that are in operation after installation.

Table 4-1 Default Web and FTP scanning settings

Feature	Default Setting
Web (HTTP) scanning of file downloads	Enabled using All Scannable Files as the default scanning method
Webmail scanning	Configured to scan Webmail sites for Yahoo™, AOL™, MSN™, and Google™ by default
File transfer (FTP) scanning for file transfers	Enabled using All Scannable Files as the default scanning method

Table 4-1 Default Web and FTP scanning settings (continued)

Feature	Default Setting
Web (HTTP) compressed file handling for downloading from the Web, and File transfer (FTP) compressed file handling for file transfer from an FTP server	Configured to skip scanning of compressed files when: • Decompressed file count is greater than 200 • Decompressed file size exceeds 30 MB • Number of compression layers exceeds 3 • Decompressed/compressed file size ratio is greater than 100/1
Web (HTTP) and file transfer (FTP) large file handling (do not scan files larger than a specified size - enabled deferred scanning of files larger than a specified size)	Configured to skip scanning of files larger than 50 MB, and to enable deferred scanning of files larger than 2 MB
Web (HTTP) downloads, and file transfers (FTP) action for files in which malware is detected	Clean the download and/or file in which the malware was detected If uncleanable, delete
Web (HTTP) downloads, and file transfers (FTP) action for files in which spyware/grayware is detected	Files are deleted
Web (HTTP) downloads, and file transfers (FTP) notification when malware is detected	An inline notification is inserted in the user's browser, stating that InterScan for CSC SSM has scanned the file you are attempting to transfer, and has detected a security risk.

These default settings give you some protection for your Web and FTP traffic after you install Trend Micro InterScan for Cisco CSC SSM. You may change these settings; for example, you may prefer to use the **Scan by specified file extensions...** option rather than **All Scannable Files** for malware detection. Review the online help carefully for more information about these selections before making changes.

There are additional configuration settings that you may want to update post-installation to get the maximum protection for your Web and FTP traffic. These additional settings are described in the remaining pages of this chapter.

If you purchased the Plus License, which entitles you to receive URL blocking, anti-phishing, and URL filtering functionality, you must configure these features; they are not operable by default.

Downloading Large Files

The Target tabs on the HTTP Scanning and FTP Scanning windows allow you to define the size of the largest download you want scanned. For example, you might specify that a download under 20MB is scanned, but a download larger than 20 MB is not scanned.

In addition, you can:

- Specify whether to allow these unscanned large downloads to be delivered without scanning, which may introduce a security risk, or
- Specify that downloads greater than the specified limit are deleted

By default, the CSC SSM software specifies that files under 50 MB are scanned, and files 50MB and over are delivered without scanning to the requesting client.

Deferred Scanning

The deferred scanning feature is not enabled by default. This feature, when enabled, allows a user to begin downloading data without scanning the entire download. Deferred scanning thus allows a user to begin viewing the data without a prolonged wait while the entire body of information is scanned.

Caution When deferred scanning is enabled, the unscanned portion of the information can introduce a security risk.

If deferred scanning is not enabled, the entire content of the download must be scanned before it is presented to the user. However, some client software may timeout due to the time it takes to collect sufficient network packets to compose complete files for scanning.

To summarize:

Method	Advantage	Disadvantage
Deferred scanning enabled	Prevents client timeouts	May introduce a security risk
Deferred scanning disabled	Safer, the entire file is scanned for security risks before being presented to the user	May result in client timeouts before the download is complete

Scanning HTTPS Traffic

Traffic moving via HTTPS protocol cannot be scanned for viruses and other threats by the CSC SSM software.

Detecting Spyware/Grayware

Grayware is a category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

Spyware/grayware detection is *not* enabled by default. To begin detecting spyware and other forms of spyware and other grayware in your Web and file transfer traffic, configure this feature on the following windows:

- **Web (HTTP) > Scanning > HTTP Scanning/Target**
- **File Transfer (FTP) > Scanning > FTP Scanning/Target**

You can go directly to the Target tab of the HTTP Scanning window by clicking the Configure Web Scanning link on **Configuration > Trend Micro Content Security > Web** in ASDM. You can go directly to the Target tab of the FTP Scanning window by clicking the Configure File Scanning link on **Configuration > Trend Micro Content Security > File Transfer** in ASDM.

See the "Enabling SMTP & POP3 Spyware/Grayware Detection" section on page 3-3 for more information. Also see the online help for the above-mentioned windows.

Scanning Webmail

Caution If you elect to scan only Webmail, HTTP scanning is restricted to the sites specified on the Webmail Scanning tab of the **Web (HTTP) > Scanning > HTTP Scanning** window. Other HTTP traffic is *not* scanned.

As mentioned in Table 4-1, Webmail scanning for Yahoo, AOL, MSN, and Google are already configured by default. To add additional sites, click the Configure Web Scanning link on **Configuration > Trend Micro Content Security > Web** in ASDM. The Target tab of the **HTTP Scanning** window displays. Click the **Webmail Scanning** tab.

Enter the Webmail site in the **Name** field using:

- The exact Web site name
- A URL keyword
- A string

Note Attachments to messages that are managed via Webmail are scanned.

See the online help for more information about how to configure additional Webmail sites for scanning. Configured sites are scanned until you remove them from the **Scan Webmail at following sites** section of the window by clicking the trashcan icon. Click **Save** to update your configuration.

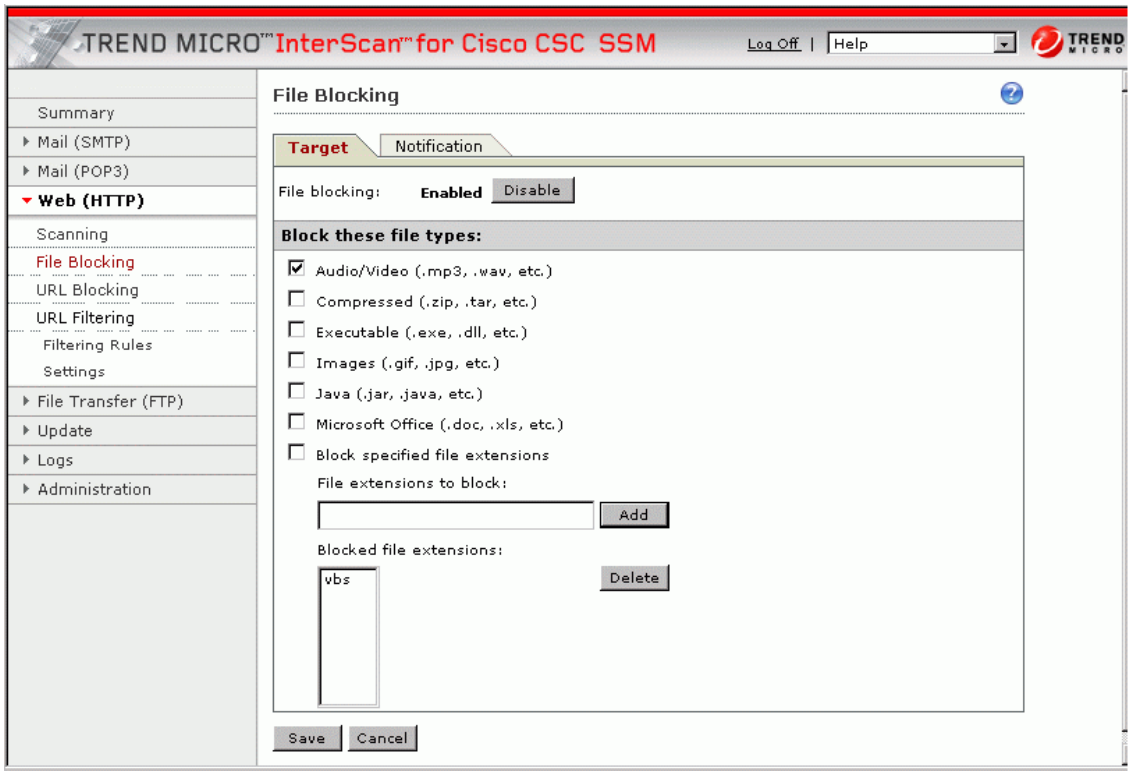
File Blocking

This feature is enabled by default, but doesn't block any files until you specify the types of files you want blocked. File blocking helps you enforce your organization's policies regarding the use of the Internet and other computing resources during work time. For example, suppose your company does not allow downloading of music, both because of legal issues as well as employee productivity issues.

To block downloads via HTTP protocol, click the Configure File Blocking link on **Configuration > Trend Micro Content Security > Web** in ASDM to display the **File Blocking** window. To block downloads via FTP protocol, click the Configure File Blocking link on **Configuration > Trend Micro Content Security > File Transfer** in ASDM. The **File Blocking** window is the sam e for both protocols.

On the **Target** tab of the **File Blocking** window, block transferring of music files by choosing Audio/Video, as shown in Figure 4-1.

Figure 4-1 Enable File Blocking



You can specify additional file types by file name extension. Click **Block specified file extensions** to enable this feature. Then, add additional file types in the **File extensions to block** field, and click **Add**. In the example, .vbs files are also blocked.

See the online help for more information about file blocking, and for information on deleting file extensions you no longer want to block.

Click the **Notifications** tab of the **File Blocking** window to view the default notification that displays in the user's browser/FTP client when a file blocking event is triggered. You can customize the text of these messages by highlighting and typing over the default message. An optional notification to the administrator is available for HTTP file-blocking events, but is turned off by default. Click **Send the following message...** check box to activate the notification.

Click **Save** when you are finished, to update your configuration.

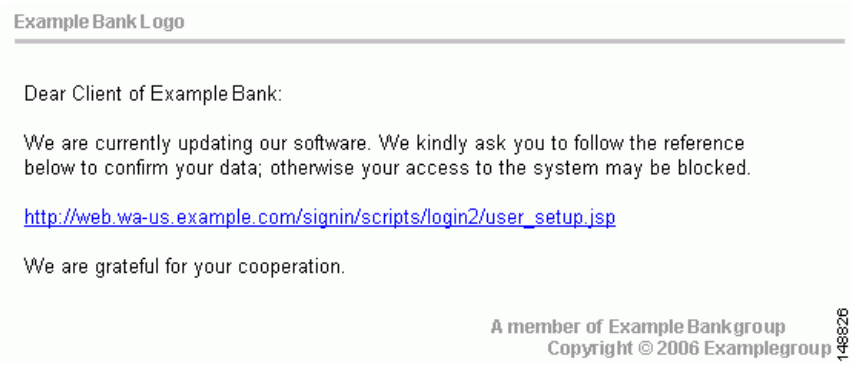
URL Blocking

Note This feature requires the Plus License.

The URL blocking feature helps you prevent employees from accessing prohibited websites. For example, suppose you want to block some sites because policies in your organization prohibit use of dating services, online shopping services, or viewing offensive sites.

You may also want to block sites that are known for perpetrating fraud, such as phishing. Phishing is a technique used by criminals who send email messages that *appear* to be from a legitimate organization, leading users into revealing private information such as bank account numbers. Figure 4-2 shows a common example of an email message used for phishing.

Figure 4-2 Example of Phishing



By default, URL blocking is enabled, but only sites in the TrendMicro PhishTrap pattern file are blocked, until you specify additional sites for blocking.

Blocking Via Local List

To configure URL blocking, perform the following steps:

Step 1 Click **Configure URL Blocking** on **Configuration > Trend Micro Content Security > Web** in ASDM to display the **URL Blocking** window.

Step 2 On the **Via Local List** tab of the **URL Blocking** window, type the URLs you want to block in the **Match** field. You can specify:

- The exact Web site name
- A URL keyword
- A string

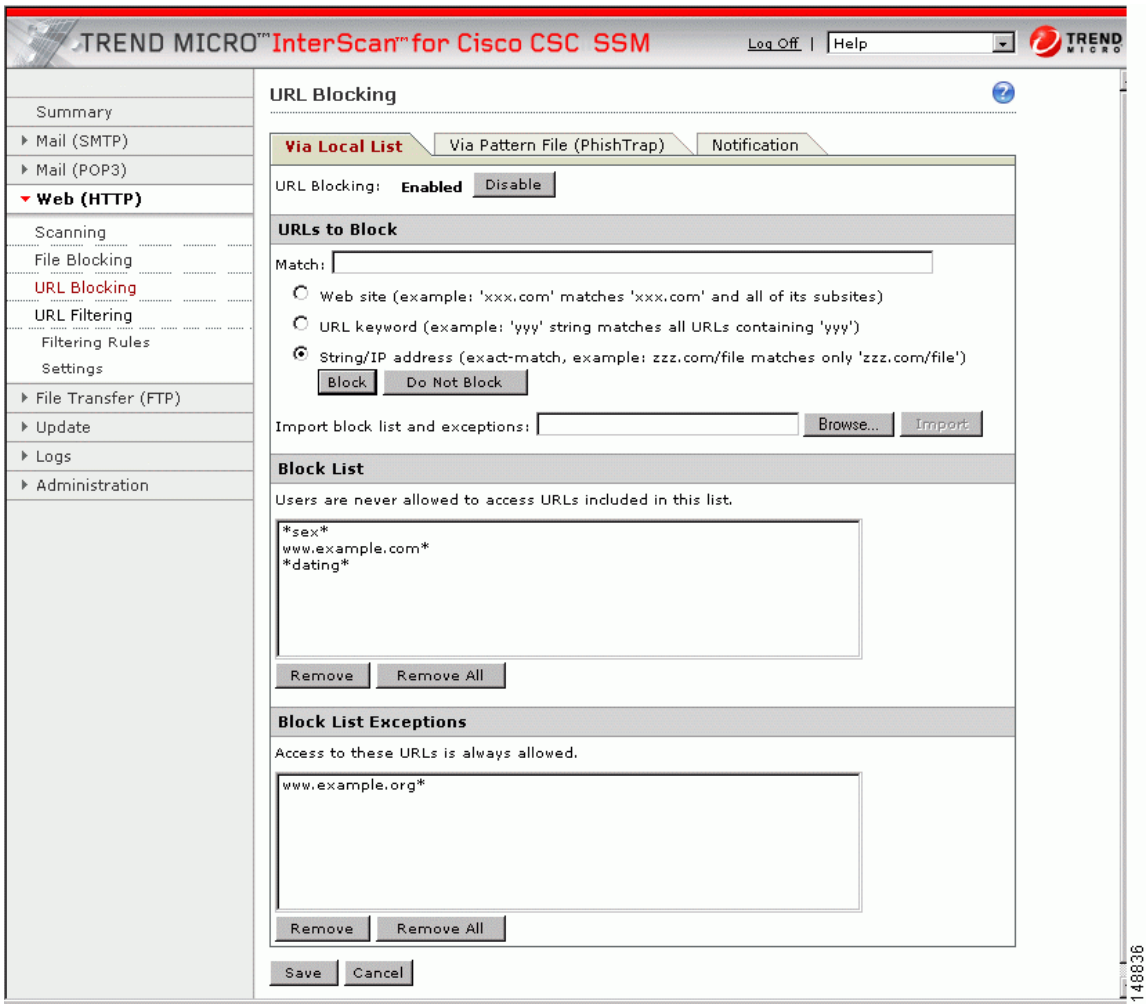
See the online help for more information about formatting entries in the **Match** field.

Step 3 Click **Block** after each entry, to move the URL to the **Block List**. To specify your entry as an exception, click **Do Not Block** to add the entry to **Block List Exceptions**. Entries remain as blocked or exceptions until you remove them.

Note You can also import a block and exception list. The imported file must be in a specific format. See the online help for instructions.

Figure 4-3 shows an example of the **URL Blocking** window (**Via Local List** tab) with some entries.

Figure 4-3 URL Blocking Window



Blocking Via Pattern File (PhishTrap)

Click the Configure URL Blocking link on **Configuration > Trend Micro Content Security > Web** in ASDM to display the **URL Blocking** window. Then click the **Via Pattern File (PhishTrap)** tab.

By default, the Trend Micro PhishTrap pattern file detects and blocks known phishing sites, spyware sites, virus accomplice sites (sites associated with known exploits), and disease vectors (websites that exist only for malicious purposes). Use the **Submit the Potential Phishing URL to TrendLabs** fields to submit sites that you suspect should be added to the PhishTrap pattern file. TrendLabs evaluates the site and may add the site if such action is warranted.

Click the **Notification** tab to review the text of the default message that appears in a user's browser when an attempt is made to access a blocked site. An example is shown in the online help. Customize the text by highlighting and typing over the default message.

Click **Save** when you are finished to update your configuration.

URL Filtering

Note This feature requires the Plus License.

URLs defined on the **URL Blocking** windows described previously are either always allowed or always disallowed. The URL filtering feature, however, allows you to configure URLs in categories, which you can schedule to allow during certain times (defined as leisure time) and disallow during work time.

There are six URL categories:

- Company-prohibited
- Not work related
- Research topics
- Business function
- Customer defined
- Others

By default, company-prohibited sites are blocked during both work and leisure time.

