CHAPTER 1

Introducing the CSC SSM

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

Overview

solution for your network. This guide describes how to manage the CSC SSM, which resides in your adaptive security 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 The CSC SSM does not scan traffic using other protocols, such as HTTPS.

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

These features are available to all customers with the Base License for the CSC SSM software. If you have 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 SMTP and POP3 traffic.
- Set up content filters to allow or prohibit e-mail 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.

-

"Licensing" section on page 1-11.

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

With Trend Micro InterScan for Cisco CSC SSM, you do not need to install separate applications for virus protection, spyware blocking, spam detection, or content filtering—all of these functions are available in a single, easy-to-maintain 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 do not accidentally introduce viruses from their personal e-mail accounts.

For information about installing the appliance, see your Cisco documentation.

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. For a description of fields in 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	Benefits
Scans for traffic containing viruses, and manages infected messages and files.	Together with powerful Cisco firewall protection, Trend Micro InterScan for Cisco CSC SSM secures your network from threats, spam, and unwanted content.
Scans for spam at low to high threshold levels, and allows you to determine how spam is handled.	Easy to install, with a Setup Wizard.

Table 1-1 Features and Benefits (continued)

Filters offensive or inappropriate content.	Antivirus, spyware and grayware detection, file blocking, and other protections against security risks in your network traffic are integrated with ASDM.
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.	
Allows you to fine-tune configuration of scanning, anti-spam, and filtering features after installation.	
Can be configured to update the virus pattern file, scan engine, and spam-detection components automatically when a new version becomes available from Trend Micro.	
Provides e-mail and system log message 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*

Cisco Content Security and Control SSM Administrator Guide

–

– General help, which explains tasks that require action in several windows, or additional knowledge needed to complete tasks.

- Knowledge Base—An online database of problem-solving and troubleshooting information. Knowledge Base provides the most current information about known product issues. To access the Knowledge Base, go to the following URL:

  http://kb.trendmicro.com/solutions/solutionSearch.asp

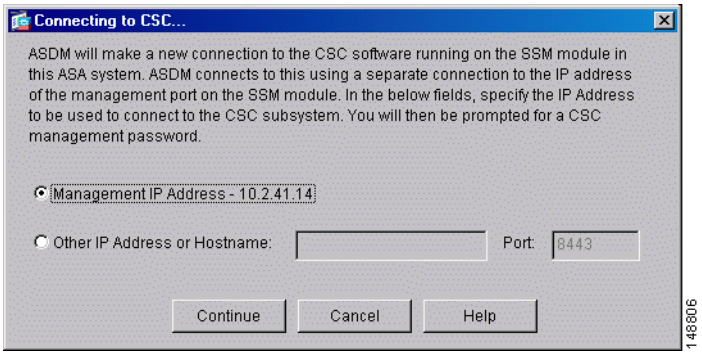
Terminology

Introducing the Content Security Tab

Content Security

You are prompted to connect to the CSC SSM. The Connecting to CSC dialog box appears (shown in Figure 1-1), in which you choose the IP address that ASDM recognizes, or an alternate. You can use an alternate if you access ASDM through a NAT device, in which 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.

Figure 1-1 Connecting to the CSC

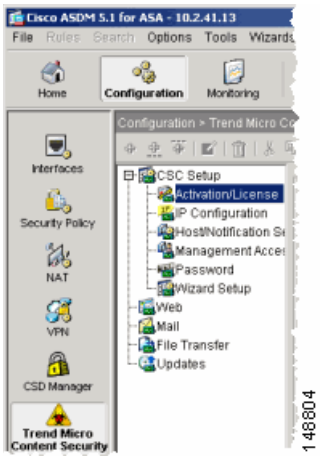


OK

page 7-1.

To open the CSC SSM, choose **Configuration > Trend Micro Content Security.**

Figure 1-2 Configuration Options on ASDM



Managing Updates and Log Queries.”

