Cisco Content Security and Control SSM Administrator Guide

Version 6.1.1587.0

Americas 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: 408 527-0883

Text Part Number: OL-13089-01

Cisco Content Security and Control SSM Administrator Guide

CONTENTS

About This Guide ix

Document Objectives ix

Audience ix

Document Organization x

Document Conventions x

Related Documentation xi

Obtaining Documentation, Obtaining Support, and Security Guidelines xi

CHAPTER 1 **Introducing the CSC SSM** 1-1

Overview 1-1

Features and Benefits 1-2

Available Documentation 1-3

Terminology 1-4

Introducing the Content Security Tab 1-4

Configuring Content Security 1-4

Introducing the CSC SSM Console 1-6

Navigation Pane 1-7

Tab Behavior 1-7

Save Button 1-8

Default Values 1-8

Tooltips 1-9

Online Help 1-9

Links in Online Help 1-11

Licensing 1-11

Windows That Require Plus Licensing 1-11

Process Flow 1-12

CHAPTER 2 **Verifying Initial Setup** 2-1

Verifying ASA Clock Setup 2-1

Verifying CSC SSM Activation 2-1

Verifying Scanning 2-2

Testing the Antivirus Feature 2-3

Verifying Component Status 2-4

Viewing the Status LED 2-5
Understanding SSM Management Port Traffic 2-6

CHAPTER 3 **Configuring SMTP and POP3 Mail Traffic 3-1**
Default Mail Scanning Settings 3-1
Defining Incoming and Outgoing SMTP Mail 3-2
Enabling SMTP and POP3 Spyware and Grayware Detection 3-3
Reviewing SMTP and POP3 Notifications 3-3
Types of Notifications 3-4
Modifying Notifications 3-4
Configuring SMTP Settings 3-5
Enabling SMTP and POP3 Spam Filtering 3-6
Enabling SMTP and POP3 Content Filtering 3-7
Enabling Network Reputation Services 3-8
About RBL+ and QIL 3-9

CHAPTER 4 **Configuring Web (HTTP) and File Transfer (FTP) Traffic 4-1**
Default Web and FTP Scanning Settings 4-1
Downloading Large Files 4-2
Deferred Scanning 4-3
Detecting Spyware and Grayware 4-3
Scanning Webmail 4-4
File Blocking 4-4
URL Blocking 4-5
Blocking from the Via Local List Tab 4-6
Blocking from the Via Pattern File (PhishTrap) Tab 4-7
URL Filtering 4-8
Filtering Settings 4-8
Filtering Rules 4-9

CHAPTER 5 **Managing Updates and Log Queries 5-1**
Updating Components 5-1
Manual Update 5-2
Scheduled Update 5-2
Configuring Proxy Settings 5-3
Configuring System Log Message Settings 5-3
Viewing Log Data 5-4

Logging of Scanning Parameter Exceptions 5-5

CHAPTER 6 **Administering Trend Micro InterScan for Cisco CSC SSM 6-1**

Configuring Connection Settings 6-1
Managing Administrator E-mail and Notification Settings 6-2
Backing Up Configuration Settings 6-3
Exporting a Configuration 6-4
Importing a Configuration 6-4
Configuring Failover Settings 6-5
Installing Product Upgrades 6-6
Viewing the Product License 6-7
License Expiration 6-8
Licensing Information Links 6-9
Activating the Product 6-9
Renewing a License 6-9

CHAPTER 7 **Monitoring Content Security 7-1**

Features of the Content Security Tab 7-1
Monitoring Content Security 7-3
Monitoring Threats 7-3
Monitoring Live Security Events 7-5
Monitoring Software Updates 7-6
Monitoring Resources 7-7

CHAPTER 8 **Troubleshooting Trend Micro InterScan for Cisco CSC SSM 8-1**

Troubleshooting Installation 8-1
What To Do If Installation Fails 8-3
Troubleshooting Activation 8-4
Troubleshooting Basic Functions 8-4
Cannot Log On 8-4
Recovering a Lost Password 8-4
Summary Status and Log Entries Out of Synch 8-5
Delays in HTTP Connections 8-6
Access to Some Websites Is Slow or Inaccessible 8-6
Performing a Packet Capture 8-6
FTP Download Does Not Work 8-7

Reimaging or Recovery of CSC Module 8-7
Troubleshooting Scanning Functions 8-7
Cannot Update the Pattern File 8-8
Spam Not Being Detected 8-8
Cannot Create a Spam Stamp Identifier 8-8
Unacceptable Number of Spam False Positives 8-9
Cannot Accept Any Spam False Positives 8-9
Unacceptable Amount of Spam 8-9
Virus Is Detected but Cannot Be Cleaned 8-9
Virus Scanning Not Working 8-9
Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration 8-10
Scanning Not Working Because the CSC SSM Is in a Failed State 8-10
Downloading Large Files 8-11
Restart Scanning Service 8-12
Troubleshooting Performance 8-13
CSC SSM Console Timed Out 8-13
Status LED Flashing for Over a Minute 8-13
SSM Cannot Communicate with ASDM 8-13
Logging in Without Going Through ASDM 8-13
CSC SSM Throughput is Significantly Less Than ASA 8-14
Using Knowledge Base 8-15
Using the Security Information Center 8-15
Understanding the CSC SSM System Log Messages 8-16
SSM Application Mismatch [1-105048] 8-18
Data Channel Communication Failure [3-323006] 8-18
Traffic Dropped Because of CSC Card Failure [3-421001] 8-18
Drop ASDP Packet with Invalid Encapsulation [3-421003] 8-19
Daily Node Count [5-421006] 8-19
Data Channel Communication OK [5-505010] 8-19
New Application Detected [5-505011] 8-19
Application Stopped [5-505012] 8-20
Application Version Changes [5-505013] 8-20
Skip Non-applicable Traffic [6-421002] 8-21
Account Host Toward License Limit [6-421005] 8-21
Traffic Dropped Because of CSC Card Failure [6-421007] 8-21
Failed to Inject Packet [7-421004] 8-22
Connection capacity has been reached 8-22
Connection capacity has been restored 8-22
CSC has actively disconnected a connection 8-23

CSC SSM status message 8-23
Failover service communication failed 8-24
Failover service email could not be sent 8-24
Failover service encountered an internal error 8-24
HTTP URL blocking event 8-25
HTTP URL filtering event 8-26
License upgrade notice 8-26
Resource availability of the CSC SSM falls below the desired level 8-26
Resource availability of the CSC SSM has been restored 8-27
Scan service failed 8-27
Scan service recovered 8-28
Scheduled update report 8-28
Service module cannot create FIFO 8-28
Service module encountered a problem when communicating with the ASA chassis 8-29
Service module informational report 8-29
Service module internal communication error 8-30
Service module show module 1 details 8-30
SMTP/POP3 anti-spam event 8-31
Spyware/Grayware detection event 8-31
Syslog adaptor starting 8-32
System monitor started 8-32
Time synchronization with the ASA chassis failed 8-32
Virus detection event 8-32
Before Contacting Cisco TAC 8-33

APPENDIX A **Reimaging and Configuring the CSC SSM Using the CLI** A-1
Installation Checklist A-1
Preparing to Reimage the Cisco CSC SSM A-2
Reimaging the CSC SSM A-4
Confirming the Installation A-7
Viewing or Modifying Network Settings A-8
Viewing Date and Time Settings A-9
Viewing Product Information A-9
Viewing or Modifying Service Status A-9
Using Password Management A-10
Changing the Current Password A-10
Modifying the Password-reset Policy A-11
Restoring Factory Default Settings A-12
Troubleshooting Tools A-12

Enabling Root Account A-13
Showing System Information A-13
Collecting Logs A-15
Enabling Packet Tracing A-15
Modifying Upload Settings A-16
Resetting the Management Port Access Control A-16
Pinging an IP Address A-17
Exiting the Setup Wizard A-17
Resetting the Configuration via the CLI A-17

APPENDIX B **Using CSC SSM with Trend Micro Control Manager** B-1
About Control Manager B-1
Control Manager Interface B-2
Using the Management Console B-2
Opening the Control Manager Console B-3
Accessing the HTTPS Management Console B-3
About the Product Directory B-4
Downloading and Deploying New Components B-4
Deploying New Components from the TMCM Product Directory B-5
Viewing Managed Products Status Summaries B-5
Configuring CSC SSM Products B-6
Issuing Tasks to the CSC SSM B-6
Querying and Viewing Managed Product Logs B-7

GLOSSARY

INDEX

About This Guide

This preface introduces the *Cisco Content and Security SSM Administrator Guide*, and includes the following sections:

- Document Objectives, page ix
- Audience, page ix
- Document Organization, page x
- Document Conventions, page x
- Related Documentation, page xi
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xi

Document Objectives

This guide describes how to configure Trend Micro InterScan for Cisco, where the CSC SSM is in a Cisco ASA 5500 series adaptive security appliance (ASA 5510, ASA 5520, and ASA 5540). You access the GUI for Trend Micro InterScan for Cisco CSC SSM by using ASDM, a web-based adaptive security appliance device manager. ASDM includes a Setup Wizard for initial configuration of CSC SSM and online help to assist in fine-tuning a Cisco ASA 5500 series adaptive security appliance. For more information, see http://www.cisco.com/en/US/products/ps6121/tsd_products_support_series_home.html.

Audience

This guide is for network managers who perform any of the following tasks:

- Manage content security policies
- Install and configure security appliances and network security applications
- Troubleshoot issues with content security enforcement

Document Organization

This guide includes the chapters and appendixes described in Table 1.

Table 1 Document Organization

Chapter or Appendix	Description
Chapter 1, "Introducing the CSC SSM"	Provides an overview of Trend Micro InterScan for Cisco CSC SSM.
Chapter 2, "Verifying Initial Setup"	Describes how to verify that Trend Micro InterScan for Cisco CSC SSM is operating correctly,
Chapter 3, "Configuring SMTP and POP3 Mail Traffic"	Describes how to configure Trend Micro InterScan for Cisco CSC SSM to scan SMTP and POP3 mail traffic.
Chapter 4, "Configuring Web (HTTP) and File Transfer (FTP) Traffic"	Describes how to configure Trend Micro InterScan for Cisco CSC SSM to scan HTTP and FTP traffic.
Chapter 5, "Managing Updates and Log Queries"	Describes how to manage updates and log queries.
Chapter 6, "Administering Trend Micro InterScan for Cisco CSC SSM"	Describes administration tasks for Trend Micro InterScan for Cisco CSC SSM.
Chapter 7, "Monitoring Content Security"	Describes the monitoring features available with CSC SSM.
Chapter 8, "Troubleshooting Trend Micro InterScan for Cisco CSC SSM"	Describes how to troubleshoot issues with Trend Micro InterScan for Cisco CSC SSM.
Appendix A, "Reimaging and Configuring the CSC SSM Using the CLI"	Describes how to install and perform initial configuration of Trend Micro InterScan for Cisco CSC SSM from the SSM CLI.
Appendix B, "Using CSC SSM with Trend Micro Control Manager"	Describes how to manage Trend Micro InterScan for CSC SSM from Trend Micro Control Manager (TMCM).

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **boldface screen** font.
- Filenames, directory names, and variables for which you must supply a value are shown in *italic screen* font.

- Examples might include output from different platforms. For example, you might not recognize an interface type in an example because it is not available on your platform. Differences should be minor.
- Selecting a menu item (or screen) is indicated with the following convention:

  Click **screen1 > screen2 > screen3**.
- The caret symbol (**^**) represents the key labeled **Ctrl** (control). To enter a control key (for example, **^z**), hold down the **Ctrl** key while you press the **z** key.

Note This symbol means *reader take note*. Notes contain helpful suggestions or references to material not addressed in the guide.

Related Documentation

Use this document with the adaptive security appliance documentation set, which is available online at the following website:

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section.

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, page 1-1
- Features and Benefits, page 1-2
- Available Documentation, page 1-3
- Introducing the Content Security Tab, page 1-4
- Configuring Content Security, page 1-4
- Introducing the CSC SSM Console, page 1-6
- Licensing, page 1-11
- Process Flow, page 1-12

Overview

Trend Micro InterScan for Cisco CSC SSM provides an all-in-one antivirus and spyware management 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.

- Filter URL traffic according to predefined categories that you allow or disallow, such as adult or mature content, games, chat or instant messaging, or gambling sites.

For more information about the Base License and Plus License, see the "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)

Features	Benefits
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*. This 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 types of online help are available:
  - Context-sensitive window help, which explains how to perform tasks in one window.
  - 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

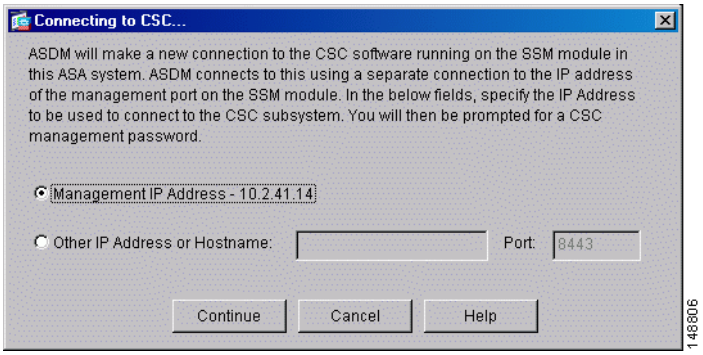
Certain terms are used throughout the documentation and online help that may not be familiar to you, or may be used in an alternate way from what you might expect. A definition of terms is available in the Glossary.

Introducing the Content Security Tab

When you open ASDM, the ASA Main System tab is the default view. Click the **Content Security** tab to view a summary of CSC SSM activities.

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



Click **Continue** after choosing the local host or the alternate.

Enter your CSC SSM password, which you configured during installation, and click **OK**.

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

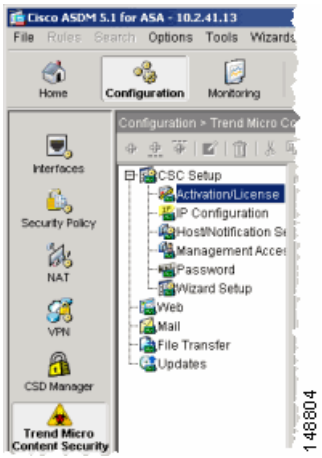
Configuring Content Security

To open the CSC SSM, choose **Configuration > Trend Micro Content Security.** From the Configuration menu (shown in Figure 1-2), select from the following configuration options:

- CSC Setup—Launches the Setup Wizard to install and configure the CSC SSM.
- Web—Configures Web scanning, file blocking, URL filtering, and URL blocking.

- Mail—Configures scanning, content filtering, and spam prevention for incoming and outgoing SMTP and POP3 e-mail.
- File Transfer—Configures file scanning and blocking.
- Updates—Schedules updates for content security scanning components (virus pattern file, scan engine, and others).

Figure 1-2 Configuration Options on ASDM



The Setup options are described in the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*. The online help provides more detailed information about each of these options.

The Web, Mail, File Transfer, and Updates options are described in more detail in these chapters:

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

Introducing the CSC SSM Console

This section describes the CSC SSM console, and includes the following topics:

- Navigation Pane, page 1-7
- Tab Behavior, page 1-7
- Default Values, page 1-8
- Tooltips, page 1-9
- Online Help, page 1-9

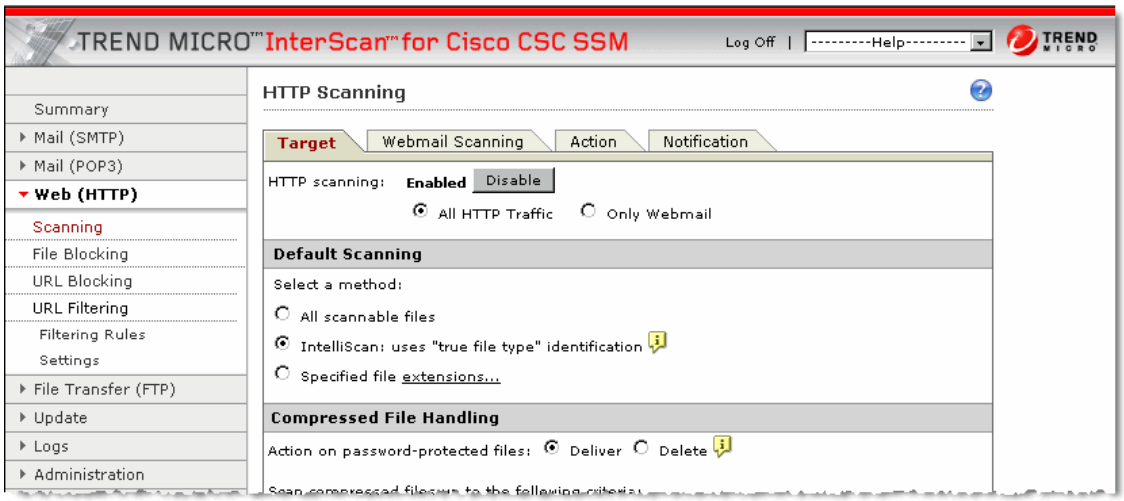
After you have successfully installed Trend Micro InterScan for Cisco CSC SSM and have configured the adaptive security appliance to send traffic to CSC SSM, the virus scanning and detection feature is activated and your network traffic is scanned according to the default settings. Additional features, 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** link to go to the HTTP Scanning window, where you can configure Web scanning settings.

The first time you log in to the CSC SSM, ASDM displays a security certificate, followed by the 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.

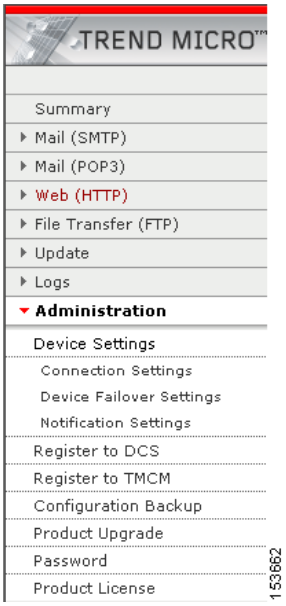
Figure 1-3 HTTP Scanning Window



Navigation Pane

The left pane of the Trend Micro CSC SSM console is the main menu, which also serves as a navigation pane (shown in Figure 1-4). Click a menu item in the navigation pane to open the corresponding window. 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

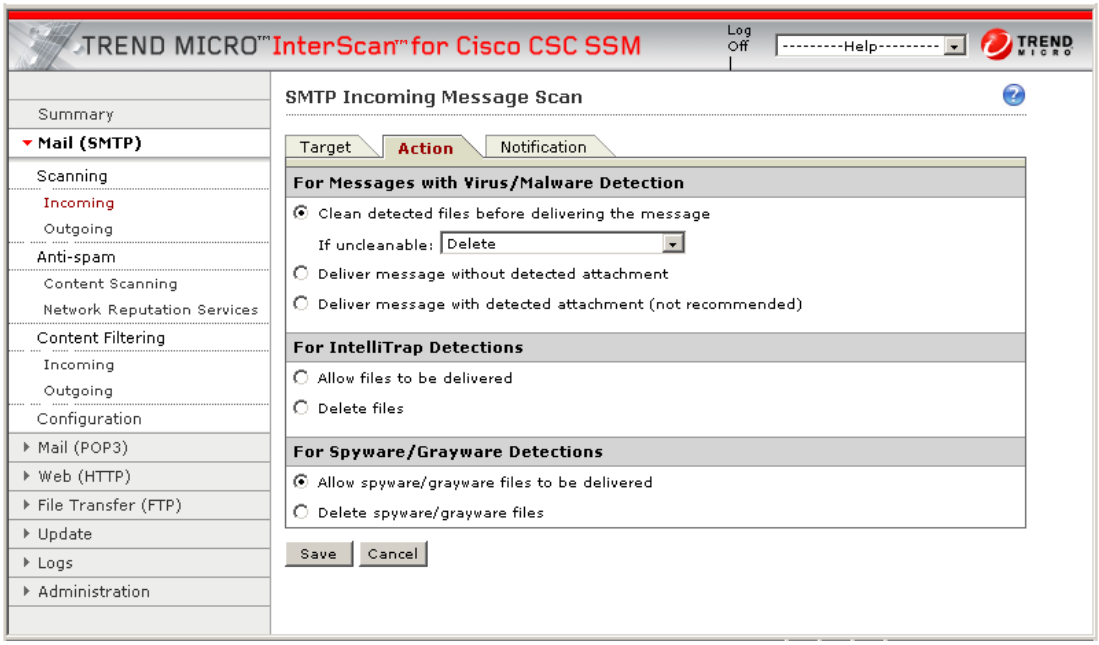


Tab Behavior

The interactive windows for your selection appear 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 three views: Target, Action, and Notification. You can switch among views by clicking the appropriate tab for the information you want. The active tab name appears in brown text; inactive tab names appear in black text.

Typically the tabs are related and work together. For example, in Figure 1-5, you need to use all three tabs to configure virus scanning of incoming SMTP traffic.

Figure 1-5 Tabs Working 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 threat is detected—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, you can click **Save** once to retain work on all three tabs.

Save Button

The Save button is disabled when the window first opens. After you perform tasks, the text on the button appears black instead of gray. This is an indication that you must click the button to retain the work you have done.