Filtering Settings

To configure the URL filtering feature, perform the following steps:

Step 1 Click **Configure URL Filtering Settings** on **Configuration > Trend Micro Content Security > Web** in ASDM to display the **URL Filtering Settings** window. On the URL Categories tab, review the sub-categories listed and the default classifications assigned to each category to see if the assignments are appropriate for your organization. For example, “Illegal Drugs” is a sub-category of the “Company-prohibited” category. If your organization is a financial services company, you may want to leave this category classified as company-prohibited. Simply click the **Illegal Drugs** check box to enable filtering for sites related to illegal drugs. However, if your organization is a law enforcement agency, you should probably reclassify the “Illegal Drugs” subcategory to the “Business function” category. See the online help for more information about reclassification.

Step 2 After you have reviewed and refined the sub-category classifications, enable all the sub-categories for which you want filtering performed by choosing the sub-category check box.

Step 3 If there are sites within some of the enabled sub-categories that you do not want filtered, click the **URL Filtering Exceptions** tab. Type the URLs you want to exclude from filtering in the **Match** field. You can specify:

- The exact Web site name
- A URL keyword
- A string

See the online help for more information about formatting entries in the **Match** field.

Step 4 Click **Add** after each entry, to move the URL to the **Do Not Filter the Following Sites** list. Entries remain as exceptions until you remove them.

Note You can also import an exception list. The imported file must be in a specific format. See the online help for instructions.

Step 5 Click the **Schedule** tab to define the days of the week and hours of the day that should be considered work time. Time not designated as work time is automatically designated as leisure time.

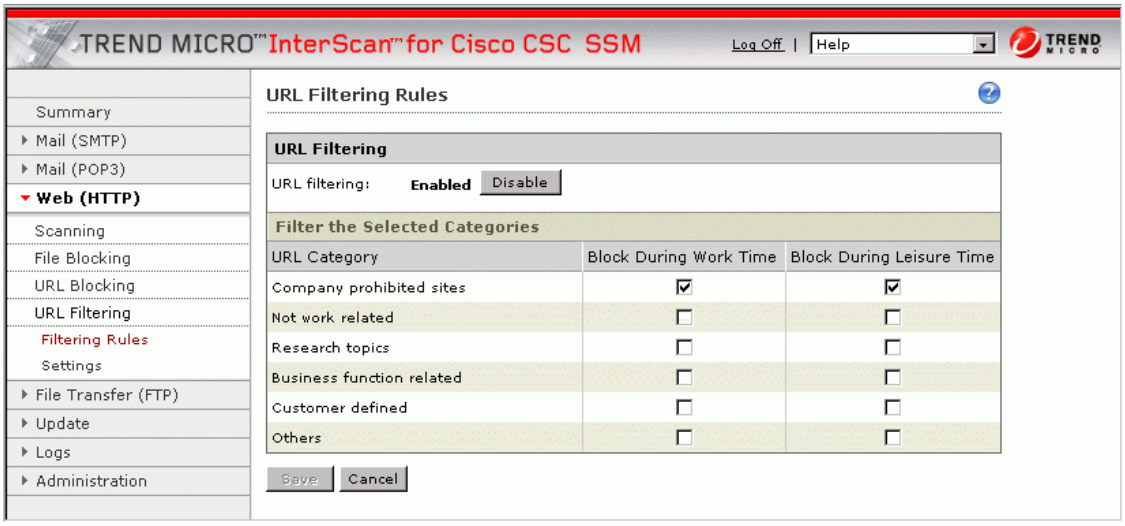
Step 6 Click **Save** to update your URL filtering configuration.

Click the **Reclassify URL** tab to submit questionable URLs to TrendLabs for evaluation.

Filtering Rules

Now that you have assigned your URL sub-categories to categories appropriate for your organization, defined exceptions (if any), and created the work/leisure time schedule, assign the filtering rules that determine when a category is filtering. Click the Configure URL Filtering Rules link on **Configuration > Trend Micro Content Security > Web** in ASDM to display the **URL Filtering Rules** window, shown in Figure 4-4.

Figure 4-4 URL Filtering Rules Window



For each of the six major categories, specify whether the URLs in that category are blocked, and if so, during work time, leisure time, or both. See the online help for more information. Click **Save** to update your configuration.

Managing Updates and Log Queries

This chapter describes managing updates, proxy and syslog settings, and log queries, and includes the following sections:

Updating Components

New viruses and other security risks are released “into the wild” (meaning perpetrated on the global computing community) via the Internet or other distribution means at any time and on any day of the week. TrendLabs immediately analyzes a new threat, and takes appropriate steps to update the components required to detect the new threat, such as the virus pattern file. This quick response enables Trend Micro InterScan for Cisco CSC SSM to detect, for example, a new worm that was launched from the computer of a malicious hacker in Amsterdam at 3:00 A.M. this morning.

It is vital that you keep your components up-to-date to help ensure that a new threat does not penetrate your network. To accomplish this, you can:

- Perform a manual update of the components at any time, on demand
- Set up an update schedule that automatically updates the components on a periodic basis

The components managed, either manually or via a schedule, are:

- Virus pattern file
- Virus scan engine
- Spyware pattern file (which includes patterns for other types of grayware as well)
- PhishTrap pattern file
- Anti-spam rules
- Anti-spam engine

The PhishTrap pattern file, anti-spam rules, and anti-spam engine components are active and updated only if you purchased the Plus License.

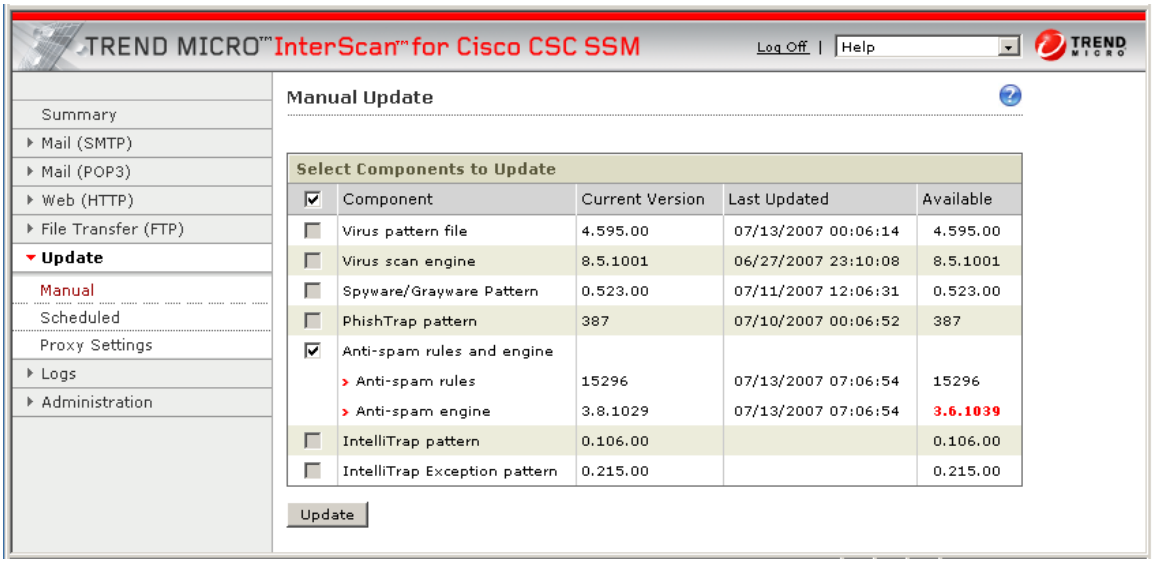
To find out whether you have the most current components installed, go to the **Manual Update** window and check the component status.

Note The CSC SSM software does *not* support rollback of these updates for either the scan engine or the pattern file.

Manual Update

To view component status, or manually update components, go to **Updates > Manual**. The **Manual Update** window displays (shown in Figure 5-1).

Figure 5-1 Manual Update Window



You can see at a glance whether any of the components are out of date by scanning the **Available** column on the right side of the window. If a more current component is available, the component version displays in red.

For example, click **Update** to download the latest pattern file version. A progress message displays while the new pattern is downloading. When the update is complete, the **Manual Update** window refreshes, showing that the latest update has been applied.

See the online help for more information about this feature.

Scheduled Update

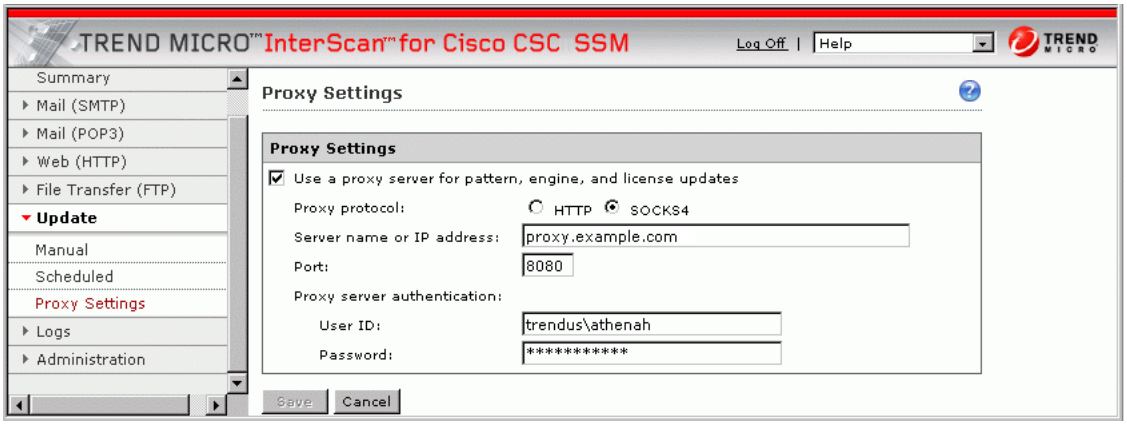
The **Scheduled Update** window enables you to configure component updates as often as every 15 minutes. Go to **Updates > Scheduled** to view the **Scheduled Update** window. Choose the components to be updated per the update schedule.

Leave the schedule as is, or change it to more or less frequent. See the online help for more information. Click **Save** to update your configuration.

Configuring Proxy Settings

If you are using a proxy server to communicate with the Trend Micro ActiveUpdate server, you specified a proxy server IP and port during installation. Click **Update > Proxy Settings** to view these selections on the **Proxy Settings** window, shown in Figure 5-2.

Figure 5-2 Proxy Settings Window



If you set up a proxy during installation, by default the HTTP proxy protocol is configured. To change to SOCKS4, click the **SOCKS4** radio button. See the online help for more information.

The only other change you might want to make on this window is to add an optional proxy authentication user name and password in the **User ID** and **Password** fields. Click **Save** to update your configuration when you are finished.

Configuring Syslog Settings

After installation, log data such as virus or spyware/grayware detections is saved temporarily. To store log data, configure at least one (up to three) syslog servers. Go to **Logs > Settings** to display the **Log Settings** window.

Configure at least one syslog server. Click the **Enable** check box, then enter the syslog server IP, port, and preferred protocol (either UDP or TCP). See the online help for more information.

By default, detected security risks are logged. You can turn off logging for features you are not using, for example, you can turn off URL blocking/Anti-phishing and URL filtering if you did not purchase the Plus License.

For information on choosing and viewing log data, see the "Viewing Log Data" section on page 5-3. Syslogs are also viewable from the ASDM. See the online help for ASDM for more information.

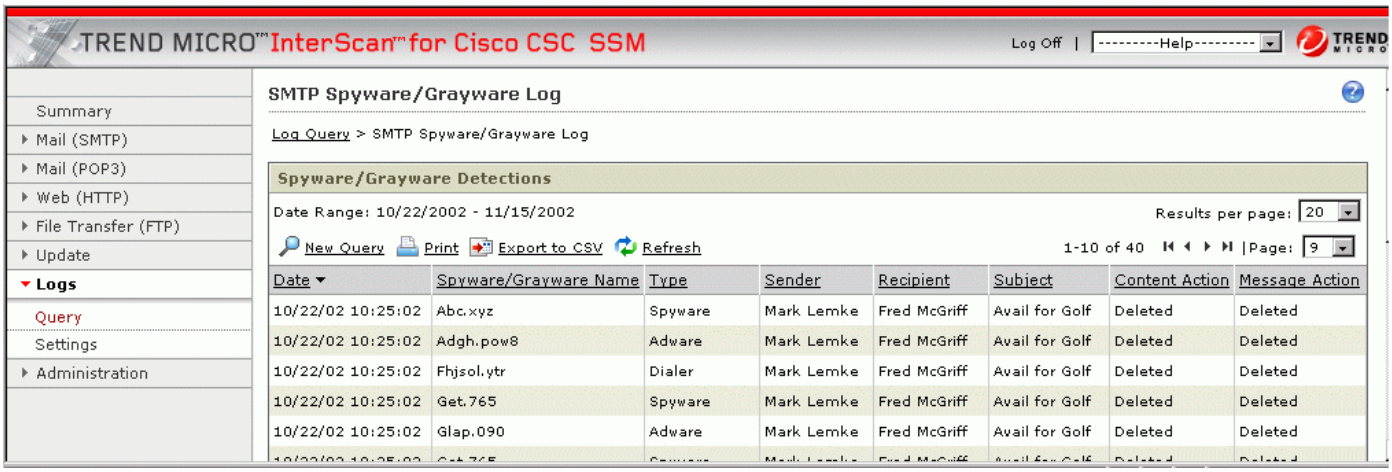
Viewing Log Data

After you have installed and configured Trend Micro InterScan for Cisco CSC SSM, security risks are being detected and acted upon according to the actions you chose for each type of risk. These events are recorded in the logs. To conserve system resources, these logs may be purged periodically.

To view the log, go to **Logs > Query** to display the **Log Query** window. Specify the inquiry parameters and click **Display Log** to view the log. See the online help for more information.

Figure 5-3 shows an example of the spyware/grayware log.

Figure 5-3 Spyware/Grayware Log



Logging of Scanning Parameter Exceptions

Exceptions to the following scanning parameters, which are specified on the Target tab, display in the Virus/Malware log.

For SMTP, POP3, HTTP and FTP:

- Compressed files that when decompressed exceed the specified file count limit
- Compressed files that when decompressed exceed the specified file size limit
- Compressed files that exceed the number of layers of compression limit
- Compressed files that exceed the compression ratio limit (the size of the decompressed files is “x” times the size of the compressed file)
- Password-protected files (if configured for deletion)

For HTTP and FTP only:

- Files or downloads that are too large for scanning

In place of the virus/malware name, these files are identified with messages similar to the following:

- Decompressed_File_Size_Exceeded
- Large_File_Scanning_Limit_Exceeded

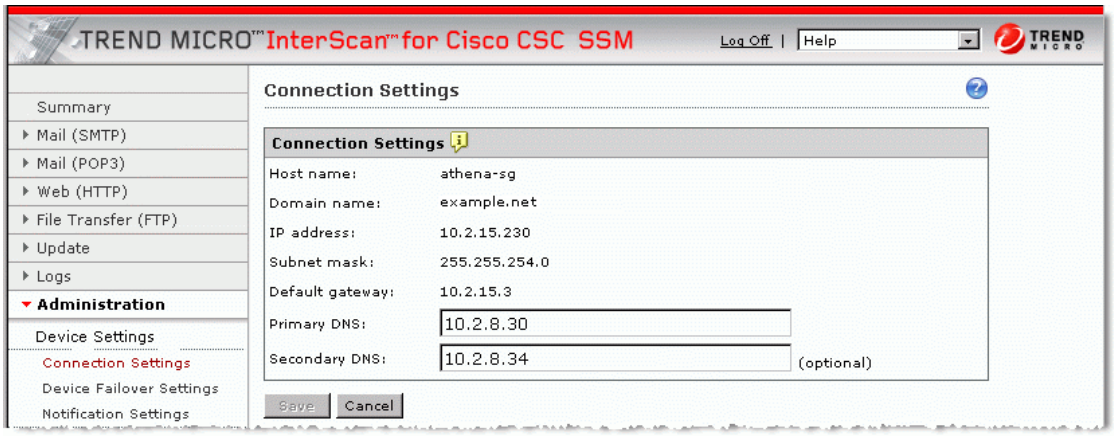
Administering Trend Micro InterScan for Cisco CSC SSM

This chapter describes tasks you might perform infrequently, such as installing a patch, and includes the following sections:

Configuring Connection Settings

To view your network connection settings, select **Administration > Device Settings > Connection Settings**. The **Connection Settings** window (shown in Figure 6-1) displays selections you made during installation.

Figure 6-1 Connection Settings Window



The **Primary DNS** and **Secondary DNS** IP address fields can be changed on this screen. To change your other connection settings, such as host name, domain name, or IP address, go to **Configuration > Trend Micro Content Security** and select **CSC Setup** from the menu.

