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

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
Benefits
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

Features and Benefits (continued)

Available Documentation

Cisco ASA 5500 Series Adaptive Security Appliance

Getting Started Guide *Quick Start Guide*

Cisco Content Security and Control SSM Administrator Guide

–

– 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

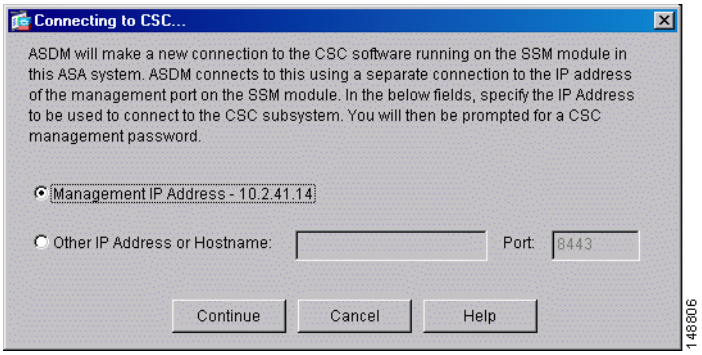
Important Terms

Introducing the ASDM Content Security Tab

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



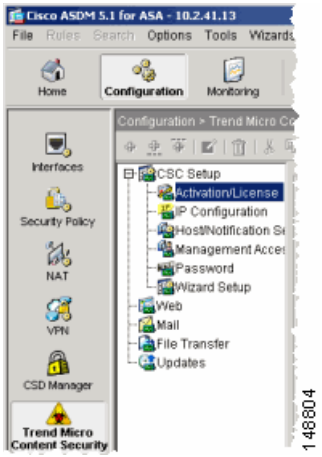
Continue

OK

, page 7-1 for more information.

From the ASDM console, click **Configuration > Trend Micro Content Security**

Figure 1-2 Configuration Options on ASDM



Managing Updates and Log Queries”

Introducing the CSC SSM Console

Configuration > Trend Micro Content Security.

Web **Configuration > Trend Micro Content Security**

HTTP Scanning

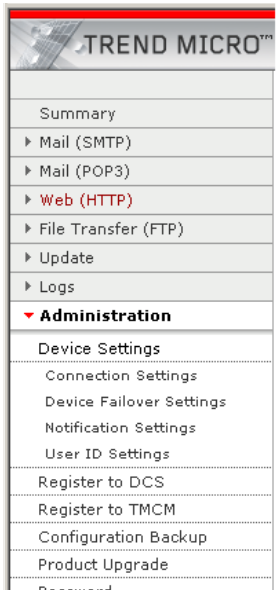
Connecting to CSC <link name>

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

Log Off

Navigation Panel

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



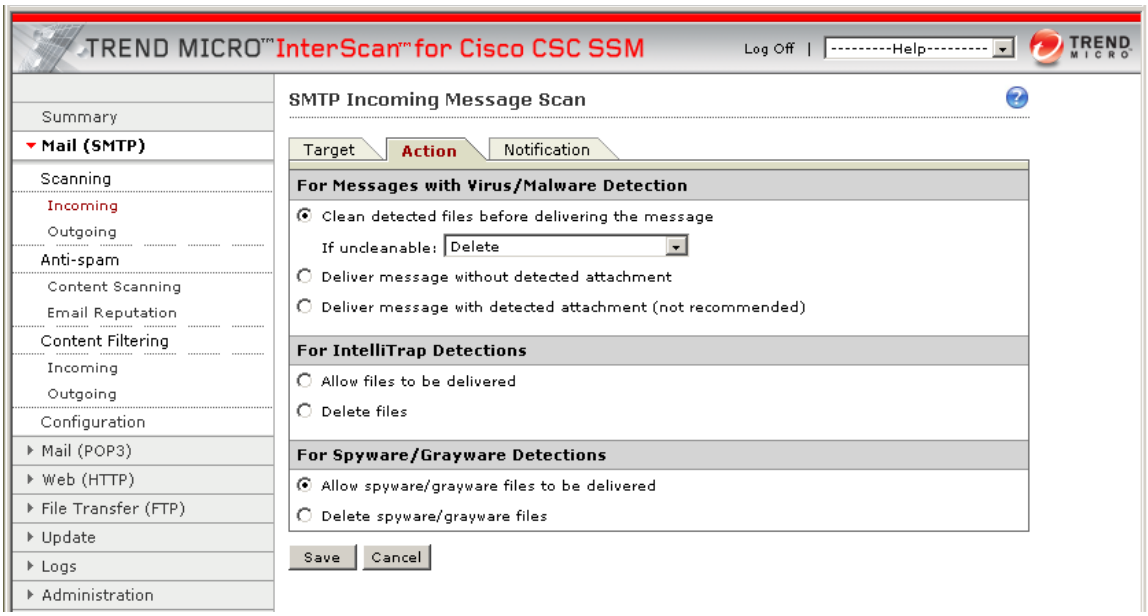
Mail (SMTP) > Scanning > Incoming > Action

