Cisco Content Security and Control SSM Administrator Guide

Version 6.3.1172.0
June 2009

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-18970-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Content Security and Control SSM Administrator Guide

CONTENTS

Preface

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Introducing the CSC SSM

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

Overview

Trend Micro™ InterScan™ for Cisco CSC SSM™ provides an all-in-one content management solution for your network. CSC SSM is powered by Trend Micro Smart Protection Network, a next-generation cloud-client content security infrastructure designed to protect customers from web threats. CSC SSM includes powerful in-the-cloud email and web reputation technologies that are part of Smart Protection Network to prevent spam, phishing attempts and access to dangerous web pages. Spam not only clogs user inboxes with unwanted information which can zap user productivity, it also increasingly includes links to URLs which direct users to legitimate or illegitimate web pages designed to steal information from or take un-authorized control of computers. Trend Micro Smart Protection Network checks files, e-mail messages and URLs against our continuously updated and correlated threat databases in the cloud, ensuring immediate and automatic protection from these and other threats.

Summary information about this product is available at the following URLs:

- http://www.cisco.com/en/US/products/ps6823/index.html
- http://www.cisco.com/go/cscssm

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.
- Use Web Reputation technology to set your level of real-time protection against malicious websites
- Block URLs (globally or by user/group) that you do not want employees to access, or URLs that are known to have hidden or malicious purposes.
- Filter URL traffic (globally or by user/group) according to predefined categories that you allow or disallow adult or mature content, games, social networking, or gambling sites.

For more information about the Base License and Plus License, see the "Licensing" section on page 1-12.

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 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—HTTP, FTP, and SMTP 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.	Working with powerful Cisco firewall protection, Trend Micro InterScan for Cisco CSC SSM secures your network from threats, spam, and unwanted content.
Virus protection, spyware and grayware detection, and file blocking	Provides protection integrated with ASDM against security risks endangering your network traffic.

Table 1-1 Features and Benefits (continued)

Features	Benefits
Filters offensive or inappropriate content (globally or by user/group).	Provides a flexible way to control content accessed over your network.
Scans for spam at low to high threshold levels.	Utilizes Email Reputation technology that maximizes your protection that is easy to install with a Setup Wizard.
Allows you to determine how spam is handled	Can block unwanted correspondence while providing flexible notifications methods that can be customized to fit your needs.
Blocks incoming file types that can damage your network (globally or by user/group).	Preserves network integrity and conserves network resources from unnecessary scanning.
Helps prevent Denial of Service attacks by setting limits on message size.	Keeps your network up and running.
Provides approved senders and blocked senders functionality for file and URL blocking.	Allows you to customize your network protection.
Offers Web Reputation technology, a component of the Trend Micro Smart Protection Network	Scrutinizes URLs before you access potentially dangerous websites, especially sites known to be phishing or pharming sites. Provides real-time protection, conserves system scanning resources, and saves network bandwidth by preventing the infection chain or breaking it early.
Filters access to URLs by category.	Provides an intuitive method of configuring URL access as needed for your company, or for groups and users within your company.
Blocks connections to URLs or FTP sites prohibited by your corporate policies for all employees or specific users or groups.	Increases productivity by restricting access globally or by users and groups to URLs or FTP sites that are not work-related.
Allows you to fine-tune configuration of scanning, anti-spam, and filtering features after installation.	Provides the ability to adapt your network security needs to what you need now.
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 up-to-date information that keeps your network safe.
Provides e-mail and system log message notifications	Allows you to stay informed about activity on your network.
Provides log files that are purged automatically after 30 days.	Cleans out old records without intervention to prevent performance issues.
Provides a user-friendly console that includes online help to guide you through tasks.	Gives you the information you need to maximize and customize your security options.
Automatically displays a notification when your license is about to expire.	Ensures that you have ample notification to keep your network protected at all times.

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 the *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*
- *Open Source Software Licenses for ASA and PIX Security Appliances*
- *Cisco ASA 5500 Series Adaptive Security Appliance System Log Messages 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://esupport.trendmicro.com/support/

Terminology

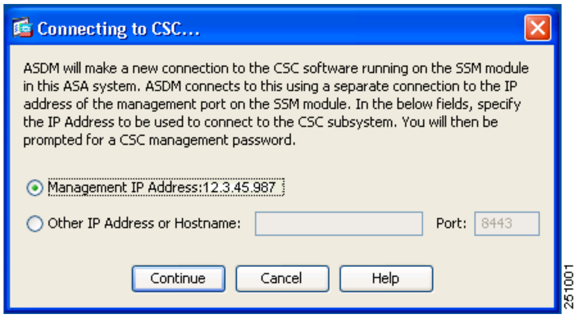
Certain terms are used throughout the documentation and online help that may not be familiar to you, or may be used in an alternate way from what you might expect. A definition of terms is available in the Glossary.

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



Connecting to CSC...

ASDM will make a new connection to the CSC software running on the SSM module in this ASA system. ASDM connects to this using a separate connection to the IP address of the management port on the SSM module. In the below fields, specify the IP Address to be used to connect to the CSC subsystem. You will then be prompted for a CSC management password.

● Management IP Address:12.3.45.987

○ Other IP Address or Hostname: Port: 8443

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

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

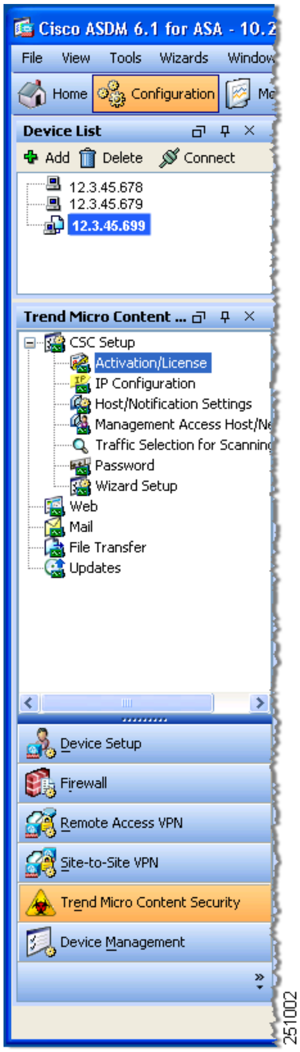
The Content Security tab appears. For more information, see the“Features of the Content Security Tab” section on page 7-1.

Configuring Content Security

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

- CSC Setup—Launches the Setup Wizard to install and configure the CSC SSM.
- Web—Configures Web scanning, Web Reputation protection, 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 1-8

- Default Values, page 1-9
- Tooltips, page 1-10
- Online Help, page 1-10

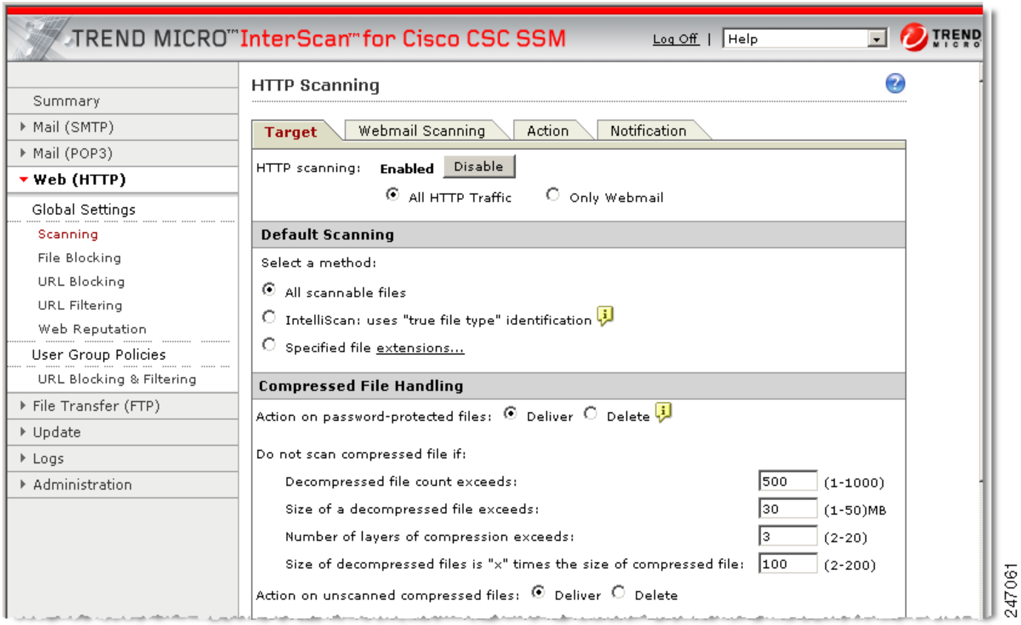
After you have successfully installed Trend Micro InterScan for Cisco CSC SSM and have configured the adaptive security appliance to send traffic to CSC SSM, the virus scanning and detection feature is activated and your network traffic is scanned according to the default settings. Additional features, 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. The Configuration window in ASDM has links to perform 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



HTTP Scanning

HTTP scanning: **Enabled** Disable

● All HTTP Traffic ○ Only Webmail

Default Scanning

Select a method:

● All scannable files

○ IntelliScan: uses "true file type" identification

○ Specified file extensions...

Compressed File Handling

Action on password-protected files: ● Deliver ○ Delete

Do not scan compressed file if:

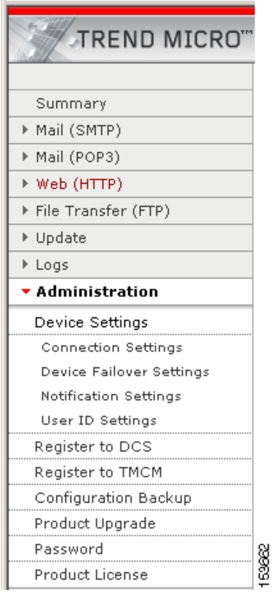
Decompressed file count exceeds:	500	(1-1000)
Size of a decompressed file exceeds:	30	(1-50)MB
Number of layers of compression exceeds:	3	(2-20)
Size of decompressed files is "x" times the size of compressed file:	100	(2-200)

Action on unscanned compressed files: ● Deliver ○ Delete

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 an item on the main menu.

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

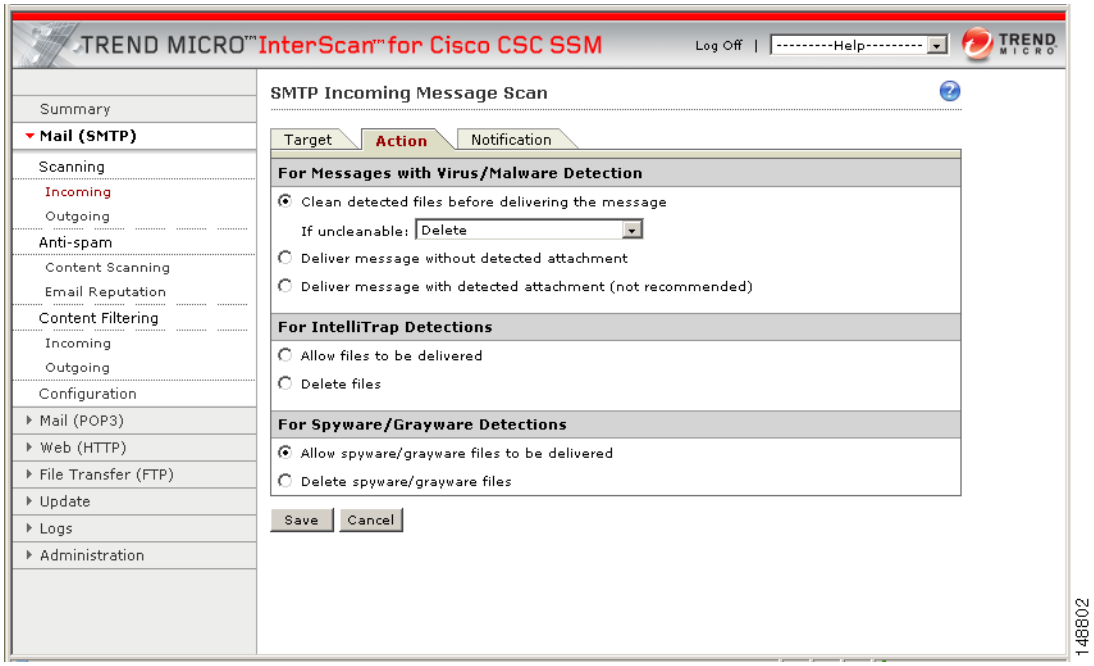


Tab Behavior

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



SMTP Incoming Message Scan

Target | Action | Notification

For Messages with Virus/Malware Detection

● Clean detected files before delivering the message

If uncleanable: Delete

○ Deliver message without detected attachment

○ Deliver message with detected attachment (not recommended)

For IntelliTrap Detections

○ Allow files to be delivered

○ Delete files

For Spyware/Grayware Detections

● Allow spyware/grayware files to be delivered

○ Delete spyware/grayware files

Save Cancel

- 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 make configuration changes, 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

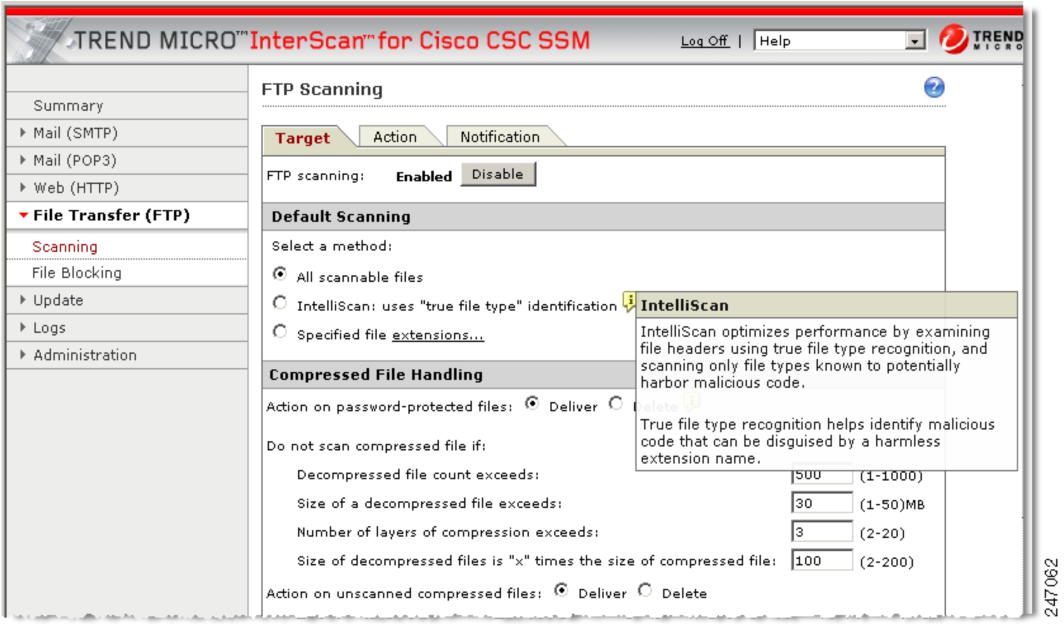
Many windows in the Trend Micro for Cisco CSC SSM user interface include fields that contain default settings. A default setting represents the choice that is best for most users, but you may change the default if another choice is better for your environment. For more information about entries in a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



FTP Scanning

FTP scanning: **Enabled**

Default Scanning

Select a method:

● All scannable files
○ IntelliScan: uses "true file type" identification
○ Specified file extensions...

IntelliScan
IntelliScan optimizes performance by examining file headers using true file type recognition, and scanning 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.

Compressed File Handling

Action on password-protected files: ● Deliver ○ Delete

Do not scan compressed file if:

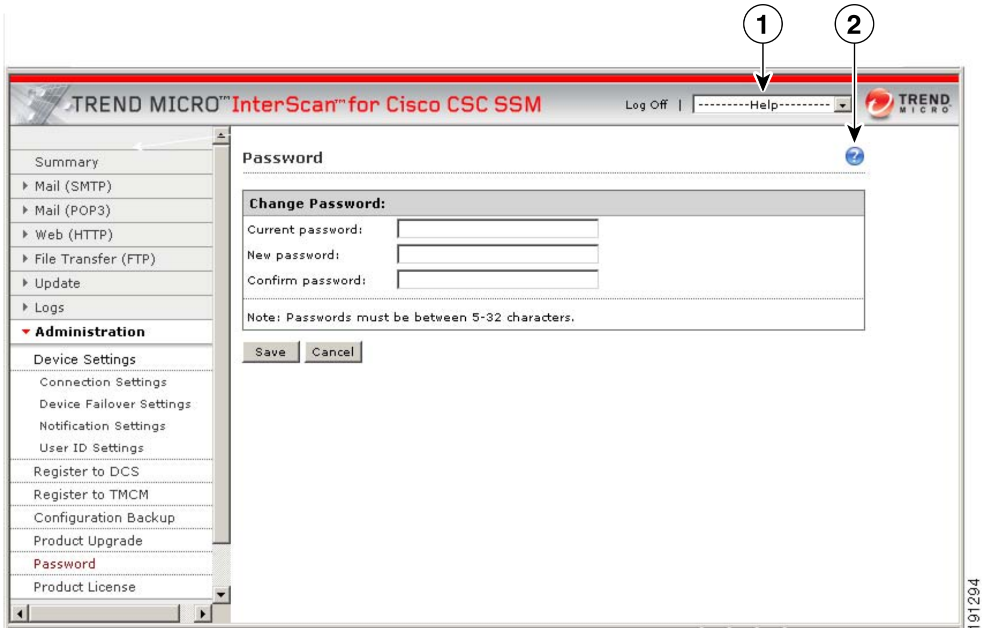
Decompressed file count exceeds:	500	(1-1000)
Size of a decompressed file exceeds:	30	(1-50)MB
Number of layers of compression exceeds:	3	(2-20)
Size of decompressed files is "x" times the size of compressed file:	100	(2-200)

Action on unscanned compressed files: ● Deliver ○ Delete

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



Password

Change Password:

Current password:

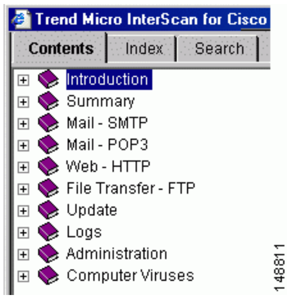
New password:

Confirm password:

Note: Passwords must be between 5-32 characters.

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.

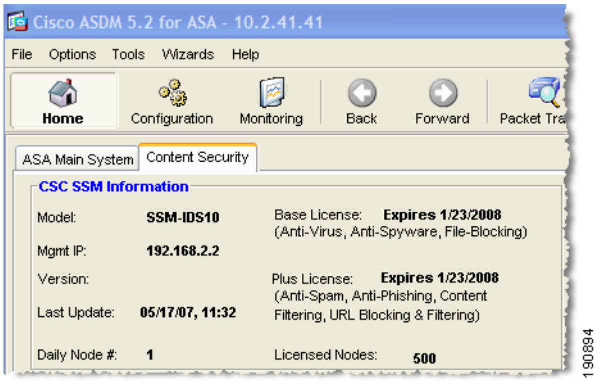
Licensing

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, Web Reputation technology, 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 Home > 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



CSC SSM Information

Model: SSM-IDS10

Mgmt IP: 192.168.2.2

Version:

Last Update: 05/17/07, 11:32

Daily Node #: 1

Base License: Expires 1/23/2008
(Anti-Virus, Anti-Spyware, File-Blocking)

Plus License: Expires 1/23/2008
(Anti-Spam, Anti-Phishing, Content Filtering, URL Blocking & Filtering)

Licensed Nodes: 500

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 > Content Scanning > Target/Action		x

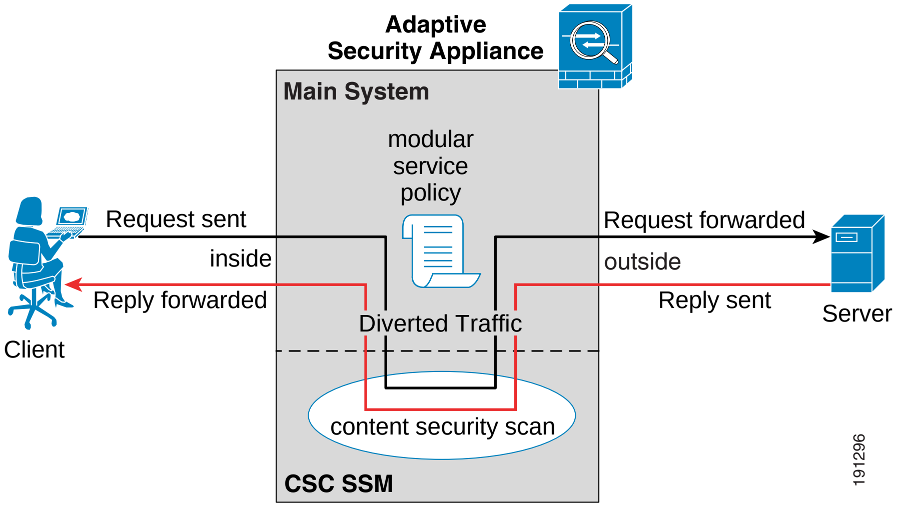
Table 1-2 Windows Available Based on License Type (continued)

Window Title	Base License	Plus License
Mail (SMTP) > Anti-spam > Email Reputation > Target/Action		x
Mail (SMTP) > Content Filtering > Incoming > Target/Action/Notification		x
Mail (SMTP) > Content Filtering > Outgoing > Target/Action/Notification		x
Mail (SMTP) > Configuration > Message Filter/Disclaimer/Incoming Mail Domain/Advanced Settings		x
Mail (POP3) > Scanning > Target/Action/Notification	x	
Mail (POP3) > Anti-spam > Target/Action		x
Mail (POP3) > Content Filtering > Target/Action/Notification		x
Web (HTTP) > Global Settings > Scanning > Target/Webmail Scanning/Action/ Notification	x	
Web (HTTP) > Global Settings >Web Reputation > Settings/Exceptions		x
Web (HTTP) > Global Settings > File Blocking > Target/Notification	x	
Web (HTTP) > Global Settings > URL Blocking > Via Local List/Notification		x
Web (HTTP) > Global Settings > URL Filtering > Rules/Exceptions/Time Allotment		x
Web (HTTP) > User Group Policies > URL Blocking & Filtering > All Policies/Policies by users/groups		x
File Transfer (FTP) > Scanning > Target/Action/Notification	x	
File Transfer (FTP) > File Blocking> Target/Notification	x	
Update > all windows	x	
Logs > all windows	x	
Administration > all windows	x	x (User ID settings only)

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 through the ASA server 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

To begin setup verification, you must confirm that the adaptive security appliance clock has been set correctly. CSC SSM will synchronize its clock with the adaptive security appliance.

Note CSC SSM may not function correctly if the adaptive security appliance time is not accurate.

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 2-6.

Step 2 If you do not have physical access to the device, do one of the following to assure activation:

- Log into the CSC web console at https://<CSC IP address>:8443 and check the Summary page license expiration, as shown in Figure 8-4 on page 8-15.
- Click the **Content Security** tab in the ASDM (see Figure 1-9 on page 1-12). You should see the device model number, management IP address, version, and other details displayed in the upper left corner.
- Run the **show module 1 details** command. You should see output that states "CSC SSM scan services are available."