Default Values

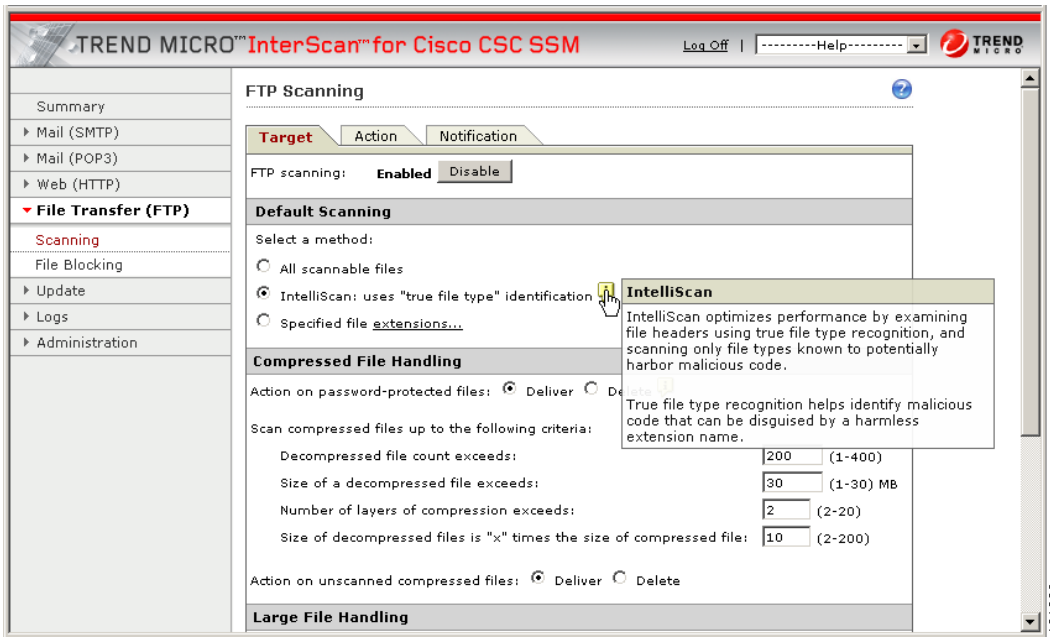
Many windows in the Trend Micro for Cisco CSC SSM user interface include fields that contain default selections. A default selection represents the choice that is best for most users, but you may change the default if another choice is better for your environment. For more information about entries in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

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

Tooltips

Some windows on the CSC SSM console contain information called a tooltip. Place your mouse over an icon to display a pop-up text box with additional information that helps you make a decision or complete a task. In the following example (shown in Figure 1-6), positioning the mouse over an icon displays more information about IntelliScan, one of several virus scanning options.

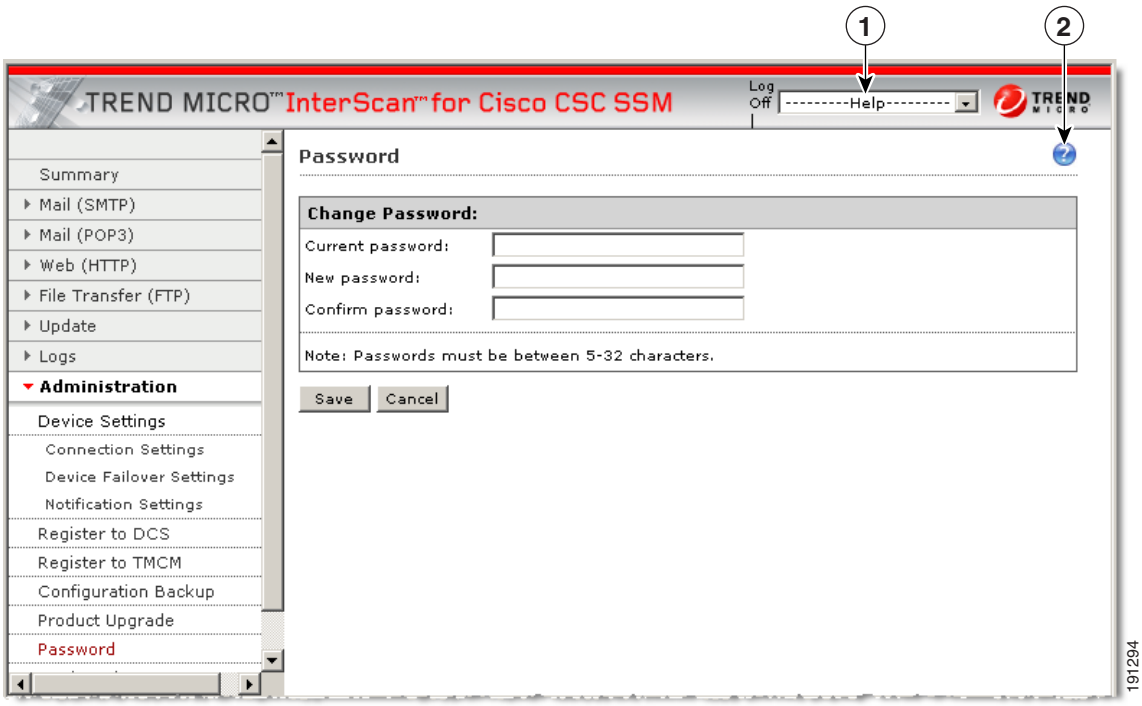
Figure 1-6 Tooltip Example



Online Help

Figure 1-7 shows the two types of online help available with Trend Micro InterScan for Cisco CSC SSM: general help from the Help drop-down menu (1) and context-sensitive help from the Help icon (2).

Figure 1-7 General and Context-Sensitive Online Help



To open general help, click the **Contents** and **Index** entry from the Help drop-down menu. A second browser window opens, which allows you to view the help contents shown in Figure 1-8. Click the **plus** sign to expand a help topic.

Figure 1-8 Online Help Contents

After an introduction, the organization of the online help topics follows the structure of the menu on the left in the user interface. Additional information about computer viruses is also available.

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

To open context-sensitive help, click the window help icon (). A second browser window appears, which includes information for the window that you are currently viewing.

Links in Online Help

The online help contains links, indicated by blue underlined text. Clink a link to go to another help window or display a pop-up text box with additional information, such as a definition. Disable pop-up blocking in your browser to use this feature.

For more information about Trend Micro InterScan for Cisco CSC SSM, see the online help.

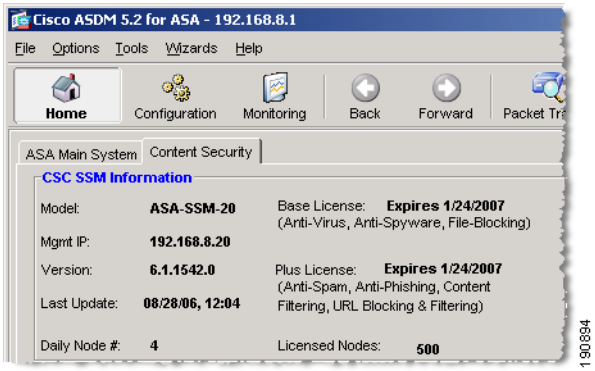
Licensing

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 on the CSC SSM console, but unlicensed features are not operational. 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 of which level of license your organization purchased, review the CSC SSM Information section of the Content Security tab, which summarizes your licensing information, as shown in Figure 1-9.

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



Alternatively, on the CSC SSM console, choose **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 is set to "Activated," you have the Plus License functionality. Otherwise, this field is set to "Not Activated."

Windows That Require Plus Licensing

Table 1-2 indicates which windows on the CSC SSM console are available with the Base License, and which are available only when you purchase the additional Plus License.

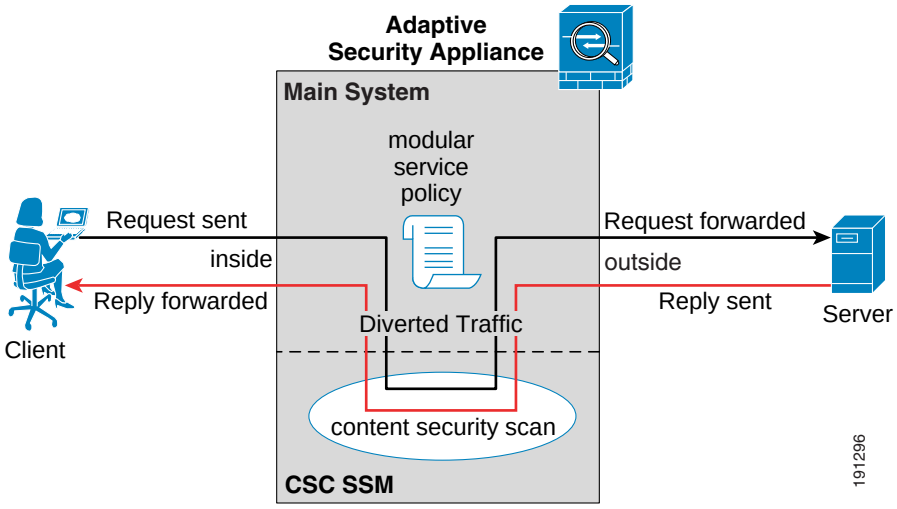
Table 1-2 Windows Available Based on License Type

Window 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 windows	x	
Logs > all windows	x	
Administration > all windows	x	

Process Flow

Figure 1-10 illustrates the flow of traffic when the CSC SSM is installed in the adaptive security appliance. A request is sent from a client workstation to a server. As the request is processed through the adaptive 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, but in the reverse direction.

Figure 1-10 Process Flow



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

CHAPTER 2

Verifying Initial Setup

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

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

Verifying ASA Clock Setup

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

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

Step 1 Choose **Configuration > Properties**.

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

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

Verifying CSC SSM Activation

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

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

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

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

Verifying Scanning

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

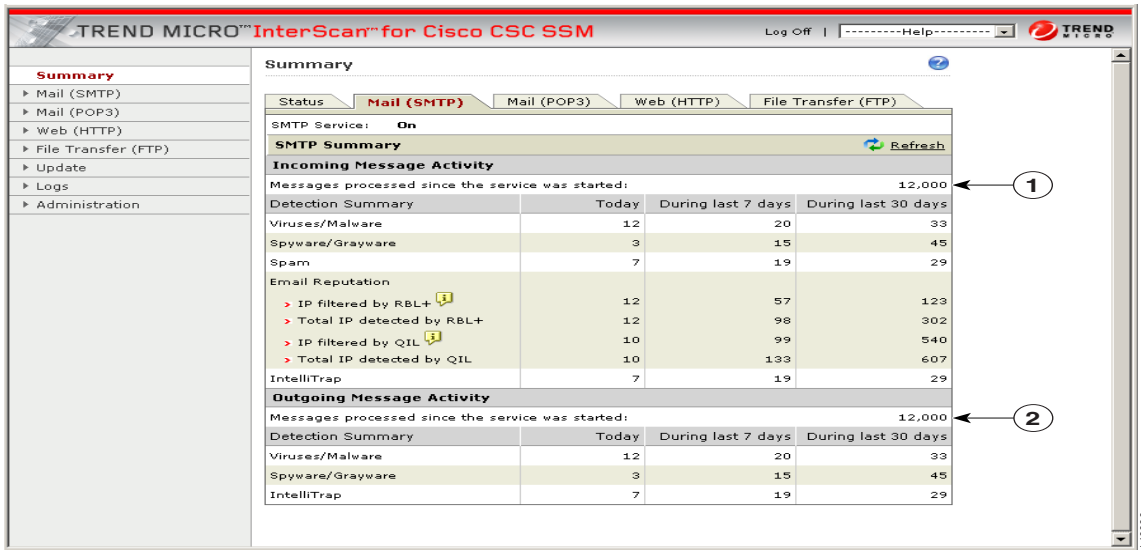
To verify that Trend Micro InterScan for Cisco CSC SSM is scanning your SMTP network traffic, perform the following steps:

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

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

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

Figure 2-1 Verify Scanning on the Summary Window



1	Incoming message activity counter	2	Outgoing message activity counter

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

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

Note The counters also reset whenever service is restarted.

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

Testing the Antivirus Feature

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

To test the antivirus feature, perform the following steps:

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

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

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

Figure 2-2 EICAR Download Area

Download area using the standard protocol http

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

Download area using the secure, SSL enabled protocol https

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

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

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

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

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

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

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

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

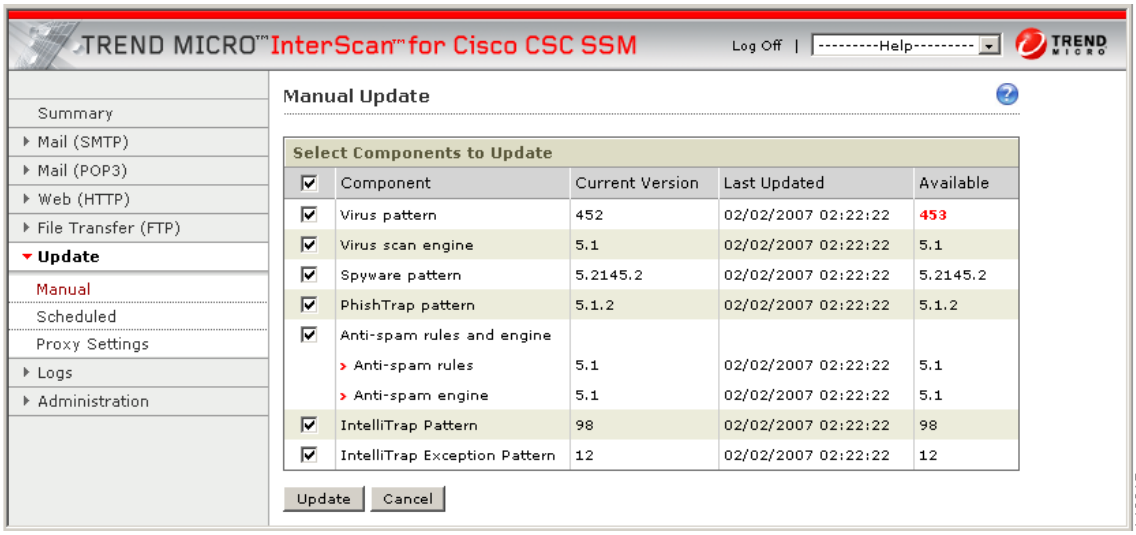
Verifying Component Status

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

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

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

Figure 2-3 Manual Update Window



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

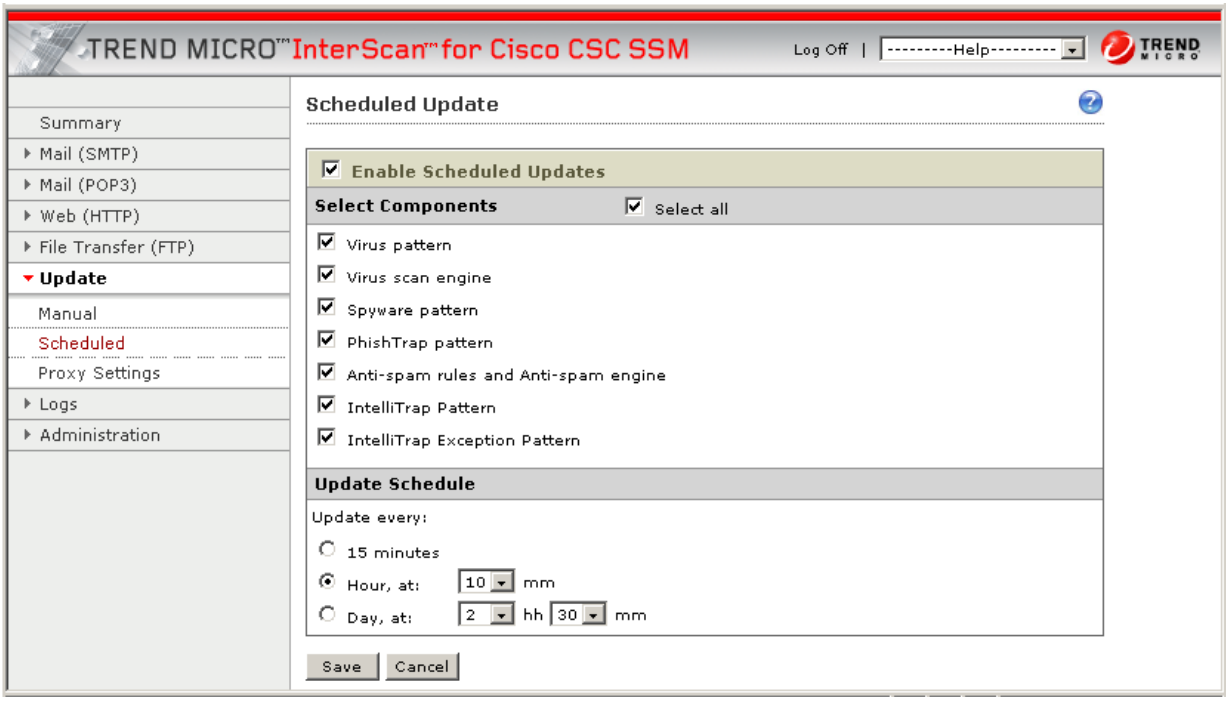
If the current and available versions are the same, and you think a new version is available, or if the Available column is blank, it could mean one of the following:

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

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

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

Figure 2-4 Scheduled Update Window

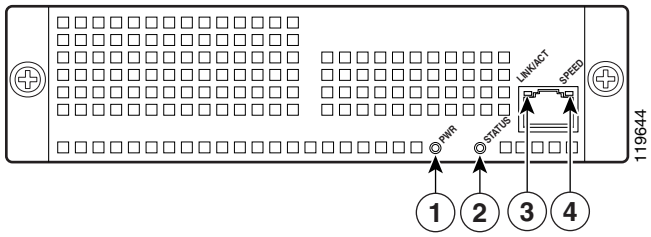


By default, Trend Micro InterScan for Cisco CSC SSM updates components periodically, with an automatic notification after a scheduled update has occurred. You can modify the scheduled update interval.

Viewing the Status LED

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

Figure 2-5 ASA SSM Indicators



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

Table 2-1 ASA SSM LED Indicators

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

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

Understanding SSM Management Port Traffic

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

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

CHAPTER 3

Configuring SMTP and POP3 Mail Traffic

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, page 3-1
- Defining Incoming and Outgoing SMTP Mail, page 3-2
- Enabling SMTP and POP3 Spyware and Grayware Detection, page 3-3
- Reviewing SMTP and POP3 Notifications, page 3-3
- Configuring SMTP Settings, page 3-5
- Enabling SMTP and POP3 Spam Filtering, page 3-6
- Enabling SMTP and POP3 Content Filtering, page 3-7

Default Mail Scanning Settings

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

Table 3-1 Default Mail Scanning Settings

Feature	Default Setting
SMTP scanning for incoming and outgoing mail	Enabled using All Scannable Files as the scanning method.
POP3 scanning	Enabled using All Scannable Files as the scanning method.
SMTP and POP3 scanning message filter (reject messages larger than a specified size)	Enabled to reject messages larger than 20 MB.
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
SMTP and POP3 compressed file handling for incoming and outgoing mail	Configured to skip scanning of compressed files when one of the following is true: • Decompressed file count is greater than 200. • Decompressed file size exceeds 20 MB. • Number of compression layers exceeds three. • Decompressed or compressed file size ratio is greater than 100 to 1. • Compressed files exceed specified scanning criteria.
SMTP incoming and outgoing messages POP3 messages in which malware is detected	Clean the message or attachment in which the malware was detected. If the message or attachment is uncleanable, delete it.
SMTP incoming and outgoing messages POP3 messages in which spyware or grayware is detected	Allows files to be delivered.
SMTP incoming and outgoing messages 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 SMTP and POP3 e-mail messages	Allows files to be delivered without scanning.

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

To obtain the maximum protection for your e-mail traffic, additional configuration settings are available that you may want to update. If you purchased the Plus License, which entitles you to receive anti-spam and content filtering functionality, you must configure these features.

Defining Incoming and Outgoing SMTP Mail

When an e-mail 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.

The message from psmith to jdoe and gwood is treated as an incoming message for both recipients, although gwood is considered an “outgoing” recipient.

You should set scanning to the Scan all option for incoming SMTP messages, and scanning to the IntelliScan option for outgoing messages. Make sure that you enable spyware or grayware detection for incoming messages only.

Enabling SMTP and POP3 Spyware and 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; however, it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

To detect spyware and other forms of grayware in your e-mail traffic, you must configure this feature on the SMTP Incoming Message Scan/Target, SMTP Outgoing Message Scan/Target, and POP3 Scanning/Target windows according to the following steps:

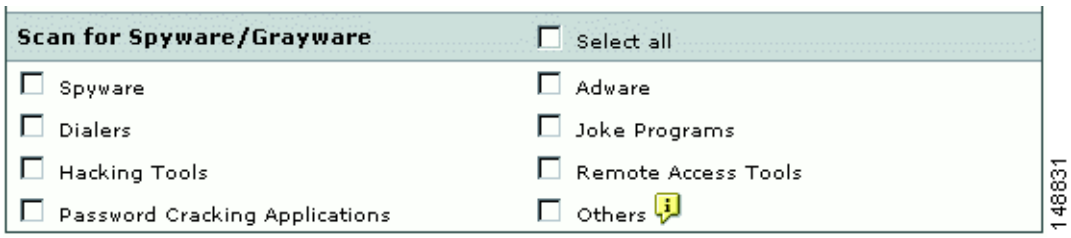
Step 1 To display the SMTP Incoming Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Incoming Scan** link.

Step 2 To display the SMTP Outgoing Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Outgoing Scan** link.

Step 3 To display the POP3 Scanning/Target window, in the CSC SSM console, choose **Mail (POP3) > Scanning > POP3 Scanning/Target**.

Step 4 In the Scan for Spyware/Grayware section of these windows (shown in Figure 3-1), choose the types of grayware that you want detected by Trend Micro InterScan for Cisco CSC SSM. See the online help for a description of each type of grayware listed.

Figure 3-1 Spyware and Grayware Scanning Configuration



Step 5 Click **Save** to enable the new configuration.

Reviewing SMTP and POP3 Notifications

This section describes notification settings and includes the following topics:

- Types of Notifications, page 3-4
- Modifying Notifications, page 3-4

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 e-mail message. For SMTP, you can also notify the sender or recipient.

You may also want to tailor the default text in the notification message to something more appropriate for your organization.