You can also change these settings using the command-line interface (CLI). Log in to the CLI, and issue a **session 1** command. If this is your first time logging in to the CLI, use the default user name (cisco) and password (cisco). You are prompted to change your password.

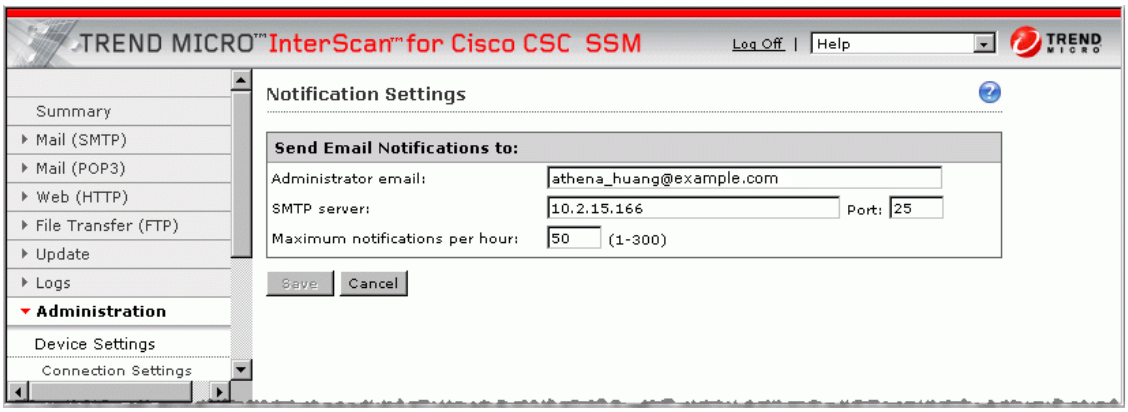
After you log in, select option **1**, Network Settings, from the Trend Micro InterScan for Cisco CSC SSM Setup Wizard menu. Follow the prompts to change the settings. See the "Reimaging the CSC SSM" section on page A-4, for more information.

Managing Admin Email and Notification Settings

The **Notification Settings** window (shown in Figure 6-2) allows you to:

- View and/or change the administrator email address you selected during installation (on the **Host Configuration** window)
- View the SMTP server IP and port you selected during installation (on the **Host Configuration** window)
- Configure the maximum number of administrator notifications per hour

Figure 6-2 Notification Settings Window



To make changes on this window, enter the new information and click **Save**.

You can also make these changes in the ASDM by selecting **Configuration > Trend Micro Content Security**, then select **CSC Setup** from the menu.

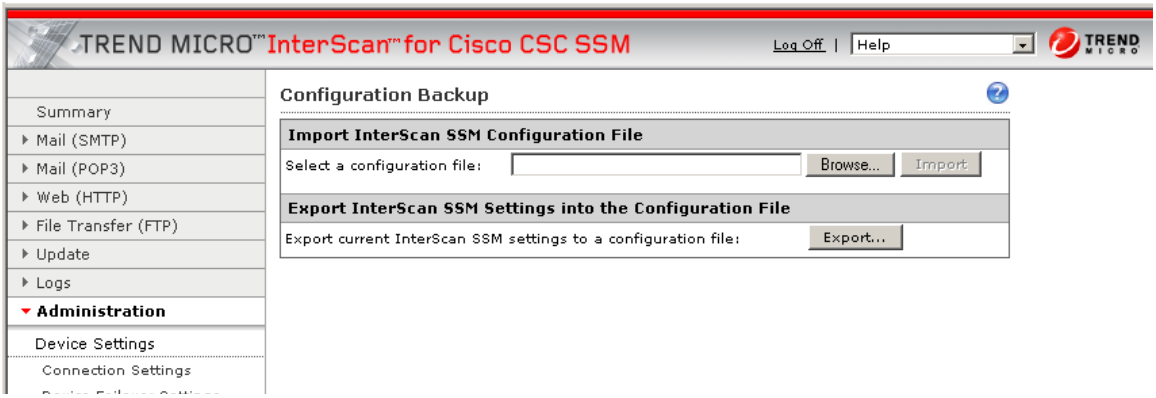
Performing Configuration Backup

Trend Micro InterScan for Cisco CSC SSM provides the ability to back up your device configuration and save it in a compressed file. You can import the saved configuration and thus restore your system to the settings configured at the time of the save.

Note A configuration backup is essential for recovery in case you lose your ASDM/Web GUI password. See Recovering a Lost Password, page 8-5 for more information.

As soon as you finish configuring Trend Micro InterScan for Cisco CSC SSM as described in previous chapters, perform a configuration backup. Go to **Administration > Configuration Backup** to display the **Configuration Backup** window, shown in Figure 6-3.

Figure 6-3 Configuration Backup Window



Export (Save) Configuration

Click **Export** to save your configuration settings. A **File Download** dialog box displays. You can open the file, which is named config.tgz by default, or save the file to your computer.

Import Configuration

To restore a saved configuration file, on the **Backup Configuration** window, click **Browse**. Locate the config.tgz file and click **Import**. The file name displays in the **Select a configuration file** field. The saved configuration settings are restored to the appliance.

Importing a saved configuration file restarts scanning service. You should notice, for example, that the counters on the **Summary** window reset.

Configuring Failover Settings

Trend Micro InterScan for Cisco CSC SSM provides capability to replicate configuration to a peer unit in supporting the device failover feature on the ASA. Before you configure the peer device, or the CSC SSM on the failover device, finish configuring the primary device first, that is, enable spyware/grayware scanning, customize your notifications if you plan to do so, and so on.

When you have fully configured the primary device to perform as you want it, follow the steps exactly as described in the checklist below to configure the failover peer. Print a copy of the checklist that you can use to record your steps as you progress.

Step	Configure Failover Checklist	Checkoff
1	Decide which appliance should act as the primary device, and which should act as the secondary device. Record the IP address of each here: **Notes:** _____ _____	❑ ❑
2	Open a browser window and enter the following URL in the **Address** field: http://<primary device IP address>:8443. The **Logon** window displays. Log on, and navigate to **Administration > Device Settings > Device Failover Settings**.	❑
3	Open a second browser window and enter the following URL in the **Address** field: http://<secondary device IP address>:8443. As in step 2, log on, and navigate to the **Device Failover Settings** window.	❑
4	On the **Device Failover Settings** window for the primary device, enter the IP address of the secondary device in the **Peer IP address** field. Enter an encryption key of 1-8 alphanumeric characters in the **Encryption key** field. Click **Save**, and then click **Enable**. The following message displays under the window title: `InterScan for CSC SSM could not establish a connection because the failover peer device is not yet configured. Please configure the failover peer device, then try again.` This message is normal and appears because the peer is not yet configured. Do not be concerned about this message at this time.	❑
5	On the **Device Failover Settings** window for the secondary device, enter the IP address of the primary device in the **Peer IP address** field. Enter the encryption key of 1-8 alphanumeric characters in the **Encryption key** field. The encryption key must be identical to the key entered for the primary device. Click **Save**, and then click **Enable**. The following message displays under the window title: `InterScan for CSC SSM has successfully connected with the failover peer device.` *Do not click anything else* at this time for the secondary device.	❑
6	Go back to the **Device Failover Settings** window for the primary device and click **Synchronize with peer**.	❑
7	The message in the **Status** field at the bottom of the windows should now state the date and time of the synchronization, for example: `Status: Last synchronized with peer on: 09/29/2005 15:20:11`	❑

Caution Be sure you do not click **Synchronize with peer** at the end of Step 5 while you are still on the **Device Failover Settings** window for the secondary device. If you do, the configuration you have already set up on the primary device is erased. You must perform manual synchronization from the primary device as described in Step 6.

When you complete the steps on the checklist, the failover relationship is successfully configured.

If at a future time you want to make a change to the configuration, for example, you change the spam filtering threshold from Low to Medium, you should modify the configuration on the primary device only. Trend Micro InterScan for Cisco CSC SSM detects the configuration mismatch, and updates the peer with the configuration change you made on the first device.

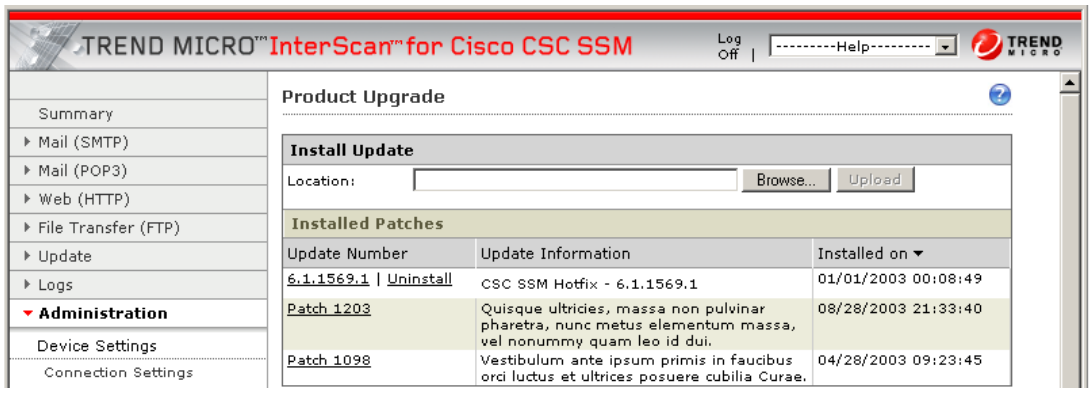
The exception to the auto-synchronization feature is uploading a system patch. A patch must be applied on both the primary and secondary devices. See the "Installing Product Upgrades" section on page 6-5 for more information.

If for some reason the peer device becomes unavailable, an email notification is sent to the administrator. The message continues to be sent periodically until the problem with the peer is resolved.

Installing Product Upgrades

From time to time, a product upgrade becomes available that fixes a known issues or offers new functionality. First download the system patch from the Web site or CD provided, then go to **Administration > Product Upgrades** to display the **Upgrade** window, shown in Figure 6-4.

Figure 6-4 Product Upgrades Window



Caution Upgrades may restart system services and interrupt system operation. Upgrading the system while the device is in operation may allow traffic containing viruses and malware through the network.

See the online help for this window for information about installing and removing upgrades.

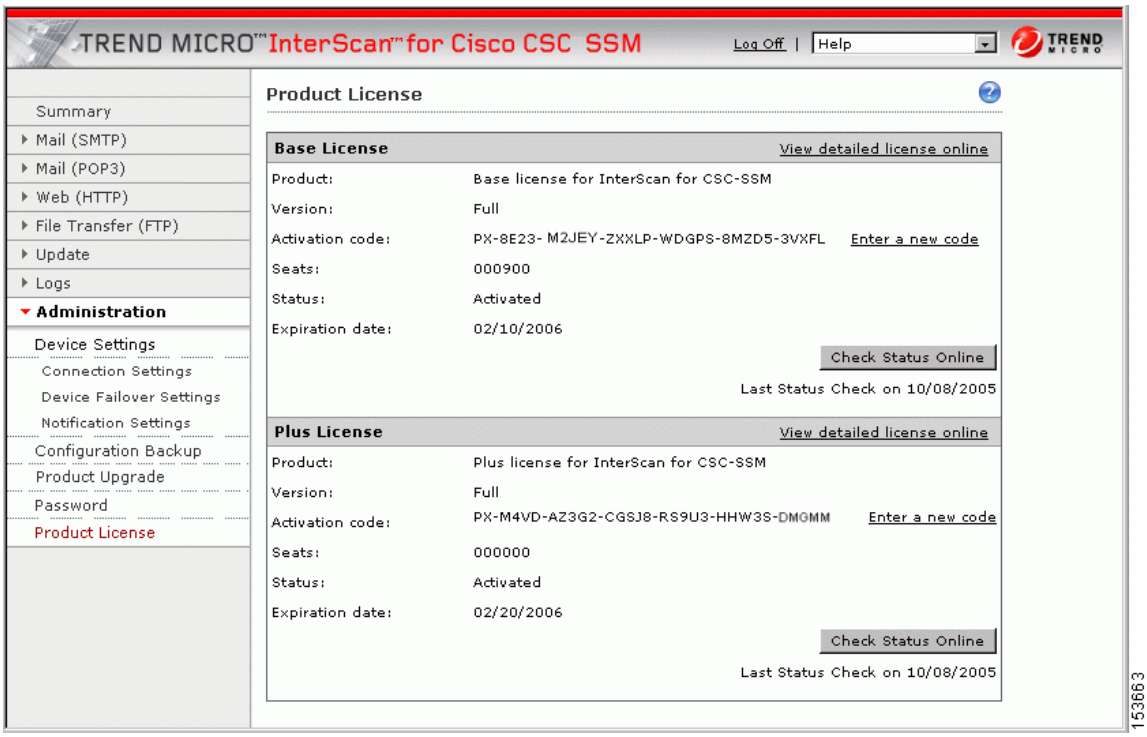
Viewing the Product License

The **Product License** window (shown in Figure 6-5) allows you to view the status of your product license, including:

- Which license(s) are activated (Base License only, or Base License and Plus License)
- License version, which should state "Full" unless you are temporarily using an "Evaluation" copy
- Activation Code for your license
- Number of licensed seats (users)—this information displays only for the Base License, even if you purchased the Plus License

- Status, which should be “Activated”
- License expiration date—if you have both the Base and Plus Licenses, the expiration dates can be different

Figure 6-5 Product License Window

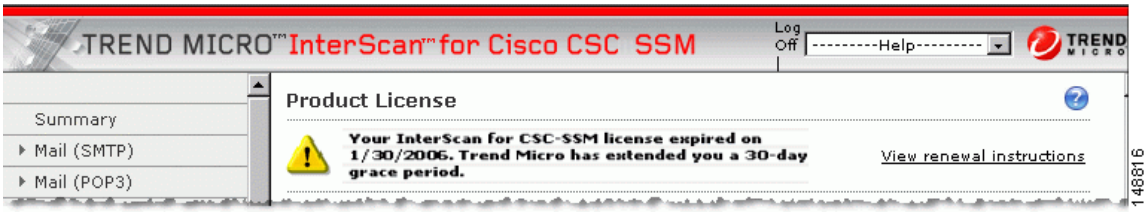


If your license is not renewed, antivirus scanning continues with the version of the pattern file and scan engine that was valid at the time of expiration plus a short grace period. However, other features may become unavailable. See the License Expiration section for more information.

License Expiration

As you approach and even pass the expiration date, a message displays in the **Summary** window under the window header, similar to the example shown in Figure 6-6.

Figure 6-6 License Expiration Message



When your product license expires, you can continue using Trend Micro InterScan for Cisco CSC SSM, but you are no longer eligible to receive updates (to the virus pattern file, scan engine, and so on). Your network may no longer be protected against new security threats.

If your Plus license expires, content-filtering and URL-filtering are no longer available. In this case, traffic is passed without filtering content or URLs.

If you purchased the Plus License at a later time after you purchased and installed the Base License, the expiration dates are different. You can renew each license at different times as the renewal date approaches.

License Information Links

The Product License window contains some helpful links. These are:

- View detailed license online
- Check Status Online

The View detailed license online link takes you to the Trend Micro online registration Web site where you can view information about your license, and find instructions for renewing. **Check Status Online** displays a message below the **Product License** window title that describes the status of your license, similar to the example in the previous figure.

View the online help for the **Product License** window for additional information.