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-10
.
. . . lines deleted for brevity...
.
App. name: CSC SSM
App. Status: Up
App. Status Desc: CSC SSM scan services are available
App. version: 6.2.xxxx.x
.
. . . lines deleted for brevity...
.
hostname#
```

Step 3 If these suggestions do not resolve your issues, 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.

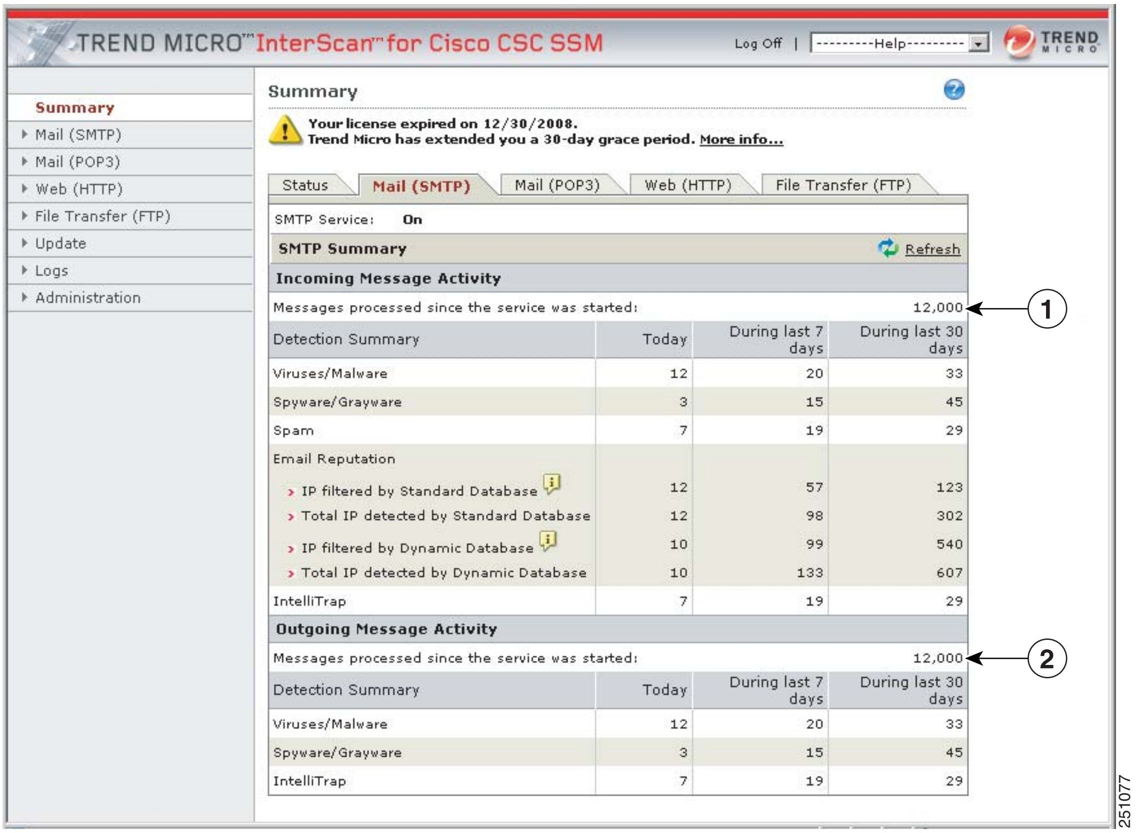
To verify that Trend Micro InterScan for Cisco CSC SSM is scanning your SMTP network traffic, perform the following steps:

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 ASA 5500 Series Configuration Guide using the CLI*.

Figure 2-1 Verify Scanning on the Summary Window



Summary

Your license expired on 12/30/2008.
Trend Micro has extended you a 30-day grace period. More info...

SMTP Service: On

SMTP Summary

Incoming Message Activity

Messages processed since the service was started: 12,000

Detection Summary	Today	During last 7 days	During last 30 days
Viruses/Malware	12	20	33
Spyware/Grayware	3	15	45
Spam	7	19	29
Email Reputation			
› IP filtered by Standard Database	12	57	123
› Total IP detected by Standard Database	12	98	302
› IP filtered by Dynamic Database	10	99	540
› Total IP detected by Dynamic Database	10	133	607
IntelliTrap	7	19	29

Outgoing Message Activity

Messages processed since the service was started: 12,000

Detection Summary	Today	During last 7 days	During last 30 days
Viruses/Malware	12	20	33
Spyware/Grayware	3	15	45
IntelliTrap	7	19	29

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.

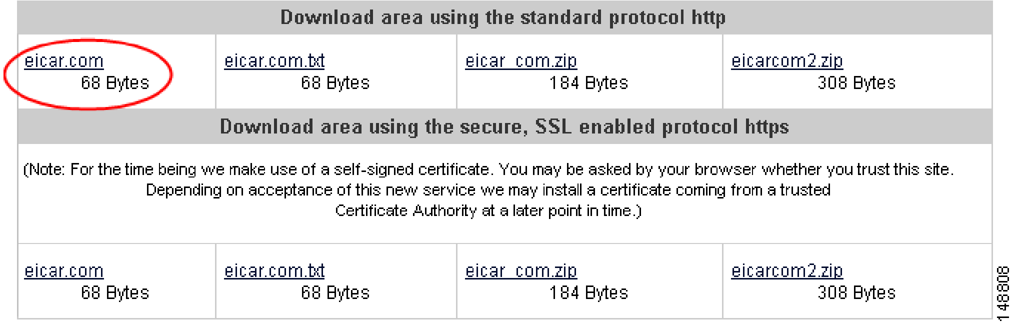
To test the antivirus feature, perform the following steps:

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 on-screen 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 Service-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. For more information, see Scanning Not Working Because the CSC SSM Is in a Failed State, page 8-10.

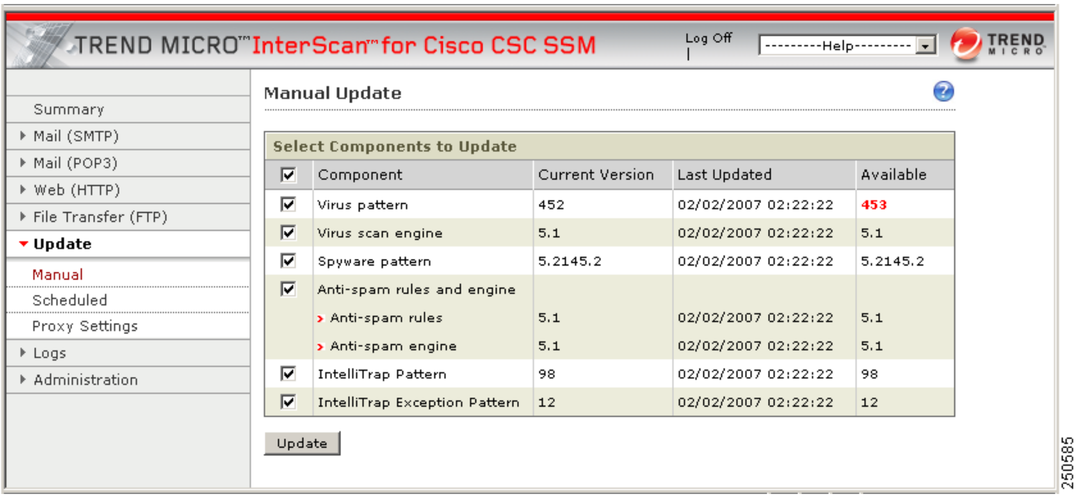
Verifying Component Status

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 engine and IntelliTrap pattern and pattern exceptions, 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



Manual Update

Select Components to Update

☑	Component	Current Version	Last Updated	Available
☑	Virus pattern	452	02/02/2007 02:22:22	453
☑	Virus scan engine	5.1	02/02/2007 02:22:22	5.1
☑	Spyware pattern	5.2145.2	02/02/2007 02:22:22	5.2145.2
☑	Anti-spam rules and engine			
	› Anti-spam rules	5.1	02/02/2007 02:22:22	5.1
	› Anti-spam engine	5.1	02/02/2007 02:22:22	5.1
☑	IntelliTrap Pattern	98	02/02/2007 02:22:22	98
☑	IntelliTrap Exception Pattern	12	02/02/2007 02:22:22	12

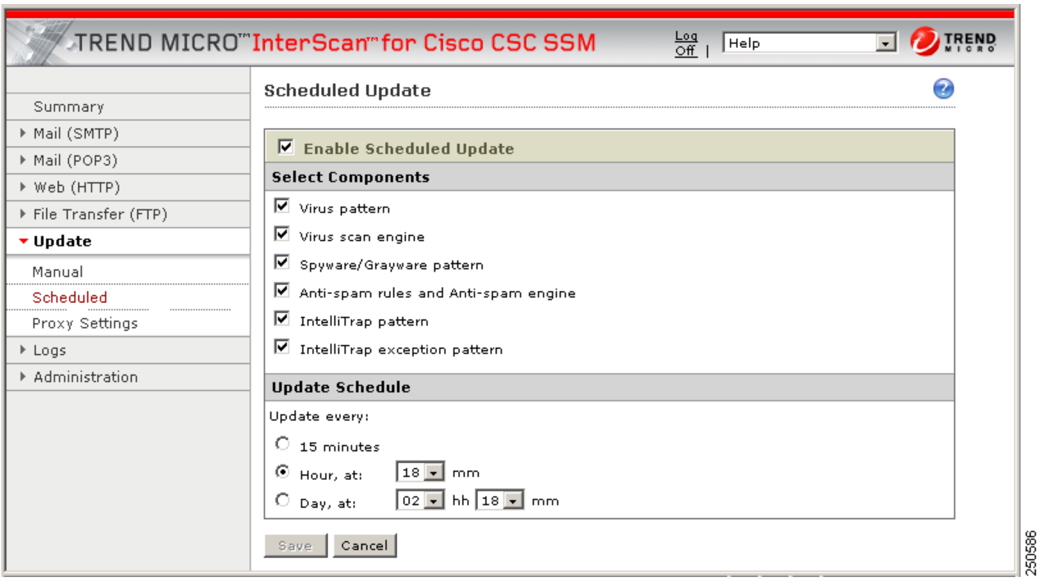
Step 2 If a more current version is available, the update version number displays in red in the Available column. Choose those components you want to update and click **Update** to download the most recent versions.

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:

- 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.
- The Trend Micro ActiveUpdate server is down.

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



Scheduled Update

☑ Enable Scheduled Update

Select Components

☑ Virus pattern
☑ Virus scan engine
☑ Spyware/Grayware pattern
☑ Anti-spam rules and Anti-spam engine
☑ IntelliTrap pattern
☑ IntelliTrap exception pattern

Update Schedule

Update every:

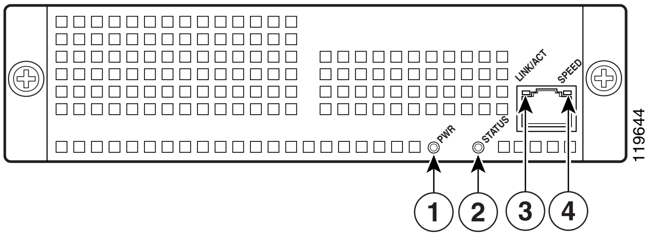
○ 15 minutes
● Hour, at: 18 mm
○ Day, at: 02 hh 18 mm

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 and Amber	Flashing	The SSM is running and activated, but the 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 hostname 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

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	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	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 500. • 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	Cleans the message or attachment in which the malware was detected. If the message or attachment is uncleanable, delete it (SMTP only) or replace with notification.
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 settings 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 “All scannable files” option for incoming SMTP messages, and scanning to the IntelliScan option for outgoing messages. You should set IntelliTrap to scan incoming messages, although it can also be configured to scan outgoing messages. Make sure that you enable spyware or grayware detection for incoming messages only.

About IntelliScan™

Most antivirus solutions today offer you two options in determining which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file name extensions (considered the most vulnerable to infection) are scanned. But recent developments involving files being “disguised” through having their extensions changed has made this latter option less effective. IntelliScan is a Trend Micro technology that identifies a file’s “true file type,” regardless of the file name extension.

Note IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

True File Type

When set to scan true file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named “family.gif,” it does not assume the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .gif and .jpg files make up a large volume of all Web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. However, this does not mean that they are entirely safe. It is possible for a malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

Note For the highest level of security, Trend Micro recommends scanning all files.

About IntelliTrap™

IntelliTrap works in real-time to detect potentially malicious code in compressed files that arrive as e-mail attachments. This feature is turned off by default. Enabling IntelliTrap allows CSC SSM to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Enable IntelliTrap by checking the check box in the IntelliTrap sections of the following locations:

- Mail (SMTP) > Scanning > Incoming or Outgoing/Target

- Mail (POP3) > Scanning/Target

When IntelliTrap detects malware, the users can choose one of the following actions:

- Allow files to be delivered
- Delete files

IntelliTrap technology is heuristically based, which allows it to detect previously unknown or new viruses. However, there are always a certain number of false positives. For this reason, Trend Micro recommends using the “Allow files to be delivered” action setting when you use this feature. With the action setting “Delete files,” the only way to recover the file is to have the sender resend the e-mail message with the attachment.

The action settings are available at the following locations:

- Mail (SMTP) > Scanning > Incoming or Outgoing/Action
- Mail (POP3) > Scanning/Action

Notifications can be configured at the following locations:

- Mail (SMTP) > Scanning > Incoming or Outgoing/Notification
- Mail (POP3) > Scanning/Notification

For more information about Notifications, see Reviewing SMTP and POP3 Notifications, page 3-5.

To update the IntelliTrap Pattern and IntelliTrap Exception Pattern, check the check box for each component on the Summary page and click **Update,** or set up schedule updates by choosing **Update > Scheduled**. For more information about scheduled updates, see Scheduled Update, page 5-2.

Enabling SMTP and POP3 Spyware and Grayware Detection

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:

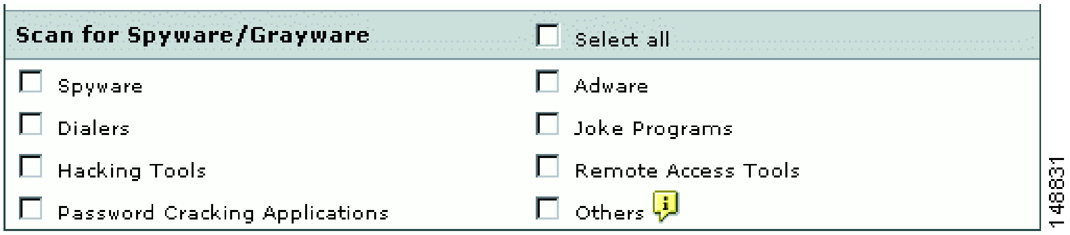
Step 1 To display the SMTP Incoming Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Incoming Scan** link.

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 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



Scan for Spyware/Grayware □ Select all

□ Spyware □ Adware

□ Dialers □ Joke Programs

□ Hacking Tools □ Remote Access Tools

□ Password Cracking Applications □ Others

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 3-5
- Modifying Notifications, page 3-6

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.

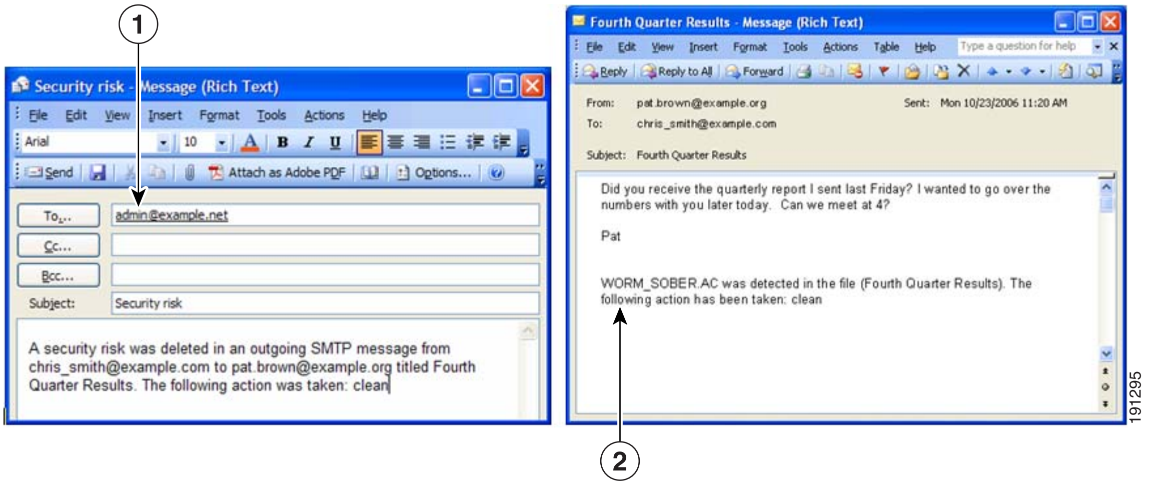
To review and reconfigure e-mail notifications, go to each of the following windows in the CSC SSM console:

- 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
Security risk - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Arial 10
Send
Attach as Adobe PDF
Options...
To...
Cc...
Bcc...
Fourth Quarter Results - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Type a question for help
Reply Reply to All Forward
2
191295

To: admin@example.net

Subject: Security risk

A security risk was deleted in an outgoing SMTP message from chris_smith@example.com to pat.brown@example.org titled Fourth Quarter Results. The following action was taken: clean

From: pat.brown@example.org

Sent: Mon 10/23/2006 11:20 AM

To: chris_smith@example.com

Subject: Fourth Quarter Results

Did you receive the quarterly report I sent last Friday? I wanted to go over the numbers with you later today. Can we meet at 4?

Pat

WORM_SOBER.AC was detected in the file (Fourth Quarter Results). The following action has been taken: clean

1	E-mail notification	**2**	Inline notification

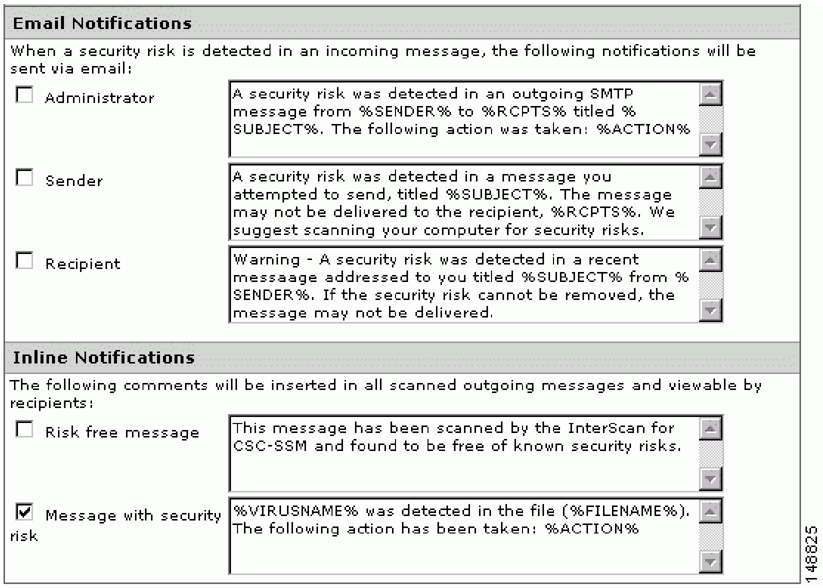
Notifications use variables called *tokens* to provide information that makes the notification more meaningful. For example, a token called %VIRUSNAME% is replaced with the text `WORM_SOBER.AC` in the inline notification example on the right.

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



Email Notifications

When a security risk is detected in an incoming message, the following notifications will be sent via email:

□ Administrator — A security risk was detected in an outgoing SMTP message from %SENDER% to %RCPTS% titled %SUBJECT%. The following action was taken: %ACTION%

□ Sender — A security risk was detected in a message you attempted to send, titled %SUBJECT%. The message may not be delivered to the recipient, %RCPTS%. We suggest scanning your computer for security risks.

□ Recipient — Warning - A security risk was detected in a recent messaage addressed to you titled %SUBJECT% from %SENDER%. If the security risk cannot be removed, the message may not be delivered.

Inline Notifications

The following comments will be inserted in all scanned outgoing messages and viewable by recipients:

□ Risk free message — This message has been scanned by the InterScan for CSC-SSM and found to be free of known security risks.

☑ Message with security risk — %VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION%

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, perform the following steps:

Step 1 In the Email Notifications section of the window, check the applicable check boxes provided to have additional people receive e-mail notifications.

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 Disclaimer tab of the SMTP Configuration window, you may add an organizational disclaimer that appears at the beginning or end of SMTP messages.

- To enable this feature, check one or both of the following check boxes:
  - Display disclaimer in all incoming e-mail messages.
  - Display disclaimer in all outgoing e-mail messages.

Note Leave this option blank if you do not want to use this feature.

- Select the location of the disclaimer using the Location drop-down box.
- If needed, customize the disclaimer text by highlighting it and redefining the message.
- Click **Save**.

Step 3 In the Incoming Mail Domain 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** check box is disabled by default. This setting allows sending and receiving MTAs to communicate using the encrypted TLS protocol.

Caution SMTP e-mail messages delivered via TLS are not scanned or filtered by CSC SSM, and could allow malicious content to enter the network. Email Reputation still scans all SMTP e-mail messages for spam.

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 Anti-spam > Content Scanning/Target window.

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

Step 3 For each of these windows (SMTP and POP3), 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 Mail (SMTP) > Anti-spam > Content Scanning/Target or 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 Mail (POP3) > Anti-spam/Target window. Open the SMTP Anti-spam > Content Scanning/Target window. The address for yourname@example.com has already been added to the list of Approved Senders on the Mail (SMTP) > Anti-spam > Content Scanning/Target window.

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

Approved and blocked senders lists can also be imported. The imported file must be in a specific format. See the online help for instructions.

Step 6 In the Blocked Senders section of the Mail (SMTP) > Anti-spam > Content Scanning/Target and Mail (POP3) > Anti-spam/Target windows, add the blocked senders. Mail (spam and non-spam) 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.

a. Go to the **Mail (SMTP) > Anti-spam > Content Scanning/Action** tab, and select 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 message.

b. Go to the **Mail (POP3) > Anti-spam/Action** tab, and select 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!").
  - Replace with notification to inform the recipient that the mail was not delivered because it violated an anti-spam policy.

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 (SMTP Incoming and Outgoing, and POP3), 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:

a. Go to the **Mail (SMTP) > Content Filtering > Incoming or Outgoing/Action** tab, and select one of the following options:

   - Delete messages (messages will not be delivered).
   - Deliver messages anyway.

   For attachments, select from the following options:

   - 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.

b. Go to the **Mail (POP3) > Content Filtering/Action** tab, and select one of the following options:

   For messages that match the filtering criteria:

   - Replace with notification to inform the recipient that the mail was not delivered because it violated a content filtering policy.
   - Deliver messages anyway.

   For messages that match the attachment criteria, select from the following options:

   - 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 Email Reputation

In addition to filtering spam on the basis of content, CSC SSM provides Email Reputation (ER) technology, which allow you to determine spam based on the reputation of the originating MTA. This off-loads the task from the CSC SSM server. With ER 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.

Note For Email Reputation Services to function properly, all address translation on inbound SMTP traffic must occur after traffic passes through the CSC SSM. If NAT or PAT takes place before the inbound SMTP traffic reaches the CSC SSM, CSC SSM will always see the local address as the originating MTA. ERS only blocks connections from suspect MTA public IP addresses, not private or local addresses. Therefore, customers using Email Reputation Services should not translate inbound SMTP connections before they are scanned by CSC SSM.

About Standard and Advanced Services

*Email Reputation Services — Standard (*ERS — Standard*)* service (formerly known as Realtime Blackhole List or 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.

Email Reputation Services — Advanced (ERS — Advanced) service (formerly RBL + and Quick IP Lookup or QIL combined) is a DNS, query-based service like Email Reputation Services Standard. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database. This service stops sources of spam while they are in the process of sending millions of messages.

When an IP address is found in either database, ER "marks" the connection and CSC SSM behaves according to the settings that you have chosen.

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 dynamic reputation database (used by ERS — Advanced) 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 standard reputation database (used by ERS-Standard), many that are only temporarily problematic (but nonetheless responsible for millions of spam) are not flagged by the standard reputation database. After these IP addresses have been added to the standard reputation database, however, it is more difficult to remove them from the database.

Note There is a higher degree of certainty that IP addresses in the standard reputation database 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.

Enabling and Configuring ER

Note This feature requires the Plus License.

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

Step 1 On the CSC SSM console, choose **Mail (SMTP) > Anti-spam > Email Reputation** to open the Target window.

Step 2 Click **Enable**.

Step 3 Choose the level of service you want to use: Standard or Advanced. The Advanced service level uses both standard and dynamic reputation database 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 databases used by the standard or advanced service. 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

After installation, your HTTP and FTP traffic is scanned by default for viruses, worms, and Trojans. Malware, such as spyware and other grayware, require a configuration change before they are detected. If you have a Plus License, you can block or allow URLs classified as phishing sites during work or leisure time.

Note Some categories, such as pornography, are blocked by default. Customers should review the categories blocked by default and make the appropriate adjustments. With a Plus License for URL Filtering and Blocking, URLs can be blocked with both global and/or user/group policies.

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 Hotmail, and Google.
File transfer (FTP) scanning of file transfers	Enabled using All Scannable Files as the scanning method.
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 500. • 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 (no scanning of 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 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 CSC SSM. You may change these settings. For example, you may prefer to scan by the “Specified file extensions. . .” option rather than the “All Scannable Files” option 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. You must configure these additional features if you purchased the Plus License, which entitles you to receive Web Reputation, URL blocking, and URL Filtering functionality (for both global and user/group policies).

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 extra time required to collect sufficient network packets to compose complete files for scanning. Table 4-1 summarizes the advantages and disadvantages of each method.

Table 4-2 Deferred Scanning Safety Comparison

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.

When the file is eventually scanned by CSC SSM, it may be found to contain malicious content. If so, CSC SSM takes following action:

- Sends a notification message, provided notifications are enabled
- Logs the event details
- Automatically blocks the URL from other users for four hours after malicious code detection. Access to the URL is restored after four hours elapses, and content from it will be scanned

If CSC SSM has been registered to a Damage Cleanup Services (DCS) server, a DCS clean-up request is issued under one of the following conditions:

- Someone (usually using a client PC) attempts to access a URL classified as Spyware, Disease Vector, or Virus Accomplice through URL Filtering (requires a Plus License).
- Someone (usually using a client PC) uploads a virus classified as a "worm."

DCS connects to the client to clean the file. For more information about DCS, see Appendix D, "Using CSC SSM with Trend Micro Damage Cleanup Services".

Spyware and Grayware Detection and Cleaning

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 creates two main problems to network administrators. It can compromise sensitive company information and reduce employee productivity by causing infected machines to malfunction. In addition to detecting and blocking incoming files that may install spyware, CSC SSM can prevent installed spyware from sending confidential data via HTTP.

If a client tries to access a URL classified as Spyware, Disease Vector, or Virus Accomplice, or a client PC uploads a virus classified as a worm as a webmail attachment, CSC SSM can send a request to Trend Micro Damage Cleanup Services (DCS) to clean the infected machine. DCS reports the outcome of the cleaning attempt (either successful or unsuccessful) to the CSC SSM server.

If the cleaning attempt is not successful, the client's browser is redirected to a special DCS-hosted cleanup page the next time the browser tries to access the Internet. This page contains an ActiveX control that again tries to clean the infected machine. If access permissions were the reason for the first failed cleaning attempt, the ActiveX control may be successful where cleaning via remote logon was unsuccessful.

For more information about DCS, see Using CSC SSM with Trend Micro Damage Cleanup Services, page D-1.

Note To avoid excessive cleanup attempts, CSC SSM only sends requests to clean up a target IP address once every four hours by default. If the client at that IP address continues to perform suspicious actions, then no further cleanup requests will be issued until this lockout period has expired. You can modify the length of this lockout period by going to `/opt/trend/isvw/config/web/intscan.ini` on the CSC SSM and changing the value of the `[DCS]/cleanup_lockout_hours` field. The value in this field is interpreted as the number of hours, and partial values (such as 0.5) are supported.

Detecting Spyware and Grayware

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 3-4 and the online help for these windows.

Scanning Webmail

As specified in Table 4-1, Webmail scanning for Yahoo, AOL, MSN Hotmail, 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 from scanning 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, enter a name for the Webmail site.

Step 4 In the Match field, enter the exact website name/IP address, a URL keyword, and a string.

Step 5 Choose the appropriate radio button to correspond with the text entered in the Match field.

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

Step 6 Click **Add**.

Step 7 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.

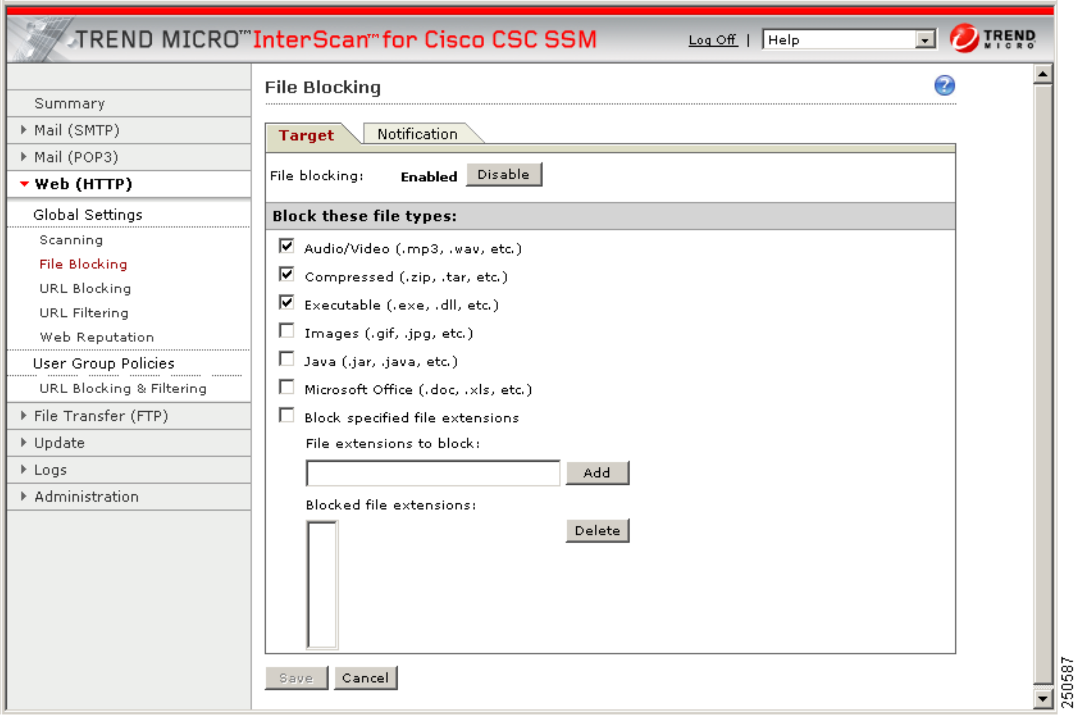
To configure file blocking, perform the following steps:

Step 1 To block downloads over 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 over 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



File Blocking

File blocking: **Enabled**

Block these file types:

- ☑ Audio/Video (.mp3, .wav, etc.)
- ☑ Compressed (.zip, .tar, etc.)
- ☑ Executable (.exe, .dll, etc.)
- ☐ Images (.gif, .jpg, etc.)
- ☐ Java (.jar, .java, etc.)
- ☐ Microsoft Office (.doc, .xls, etc.)
- ☐ Block specified file extensions

File extensions to block:

Blocked file extensions:

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**.

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:

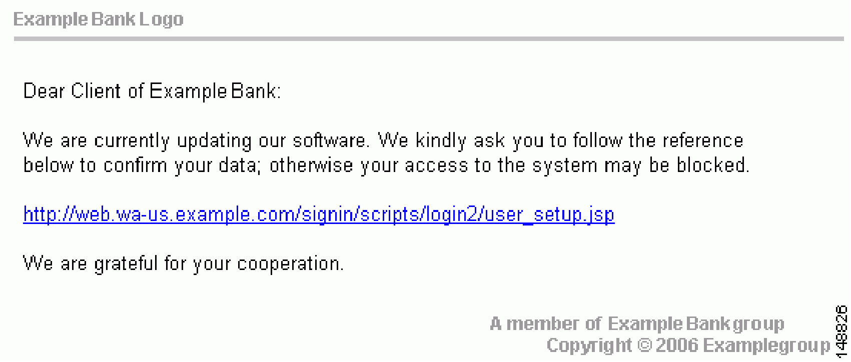
- Blocking from the Via Local List Tab, page 4-7
- URL Blocking Notifications, page 4-8

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. URL blocking policies, set by going to Web (HTTP) > Global Settings > URL Blocking, affect all users. URL blocking policies can also be set for specific users or groups. For more information, see the "URL Blocking and Filtering Policies for Users/Groups" section on page 4-21.

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



Example Bank Logo

Dear Client of Example Bank:

We are currently updating our software. We kindly ask you to follow the reference below to confirm your data; otherwise your access to the system may be blocked.

http://web.wa-us.example.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

A member of Example Bank group
Copyright © 2006 Examplegroup

By default, URL blocking is enabled (including blocking URLs based on user group policies).

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. (See Figure 4-3.)

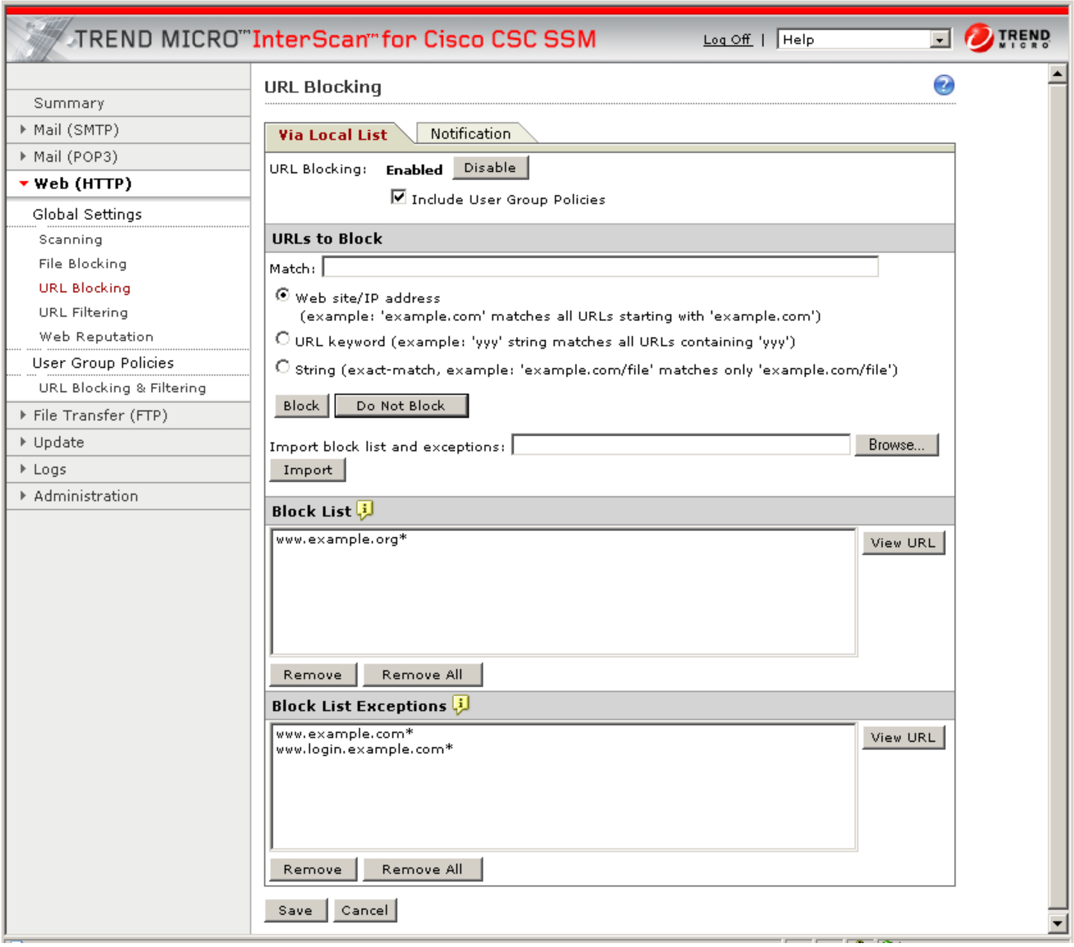
Step 2 On the Via Local List tab of the URL Blocking window, type the URLs you want to block in the Match field. You can specify the exact website name/IP address, a URL keyword, or a string.

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 URL Blocking Window



URL Blocking: Enabled

☑ Include User Group Policies

Match:

● Web site/IP address (example: 'example.com' matches all URLs starting with 'example.com')

○ URL keyword (example: 'yyy' string matches all URLs containing 'yyy')

○ String (exact-match, example: 'example.com/file' matches only 'example.com/file')

Import block list and exceptions:

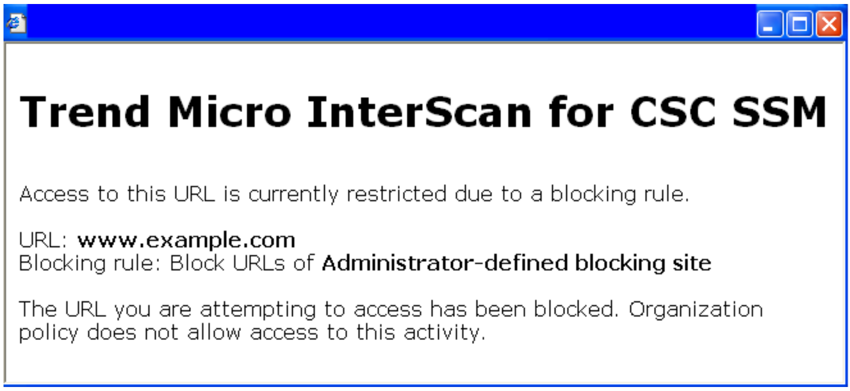
Block List:
www.example.org*

Block List Exceptions:
www.example.com*
www.login.example.com*

URL Blocking Notifications

A configurable message informs the end user when CSC SSM detects an attempt to access a blocked URL via HTTP. A default notification message is provided, but other text and variables can be used to create a custom message. URL Blocking and URL Filtering use the same notification message.

Figure 4-4 URL Blocking and Filtering Default Notification Message



Trend Micro InterScan for CSC SSM

Access to this URL is currently restricted due to a blocking rule.

URL: **www.example.com**
Blocking rule: Block URLs of **Administrator-defined blocking site**

The URL you are attempting to access has been blocked. Organization policy does not allow access to this activity.

To configure the notification message, 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 Notification tab of the URL Blocking window, type your custom message.

Step 3 Use the variables or tokens listed in the online help to customize your message.

Step 4 Click **Restore Default** to return to the default message.

Step 5 Click **Save** to save your work in this screen.

URL Filtering

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, such as leisure and work time. URL filtering policies set by going to Web (HTTP) > Global Settings > URL Filtering affect all users. URL filtering policies can also be set for specific users or groups. For more information, see the "URL Blocking and Filtering Policies for Users/Groups" section on page 4-21.

Note This feature requires the Plus License.

URL categories are organized into the URL filtering groups shown in Table 4-3.

Table 4-3 Grouping Definition for URL Categories

Category Group	Description
Adult	Sites that may be considered inappropriate for children
Business	Sites related to business, employment, or commerce
Communications and Search	Sites that provide tools and services for online communications and search
General	Sites not classified in other category groups, including unrated sites

Table 4-3 Grouping Definition for URL Categories (continued)

Category Group	Description
Internet Security	Potentially harmful sites, including sites known to have malware
Lifestyle	Sites about lifestyle preferences, including sexual, political, or religious orientations, as well as recreation and entertainment
Network Bandwidth	Sites that offer services that can significantly impact available network bandwidth

Note For URL Filtering to work correctly, the CSC SSM 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**.

URL Filtering Categories

Table 4-4 lists definitions of the URL Filtering categories and the assigned group.

Table 4-4 URL Filtering Category Definitions

Category Group	Category Type	Category Definition
Adult	Abortion	Sites that promote, encourage, or discuss abortion, including sites that cover moral or political views on abortion
Adult	Adult/Mature Content	Sites with profane or vulgar content generally considered inappropriate for minors; includes sites that offer erotic content or ads for sexual services, but excludes sites with sexually explicit images
Adult	Alcohol/Tobacco	Sites that promote, sell, or provide information about alcohol or tobacco products
Adult	Gambling	Sites that promote or provide information on gambling, including online gambling sites
Adult	Illegal Drugs	Sites that promote, glamorize, supply, sell, or explain how to use illicit or illegal intoxicants
Adult	Illegal/Questionable	Sites that promote and discuss how to perpetrate "nonviolent" crimes, including burglary, fraud, intellectual property theft, and plagiarism; includes sites that sell plagiarized or stolen materials
Adult	Intimate Apparel/ Swimsuit	Sites that sell swimsuits or intimate apparel with models wearing them
Adult	Marijuana	Sites that discuss the cultivation, use, or preparation of marijuana, or sell related paraphernalia
Adult	Nudity	Sites showing nude or partially nude images that are generally considered artistic, not vulgar or pornographic
Adult	Pornography	Sites with sexually explicit imagery designed for sexual arousal, including sites that offer sexual services

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Adult	Sex Education	Sites with or without explicit images that discuss reproduction, sexuality, birth control, sexually transmitted disease, safe sex, or coping with sexual trauma
Adult	Tasteless	Sites with content that is gratuitously offensive and shocking; includes sites that show extreme forms of body modification or mutilation and animal cruelty
Adult	Violence/Hate/ Racism	Sites that promote hate and violence; includes sites that espouse prejudice against a social group, extremely violent and physically dangerous activities, mutilation and gore, or the creation of destructive devices
Adult	Weapons	Sites about weapons, including their accessories and use; excludes sites about military institutions or sites that discuss weapons as sporting or recreational equipment
Business	Auctions	Sites that serve as venues for selling or buying goods through bidding, including business sites that are being auctioned
Business	Brokerage/Trading	Sites about investments in stocks or bonds, including online trading sites; includes sites about vehicle insurance
Business	Business/Economy	Sites about business and the economy, including entrepreneurship and marketing; includes corporate sites that do not fall under other categories
Business	Financial Services	Sites that provide information about or offer basic financial services, including sites owned by businesses in the financial industry
Business	Job Search/Careers	Sites about finding employment or employment services
Business	Real Estate	Sites about real estate, including those that provide assistance selling, leasing, purchasing, or renting property
Business	Shopping	Sites that sell goods or support the sales of goods that do not fall under other categories; excludes online auction or bidding sites
Communications and Search	Blogs/Web Communications	Blog sites or forums on varying topics or topics not covered by other categories; sites that offer multiple types of Web-based communication, such as email or instant messaging
Communications and Search	Chat/Instant Messaging	Sites that provide Web-based services or downloadable software for text-based instant messaging or chat
Communications and Search	Email Related	Sites that provide email services, including portals used by companies for Web-based email
Communications and Search	Infrastructure	Content servers, image servers, or sites used to gather, process, and present data and data analysis, including Web analytics tools and network monitors
Communications and Search	Internet Telephony	Sites that provide Web services or downloadable software for Voice over Internet Protocol (VoIP) calls

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Communications and Search	Newsgroups	Sites that offer access to Usenet or provide other newsgroup, forum, or bulletin board services
Communications and Search	Search Engines/ Portals	Search engine sites or portals that provide directories, indexes, or other retrieval systems for the Web
Communications and Search	Social Networking	Sites devoted to personal expression or communication, linking people with similar interests
Communications and Search	Web Hosting	Sites of organizations that provide top-level domains or Web hosting services
General	Computers/Internet	Sites about computers, the Internet, or related technology, including sites that sell or provide reviews of electronic devices
General	Education	School sites, distance learning sites, and other education-related sites
General	Government/Legal	Sites about the government, including laws or policies; excludes government military or health sites
General	Health	Sites about health, fitness, or well-being
General	Military	Sites about military institutions or armed forces; excludes sites that discuss or sell weapons or military equipment
General	News/Media	Sites about the news, current events, contemporary issues, or the weather; includes online magazines whose topics do not fall under other categories
General	Political	Sites that discuss or are sponsored by political parties, interest groups, or similar organizations involved in public policy issues; includes non-hate sites that discuss conspiracy theories or alternative views on government
General	Reference	General and specialized reference sites, including map, encyclopedia, dictionary, weather, how-to, and conversion sites
General	Translators (circumvent filtering)	Online page translators or cached Web pages (used by search engines), which can be used to circumvent proxy servers and Web filtering systems
General	Unrated	Sites that have not been classified under a category
General	Vehicles	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Internet Security	Adware	Sites with downloads that display advertisements or other promotional content; includes sites that install browser helper objects (BHOs)
Internet Security	Cookies	Sites that send malicious tracking cookies to visiting Web browsers

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Internet Security	Dialers	Sites with downloads that dial into other networks or premium-rate telephone numbers without user consent
Internet Security	Disease Vector	Sites that directly or indirectly facilitate the distribution of malicious software or source code
Internet Security	Hacking	Sites that provide downloadable software for bypassing computer security systems
Internet Security	Joke Program	Sites that provide downloadable “joke” software, including applications that can unsettle users
Internet Security	Made for AdSense sites (MFA)	Sites that use scraped or copied content to pollute search engines with redundant and generally unwanted results
Internet Security	Malware/Virus Accomplice	Sites used by malicious programs, including sites used to host upgrades or store stolen information
Internet Security	Password Cracking Application	Sites that distribute password cracking software
Internet Security	Phishing	Fraudulent sites that mimic legitimate sites to gather sensitive information, such as user names and passwords
Internet Security	Potentially Malicious Software	Sites that contain potentially harmful downloads
Internet Security	Proxy Avoidance	Sites about bypassing proxy servers or Web filtering systems, including sites that provide tools for that purpose
Internet Security	Remote Access Program	Sites that provide tools for remotely monitoring and controlling computers
Internet Security	Spam	Sites whose addresses have been found in spam messages
Internet Security	Spyware	Sites with downloads that gather and transmit data from computers owned by unsuspecting users
Internet Security	Web Advertisement	Sites dedicated to displaying advertisements, including sites used to display banner or popup ads
Lifestyle	Activist Groups	Sites that promote change in public policy, public opinion, social practice, economic activities, or economic relationships; includes sites controlled by service, philanthropic, professional, or labor organizations
Lifestyle	Alternative Journals	Online equivalents of supermarket tabloids and other fringe publications
Lifestyle	Arts/Entertainment	Sites that promote or provide information about movies, music, non-news radio and television, books, humor, or magazines
Lifestyle	Cult/Occult	Sites about alternative religions, beliefs, and religious practices, including those considered cult or occult
Lifestyle	Cultural Institutions	Sites controlled by organizations that seek to preserve cultural heritage, such as libraries or museums; also covers sites owned by the Boy Scouts, the Girl Scouts, Rotary International, and similar organizations

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Lifestyle	For Kids	Sites designed for children
Lifestyle	Games	Sites about board games, card games, console games, or computer games; includes sites that sell games or related merchandise
Lifestyle	Gay/Lesbian	Sites about gay, lesbian, transgender, or bisexual lifestyles
Lifestyle	Humor/Jokes	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Lifestyle	Personal Websites	Sites maintained by individuals about themselves or their interests; excludes personal pages in social networking sites, blog sites, or similar services
Lifestyle	Personals/Dating	Sites that help visitors establish relationships, including sites that provide singles listings, matchmaking, or dating services
Lifestyle	Recreation/Hobbies	Sites about recreational activities and hobbies, such as collecting, gardening, outdoor activities, traditional (non-video) games, and crafts; includes sites about pets, recreational facilities, or recreational organizations
Lifestyle	Religion	Sites about popular religions, their practices, or their places of worship
Lifestyle	Restaurants/Dining/ Food	Sites that list, review, discuss, advertise, or promote food, catering, dining services, cooking, or recipes
Lifestyle	Society/Lifestyle	Sites that provide information about life or daily matters; excludes sites about entertainment, hobbies, sex, or sports, but includes sites about cosmetics or fashion
Lifestyle	Sport Hunting and Gun Clubs	Sites about gun clubs or similar groups; includes sites about hunting, war gaming, or paintball facilities
Lifestyle	Sports	Sites about sports or other competitive physical activities; includes fan sites or sites that sell sports merchandise
Lifestyle	Travel	Sites about travelling or travel destinations; includes travel booking and planning sites
Network Bandwidth	Internet Radio and TV	Sites that primarily provide streaming radio or TV programming; excludes sites that provide other kinds of streaming content
Network Bandwidth	Pay to Surf	Sites that compensate users who view certain Web sites, email messages, or advertisements or users who click links or respond to surveys