Introducing the CSC SSM Console

-
-
- Default Values, page 1-8

  Tooltips, page 1-9

  Online Help, page 1-9

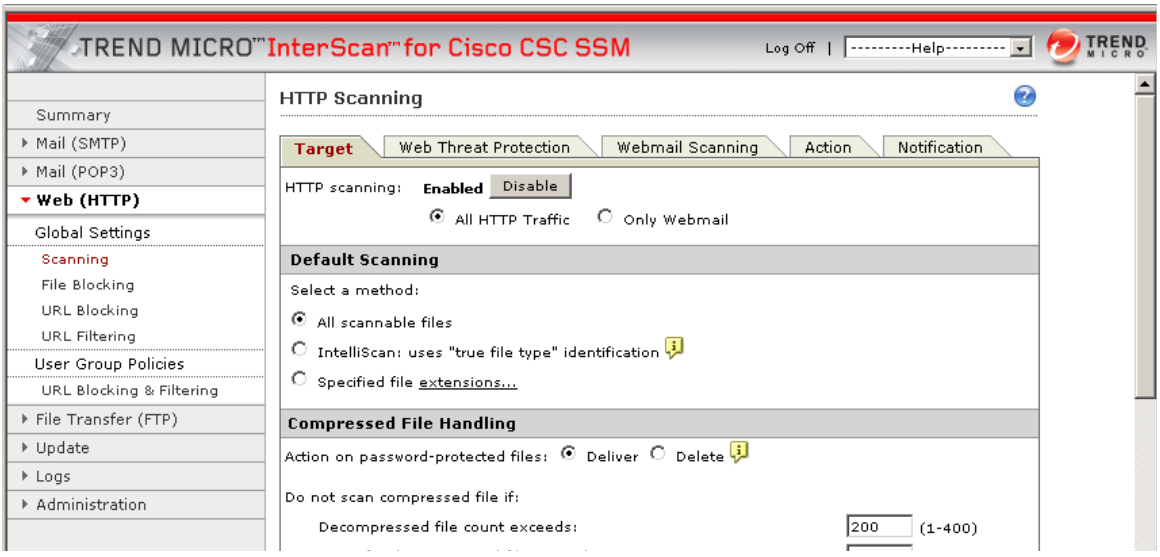
After you have successfully installed Trend Micro InterScan for Cisco CSC SSM and have configured the adaptive security appliance to send traffic to CSC SSM, the virus scanning and detection feature is activated and your network traffic is scanned according to the default settings. Additional features, such as spyware or grayware detection, are not enabled by default and you must configure them in the CSC SSM.

The CSC SSM displays in a browser window, as shown in Figure 1-3. On the left side of the Configuration window in ASDM are links to perform the tasks of interest. The default view in the Trend Micro InterScan for Cisco CSC SSM is context-sensitive, depending on the link selected. For example, click the **Configure Web Scanning**

Connecting to CSC <link name> window. If you exit the CSC SSM and then return without logging out of ASDM, only the security certificate appears.

To exit the application, click **Log Off**, and then close the browser window.