Monitoring Content Security

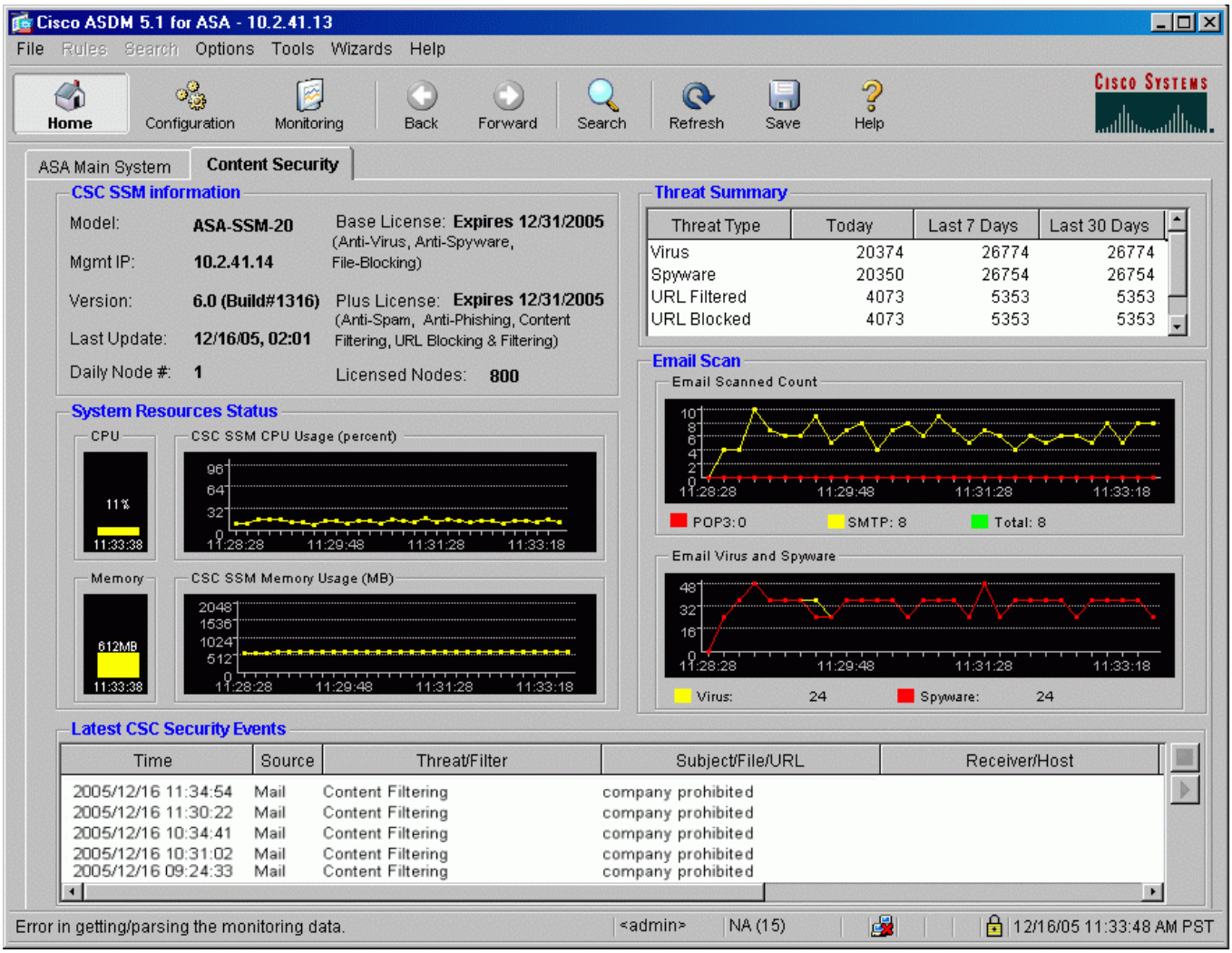
This chapter describes monitoring content security from ASDM, and includes the following sections:

Features of the Content Security Tab

After you have connected to the CSC SSM, the Content Security tab displays, as shown in Figure 7-1 on page 7-2. The Content Security tab shows you content security status at a glance, including:

- CSC SSM Information — Displays the product model number, IP address of the device, version and build number of the CSC SSM software, and important information
- Threat Summary — Displays a table summarizing threats detected today, within the last 7 days, and within the last 30 days
- System Resources Status — Allows you to view CPU and memory utilization on the SSM
- Email Scan — Provides a graphical display of number of email messages scanned and number of threats detected in the scanned email
- Latest CSC Security Events — Lists the last 25 security events that were logged

Figure 7-1 Content Security Tab



Click the Help icon to view more detailed information about the information that appears in this window.

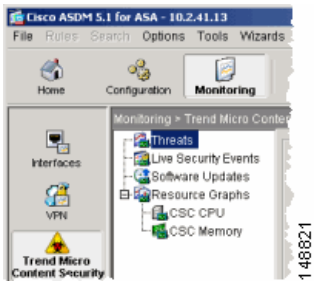
Monitoring Content Security

Click **Monitoring > Trend Micro Content Security** to display the Monitoring options. These options are:

- Threats—View graphs that display recent threat activity in the following categories:
- Live Security Events—Displays a report of recent security events (content-filtering violations, spam, virus detections, spyware detections, and so on) for monitored protocols
- Software Updates—Displays the version and last update date/time for content security scanning components (virus pattern file, scan engine, spyware/grayware pattern, and so on)
- Resource Graphs—Displays graphs of CPU utilization and memory utilization for the SSM

The appearance of the Monitoring options in ASDM is shown in Figure 7-2:

Figure 7-2 Content Security Monitoring Options in ASDM



Monitoring Threats

When you click Threats in the Monitoring pane, as shown in Figure 7-2, you can choose up to 4 categories of threats for graphing. You can display recent activity in the following categories:

- Viruses and other threats detected
- Spyware blocked
- Spam detected (this feature requires the Plus license)
- URL filtering activity and URL blocking activity (this feature requires the Plus license)

For example, assume you have both the Base and Plus license, and you choose all four threat types for monitoring. The graphs might appear as shown in Figure 7-3:

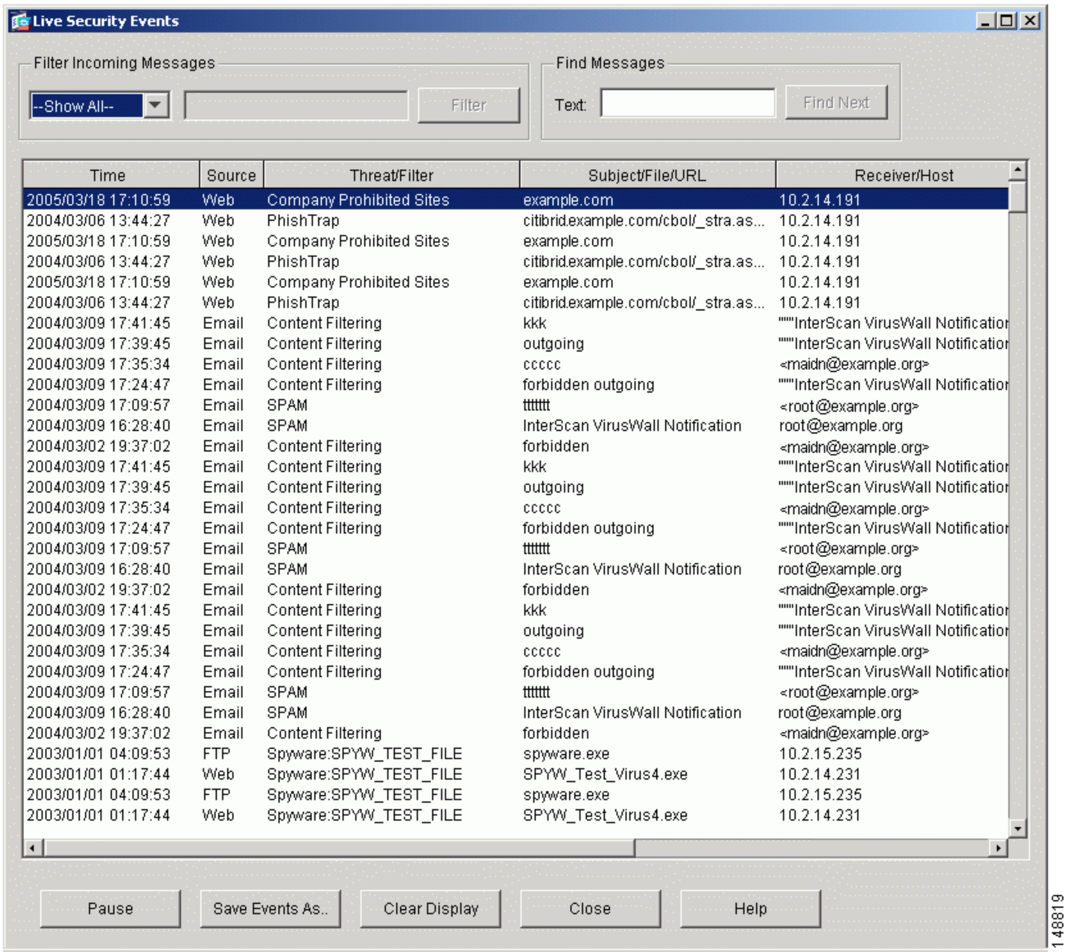
Figure 7-3 Threat Monitoring Graphs

The graphs refresh on frequent intervals (every 10 seconds), allowing you to see recent activity at a glance. See the online help for more information.

Monitoring Live Security Events

When you click Live Security Events in the Monitoring pane, after you click **View**, a report similar to the example in Figure 7-4 is created:

Figure 7-4 Live Security Events Monitoring Report

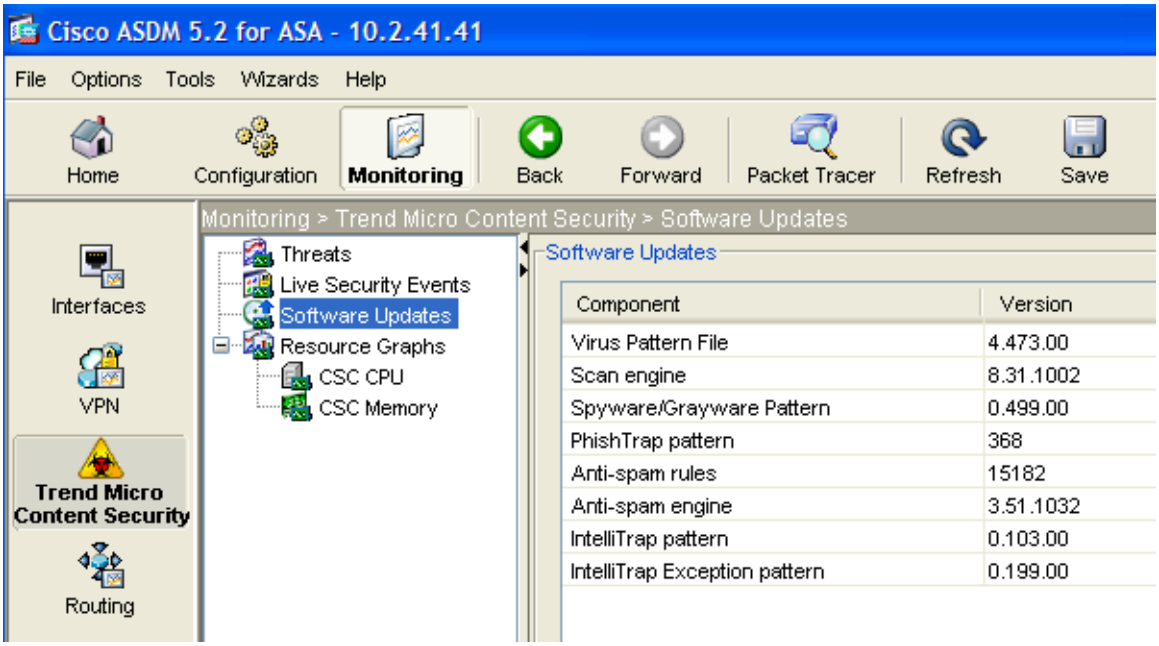


This report lists events detected by CSC SSM. The **Source** column displays “Email” for both SMTP and POP3 protocols. The horizontal and vertical scroll bars allow you to view additional report content. Filters at the top of the screen allow you to refine your search for specific events. See the online help for more information.

Monitoring Software Updates

When you click Software Updates in the Monitoring pane, as shown in Figure 7-5, the following information about the CSC SSM components displays:

Figure 7-5 Software Updates Monitoring Window



Click the **Configure Updates** link on **Monitoring > Trend Micro Content Security > Software Updates** in ASDM to display the Scheduled Update window in the CSC SSM console. See Figure 2-4 on page 2-5.

The Scheduled Update window allows you to specify the interval at which CSC SSM receives component updates from the Trend Micro ActiveUpdate server, which can be daily, hourly, or every 15 minutes.

You can also update components on demand via the Manual Update window in the SCS SSM console. See Figure 5-1 on page 5-2. Also see the online help for more information about both types of updates.

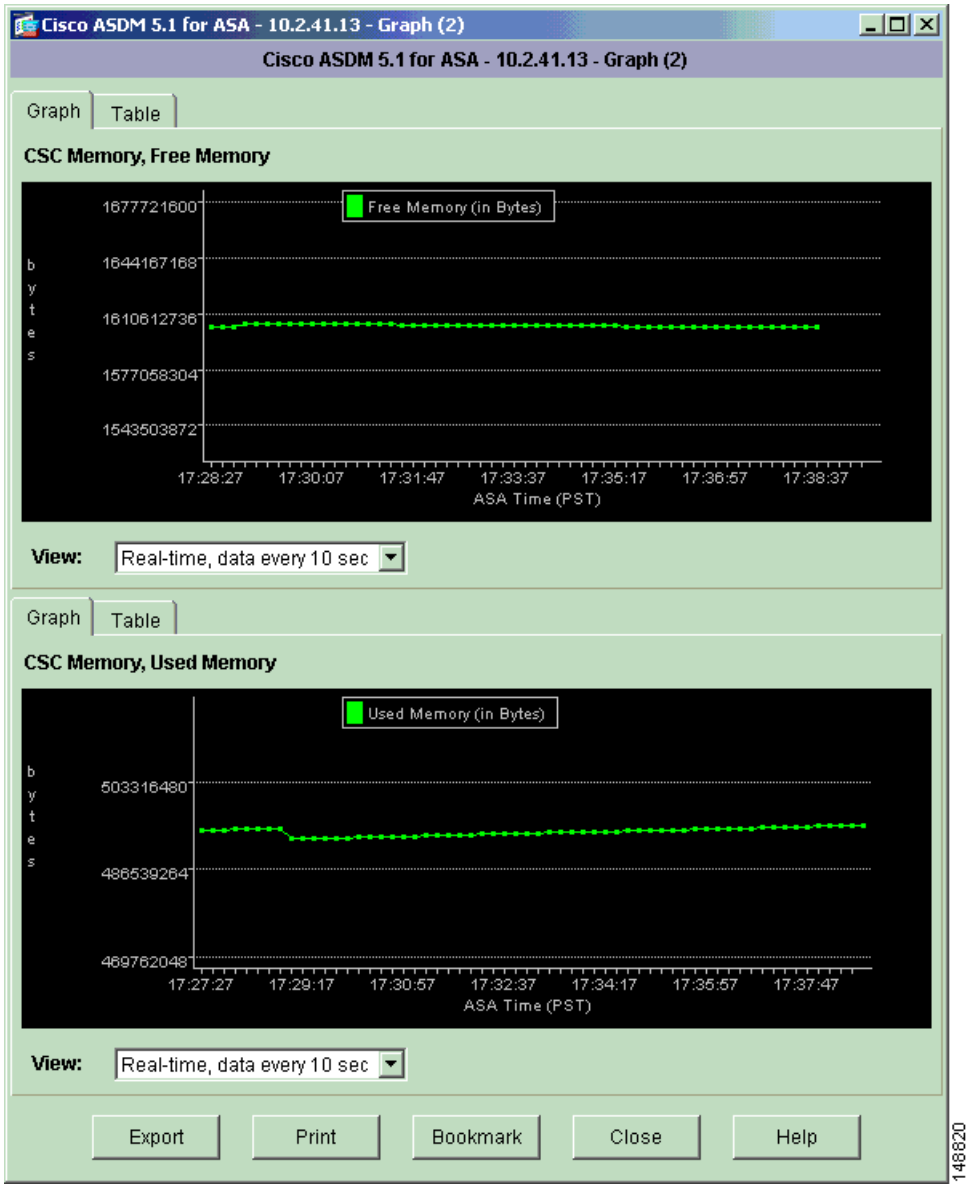
Monitoring Resources

When you click Resource Graphs in the Monitoring pane, there are two types of resources you can monitor, CPU usage, and memory. If these resources are running close to 100% usage, you might want to:

- Upgrade to ASA-SSM-20 (if you are currently using ASA-SSM-10), or
- Purchase another ASA appliance

To view CPU or memory usage, choose the information for viewing and click **Show Graphs**. For example:

Figure 7-6 Memory Monitoring Graphs



CHAPTER 8

Troubleshooting Trend Micro InterScan for Cisco CSC SSM

This chapter is provided to help you troubleshoot potential issues before contacting Cisco TAC for assistance, and includes the following sections:

Troubleshooting Installation

The following describes a successful command-line version of the installation. If trouble arises during the installation, see the "What To Do If Installation Fails" section on page 8-4.

To install the CSC SSM via the command-line interface, perform the following steps.

Step 1 From the command-line prompt, type the following to begin the installation:

```
hostname# hw-module module 1 recover configure
```

The output appears similar to the following:

```
Image URL [tftp://171.69.1.129/dqu/sg-6.0-1345-tftp.img]:
Port IP Address [30.0.0.3]:
VLAN ID [0]:
Gateway IP Address [30.0.0.254]:
hostname# 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#
hostname# debug module-boot
```

```
debug module-boot enabled at level 1
```

Step 2 After about a minute, the CSC-SSM drops into ROMMON, and prints messages similar to the following:

```
hostname# Slot-1 206> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50 PST
2005
Slot-1 207>     morlee@bowmore:/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/sg-6.0-1345-tftp.img
Slot-1 219>   CONFIG=
Slot-1 220>   LINKTIMEOUT=20
Slot-1 221>   PKTTIMEOUT=2
Slot-1 222>   RETRY=20
Slot-1 223> tftp dqu/sg-6.0-1345-tftp.img@171.69.1.129 via 30.0.0.254
```

Step 3 The SSM attempts to connect to the TFTP server to download the image. 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
```

Step 4 The TFTP download is complete. Note the number of received bytes, which should be the same size as your CSC SSM image. ROMMON then launches the image.

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

Step 5 The image is being unpacked and installed. After several minutes, CSC SSM reboots. Messages similar to the follow appear.