Network Bandwidth	Peer-to-Peer	Sites that provide information about or software for sharing and transferring files within a peer-to-peer (P2P) network
Network Bandwidth	Personal Network Storage/File Download Servers	Sites that provide personal online storage, backup, or hosting space, including those that provide encryption or other security services
Network Bandwidth	Photo Searches	Sites that primarily host images, allowing users to share, organize, store, or search for photos or other images

Table 4-4 URL Filtering Category Definitions (continued)

Category Group	Category Type	Category Definition
Network Bandwidth	Ringtones/Mobile Phone Downloads	Sites that provide content for mobile devices, including ringtones, games, or videos
Network Bandwidth	Software Downloads	Sites dedicated to providing free, trial, or paid software downloads
Network Bandwidth	Streaming Media/ MP3	Sites that offer streaming video or audio content without radio or TV programming; sites that provide music or video downloads, such as MP3 or AVI files

Filtering Rules, Exceptions, and Time

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 Rules** to display the URL Filtering: Rules window.

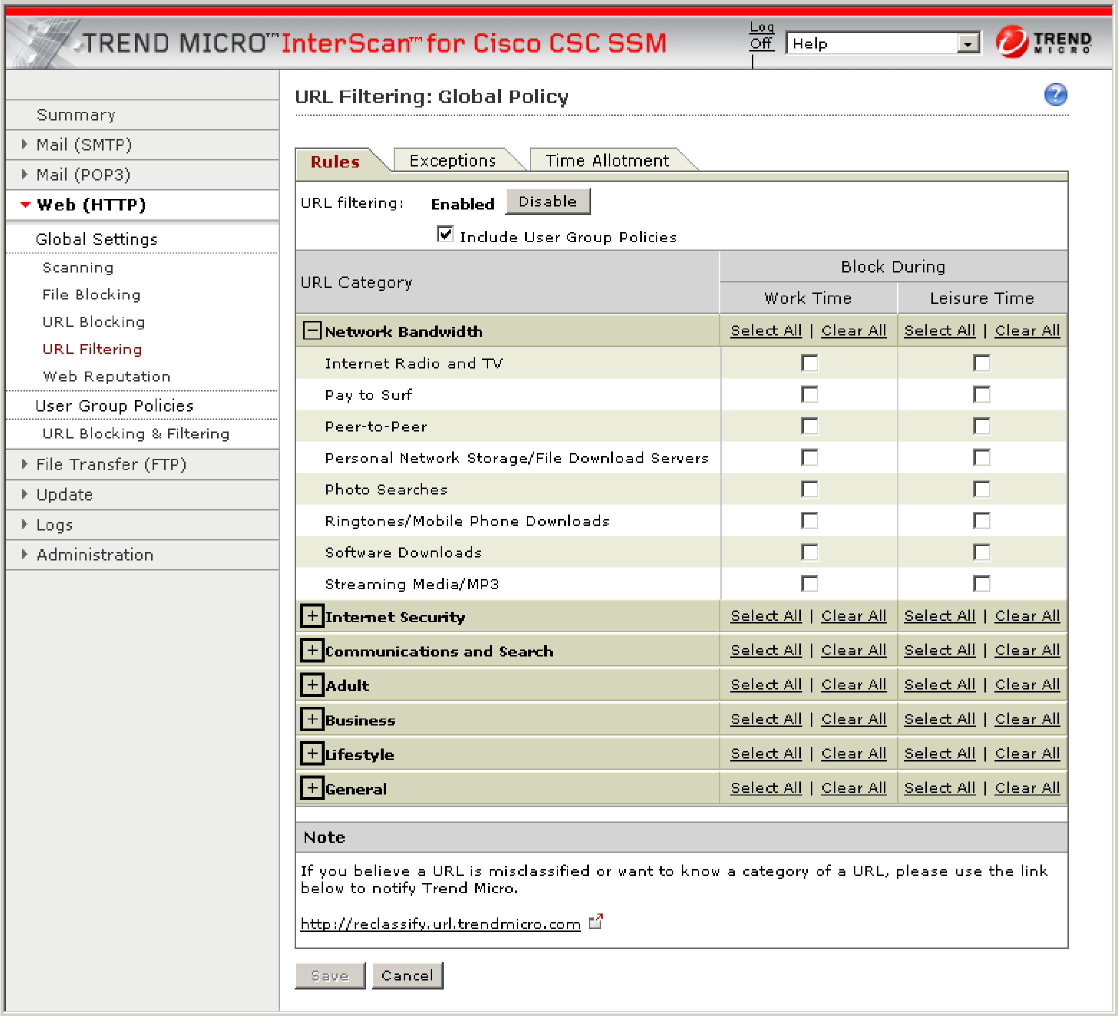
Step 2 Click **Enable** to enable the URL Filtering feature. (It is enabled by default.)

Step 3 Check the "Include User Group Policies" check box to included User Group Policies, if appropriate.

Step 4 On the Rules tab, review the subcategories listed under each category. (See Figure 4-5.) For example, "Illegal Drugs" is a subcategory of the "Adult" category. If your organization is a financial services company, you may want to filter this category. Check the "Illegal Drugs" check boxes for Work and Leisure time to enable filtering for sites related to illegal drugs. However, if your organization is a law enforcement agency, you should uncheck the "Illegal Drugs" subcategory.

Step 5 For each of the seven groups of categories, specify whether the URLs are blocked, and if so, during work time, leisure time, or both.

Figure 4-5 URL Filtering Rules Tab



URL Filtering: Global Policy

URL filtering: **Enabled** Disable

☑ Include User Group Policies

URL Category	Block During	
	Work Time	Leisure Time
⊟ **Network Bandwidth**	Select All | Clear All	Select All | Clear All
Internet Radio and TV	□	□
Pay to Surf	□	□
Peer-to-Peer	□	□
Personal Network Storage/File Download Servers	□	□
Photo Searches	□	□
Ringtones/Mobile Phone Downloads	□	□
Software Downloads	□	□
Streaming Media/MP3	□	□
⊞ **Internet Security**	Select All | Clear All	Select All | Clear All
⊞ **Communications and Search**	Select All | Clear All	Select All | Clear All
⊞ **Adult**	Select All | Clear All	Select All | Clear All
⊞ **Business**	Select All | Clear All	Select All | Clear All
⊞ **Lifestyle**	Select All | Clear All	Select All | Clear All
⊞ **General**	Select All | Clear All	Select All | Clear All

Note

If you believe a URL is misclassified or want to know a category of a URL, please use the link below to notify Trend Micro.

http://reclassify.url.trendmicro.com

Step 6 If you believe a particular URL has been misclassified, you can check the category of the URL and request it be reclassified by clicking the link in the Note section at the bottom of the page.

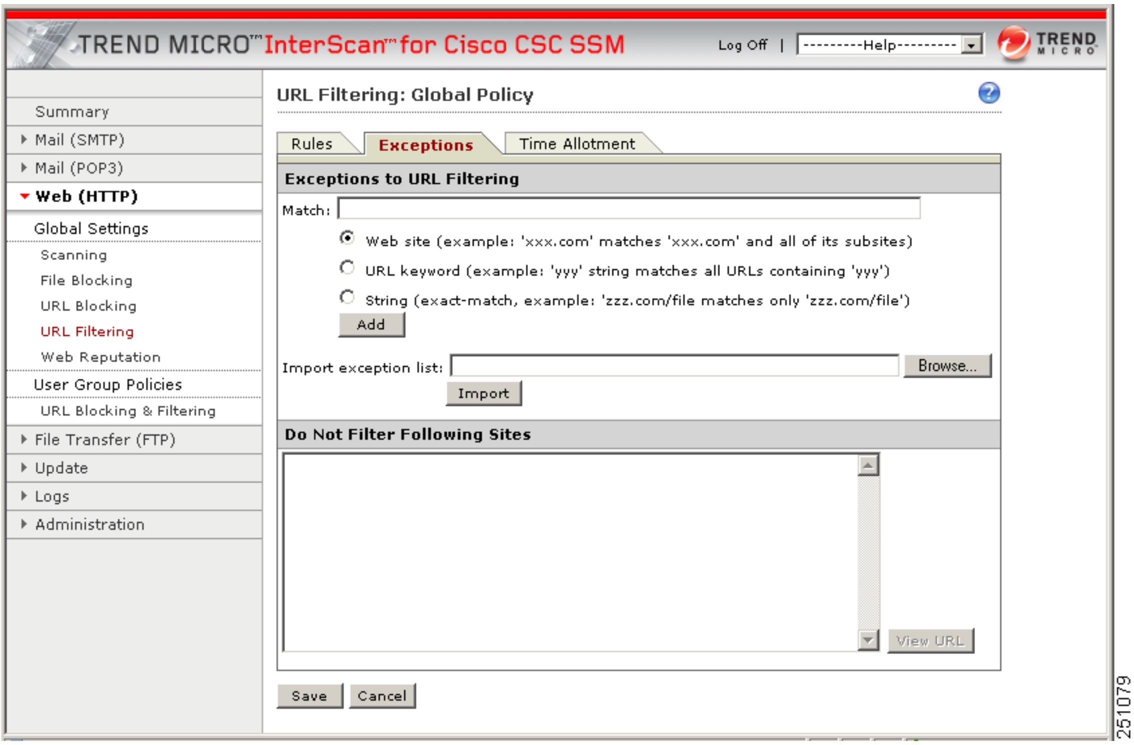
Step 7 If there are sites within the enabled subcategories that you do not want filtered, click the **Exceptions** tab. (See Figure 4-6.)

Step 8 Type the URLs you want to exclude from filtering in the Match field. You can specify the exact website name or IP address, a URL keyword, and a string.

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

Note You can also import a list of URL filtering exceptions. The imported file must be in a specific format. See the online help for instructions.

Figure 4-6 URL Filtering Exception Tab



URL Filtering: Global Policy

Exceptions to URL Filtering

Match:

● Web site (example: 'xxx.com' matches 'xxx.com' and all of its subsites)

○ URL keyword (example: 'yyy' string matches all URLs containing 'yyy')

○ String (exact-match, example: 'zzz.com/file matches only 'zzz.com/file')

Import exception list:

Do Not Filter Following Sites

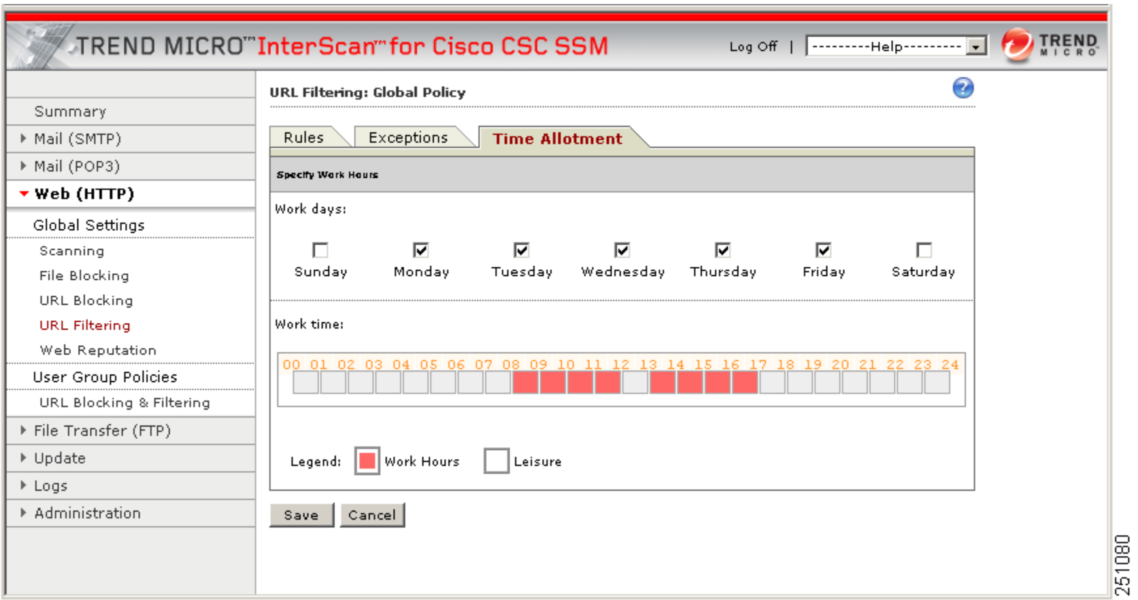
Step 9 Click **Add** after each entry to move it to the “URL to the Do Not Filter the Following Sites” list. Entries remain as exceptions until you remove them.

Step 10 Click the **Time Allotment** tab.

Step 11 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. Figure 4-7 shows 8:00 a.m. through 12:00 a.m. and 1:00 p.m. through 5:00 p.m. as work time.)

- For setting work days, check the check box for the days of the week to be designated as work days.
- For setting work time, click the hours to be designated as work time.

Figure 4-7 URL Filtering Time Allotment Tab



Work days:

☐ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday

Work time:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
□	□	□	□	□	□	□	□	🟥	🟥	🟥	🟥	□	🟥	🟥	🟥	🟥	□	□	□	□	□	□	□

Legend: 🟥 Work Hours □ Leisure

Step 12 Click **Save** to update the URL filtering configuration.

Web Reputation

Web Reputation guards end-users against emerging Web threats. Because a Web Reputation query returns URL category information (used by URL Filtering), CSC SSM does not use a locally stored URL database. Web Reputation requires a Plus License.

Web Reputation also assigns reputation scores to URLs. For each accessed URL, CSC SSM queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.

CSC SSM has a feature that enables the device to automatically provide feedback on infected URLs, which helps improve the Web Reputation database. If enabled, this feedback includes product name and version, URL, and virus name. (It does not include IP address information, so all feedback is anonymous and protects company information.) Web Reputation results are located in the Web Reputation log (Logs > Query > Web Reputation) and the Summary > Web (HTTP) tab.

Using Trend Micro Web Reputation technology (part of the Smart Protection Network), you perform website scanning at varying levels of protection (low, medium, and high) and add websites to the Exceptions List (yourcompany.com, for example) so that websites can be viewed without scanning or blocking.

Note Pre-approving websites must be done carefully. Not scanning or blocking a website could pose a security risk.

Anti-phishing using Web Reputation

CSC SSM provides anti-phishing through Web Reputation and URL Filtering. Both features require a Plus License.

- Phishing sites blocked by URL Filtering are blocked by the Phishing category and will give a "Phishing" message
- Phishing sites blocked by Web Reputation will provide a "low reputation" message.

Web Reputation Database

The Web Reputation database resides on a remote server. When a user attempts to access a URL, CSC SSM retrieves information about this URL from the Web Reputation database and stores it in the local cache. Having the Web Reputation database on a remote server and building the local cache with this database information reduces the overhead on CSC SSM and improves performance.

The Web Reputation database is updated with the latest security information about web pages. If you believe the reputation of a URL is misclassified or you want to know the reputation of a URL, use the following link to notify Trend Micro:

http://reclassify.wrs.trendmicro.com/submit-files/wrsonlinequery.asp

Settings

Setting the security sensitivity level prevents users from being misdirected to malicious websites and provides administrators the ability to set the protection level.

Web Reputation settings involve specifying the following:

- Enable or disable Web Reputation
- Select the appropriate security sensitivity level for your company
- (Optional) Provide anonymous feedback on infected URLs to Trend Micro

Security Sensitivity Level

Upon receiving a Web Reputation score, CSC SSM determines whether the score is below or above the preferred threshold. The threshold of sensitivity level is defined by the user. Medium is the default sensitivity setting. Trend Micro recommends this setting because it blocks most web threats while not creating many false positives.

To set the sensitivity level, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Settings** tab.

Step 2 Click **Enable** to enable Web Reputation (Enabled is the default setting.)

Step 3 Specify the URL blocking sensitivity level. Select from the following:

- **High** — Blocks more websites, but risks blocking non-malicious websites
- **Medium** — (default) Balances risks between High and Low settings
- **Low** — Blocks fewer websites, but risks not blocking potentially malicious websites

Step 4 Click **Save**.

Feedback Option

Web Reputation scan results can be fed back to an external backend Rating Server. The Feedback option is disabled by default.

To enable the feedback option, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Settings** tab.

Step 2 Check the "Send anonymous feedback on infected URLS to Trend Micro" check box.

Step 3 Click **Save**.

Exceptions

Listing a website within the Web Reputation approved list allows CSC SSM to bypass any malicious code scans on the listed site. Web Reputation scanning exceptions can be defined by entering the complete website URL or IP address, a URL keyword, a string, or by importing an existing exception list of URLs.

⚠ **Caution** Lack of scanning could cause security holes if a website on the Approved list has been hacked and had malicious code injected.

To specify Web Reputation exceptions, perform the following steps:

Step 1 Go to the **Web (HTTP) > Global Settings > Web Reputation > Exceptions** tab.

Step 2 Do one of the following:

- Enter text in the Match file, specify the match type, and then click **Add.**

Note The default option is Web site/IP address.

- Import the URL approved list. For more information about importing the URL exceptions list, see the online help topic named "HTTP URL Filtering Settings - URL Filtering Exceptions".

Step 3 Click **Add**.

Step 4 Click **Save**.

After you have specified a URL as an exception to Web Reputation, you can include it in Web Reputation scanning by selecting the URL in the Approved List and clicking **Remove** to remove it from the list. Click **Remove All** to delete all URLs in the Approved List.

URL Blocking and Filtering Policies for Users/Groups

CSC SSM has a policy framework that allows the association of URL Filtering and Blocking policies to specific groups or individual users based on the user or group identity. This feature includes:

- Identification settings
- Microsoft Active Directory service support
- Policy item management
- User/Group-based log and report

Note Both URL Filtering and URL Blocking require a Plus License.

CSC SSM supports up to 20 URL Filtering and Blocking policies for users and groups. The Domain Controller Agent software can be deployed on a Domain Controller Server or Windows machine that is on the Intranet. The agent communicates with CSC SSM over a secure, TCP port and works with Microsoft Active Directory.

Before using user/group policies for URL Filtering and Blocking, enable the following:

- Select a method of user/group identification by going to: **Administration > Device Settings > User Id Settings**. For more information about User ID settings, see the "Configuring User ID Settings" section on page 6-3.
- Download and install the Domain Controller Agent. For more information, see the "Installing the Domain Controller Agent" section on page 6-6.
- Add the Domain Controller Agent and Domain Controller information. For more information, see the "Adding A Domain Controller Agent or Server to CSC SSM" section on page 6-7.
- Enable URL Filtering at the global level by going to: **Web (HTTP) > Global Settings > URL Filtering**, and check the 'Include User Group Policies" check box.
- Enable URL Blocking at the global level by going to: **Web (HTTP) > Global Settings > URL Blocking**, and check the 'Include User Group Policies" check box.

The All Policies tab on the URL Blocking & Filtering Policies screen displays existing policies and provides the following information:

- Policy Type — Lists the policy by type, either Filtering or Blocking
- Policy Name — Shows the descriptive name assigned to identify the policy
- Status — Indicates if the policy is enabled (green check) or disabled (red check)
- Priority — Indicates the order in which the policies will be enforced. For example, if a policy has an exception and has a higher priority than another policy, this policy will override the rules of the lower priority policy. Any global policies configured under URL Filtering or URL Blocking will always have the lowest priority.

The Policies by User/Group tab offers search capabilities for existing policies. Editing policies is possible from this screen by clicking the policy name.

Add/Edit URL Blocking Policies for Users/Groups

URL blocking is an important tool for managing employee Internet use in your organization. With URL blocking, you can prohibit access to URLs that may distract employees from productive use of their time or may even result in legal liability. The process of adding a blocking policy for groups or users begins with choosing a template and creating an account.

If "Global Policy - URL Blocking" appears in the list of policies, this policy was configured on the Web (HTTP) > Global Settings > URL Blocking screen. Priority settings can be changed for user and group policy by going to Web (HTTP) > User Group Policies > URL Blocking & Filtering. Go to the far right column in the table that lists the policies, and click the up and down arrows to adjust the priority. Global policies will always have the lowest priority.

Prerequisites

Before a blocking policy can be added, do the following:

- URL Blocking must be enabled on the global level by going to Web (HTTP) > Global Settings > URL Blocking.
- A method of user/group identification must be selected by going to Administration > Device Settings > User ID Settings screen, and the Domain Controller Agent must be installed and configured. For more information, see the "Configuring User ID Settings" section on page 6-3.

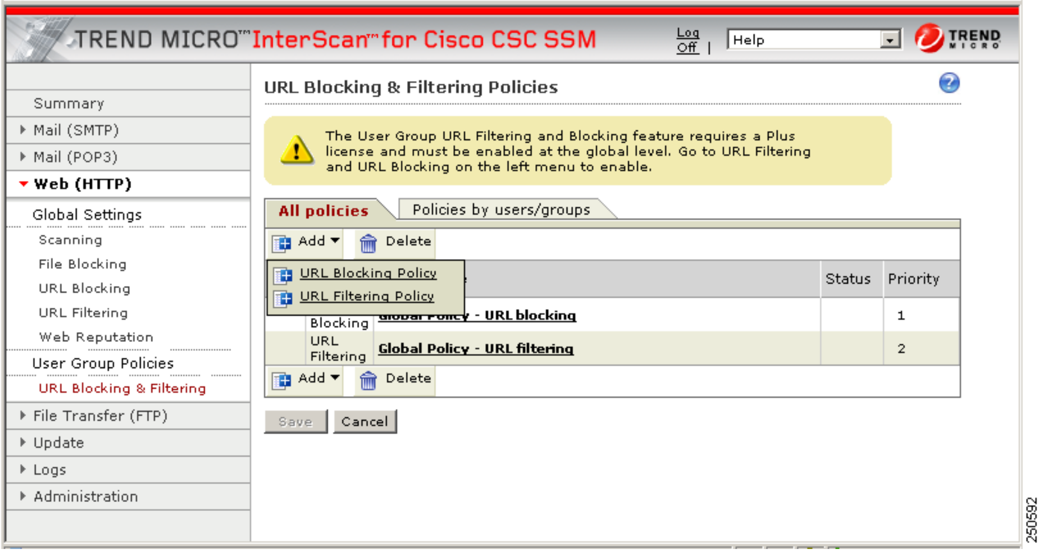
Selecting a Template

To select a template for the first rule of a URL Blocking Policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > URL Blocking and Filtering > All policies** tab.

Step 2 Click **Add** and select **URL Blocking Policy**. (See Figure 4-8.)

Figure 4-8 To Add a User Group Policy



The User Group URL Filtering and Blocking feature requires a Plus license and must be enabled at the global level. Go to URL Filtering and URL Blocking on the left menu to enable.

		Status	Priority
Blocking	Global Policy - URL blocking		1
URL Filtering	Global Policy - URL filtering		2

Step 3 (Optional) Check the **Enable policy** check box to have the policy enabled as soon as it is created. (See Figure 4-9.)

Note To enable the policy later, see the "Enabling a User/Group Blocking Policy" section on page 4-24.

Step 4 Go to the Template section of the URL Blocking Policy: Add Policy page.

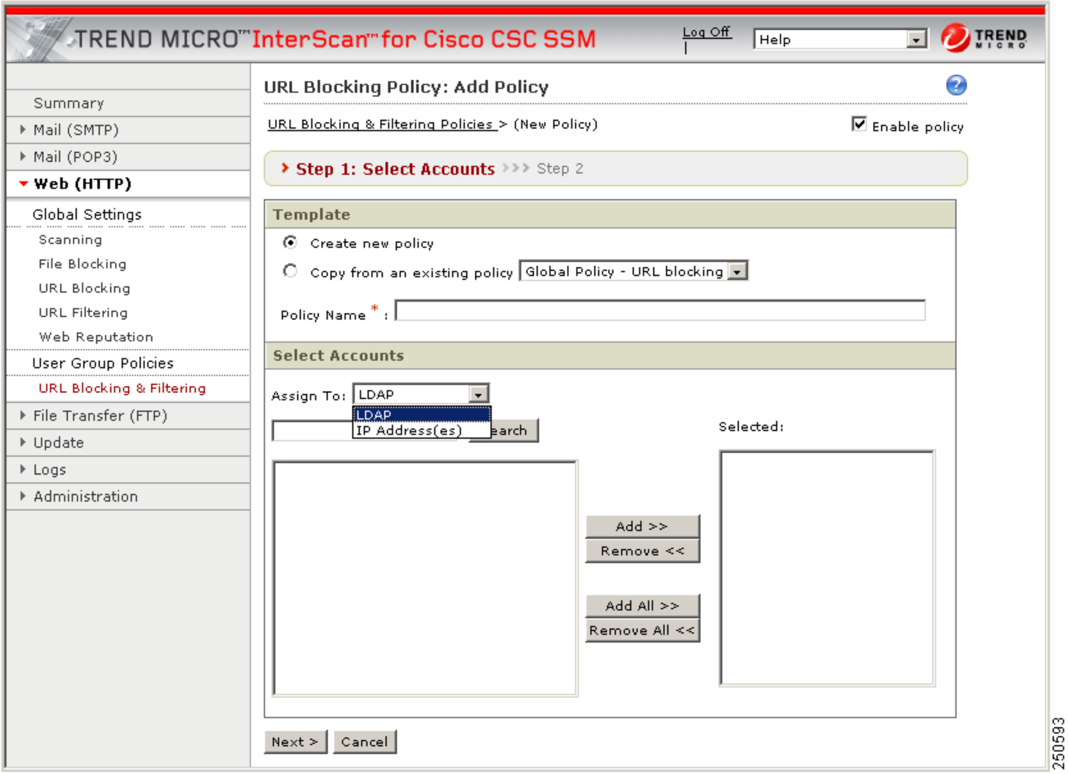
Step 5 Select one of the following options:

- Create a new policy
- Copy from an existing policy. If this option is chosen, use the drop-down list to select the policy to use as a template.

Step 6 Type a descriptive policy name.

Step 7 Select accounts according to the "Creating Accounts" section on page 4-26.

Figure 4-9 Selecting a Template and User ID Method



URL Blocking Policy: Add Policy

URL Blocking & Filtering Policies > (New Policy)

☑ Enable policy

Step 1: Select Accounts

Template

● Create new policy

○ Copy from an existing policy: Global Policy - URL blocking

Policy Name * :

Select Accounts

Assign To: LDAP (LDAP, IP Address(es))

Selected:

Creating Accounts

To create accounts, perform the following steps:

Step 1 Select a template according to the "Selecting a Template" section on page 4-26, then create the account.

Step 2 In the Select Accounts section, select the method of user or group identification you will use: LDAP and/or IP address(es). (See Figure 4-9.) This selection must match the user identification method selected by going to Administration > Device Settings > User ID Settings.

Note If no users or groups display, the Domain Controller Agent may not be well configured.

Step 3 To select users:

- For LDAP identification, select the radio button for either the entire LDAP list or use the search function to find a specific name or group.
- For IP address identification, enter a range of IP addresses, a single IP address, or a host name.

Step 4 Click the user name, group name or IP address, and then click **Add** to add users, groups, or IP addresses to the **Selected** field.

Step 5 Click **Next** to continue creating your policy.

Step 6 Continue with the "Step 2: Specify Block Rule via Local List" page to create a blocking policy as described in "Blocking from the Via Local List Tab" section on page 4-7.

Step 7 Click **Finish**. The new policy displays in the policy list of the All Policies tab.

Allowing or Blocking Specific URLs

Blocking URLs, importing lists of blocked URLs, and exceptions to the blocking are described in the "Blocking from the Via Local List Tab" section on page 4-7. Format and other descriptions are available in the online help.

URL blocking is implemented in two ways:

- You define specific URLs to be blocked (via local list).
- URLs are blocked by the Trend Micro scan engine (via pattern file).

The "Step 2: Specify Block Rule via Local List" page is similar to Figure 4-3 and used in Step 6 of the Creating Accounts procedure. It allows you to specify sites that you want to allow or prohibit access to for specific users or groups in your organization via a local list.

Enabling a User/Group Blocking Policy

When the URL blocking function is disabled at the global level, end users can access any domains or URLs from your network via HTTP. When URL blocking is enabled at the global level, all users in your network are prevented from accessing certain domains and URLs. User/group policies allow you to select the domains and URLs that can be viewed by specific users or groups.

Note A URL Blocking policy can be enabled at the time of creation or later. For more information, see the "Selecting a Template" section on page 4-26.

To enable a URL Blocking Policy, perform the following steps:

Step 1 Verify that the URL Blocking feature is enabled at the global level by going to **Web (HTTP) > Global Settings > URL Blocking**.

Step 2 Go to the **Web (HTTP) > User Group Policies > All Policies** tab.

Step 3 Click the name of the policy to be enabled.

Step 4 Check the check box to immediately enable the policy.

Step 5 Click **Save**.

Step 6 Uncheck the check box to disable a policy and then click **Save**.

Editing a User/Group Blocking Policy

To edit a specific user group blocking policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > All Policies** tab**.**

Step 2 Click the blocking policy name.

Step 3 Edit the blocking policy on the Accounts and/or Via Local List tabs.