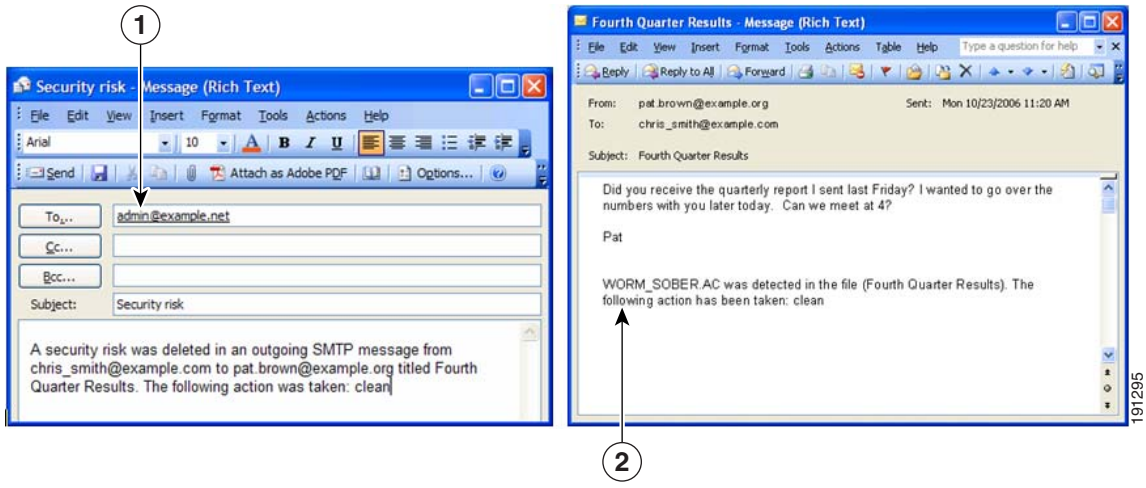
To review and reconfigure e-mail notifications, go to each of the following windows in the CSC SSM console:

- 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 e-mail traffic: e-mail notifications and inline notifications, as shown in Figure 3-2.

Figure 3-2 Examples of Notifications



1	E-mail notification	2	Inline notification

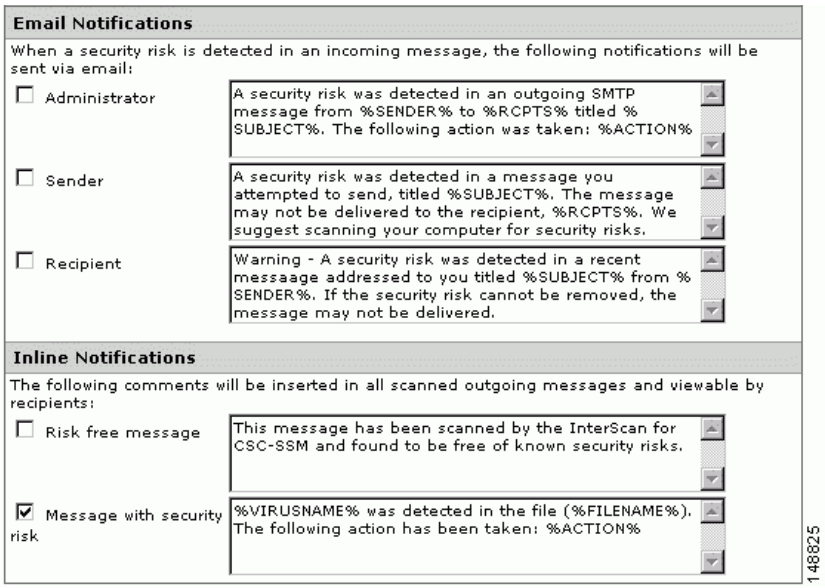
Notifications use variables called *tokens* to provide information that makes the notification more meaningful. For example, a token called **%VIRUSNAME%** is replaced with the text `WORM_SOBER.AC` in the inline notification example on the right.

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 an event occurs, go to the applicable window to update the settings. For example, Figure 3-3 shows the notification options on the Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification window.

Figure 3-3 Configure Notifications for Outgoing SMTP Messages



By default, the only notification is an inline notification to the message recipient, which means neither the sender nor the administrator of the originating organization is aware that a security threat has been detected and cleaned.

To make changes to these notifications:

Step 1 In the Email Notifications section of the window, select additional people to receive an e-mail notification.

Step 2 In the Inline Notifications section of the window, choose one of the listed options, neither, or both.

Step 3 Highlight the existing text and type your own message in the field provided.

Step 4 Click **Save** when you are finished.

Configuring SMTP Settings

Review the configuration settings available in the Mail (SMTP) > Configuration > SMTP Configuration window. The SMTP Configuration window contains the following four tabs:

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

Note These settings apply to SMTP messages only.

To configure settings in this window, perform the following steps:

Step 1 In the Message Filter tab, Trend Micro InterScan for Cisco CSC SSM is already configured to reject messages larger than 20 MB and messages addressed to more than 100 recipients. These settings protect you from an assault on your network that consumes CPU time while your e-mail server tries to handle large, 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 In 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. Check **Add this disclaimer** to enable this feature, or leave this option blank if you do not want to use this feature. To customize the disclaimer text, highlight it and redefine the message.

Step 3 In the Incoming Mail tab of the SMTP Configuration window, you can define additional incoming e-mail domains to do the following:

- Scan for viruses and other threats.
- Provide anti-spam functions.
- Perform content-filtering.

The Incoming mail domains field should already contain the incoming e-mail domain name you entered in the Host Configuration installation window during installation. If you have additions, enter the top-level domain (tld) name only. For example, enter only **example.com**; exclude subsidiary domains such as example1.com, example2.com, and so on. If there are no other incoming domains, no further action is needed.

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

- 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 a system because you have performed the following:
  - Set a shorter timeout for sending an e-mail (often an e-mail that takes longer to send is part of an intentional attempt to consume resources).
  - Limited the allowed number of errors triggered, indicative of someone resending a message over and over.
  - Limited the number of times the sender resets the conditions for attempting to send the same e-mail.
- The **Enable SMTP TLS traffic pass-through mode** checkbox is disabled by default. This setting allows sending and receiving MTAs to communicate using the encrypted TLS protocol.

Step 5 After you make changes, click **Save** to activate your updated SMTP configuration.

Enabling SMTP and POP3 Spam Filtering

You must configure the SMTP and POP3 anti-spam feature.

Note This feature requires the Plus License.

To configure the anti-spam feature, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Anti-spam** link to display the SMTP Incoming Anti-spam window.

Step 2 In the CSC SSM console, choose **Mail (POP3) > Anti-spam > POP3 Anti-spam** to display the POP3 Anti-spam window.

Step 3 For each of these windows, click **Enable**.

Step 4 Reset the anti-spam threshold to **Medium** or **High** if you do not want to use the default value.

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, a high incidence of false positives (legitimate messages that are identified as spam) occurs.

Step 5 In the Approved Senders section of the SMTP Incoming Anti-spam and POP3 Anti-spam/Target windows, add approved senders. Mail from approved senders is always accepted without being evaluated.

Note Approved senders that you have added and saved in either window appear in both windows. For example, if you add yourname@example.com to the Approved Senders list on the POP3 Anti-spam window. Open the SMTP Incoming Anti-spam window. The address for yourname@example.com has already been added to the list of Approved Senders on the SMTP Incoming Anti-spam window.

You can create the Blocked Senders list in either window; however, the list appears in both windows.

Step 6 In the Blocked Senders section of the SMTP Incoming Anti-spam and POP3 Anti-spam/Target windows, add the blocked senders. Mail from blocked senders is always rejected. Blocked senders that you have added and saved in either window appear in both windows.

Step 7 Configure the action for messages identified as spam on the SMTP Incoming Anti-spam and POP3 Anti-spam/Action windows. Choose one of the following options:

- 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 8 Click **Save** to activate the new anti-spam configuration settings.

Enabling SMTP and POP3 Content Filtering

You must configure the SMTP and POP3 content filtering feature.

Note This feature requires the Plus License.

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

Step 1 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Incoming Filtering** link to display the SMTP Incoming Content Filtering/Target window.

Step 2 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Outgoing Filtering** link to display the SMTP Outgoing Content Filtering/Target window.

Step 3 On the CSC SSM console, choose **Mail (POP3) > Content Filtering > POP3 Content Filtering/Target** to display the POP3 Content Filtering/Target window.

Step 4 For each of these windows, click **Enable**.

Step 5 Decide whether to use 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 6 In the Message Subject and Body section of the windows, specify words that if present in the message subject or body, trigger content filtering.

Step 7 In the Message Attachment section of the windows, specify characters or words that if present in the attachment name, trigger content filtering. 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 8 On each of these windows, click the **Action** tab to specify what action triggers content filtering. For e-mail messages, the options are as follows:

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

For attachments, the options are as follows:

- Allow violating attachments to pass. In this 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 9 On each of these windows, click the **Notification** tab to specify whether a notification is sent to the administrator for a content filtering violation. For SMTP, you can also notify the sender or recipient. Change the default text in the notification message by selecting it and redefining the message.

Step 10 Click **Save** to activate content filtering according to the new configuration settings.

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, which off-loads the task from the CSC SSM server. With NRS enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.

About RBL+ and QIL

The Realtime Blackhole List (RBL+) is a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed. The Quick IP Lookup (QIL) list is another database for tracking the reputation of IP addresses, but with this database, IP addresses 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 behaves according to the settings that you have selected.

For example, an MTA has been hijacked or an open relay exploited and used by a third party to deliver spam messages. The system administrator may discover the exploit after a brief period of time and correct it. Nevertheless, during this period of time, millions of spam messages are being and have been sent by the server. The tainted IP address may be added to the QIL database after only a few reports of spam, but then removed after the reports have subsided. On the other hand, because it takes longer for an IP address to be added to the RBL+, many that are only temporarily problematic (but nonetheless responsible for millions of spam) are not flagged by RBL+. After these IP addresses have been added to the RBL+, however, it is more difficult to remove them from the database.

Note There is a higher degree of certainty that IP addresses in the RBL+ are confirmed 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 and routing the mail at the same time.

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

Step 1 On the CSC SSM console, choose **Mail (SMTP) > Network Reputation Services** to open the Target window.

Step 2 Click **Enable**.

Step 3 Choose the level of service you want to use: High or Low. The high service level uses both the RBL+ and Quick IP Lookup services to check the reputation of the MTA from which the e-mail is received.

Step 4 In the Approved IP Address field, add the IP address or a range of IP addresses for any PCs you want to exempt from the lookup service.

Step 5 Click the **Action** tab to make that page active, and then choose the action you want the CSC SSM to take on messages found to match an entry in the RBL+ or QIL database. The available actions are as follows:

- 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 action 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, and other scanning rules are applied. This action is typically used only for troubleshooting.

CHAPTER 4

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

This chapter describes how to make HTTP and FTP traffic configuration updates, and includes the following sections:

- Default Web and FTP Scanning Settings, page 4-1
- Downloading Large Files, page 4-2
- Detecting Spyware and Grayware, page 4-3
- Scanning Webmail, page 4-4
- File Blocking, page 4-4
- URL Blocking, page 4-5
- URL Filtering, page 4-8

Default Web and FTP Scanning Settings

After installation, by default your HTTP and FTP traffic is scanned for viruses, worms, and Trojans. Malware such as spyware and other grayware require a configuration change before they are detected. Table 4-1 summarizes the web and file transfer configuration settings, and the default values that are in effect 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 scanning method.
Webmail scanning	Configured to scan Webmail sites for Yahoo, AOL, MSN, and Google.
File transfer (FTP) scanning of file transfers	Enabled using All Scannable Files as the 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 File transfer (FTP) compressed file handling for file transfers from an FTP server	Configured to skip scanning of compressed files when one of the following is true: • Decompressed file count is greater than 200. • Decompressed file size exceeds 30 MB. • Number of compression layers exceeds three. • Decompressed or compressed file size ratio is greater than 100 to 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. Configured to enable deferred scanning of files larger than 2 MB.
Web (HTTP) downloads and file transfers (FTP) for files in which malware is detected	Clean the downloaded file or file in which the malware was detected. If uncleanable, delete the file.
Web (HTTP) downloads and file transfers (FTP) for files in which spyware or grayware is detected	Files are deleted.
Web (HTTP) downloads when malware is detected	An inline notification is inserted in the browser, stating that Trend Micro InterScan for CSC SSM has scanned the file you are attempting to transfer, and has detected a security risk.
File transfers (FTP) notification	The FTP reply has been received.

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. Before making changes, review the online help for more information about these selections.

After installation, you may want to update additional configuration settings to obtain the maximum protection for your Web and FTP traffic. If you purchased the Plus License, which entitles you to receive URL blocking, anti-phishing, and URL filtering functionality, you must configure these additional features.

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 20 MB is scanned, but a download larger than 20 MB is not scanned.

In addition, you can:

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

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

Deferred Scanning

The deferred scanning feature is not enabled by default. When enabled, this feature allows you to begin downloading data without scanning the entire download. Deferred scanning allows you 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 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 you. However, some client software may time out because of the time required to collect sufficient network packets to compose complete files for scanning. The following table summarizes the advantages and disadvantages of each method.

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 you.	May result in the client timing out before the download is complete

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

Detecting Spyware and 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 or grayware detection is not enabled by default. To detect spyware and other forms of spyware and other grayware in your Web and file transfer traffic, you must configure this feature in the following windows:

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

To configure web scanning, do the following:

On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Web Scanning** link.

To configure FTP scanning, do the following:

On the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Scanning** link.

For more information, see the "Enabling SMTP and POP3 Spyware and Grayware Detection" section on page 3-3 and the online help for these windows.

Scanning Webmail

As specified in Table 4-1, Webmail scanning for Yahoo, AOL, MSN, and Google is already configured by default.

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. Configured sites are scanned until you remove them by clicking the **Trashcan** icon.

To add additional sites, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure Web Scanning** link.

The Target tab of the HTTP Scanning window appears.

Step 2 Click the **Webmail Scanning** tab.

Step 3 In the Name field, define the Webmail site by entering the exact website name, a URL keyword, and a string.

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

Step 4 Click **Save** to update your configuration.

For more information about how to configure additional Webmail sites for scanning, see the online help.

File Blocking

This feature is enabled by default; however, you must specify the types of files you want blocked. File blocking helps you enforce your organization policies for Internet use and other computing resources during work time. For example, your company does not allow downloading of music, both because of legal issues as well as employee productivity issues.

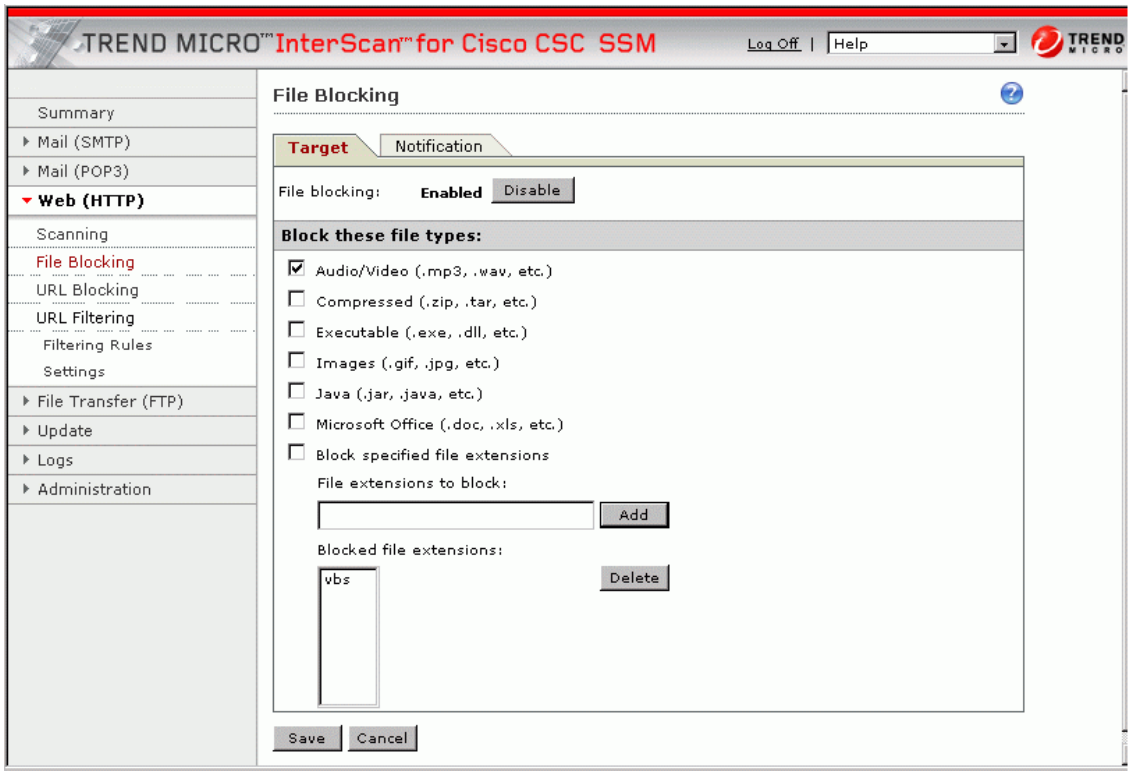
To configure file blocking, perform the following steps:

Step 1 To block downloads via HTTP, on the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure File Blocking** link to display the File Blocking window.

Step 2 To block downloads via FTP, on the Configuration > Trend Micro Content Security > File Transfer window in ASDM, click the **Configure File Blocking** link.

Step 3 To block transferring of music files, on the Target tab of the File Blocking window, check the **Audio/Video** check box, as shown in Figure 4-1.

Figure 4-1 Enable File Blocking



Step 4 You can specify additional file types by file name extension. To enable this feature, check the **Block specified file extensions** check box.

Step 5 Then enter additional file types in the File extensions to block field, and click **Add**. In the example, .vbs files are blocked.

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

Step 6 To view the default notification that displays in the browser or FTP client when a file blocking event is triggered, click the **Notifications** tab of the File Blocking window.

Step 7 To customize the text of these messages, select and redefine the default message. An optional notification to the administrator is available for HTTP file-blocking events, but is turned off by default. Check the **Send the following message** check box to activate the notification.

Step 8 Click **Save** when you are finished to update the configuration.

URL Blocking

This section describes the URL blocking feature, and includes the following topics:

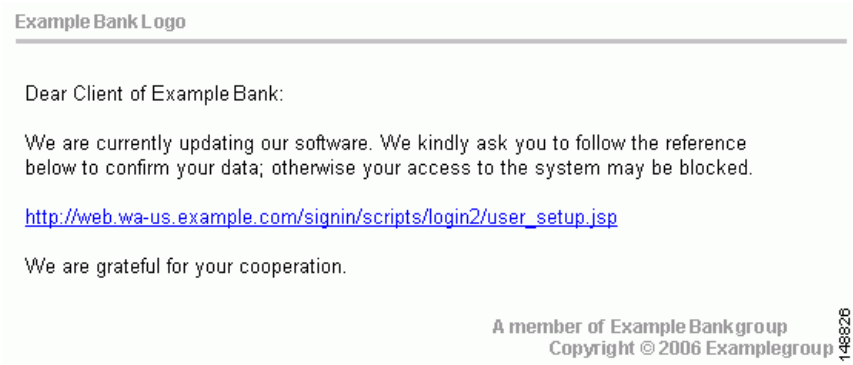
- Blocking from the Via Local List Tab, page 4-6
- Blocking from the Via Pattern File (PhishTrap) Tab, page 4-7

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

Note This feature requires the Plus License.

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 e-mail messages that appear to be from a legitimate organization, which request revealing private information such as bank account numbers. Figure 4-2 shows an example of an e-mail message used for phishing.

Figure 4-2 Example of Phishing



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

Blocking from the Via Local List Tab

To configure URL blocking from the Via Local List tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Blocking** 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 website name, a URL keyword, and a string.

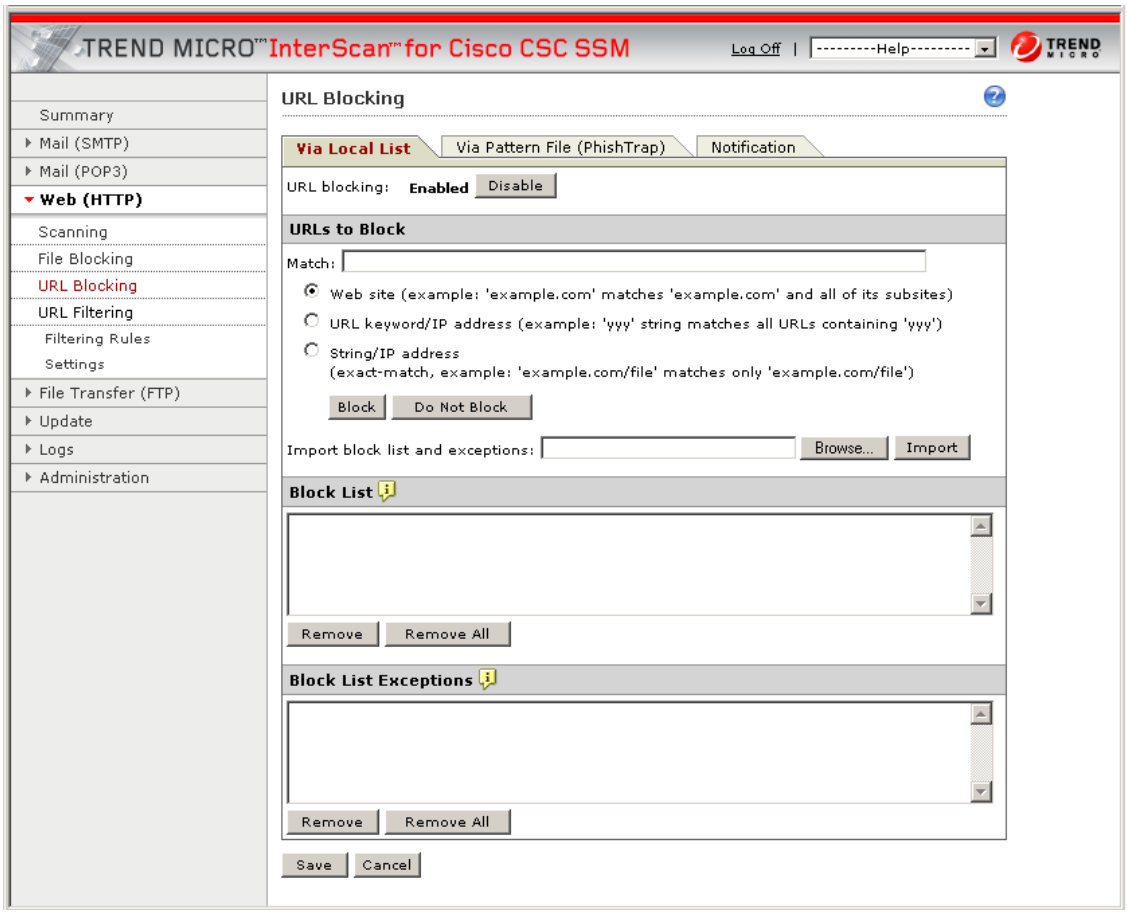
See the online help for more information about formatting entries in the Match field.