```
Slot-1 408> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50 PST 2005
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...
```

Step 6 After a minute or two, the CSC SSM boots up. Verify that the system has booted as follows:

```
hostname# show module 1
```

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 6.0 (Build#1345)

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down              6.0 (Build#1345)

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

Look for the two instances of “Up” in the Mod Status table (the last line of the output). The “Down” 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 failure occurs during the steps described in the “Troubleshooting Installation” section on page 8-2.

Table 8-1 What to Do If Installation Fails

If installation failure occurs at this step:	Your action is:
Step 2	Call Cisco TAC.
Step 3	1. Make sure you set the gateway IP address to 0.0.0.0 if your TFTP server is in the same IP subnet as your CSC SSM. 2. If there is any router/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 the TFTP server itself. 3. Verify the image path exists on the TFTP server, and that the directory and file are readable to all users.
Step 4	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. Try another TFTP server in this case.
Step 5	Download the image again and try once more to install. If the install is not successful a second time, contact Cisco TAC.
Step 6	Download the image again and try once more to install. If the install 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 ASA. See *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for more information, as well as the ASDM online help.

Next, 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

The following sections describe issues you may encounter with basic functions, such as logging on or password recovery:

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. This is not the same password that you use to access ASDM. Passwords are case-sensitive, so be sure you have entered the characters correctly.

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

Recovering a Lost Password

There are three passwords used to manage the ASDM/CSC SSM. They are:

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

The default entry for all three passwords is “cisco.”

The following describes how to recover your passwords in case you lose one or more of them:

- If you have the ASDM/Web interface password, but have lost the cisco and root account passwords, you can continue to manage the CSC SSM via the Web interface. However, there is no way to use the command-line interface or root account if you should need to at some time in the future. To recover these two passwords, re-image the CSC SSM and restore your configuration using the steps described below.
- If you have only the CLI password, you can log in to the CSC SSM and navigate to the "Restore Factory Defaults" option to reset the SSM, which has the same effect as re-imaging the device. Then import your saved configuration. See Restore Factory Defaults, page A-10 for more information about the Restore Factory Defaults option.
- If you have only the root account password, log in and use the **password** command to set the CLI password. Then proceed as described in the previous paragraph.

Caution Only access the root account under the supervision of Cisco TAC. Unauthorized modifications made through the root account are not supported and will require the device to be reimaged to guarantee proper operation.

- If you have lost all three passwords you must re-image the device and restore your configuration as described below.

To re-image the CSC SSM and recover your configuration, follow these steps:

Step 1 Re-image the CSC SSM, which restores the factory default settings. Re-imaging transfers a factory default software image to the SSM. Transferring an image is described in the "Reimaging and Configuring the CSC SSM Using the Command Line" section on page A-1.

Step 2 After re-imaging, all passwords are restored to their default value. You can now log in using the default password "cisco" and create a new ASDM/Web interface password.

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

Step 4 Import the most recent configuration backup to restore your configuration settings.

Step 5 Using the default password "cisco," access the command-line interface and the root account to update the default CLI and root account passwords as well.

Summary Status and Log Entries Out of Synch

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 to the statistics displayed in the log reports. (In the CSC SSM console, the logs are accessed by choosing **Logs > Query**.) This "mismatch" happens because:

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

Delay in HTTP Connection

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. CSC SSM attempts to access the URL database when intercepting an HTTP request from a client. If you cannot grant Internet access to CSC SSM (either direct, or indirect via a proxy), disable URL filtering.

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 hard-coded 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 fail.

The workaround is to exclude the site from scanning. To do so from the command-line interface, for example, for a site on the outside network with the IP address 192.168.10.10:

```
! exempt http traffic to 192.168.10.10
    access-list 101 deny tcp any host 192.168.10.10 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
```

The above configuration exempts HTTP traffic to 192.168.10.10 from being scanned by the CSC SSM.

Performing a Packet Capture

If there are sites you can access without going through CSC SSM, but cannot access when traffic is being scanned, report the URL to Cisco TAC. If possible, do a packet capture and send the information to Cisco TAC as well. For example, assuming the client has IP address 1.1.1.1, and the outside website has IP address 2.2.2.2:

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

FTP Download Does Not Work

If your FTP login works, but you cannot download via FTP, verify whether the **inspect ftp** setting is enabled on the ASA. See the *Cisco Security Appliance Command Line Configuration Guide* for more information.

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

The following sections describe issues you may encounter with scanning for viruses and/or spam.

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 on 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.

Another possible cause is that the Trend Micro ActiveUpdate server is temporarily down. Try to update again in a few minutes.

Spam Not Being Detected

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

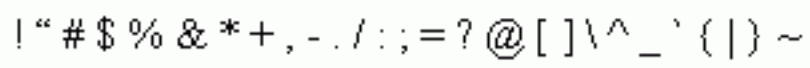
- You have the Plus License installed.
- You have enabled the feature; the anti-spam option is *not* enabled by default (See Enabling SMTP & POP3 Spam Filtering, page 3-6 for more information)
- You have configured the incoming mail domain (See Configuring SMTP Message Filter, Disclaimer, & Incoming Mail Domain, page 3-5 for more information)

Cannot Create a Spam Stamp Identifier

A spam stamp identifier is a message that appears in the email 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 upper and lowercase characters, digits 0-9, or the set of special characters shown in Figure 8-1.

Figure 8-1 Special characters for spam stamp identifier



If you attempt to use characters other than those specified, you cannot use the spam identifier for your 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. See the online help for these two windows for more information.

Also, if users in your network are receiving newsletters, this type of message tends to trigger a high number of false positives. Add the newsletter email 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

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 > SMTP Incoming Anti-spam** window and the **Mail (POP3) > Anti-spam > POP3 Anti-spam** window.

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 on what to do, including how to submit your suspected virus to TrendLabs for evaluation.

Virus Scanning Not Working

Ensure that no one has disabled the virus scanning feature on the SMTP Incoming, SMTP Outgoing, POP3, HTTP, and FTP Scanning windows. If scanning is enabled but viruses are not being detected, contact customer support for assistance.

Also, test the virus scanning feature by following the directions described in the "Test the Antivirus Feature" section on page 2-3.

Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration

Another possible cause is that a file has not been scanned due to incorrect ASA firewall policy configuration. Use the ASA **show service-policy csc** command in the CLI to configure the SSM to process traffic. For example:

```
show service-policy flow tcp host [clientIP] host [server IP] eq [proto]
```

For example:

```
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, a syslog error 421007 is generated. In the CLI, enter the following command to view the status of the SSM card:

```
hostname# show module 1
```

The output appears in several tables, as shown in the following example. The third table (SSM Application Name) displays a status. In this example, the status of the SSM is "Down."

```
Mod Card Type                                    Model  Serial No.
--- -------------------------------------------- ---------------------------
1 ASA 5500 Series Security Services Module-10  ASA-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 6.0 (Build#1345)

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------------------
  1 CSC SSM                        Down             6.0 (Build#1345)
```

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

There are three possible states that could display in the **Status** field for the third table:

- **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, issue the following command in the CLI:

```
hostname# show module 1 detail
```

The output appears similar to the following:

```
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 6.0 (Build#1345)
    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:       6.0 (Build#1345)
    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 is shown in the **App. Status** field. In the example, the status is “Down.” The possible states for this field are:

- **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 card is 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

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, 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 could:

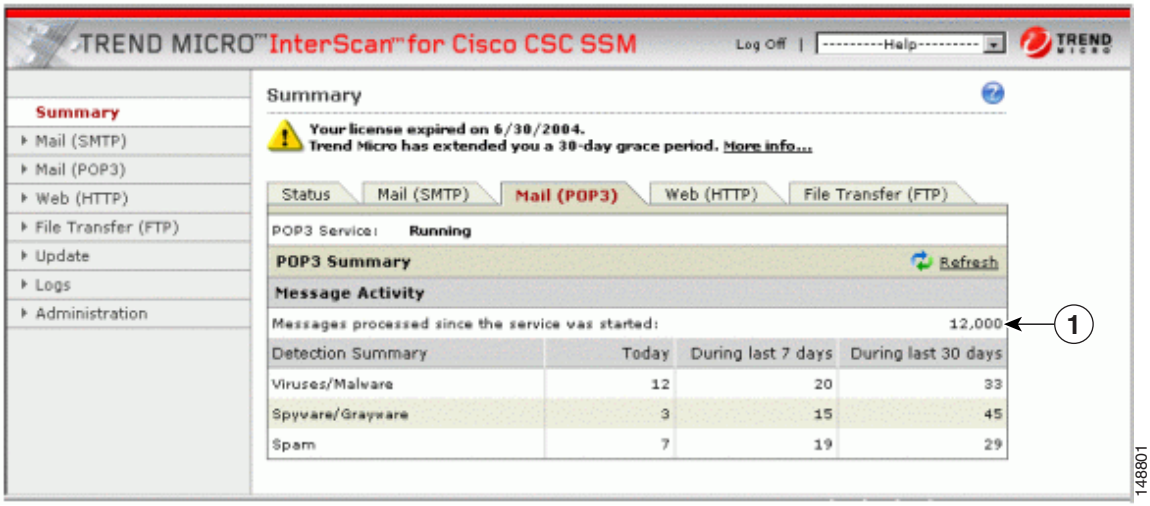
- Result in the file being downloaded, but very slowly at first with more rapid speed as the download progresses
- Take longer than the automatic browser timeout period, with the result being that the user is unable to receive the file contents at all (because the browser times out before the download completes)

If you enabled deferred scanning, part of the content of the large file is delivered without scanning to prevent timeout. 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, but the unscanned portion of the large file is already stored on the user's machine and may introduce a security risk.

Restart Scanning Service

The Mail (SMTP and POP3) tabs on the Summary window display a count of **Messages processed since the service was started** in the Message Activity area of the window. For an example, see Figure 8-2.

Figure 8-2 Messages Processed Counter on the Mail (POP3) Tab of the Summary Window



1	Message activity counter

Several events can cause these counters to reset to zero. The events are:

- A pattern file or scan engine update
- A configuration change
- 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, regardless of the above events.

There is nothing wrong when the counters reset. If, however, you have a continuous zero in the **Messages processed...** fields, this indicates that email traffic is not being scanned and you should investigate the situation.

Troubleshooting Performance

The following sections describe issues you may encounter with performance.

CSC SSM Console Timed Out

If you leave the CSC SSM console active and there is no activity detected for approximately 10 minutes, your session is timed out. Log in again to resume work. Unsaved changes to your work are lost. If you are called away, it's best to save your work and log off until your return.

Status LED Flashing for Over a Minute

If the **Status** LED continues flashing for more than a minute, the scanning service is not available. To resolve this problem, reboot the system from ASDM, or contact customer support for assistance.

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

See the "Reset Management Port Access Control" section on page A-14 for information on resetting port access controls, which may solve this problem.

Logging in Without Going Through ASDM

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

Step 1 Type the following URL in a browser window:

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

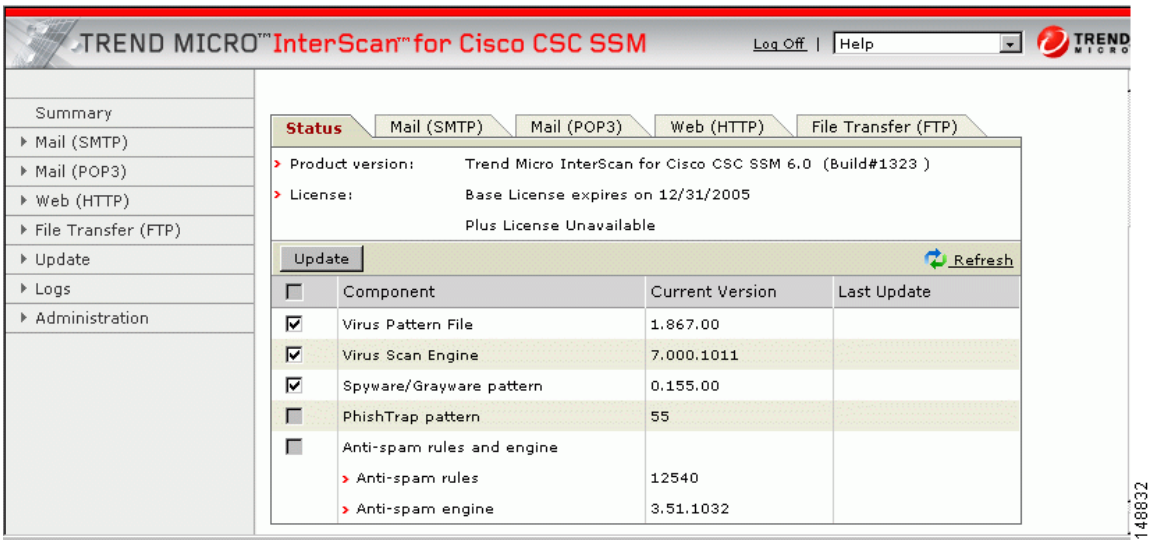
For example:

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

Step 2 The **Logon** window displays. Type the password you created on the **Password Configuration** installation window in the setup wizard and click **Log On**.

Step 3 The default view of the CSC SSM console is the Status tab on the **Summary** window:

Figure 8-3 Status Tab of the Summary Screen on the CSC SSM Console



CSC SSM Throughput is Significantly Less Than ASA

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

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

Refer to the "Managing AIP SSM and CSC SSM" chapter of the *Cisco Security Appliance Command Line Configuration Guide* for more information.

Using Knowledge Base

You are welcome to search for more information in the Trend Micro online Knowledge Base. The Knowledge Base URL is:

http://esupport.trendmicro.com

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

Using the Security Information Center

Comprehensive security information is available 24x7 from the Trend Micro Security Information Center, which is a free online resource. The Security Information Center URL is:

http://trendmicro.com/vinfo/

The Security Information Center provides information such as the following:

- **Virus Encyclopedia**—A compilation of knowledge about all known threats, including viruses, worms, Trojans, and others
- **Security Advisories**—View 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/Grayware**—Information about the top ten spyware/grayware programs, and a searchable database of spyware/grayware 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

Figure 8-4 Virus Map

- **Weekly Virus Report** —Current news about threats that have appeared in the past week (Subscribe to the Weekly Virus Report to automatically receive a copy each week via email.)
- General virus information, including:
  - **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/grayware threats 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 Syslogs

CSC SSM-related syslog messages are listed and described as follows:

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 re-enable failover.

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 1 message every 10 seconds.

interface_name—The interface name.

IP_address—The IP address.

port—The port number.

application—The CSC SSM is the only application supported in the current release.

Recommended Action Immediately investigate the problem with the service module.

Skip Non-applicable Traffic [6-421002]

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

Explanation Connection bypassed 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 1 message every 10 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 is the only application supported in the current release.

Recommended Action The configuration should be modified to only include protocols that are supported by 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 a Cisco proprietary protocol called ASDP. Any packet that does not have the proper 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.

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 security appliance has failed to inject a packet as instructed by the service module. This could happen if the security appliance tries to inject a packet into a flow that has already been released.

IP_address—The IP address.

port—The port number.

Recommended Action This could happen because the security appliance maintains its connection table independently from the service module. Normally it will not cause any problem. If this affects security appliance performance, contact Cisco TAC.

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 is the only application supported in the current release.

Recommended Action No action required. However, if the overall count exceeds the user license you have purchased, contact Cisco to upgrade your license.

Daily Node Count [5-421006]

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

Explanation 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.

Recommended Action No action required. However, if the overall count exceeds the user license you have purchased, contact Cisco to upgrade your license.

Traffic Dropped Because of CSC Card Failure [6-421007]

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 1 message every 10 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 is the only application supported in the current release.

Recommended Action Immediately investigate the problem with the service module.

New Application Detected [5-505011]

Error Message `%ASA-5-505011: Module in slot` *slot*`, application detected` *application*`, version` *version*`.`

Explanation A new application was detected on a 4GE SSM. This may occur when the system boots, when the 4GE SSM boots, or when the 4GE SSM starts a new application.

slot—The slot in which the application was detected.

application—The name of the application detected.

version—The application version detected.

Recommended Action No action required if the activity described is normal and expected.

Application Stopped [5-505012]

Error Message `%ASA-5-505012: Module in slot` *slot*`, application stopped` *application*`, version` *version*

Explanation This message is generated whenever an application is stopped or removed from a 4GE SSM. This may occur when the 4GE SSM upgrades an application or when an application on the 4GE SSM is stopped or uninstalled.

slot—The slot in which the application was stopped.

application—The name of the application stopped.

version—The application version stopped.

Recommended Action If an upgrade was not occurring on the 4GE SSM or the application was not intentionally stopped or uninstalled, review the logs from the 4GE SSM to determine why the application stopped.

Application Version Changes [5-505013]

Error Message `%ASA-5-505013: 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.

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.

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 4GE SSM. This failure triggers a failover when it occurs on the active 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 4GE SSM. This message is

generated whenever there is a communication problem over the security appliance dataplane between the system module and the 4GE SSM. This can be caused when the 4GE SSM stops, resets, or is removed.

slot—The slot in which the failure occurred.

Recommended Action If this is not the result of the 4GE SSM reloading or resetting and a corresponding message 5-505010 is not seen after the 4GE SSM returns to an UP state, the module may need to be reset using the **hw-module module 1 reset** command.

Data Channel Communication OK [5-505010]

Error Message `%ASA-5-505010: 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 No action required unless this message was generated as a result of a previous data channel communication failure (message 3-323006). In that case, check the 4GE SSM messages to determine the cause of the communication failure.

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-protocol-virus: 2006/01/01 16:33:01|
WORM_GREW.A|grayware|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete|Deli
ver|
```

Explanation This syslog 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 -email.

action_on_the_content—Action taken on the e-mail content.

action_on_the_email—Action taken on the entire e-mail.