Step 4 Click **Save**.

Adding or Editing URL Filtering Policies for Users/Groups

URL Filtering for users/groups allows you to filter categories of websites such as “Adult” or “Social,” that specific users or groups of users can access. Site classification will vary from one organization to the next, depending on the business being conducted. For example, the sub-category “violence/hate crime” may not be work related in a manufacturing company, but may be defined as work related in a news reporting organization.

Some company prohibited sites may always be blocked (on the HTTP URL Filtering Rules screen) during both work time and leisure time, but if you want to allow employees to use chat sites during leisure time, you can specify those sites be blocked only during work time.

If a “Global Policy - URL Filtering” policy already exists, it was configured by going to Web (HTTP) > Global Settings > URL Filtering and was applied to all users. User or group policy will always have a higher priority than the global policy. Priority settings can be changed for user and group policy by going to Web (HTTP) > User Group Policies > URL Blocking & Filtering screen. Go to the far right column in the table that lists the policies, and click the up and down arrows to adjust the priority. Global policies will always have the lowest priority.

Prerequisites

Before a filtering policy can be added, the user must:

- Enable URL Filtering must be enabled on the global level by going to the Web (HTTP) > Global Settings > URL Filtering screen.
- Select a method of user/group identification by going to the Administration > Device Settings > User ID Settings screen. For more information, see the “Configuring User ID Settings” section on page 6-3.

- Download and install the Domain Controller agent. For more information, see the "Installing the Domain Controller Agent" section on page 6-6
- Add the Domain Controller Agent IP address.
- Auto-detect or manually add the Domain controller server.
- Configure the proxy setting by going to Update > Proxy Settings, if an HTTP proxy is required.

Note For URL Filtering to work properly, the CSC SSM must be able to send HTTP requests to the Trend Micro service.

Selecting a Template

To select a template for the first rule of a URL Filtering Policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > URL Blocking and Filtering (All policies** tab).

Step 2 Click **Add** and select **URL Filtering Rule**.

Step 3 Go to the Template section of the URL Filtering Policy: Add Policy screen, similar to what is shown in Figure 4-7.

Step 4 Select one of the following options:

- Create new policy
- Copy from an existing policy. If this option is chosen, use the drop-down list to select the policy to use as a template.

Step 5 Enter a descriptive policy name.

Step 6 Create an account according to the steps in the "Creating Accounts" section on page 4-26.

Creating Accounts

To create accounts, perform the following steps:

Step 1 Select a template according to the steps in "Selecting a Template" section on page 4-26.

Step 2 In the accounts section (similar to what is shown in Figure 4-9), select the method of user or group identification you will use: LDAP or IP address. This selection must match the user identification method selected by going to Administration > Device Settings > User ID Settings. Both methods of identification (LDAP and IP address) can be used if the identification method is configured correctly.

Step 3 To select users:

- For LDAP identification, select the radio button for either the entire LDAP list or use the search function to find a specific name or group.
- For IP address identification, enter a range of IP addresses, a single IP address, or a host name.

Step 4 Select the user name, group name, IP address or range of IP addresses, and then click **Add** to add users, groups or IP addresses to the Selected field.

Step 5 Click **Next**.

Step 6 Continue to the “Step 2: Specify the URL Filtering Rules” screen, using the instructions in “Filtering Rules, Exceptions, and Time” section on page 4-15.

Step 7 Click Finish. The new policy displays in the policy list of the All Policies tab.

Adding User Group Filtering Policy Rules

This screen allows you to define rules for user or group policies that allow or disallow access to categories, or parts of categories, of URLs during work or leisure time. The categories are:

- Computers/Bandwidth
- Computers/Harmful
- Computers/Communications
- Adults
- Business
- Social
- General

For information about how to set your policy rules, see the “Filtering Rules, Exceptions, and Time” section on page 4-15 and follow Steps 4 through 6.

Note Work and leisure time parameters are configured in the Web (HTTP) > Global Settings> URL Filtering screen. For more information, see the “Filtering Rules, Exceptions, and Time” section on page 4-15, step 10. Notification messages are configured in the Global Settings for URL Blocking. For more information, see the “URL Blocking Notifications” section on page 4-8.

Specifying Exceptions to the User Group Filtering Policy

The “URL Filtering Policy: Add Policy (Step 3: Specify Exceptions)” screen, similar to what is shown in Figure 4-6, allows you to identify URLs that are excluded from filtering. For example, you may have elected to assign the sub-category “shopping” to the work-time filtered category. However, your Finance Department needs access to URLs of certain vendors offering online shopping service to purchase office supplies, furniture, software, hardware and other business equipment, airline tickets, and so on. Identify those vendors as exceptions to allow access to their URLs.

For more information about how to set your policy rules, see the “Filtering Rules, Exceptions, and Time” section on page 4-15 and follow steps 7 through 9. Online help also provides detailed instructions.

Editing a User/Group Filtering Policy

To edit a specific user group filtering policy, perform the following steps:

Step 1 Go to the **Web (HTTP) > User Group Policies > All Policies** tab**.**

Step 2 Click the filtering policy name.

Step 3 Edit the filtering policy on the Accounts, Rules, and/or Exceptions tabs.

Step 4 Click **Save**.

Deleting a User Group Blocking or Filtering Policy

Policies can be deleted from the Web (HTTP) > User/Group Policies > URL Blocking & Filtering screen.

To delete a policy, perform the following steps:

Step 1 Check the check box at the beginning of the row for the policy to be deleted.

Step 2 Click the **Trashcan** icon to delete the policy. (See Figure 4-8.)

CHAPTER 5

Managing Updates and Log Queries

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

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^{SM} 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 new threats do not penetrate your network. To accomplish this, you can do the following:

- 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 managed components, either manually or via a schedule, are the following:

- Virus pattern file
- Virus scan engine
- Spyware pattern file (also includes patterns for other types of grayware)
- Anti-spam rules
- Anti-spam engine
- IntelliTrap pattern
- IntelliTrap exception pattern

The anti-spam rules and anti-spam engine are active and updated only if you have purchased the Plus License.

To determine if 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.

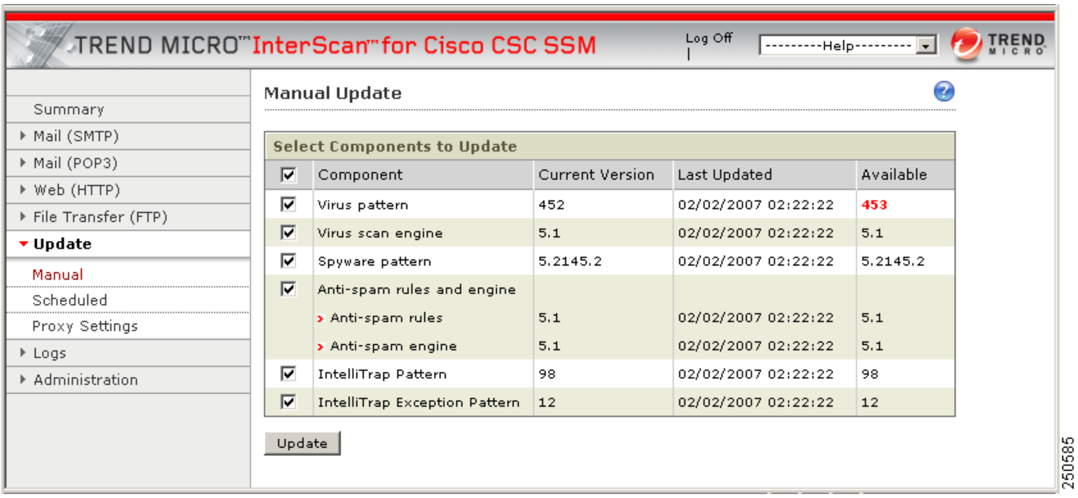
Manual Update

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

Step 1 Choose **Update > Manual**.

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

Figure 5-1 Manual Update Window



Manual Update

Select Components to Update

☑	Component	Current Version	Last Updated	Available
☑	Virus pattern	452	02/02/2007 02:22:22	453
☑	Virus scan engine	5.1	02/02/2007 02:22:22	5.1
☑	Spyware pattern	5.2145.2	02/02/2007 02:22:22	5.2145.2
☑	Anti-spam rules and engine			
	› Anti-spam rules	5.1	02/02/2007 02:22:22	5.1
	› Anti-spam engine	5.1	02/02/2007 02:22:22	5.1
☑	IntelliTrap Pattern	98	02/02/2007 02:22:22	98
☑	IntelliTrap Exception Pattern	12	02/02/2007 02:22:22	12

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 **Update > Scheduled** to view the Scheduled Update window.

Step 2 Check the “Enable Scheduled Update” check box.

Step 3 Choose the components to be updated according to the update schedule.

Step 4 Make the desired schedule changes.

Step 5 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 must specify a proxy server name or IP address and port during installation.

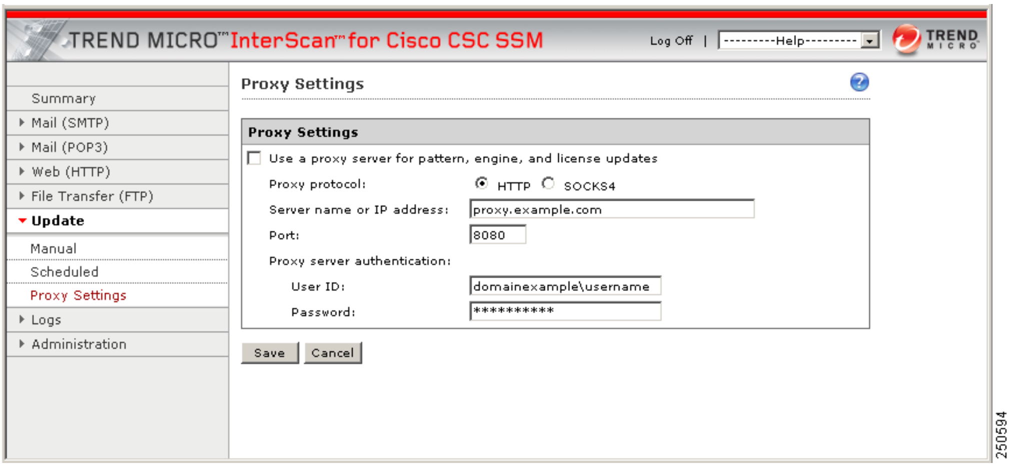
If you use a proxy server to access the Internet, you must enter the proxy server information into the CSC SSM before attempting to update components and Web Reputation queries. Any proxy information that you enter is used for both updating components from Trend Micro’s update servers and for product registration and licensing.

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**.

The Proxy Settings window appears.

Figure 5-2 Proxy Settings Window



Proxy Settings

Proxy Settings

☐ Use a proxy server for pattern, engine, and license updates

Proxy protocol: ● HTTP ○ SOCKS4

Server name or IP address: proxy.example.com

Port: 8080

Proxy server authentication:

User ID: domainexample\username

Password: **********

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 finish.

See the online help for more information about this feature.

Configuring Syslog Message Settings

After installation, log data such as virus and spyware or grayware detection are saved temporarily. To store log data, you must configure at least one syslog server. You may configure up to three syslog servers. For more information on specific syslog messages, see CSC SSM Syslog Messages, page A-1.

Configuring Syslog Servers

To configure syslog 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 the **Enable** check box, and then enter the syslog server IP address, port, and preferred protocol (either UDP or TCP).

Step 3 Click **Save**.

See the online help for more information about this feature.

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

Configuring Syslog Settings

Syslog settings may be configured by the syslog facility, syslog priority, and by selecting the logs that should be saved.

By default, detected security risks are logged. You can turn off logging for features you are not using. For example, if you purchased a Plus License, but do not want to log data for URL Filtering/Anti-Phishing and URL Blocking, uncheck those options.

To configure the syslog settings, perform the following steps:

Step 1 Choose **Logs > Settings**, and go to the Syslog Settings section.

Step 2 Choose a facility from the drop-down list to associate an identifier (local0 to local7) with the device you are configuring to the syslog server.

Step 3 Choose a priority settings from the drop-down list. This selection assigns a logging priority for the syslog server to consider when allocating resources for processing the system logs; the lowest priority is "debug," and the highest priority is "emerg" (emergency).

Step 4 Check the check boxes of the logs that should be saved. The options are shown in Table 5-1.

Table 5-1 Available Log Settings

Log Type	Available Logs
SMTP/POP3	• Anti-spam • Content Filtering • Email Reputation • IntelliTrap • Spyware/Grayware • Virus/Malware
HTTP	• Damage Cleanup Services • File Blocking • Spyware/Grayware • URL Blocking • URL Filtering/Anti-Phishing • Virus/Malware • Web Reputation
FTP	• File Blocking • Spyware/Grayware • Virus/Malware
Debug logs	• FTP • HTTP • Email

Step 5 Click **Save**.

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 need to purge these logs periodically.

Note Ad hoc queries are available through Trend Micro Control Manager. For more information, see Ad Hoc Queries, page C-8. Ad hoc queries allow users to search, sort and save CSC SSM data in a user-friendly format.

To view log data, perform the following steps:

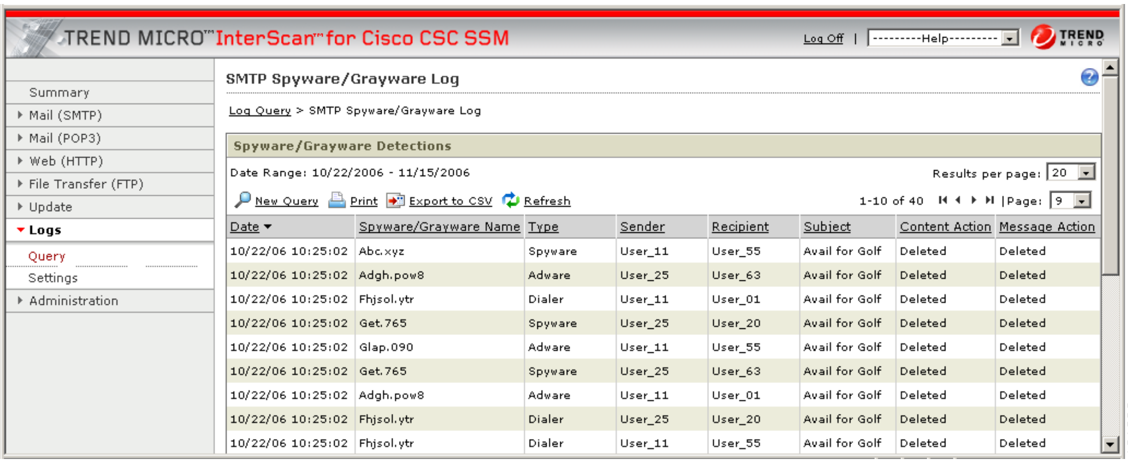
Step 1 Choose **Logs > Query** to display the Log Query window.

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

See the online help for more information about this feature and exporting logs.

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

Figure 5-3 SMTP Spyware/Grayware Log



SMTP Spyware/Grayware Log

Log Query > SMTP Spyware/Grayware Log

Spyware/Grayware Detections

Date Range: 10/22/2006 - 11/15/2006

Results per page: 20

1-10 of 40 |Page: 9

Date	Spyware/Grayware Name	Type	Sender	Recipient	Subject	Content Action	Message Action
10/22/06 10:25:02	Abc.xyz	Spyware	User_11	User_55	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Adgh.pow8	Adware	User_25	User_63	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Fhjsol.ytr	Dialer	User_11	User_01	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Get.765	Spyware	User_25	User_20	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Glap.090	Adware	User_11	User_55	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Get.765	Spyware	User_25	User_63	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Adgh.pow8	Adware	User_11	User_01	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Fhjsol.ytr	Dialer	User_25	User_20	Avail for Golf	Deleted	Deleted
10/22/06 10:25:02	Fhjsol.ytr	Dialer	User_11	User_55	Avail for Golf	Deleted	Deleted

Logging of Scanning Parameter Exceptions

Exceptions to the scanning parameters are specified in the following locations:

- Mail (SMTP)> Scanning > Incoming/Target tab
- Mail (SMTP)> Scanning > Outgoing/Target tab
- Mail (POP3) > Scanning/Target tab
- Web (HTTP) > Scanning/Target tab
- File Transfer (FTP) > Scanning/Target tab

Exceptions to the following scanning parameters 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 files).
- Password-protected files (if configured for deletion).

Note For HTTP and FTP only, an additional exception is 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:

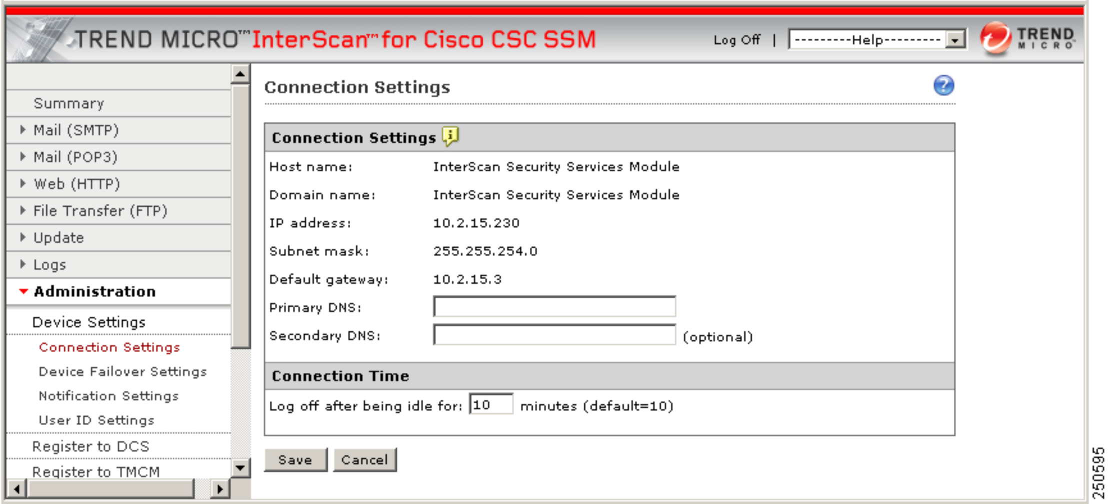
Configuring Connection Settings

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



Connection Settings

Connection Settings

Host name: InterScan Security Services Module
Domain name: InterScan Security Services Module
IP address: 10.2.15.230
Subnet mask: 255.255.254.0
Default gateway: 10.2.15.3
Primary DNS:
Secondary DNS: (optional)

Connection Time

Log off after being idle for: 10 minutes (default=10)

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

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

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 Choose 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.

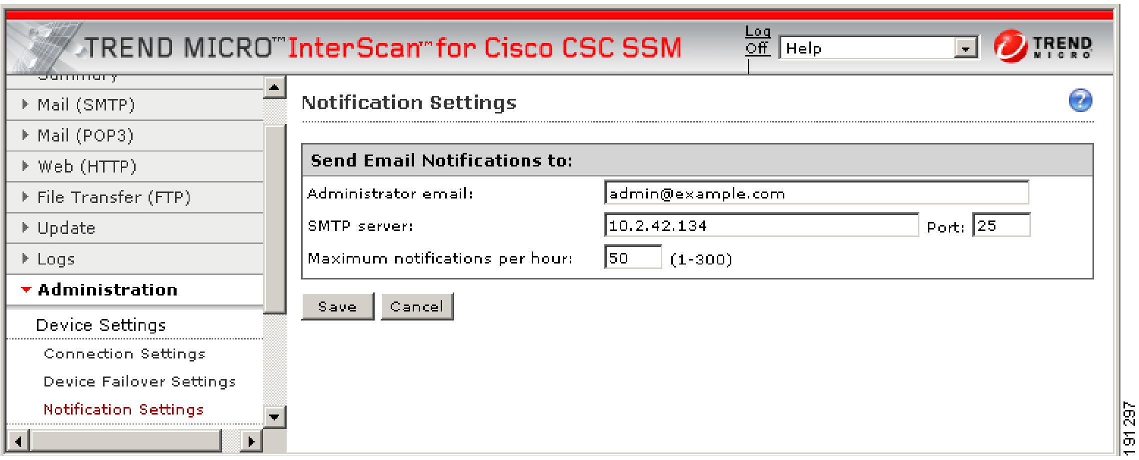
For more information, see the "Reimaging the CSC SSM" section on page B-5.

Managing Administrator E-mail and Notification Settings

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

- View or change the administrator e-mail address that you chose on the Host Configuration window during installation.
- View the SMTP server IP address and port you chose during installation on the Host Configuration window.
- Configure the maximum number of administrator notifications per hour.

Figure 6-2 Notification Settings Window



Notification Settings

Send Email Notifications to:

Administrator email: admin@example.com

SMTP server: 10.2.42.134 Port: 25

Maximum notifications per hour: 50 (1-300)

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 from the menu, choose **CSC Setup**.

Note For more information about the Register to DCS and Register to TMCM menu items, see Using CSC SSM with Trend Micro Damage Cleanup Services, page D-1 and Using CSC SSM with Trend Micro Control Manager, page C-1.

Configuring User ID Settings

The User Identification Settings allow you to identify individual users and groups in your organization making HTTP connections through CSC SSM. The domain user's identification allows you to:

- Identify the user roles
- Apply group HTTP access rules
- Create URL filtering and blocking policies that are user or group specific

The Trend Micro Domain Controller Agent offers transparent user identification for users in a Windows-based directory service. The Domain Controller Agent communicates with the Domain Controller to gather up-to-date user logon information and provide it to the CSC SSM. This information can be used to create URL filtering and blocking policies applied to specific users and groups.

The User Identification page includes the following information:

- Selecting the User Identification Method, page 6-4
- Configuring the Cache Time Limitations, page 6-5
- About the Domain Controller Agent, page 6-5
- Adding Domain Controller Server Credentials, page 6-10

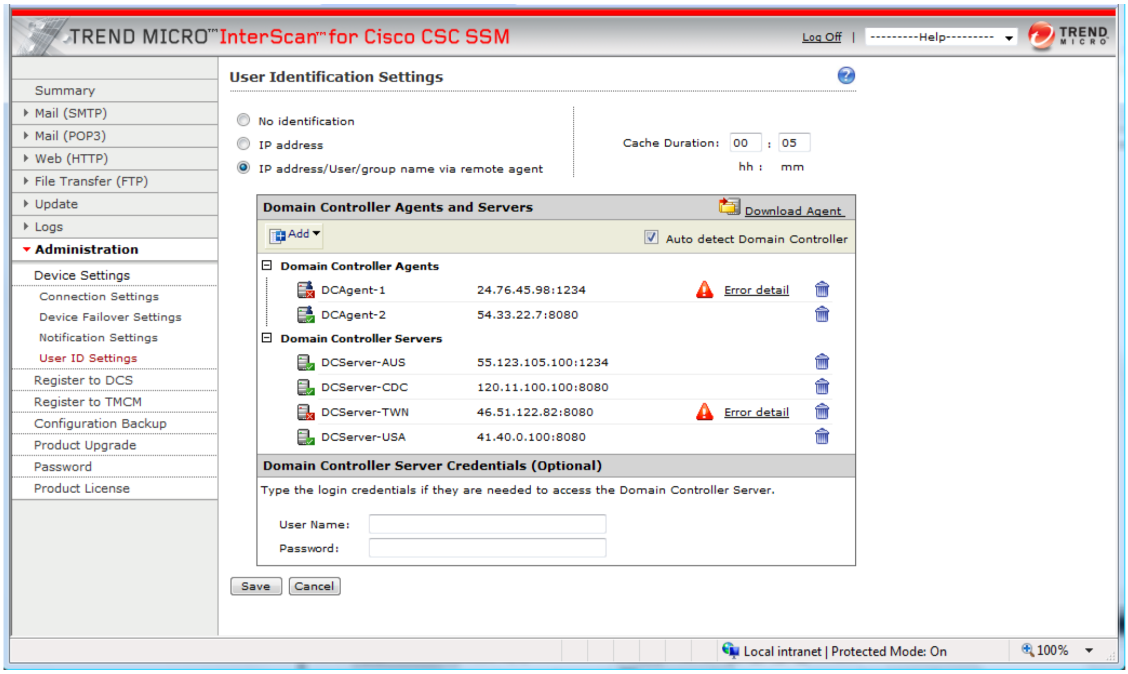
Selecting the User Identification Method

You can identify users through IP addresses or by user/group names via proxy authorization, as shown in Figure 6-3.

Identifying users enables you to do the following:

- Set up user and group policies for URL Filtering and Blocking
- Display user information in the violation logs
- Have domain name and account information appear in the HTTP debugging log

Figure 6-3 User Identification Settings



User Identification Settings

○ No identification
○ IP address
● IP address/User/group name via remote agent

Cache Duration: 00 : 05
hh : mm

Domain Controller Agents and Servers Download Agent

Add ☑ Auto detect Domain Controller

⊟ **Domain Controller Agents**

DCAgent-1	24.76.45.98:1234	Error detail	
DCAgent-2	54.33.22.7:8080		

⊟ **Domain Controller Servers**

DCServer-AUS	55.123.105.100:1234		
DCServer-CDC	120.11.100.100:8080		
DCServer-TWN	46.51.122.82:8080	Error detail	
DCServer-USA	41.40.0.100:8080		

Domain Controller Server Credentials (Optional)

Type the login credentials if they are needed to access the Domain Controller Server.

User Name:
Password:

Save Cancel

To configure the user identification settings, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 Select one of the following radio buttons:

- No identification — No user or group identification is used for the connection and the global user policy applies.
- IP address — Users will be identified by an IP address.
- IP address/User/group name via remote agent — Using this setting allows you to identify both individual users and groups, by name (first) or IP address (second). Requires configuring the Domain Controller agent and server.

Step 3 Perform the steps in the cache time limitation procedure listed in Configuring the Cache Time Limitations, page 6-5.

Configuring the Cache Time Limitations

The cache settings pertain to the amount of time that the IP address remains associated with a user without re-verification. The time value you set for caching specifies how often the Domain Controller agent should verify that a particular IP address is still associated with a specific user.

Note Cache configuration is only necessary if you elect to use **IP address/User/group name via remote agent** as the method of user identification.

To identify the cache duration, perform the following steps:

Step 1 Enter the hours and minutes values to define the length of time that cached information will associate an IP address with a specific user. By default, the client IP address is reverified every 15 minutes.