Step 3 To move the URL to the Block List, click **Block** after each entry. 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.

Figure 4-3 URL Blocking Window



Blocking from the Via Pattern File (PhishTrap) Tab

To configure URL file blocking from the Via Pattern File (Phishtrap) Tab, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Blocking** link to display the URL Blocking window.

Step 2 Then click the **Via Pattern File (PhishTrap)** tab.

Step 3 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). To submit sites that you think should be added to the PhishTrap pattern file, use the **Submit the Potential Phishing URL to TrendLabs** fields. TrendLabs evaluates the site and may add the site to this file if such action is warranted.

Step 4 To review the text of the default message that appears in the browser when an attempt is made to access a blocked site, click the **Notification** tab. The online help shows an example. Customize the default message by highlighting and redefining it.

Step 5 Click **Save** when you are finished to update the configuration.

URL Filtering

This section describes how to configure the URL filtering feature, and includes the following topics:

- Filtering Settings, page 4-8
- Filtering Rules, page 4-9

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

Note This feature requires the Plus License.

There are six URL filtering categories as follows:

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

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

Filtering Settings

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

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click **Configure URL Filtering Settings** to display the URL Filtering Settings window.

Step 2 On the URL Categories tab, review the subcategories listed and the default classifications assigned to each category to see whether the assignments are appropriate for your organization. For example, “Illegal Drugs” is a subcategory of the “Company-prohibited” category. If your organization is a financial services company, you may want to leave this category classified as company-prohibited. Check 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 reclassify the “Illegal Drugs” subcategory to the “Business function” category. See the online help for more information about reclassification.

Step 3 After you have reviewed and refined the subcategory classifications, check the associated subcategory to enable all the subcategories for which you want filtering performed.

Step 4 If there are sites within some of the enabled subcategories that you do not want filtered, click the **URL Filtering Exceptions** tab.

Step 5 Type the URLs you want to exclude from filtering in the Match field. You can specify the exact website name, a URL keyword, and a string.

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

Step 6 To move the URL to the Do Not Filter the Following Sites list, click **Add** after each entry. 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 7 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 8 Click **Save** to update the URL filtering configuration.

Step 9 Click the **Reclassify URL** tab to submit suspect URLs to TrendLabs for evaluation.

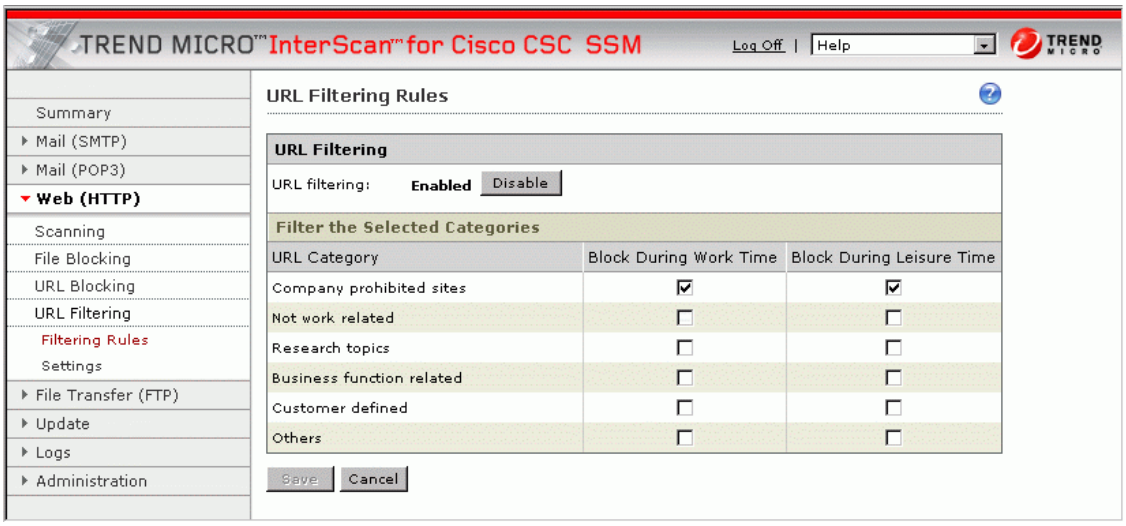
Filtering Rules

After you have assigned the URL subcategories to correct categories for your organization, defined exceptions (if any), and created the work and leisure time schedule, assign the filtering rules that determine when a category is filtering.

To assign the URL filtering rules, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Web window in ASDM, click the **Configure URL Filtering Rules** link to display the URL Filtering Rules window, shown in Figure 4-4.

Figure 4-4 URL Filtering Rules Window



Step 2 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.

Step 3 Click **Save** to update the configuration.

Note For URL Filtering to work correctly, the CSC SSM module must be able to send HTTP requests to the Trend Micro service. If an HTTP proxy is required, configure the proxy setting by choosing **Update > Proxy Settings**. The URL Filtering component does not support the SOCKS4 proxy.

CHAPTER 5

Managing Updates and Log Queries

This chapter describes how to manage component updates, proxy and system log message settings, and log queries, and includes the following sections:

- Updating Components, page 5-1
- Configuring Proxy Settings, page 5-3
- Configuring System Log Message Settings, page 5-3
- Viewing Log Data, page 5-4

Updating Components

New viruses and other security risks are released on the global computing community via the Internet or other distribution means at various times. 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. in the morning.

It is critical that you keep your components up-to-date to 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 the following:

- The virus pattern file
- The virus scan engine
- The spyware pattern file (also includes patterns for other types of grayware)
- The PhishTrap pattern file
- Anti-spam rules
- The anti-spam engine

The PhishTrap pattern file, anti-spam rules, and anti-spam engine are active and updated only if you have 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.

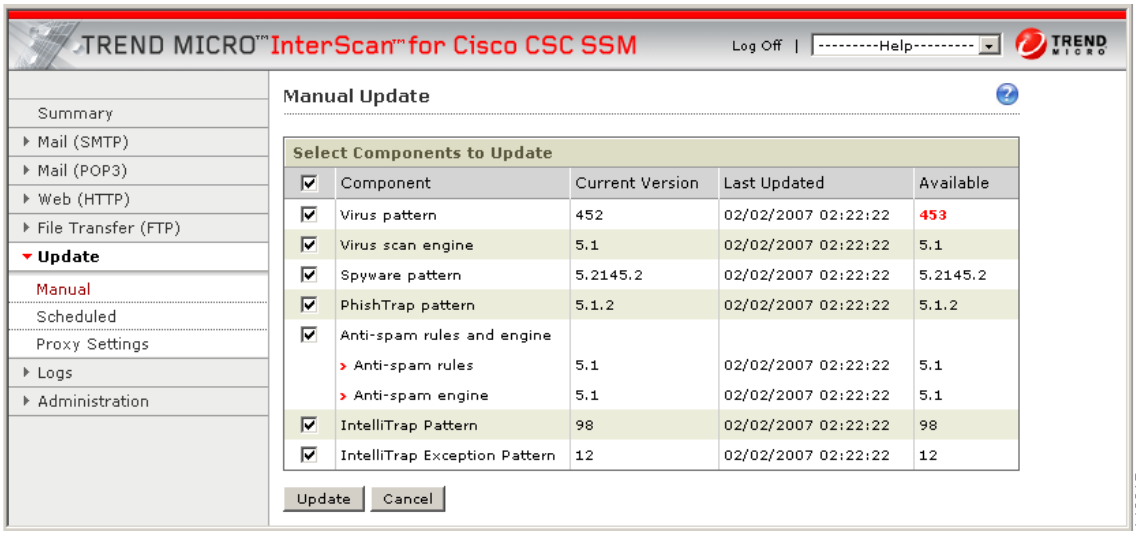
Manual Update

To view component status or update components manually, perform these steps:

Step 1 Choose **Updates > Manual**.

The Manual Update window displays (shown in Figure 5-1).

Figure 5-1 Manual Update Window



To view the component status, check the Available column on the right side of the window. If a more current component is available, the component version displays in red.

Step 2 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

You can configure component updates to occur as frequently as every 15 minutes.

To schedule component updates, perform the following steps:

Step 1 Choose **Updates > Scheduled** to view the Scheduled Update window.

Step 2 Choose the components to be updated according to the update schedule.

Step 3 Make the desired schedule changes.

Step 4 Click **Save** to update the configuration.

See the online help for more information about this feature.

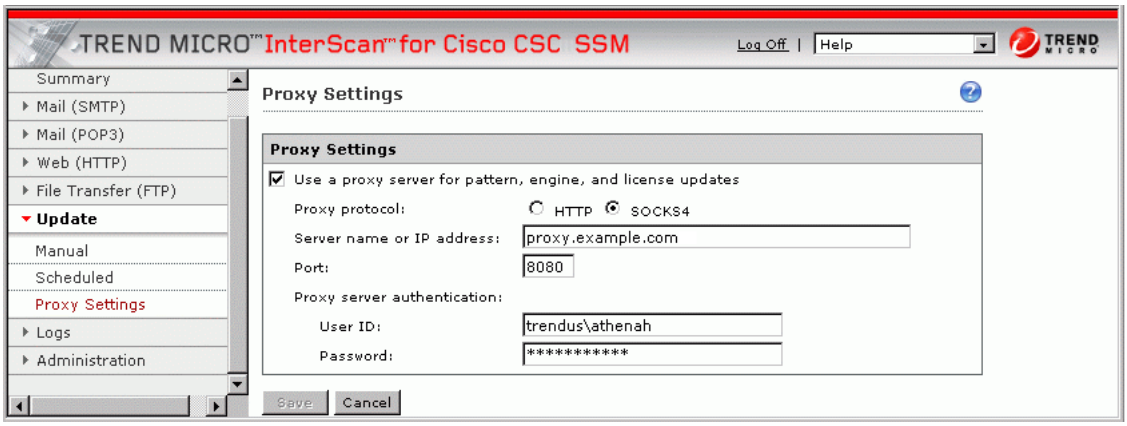
Configuring Proxy Settings

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.

To configure proxy settings, perform the following steps:

Step 1 To view current proxy server settings on the Proxy Settings window (shown in Figure 5-2), choose **Update > Proxy Settings**.

Figure 5-2 Proxy Settings Window



Step 2 If you set up a proxy server during installation, the HTTP proxy protocol is configured by default. To change the proxy protocol to SOCKS4, click the **SOCKS4** radio button.

Step 3 If needed, add an optional proxy authentication username and password in the User ID and Password fields.

Step 4 Click **Save** to update the configuration when you are finished.

See the online help for more information about this feature.

Configuring System Log Message Settings

After installation, log data such as virus and spyware or grayware detection is saved temporarily. To store log data, you must configure at least one syslog server. You may configure up to three syslog servers.

To configure system log messages, perform the following steps:

Step 1 Choose **Logs > Settings** to display the Log Settings window.

Step 2 Configure at least one syslog server. Check **Enable**, and then enter the syslog server IP address, port, and preferred protocol (either UDP or TCP).

See the online help for more information about this feature.

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 or anti-phishing and URL filtering if you did not purchase the Plus License.

For information about choosing and viewing log data, see the "Viewing Log Data" section on page 5-4. System log messages are also viewable from the ASDM. For more information, see the ASDM online help.

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 settings you chose for each type of risk. These events are recorded in the logs. To conserve system resources, you can purge these logs periodically.

To view log data, perform the following steps:

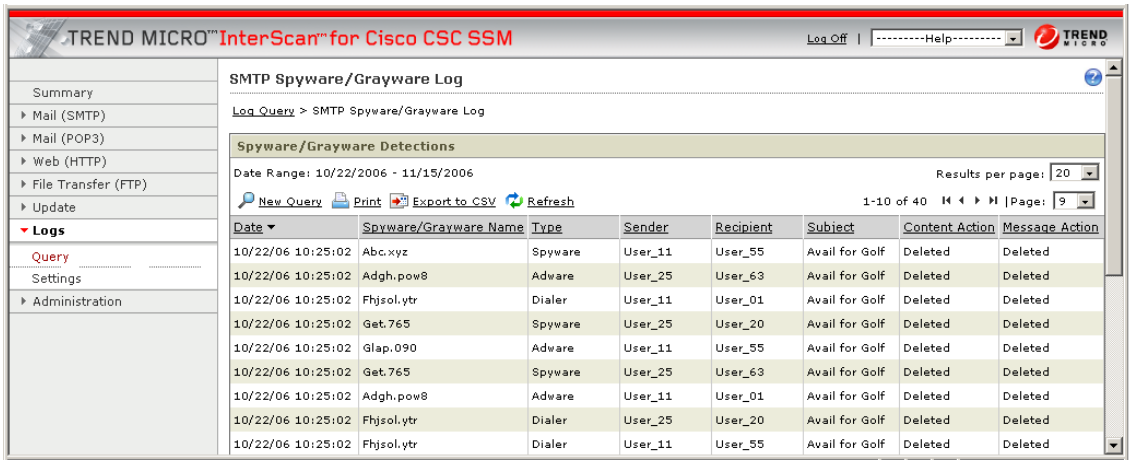
Step 1 Choose **Logs > Query** to display the Log Query window.

Step 2 Specify the inquiry parameters and click **Display Log** to view the log.

See the online help for more information about this feature.

Figure 5-3 shows an example of the spyware and 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, the exceptions are as follows:

- 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, the exceptions are as follows:

- Files or downloads that are too large for scanning.

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

```
Decompressed_File_Size_Exceeded
Large_File_Scanning_Limit_Exceeded
```

CHAPTER 6

Administering Trend Micro InterScan for Cisco CSC SSM

This chapter describes administration tasks, and includes the following sections:

- Configuring Connection Settings, page 6-1
- Managing Administrator E-mail and Notification Settings, page 6-2
- Backing Up Configuration Settings, page 6-3
- Configuring Failover Settings, page 6-5
- Installing Product Upgrades, page 6-6
- Viewing the Product License, page 6-7

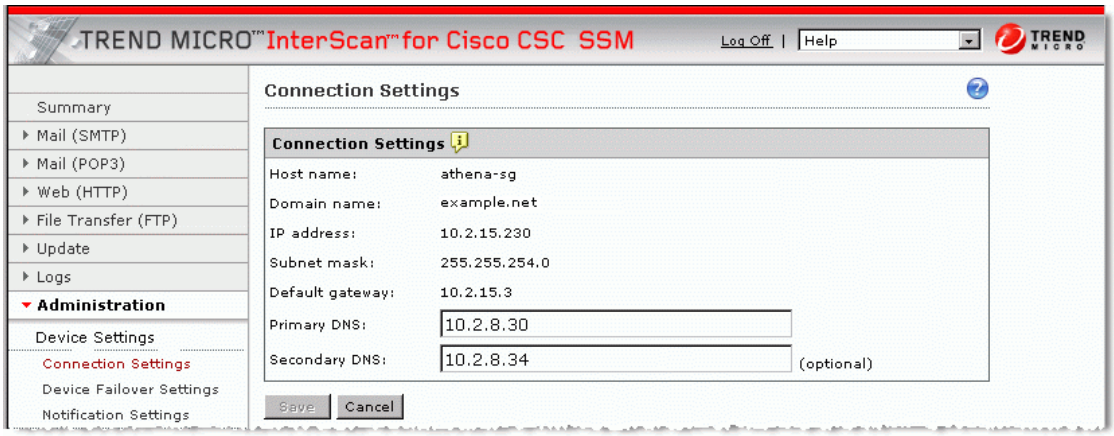
Configuring Connection Settings

To configure connection settings, perform the following steps:

Step 1 To view current network connection settings, choose **Administration > Device Settings > Connection Settings**.

The Connection Settings window (shown in Figure 6-1) displays selections that you made during installation.

Figure 6-1 Connection Settings Window



You can change the Primary DNS and Secondary DNS IP address fields in this window.

Step 2 To change other connection settings, such as hostname, domain name, or IP address, choose **Configuration > Trend Micro Content Security** and choose **CSC Setup** from the menu.

Step 3 You can also change these settings using the CLI. Log in to the CLI, and enter the **session 1** command. If this is the first time you have logged in to the CLI, use the default username (cisco) and password (cisco). You are prompted to change your password.

Step 4 Select option **1**, Network Settings, from the Trend Micro InterScan for Cisco CSC SSM Setup Wizard menu.

Step 5 Follow the on-screen instructions to change the settings.

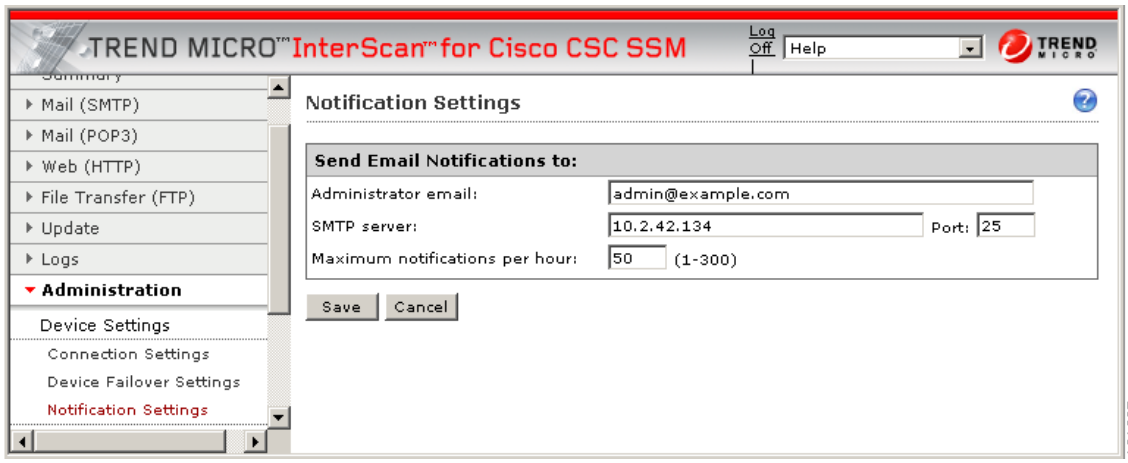
For more information, see the "Reimaging the CSC SSM" section on page A-4.

Managing Administrator E-mail and Notification Settings

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

- View or change the administrator e-mail address that you selected during installation on the Host Configuration window.
- View the SMTP server IP address 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 the Notification Settings window, perform the following steps:

Step 1 Enter the new information and click **Save**.

Step 2 You can also make these changes in the ASDM. Choose **Configuration > Trend Micro Content Security**, and then choose **CSC Setup** from the menu.

Backing Up Configuration Settings

This section describes how to back up configuration settings, and includes the following topics:

- Exporting a Configuration, page 6-4
- Importing a Configuration, page 6-4

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

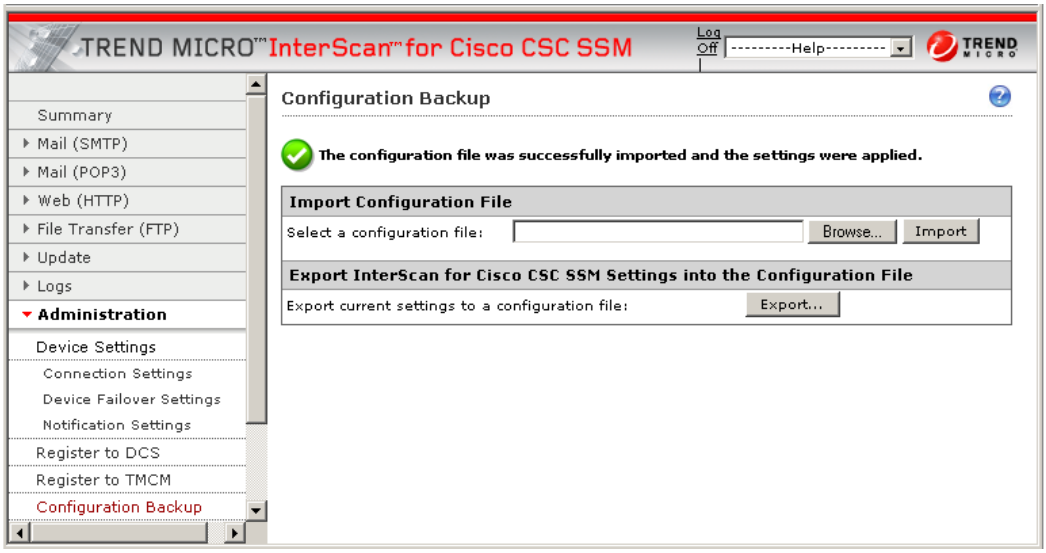
Note A configuration backup is essential for recovery in case you forget your ASDM or Web GUI password, depending on how you have set your password-reset policy. For more information, see Recovering a Lost Password, page 8-4 and Modifying the Password-reset Policy, page A-11.

As soon as you finish configuring Trend Micro InterScan for Cisco CSC SSM, create a configuration backup.

To back up configuration settings:

Choose **Administration > Configuration Backup** to display the Configuration Backup window, shown in Figure 6-3.

Figure 6-3 Configuration Backup Window



Exporting a Configuration

To save configuration settings, perform the following steps:

Step 1 On the Configuration Backup window, click **Export**.

A File Download dialog box appears.

Step 2 You can open the file, called config.tgz, or save the file to your computer.

Importing a Configuration

To restore configuration settings, perform the following steps:

Step 1 On the Configuration Backup window, click **Browse**.

Step 2 Locate the config.tgz file and click **Import**.

The filename appears in the Select a configuration file field. The saved configuration settings are restored to the adaptive security appliance.

Importing a saved configuration file restarts the scanning service and the counters on the Summary window are reset.

Configuring Failover Settings

Trend Micro InterScan for Cisco CSC SSM enables you to replicate a configuration to a peer unit to support the device failover feature on the adaptive security appliance. Before you configure the peer device, or the CSC SSM on the failover device, finish configuring the primary device.

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

Step	Configuring Failover Settings Checklist	Status
1	Decide which appliance should act as the primary device, and which should act as the secondary device. Record the IP address of each device in the space provided: **Notes:** _____ _____	❑ ❑
2	Open a browser window and enter the following URL in the Address field: http://<primary device IP address>:8443. The Logon window appears. Log on, and choose **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 choose **Administration > Device Settings > Device Failover Settings**.	❑
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 one to eight alphanumeric characters in the Encryption key field. Click **Save**, and then click **Enable**. The following message appears 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 behavior and appears because the peer is not yet configured.	❑
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 one to eight 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 appears 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	On the Device Failover Settings window for the primary device, click **Synchronize with peer**.	❑
7	The message in the Status field at the bottom of the windows should 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 has been successfully configured.