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

Spyware/Grayware detection event

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

Example:

```
is-mail-grayware: 2006/01/01 16:33:01|
|Spyware|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete|Deliver|
```

Explanation This syslog 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.

mail—The e-mail message involved.

time—Date and time of the event.

malware_name—Name of the malware.

malware_type—Type of the malware.

from_address—From address of the -email.

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 email.

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

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: 2006/01/01
19:37:02|fromtester@trendmicro|totester@trendmicro.com|subject|Delete|Deliver|
```

Explanation This syslog 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_address—From address of the email

to_address—To address of the email

action_on_the_content—Action taken on the email content

action_on_the_email—Action taken on the whole email

Recommended Action No action is required. If the spam mail is generated from a similar source, you may add this source to the Blocked Sender list to reduce the email volume.

HTTP URL filtering event

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

Example:

```
is-url-filtering: 2006/01/01 17:10:59|forbidden.com/|10.2.3.4|Company Prohibited Sites|
```

Explanation This syslog 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 No action is required. Adjust the URL filtering setting if you want this URL (category) to be allowed.

HTTP URL blocking event

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

Example:

```
is-url-blocking: 2006/01/01 17:10:59|blocked.com/|10.2.3.4|PhishTrap|
```

Explanation This syslog 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 No action is required.

Syslog adaptor starting

Error Message `is-syslog: ISSyslog Adaptor 1.0`

Example:

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

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

Recommended Action No action is required.

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 syslog 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 syslog, a notification email 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—equals the daily count minus the number of seats

Recommended Action Contact a Trend Micro sales representative for a license upgrade.

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 syslog 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 CSC SSM or contact Cisco TAC.

Scan service recovered

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

Example:

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

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

service_title—The name of the service.

Recommended Action No action is required.

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 syslog 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/pattern, the status is set to RELOAD and the ASA will perform 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. ASA will perform fail-open, fail-close or fail-over depending how it has been configured on the ASA.

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.

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 syslog 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 syslog message is generated when 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 No action is required.

System monitor started

Error Message `SysMonitor: INFO: SysMonitor started.`

Example:

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

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

Recommended Action No action is required.

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 syslog message is generated when a socket timeout is experienced when 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 No action is required.

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 syslog message is generated when CSC SSM reaches the maximum number of concurrent connections set for a given protocol.

protocol—The protocol involved

Recommended Action Configure ASA to bypass certain traffic from CSC SSM scanning or segment the network to another ASA device.

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

protocol—The protocol involved

Recommended Action No action is required.

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 syslog 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.

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 syslog 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.

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 syslog 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 ASA 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 syslog message is generated when the automatic "heartbeat failure" notification emailed 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.

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 6.0 (Build#1349)
```

Explanation This syslog message displays the CSC application name, version and running state during Service Module start up.

process_id—Process ID of the daemon

text—Description of name or version

up/down—Service is up or down

Recommended Action No action is required.

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 6.0 (Build#1349)
```

Explanation This syslog message displays the output of the "show module 1 details" command produced by the Service Module.

process_id—Process ID of the service module

text—Description of name or version

up/down—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 No action is required.

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 syslog message is generated when the Service Module is unable to synchronize the SSM system time with the PIX system time.

process_id—Process ID of the service module

Recommended Action No action is required.

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 syslog 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 CSC subsystem

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

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 syslog message is generated when the IPC is unable to communicate with another CSC subsystem.

process_id—Process ID of the service module

ipc_operation—IPC (Inter-process Communication) operation

Recommended Action No action is required.

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 syslog message is generated when the Service Module fails to communicate with the ASA chassis.

process_id—Process ID

Recommended Action No action is required.

Before Contacting Cisco TAC

Before you contact the Technical Assistance Center (TAC), check the documentation and online help to see if it contains the answer you are looking for. If you have checked the documentation, as well as Knowledge Base, and still need help, please be prepared to give the following information to speed the resolution of your problem:

- 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.

Reimaging and Configuring the CSC SSM Using the Command Line

The Trend Micro InterScan for Cisco CSC SSM software is preinstalled on the appliance. Typically, you will only need to use the information in this appendix for password or system recovery procedures.

Note The setup wizard launched from the ASDM is the preferred method of installation, if installation is required. See *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for more information.

This appendix includes the following sections:

Installation Checklist

Before you start, be prepared to supply the following information. Print a copy of this page and use it as a checklist if you prefer, to record the values you are prompted to enter during installation.

You are prompted to enter:	Your entry is:	Checkoff
Administrator password (for the CLI)	Do not record your password	
SSM card IP address		❑
Subnet mask		❑
Host name (1-63 alphanumeric characters; can include hyphens except as the first character)—for example, cisco1-ssm-csc		❑
Domain name		❑
Primary DNS IP address		❑
Secondary DNS IP address (optional)		❑

You are prompted to enter:	Your entry is:	Checkoff
Gateway IP address		❑
Proxy server? (optional) If yes: Proxy server IP Proxy server port		 ❑ ❑
Domain name for incoming mail		❑
Administrator password for the CSC SSM console	Do not record your password	
Administrator email address		❑
Notification email server IP		❑
Notification email server port		❑
Base License Activation Code		❑
Plus License Activation Code (optional)		❑

Preparing to Reimage the Cisco CSC SSM

During installation, you are prompted to synchronize the date and time on the SSM with the security appliance. Before you begin, make sure that the date/time settings on the appliance are correct.

To install via the command line, perform the following steps:

Step 1 Download the Trend Micro InterScan for Cisco CSC SSM software to your TFTP server.

Step 2 Using a terminal application such as Windows HyperTerminal, log on and open a terminal session to the ASA console. At the prompt, enter:

```
hostname# hw module 1 recover config
```

The system response is similar to the following example:

```
Image URL [tftp://insidehost/sg-6.0-1177-tftp.img]: tftp://insidehost/sg-6.0-1177-tftp.img
Port IP Address [192.168.7.20]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
hostname# hw 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]
```

Step 3 Enter **y** to confirm.

```
Recover issued for module in slot 1
```

Caution The module recovery can loop if the image is corrupt or if the size of the image file exceeds the limitations on the TFTP server. If the module is stuck in a recovery loop, you must enter the following command to stop the module from trying to load the image.

```
hw module 1 recover stop
```

Step 4 Enable the debug-module boot command:

```
hostname# debug module-boot
debug module-boot enabled at level 1
hostname# Slot-1 199> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49 PST
2005
Slot-1 200> Platform SSM-IDS20
Slot-1 201> GigabitEthernet0/0
Slot-1 202> Link is UP
Slot-1 203> MAC Address: 000b.fcf8.0134
Slot-1 204> ROMMON Variable Settings:
Slot-1 205>   ADDRESS=192.168.7.20
Slot-1 206>   SERVER=192.168.7.100
Slot-1 207>   GATEWAY=0.0.0.0
Slot-1 208>   PORT=GigabitEthernet0/0
Slot-1 209>   VLAN=untagged
Slot-1 210>   IMAGE=sg-6.0-1177-tftp.img
Slot-1 211>   CONFIG=
Slot-1 212> tftp sg-6.0-1177-tftp.img@192.168.7.100
Slot-1 213> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 214> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
```

Note This process takes about 10 minutes.

```
.
.
.
Slot-1 389>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 390> Received 57985402 bytes
Slot-1 391> Launching TFTP Image...
Slot-1 392> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49 PST 2005
Slot-1 393> Platform SSM-IDS20
Slot-1 394> GigabitEthernet0/0
Slot-1 395> Link is UP
Slot-1 396> MAC Address: 000b.fcf8.0134
Slot-1 397> Launching BootLoader...
```

Step 5 Disable the debug-module boot command:

```
hostname# no debug module-boot
```

Step 6 Show module 1 details. Sample code output is shown below:

```
JDPIX# show module 1 d
Getting details from the Service Module, please wait...
SSM-IDS/10-K9
Model:              SSM-IDS10
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.0 (Build#1345)
MAC Address Range:  000b.fcf8.0159 to 000b.fcf8.0159
App. name:          CSC SSM
App. Status:        Down
App. Status Desc:   CSC SSM scan services are not available
App. version:       6.0 (Build#1345)
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>
```

Step 7 Open a command session:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 8 Log in to Trend Micro InterScan for Cisco CSC SSM using the default login name “cisco” and password “cisco.”

```
login: cisco
Password:
```

Step 9 You are prompted to change your password immediately. Do not use the same password that you use to access the ASDM.

```
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
New password:
Retype new password:
```

Reimaging the CSC SSM

To reimage the appliance using the command line Setup Wizard:

Step 1 After you confirm your administrator CLI password, the Trend Micro InterScan for Cisco CSC SSM Setup Wizard appears.

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
------------------------------------------------------------------------------
To set up the SSM, the wizard prompts for the following information:
    1. Network settings
    2. Date/time settings verification
    3. Incoming email domain name
    4. Web console administrator password
    5. Notification settings
    6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

Choose **1** to configure network settings and press **Enter**.

Step 2 The Network Settings prompts appear:

```
Network Settings
------------------------------------------------------------------------------
Enter the SSM card IP address:
Enter subnet mask:
Enter host name:
Enter domain name:
```

```
Enter primary DNS IP address:
Enter optional secondary DNS IP address:
Enter gateway IP address:
Do you use a proxy server? [y|n]
```

Respond to the network settings prompts, using values from the installation checklist. When you are finished with the last network settings prompt, your entries display for a visual verification. For example:

```
Network Settings
------------------------------------------------------------------------
IP              192.168.7.20
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     example.com

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         192.168.7.1
No Proxy

Are these settings correct? [y|n] y
```

Step 3 If the settings are correct, enter **y** to confirm. (If you choose **n**, the Network Settings prompts appear again; repeat Step 2.)

Step 4 After you confirm your network settings, the system responds with the following message:

```
Applying network settings ...
```

Optionally confirm the network settings by pinging the gateway IP address. To skip pinging, enter **n**.

```
Do you want to confirm the network settings using ping? [y|n] y
Enter an IP address to ping: 192.168.7.1
PING 192.168.7.1 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue ...
```

Step 5 The Date/Time Settings prompt appears.

```
                        Date/Time Settings
------------------------------------------------------------------------

SSM card date and time: 10/06/2005 18:14:14

The SSM card periodically synchronizes with the chassis.
Is the time correct? [y|n] y
```

Respond **y** to set the date and time to be synchronous with the chassis. To update the date and time, enter **n**, exit the installation wizard, update the date/time or NTP settings on the ASA chassis, and restart installation of the SSM.

Step 6 The Incoming Domain Name prompt appears.

```
Incoming Domain Name
------------------------------------------------------------------------
```

```
Enter the domain name that identifies incoming email messages: (default:example.com)
Domain name of incoming email: example.com
Is the incoming domain correct? [y|n] y
```

Type your highest level domain name for your organization and enter **y** to continue.

Step 7 The Administrator/Notification Settings prompts appear.

```
Administrator/Notification Settings
------------------------------------------------------------------------

The password will be hidden while you type.
Web console administrator password:
Retype Web console administrator password:
Administrator email address:
Notification email server IP:
Notification email server port: (default:25)
```

When you have made your entries, a confirmation appears as shown in the following example:

```
Administrator/Notification Settings
------------------------------------------------------------------------

Administrator email address: tester@example.com
Notification email server IP: 10.2.202.28
Notification email server port: 25
Are the notification settings correct? [y|n] y
```

Enter **y** to continue.

Step 8 The Activation prompts appear.

```
                            Activation
------------------------------------------------------------------------

You must activate your Base License, which enables you to update
your virus pattern file. You may also activate your Plus License.

Activation Code example: BV-43CZ-8TYY9-D4VNM-82We9-L7722-WPX41
Enter your Base License Activation Code: PX-ABTD-L58LB-XYZ9K-JYEUY-H5AEE-LK44N
Base License activation is successful.

(Press Enter to skip activating your Plus License.)
Enter your Plus License Activation Code: PX-6WGD-PSUNB-9XBA8-FKW5L-XXSHZ-2G9MN
Plus License activation is successful.
```

Step 9 The Activation Status appears.

```
Activation Status
------------------------------------------------------------------------

Your Base License is activated.
Your Plus License is activated.

Stopping services: OK
Starting services: OK

The Setup Wizard is finished.
Please use your Web browser to connect to the management console at:
https://192.168.7.20:8443
Press Enter to exit ...

Remote card closed command session. Press any key to continue.
```

```
Command session with slot 1 terminated.
hostname#
```

The services starting message lets you know that installation is complete. As suggested in the prompt at the end of the Setup Wizard, use your browser to log on to the CSC SSM console. Enter the URL in the following format:

```
https://<SSM IP address>:8443/
```

Confirming the Installation

When the reimaging is complete, perform the following steps:

Step 1 Enter the following command to view information about the SSM and the services you configured during installation:

```
hostname# show module 1 details
```

The system responds as follows:

```
Getting details from the Service Module, please wait...
SSM-IDS/20-K9
Model: SSM-IDS20
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.0 (Build#1177)
MAC Address Range:  000b.fcf8.0134 to 000b.fcf8.0134
App. name:          CSC SSM proxy services are not available
App. version:
App. name:          CSC SSM
App. version:       6.0 (Build#1177)
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Mail Service:       Up
FTP  Service:       Up
Activated:          Yes
Mgmt IP addr:       192.168.7.20
Mgmt web port:      8443
Peer IP addr:       <not enabled>
hostname#
```

Step 2 Open a command session as follows:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 3 Log in using the default login name “cisco” and the password that you configured on the Administrator/Notification Settings window during installation.

```
login: cisco
Password:
Last login: Mon Oct 10 13:24:07 from 127.0.1.1
```

The Trend Micro InterScan for Cisco CSC SSM Setup Main menu appears.

```
     Trend Micro InterScan for Cisco CSC SSM Setup Main Menu
------------------------------------------------------------------------

1. Network Settings
2. Date/Time Settings
3. Product Information
4. Service Status
5. Change Password for Command Line Interface
6. Restore Factory Default Settings
7. Troubleshooting Tools
8. Reset Management Port Access Control List
9. Ping
10. Exit ...

Enter a number from [1-10]:
```

View/Change Network Settings

Choose option **1** to view and/or modify your network settings configuration. The following appears:

```
Network Settings
------------------------------------------------------------------------

IP              192.168.7.20
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     tester@example.com
MAC address     00:0B:FC:F8:01:34

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         192.168.7.1
No Proxy

Do you want to modify the network settings? [y|n] n
```

Any of these settings can be changed via the command-line interface.

View Date/Time Settings

Choose option **2** to view the SSM date and time settings. The Date/Time Settings prompts appear:

```
Date/Time Settings
------------------------------------------------------------------------

SSM card date and time: 10/10/2005 13:27:09 PDT

Press Enter to continue ...
```

The settings cannot be changed, this information is for reference only.

View Product Information

Choose option **3** to view the component (version and build) settings. The Product Information prompts appear:

```
Product Information
----------------------------------------------------------------------

Main           version 6.0 build 1177
Mail component version 5.5 build 1064
Web component  version 2.1 build 1103

Press Enter to continue ...
```

The settings cannot be changed, this information is for reference only.

View Service Status

Choose option **4** to view the component (version and build) settings. The following appears:

```
Service Status
----------------------------------------------------------------------

The CSC SSM RegServer service is running
The CSC SSM HTTP service is running
The CSC SSM FTP service is running
The CSC SSM Notification service is running
The CSC SSM Mail service is running
The CSC SSM GUI service is running
The CSC SSM SysMonitor service is running
The CSC SSM Failoverd service is running
The CSC SSM LogServer service is running
The CSC SSM SyslogAdaptor service is running
The CSC SSM Syslog-ng service is running

Do you want to restart all services? [y|n] n
```

The **Do you want to restart all services prompt** allows you to restart scanning services. If everything is running smoothly, there is no need to restart. If you are trying to troubleshoot a problem, restarting may get you back in a proper operating status. See the "Restart Scanning Service" section on page 8-12 for more information about the impact of restarting services.

Change Password for Command Line Interface

Choose option **5** to display the Set Password for Command Line Interface prompts. The following appears:

```
Set Password for Command Line Interface
----------------------------------------------------------------------
This option allows you to change the password for the Command Line Interface
that you are currently using.
Do you want to continue? [y|n]

The password will be hidden while you type.
Changing password for cisco
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
```

```
Re-enter new password:
Password changed.
```

Follow the prompts to update your password.

Restore Factory Defaults

Choose option **6** to restore the pre-installation configuration settings. The Restore Factory Default Settings prompt appears:

```
Restore Factory Default Settings
------------------------------------------------------------------

Are you sure you want to restore the factory default settings? [y|n] n
```

Caution If you choose **y**, all your configuration settings are returned to the pre-installation default settings. See the "Default Mail Scanning Settings" section on page 3-1 and the "Default Web and FTP Scanning Settings" section on page 4-1 for a description of the default settings. Additional configurations you have made since installation, such as registration/activation, licensing, enabling spyware/grayware detection, file blocking, file blocking exceptions, and so on are lost.

While this option is available from the command line, a better alternative for restoring configuration settings is available from the CSC SSM console. Click **Administration > Configuration Backup** to view the Configuration Backup window. The Configuration Backup window allows you to save (export) your configuration settings into a configuration file that can be imported (restored) at a later time.

Choose the Restore Factory Default Settings option only if you need to start over and re-install the CSC SSM.

Troubleshooting Tools

Choose option **7** to display a menu of troubleshooting tools.