```
Example:
    Cache duration: 24: (hh) 00: (mm)
```

Step 2 Install the Domain Controller Agent as shown in Installing the Domain Controller Agent, page 6-6.

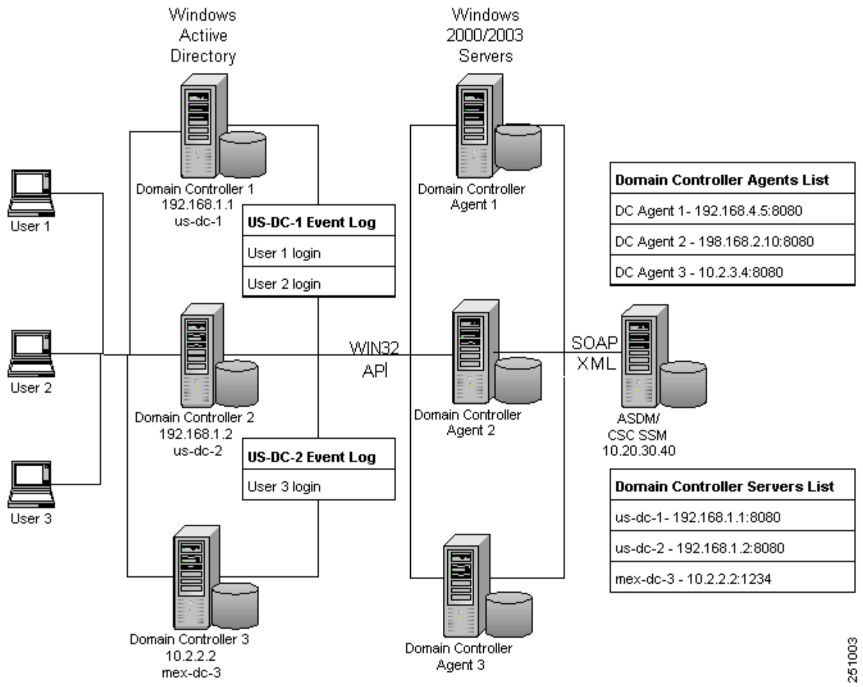
About the Domain Controller Agent

The Trend Micro Domain Controller Agent queries each domain controller for user login sessions every ten seconds by default, obtaining the user name and workstation name for each login session. For each login session identified, the Domain Controller Agent performs a DNS lookup to resolve the workstation name to an IP address, and records the resulting user name/IP address pair.

The Domain Controller Agent uses the Win32 API to communicate with the Domain Controller server and SOAP/XML to transmit login data to the CSC SSM. The user data that Domain Controller Agent sends to CSC SSM software components equals about 80 bytes per user name/IP address pair. On average, the Domain Controller Agent uses 8-10 MB of RAM, but this varies according to the number of login sessions per network Domain Controller.

CSC SSM supports up to 32 Domain Controllers, and up to eight Domain Controller Agents can be assigned to CSC SSM. Having multiple agents provides redundancy. If one agent goes down, another agent will act as backup. Although eight Domain Controller Agents can be assigned to CSC SSM, only two or three would be necessary in most network configurations.

Figure 6-4 Network Configuration for Domain Controller Agent Installation


Windows Actiive Directory
Windows 2000/2003 Servers
User 1
User 2
User 3
Domain Controller 1 192.168.1.1 us-dc-1
Domain Controller 2 192.168.1.2 us-dc-2
Domain Controller 3 10.2.2.2 mex-dc-3
Domain Controller Agent 1
Domain Controller Agent 2
Domain Controller Agent 3
WIN32 API
SOAP XML
ASDM/ CSC SSM 10.20.30.40
251003

US-DC-1 Event Log
User 1 login
User 2 login

US-DC-2 Event Log
User 3 login

Domain Controller Agents List
DC Agent 1 - 192.168.4.5:8080
DC Agent 2 - 198.168.2.10:8080
DC Agent 3 - 10.2.3.4:8080

Domain Controller Servers List
us-dc-1 - 192.168.1.1:8080
us-dc-2 - 192.168.1.2:8080
mex-dc-3 - 10.2.2.2:1234

Installing the Domain Controller Agent

Trend Micro recommends installing the Domain Controller Agents on the Domain Controller server, if your company policy allows it. Domain Controller Agents can also be installed on a separate server, if needed.

If possible, the Domain Controller Agent should be installed on a Windows 2003 server, separate from both the Domain Controller and the ASDM/CSC SSM machines. Windows 2003 servers support the CSC SSM auto-discovery feature for all Windows Active Directory Domain Controller servers, whether they are running on Windows 2000 or Windows 2003 servers. If the Domain Controller Agent is installed on a Windows 2000 server, the agent will work, but auto-discovery of Domain Controllers is not supported and the location of the Domain Controllers must be added manually to the CSC SSM, as discussed in Adding A Domain Controller Agent or Server to CSC SSM, page 6-7.

After installation, Domain Controller Agents will poll Domain Controllers every ten seconds for new logon information. The logon information is then used to configure and enforce URL Filtering and Blocking policies for users and groups.

To install the Domain Controller Agent, perform the following steps:

Step 1 Before installation, verify that logging is enabled for logon events. If it is not, the Domain Controller Agent cannot access user information from the Domain Controller logs.

a. To enable 672/673 logon events in the Domain Controller event log, choose **Start > Administrative Tools > Domain Controller Security Policy** on each Domain Controller machine.

b. Choose **Security Settings > Local Policies > Audit Policy**.

c. Define the policy setting for “Audit Account logon events” policy (audit success).

Step 2 Log in with Domain Controller privileges (and administrator privileges) to the server (Windows 2000 or Windows 2003) on which the Domain Controller Agent will be installed.

Step 3 Access the CSC SSM UI at: http://<CSC SSM IP address:port_number> and log in.

Step 4 Choose **Administration > Device Settings > User ID Settings**.

Step 5 Click the **Download Agent** link and follow the on-screen instructions.

a. Click **Run** or **Save**.

Note This operation is fully supported in Internet Explorer™ 6.0 or later. If you are using Mozilla Firefox™, you can only save, not run, the installation.

- If you choose **Run**, the agent installation will be saved to a temp folder and launched.
- If you choose **Save**, you will need to launch it later manually.

Note To launch the agent installer later, browse to the folder in which it was saved and double-click the file named “IdAgentInst.msi”.

b. In the Setup wizard, click **Next**.

c. Check the license agreement check box and click **Next**.

d. Click **Next** in the Destination folder screen.

Note The destination folder cannot be changed. The installer auto-detects the appropriate system drive.

e. Click **Install**. A progress bar displays.

f. Click **Finish** when the setup is complete.

Step 6 Repeat Step 1 through Step 5 for additional installations of Domain Controller Agents. A maximum of eight Domain Controller Agents can point to one CSC SSM.

Step 7 Add the Domain Controller Agent and Domain Controller to CSC SSM according to the procedure listed in Adding A Domain Controller Agent or Server to CSC SSM, page 6-7.

Step 8 Add the Domain Controller log on credentials according to the procedure listed in Adding Domain Controller Server Credentials, page 6-10.

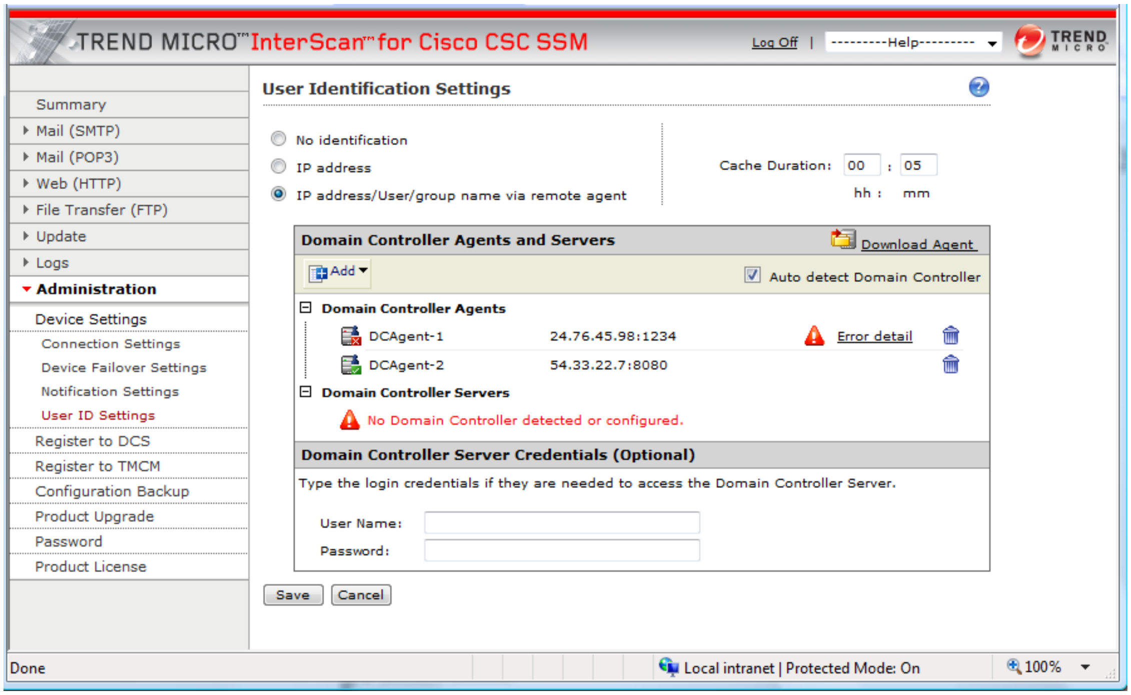
Adding A Domain Controller Agent or Server to CSC SSM

CSC SSM requires that the Domain Controller agents and servers be added to the CSC SSM to permit URL Filtering and Blocking policies that are user or group specific.

- Adding Domain Controller Agents allows the CSC SSM to access user logon information from the Domain Controller Agent.
- Adding the Domain Controller server provides information to the Domain Controller Agent, which accesses the Domain Controller logon events to retrieve user information.

Domain Controller Agents must be added manually. Domain Controllers can be added manually or automatically detected. If the auto-detect feature is enabled, Domain Controller Servers may still be added manually.

Figure 6-5 No Domain Controller Servers Detected



User Identification Settings

○ No identification
○ IP address
● IP address/User/group name via remote agent

Cache Duration: 00 : 05
hh : mm

Domain Controller Agents and Servers

☑ Auto detect Domain Controller

⊟ Domain Controller Agents

DCAgent-1	24.76.45.98:1234	Error detail
DCAgent-2	54.33.22.7:8080	

⊟ Domain Controller Servers

No Domain Controller detected or configured.

Domain Controller Server Credentials (Optional)

Type the login credentials if they are needed to access the Domain Controller Server.

User Name:

Password:

Auto-detecting a Domain Controller Server

To auto-detect a Domain Controller Server, perform the following steps:

Step 1 Check the **Auto detect Domain Controller servers** check box.

Step 2 Verify that the detected Domain Controller servers display in the Domain Controller servers list.

Note The auto-detect feature is only available for Domain Controller Agents installed on Windows 2003 servers. (Windows 2000 servers are not supported.) All Windows Active Directory Domain Controller servers will be auto-detected, whether they are on Windows 2003 or Windows 2000 servers.

After configuring the Domain Controller Agent on CSC SSM, the same configuration will be automatically propagated to the failover CSC SSM device(s).

Adding a Domain Controller Agent or Server Manually

To manually add a Domain Controller agent or server, perform the following steps:

Step 1 Click the **Add** icon in the Domain Controller Agents and Servers section, shown in Figure 6-3.

Step 2 Click **Agent** or **Server**, depending on what you need to add.

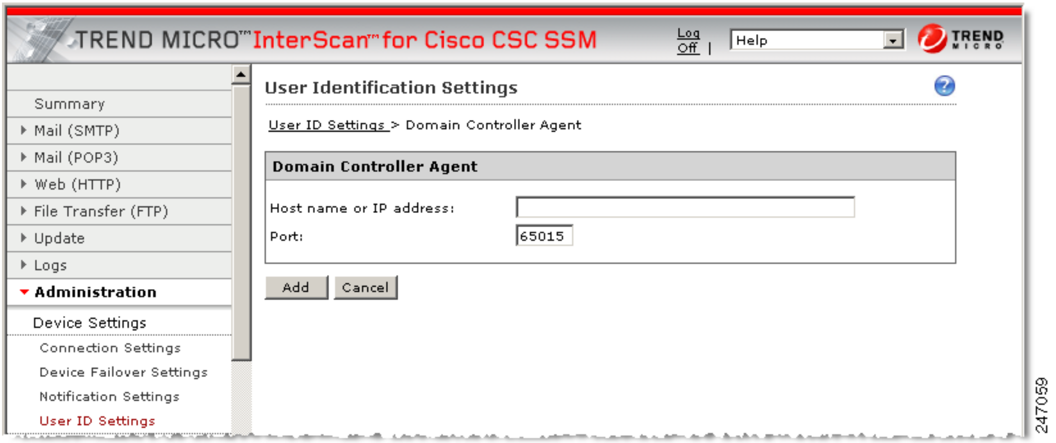
Step 3 For a Domain Controller Agent, type the following information:

- Host name or IP address — The host name or IP address of the machine where the Domain Controller Agent is installed. (See Figure 6-6.)
- Port number — The port number of the machine on which the Domain Controller Agent is installed (The default port number 65015 is specified in the IdAgent.ini file ([Setting]/AgentPort parameter).

Step 4 Click **Save**.

The Domain Controller Agent name appears in the list shown in Figure 6-3.

Figure 6-6 Add a Domain Controller Agent



User Identification Settings

User ID Settings > Domain Controller Agent

Domain Controller Agent

Host name or IP address:

Port: 65015

Step 5 For a Domain Controller Server, add the following information:

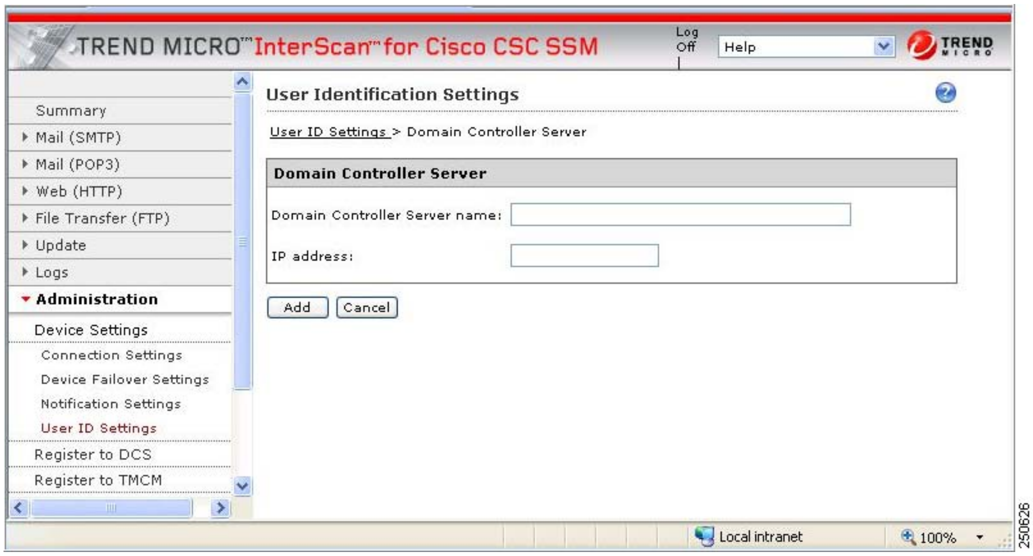
> **Note** If the auto-detection method of adding Domain Controllers was used, do not add them manually.

- Server Name — A descriptive name given to identify a specific Domain Controller server, not necessarily the machine name
- Server IP address — The IP address of the Domain Controller server (See Figure 6-7.)

The server name appears in the list shown in Figure 6-3.

Step 6 Click **Save**.

Figure 6-7 Add a Domain Controller Server



Domain Controller Server name:

IP address:

Step 7 To add Domain Controller Server credentials, see Adding Domain Controller Server Credentials, page 6-10.

After configuring the Domain Controller Agent on CSC SSM, the same configuration will be automatically propagated to the failover CSC SSM device(s).

Deleting a Domain Controller Agent or Server

To remove a Domain Controller agent or server from the list, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 Find the agent or server in the list.

Step 3 Click the trash can icon next to the name.

Step 4 Click **Save**.

Note To uninstall the Domain Controller Agent, go to the machine on which it was installed. Choose **Start > Settings > Control Panel > Add or Remove Programs**.

Adding Domain Controller Server Credentials

Adding Domain Controller server credentials allows single sign-on, offering one-time authentication.

If the Domain Controller Agent is installed on a Windows machine, where the local system account does not have the permission to access the domain controller, the CSC SSM will not be able to query domain users and groups. The CSC SSM user can enter the domain controller credential in the user name and password fields of the Domain Controller Server Credentials section of the screen shown in Figure 6-5 to enable access.

Note It is important that all Domain Controller servers share the same user name and password credentials if the credentials are entered on this screen.

Domain Controller Agent installation requires administrator privileges. If the Domain Controller Agent was installed by the domain administrator, then the agent service has domain administrator privileges. In that case, the user does not have to set the server credentials from the CSC SSM console.

To add Domain Controller server credentials, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 Go to the **Domain Controller Server Credentials** section at the bottom of the screen. (See Figure 6-3.)

Step 3 Type the user name in the **domain name\username** format.

Note The user name added here must be a domain user with the privilege to access the Domain Controller server event log.

Step 4 Type the password.

Step 5 Click **Save**.

Backing Up Configuration Settings

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

- Exporting a Configuration, page 6-12
- Importing a Configuration, page 6-12

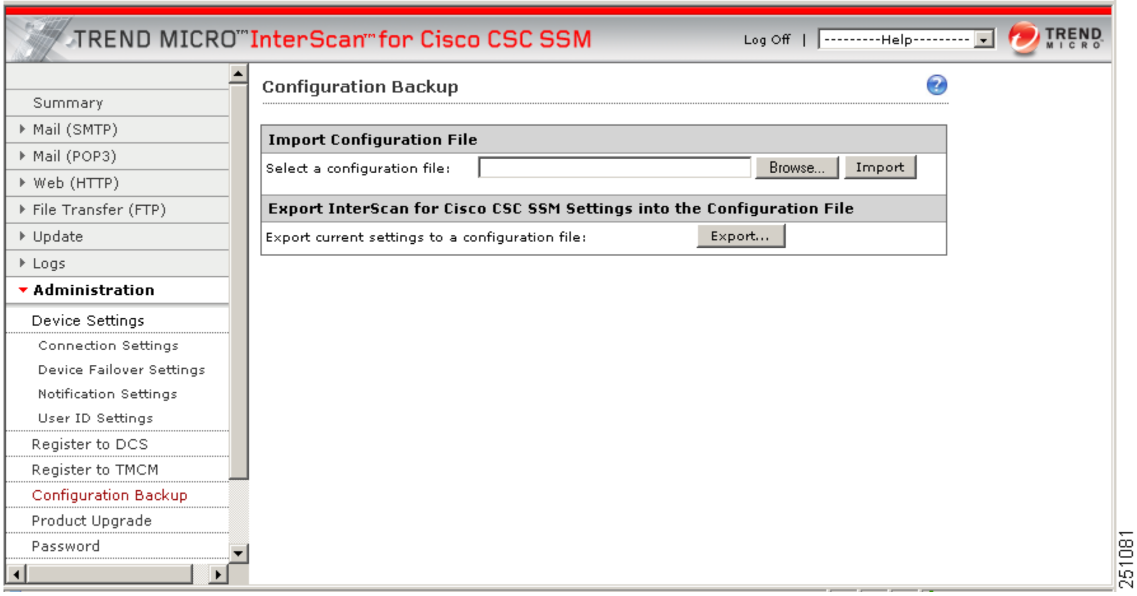
Trend Micro InterScan for Cisco CSC SSM provides the ability to back up your device configuration settings and save them in a compressed file. You can import the saved configuration settings and restore your system to those settings configured at the time of the save.

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 8-5 and Modifying the Password-reset Policy, page B-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 6-8.

Figure 6-8 Configuration Backup Window with Successful Import Confirmation



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 Table 6-1 to configure the failover peer. Print a copy of the checklist that you can use to record your progress.