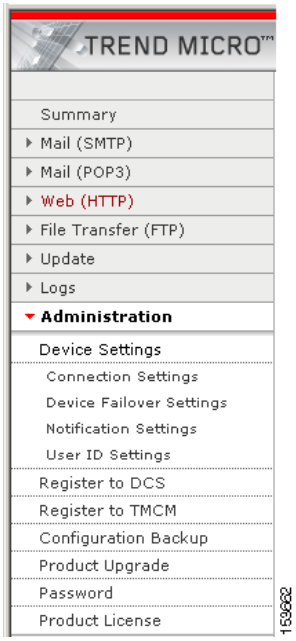
Figure 1-3 HTTP Scanning Window



Navigation Pane

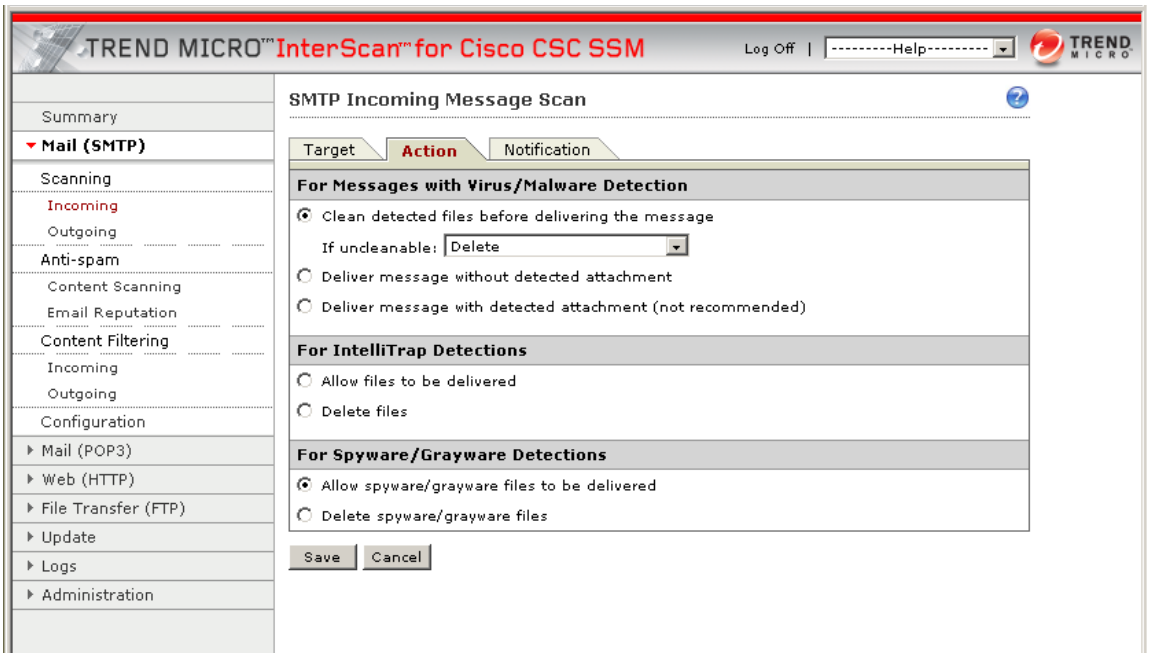
A selection is compressed when the arrow is pointing to the right; a selection is expanded when the arrow is pointing down. The corresponding panes do not refresh until you choose a selection on the main menu.