```
Troubleshooting Tools
------------------------------------------------------------------

1. Enable Root Account
2. Show System Information
3. Gather Logs
4. Gather Packet Trace
5. Modify Upload Settings
6. Return to Main Menu

Enter a number from [1-6]:
```

These tools are available to help you or Cisco TAC get information from the system to troubleshoot a problem.

Enable Root Account

Option **1** enables the root account. The following warning appears:

```
********************** WARNING **********************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
```

```
This account is intended to be used for support and
troubleshooting purposes only. Unauthorized modifications
are not supported and will require this device to be
re-imaged to guarantee proper operation.
******************************************************
Do you want to accept the warning and enable the root account? [y|n]
```

This warning appears only the first time you enable the root account. Once the root account is enabled, it cannot be disabled.

Caution This option is not intended for use by system administrators; it is provided for use by Cisco service personnel only. Do not select this option unless directed to do so by Cisco TAC.

Show System Information

Option **2** allows you to view helpful system information, either directly on the screen, or you can save the data to a file and transfer the information using FTP or TFTP. When you select option **2**, Show System Information menu displays:

```
Troubleshooting Tools - Show System Information
------------------------------------------------------------------------

1. Show System Information on Screen
2. Upload System Information
3. Return to Troubleshooting Tools Menu
```

Show System Information on Screen

Here is an example of system information displayed on the screen when you select option **1** from the Show System Information menu. This information is available from various locations on the ASDM and CSC SSM interfaces, but this CLI version makes it quickly available all in one place:

```
++++++++++++++++++++++
Mon Jan 9 18:38:01 PST 2006 (-8)

System is : Up

# Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.0 (Build#1340 )
SSM Model: SSM-10

# Scan Engine and Pattern Information
Virus Scan Engine: 8.100.1002 (Updated: 2006-01-09 14:10:07)
Virus Pattern: 3.149.00 (Updated: 2006-01-09 14:10:39)
Garyware Pattern: 0.327.00 (Updated: 2006-01-09 14:13:11)
PhishTrap Pattern: 223 (Updated: 2006-01-09 14:13:28)
AntiSpam Engine: 14196 (Updated: 2006-01-09 14:11:04)
AntiSpam Rule: 3.51.1033 (Updated: 2006-01-09 14:12:53)

# License Information
Product:Base License
Version:Full
Activation Code:BX-9YWQ-3685S-X39PZ-H96NW-MAJR7-CWBXR
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005
Product:Plus License
```

```
Version:Full
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005

Daily Node Count: 0
Current Node Count: 0

# Kernel Information
Linux csc 2.4.26-cscssm #2 SMP Mon Dec 19 11:53:05 PST 2005 (1.0.6) i686
unknn

ASDP Driver 1.0(0) is UP:
    Total Connection Records: 169600
    Connection Records in Use: 0
    Free Connection Records: 169600
```

The information continues to scroll. Enter **q** to quit.

Upload System Information

When you select option **2** from the Show System Information menu, the following prompts display:

```
Gathering System Information ...
Creating temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading file ...
Deleting temporary file CSCSSM-SYSINFO-20060109-184511.txt
Press Enter to continue ...
```

Follow and respond to the prompts to upload the system information. The system information is sent using the upload settings created using option **5**, Modify Upload Settings. See Modify Upload Settings, page A-13 for more information. If you did not configure the upload settings, the prompts are preceded by the following:

```
Choose a protocol [1=FTP 2=TFTP]: 1
Enter FTP server IP: 10.2.15.235
Enter FTP server port: (default:21)
Enter FTP user name: ftp
The password will be hidden while you type.
Enter FTP password:
Retype FTP server password:
Saving Upload Settings: OK
```

Select option **3**, Return to Troubleshooting Tools menu, when you are finished on the Show System Information menu.

Gather Logs

Option **3** allows you to collect all logs on the CSC SSM and send them out via FTP or TFTP, for example, to Cisco TAC. The logs are sent using the upload settings created using option **5**, Modify Upload Settings. See Modify Upload Settings, page A-13 for more information.

```
Troubleshooting Tools - Gather Logs
-------------------------------------------------------------------

Gather logs now? [y|n] y
Gathering logs ...
Creating temporary file CSCSSM-LOG-20060109-184525.tar.gz
Uploading temporary file CSCSSM-LOG-20060109-184525.tar.gz
```

```
Uploading file ...
Deleting temporary file CSCSSM-LOG-20060109-184525.tar.gz
```

Note Logs are automatically named using the following convention: CSCSSM-LOG-<date-time>.tar.gz. A similar convention for packets (described below) is used: CSCSSM-PACKET-<date-time>.gz.

Gather Packet Trace

Option **4** allows you to capture packets passing between the CSC SSM and ASA. This information is typically used by Cisco TAC.

The following prompts display:

```
Troubleshooting Tools - Gather Packet Trace
-------------------------------------------------------------------

Gather packet trace now? [y|n] y
Press Control-C to stop.
Gathering packet trace ...
Creating temporary file CSCSSM-PACKET-20060109-184529.gz
Upload the packet trace now? [y|n] y
Uploading temporary file CSCSSM-PACKET-20060109-184529.gz
Uploading file ...
```

To enable packet tracing:

Step 1 Select **y** when prompted to gather packet traces.

Step 2 Press Control-C to stop.

Step 3 Select **y** to when prompted to upload packet traces.

The packets are uploaded using the protocol defined using option **5**, Modify Upload Settings. See Modify Upload Settings, page A-13 for more information.

Modify Upload Settings

Option **5** allows you to set the uploading method to either FTP or TFTP, as used by features described previously in this chapter.

Note Your FTP or TFTP server must be set up to enable uploading.

When you select option **5**, the following prompts display:

```
Troubleshooting Tools - Upload Settings
-------------------------------------------------------------------

Choose a protocol [1=FTP 2=TFTP]: (default:1) 2
Enter TFTP server IP: (default:10.2.42.134)
Enter TFTP server port: (default:69)
Saving Upload Settings: OK
Press Enter to continue ...
```

Follow and respond to the prompts to configure the upload settings. The settings are saved for future use.

Select option **6**, Return to Main menu, when you are finished on the Troubleshooting Tools menu.

Reset Management Port Access Control

Choose option **8** to reset the management port access control list. The following appears:

```
Resetting management port access control list: OK
Press Enter to continue ...
```

If the ASDM is unable to communication with the SSM, try resetting port access via this option.

Ping IP

The ping option is available for diagnostic purposes. Choose option **9** to ping an IP address. The following appears:

```
Enter an IP address to ping:
```

After you enter the IP address, the system responds as follows:

```
PING 192.168.7.1 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue ...
```

Exit Options

Choose option **10**, Exit, to exit the setup options. The Exit Options menu appears:

```
Exit Options
------------------------------------------------------------------------