Table 6-1 Configuring Failover Settings Checklist

Step 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: **IP Address:** ______________________ ______________________	❑ ❑
Step 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**.	❑
Step 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**.	❑
Step 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.	❑

Step 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.`
		❑

Step 6	On the Device Failover Settings window for the primary device, click **Synchronize to peer**. 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: 04/29/2007 15:20:11`	❑

Caution Be sure you do not click **Synchronize to 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 Installing Product Upgrades.

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

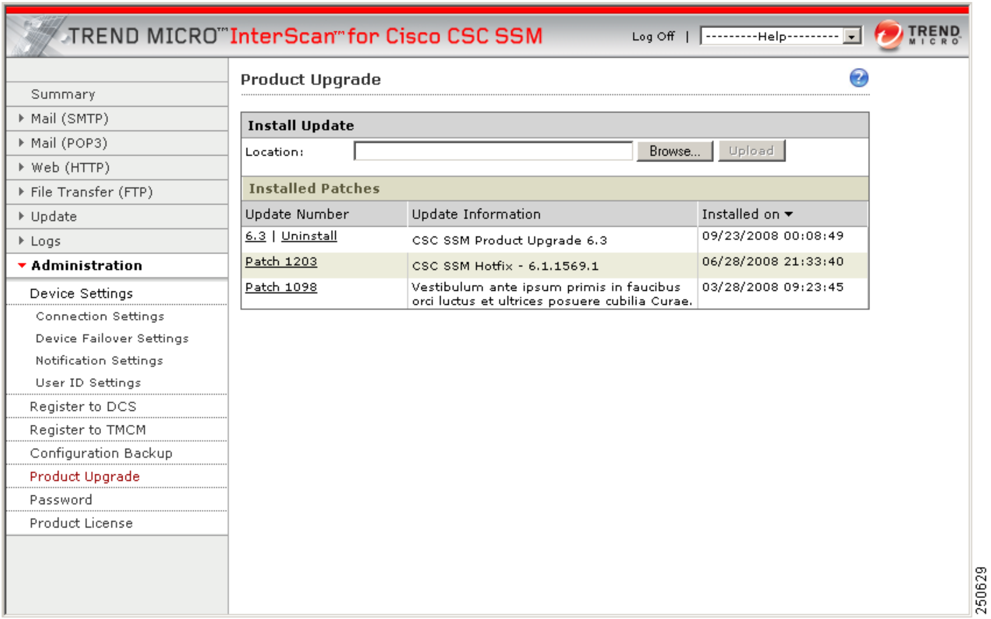
From time to time, a product upgrade becomes available that corrects a known issue or offers new functionality.

To install a product upgrade, perform the following steps:

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 6-9.

Figure 6-9 Product Upgrade Window



Product Upgrade

Install Update

Location: Browse... Upload

Installed Patches

Update Number	Update Information	Installed on ▾
6.3 | Uninstall	CSC SSM Product Upgrade 6.3	09/23/2008 00:08:49
Patch 1203	CSC SSM Hotfix - 6.1.1569.1	06/28/2008 21:33:40
Patch 1098	Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae.	03/28/2008 09:23:45

⚠ **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.

Step 3 Click **Browse** and locate the upgrade file.

Step 4 Click **Upload** to upload and install the upgrade.

The version number displays under the Update Number column if the upgrade is successful.

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

Viewing the Product License

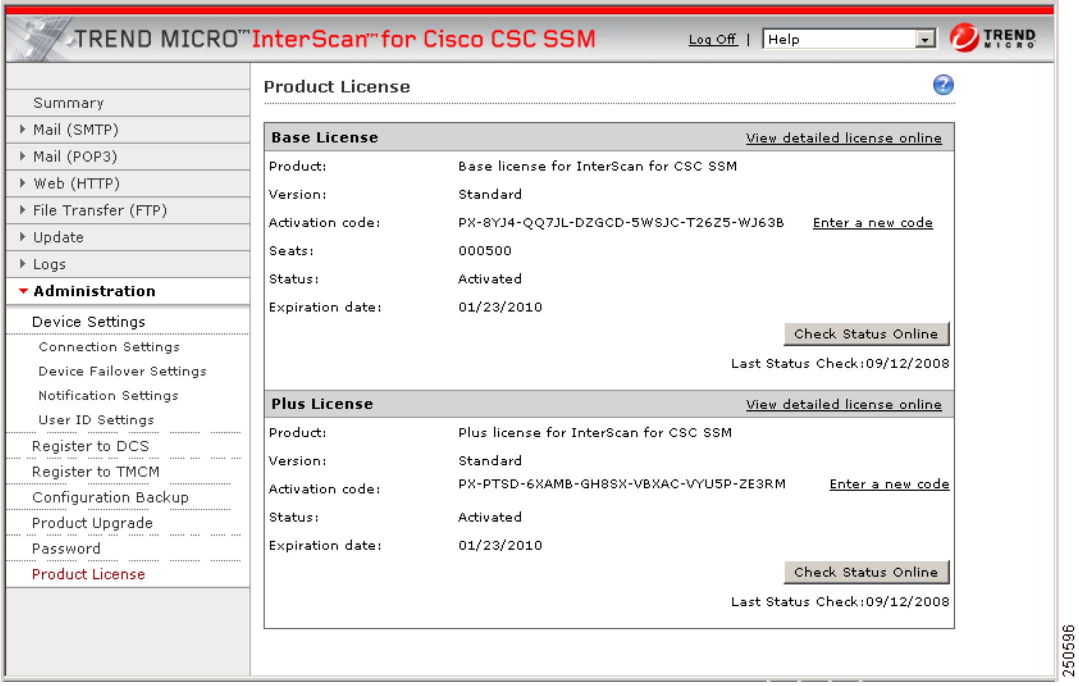
This section describes product licensing information, and includes the following topics:

- License Expiration, page 6-16
- Licensing Information Links, page 6-17
- Renewing a License, page 6-17

The Product License window (shown in Figure 6-10) allows you to view the status of your product license, which includes the following information:

- 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 6-10 Product License Window



Product License

Base License View detailed license online

Product:	Base license for InterScan for CSC SSM
Version:	Standard
Activation code:	PX-8YJ4-QQ7JL-DZGCD-5WSJC-T26Z5-WJ63B Enter a new code
Seats:	000500
Status:	Activated
Expiration date:	01/23/2010

Check Status Online

Last Status Check:09/12/2008

Plus License View detailed license online

Product:	Plus license for InterScan for CSC SSM
Version:	Standard
Activation code:	PX-PTSD-6XAMB-GH8SX-VBXAC-VYU5P-ZE3RM Enter a new code
Status:	Activated
Expiration date:	01/23/2010

Check Status Online

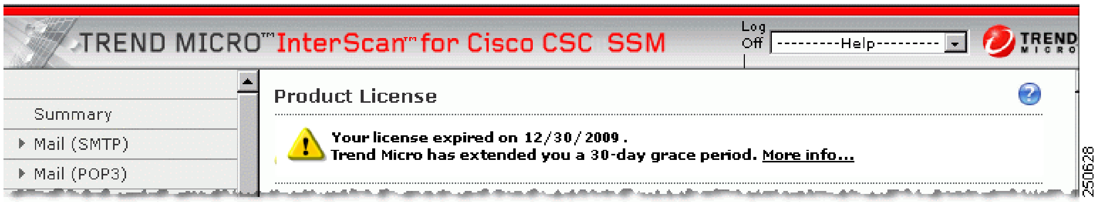
Last Status Check:09/12/2008

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 6-11.

Figure 6-11 License Expiration Message



Product License

Your license expired on 12/30/2009 .
Trend Micro has extended you a 30-day grace period. More info...

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** button to display a message below the button 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.

Note For information about product activation, see the *Cisco Security Appliance Configuration Guide using ASDM*.

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:

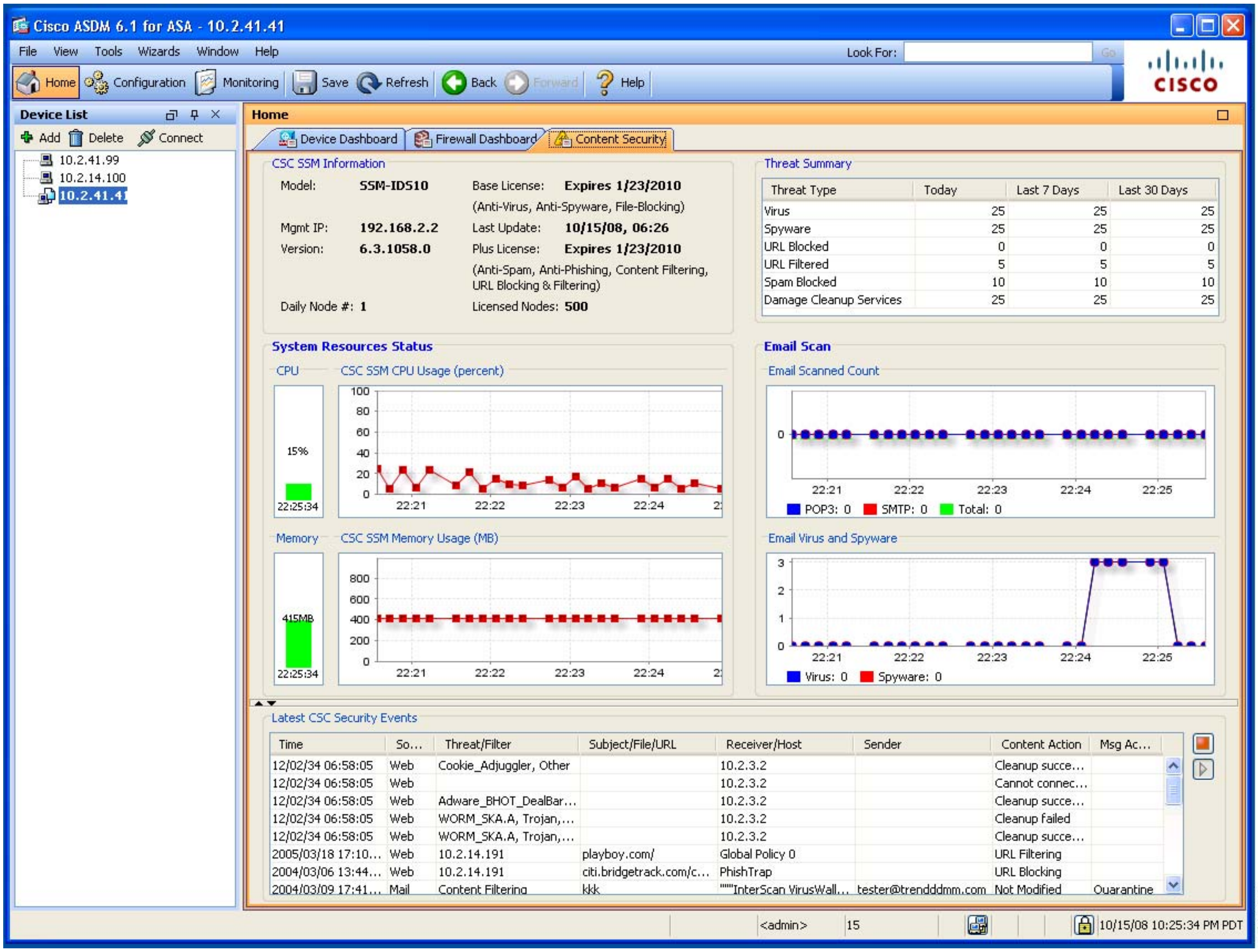
- Features of the Content Security Tab, page 7-1
- Monitoring Content Security, page 7-2

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



CSC SSM Information

Model:	SSM-ID510	Base License:	Expires 1/23/2010
			(Anti-Virus, Anti-Spyware, File-Blocking)
Mgmt IP:	192.168.2.2	Last Update:	10/15/08, 06:26
Version:	6.3.1058.0	Plus License:	Expires 1/23/2010
			(Anti-Spam, Anti-Phishing, Content Filtering, URL Blocking & Filtering)
Daily Node #:	1	Licensed Nodes:	500

Threat Summary

Threat Type	Today	Last 7 Days	Last 30 Days
Virus	25	25	25
Spyware	25	25	25
URL Blocked	0	0	0
URL Filtered	5	5	5
Spam Blocked	10	10	10
Damage Cleanup Services	25	25	25

Latest CSC Security Events

Time	So...	Threat/Filter	Subject/File/URL	Receiver/Host	Sender	Content Action	Msg Ac...
12/02/34 06:58:05	Web	Cookie_Adjuggler, Other		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web			10.2.3.2		Cannot connec...	
12/02/34 06:58:05	Web	Adware_BHOT_DealBar...		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan,...		10.2.3.2		Cleanup failed	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan,...		10.2.3.2		Cleanup succe...	
2005/03/18 17:10...	Web	10.2.14.191	playboy.com/	Global Policy 0		URL Filtering	
2004/03/06 13:44...	Web	10.2.14.191	citi.bridgetrack.com/c...	PhishTrap		URL Blocking	
2004/03/09 17:41...	Mail	Content Filtering	kkk	"""InterScan VirusWall...	tester@trenddmm.com	Not Modified	Quarantine

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

Monitoring Content Security

This section describes how to monitor content security, and includes the following topics:

- Monitoring Threats, page 7-3
- Monitoring Live Security Events, page 7-5
- Monitoring Software Updates, page 7-6
- Monitoring Resources, page 7-7

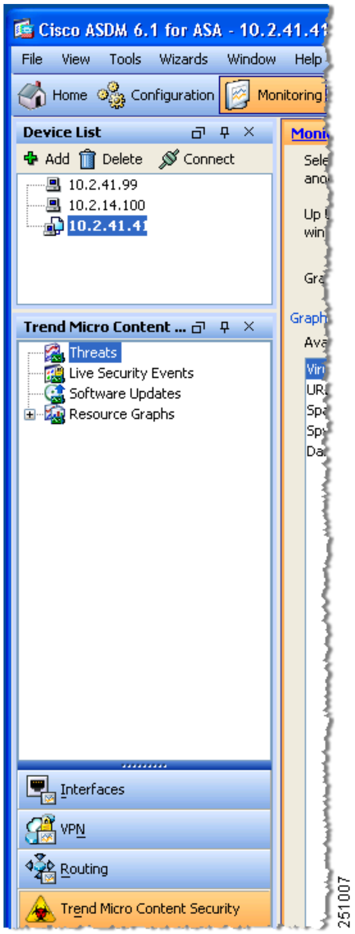
To display the content security monitoring settings for recent threat activity, perform the following steps:

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

Step 2 Choose 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, perform 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.

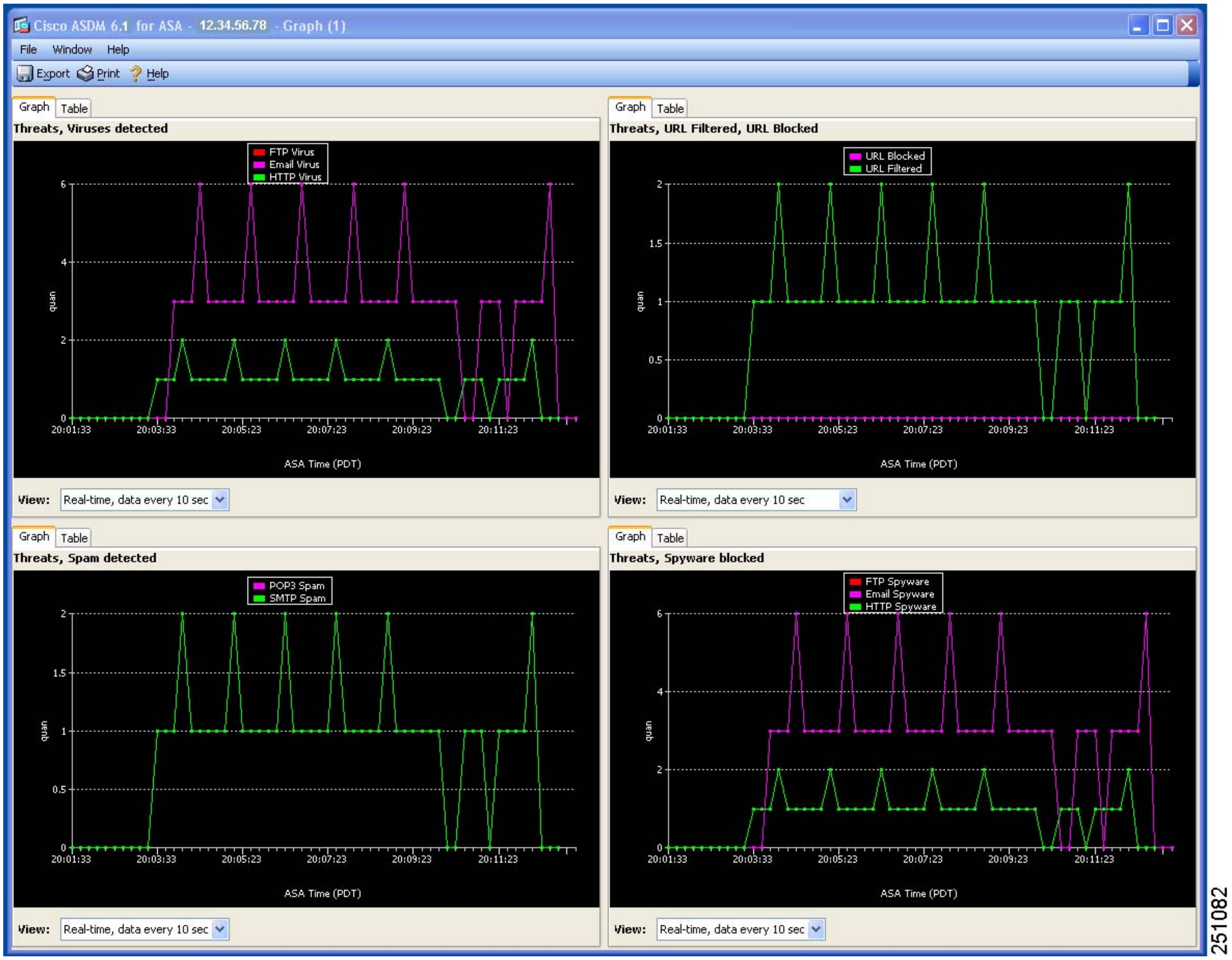
Step 2 To display recent activity, choose one or more of the following categories:

- 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 the Base license 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



View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

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.

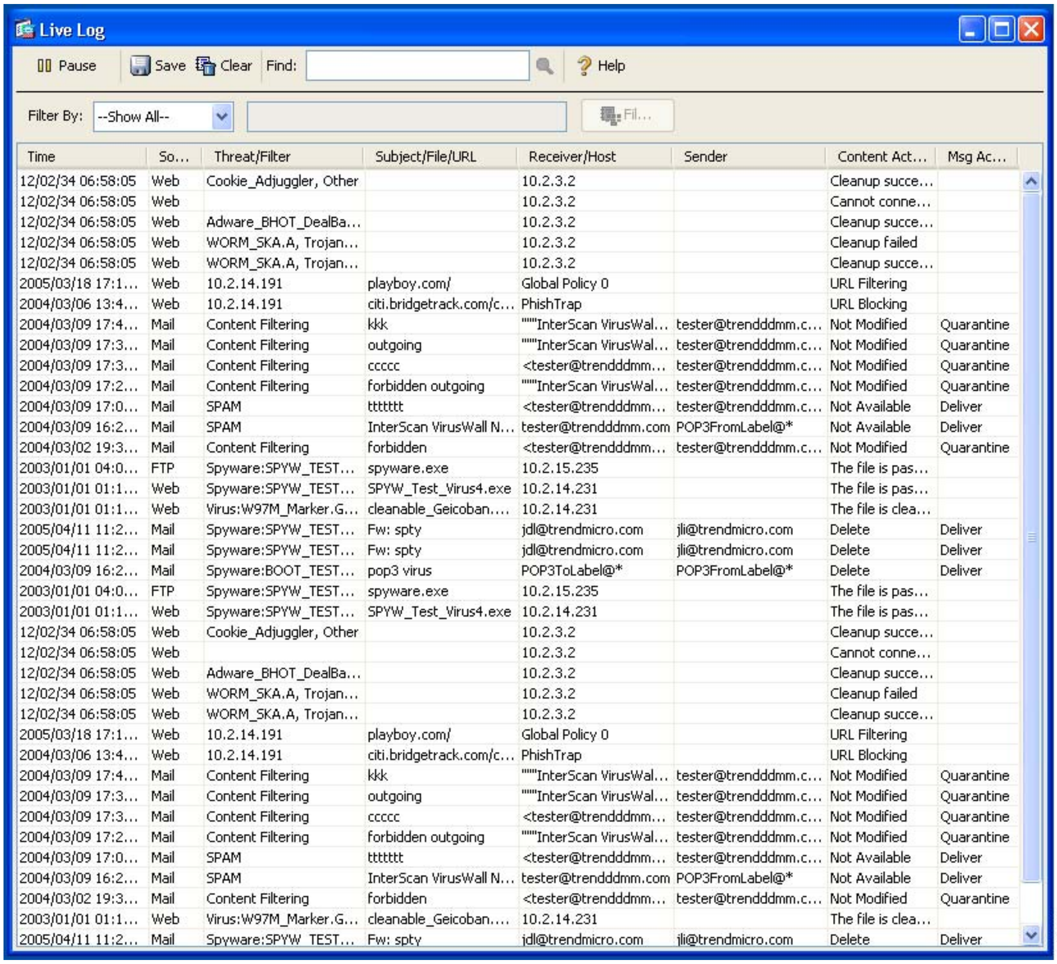
Monitoring Live Security Events

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 shown in Figure 7-4.

Figure 7-4 Live Security Events Report



Time	So...	Threat/Filter	Subject/File/URL	Receiver/Host	Sender	Content Act...	Msg Ac...
12/02/34 06:58:05	Web	Cookie_Adjuggler, Other		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web			10.2.3.2		Cannot conne...	
12/02/34 06:58:05	Web	Adware_BHOT_DealBa...		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan...		10.2.3.2		Cleanup failed	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan...		10.2.3.2		Cleanup succe...	
2005/03/18 17:1...	Web	10.2.14.191	playboy.com/	Global Policy 0		URL Filtering	
2004/03/06 13:4...	Web	10.2.14.191	citi.bridgetrack.com/c...	PhishTrap		URL Blocking	
2004/03/09 17:4...	Mail	Content Filtering	kkk	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:3...	Mail	Content Filtering	outgoing	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:3...	Mail	Content Filtering	ccccc	<tester@trenddmm...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:2...	Mail	Content Filtering	forbidden outgoing	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:0...	Mail	SPAM	ttttttt	<tester@trenddmm...	tester@trenddmm.c...	Not Available	Deliver
2004/03/09 16:2...	Mail	SPAM	InterScan VirusWall N...	tester@trenddmm.com	POP3FromLabel@*	Not Available	Deliver
2004/03/02 19:3...	Mail	Content Filtering	forbidden	<tester@trenddmm...	tester@trenddmm.c...	Not Modified	Quarantine
2003/01/01 04:0...	FTP	Spyware:SPYW_TEST...	spyware.exe	10.2.15.235		The file is pas...	
2003/01/01 01:1...	Web	Spyware:SPYW_TEST...	SPYW_Test_Virus4.exe	10.2.14.231		The file is pas...	
2003/01/01 01:1...	Web	Virus:W97M_Marker.G...	cleanable_Geicoban....	10.2.14.231		The file is clea...	
2005/04/11 11:2...	Mail	Spyware:SPYW_TEST...	Fw: spty	jdl@trendmicro.com	jli@trendmicro.com	Delete	Deliver
2005/04/11 11:2...	Mail	Spyware:SPYW_TEST...	Fw: spty	jdl@trendmicro.com	jli@trendmicro.com	Delete	Deliver
2004/03/09 16:2...	Mail	Spyware:BOOT_TEST...	pop3 virus	POP3ToLabel@*	POP3FromLabel@*	Delete	Deliver
2003/01/01 04:0...	FTP	Spyware:SPYW_TEST...	spyware.exe	10.2.15.235		The file is pas...	
2003/01/01 01:1...	Web	Spyware:SPYW_TEST...	SPYW_Test_Virus4.exe	10.2.14.231		The file is pas...	
12/02/34 06:58:05	Web	Cookie_Adjuggler, Other		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web			10.2.3.2		Cannot conne...	
12/02/34 06:58:05	Web	Adware_BHOT_DealBa...		10.2.3.2		Cleanup succe...	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan...		10.2.3.2		Cleanup failed	
12/02/34 06:58:05	Web	WORM_SKA.A, Trojan...		10.2.3.2		Cleanup succe...	
2005/03/18 17:1...	Web	10.2.14.191	playboy.com/	Global Policy 0		URL Filtering	
2004/03/06 13:4...	Web	10.2.14.191	citi.bridgetrack.com/c...	PhishTrap		URL Blocking	
2004/03/09 17:4...	Mail	Content Filtering	kkk	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:3...	Mail	Content Filtering	outgoing	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:3...	Mail	Content Filtering	ccccc	<tester@trenddmm...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:2...	Mail	Content Filtering	forbidden outgoing	""""InterScan VirusWal...	tester@trenddmm.c...	Not Modified	Quarantine
2004/03/09 17:0...	Mail	SPAM	ttttttt	<tester@trenddmm...	tester@trenddmm.c...	Not Available	Deliver
2004/03/09 16:2...	Mail	SPAM	InterScan VirusWall N...	tester@trenddmm.com	POP3FromLabel@*	Not Available	Deliver
2004/03/02 19:3...	Mail	Content Filtering	forbidden	<tester@trenddmm...	tester@trenddmm.c...	Not Modified	Quarantine
2003/01/01 01:1...	Web	Virus:W97M_Marker.G...	cleanable_Geicoban....	10.2.14.231		The file is clea...	
2005/04/11 11:2...	Mail	Spyware:SPYW_TEST...	Fw: spty	jdl@trendmicro.com	jli@trendmicro.com	Delete	Deliver

This report lists events that the CSC SSM detected. The Source column displays “Mail” 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.

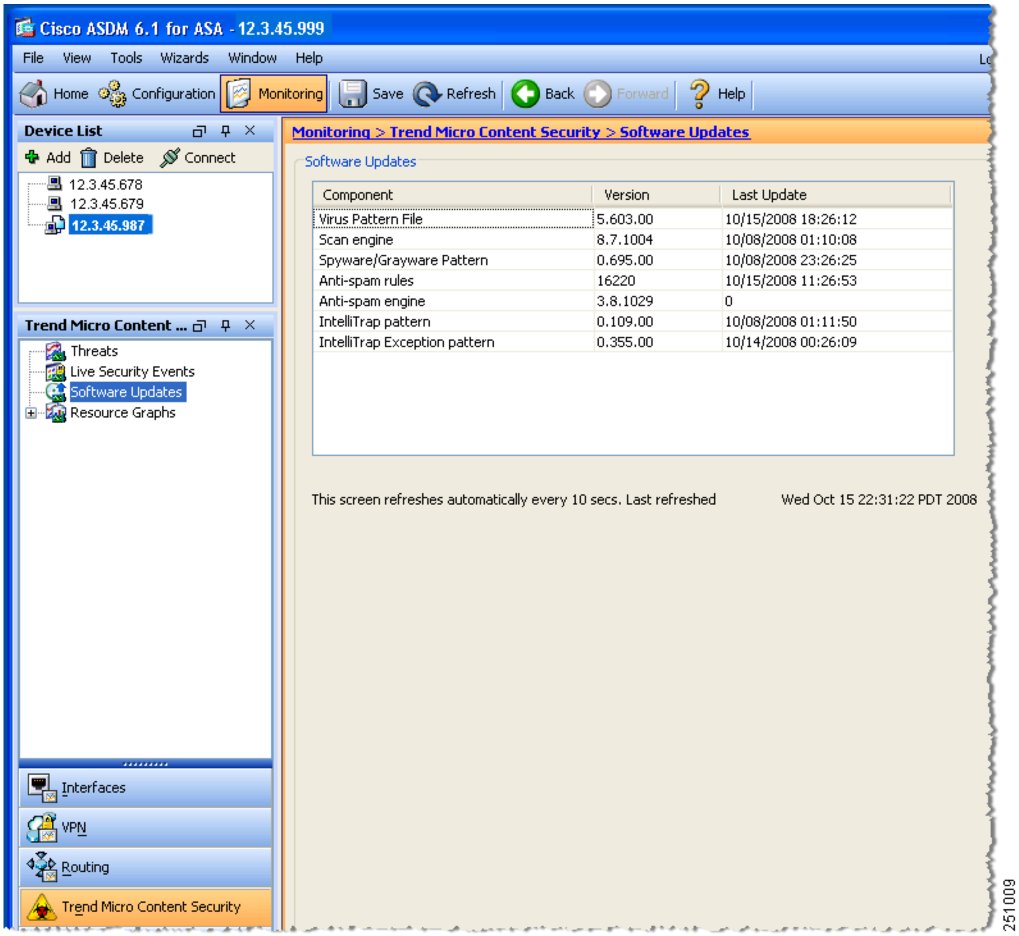
Monitoring Software Updates

To monitor software updates, perform the following steps:

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

The component name, version number, and the date and time that the CSC SSM software was last updated appears.

Figure 7-5 Software Updates Window

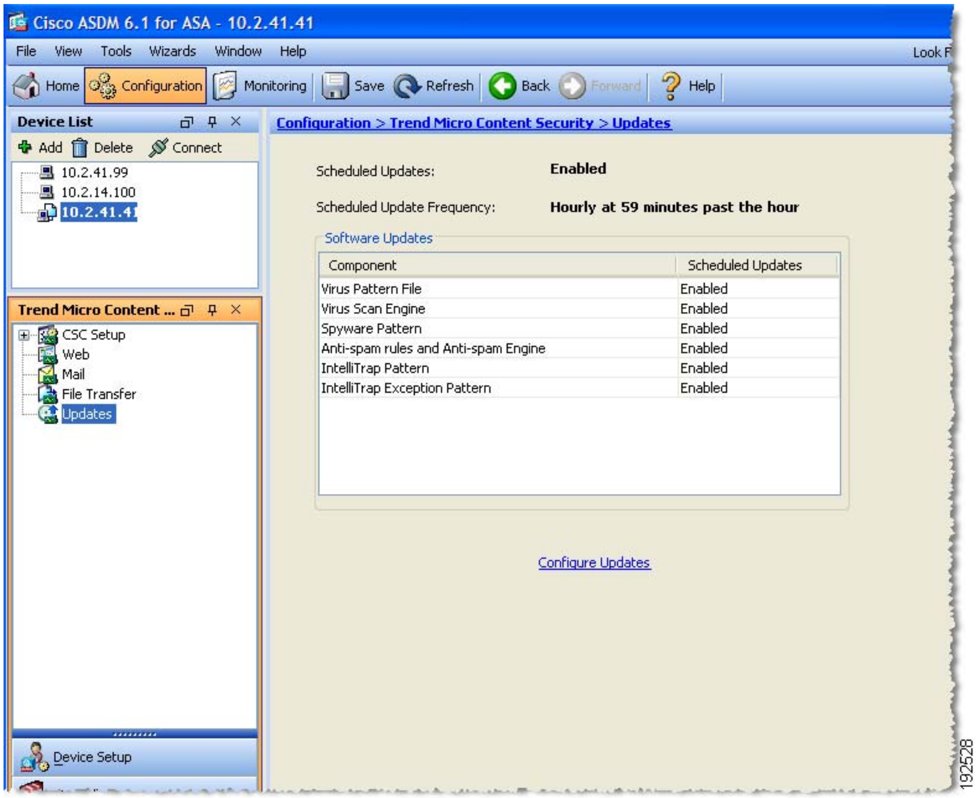

Cisco ASDM 6.1 for ASA - 12.3.45.999
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
12.3.45.678
12.3.45.679
12.3.45.987
Trend Micro Content ...
Threats
Live Security Events
Software Updates
Resource Graphs
Interfaces
VPN
Routing
Trend Micro Content Security
Monitoring > Trend Micro Content Security > Software Updates
Software Updates
251009

Component	Version	Last Update
Virus Pattern File	5.603.00	10/15/2008 18:26:12
Scan engine	8.7.1004	10/08/2008 01:10:08
Spyware/Grayware Pattern	0.695.00	10/08/2008 23:26:25
Anti-spam rules	16220	10/15/2008 11:26:53
Anti-spam engine	3.8.1029	0
IntelliTrap pattern	0.109.00	10/08/2008 01:11:50
IntelliTrap Exception pattern	0.355.00	10/14/2008 00:26:09

This screen refreshes automatically every 10 secs. Last refreshed Wed Oct 15 22:31:22 PDT 2008

Step 2 To display the Scheduled Update window shown in Figure 7-6, choose Configuration > Trend Micro Content Security > Updates window in ASDM.

Figure 7-6 ***Scheduled Updates in ASDM***


Cisco ASDM 6.1 for ASA - 10.2.41.41
File View Tools Wizards Window Help
Look F
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
10.2.41.99
10.2.14.100
10.2.41.41
Trend Micro Content ...
CSC Setup
Web
Mail
File Transfer
Updates
Device Setup
Configuration > Trend Micro Content Security > Updates
Software Updates
Configure Updates
192528

Scheduled Updates: Enabled

Scheduled Update Frequency: Hourly at 59 minutes past the hour

Component	Scheduled Updates
Virus Pattern File	Enabled
Virus Scan Engine	Enabled
Spyware Pattern	Enabled
Anti-spam rules and Anti-spam Engine	Enabled
IntelliTrap Pattern	Enabled
IntelliTrap Exception Pattern	Enabled

Step 3 Click the **Configure Updates** link to access the Scheduled Update window in CSC SSM. 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

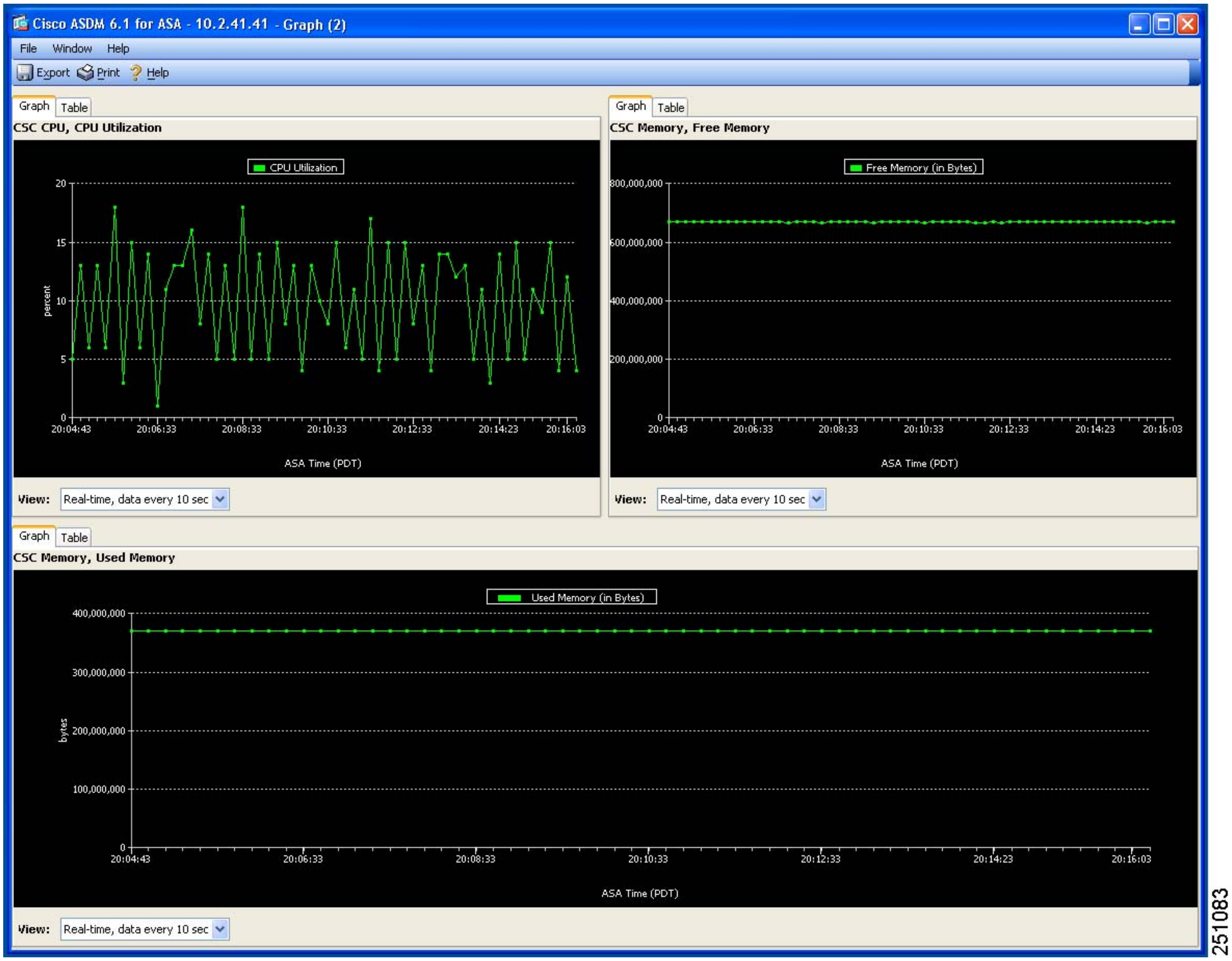
To monitor resources, perform the following steps:

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 7-7.

Figure 7-7 Memory Monitoring Graphs



View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

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

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
```