If you want to make a change to the configuration in the future, 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. For more information, see the "Installing Product Upgrades" section on page 6-6.

If the peer device becomes unavailable, an e-mail notification is sent to the administrator. The message continues to be sent periodically until the problem with the peer is resolved.

Installing Product Upgrades

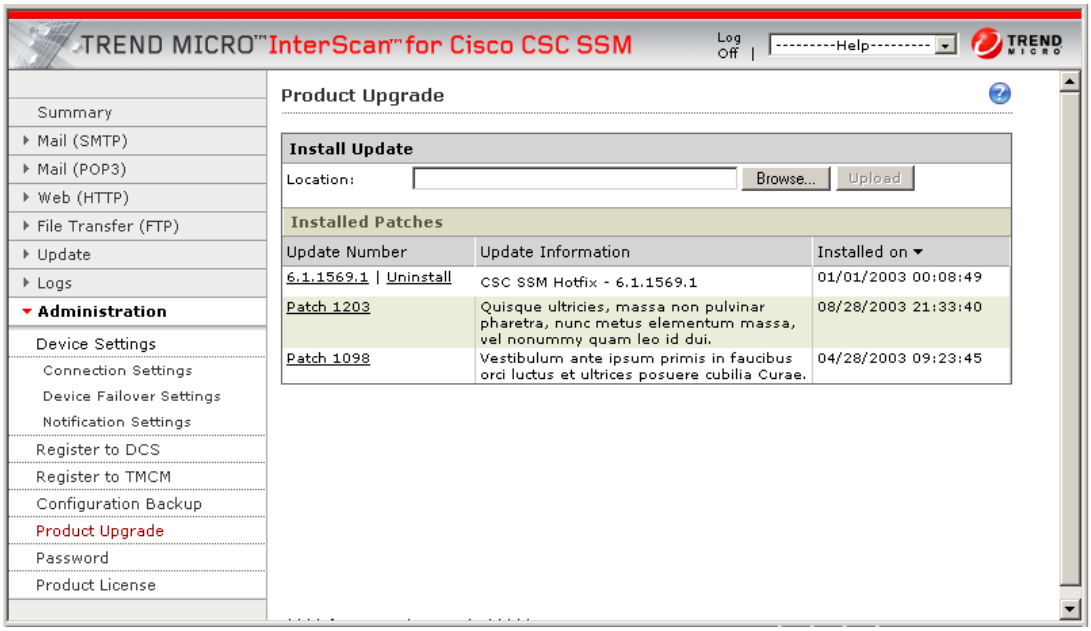
From time to time, a product upgrade becomes available that corrects a known issue or offers new functionality.

To install a product upgrade, do the following:

Step 1 Download the system patch from the website or CD provided.

Step 2 Choose **Administration > Product Upgrade** to display the Upgrade window, shown in Figure 6-4.

Figure 6-4 Product Upgrade 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.

For information about installing and removing upgrades, see the online help for this window.

Viewing the Product License

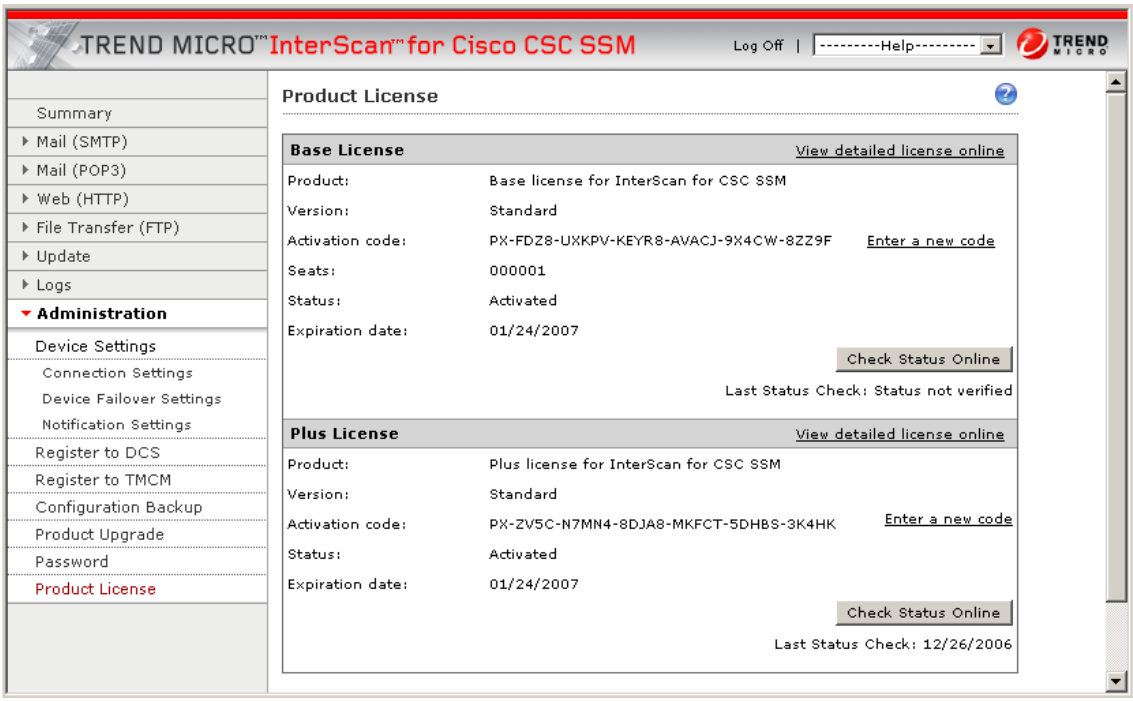
This section describes product licensing information, and includes the following topics:

- License Expiration, page 6-8
- Licensing Information Links, page 6-9
- Activating the Product, page 6-9
- Renewing a License, page 6-9

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

- Which license(s) are activated (Base License only, or Base License and Plus License)
- License version, which should state “Standard” unless you are temporarily using an “Evaluation” copy
- Activation Code for your license
- Number of licensed seats (users), which appears only for the Base License, even if you have 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. For more information, see the License Expiration section.

License Expiration

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

Figure 6-6 License Expiration Message

When your product license expires, you may 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 other components. Your network may no longer be protected from 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 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.

Licensing Information Links

To obtain licensing information, perform the following steps:

Step 1 In the Product License window, click the **View detailed license online** link to access the online registration website, where you can view information about your license, and find renewal instructions.

Step 2 Click the **Check Status Online** link to display a message below the Product License window title that describes the status of your license, similar to the example in the previous figure.

For additional information, see the online help for the Product License window.

Activating the Product

If you did not activate Trend Micro InterScan for Cisco CSC SSM during installation, you must activate the product before you can use it.

If you have not yet activated the product, the Administration Product License screen contains the following message:

```
"The product has not been activated. Activate the product now to download the current
virus pattern file and scan engine."
```

To activate the Trend Micro InterScan for Cisco CSC SSM, perform the following steps:

Step 1 Obtain an Activation Code, which is a 37-character code, including hyphens.

If you do not have an Activation Code, do one of the following:

- See http://www.cisco.com/go/license/public for Cisco registration information.
- (For registered users only). With your Cisco.com User ID, log in to http://www.cisco.com/go/license/. Use the Product Authorization Key (PAK) that came with your Cisco Software License Certificate to register. Your Activation Code will be sent to you via e-mail, usually within a few minutes.
- Contact Cisco or your reseller.

Step 2 Choose **Administration > Product License**. Click the **Enter a new code** link.

Step 3 In the New field, enter the activation code.

Step 4 Click **Activate**.

Step 5 After you have entered the activation code, run the ASDM CSC Setup Wizard to activate the product. For activation instructions, see the ASDM online help.

Renewing a License

You can renew a license at any time after the product activation. Contact your reseller or Cisco about ordering a license renewal for CSC SSM.

To renew a license for the CSC SSM, perform the following steps:

Step 1 Go to http://www.cisco.com/go/license/.

Step 2 Log in with your Cisco.com User ID, if necessary.

Step 3 Follow the on-screen instructions.

Step 4 Enter the renewal product code that you received when you registered the Product Authorization Key (PAK) that came with your Cisco Software License Certificate.

Step 5 Choose **Administration > Product License** after successfully renewing your license.

Step 6 Click **Check Status Online** to retrieve the latest license expiration date.

CHAPTER 7

Monitoring Content Security

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

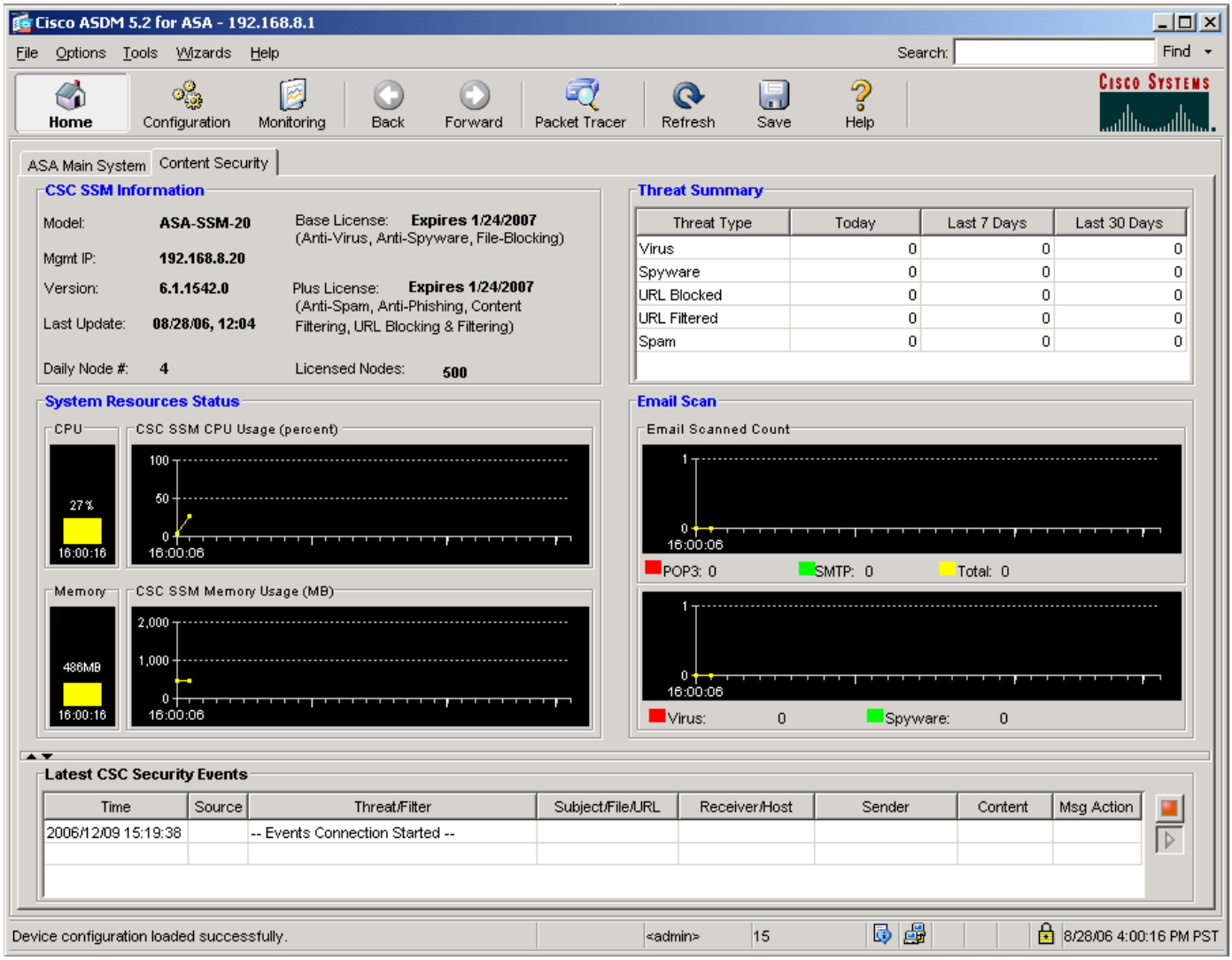
- Features of the Content Security Tab, page 7-1
- Monitoring Content Security, page 7-3
  - Monitoring Threats, page 7-3
  - Monitoring Live Security Events, page 7-5
  - Monitoring Software Updates, page 7-6
  - Monitoring Resources, page 7-7

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 the following:

- CSC SSM Information—Displays the product model number, IP address of the device, version, and build number of the CSC SSM software.
- Threat Summary—Displays a table summarizing threats detected today, within the last seven days, and within the last 30 days.
- System Resources Status—Allows you to view CPU and memory usage on the SSM.
- Email Scan—Provides a graphical display of the number of e-mail messages scanned and the number of threats detected in the scanned e-mail.
- 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 details about the information that appears in this window.

Monitoring Content Security

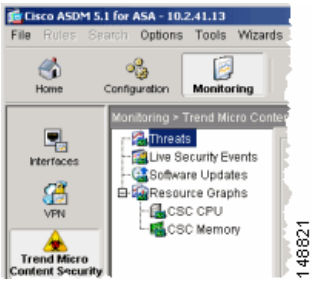
To display the content security monitoring settings for recent threat activity, perform the following steps:

Step 1 Choose **Monitoring > Trend Micro Content Security**, as shown in Figure 7-2.

Step 2 Select from the following options:

- Threats—Displays recent threat activity.
- Live Security Events—Displays a report of recent security events (content-filtering violations, spam, virus detection, and spyware detection) for monitored protocols.
- Software Updates—Displays the version and last date and time for updates to content security scanning components (virus pattern file, scan engine, and spyware or grayware pattern).
- Resource Graphs—Displays graphs of CPU usage and memory usage for the SSM.

Figure 7-2 Content Security Monitoring Options in ASDM



Monitoring Threats

To monitor threats, pefrom the following steps:

Step 1 Click **Threats** in the Monitoring pane, as shown in Figure 7-2, to choose up to four categories of threats for graphing.

Step 2 To display recent activity, select one or more of the following categories:

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

For example, if you have both the Base and Plus license, and you choose all four threat types for monitoring, the graphs appear similar to the example shown in Figure 7-3.

Figure 7-3 Threat Monitoring Graphs

The graphs refresh at frequent intervals (every ten seconds), which allows you to view recent activity at a glance. For more information, see the online help.

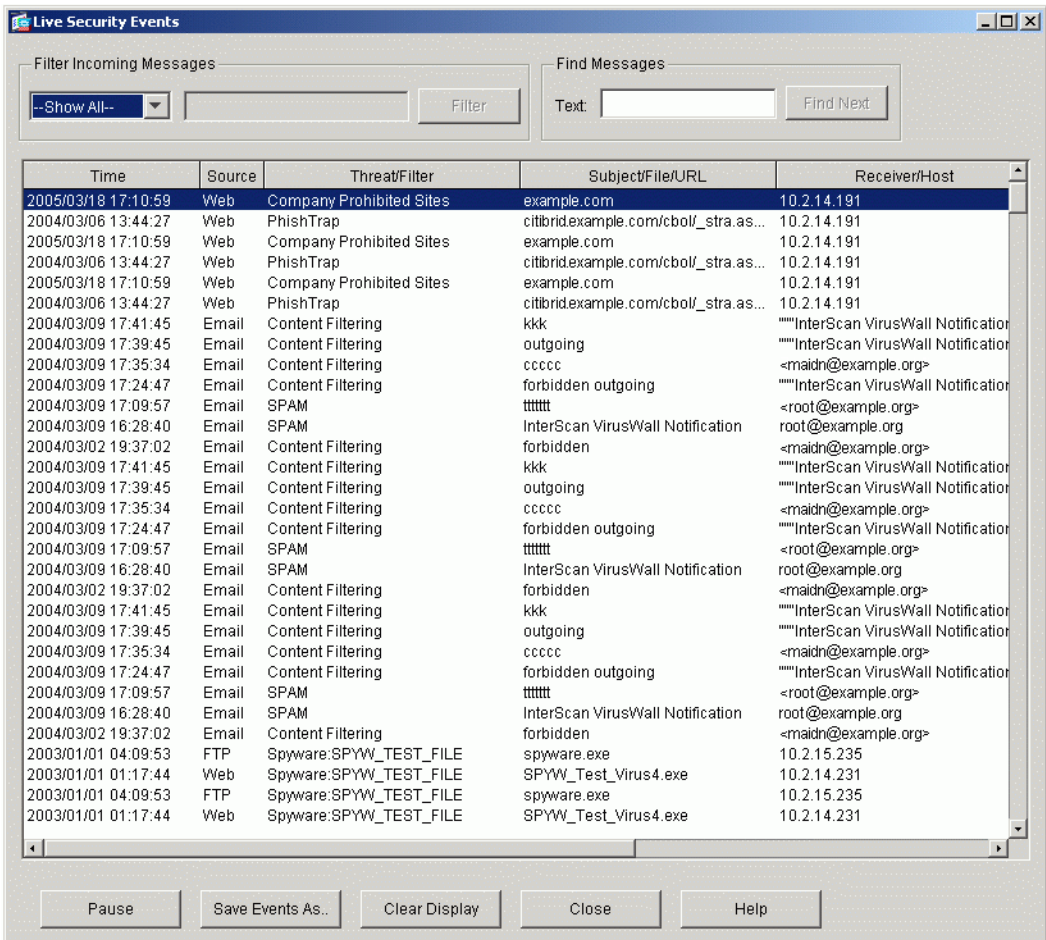
Monitoring Live Security Events

To monitor live security events, perform the following steps:

Step 1 Click **Live Security Events** in the Monitoring pane.

Step 2 Click **View** to create a report similar to the example in Figure 7-4.

Figure 7-4 Live Security Events Report



148819

This report lists events that the CSC SSM detected. 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. For more information, see the online help.

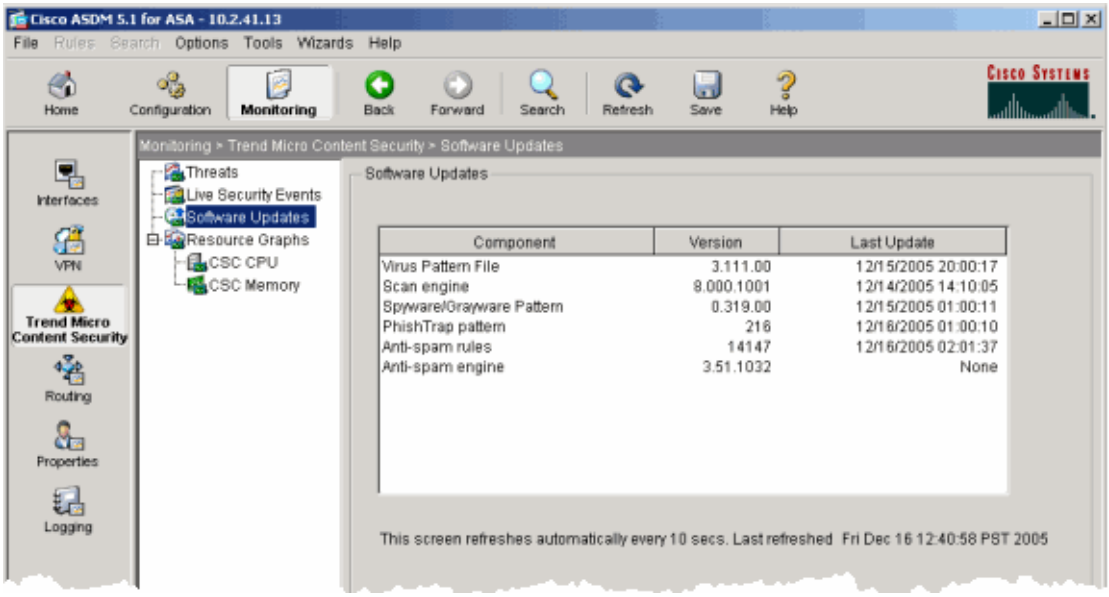
Monitoring Software Updates

To monitor software updates, perform the following steps:

Step 1 Click **Software Updates** in the Monitoring pane, as shown in Figure 7-5.

The following information about the CSC SSM components appears.

Figure 7-5 Software Updates Window



Step 2 To display the Scheduled Update window in the CSC SSM console, in the Monitoring > Trend Micro Content Security > Software Updates window in ASDM, click the **Configure Updates** link. For an example, 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 CSC SSM console. For an example, see Figure 5-1 on page 5-2. For more information about both types of updates, see the online help.