1. Logout
2. Reboot
3. Return to Main Menu

Enter a number from [1-3]: 1
Remote card closed command session. Press any key to continue.
Command session with slot 1 terminated.
hostname#
```

From the Exit Options menu, you can log out. Alternatively, you can reboot the system, or return to the Setup menu.

Configuration via Command Line

This section describes some command-line alternatives that are available for users who prefer command line over use of the CSC SSM console. Not all features have an alternative available.

Re-set Configuration

After you have installed Trend Micro InterScan for Cisco CSC SSM, if you have used TFTP to re-image the SSM, you may see this prompt for the first time when you access the CLI:

"Do you want to restore the previous configuration? [y/n]"

The question appears in the Setup Wizard menu, as shown below.

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
------------------------------------------------------------------------

Do you want to restore the previous configuration? [y|n] n
To set up the SSM, the wizard prompts for the following information:
1. Network settings
2. Date/time settings verification
3. Incoming email domain name
4. Web console administrator password
5. Notification settings
6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

If you choose **y**, the SSM configuration settings are restored to the state they were in the last time you saved configuration. This is a command-line alternative to the functionality on the **Administration > Configuration Backup** window in the CSC SSM console.

Using CSC SSM with Trend Micro Control Manager

This appendix describes how to begin managing Trend Micro InterScan for CSC SSM from Trend Micro Control Manager™ (TMCM). This Appendix assumes that you have already installed the TMCM agent and registered CSC SSM with TMCM using the SCS SSM the **Administration > Register to TMCM** screen.

About Control Manager

Trend Micro Control Manager™ (TMCM) is a central management console that allows you to manage multiple Trend Micro products and services from a central console. Control Manager allows you to monitor and report on activities such as infections, security violations, or virus entry points

In the Control Manager environment, CSC SSM is a managed product, and will appear as an icon in the Control Manager management console Product Directory . You can administer CSC SSM and other managed products, individually or by group, through the Product Directory.

With TMCM you can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Example update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals.

Control Manager benefits include:

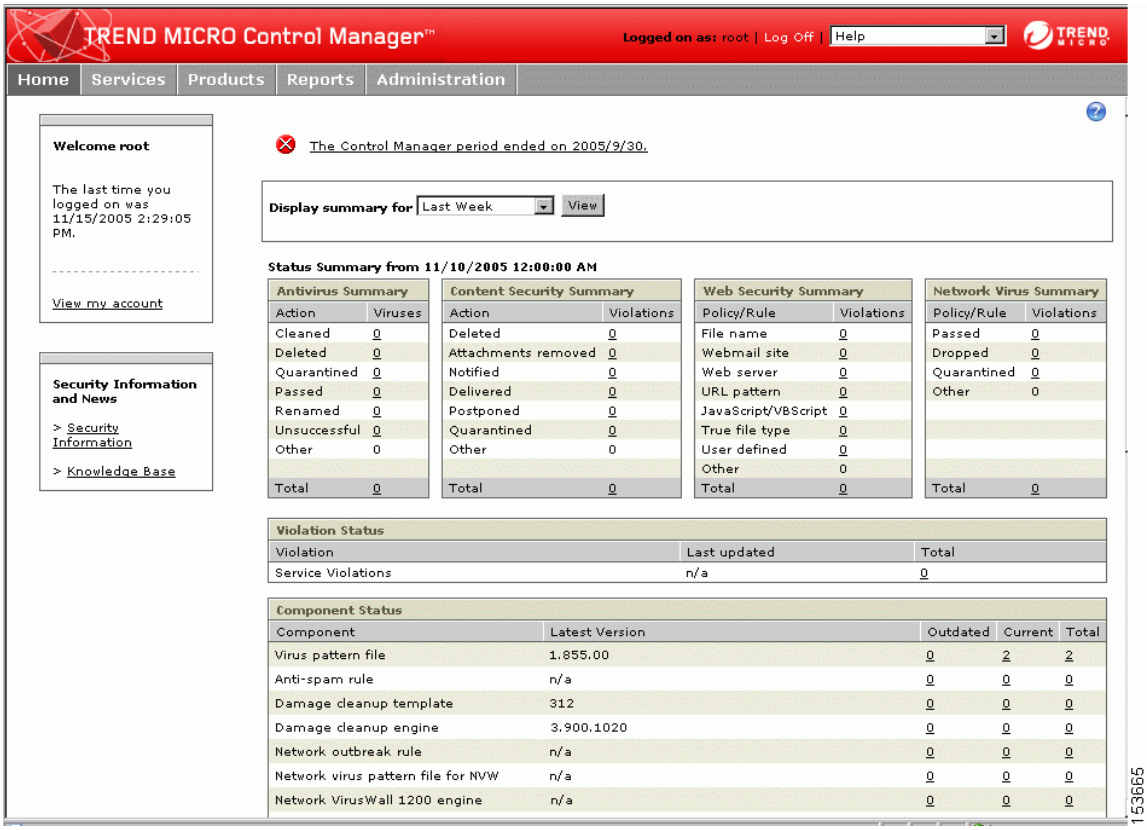
- Enterprise-Wide Coordination
- Proactive Outbreak Management
- Vulnerability Assessment (optional component)
- Outbreak Prevention Services (optional component)
- Damage Cleanup Services (optional component)
- Multi-tier Management Structure
- Flexible and Scalable Configuration of Installed Products

An explanation of the TMCM interface begins on the next page.

Control Manager Interface

Trend Micro Control Manager uses a management console for administration of managed products. When you first log in to TMCM, the default screen is the **Home** screen shown below:

Figure B-1 The Control Manager Management Console "Home" Screen.



Using the Management Console

The management console consists of the following elements:

- **Header menu:** Running across the top, the header menu provides links to the Control Manager online help, the Trend Micro Knowledge Base, Trend Micro Security Information, and the About screen for Control Manager.
- **Main menu:** Located below the header menu, the main menu provides links to the **Home, Services, Products, Reports, and Administration** menus to administer TMCM and managed products.
- **Navigation menu:** Located in the left-frame of the management console; when you select a Main Menu item, the Navigation Menu refreshes to display the available options for the menu selected.
- **Tab area:** Provides the Product Directory tabs, parent server, or child server tabs.

- **Working area:** This is where you can administer managed products or child server settings, invoke tasks, or view system status, logs, and reports. In addition to the **Navigation Menu** options, the **Working Area** also includes managed product or Child server Tabs when you select **Products** from the Main Menu.

Opening the Control Manager Console

There are two ways to access the Control Manager console, locally, from the Control Manager server, and remotely, via Web browser from any connected computer. The latter method is explain below.

To open the TMCM console from a remote computer:

Step 1 Type the following at your browser's address field to open the Log on page:

http://{hostname}/ControlManager

Where `{hostname}` is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.The TMCM log on screen appears.

Step 2 Type a TMCM **user name** and **password** in the field and click **Enter**.

Step 3 When the TMCM console opens, click **Products** in the top menu bar and locate the entry for CSC SSM.

Upon opening the console, the initial screen will show the status summary for your whole Control Manager system. This is identical to the status summary generated from the Product Directory. User rights determine the Control Manager functions you can access.

Access the HTTPS Management Console

If you want to encrypt the configuration data as it passes from the Web-based console to the Control Manager server, you must first assign HTTP to Control Manager Web access and then alter the management console URL to use the HTTPS protocol through port 443. For details on how to set up HTTPS access, refer to your TMCM documentation.

To open the TMCM console using HTTPS:

Step 1 Type the URL for encrypted communication (HTTPS) in the following format:

https://{hostname}:443/ControlManager

Where `{hostname}` is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name. The number `443` is the port allotted during an HTTPS session.

Note When you access a secure Control Manager site, it automatically sends you its certificate, and Internet Explorer displays a lock icon on the status bar.

About the Control Manager Product Directory

The Product Directory is a logical grouping of managed products in the TMCM console that allows you to perform the following for administering managed products:

- Configure products.
- View product information, as well as details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on).
- View product-level logs.
- Deploy virus pattern, scan engine, anti-spam rule, and program updates.

Newly registered managed products usually appear in the TMCM New entity folder, depending on the user account specified during the agent installation. Control Manager determines the default folder for the managed product by the privileges of the user account specified during the product agent installation.

You can use the TMCM Product Directory to administer CSC SSM after it has been registered with the Control Manager server.

Note Your ability to view and access the folders in the TMCM Product Directory depends on the Account Type and folder access rights assigned to your TMCM log on credentials. If you cannot see CSC SSM in the TMCM Product Directory, contact the TMCM administrator.

Download and Deploy New Components

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

- **Pattern files/Cleanup templates** - refer to virus pattern files, damage cleanup templates, Vulnerability Assessment patterns, network outbreak rules, and network virus pattern files.
- **Anti-spam rules** - refer to import and rule files used for anti-spam and content filtering.
- **Engines** - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux.
- **Product program** - these are product specific components (for example, Product Upgrades).

Note Only registered users are eligible for component updates. For more information, **Registering and Activating your Software > Understanding product activation** in the Control Manager online help.

Deploy New Components from the TMCM Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of CSC SSM on demand. This is useful especially during virus outbreaks. Download new components before deploying updates to specific or groups of managed products.

To manually deploy new components using the Product Directory:

Step 1 From the TMCM console, click **Products** on the main menu.

Step 2 On the leftmost menu, select **Managed Products** from the list and then click **Go**.

Step 3 On the left-hand menu, select the desired managed product or folder.

Step 4 On the working area, click the **Tasks** tab.

Step 5 Select **Deploy** *component_name* from the **Select task** list and then click **Next>>**.

Step 6 Click **Deploy Now** to start the manual deployment of new components.

Step 7 Monitor the progress via Command Tracking.

Step 8 Click the **Command Details** link to view details for the **Deploy Now** task.

View Managed Products Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

There are two ways to view the managed products status summary:

- From the Home page
- From the Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the **Status Summary** tab of the **Home** page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the **Product Status** tab in the **Product Directory Root** folder

To access through the Product Directory:

Step 1 From the TMCM console, click **Products** on the main menu.

Step 2 On the left-hand menu, select the desired folder or managed product.

- If you click a managed product, the **Product Status** tab displays the managed product's summary
- If you click the **Root** folder, **New entity**, or other user-defined folder, the **Product Status** tab displays Antivirus, Content Security, and Web Security summaries

Note By default, **Status Summary** displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the **Display Summary** list.

Configure CSC SSM Products

You can configure one or more instances of CSC SSM from TMCM, either individually or in groups, according to folder division. When performing a group configuration, verify that you want all managed product in a group to have the same configuration. Otherwise, add managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows either the product's Web console or a Control Manager-generated console

To configure a product:

Step 1 From the TMCM console, click **Products** on the main menu.

Step 2 On the leftmost menu, select **Managed Products** from the list and then click **Go**.

Step 3 On the left-hand menu, select the desired managed product or folder.

Step 4 On the working area, click the **Configuration** tab.

Step 5 Select the product to configure from the **Select product** list.

Step 6 At the **Select configuration** list, select the product feature to access or configure.

Step 7 Click *Next*. The managed product Web-based console or Control Manager-generated console appears.

Issuing Tasks to CSC SSM

Use the **Tasks** tab to invoke available actions to a group or specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable/Disable Real-time Scan
- Start Scan Now

You can deploy the latest spam rules, patterns, or scan engine to managed products with outdated components (the Control Manager server already be updated with the latest components from the Trend Micro ActiveUpdate server). Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to managed products:

Step 1 From the TMCM console, access the **Product Directory**.

Step 2 On the left-hand menu, select the desired managed product or folder.

Step 3 On the working area, click the **Tasks** tab.

Step 4 Select the task from the **Select task** list.

Step 5 Click **Next.**

Step 6 Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View Managed Product Logs

Use the Logs tab to query and view logs for a group or specific managed product.

To query and view managed product logs:

Step 1 From the TMCM console, access the **Product Directory**.

Step 2 On the left-hand menu, select the desired managed product or folder.

Step 3 On the working area, click the **Logs** tab.

Step 4 Select the client log type. The **Query Result** screen displays the results in a table format.

Step 5 The **Generated at** entity column of the result table indicates the Control Manager server time.

For additional information and instructions on using Trend Micro Control Manager, see that product's online help and PDF documentation.

A

access (noun) To read data from or write data to a storage device, such as a computer or server.

access (verb) Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.

action

(Also see target and notification) The operation to be performed when:
—a virus or other threat has been detected, or
—file blocking has been triggered.
Actions typically include clean, delete, or pass (deliver/transfer anyway). Delivering/transferring anyway is not recommended—delivering a risk-infected message can compromise your network.

activate To enable your Trend Micro InterScan for Cisco CSC SSM software during the installation process by entering the Activation Code (on the Activation Codes Configuration window). Until the product is installed and activated, the SSM is not operable.

Activation Code A 37-character code, including hyphens, that is used to activate Trend Micro InterScan for Cisco CSC SSM. Here is an example of an Activation Code: SM-9UE2-HD4B3-8577B-TB5P4-Q2XT5-48PY4

ActiveUpdate A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, spyware/grayware pattern file, PhishTrap pattern file, anti-spam rules, and anti-spam engine.

ActiveX A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.

ActiveX malicious code An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner.

Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to “high.”

address Refers to a networking address (see IP address) or an email address, which is the string of characters that specify the source or destination of an email message.

administrator Refers to “system administrator”—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.

administrator account A user name and password that has administrator-level privileges.

administrator email address The address used by the administrator of Trend Micro InterScan for Cisco CSC SSM to manage notifications and alerts.

adware Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”

anti-spam Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other “nuisance” mail.

anti-spam rules and engine The Trend Micro tools used to detect and filter spam.

antivirus Computer programs designed to detect and clean computer viruses.

approved sender A sender whose messages are always allowed into your network.

archive A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.

ASDM Adaptive Security Device Manager.

attachment A file attached to (sent with) an email message.

audio/video file A file containing sounds, such as music, or video footage.

authentication The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).

The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures.

Also see public-key encryption *and* digital signature.

B

binary A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.

block To prevent entry into your network.

blocked sender A sender whose messages are never allowed to enter your network.

boot sector virus A boot sector virus is a virus targeted at the boot sector (the operating system) of a computer. Computer systems are most likely to be attacked by boot sector viruses when you boot the system with an infected disk from the floppy drive—the boot attempt does not have to be successful for the virus to infect the hard drive.

Also, there are a few viruses that can infect the boot sector from executable programs. These are known as multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus attempts to infect every disk that is accessed by that computer. In general, boot sector viruses can be successfully removed.

browser A program which allows a person to read hypertext, such as Internet Explorer or Mozilla. The browser gives some means of viewing the contents of nodes (or “pages”) and of navigating from one node to another. A browser acts as a client to a remote Web server.

C

cache A small fast portion of memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.

case-matching Scanning for text that matches both words and case. For example, if “dog” is added to the content-filter, with case-matching enabled, messages containing “Dog” pass through the filter; messages containing “dog” do not.

cause The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.

clean To remove virus code from a file or message.

CLI Command Line Interface. See Reimaging and Configuring the CSC SSM Using the Command Line, page A-1 for more information.

client A computer system or process that requests a service of another computer system or process (a “server”) using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.

client-server environment A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to protocol, asking for information or action, and the server responds.

compressed file A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.

configuration Selecting options for how Trend Micro InterScan for Cisco CSC SSM functions, for example, selecting whether to pass or delete a virus-infected email message.

content filtering Scanning email messages for content (words or phrases) prohibited by your organization’s Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.

content violation An event that has triggered the content filtering policy.

CSC SSM console The Trend Micro InterScan for Cisco CSC SSM user interface.

D

daemon A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.

damage routine The destructive portion of virus code, also called the payload.

default A value that pre-populates a field in the CSC SSM console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.

dialer A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.

digital signature Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.

disclaimer A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** window.

DNS Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.

DNS resolution When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.

domain name The full name of a system, consisting of its local host name and its domain name, such as example.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution,” uses the Domain Name System (DNS).

DoS (Denial of Service) attack Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.

DOS virus Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs-files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.

download (noun) Data that has been downloaded, for example, from a Web site via HTTP.

download (verb) To transfer data or code from one computer to another. Downloading often refers to transfer from a larger “host” system (especially a server or mainframe) to a smaller “client” system.

dropper Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.

E

ELF Executable and Linkable Format—An executable file format for Unix and Linux platforms.

encryption Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

EULA (end user license agreement) An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” ends the installation of the software product.

Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.

executable file A binary file containing a program in machine language which is ready to be executed (run).

EXE file infector An executable program with an .exe file extension. *Also see* DOS virus.

exploit An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.

F

false positive An email message that was “caught” by the spam filter and identified as spam, but is actually not spam.

FAQ Frequently Asked Questions—A list of questions and answers about a specific topic.

file An element of data, such as an email message or HTTP download.

file infecting virus File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action.

In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file is unrecoverable.

file type The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

filename extension The portion of a file name (such as .txt or .xml) which typically indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.

filter criteria User-specified guidelines for determining whether a message and attachment(s), if any, are delivered, such as:
—size of the message body and attachment
—presence of words or text strings in the message subject
—presence of words or text strings in the message body
—presence of words or text strings in the attachment subject
—file type of the attachment

firewall A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.

FTP A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.

G

gateway An interface between an information source and a Web server.

grayware A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

group file type Types of files that have a common theme. There are five group file types in the Trend Micro InterScan for Cisco CSS SSM interface, they are:
—Audio/Video
—Compressed
—Executable
—Images
—Microsoft Office

GUI Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command-line interface where communication is by exchange of strings of text.

H

hacker *See* virus writer

hacking tool Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.

header Part of a data packet that contains transparent information about the file or the transmission.

heuristic rule-based scanning Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.

HTML virus A virus targeted at HTML (Hyper Text Markup Language), the authoring language used to create information in a Web page. The virus resides in a Web page and downloads via a user's browser.

HTTP Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

HTTPS HTTP over SSL—A variant of HTTP used for handling secure transactions.

host A computer connected to a network.

I

ICSA ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, crytography, and PC firewall products in the world today.

image file A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software.

incoming Email messages or other data routed *into* your network.

IntelliScan IntelliScan is a Trend Micro scanning technology that examines file headers using true file type recognition, and scans only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.

Internet A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.

in the wild Describes known viruses that are currently controlled by antivirus products. *Also see* "in the wild."

in the zoo Describes known viruses that are actively circulating. *Also see* "in the zoo."

interrupt An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.

intranet Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.

IP Internet Protocol—*See* IP address.

IP address Internet address for a device on a network, typically expressed using dot notation such as 10.123.123.123.

IT Information technology, to include hardware, software, networking, telecommunications, and user support.

J

Java applets Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality.

Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute—sometimes by simply changing browser security settings to "high."

Java file Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)

Java malicious code Virus code written or embedded in Java. *Also see* Java file.

JavaScript virus JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently.

A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser.

Also see VBscript virus.

K

KB Kilobyte—1024 bytes of memory.

keylogger Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.

L

license Authorization by law to use Trend Micro InterScan for Cisco CSC SSM.

link (also called hyperlink) A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.

listening port A port utilized for client connection requests for data exchange.

load balancing Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.

logic bomb Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.

M

macro A command used to automate certain functions within an application.

MacroTrap A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).

macro virus Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.

malware (malicious software) Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.

mass mailer (also known as a worm) A malicious program that has high damage potential, because it causes large amounts of network traffic.

match case *See* case-matching.

MB Megabyte—1024 kilobytes of data.

Mbps Millions of bits per second—a measure of bandwidth in data communications.

message An email message, which includes the message subject in the message header, and the message body.

message size The number of KB or MB occupied by a message and its attachments.

message subject The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”

Microsoft Office file Files created with Microsoft Office tools such as Excel or Microsoft Word.

mixed threat attack Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.

multi-partite virus A virus that has characteristics of both boot sector viruses and file-infecting viruses.

N

NAT device — Network Address Translation device—A device that allows organizations to use unregistered IP network numbers internally and still communicate well with the Internet. The purpose is typically to enable multiple hosts on a private network to access the Internet using a single public IP address; a feature called private addressing.

network virus — A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

notification

(Also see action and target) — A message that is forwarded to one or more of the following:
—system administrator
—sender of a message
—recipient of a message, file download, or file transfer
The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.

NRS (Network Reputation Service) — Network Reputation Services (NRS) is a method of spam filtering that allows you to off-load the task from the MTA to the SCS SSM. The IP address of the originating MTA is checked against a database of IP addresses.

NTP — Network Time Protocol—A time-keeping protocol for synchronizing clocks of computer systems over a data network.

O

offensive content — Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.

online help — Documentation that is bundled with the GUI

open relay — An open mail relay is an SMTP (e-mail) server configured to allow anyone on the Internet to relay or send e-mail through it. Spammers can use an open relay to send spam messages.

outgoing — Email messages or other data *leaving* your network, routed out to the Internet.

P

parameter — A variable, such as a range of values (a number from 1 to 10).

password cracker — An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.

pattern file (also known as Official Pattern Release) The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.

payload Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.

phishing Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

ping Pinging is a diagnostic tool used on TCP/IP networks that allows you to verify whether a connection from one host to another is working. See Ping IP, page A-14, for information about pinging from the command-line interface.

polymorphic virus A virus that is capable of taking different forms.

POP3 Post Office Protocol, version 3—A messaging protocol that allows a client computer to retrieve electronic mail from a server via a temporary connection, for example, a mobile computer without a permanent network connection.

POP3 server A server which hosts POP3 email, from which clients in your network retrieve POP3 messages.

port A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.

proxy A process providing a cache of items available on other servers which are presumably slower or more expensive to access.

proxy server A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

public-key encryption An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.

Q

queue A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.

R

recipient The person or entity to whom an email message is addressed.

remote access tool Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.

replicate To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

ROMMON ROM monitor program. ROMMON is executed from ROM and is a single-threaded program that initializes a board and loads a higher-level operating system. ROMMON is for debugging or to manually boot the system.

rule-based spam detection Spam detection based on heuristic evaluation of message characteristics for determining whether an email message should be considered spam. When the anti-spam engine examines an email message, it searches for matches between the mail contents and the entries in the rules files. Rule-based spam detection has a higher catch rate than signature-based spam detection, but it also has a higher false positive rate as well.
Also see signature-based spam detection.
Also see false positive.

S

scan To examine items in a file in sequence to find those that meet a particular criteria.

scan engine The module that performs antivirus scanning and detection in the host product to which it is integrated.

script A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.”

seat A license for one person to use Trend Micro InterScan for Cisco CSC SSM.

Secure Password Authentication An authentication process, by which communications can be protected, using for example, encryption and challenge/response mechanisms.

security Security refers to techniques for ensuring that data stored in or transferred via a computer cannot be accessed by unauthorized individuals. Methods for achieving system security are typically data encryption and passwords.

sender The person who is sending an email message to another person or entity.

server A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.

setup wizard The setup program used to install Trend Micro InterScan for Cisco CSC SSM. You can install using:
—A GUI setup wizard, launched from the ASDM (see the ASDM online help for details), or
—A command-line interface (see Reimaging and Configuring the CSC SSM Using the Command Line, page A-1, for more information)

signature-based spam detection — A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect "new" spam that isn't an exact match for text in the spam signature file.
Also see rule-based spam detection.
Also see false positive.

SMTP — Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.

SOCKS4 — A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.

spam — Unsolicited email messages meant to promote a product or service.

SSL — Secure Sockets Layer—A secure communications protocol on the Internet.

spyware — Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

stamp — To place an identifier, such as "Spam," in the subject field of an email message.

status bar — A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.

T

TAC — Technical Assistance Center

target (Also see action and notification) — The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.

TCP/IP — Transmission Control Protocol/Internet Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.

TELNET — The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

TFTP — Trivial File Transfer Protocol is a simple file transfer protocol used to read files from or write files to a remote server.

top-level domain (tld) — The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).

traffic — Data flowing between the Internet and your network, both incoming and outgoing.

trigger An event that causes an action to take place. For example, Trend Micro InterScan for Cisco CSC SSM detects a virus in an email message. This *triggers* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.

Trojan horse A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.

true file type Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

trusted domain A domain from which Trend Micro InterScan for Cisco CSC SSM always accepts messages, without considering whether the message is spam. For example, a company called Example, Inc. has a subsidiary called Example-Japan, Inc. Messages from example-japan.com are always accepted into the example.com network, without checking for spam, since the messages are from a known and trusted source.

trusted host A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.

U

UDP A protocol in the TCP/IP protocol suite, the User Datagram Protocol or UDP allows an application program to send datagrams to other application programs on a remote machine. Basically UDP is a protocol that provides an unreliable and connectionless datagram service where delivery and duplicate detection are not guaranteed. It does not use acknowledgments, or control the order of arrival.

URL Uniform Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.cisco.com*. The URL maps to an IP address using DNS.

V

VBscript virus VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page.

A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser.

Also see JavaScript virus.

virus A computer virus is a program – a piece of executable code – that has the unique ability to infect and replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

virus kit A template of source code for building and executing a virus, available from the Internet.

virus signature A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.

virus trap Software that helps you capture a sample of virus code for analysis.

virus writer Another name for a malicious computer hacker, someone who writes virus code.

W

Web The World Wide Web, also called the Web or the Internet.

Web server A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.

wildcard In Trend Micro InterScan for Cisco CSC SSM, the term is used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.

workstation (also known as client) A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.

worm A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.

Z

zip file A compressed archive (in other words, “zip file”) from one or more files using an archiving program such as WinZip.

Zip of Death A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W