Tab Behavior

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



Notification

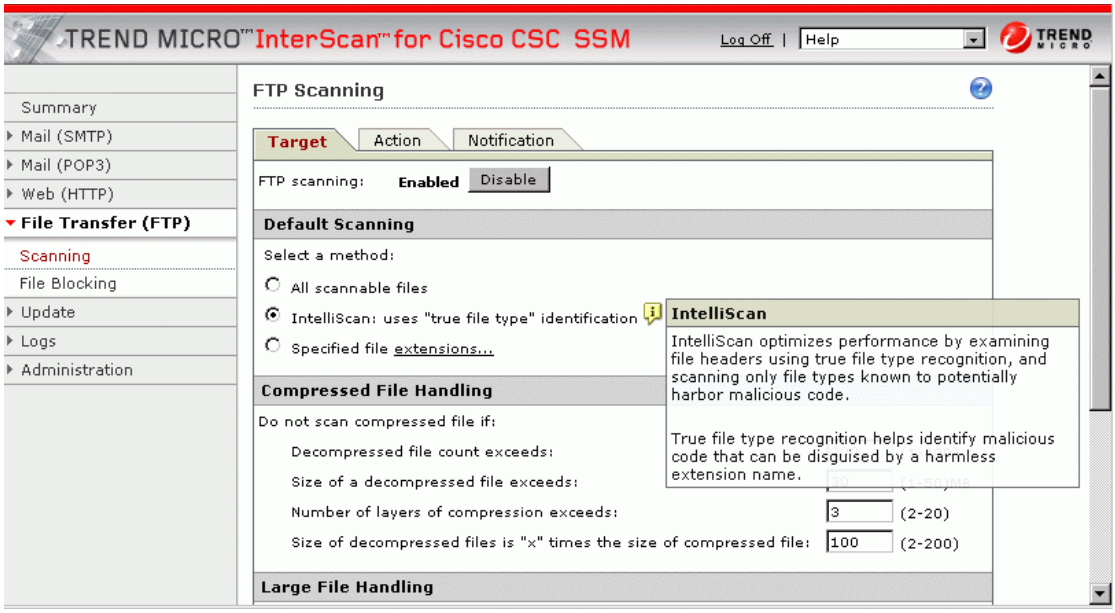
Save

Save Button

Default Values

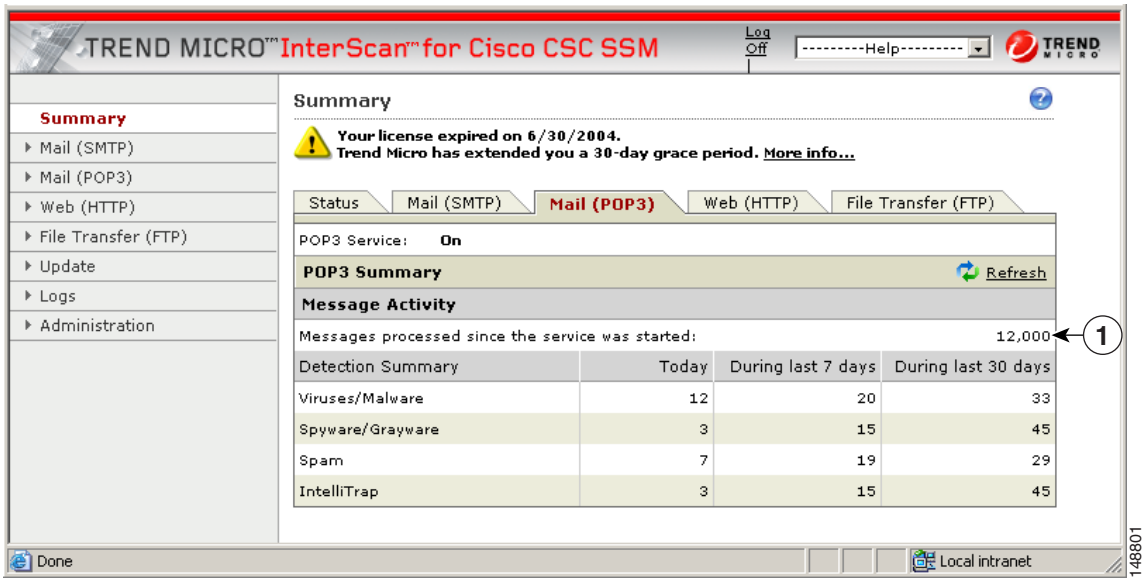
Tooltip Icons

Figure 1-6 Information Icon (Tooltip)



Online Help

Figure 1-7 General and Context-sensitive Online Help



1		2	

Figure 1-8 Online Help Contents

Index **Search**

Licensing

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

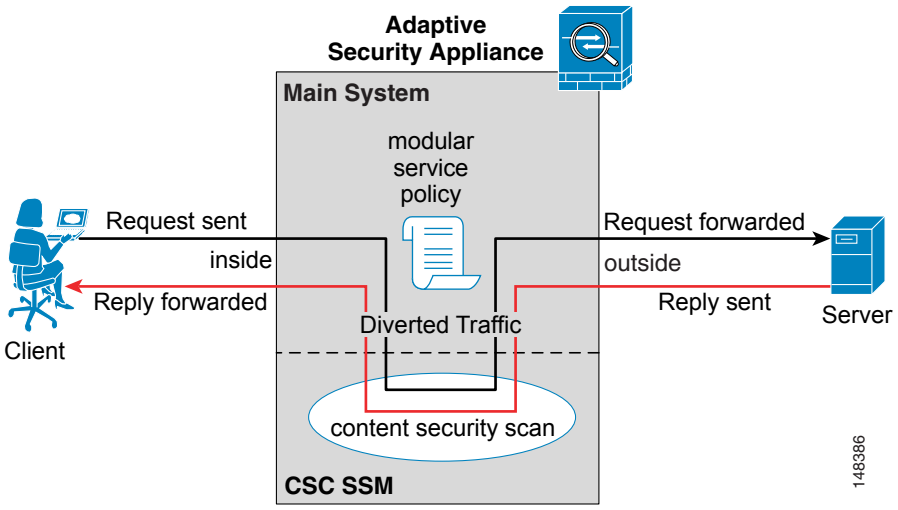
Administration > Product License
Status

Windows That Require Plus Licensing

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	
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 Process Flow



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