Monitoring Resources

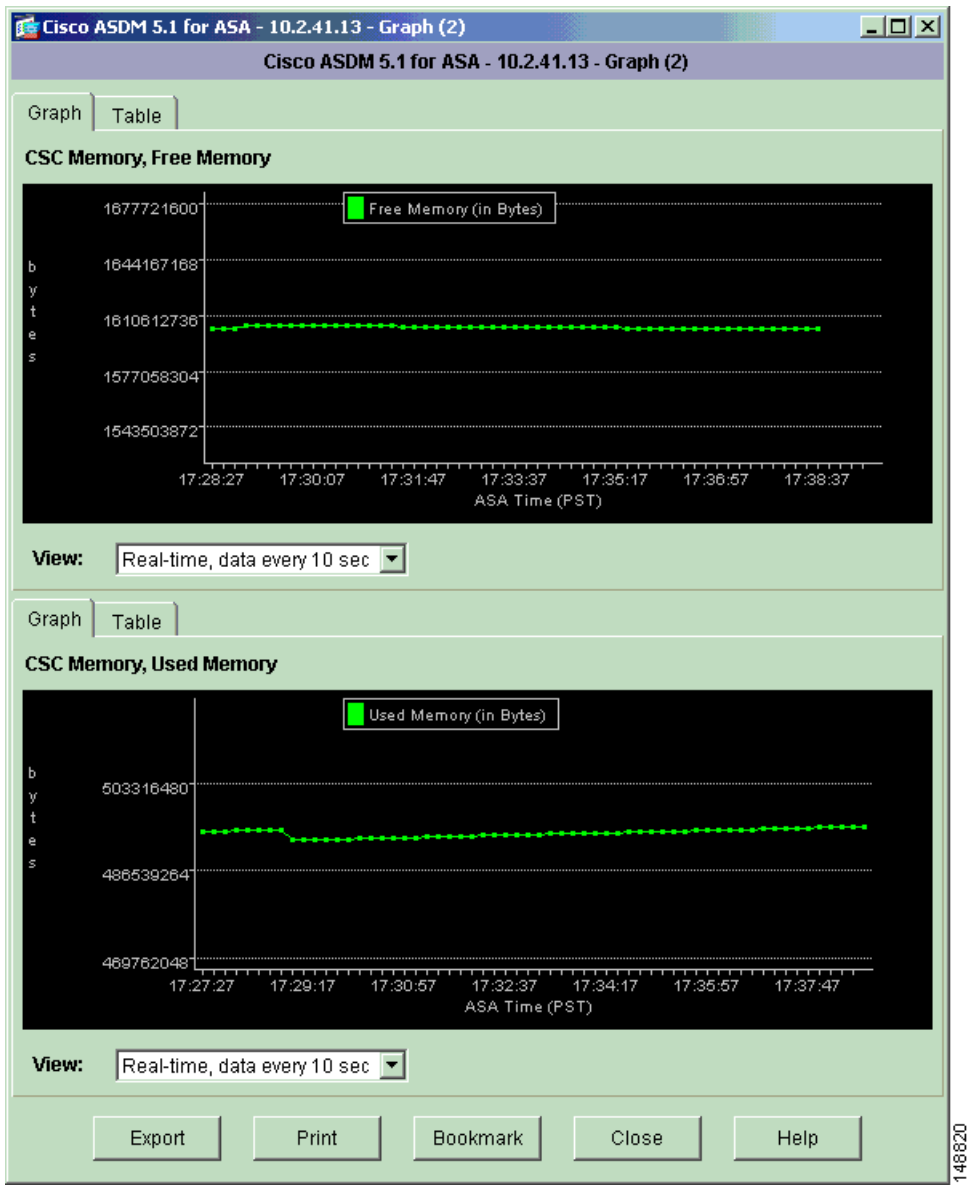
To monitor resources, perform the following steps:

Step 1 Click **Resource Graphs** in the Monitoring pane. You can monitor two types of resources: CPU usage and memory. If these resources are being used at almost 100%, you can do one of the following:

- Upgrade to ASA-SSM-20 (if you are currently using ASA-SSM-10).
- Purchase another adaptive security appliance.

Step 2 To view CPU or memory usage, select the information and click **Show Graphs**, as shown in Figure 7-6.

Figure 7-6 Memory Monitoring Graphs



CHAPTER 8

Troubleshooting Trend Micro InterScan for Cisco CSC SSM

This chapter describes how to troubleshoot various issues, and includes the following sections:

- Troubleshooting Installation, page 8-1
- What To Do If Installation Fails, page 8-3
- Troubleshooting Activation, page 8-4
- Troubleshooting Basic Functions, page 8-4
- Troubleshooting Performance, page 8-13
- Using Knowledge Base, page 8-15
- Using the Security Information Center, page 8-15
- Understanding the CSC SSM System Log Messages, page 8-16
- Before Contacting Cisco TAC, page 8-33

Troubleshooting Installation

The following describes how to install using the CLI. If problems occur during the installation, see the "What To Do If Installation Fails" section on page 8-3.

To install the CSC SSM via the CLI, perform the following steps.

Step 1 Enter the following command to begin the installation:

```
hostname(config)# hw-module module 1 recover configure
```

Output similar to the following appears:

```
Image URL [tftp://171.69.1.129/dqu/CSCSSM-6.1.1519.0.img]:
Port IP Address [0.0.0.0]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
hostname(config)# 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(config)#
hostname(config)# debug module-boot
debug module-boot enabled at level 1
```

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

```
hostname(config)# Slot-1 206> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26
00:13:50 PST 2005
Slot-1 207> domainname@yourdomain.com:/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/CSCSSM-6.1.1519.0.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/CSCSSM-6.1.1519.0.img@171.69.1.129 via 30.0.0.254
```

Step 3 The CSC 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
```

The TFTP download is complete. Note the number of received bytes, which should be the same size as the CSC SSM image.

Step 4 The ROMMON mode then launches the image.

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

The image is being unpacked and installed.

Step 5 After several minutes, the CSC SSM reboots. Messages similar to the following 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...
```

After a minute or two, the CSC SSM boots up.

Step 6 To verify that the CSC SSM has booted correctly, enter the following command:

```
hostname(config)# 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 6.1.1519.0

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.1.1519.0

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

Note 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 fails during the procedure described in the "Troubleshooting Installation" section on page 8-1.

Table 8-1 What to Do If Installation Fails

If installation fails at:	Your action is:
Step 2	Call Cisco TAC.
Step 3	**a.** Make sure you set the gateway IP address to 0.0.0.0 if your TFTP server is in the same IP subnet as the CSC SSM. **b.** If there is any router or 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 on the TFTP server. **c.** Verify the image path exists on the TFTP server, and that the directory and file are readable to all users.

Table 8-1 What to Do If Installation Fails

If installation fails at:	Your action is:
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. In this case, try another TFTP server.
Step 5 or Step 6	Download the image again and try once more to install. If the installation 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 the adaptive security appliance. For more information, see *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the ASDM online help.

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

This section describes issues you may encounter with basic functions, and includes the following topics:

- Cannot Log On, page 8-4
- Recovering a Lost Password, page 8-4
- Summary Status and Log Entries Out of Synch, page 8-5
- Delays in HTTP Connections, page 8-6
- Access to Some Websites Is Slow or Inaccessible, page 8-6
- FTP Download Does Not Work, page 8-7
- Reimaging or Recovery of CSC Module, page 8-7

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

If you forget your password, it can be recovered. For more information, see Recovering a Lost Password, page 8-4.

Recovering a Lost Password

The two passwords used to manage the CSC SSM are as follows:

- The ASDM/Web interface/CLI password

- The root account password

The default entry for both passwords is "cisco."

To recover your passwords in case you lose one or more of them, consider the following:

- If you have the ASDM/Web interface/CLI password, but have lost the root account passwords, you can continue to manage the CSC SSM via the Web interface.
- Unless you have configured the password-reset policy to "Allowed," you cannot use the root account in the future. If the password-reset policy is set to "Denied," recovering these two passwords requires reimaging of the CSC SSM and restoration of the configuration according to the subsequent procedure. For more information, see "Modifying the Password-reset Policy" section on page A-11.

Caution Access the root account only under the supervision of Cisco TAC. Unauthorized modifications made through the root account are not supported and require that the device be reimaged to guarantee correct operation.

- If you have lost all passwords, you must reimage the device and restore the configuration, unless you have configured the password-reset policy to "Allowed."

To reimage the CSC SSM and recover the configuration, perform the following steps:

Step 1 Reimage the CSC SSM, which restores the factory default settings. Reimaging transfers a factory default software image to the SSM. To transfer an image, see the "Reimaging and Configuring the CSC SSM Using the CLI" section on page A-1.

After reimaging, all passwords are restored to their default value.

Step 2 Reactivate the device and log in using the default password "cisco," and then create a new ASDM password.

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

Step 4 To restore the configuration settings, import the most recent configuration backup.

Step 5 After you have imported the configuration backup, browse through all of the configurations to verify their accuracy.

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 with the statistics displayed in the log reports. In the CSC SSM console, choose **Logs > Query** to access the logs. This mismatch happens because of the following:

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

Delays in HTTP Connections

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. The CSC SSM first checks the local URL filtering database. If no entry is located, then the CSC SSM tries to access the URL database when processing an HTTP request from a client. If you cannot grant Internet access to the CSC SSM (either direct or indirect via a proxy), disable URL filtering.

In addition, disabling Deferred Scanning may cause large file transfers to be slow or time out.

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 non-configurable, 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 will fail. The workaround is to exclude the site from scanning.

For example, for a site on the outside network with the IP address, 100.100.10.10:

```
exempt http traffic to 123.123.10.10
access-list 101 deny tcp any host 123.123.10.10 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
```

This configuration exempts HTTP traffic to 100.100.10.10 from being scanned by the CSC SSM.

Performing a Packet Capture

If there are sites you can access without going through the 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 also.

For example, if the client has an IP address, 1.1.1.1, and the outside website has an 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
```

To perform a packet capture, perform the following steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command:

```
hostname(config)# capture csc_cap interface asa_dataplance buffer 10485760
```

Note The number of bytes in the capture buffer is 10485760. The example is 10 MB.

Step 3 Start the traffic testing.

Step 4 Enter the following command to transfer the captured buffer out of the box:

```
hostname(config)# copy /pcap capture:csc_cap tftp://IP/path
```

Step 5 Enter the following command to stop the capture:

```
hostname(config)# no capture csc_cap interface asa_dataplane
```

Note You can use the last command to reset or clear the buffer between tests, but you must reenter the **capture** command.

FTP Download Does Not Work

If your FTP login works, but you cannot download via FTP, do the following:

- Verify that the inspect ftp setting is enabled on the adapative security appliance.
- Verify that Deferred Scanning is enabled on the FTP Scanning page.

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

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

This sections describes issues you may encounter with scanning for viruses or spam, and includes the following topics:

- Cannot Update the Pattern File, page 8-8
- Spam Not Being Detected, page 8-8
- Cannot Create a Spam Stamp Identifier, page 8-8
- Unacceptable Number of Spam False Positives, page 8-9
- Cannot Accept Any Spam False Positives, page 8-9
- Unacceptable Amount of Spam, page 8-9
- Virus Is Detected but Cannot Be Cleaned, page 8-9
- Virus Scanning Not Working, page 8-9
- Downloading Large Files, page 8-11
- Restart Scanning Service, page 8-12

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 in 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.

If the pattern file is current, the following may be true:

- The Trend Micro ActiveUpdate server is temporarily down. Try to update the pattern file again in a few minutes.
- Check the network settings and the connectivity of the SSM, including the proxy settings.

Spam Not Being Detected

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

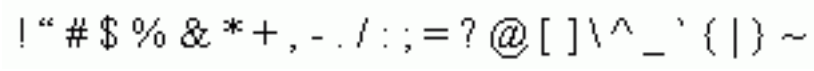
- You have the Plus License installed and it is current.
- You must have a valid Plus License and the correct DNS settings for the network-based, anti-spam NRS to function correctly.
- You have enabled the feature; the anti-spam option is not enabled by default. For more information, see Enabling SMTP and POP3 Spam Filtering, page 3-6.
- You have configured the incoming mail domain. The content-based anti-spam scanning is only applied to mail recipients belonging to Incoming Domains. For more information, see Configuring SMTP Settings, page 3-5.

Cannot Create a Spam Stamp Identifier

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

Figure 8-1 Special Characters for Spam Stamp Identifier



Note If you try to use characters other than those specified, you cannot use the spam identifier for 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. For more information, see the online help for these two windows.

Also, if users in your network are receiving newsletters through e-mail, this type of message tends to trigger a high number of false positives. Add the e-mail 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. If you still receive an unacceptable amount of spam, enable the network-based, anti-spam (NRS) setting. Choose **Mail (SMTP) > Anti-spam > Network Reputation Services**.

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

Virus Scanning Not Working

This section describes why virus scanning may not work, and includes the following topics:

- Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration, page 8-10
- Scanning Not Working Because the CSC SSM Is in a Failed State, page 8-10

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 Cisco TAC for assistance.

Also, test the virus scanning feature by following the instructions described in the "Testing 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 because of an incorrect firewall policy configuration. Use the **show service-policy csc** command to configure the SSM to process traffic.

The following example shows how to configure the SSM to process traffic:

```
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, system log message 421007 is generated.

Enter the following command to view the status of the SSM card:

```
hostname(config)# show module 1
```

The output appears in several tables, as shown in the following example. The third table, SSM Application Name, displays status, which is “Down.”

```
Mod Card Type                                    Model  Serial No.
--- -------------------------------------------- ------------------------------
1 ASA 5500 Series Security Services Module-10ASA-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 6.1.1519.0

Mod SSM Application Name           Status            SSM Application Version
--- ------------------------------ ----------------------------------------
 1 CSC SSM                        Down              6.1.1519.0

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

The three possible states that could display in the Status field for the third table are as follows:

- 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, enter the following command:

```
hostname(config)# show module 1 detail
```

Example output similar to the following appears:

```
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 6.1.1519.0
    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:       6.1.1519.0
    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 appears in the App. Status field. In the example, the status is “Down.” The possible states for this field are as follows:

- 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 application is reloading recently updated patterns or configuration changes. The traffic is interrupted temporarily with either a “fail-open” or “fail-close.” The adaptive security appliance will not perform a failover because this is an administrative 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, Trend Micro 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 action could:

- Result in the file being downloaded, very slowly at first, but more quickly as the download progresses.

- Take longer than the automatic browser timeout period. As a result, the user is unable to receive the file contents at all because the browser times out before the download completes.

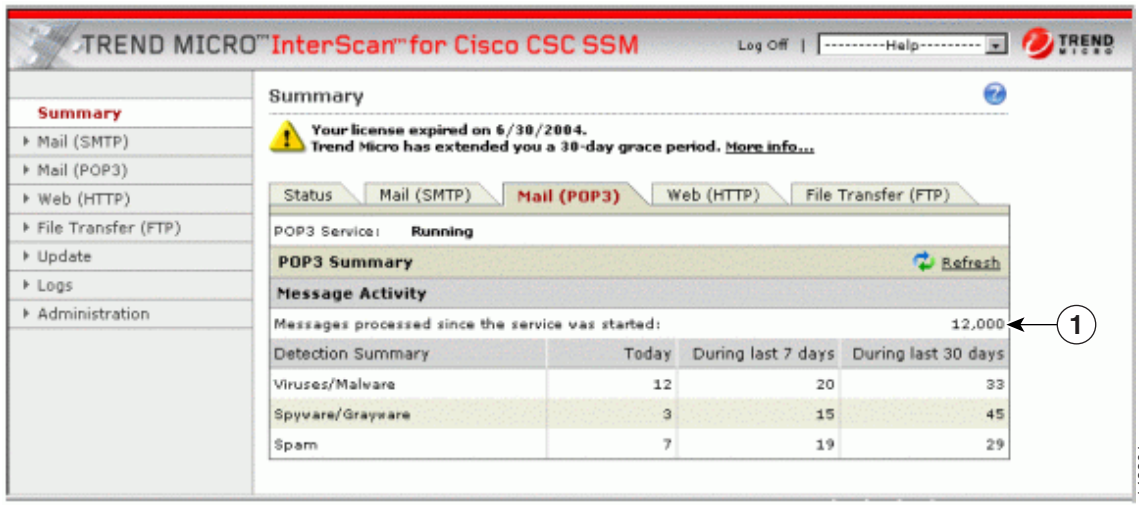
If you enabled deferred scanning, part of the content of the large file is delivered without scanning to prevent a timeout from occurring. Subsequent portions of the content are being scanned in the background and are then downloaded if no threat is detected. If a threat is detected, the rest of the file is not downloaded; nevertheless, the unscanned portion of the large file is already stored on the user machine and may introduce a security risk.

Note If you experience difficulty with Windows updates, you may need to enable deferred scanning and set the size to ten. See the logs or contact Cisco TAC for details.

Restart Scanning Service

In the Message Activity area, the Mail (SMTP and POP3) tabs on the Summary window display a count of Messages processed since the service was started. 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:

- A pattern file or scan engine update
- A configuration change
- The 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.

When the counters reset, it is normal behavior. If, however, you have a continuous zero in the Messages processed fields, e-mail traffic is not being scanned and you should investigate.

Troubleshooting Performance

This section describes issues you may encounter with performance, and includes the following topics:

- CSC SSM Console Timed Out, page 8-13
- Status LED Flashing for Over a Minute, page 8-13
- SSM Cannot Communicate with ASDM, page 8-13
- Logging in Without Going Through ASDM, page 8-13
- CSC SSM Throughput is Significantly Less Than ASA, page 8-14

CSC SSM Console Timed Out

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

Status LED Flashing for Over a Minute

If the Status LED continues flashing for more than one minute, the scanning service is not available. To resolve this problem, reboot the system from ASDM, or contact Cisco TAC 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

For information about resetting port access control, see the "Resetting the Management Port Access Control" section on page A-16.

Logging in Without Going Through ASDM

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

Step 1 Enter the following URL in a browser window:

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

For example:

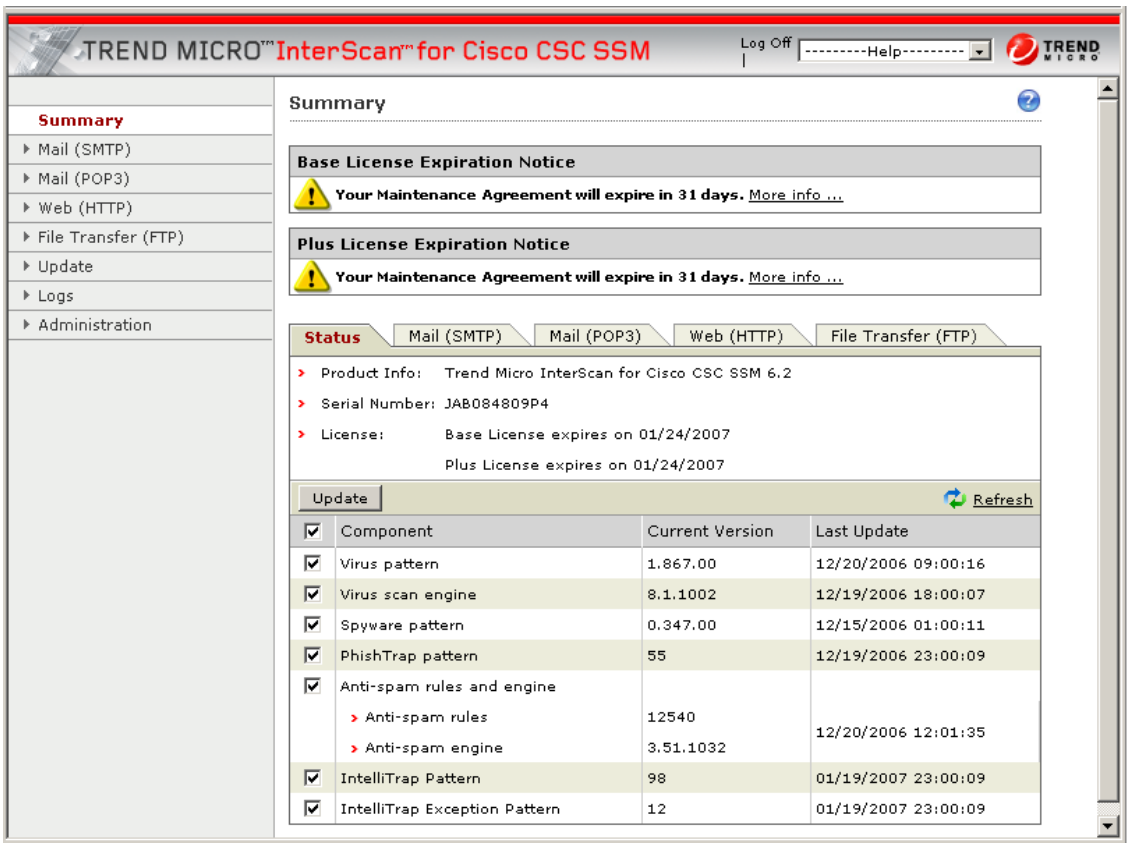
`https://10.123.123.123:8443/`

The Logon window appears.

Step 2 Enter the password you created in the Setup Wizard on the Password Configuration installation window and click **Log On**.

The default view of the CSC SSM console is the Status tab on the Summary window, as shown in Figure 8-3.

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 more overhead than the protocol-conformance checking that is usually done by a firewall. The workaround is to divert only the connections that need to be scanned to the CSC SSM to mitigate the performance mismatch.

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

For more information, see *Cisco Security Appliance Command Line Configuration Guide*.

Using Knowledge Base

You can search for more information in the Trend Micro online Knowledge Base, available at the following URL:

http://esupport.trendmicro.com

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

Using the Security Information Center

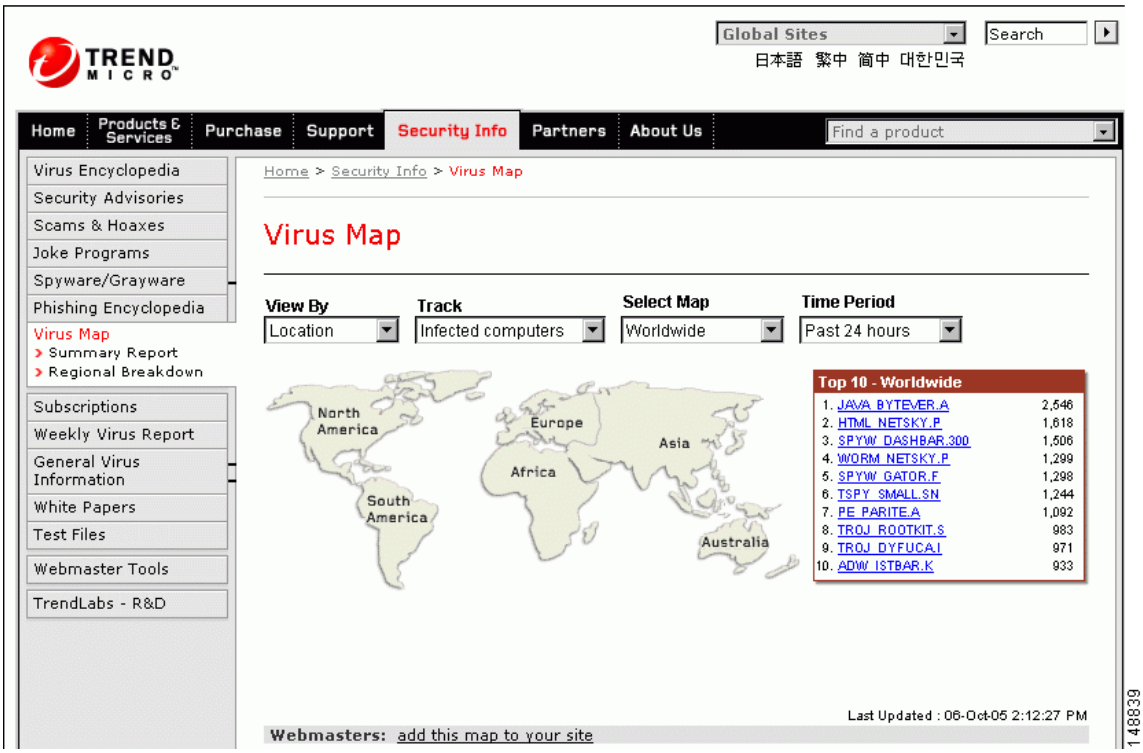
Comprehensive security information is available from the Trend Micro Security Information Center, a free online resource, at the following URL:

http://trendmicro.com/vinfo/

The Security Information Center provides the following information:

- Virus Encyclopedia—A compilation of knowledge about all known threats, including viruses, worms, Trojans, and others
- Security Advisories—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 and Grayware—Information about the top ten spyware and grayware programs, and a searchable database of these 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, shown in Figure 8-4

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 receive a copy automatically each week via e-mail.)
- General virus information, including the following:
  - 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 or grayware 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 System Log Messages

This section lists the CSC SSM-related system log messages, and includes the following topics:

- SSM Application Mismatch [1-105048], page 8-18
- Data Channel Communication Failure [3-323006], page 8-18
- Drop ASDP Packet with Invalid Encapsulation [3-421003], page 8-19

- Daily Node Count [5-421006], page 8-19
- Data Channel Communication OK [5-505010], page 8-19
- New Application Detected [5-505011], page 8-19
- Application Stopped [5-505012], page 8-20
- Application Version Changes [5-505013], page 8-20
- Traffic Dropped Because of CSC Card Failure [6-421007], page 8-21
- Account Host Toward License Limit [6-421005], page 8-21
- Skip Non-applicable Traffic [6-421002], page 8-21
- Failed to Inject Packet [7-421004], page 8-22
- Connection capacity has been reached, page 8-22
- Connection capacity has been restored, page 8-22
- Failover service communication failed, page 8-24
- Failover service email could not be sent, page 8-24
- Failover service communication failed, page 8-24
- HTTP URL blocking event, page 8-25
- Scan service failed, page 8-27
- License upgrade notice, page 8-26
- Resource availability of the CSC SSM falls below the desired level, page 8-26
- Resource availability of the CSC SSM has been restored, page 8-27
- Scan service failed, page 8-27
- Scan service recovered, page 8-28
- Scheduled update report, page 8-28
- Service module cannot create FIFO, page 8-28
- Service module encountered a problem when communicating with the ASA chassis, page 8-29
- Service module informational report, page 8-29
- Service module internal communication error, page 8-30
- Service module internal communication error, page 8-30
- Service module informational report, page 8-29
- Spyware/Grayware detection event, page 8-31
- System monitor started, page 8-32
- System monitor started, page 8-32
- Time synchronization with the ASA chassis failed, page 8-32
- Virus detection event, page 8-32

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 reenable failover.

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. The failure triggers a failover when it occurs on the active adaptive security 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. The message is generated whenever a communication problem occurs over the adaptive security appliance dataplane between the system module and the 4GE SSM. This communication problem 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 system log message 5-505010 does not appear after the 4GE SSM returns to an UP state, reset the module using the **hw-module module 1 reset** command.

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 one message every ten seconds.

- *interface_name*—The interface name
- *IP_address*—The IP address
- *port*—The port number
- *application*—The CSC SSM application supported in the current release

Recommended Action Immediately investigate the problem with 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 the ADSP protocol. Any packet that does not have the correct 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.

Daily Node Count [5-421006]

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

Explanation This system log message 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 If the overall count exceeds the user license you have purchased, contact Cisco to upgrade your license.

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 If this message was generated as a result of a previous data channel communication failure (system log message 3-323006), check the 4GE SSM system log messages to determine the cause of the communication failure.

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 adaptive security appliance 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 None required.

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 in 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.

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 The connection bypassed the 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 one message every ten 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 application supported in the current release

Recommended Action The configuration should be modified to only include protocols that are supported by the service module.

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 application supported in the current release

Recommended Action 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 one message every ten 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 application supported in the current release

Recommended Action Immediately investigate the problem with the service module.

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 adaptive security appliance has failed to inject a packet, as instructed by the service module. This could happen if the adaptive security appliance tries to inject a packet into a flow that has already been released or because the adaptive security appliance maintains its connection table independent of the service module.

- *IP_address*—The IP address
- *port*—The port number

Recommended Action If this affects adaptive security appliance performance, contact Cisco TAC.

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

- *protocol*—The protocol involved

Recommended Action Configure the adaptive security appliance to bypass certain traffic from CSC SSM scanning or segment the network to another adaptive security appliance.

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

- *protocol*—The protocol involved

Recommended Action None 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 system log message is generated when a socket timeout is experienced when the 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 None 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 system log 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 or pattern, the status is set to RELOAD and the adaptive security appliance will perform a 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. The adaptive security appliance will perform a fail-open, fail-close, or fail-over according to how it has been configured.

- *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.

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 system log 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 adaptive security 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 system log message is generated when the automatic "heartbeat failure" notification e-mailed 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.

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 system log 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.

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 system log 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 None required.

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 system log 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 Adjust the URL filtering setting if you want this URL category to be allowed.

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 system log 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 message, a notification e-mail 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*—The daily count minus the number of seats

Recommended Action Contact Cisco for a license upgrade.

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 system log 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 system log message is generated when the 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 None required.

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 system log 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 the 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 system log message is generated when a scan service recovers from a previous failure.

- *service_title*—The name of the service

Recommended Action None 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 system log 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.

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 system log 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 the CSC subsystem

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

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 system log message is generated when the Service Module fails to communicate with the adaptive security appliance chassis.

- *process_id*—Process ID

Recommended Action None required.

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 6.1.1519.0
```