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



Tab Behavior

Figure 1-5 Tabs Working Together



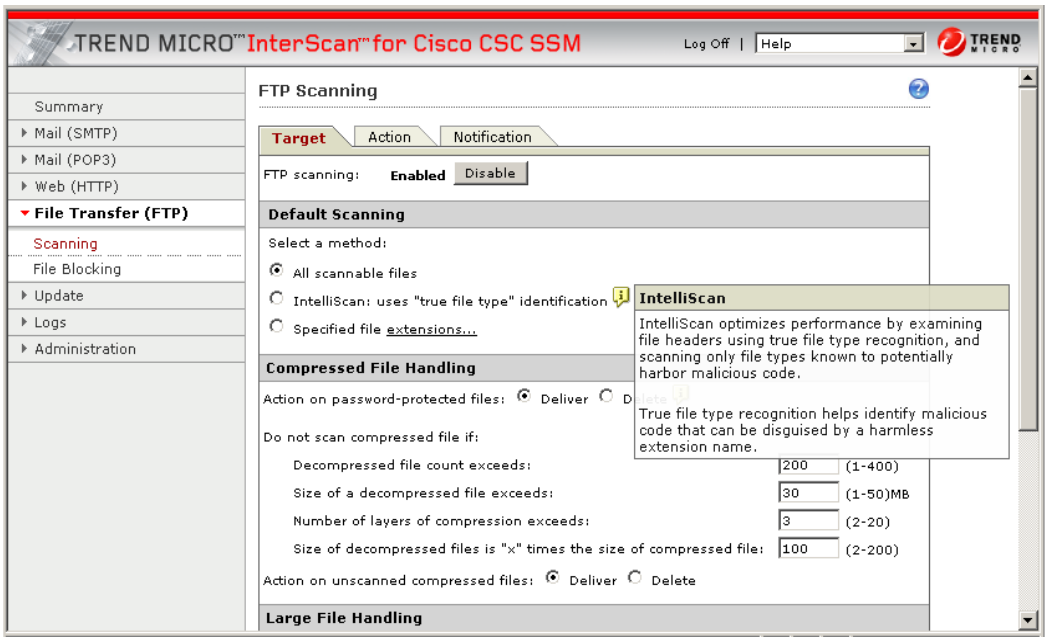
Save

Save Button

Default Values

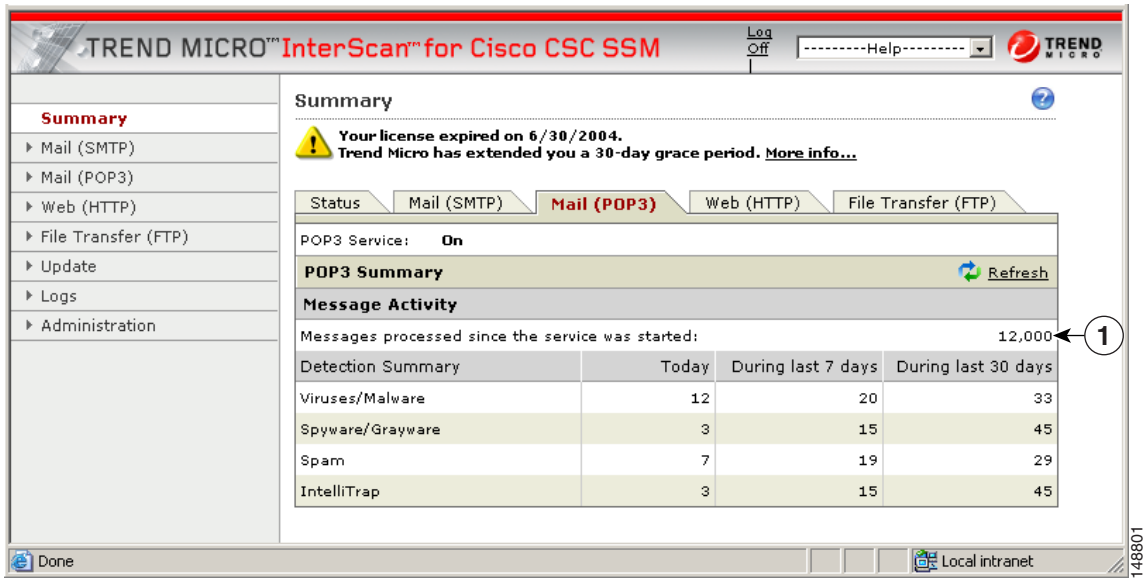
Tooltips

Figure 1-6 Tooltip Example



Online Help

Figure 1-7 General and Context-Sensitive Online Help



Contents **Index**

plus

Figure 1-8 Online Help Contents

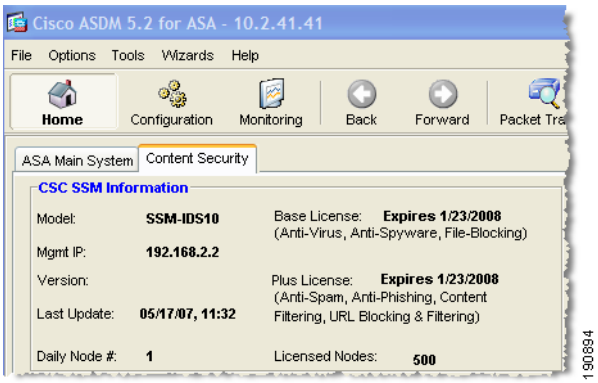
Index

Search

Links in Online Help

Licensing

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



Administration > Product License

Windows That Require Plus Licensing

Window Title	Base License	Plus License

Window Title	Base License	Plus License

Process Flow

Figure 1-10 Process Flow