Explanation This system log message displays the CSC application name, version, and running state during Service Module startup.

- *process_id*—Process ID of the daemon
- *text*—Description of name or version
- *up/dow*n—Service is up or down

Recommended Action None required.

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

- *process_id*—Process ID of the service module
- *ipc_operation*—Interprocess communication (IPC) operation

Recommended Action None 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 6.1.1519.0
```

Explanation This system log 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 None required.

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

Explanation This system log 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 e-mail
- *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 e-mail

Recommended Action If the spam mail is generated from a similar source, you may add this source to the Blocked Sender list to reduce the e-mail volume.

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

Explanation This system log 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.

- *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 e-mail.
- *action_on_the_content*—Action taken on the e-mail content.
- *action_on_the_email*—Action taken on the whole e-mail.

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

Syslog adaptor starting

Error Message `is-syslog: ISSyslog Adaptor 1.0`

Example:

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

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

Recommended Action None required.

System monitor started

Error Message `SysMonitor: INFO: SysMonitor started.`

Example:

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

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

Recommended Action None 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 system log message is generated when the Service Module is unable to synchronize the SSM system time with the adaptive security appliance system time.

- *process_id*—Process ID of the service module

Recommended Action None required.

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-mail-virus: 2006/01/01 16:33:01|
WORM_GREW.A|Virus|fromtester@trendmicro.com|totester@trendmicro.com|subject|Delete|Deliver
|
```

Explanation This system log 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 e-mail
- *action_on_the_content*—Action taken on the e-mail content
- *action_on_the_email*—Action taken on the whole e-mail

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

Before Contacting Cisco TAC

Before you contact the Cisco Technical Assistance Center (TAC), check the documentation and online help to see whether it contains the information you need. If you have checked the documentation and the Knowledge Base and still need help, be prepared to give the following information to Cisco TAC:

- 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

APPENDIX A

Reimaging and Configuring the CSC SSM Using the CLI

This appendix describes how to reimage and configure the CSC SSM using the CLI, and includes the following sections:

- Installation Checklist, page A-1
- Preparing to Reimage the Cisco CSC SSM, page A-2
- Reimaging the CSC SSM, page A-4
- Resetting the Configuration via the CLI, page A-17

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

Note If installation is required, the Setup Wizard launched from the ASDM is the preferred method of installation. For more information, see *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Installation Checklist

Before you start, be prepared to supply the following information during installation, shown in Table A-1. If you prefer, you can print a copy of this table and use it as a checklist, to record the values you enter.

Table A-1 Installation Checklist

Information Requested	Information Entered	Completed
Administrator password for the CLI	Do not record your password.	—
SSM card IP address		❑
Subnet mask		❑
Hostname (1 to 63 alphanumeric characters; can include hyphens, except as the first character). For example: cisco1-ssm-csc		❑
Domain name		❑

Table A-1 Installation Checklist (continued)

Information Requested	Information Entered	Completed
Primary DNS IP address		❑
Secondary DNS IP address (optional)		❑
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 e-mail address		❑
Notification e-mail server IP		❑
Notification e-mail 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 CSC SSM with the security appliance. Before you begin, make sure that the date and time settings on the adaptive security appliance are correct.

To prepare for reimaging, 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 adaptive security appliance console by entering the following command:

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

The system response is similar to the following example:

```
Image URL tftp://insidehost/CSCSSM-6.1.1519.0.img]:tftp://insidehost/CSCSSM-6.1.1519.0.img
Port IP Address [000.000.0.00]:
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
```

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=CSCSSM-6.1.1519.0.img
Slot-1 211>   CONFIG=
Slot-1 212> tftp CSCSSM-6.1.1519.0.img@192.168.7.100
Slot-1 213> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 214> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
```

Note This process takes about ten 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...
```

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 5 Disable the **debug-module boot** command.

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

Step 6 Show module 1 details.

Sample code output follows:

```
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 6.1.1519.0
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:       CSC SSM 6.1.1519.0
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 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

This section describes how to reimage the CSC SSM, and includes the following topics:

- Confirming the Installation, page A-7
- Viewing or Modifying Network Settings, page A-8
- Viewing Date and Time Settings, page A-9
- Viewing Product Information, page A-9
- Viewing or Modifying Service Status, page A-9
- Using Password Management, page A-10
- Restoring Factory Default Settings, page A-12
- Troubleshooting Tools, page A-12
- Resetting the Management Port Access Control, page A-16
- Pinging an IP Address, page A-17
- Exiting the Setup Wizard, page A-17

To reimage the CSC SSM using the CLI Setup Wizard, perform the following steps:

Step 1 Log in to the adaptive security appliance using the administrator username and password.

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
------------------------------------------------------------------------------
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. Notification settings
    5. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

Step 2 Enter **1** to configure network settings.

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]
```

Step 3 Respond to the network settings prompts, using values from the installation checklist. When you are finished with the last network settings prompt, your entries appear for visual verification. For example:

```
Network Settings
------------------------------------------------------------------------------
IP              000.000.0.00
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     example.com

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         000.000.0.0
No Proxy

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

Step 4 If the settings are correct, retype **y** to confirm. (If you choose **n**, the Network Settings prompts reappear; repeat Step 2.)

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

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

Step 5 (Optional) Confirm the network settings by pinging the gateway IP address. To skip pinging, choose **n**.

```
Do you want to confirm the network settings using ping? [y|n] y
Enter an IP address to ping: 000.000.0.0
PING 000.000.0.0 (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 ...
```

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
```

Step 6 Enter **y** to set the date and time to synchronize with the chassis. Enter **n** to update the date and time, exit the Setup Wizard, update the date and time or NTP settings on the ASA chassis, and reinstall the SSM.

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
```

Step 7 Enter your highest level domain name for your organization and then **y** to continue.

The Administrator/Notification Settings prompts appear.

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

Administrator email address:
Notification email server IP:
Notification email server port: (default:25)
```

Step 8 Enter the correct value for each setting.

A confirmation message 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
```

Step 9 Enter **y** to continue.

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.
```

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 informs you that installation is complete.

Step 10 Use your browser to log on to the CSC SSM console by entering 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 To view information about the CSC SSM and the services you configured during installation, enter the following command:

```
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 6.1.1519.0
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:       6.1.1519.0
```

```
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 To start a command session, enter the following command:

```
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. Password Management
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]:
```

Viewing or Modifying Network Settings

To view or modify network settings, enter **1**.

The Network Settings prompts appear.

```
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
```

Viewing Date and Time Settings

To view the date and time settings, enter **2**.

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 ...
```

Note You cannot change these settings; this information is for reference only.

Viewing Product Information

To view the product version and build numbers, enter **3**.

The Product Information prompts appear:

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

Trend Micro InterScan for Cisco CSC SSM 6.1.1542.0

Press Enter to continue ...
```

Note You cannot change these settings; this information is for reference only.

Viewing or Modifying Service Status

To view or modify service status, perform the following steps:

Step 1 Enter **4**.

The Service Status prompts appear.

```
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
```

Step 2 Enter **y** to restart scanning services. Enter **n** if everything is running smoothly.

Note If you are trying to troubleshoot a problem, restarting may return the SSM to a proper operating status. For more information about the effects of restarting services, see the "Restart Scanning Service" section on page 8-12.

Using Password Management

This section describes how to manage passwords, and includes the following topics:

- Changing the Current Password
- Modifying the Password-reset Policy

To use Password Management, enter **5**.

The following prompt appears:

```
Enter a number from [1-10]: 5

                        Password Management
------------------------------------------------------------------------

1. Change Password
2. Modify Password-reset Policy
3. Return to Main Menu

Enter a number from [1-3]: 1
```

Changing the Current Password

To change the password, perform the following steps:

Step 1 Access the Change Password command, as shown in the previous procedure.

The following screen appears.

```
                           Change Password
------------------------------------------------------------------------

This option allows you to change the password for the CSC SSM that
you are currently using.
```

Step 2 Type **y** and press **Enter**.

```
Do you want to continue? [y|n] y
```

Step 3 Type the old password and press **Enter**.

```
The password will be hidden while you type.
Press Enter to return to last menu.
Enter old password:
```

Step 4 Type the new password and press **Enter**. Then retype the new password and press **Enter** to confirm it.

```
Enter new password (minimum of 5, maximum of 32 characters)
Enter new password:
Re-enter new password:
Please wait ...
The password has been changed.
```

Modifying the Password-reset Policy

You can modify the password-reset policy to "Allowed" or "Denied."

- "Allowed" means you can reset the CSC SSM password through the ASDM without verifying the old password. Under this setting, you can reset the password, even if the current password has been lost.
- "Denied" means you cannot reset the CSC SSM password through the ASDM without reimaging and reactivating the CSC SSM. However, you can still change the password to the CSC SSM if you know the current password.

Caution Setting the password-reset policy to "Allowed" compromises the security of the application.

To modify the password-reset policy, perform the following steps:

Step 1 From the Password Management menu, enter **2**. For access details, see Using Password Management, page A-10.

The following screen appears.

```
                  Modify Password-reset Policy
------------------------------------------------------------------------

Current CSC SSM password-reset policy: Allowed

"Allowed" allows the Adaptive Security Device Manager (ASDM)
to reset the CSC SSM password without verifying the old password.

"Denied" does not allow the ASDM to reset the CSC SSM password
without re-imaging and re-activating the CSC SSM.
```

Step 2 Type **y** and press **Enter** to change the password-reset policy, as shown in the following example:

```
Do you want to modify the CSC SSM password-reset policy now? [y|n] y
```

The following confirmation appears:

```
Updated CSC SSM password-reset policy: Denied
```

Restoring Factory Default Settings

To restore factory default configuration settings, enter **6**.

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 enter **y**, all your configuration settings are returned to the preinstallation default settings. For a description of the 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. Additional configuration changes you have made since installation, such as registration or activation, licensing, enabling spyware or grayware detection, file blocking, file blocking exceptions, and other settings are lost.

Although this option is available from the CLI, a better alternative for restoring configuration settings is available from the CSC SSM console. Choose **Administration > Configuration Backup** to view the Configuration Backup window, which allows you to export your configuration settings to a configuration file that you can import at a later time.

Note Choose the **Restore Factory Default Settings** option only if you must reinstall the CSC SSM.

Troubleshooting Tools

This section describes the troubleshooting tools, and includes the following topics:

- Enabling Root Account, page A-13
- Showing System Information, page A-13
- Collecting Logs, page A-15
- Enabling Packet Tracing, page A-15
- Modifying Upload Settings, page A-16

Enter **7** to display a menu of troubleshooting tools. These tools are available to help you or Cisco TAC obtain information to troubleshoot a problem.

```
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]:
```

Enabling Root Account

To enable root account access, perform the following steps:

Step 1 Enter **1**.

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]
```

Step 2 Enter **y** to enable the root account.

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

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.

Showing System Information

This section describes how to show system information, and includes the following topics:

- Showing System Information on Screen, page A-13
- Uploading System Information, page A-14

To view system information directly on the screen, enter **2**. Alternatively, you can save the data to a file and transfer the information using FTP or TFTP. The Troubleshooting Tools - Show System Information menu appears.

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

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

Showing System Information on Screen

To show system information on screen, perform the following steps:

Step 1 Enter **1** from the Troubleshooting Tools - Show System Information menu. System information is available from various locations on the ASDM and CSC SSM interfaces; however, this CLI makes the information available in one place, as shown in the following example:

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

System is : Up

# Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.01.1519.0
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)
Grayware 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:Standard
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:Standard
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
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.

Step 2 Enter **q** to quit.

Uploading System Information

To upload system information, perform the following steps:

Step 1 From the Troubleshooting Tools - Show System Information menu, enter **2**.

The following prompts appear:

```
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 ...
```

Step 2 Respond to these prompts to upload the system information. The system information is sent using the upload settings created by entering **5**, Modify Upload Settings. For more information, see Modifying Upload Settings, page A-16.

If you did not configure the upload settings, the following prompts precede those appearing in the previous step:

```
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
```

Step 3 When you are finished, enter **3** from the Show System Information menu.

Collecting Logs

To collect all logs, perform the following steps:

Step 1 To collect all logs on the CSC SSM, enter **3**. Send them via FTP or TFTP, for example, to Cisco TAC. The logs are sent using the upload settings created by entering **5**, Modify Upload Settings. For more information, see Modifying Upload Settings, page A-16.

```
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
```

Step 2 Enter **y** to gather logs.

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

Enabling Packet Tracing

To enable packet tracing between the CSC SSM and adaptive security appliance, perform the following steps:

Step 1 Enter **4**. Cisco TAC usually needs this information.

The following prompts appear:

```
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 ...
```

Step 2 Enter **y** to gather packet traces.

Step 3 Press **Control-C** to stop.

Step 4 Enter **y** to upload packet traces.

The packets are uploaded using the protocol defined by entering **5**, Modify Upload Settings. For more information, see Modifying Upload Settings, page A-16.

Modifying Upload Settings

To modify upload settings, perform the following steps:

Step 1 To set the uploading method to either FTP or TFTP, enter **5**.

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

When you enter **5**, the following prompts appear:

```
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 ...
```

Step 2 Respond to the prompts to configure the upload settings. The settings are saved for future use.

Step 3 When you are finished, enter **6**, Return to Main menu.

Resetting the Management Port Access Control

To reset the management port access control, enter **8.**

The following appears:

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

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

Pinging an IP Address

To ping an IP address, perform the following steps:

Step 1 Enter **9**. The ping option is available for diagnostic purposes.

The following appears:

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

Step 2 Enter an 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 ...
```

Exiting the Setup Wizard

To exit the Setup Wizard, perform the following steps:

Step 1 To exit the Setup Wizard, enter **10**.

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#
```

Step 2 From the Exit Options menu, choose **1** to log out, **2** to reboot the system, or **3** to return to the Setup menu.

Resetting the Configuration via the CLI

This section describes some alternatives that are available for users who want to use the CLI instead of the CSC SSM console. Not all features have an available alternative.

After you have installed Trend Micro InterScan for Cisco CSC SSM, if you have used TFTP to reimage the SSM, the following prompt may appear for the first time when you access the CLI:

```
Do you want to restore the previous configuration? [y|n] n

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. Notification settings
5. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

Enter **y** to restore the SSM configuration settings to the state they were in the last time you saved the configuration. This is a CLI alternative to the functionality available on the Administration > Configuration Backup window on the CSC SSM console.

APPENDIX B

Using CSC SSM with Trend Micro Control Manager

This appendix describes how to manage Trend Micro InterScan for CSC SSM from Trend Micro Control Manager (TMCM), and includes the following sections:

- About Control Manager, page B-1
- Control Manager Interface, page B-2

About Control Manager

You should have already installed the TMCM agent and registered CSC SSM with TMCM using the CSC SSM Administration > Register to TMCM window. TMCM is a central management console that allows you to manage multiple Trend Micro products and services from a single console. Control Manager allows you to monitor and report on activities such as infections, security violations, or virus entry points.

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

With TMCM, you can download and deploy updated components throughout the network, to ensure that protection is consistent and up-to-date. Examples of updated components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and scheduled updates.

Control Manager provides the following:

- 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

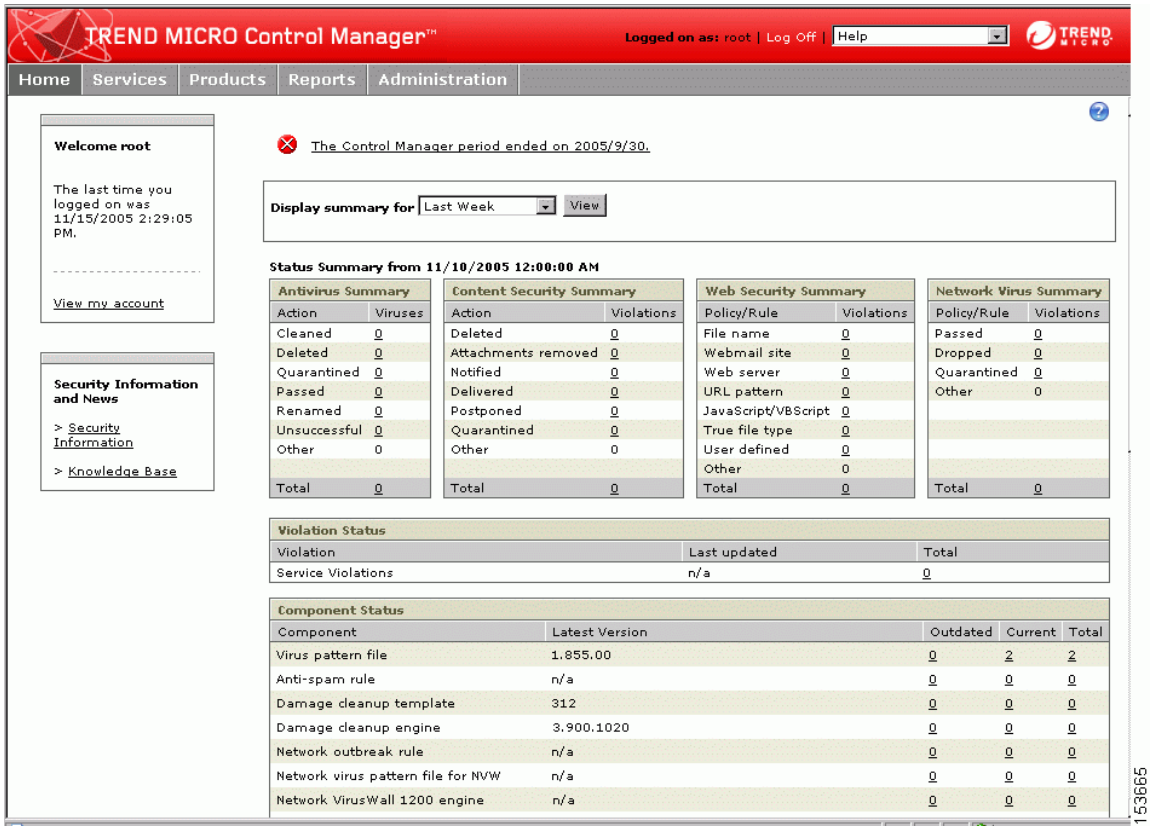
Control Manager Interface

This section describes the Control Manager interface, and includes the following topics:

- Using the Management Console, page B-2
- Opening the Control Manager Console, page B-3
- Downloading and Deploying New Components, page B-4

Trend Micro Control Manager uses a management console to administer managed products. When you log in to TMCM, the Home window appears, as shown in Figure B-1.

Figure B-1 The Control Manager Management Console Home Window.



Using the Management Console

The management console consists of the following elements:

- The title bar drop-down menu, which provides links to the Control Manager online help, the Trend Micro Knowledge Base, Trend Micro Security Information, and the About screen for Control Manager.
- Below the title bar drop-down menu, the main menu provides links to the Home, Services, Products, Reports, and Administration windows, which you use to administer TMCM and managed products.

- 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 item selected.
- The Product Directory tabs, parent server, or child server tabs.
- A working are 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 items, choose **Products** from the main menu to include managed product or child server tabs in the working area.

Opening the Control Manager Console

This section describes how to access the Control Manager console, and includes the following topics:

- Accessing the HTTPS Management Console, page B-3
- About the Product Directory, page B-4

You can access the Control Manager console locally from the Control Manager server, and remotely through a web browser from any connected computer.

To open the TMCM console from a remote computer:

Step 1 To open the Log-on screen, in the browser address field, enter the following:

http://{*hostname***}/ControlManager**

Where *hostname* is the fully qualified domain name (FQDN) for the Control Manager server, IP address, or server name. The TMCM Log-on screen appears.

Step 2 Enter a TMCM username 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.

The initial screen shows the status summary for the entire Control Manager system, which is the same as the status summary generated from the Product Directory. User privileges determine the Control Manager functions you can access.

Accessing the HTTPS Management Console

You can encrypt the configuration data as it passes from the Web-based console to the Control Manager server. You must first assign Web access to Control Manager and then alter the management console URL to use HTTPS through port 443. For details about how to set up HTTPS access, see the TMCM documentation.

To open the TMCM console using HTTPS:

Enter the URL for encrypted communication (HTTPS) in the following format:

https://{*hostname***}:443/ControlManager**

Where *hostname* is the fully qualified domain name (FQDN) for the Control Manager server, IP address, or server name. The port number allotted to an HTTPS session is 443.

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 Product Directory

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

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

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 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.

Downloading and Deploying New Components

This section describes downloading and deploying new components, and includes the following topics:

- Deploying New Components from the TMCM Product Directory, page B-5
- Viewing Managed Products Status Summaries, page B-5
- Configuring CSC SSM Products, page B-6
- Issuing Tasks to the CSC SSM, page B-6
- Querying and Viewing Managed Product Logs, page B-7

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 from the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and vulnerability assessment pattern downloads, although there is no managed product registered on the Control Manager server.

Following are the components to update, listed according to the frequency of recommended updates:

- Pattern files and 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 refer to the virus scan engine, damage cleanup engine, and VirusWall engine for Linux.
- Product program refers to product-specific components (for example, Product Upgrades).

Note Only registered users are eligible for component updates. For more information, see the online help topic, “Registering and Activating Your Software > Understanding product activation.”

Deploying 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, which is particularly useful during virus outbreaks. Download new components before deploying updates to a specific group or groups of managed products.

To manually deploy new components using the Product Directory, perform the following steps:

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

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

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

Step 4 Click the **Tasks** tab.

Step 5 From the Select task list, choose **Deploy *component_name*** 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.

Viewing 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.

You can view the managed products status summary from the Home screen or the Product Directory.

To access managed products through the Home window, open the Control Manager management console.

The Status Summary tab of the Home screen shows a summary of the entire Control Manager system. This summary is identical to the summary provided in the Product Status tab in the Product Directory Root folder.

To access managed products through the Product Directory, perform the following steps:

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 summary.
- If you click the Root folder, New entity, or another user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries.

Note By default, the Status Summary tab displays a complete week of information, ending with the day of the query. In the Display Summary list, you can change the scope to Today, Last Week, Last Two Weeks, or Last month available.

Configuring 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 configuring a group, verify that you want all managed products 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 Web console or a Control Manager-generated console.

To configure a product, perform the following steps:

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

Step 2 On the left-hand 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 Click the **Configuration** tab.

Step 5 From the Select product list, choose the product to configure.

Step 6 In the Select configuration list, choose the product feature to access or configure.

Step 7 Click **Next**.

The web-based console or Control Manager-generated console appears.

Issuing Tasks to the CSC SSM

Use the Tasks tab to make certain tasks available for 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 or cleanup templates.
- Deploy program files.
- Enable or disable Real-time Scan.
- Start Scan Now.

You can deploy the latest spam rules, patterns, or scan engine to managed products with outdated components.

Note The Control Manager server has already been updated with the latest components from the Trend Micro ActiveUpdate server.

You can perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to managed products perform the following steps:

Step 1 From the TMCM console, go to the Product Directory.

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

Step 3 Click the **Tasks** tab.

Step 4 Choose the task from the Select task list.

Step 5 Click **Next.**

Step 6 Monitor the progress through Command Tracking.

Step 7 To view command information, click the **Command Details** link at the response screen.

Querying and Viewing 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, perform the following steps:

Step 1 From the TMCM console, go to the Product Directory.

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

Step 3 Click the **Logs** tab.

Step 4 Choose the client log type.

The Query Result screen displays the results in a table.

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

For additional information and instructions about using Trend Micro Control Manager, see the online help and PDF file documentation.

GLOSSARY

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 The operation to be performed when the following has occurred:
- A virus or other threat has been detected.
- File blocking has been triggered.

Actions usually include clean, delete, or pass (deliver or transfer anyway). Delivering or transferring anyway is not recommended; delivering a risk-infected message can compromise your network.

See also notification.

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. An example of an activation code is: 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 or 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 that runs automatically when the page is viewed. ActiveX controls allow web developers to create interactive, dynamic web pages with broad functionality, such as HouseCall, the Trend Micro free online scanner.

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

address Refers to a networking address or an e-mail address, which is the string of characters that specifies the source or destination of an e-mail message.

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

administrator account A username and password that has administrator-level privileges.

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

ADSP AppleTalk Data Stream Protocol, part of the AppleTalk protocol suite, which provides a TCP-style reliable connection-oriented transport. This protocol is full duplex.

adware Advertising-supported software in which advertising banners display while the program is running. Adware that installs a "backdoor" tracking mechanism on a computer without user 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.

audio or 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 username 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.

See also public-key encryption and digital signature.

B

binary A numerical representation consisting of zeros and ones used by most 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, certain viruses 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 that allows a person to read hypertext, such as Internet Explorer or Mozilla Firefox. The browser provides a way to view the contents of nodes (or "pages") and to move from one node to another. A browser acts as a client to a remote web server.

C

cache A small, yet fast portion of memory, holding recently accessed data, which is 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.

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. For more information, see Reimaging and Configuring the CSC SSM Using the CLI, page A-1.

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 responses. A client is part of a client-server software architecture.

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

compressed file A single file containing one or more separate files and 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 e-mail message.

content filtering Scanning e-mail messages for content (words or phrases) prohibited by 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 certain 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 a system to a pay-per-call location in which the unsuspecting user is unknowingly billed for the call.

digital signature Extra data appended to a message that identifies and authenticates the sender and message data using a technique called public-key encryption.

See also public-key encryption and authentication.

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

DNS Domain Name System. A general-purpose data query service used on the Internet to translate hostnames into IP addresses.

DNS resolution When a DNS client requests hostname 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 hostname 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 DNS.

Denial of Service (DoS) attack Group-addressed e-mail messages with large attachments that clog your network resources to the point that 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, which are files that have the these extensions. Unless they have overwritten or inadvertently destroyed part of the original program code, most DOS viruses try to replicate and spread by infecting other host programs.

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

E

ELF Executable and Linkable Format, a file format for UNIX and Linux platforms.

encryption 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 only by the person who created it has. With this method, anyone may send a message encrypted with the 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 common public-key encryption schemes.

end user license agreement (EULA) A legal contract between a software publisher and the software user, which outlines user restrictions.

Many users inadvertently agree to the installation of spyware and adware on their computers when they the EULA that appears during the installation of certain free software.

executable file A binary file containing a program in machine language that is ready to be executed.

EXE file infector An executable program with an .exe file extension.

See also DOS virus.

exploit Code that takes advantage of a software vulnerability or security hole. Exploits can propagate and run intricate routines on vulnerable computers.

F

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

file infecting virus File-infecting viruses infect executable programs (files that have extensions of .com or .exe). Most viruses 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. Some viruses are very destructive and try to format the hard drive at a predetermined time or perform other malicious actions.

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

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, message body, or attachment subject
- File type of the attachment

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

FTP A client-server protocol that 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; however, 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. The five group file types in the Trend Micro InterScan for Cisco CSS SSM interface are as follows:
- Audio/Video
- Compressed
- Executable
- Images
- Microsoft Office

GUI Graphical User Interface. The use of pictures rather than words alone to represent the input and output of a program.

H

hacker See virus writer.

hacking tool Tools such as hardware and software that enable penetration testing of a computer system or network to find 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, the authoring language used to create information that appears on a web page. The virus resides in a web page and downloads through a browser.

HTTP Hypertext Transfer Protocol. The client-server TCP/IP protocol used on the web through port 80 to render HTML documents.

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 central authority for research, intelligence, and certification testing of products for the security industry. 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, that is, a picture. Images are taken from the real world, for example, via a digital camera or by a computer using graphics software.

incoming E-mail 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, for university and many other research networks. The web is the most familiar aspect of the Internet.

in the wild Describes known viruses that are currently controlled by antivirus products.

in the zoo Describes known viruses that are actively circulating.

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

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

IP Internet Protocol.

IT Information technology, which includes 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 on the web. 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—often by 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-enabled browser to view a page that contains an applet, the applet code is transferred to your system and is executed by the Java Virtual Machine in the browser.

Java malicious code Virus code written or embedded in Java.

See also Java file.

JavaScript virus JavaScript is a 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 targets these scripts in the HTML code, which enables the virus to reside in web pages and download to a desktop computer through the browser.

See also VBscript virus.

K

keylogger Keyloggers are programs that catch and store all keyboard activity. Legitimate keylogging programs 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 log-on credentials and credit card numbers.

L

link (also called hyperlink) A reference from one point in one hypertext document to another 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 it with a mouse, the browser displays the target of the link.

listening port A port used in client connection requests for data exchange.

load balancing Mapping or remapping of work to processors to improve 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 usually 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 are not specific to an operating system and can spread via e-mail attachments, web downloads, file transfers, and cooperative applications.

malware (malicious software) Programming or files that are developed to do 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.

message An e-mail message, which includes the message subject in the message header and the message body.

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 that allows organizations to use unregistered IP network numbers internally and still communicate with the Internet. Use this device 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 e-mail 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 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 Services is a method of spam filtering that allows you to off-load the task from the MTA to the CSC 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.

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.

P

password cracker An 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. This file is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. The file is most effective when used with the latest scan engine.

payload An action that a virus performs on the infected computer, which can be relatively harmless, such as displaying messages or ejecting the CD drive, or 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 website.

ping A diagnostic tool used on TCP/IP networks that allows you to verify whether a connection from one host to another is working. For more information, see Pinging an IP Address, page A-17.

polymorphic virus A virus that can take different forms.

POP3 Post Office Protocol, 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 that hosts POP3 e-mail, from which clients in your network retrieve POP3 messages.

proxy A service that provides a cache of items available on other servers that are slower or more expensive to access.

proxy server A web server that accepts URLs with a special prefix, which is used to retrieve 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 public key is published, while the private key is kept secret. Messages are encrypted using the recipient public key and can only be decrypted using the private key.

See also authentication and digital signature.

R

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 system security.

replicate To self-reproduce. 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 use to debug or to boot the system manually.

rule-based spam detection Spam detection based on heuristic evaluation of message characteristics to determine whether an e-mail message should be considered spam. When the anti-spam engine examines an e-mail message, the engine searches for matches between the mail content 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.

See also signature-based spam detection and false positive.

S

scan engine The module that performs antivirus scanning and detection in the host product into which it is integrated.

seat A license for a single user 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.

setup wizard The setup program used to install Trend Micro InterScan for Cisco CSC SSM, which can be one of the following:

- A GUI setup wizard, launched from the ASDM. For more information, see the ASDM online help.
- A CLI. For more information, see Reimaging and Configuring the CSC SSM Using the CLI, page A-1.

signature-based spam detection A method of determining whether an e-mail message is spam by comparing the message content 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 is not an exact match for text in the spam signature file.

See also rule-based spam detection and false positive.

SMTP Simple Mail Transfer Protocol, a protocol used to transfer electronic mail between computers, usually over Ethernet. SMTP is a server-to-server protocol; as a result, other protocols are used to access the messages.

SOCKS4 A protocol that relays TCP sessions to a firewall host to allow transparent access across the firewall to application users.

spam Unsolicited e-mail messages to promote a product or service.

SSL Secure Sockets Layer, a secure communications protocol on the Internet.

spyware Advertising-supported software that usually installs tracking software on a system, capable of sending information about the system to another party. The danger is that users cannot control the data being collected, or how it is used.

stamp To place an identifier, such as "Spam," in the subject field of an e-mail message.

status bar A feature of the user interface that displays the status or progress of a particular activity, such as loading files on a machine.

T

TAC Technical Assistance Center, a support service that Cisco provides to users of Cisco products.

TCP/IP Transmission Control Protocol/Internet Protocol, a networking protocol commonly used in combination with the 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. 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 the top-level domain "uk" (for United Kingdom).

trigger An event that causes an action to take place. For example, Trend Micro InterScan for Cisco CSC SSM detects a virus in an e-mail message, which 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. 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, because the messages are from a known and trusted source.

trusted host A server that is allowed to relay mail through a network because they are trusted to act appropriately and not, for example, relay spam through a network.

U

UDP A protocol in the TCP/IP protocol suite, the User Datagram Protocol allows an application to send datagrams to other applications on a remote machine. UDP is a protocol that provides an unreliable and connectionless datagram service, in which delivery and duplicate detection are not guaranteed. This protocol does not use acknowledgments, or control the order of arrival.

URL Uniform Resource Locator, a standard way of specifying the location of an object, usually a web page, on the Internet, for example, www.cisco.com. The URL maps to an IP address using DNS.

V

VBscript virus Microsoft Visual Basic scripting language is a programming language that allows web developers to add interactive functionality to HTML pages displayed in a browser.

A VBscript virus targets these scripts in the HTML code, which enables the virus to reside in web pages and download to a desktop through the browser.

See also JavaScript virus.

virus 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 a 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 a computer.

virus kit A template of source code for building and executing a virus, available from the Internet.

virus signature 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 e-mail 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 the defined 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 website that distributes 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 character.

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 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 a network.

INDEX

A

activation 6-9, A-6
  status A-7
Activation Code 6-7, 6-9, A-7
ActiveUpdate 2-6
  proxy settings 5-3
  server 8-8
administrator
  email address 6-2
  maximum notifications/hour 6-2
  notifications A-6
  password 8-4, A-4
approved senders 3-7

B

Base License 1-1, 1-11, A-6
blocked senders 3-7

C

Cisco ASDM/Trend Micro GUI access 2-6
Cisco TAC
  contacting 8-33
clock setup 2-1
collecting logs A-15
command line interface
  installing via A-1
components
  manual update 5-2
  scheduled update 5-2
  updating 5-1
  view version and build A-9
component status 2-4
compressed file handling 3-2, 4-2
configuration
  backup 6-3
  export 6-4
  import 6-4
  reset via CLI A-17
confirming the installation A-7
connection settings 6-1
content filtering 3-7
  enabling 3-8, 3-9

D

date/time settings A-6
  view A-9
default mail scanning settings 3-1
defaults
  restore factory A-12
default values 1-8
default Web and FTP scanning settings 4-1
device
  reimaging A-1
disclaimer 3-6
displaying system information A-13
DNS lookup 2-6
documentation 1-3

E

EICAR test virus 2-3
email notifications 3-4

Exiting the Setup Wizard A-17

F

failover 6-5
checklist 6-5
notification when peer is down 6-6
synchronize with peer 6-6
false positive
troubleshooting 8-9
features and benefits of Trend Micro for Cisco CSC SSM 1-2
file blocking 4-4
by file name extension 4-5
by group type 4-4

G

glossary 1-4
grayware
defined 4-3
definition 3-3
detecting 3-3

H

HyperTerminal A-2

I

incoming/outgoing SMTP mail 3-2
incoming domain A-6
incoming mail domain 3-6
inline notifications 3-4
installation
confirmation A-7
handling failure at stages of 8-3
steps 8-1
IP address
pinging A-17

J

Joke Programs 8-15

K

Knowledge Base 1-4, 8-15

L

large file handling 4-2
large files 4-2, 8-11
license
activating the product 6-9
informational links 6-9
renewing the license 6-9
license expiration date 6-7
license feature table 1-12
local list 4-6
logging in without going through ASDM 8-13
logs 5-4
collecting A-15

M

management console
default view 8-14
timeout 8-13
management port 2-6
access control A-16
manual update 5-2
message filter 3-1
message filtering 3-6
message size 3-8

N

navigation panel 1-7
network settings A-5
  view or modify A-8
notifications
  content-filtering violations 3-8
  file blocking 4-5
  for SMTP/POP3 events 3-3
  modifying 3-4
  types of 3-4
  using tokens in 3-4

O

online help 1-9
  contents 1-10
  context-sensitive 1-3
  general help 1-3
  index 1-10
  links in 1-11
  popup blocking 1-11
  search feature 1-10

P

packet capture 8-6
packet traces
  collecting A-15
password A-4
  change A-10
  recovery 8-4
  reset A-10
Password-reset policy
  modify A-11
pattern file
  troubleshooting 8-8
phishing
  example of 4-6
Phishing Encyclopedia 8-15
PhishTrap 4-7
ping IP A-16
Plus License 1-2, 1-11, A-7
popup blocking 1-11
product upgrade 6-6
proxy settings for ActiveUpdate 5-3

R

reimaging
  CSC SSM A-1
reimaging or recovery of CSC module 8-7
risk ratings 8-16
root account A-13

S

Safe Computing Guide 8-16
Save button 1-8
Scams and Hoaxes 8-15
Scan by specified file extensions 4-2
scanning
  testing with EICAR 2-3
  verify it is operating 2-2
scheduled update 5-2
seats 6-7
Security Information Center 8-15
service status
  restart A-9
  view A-9
  view or modify A-9
setup wizard 1-2
  exiting A-17
SOCKS4 5-3
spam
  troubleshooting 8-9
spam filtering

enabling in SMTP and POP3 3-6
spyware
detecting 3-3
Spyware/Grayware advisories 8-15
spyware/grayware detection
enabling for SMTP and POP3 3-3
stamp
spam identifier 8-8
valid characters 8-8
Status LED 2-5
flashing 8-13
synchronization
auto-synchronization feature 6-6
with peer 6-6
Syslog 2-6
syslog 5-3
enabling 5-3
viewing from ASDM 5-3
syslog entries 8-16
system information
view A-13

T

tab behavior 1-7
terminal session A-2
test files 8-16
tld 3-6
TLS, using 3-6
tooltips 1-9
TrendLabs 8-16
troubleshooting
activation 8-4
cannot create spam identifier 8-8
cannot log on 8-4
cannot update pattern file 8-8
CSC SSM throughput is less than ASA 8-14
delay in HTTP connection 8-6
downloading large files 8-11
false positives must be zero 8-9
FTP download does not work 8-7
installation 8-1
logging in without going through ASDM 8-13
management console timed out 8-13
recovering a lost password 8-4
restarting scanning service 8-12
spam not being detected 8-8
SSM cannot communicate with ASDM 8-13
Status LED flashing 8-13
summary status & log entries out of synch 8-5
too many false positives 8-9
too much spam 8-9
virus detected but not cleaned 8-9
virus scanning not working 8-9
website access slow or inaccessible 8-6
troubleshooting tools A-12

U

upload settings
modify A-16
URL blocking 4-6
via local list 4-6
via pattern file (PhishTrap) 4-7
URL filtering 4-8
categories 4-8
reclassify URL 4-9
rules 4-9
schedule work/leisure time 4-9
settings 4-8
URL rating lookups 2-6
URLs
Knowledge Base site 1-4, 8-15
Trend Micro Virus Submission Wizard site 8-9
Virus Information Center site 8-15

V

Virus Encyclopedia 8-15
Virus Map 8-15
Virus Primer 8-16

W

Webmail scanning 4-4
Webmaster tools 8-16
Weekly Virus Report 8-16
white papers (Trend Micro) 8-16
work/leisure time 4-9