Step 2 Output similar to the following appears:

```
Image URL [tftp://171.69.1.129/dqu/csc6.3.xxxx.x.bin]:
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 3 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 2007
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/csc6.3.xxxx.x.bin
Slot-1 219> CONFIG=
Slot-1 220> LINKTIMEOUT=20
Slot-1 221> PKTTIMEOUT=2
Slot-1 222> RETRY=20
Slot-1 223> tftp dqu/csc6.3.xxxx.x.bin@171.69.1.129 via 30.0.0.254
```

Step 4 The CSC SSM attempts to connect to the TFTP server to download the image.

Note The TFTP server must support files sizes greater than 60 MB. The .bin files are full binary images that are to be uploaded via a TFTP server. The .pkg files are used to upgrade image files from the CSC Admin Console, which are then uploaded through a web browser. Do not upload .bin files using the CSC Admin Console.

Step 5 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 6 The ROMMON mode then launches the image.

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

The image is being unpacked and installed.

Step 7 After several minutes, the CSC SSM reboots.

Step 8 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 2007
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 9 To verify that the CSC SSM has booted correctly, enter the following command:

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

Step 10 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 6.3.xxxx.x

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.3.xxxx.x

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" entry 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 3	**a.** Make sure the TFTP server supports downloading of files larger than 60 MB. **b.** Check the size of the CSC image as it appears on your TFTP server. **c.** Can you perform an MD5 checksum to see whether it matches the checksum published with the image. **d.** Verify the image size that transferred according to the **verbose** output of the adaptive security appliance.
Step 4	**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.
Step 6	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 7 or Step 9	Download the image again and try to install it again. For more information, see Appendix B, "Preparing to Reimage the Cisco CSC SSM." 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 the following:

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- 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 8-5
- Recovering a Lost Password, page 8-5
- Summary Status and Log Entries Out of Sync, page 8-6

- 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 8-8

Note You must configure the syslog server to save the log buffer content to a file, so that it will be available for troubleshooting and debugging purposes.

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 8-5.

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 the “Modifying the Password-reset Policy” section on page B-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 B-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 Sync

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 100.100.10.10
access-list 101 deny tcp any host 100.100.10.10 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 backplane 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
capture cap access-list cap_acl interface inside
```

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_dataplane 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 adaptive 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 that 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 8-9
- 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 8-10
- Virus Scanning Not Working, page 8-10
- Downloading Large Files, page 8-12
- Restart Scanning Service, page 8-13

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 Email Reputation 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 3-9.

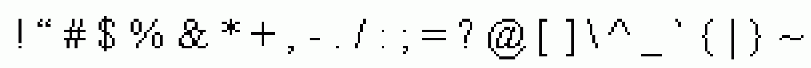
- You have configured the incoming mail domain. The content-based anti-spam scanning is only applied to mail recipients belonging to Incoming Domains. For more information, see Configuring SMTP Settings, page 3-7.

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

If you receive an unacceptable amount of spam, enable the network-based, anti-spam Email Reputation (ER) setting. Choose **Mail (SMTP) > Anti-spam > Email Reputation**.

If you do not use Email Reputation, 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 > Content Scanning/Target window and the Mail (POP3) > Anti-spam/Target.

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 Service-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. 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 Service-Policy Configuration

Another possible cause is that a file has not been scanned because of an incorrect service-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 6.3.xxxx.x

Mod SSM Application Name           Status           SSM Application Version
--- -----------------------------  -------------------------------------------
 1 CSC SSM                        Down             6.3.xxxx.x

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 details
```

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 6.3.xxxx.x
    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:       6.3.xxxx.x
    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.

If you have verified your configuration and CSC module status, and viruses are still not found, contact Cisco TAC.

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 following:

- 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.

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.

Enabling Deferred Scanning

Note If you experience difficulty with Windows updates, you may need to enable deferred scanning and set the size to ten. See the logs for more information.

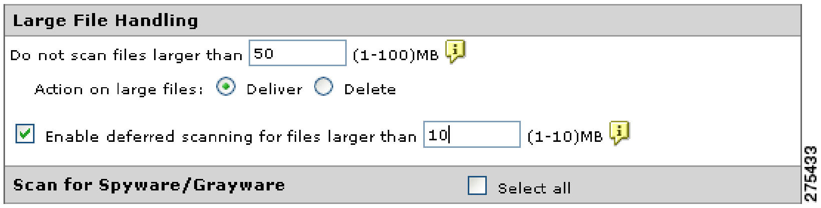
To enable deferred scanning, perform the following steps:

Step 1 Go to the **Web (HTTP) > HTTP scanning** tab.

Step 2 In the Large File Handling section, click the check box and set the "Enable deferred scanning for files larger than" value to 10, as shown in Figure 8-2.

Step 3 Click **Save**.

Figure 8-2 Enabling Deferred Scanning



Large File Handling

Do not scan files larger than 50 (1-100)MB

Action on large files: ● Deliver ○ Delete

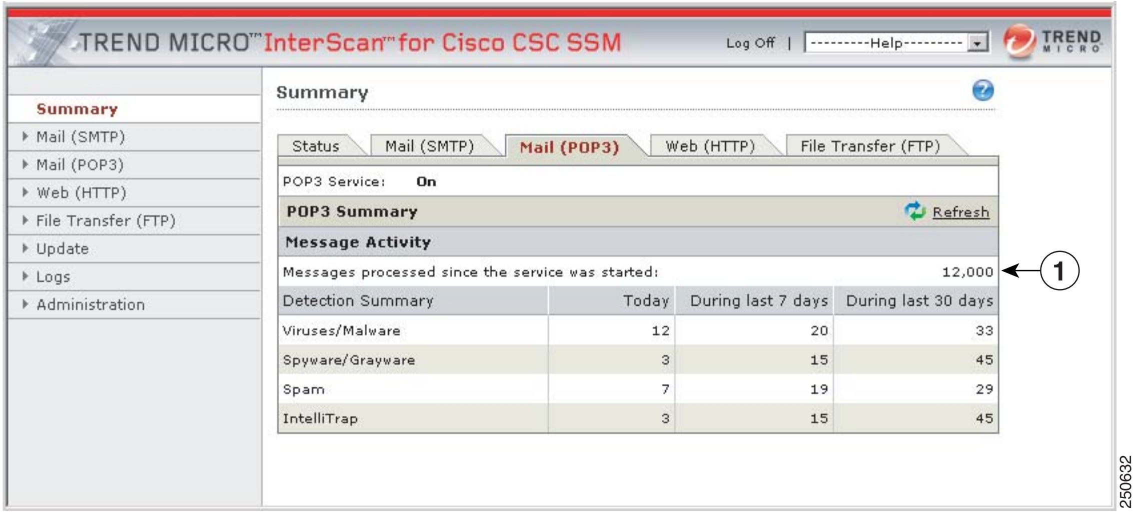
☑ Enable deferred scanning for files larger than 10 (1-10)MB

Scan for Spyware/Grayware □ Select all

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 8-3.

Figure 8-3 Messages Processed Counter on the Mail (POP3) Tab of the Summary Window



Summary

POP3 Service: **On**

POP3 Summary

Message Activity

Messages processed since the service was started: 12,000

Detection Summary	Today	During last 7 days	During last 30 days
Viruses/Malware	12	20	33
Spyware/Grayware	3	15	45
Spam	7	19	29
IntelliTrap	3	15	45

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 8-14
- Status LED Flashing for Over a Minute, page 8-14
- ASDM Cannot Communicate with SSM, page 8-14
- Logging in Without Going Through ASDM, page 8-14
- CSC SSM Throughput is Significantly Less Than ASA, page 8-15

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, enter the **show module 1 details** command to collect relevant information, and then reboot the system from ASDM.

ASDM Cannot Communicate with SSM

For information about resetting port access control, see the "Changing the Management Port Console Access Settings" section on page B-17.

Logging in Without Going Through ASDM

ASDM may have a problem with the environment, such as the Java version, or a net work problem. For more information, enable the ASDM Java console by choosing **ASDM > Tools**. If an IP access list is enabled on CSC, you can reset it. For more information, see the "Changing the Management Port Console Access Settings" section on page B-17.

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:

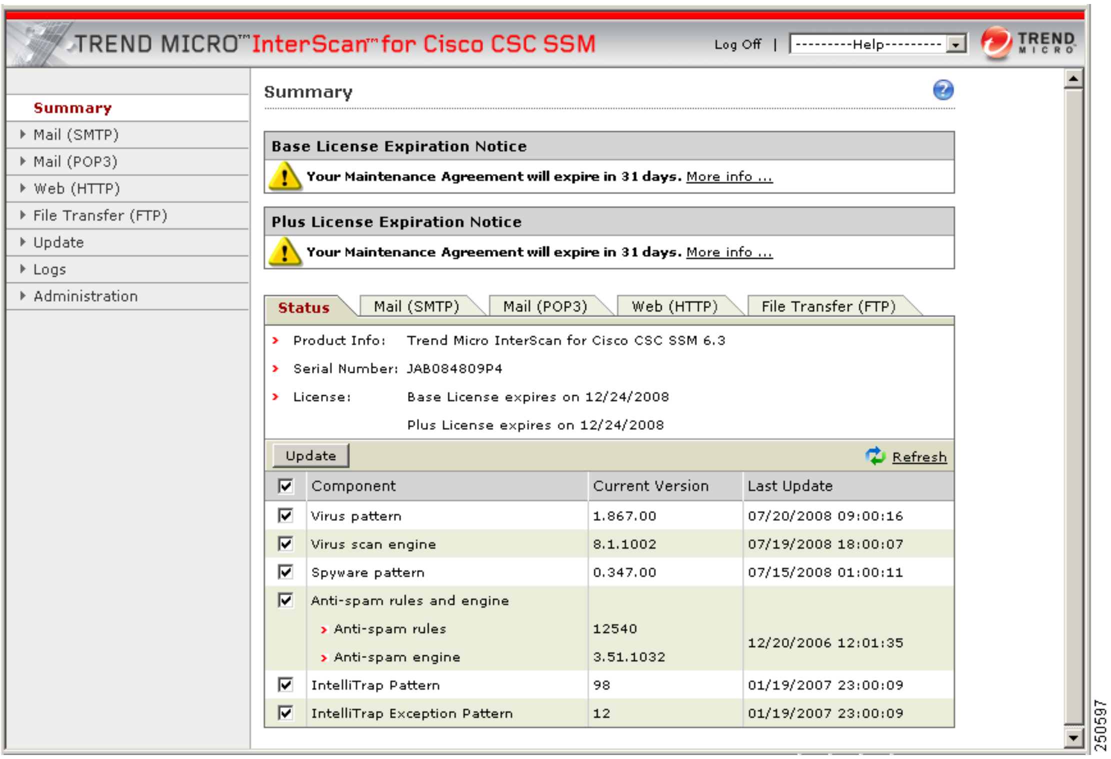
```
https://10.123.123.123:8443/
```

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 8-4.

Figure 8-4 Status Tab of the Summary Screen on the CSC SSM Console



Base License Expiration Notice

Your Maintenance Agreement will expire in 31 days. More info ...

Plus License Expiration Notice

Your Maintenance Agreement will expire in 31 days. More info ...

› Product Info: Trend Micro InterScan for Cisco CSC SSM 6.3

› Serial Number: JAB084809P4

› License: Base License expires on 12/24/2008
Plus License expires on 12/24/2008

☑	Component	Current Version	Last Update
☑	Virus pattern	1.867.00	07/20/2008 09:00:16
☑	Virus scan engine	8.1.1002	07/19/2008 18:00:07
☑	Spyware pattern	0.347.00	07/15/2008 01:00:11
☑	Anti-spam rules and engine		12/20/2006 12:01:35
	› Anti-spam rules	12540	
	› Anti-spam engine	3.51.1032	
☑	IntelliTrap Pattern	98	01/19/2007 23:00:09
☑	IntelliTrap Exception Pattern	12	01/19/2007 23:00:09

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 security appliance. 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 and inbound traffic for viruses, but ignore the intranet traffic.

For more information, see the following:

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Configuration Guide using the CLI*

Troubleshooting User/Group Policy

CSC SSM user/group policy feature relies on a remote Domain Controller Agent installed in the domain. In almost all cases, diagnosing user group policy problems requires logging into one of the following:

- The Domain Controller server
- The server where the Domain Controller Agent is installed
- A remote desktop connection to the Windows server that runs the Domain Controller Agent program

Diagnostics Tools

Use the following diagnostic tools to help resolve issues with the Domain Controller Agent or server. See information in this appendix about the following tools:

- Microsoft Active Directory Service Interfaces Editor (ADSI Edit), page 8-16
- Windows Event Viewer, page 8-17

Microsoft Active Directory Service Interfaces Editor (ADSI Edit)

Active Directory® Service Interfaces Editor (ADSI Edit) (Adsiedit.msc) is a Microsoft Management Console (MMC) snap-in. You can add the snap-in to any .msc file through the Add/Remove Snap-in menu option in MMC by choosing **Start > Run >** type **mmc** and press Enter, or open the Adsiedit.msc file from Windows Explorer. Figure 8-5 shows the ADSI Edit interface.

Note You can find information on how to download and install ADSI Edit at the following URL:

http://technet.microsoft.com/en-us/library/cc773354.aspx#BKMK_InstallingADSIEdit

ADSI Edit is used for testing the Active Directory (AD) connectivity and troubleshooting problems with the Active Directory/Lightweight Directory Access Protocol (AD/LDAP) search function.

Use regsvr32 to register the Adsiedit.dll file before launching Adsiedit.msc.

Note Adsiedit.msc will not run unless the Adsiedit.dll file is registered. This happens automatically if the support tools are installed. However, if the support tool files are copied instead of installed, you must run the regsvr32 command to register Adsiedit.dll before you run the Adsiedit.msc snap-in.

RegSvr32.exe has the following command-line options:

```
Regsvr32 [/u] [/n] [/i[:cmdline]] dllname

/u - Unregister server
/i - Call DllInstall passing it an optional [cmdline]; when used with /u calls dll
uninstall
/n - do not call DllRegisterServer; this option must be used with /i
/s - Silent; display no message boxes (added with Windows XP and Windows Vista)
```

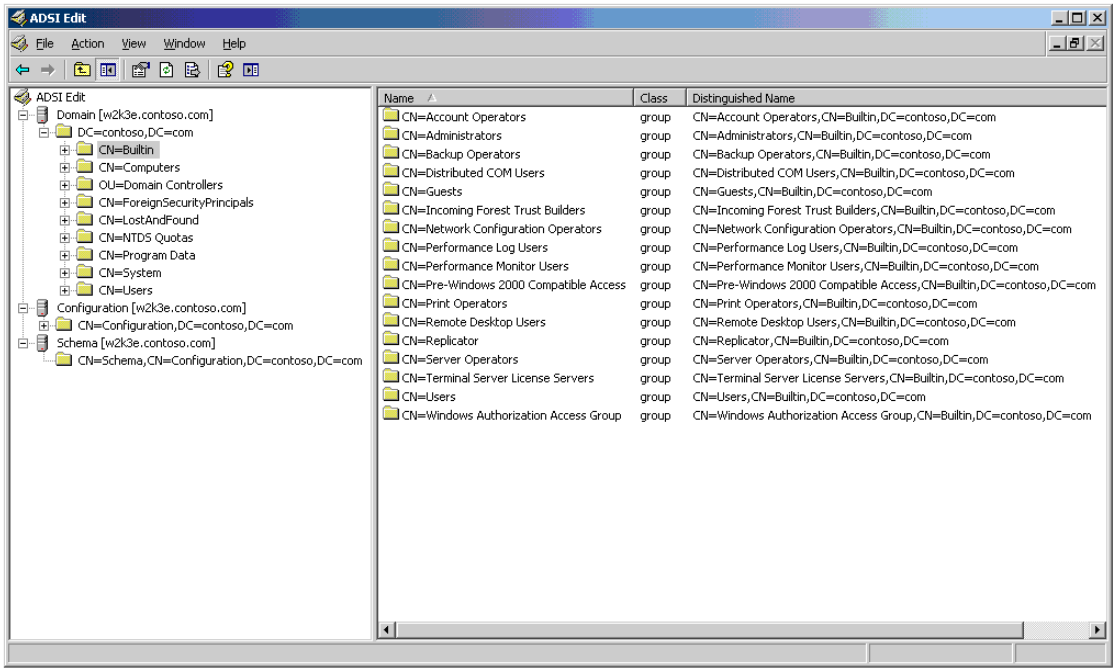
Example:

```
regsvr32 /i adsiedit.dll
```

Note More information about the regsvr32 command is available at the following URL:

http://support.microsoft.com/kb/249873

Figure 8-5 ADSI Edit Tool Interface


ADSI Edit
File
Action
View
Window
Help
ADSI Edit
Domain [w2k3e.contoso.com]
DC=contoso,DC=com
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=NTDS Quotas
CN=Program Data
CN=System
CN=Users
Configuration [w2k3e.contoso.com]
CN=Configuration,DC=contoso,DC=com
Schema [w2k3e.contoso.com]
CN=Schema,CN=Configuration,DC=contoso,DC=com
275357

Name	Class	Distinguished Name
CN=Account Operators	group	CN=Account Operators,CN=Builtin,DC=contoso,DC=com
CN=Administrators	group	CN=Administrators,CN=Builtin,DC=contoso,DC=com
CN=Backup Operators	group	CN=Backup Operators,CN=Builtin,DC=contoso,DC=com
CN=Distributed COM Users	group	CN=Distributed COM Users,CN=Builtin,DC=contoso,DC=com
CN=Guests	group	CN=Guests,CN=Builtin,DC=contoso,DC=com
CN=Incoming Forest Trust Builders	group	CN=Incoming Forest Trust Builders,CN=Builtin,DC=contoso,DC=com
CN=Network Configuration Operators	group	CN=Network Configuration Operators,CN=Builtin,DC=contoso,DC=com
CN=Performance Log Users	group	CN=Performance Log Users,CN=Builtin,DC=contoso,DC=com
CN=Performance Monitor Users	group	CN=Performance Monitor Users,CN=Builtin,DC=contoso,DC=com
CN=Pre-Windows 2000 Compatible Access	group	CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=contoso,DC=com
CN=Print Operators	group	CN=Print Operators,CN=Builtin,DC=contoso,DC=com
CN=Remote Desktop Users	group	CN=Remote Desktop Users,CN=Builtin,DC=contoso,DC=com
CN=Replicator	group	CN=Replicator,CN=Builtin,DC=contoso,DC=com
CN=Server Operators	group	CN=Server Operators,CN=Builtin,DC=contoso,DC=com
CN=Terminal Server License Servers	group	CN=Terminal Server License Servers,CN=Builtin,DC=contoso,DC=com
CN=Users	group	CN=Users,CN=Builtin,DC=contoso,DC=com
CN=Windows Authorization Access Group	group	CN=Windows Authorization Access Group,CN=Builtin,DC=contoso,DC=com

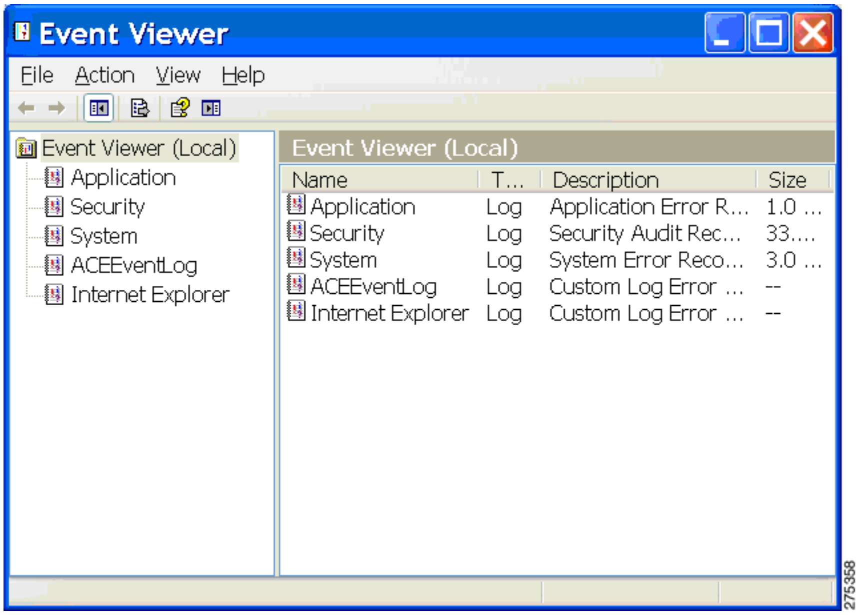
Windows Event Viewer

Microsoft Windows Event Viewer is a MMC snap-in that allows you to browse and manage event logs. This tool is helpful for monitoring your system health and user logon detection problems.

To start the Event Viewer in Windows, perform the following step:

Select **Start > Control Panel > Administrative Tools > Event Viewer** or use the Microsoft Management MMC command **eventvwr.msc**.

Figure 8-6 Event Viewer Interface



Name	T...	Description	Size
Application	Log	Application Error R...	1.0 ...
Security	Log	Security Audit Rec...	33....
System	Log	System Error Reco...	3.0 ...
ACEEventLog	Log	Custom Log Error ...	--
Internet Explorer	Log	Custom Log Error ...	--

To connect to the remote event log service, perform the following steps:

Step 1 In Event Viewer window, choose **Action > Connect to another computer**.

Step 2 Enter the name of the remote domain controller server or browse to its location.

Step 3 Click **OK**.

Step 4 Access the domain controller server event log.

Domain Controller Agent Debugging

Turn on the Domain Controller Agent debugging log when you troubleshoot user group policy problems. The debugging log is helpful and is needed for the user/group feature technical support cases.

Enabling Domain Controller Agent Debugging

To enable Domain Controller Agent debugging, perform the following steps:

Step 1 Log on to the server that runs the agent program.

Step 2 Open the Registry Editor, or remotely connect to the registry on that server.

Step 3 Assign a non-zero value to the following registry value:

a. Choose **Start > Run**.

a. Type **`regedit`**.

a. Navigate to **`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IdAgent\`**.

a. Double-click **DebugLevel**.

b. Change the value data from 0 to 1

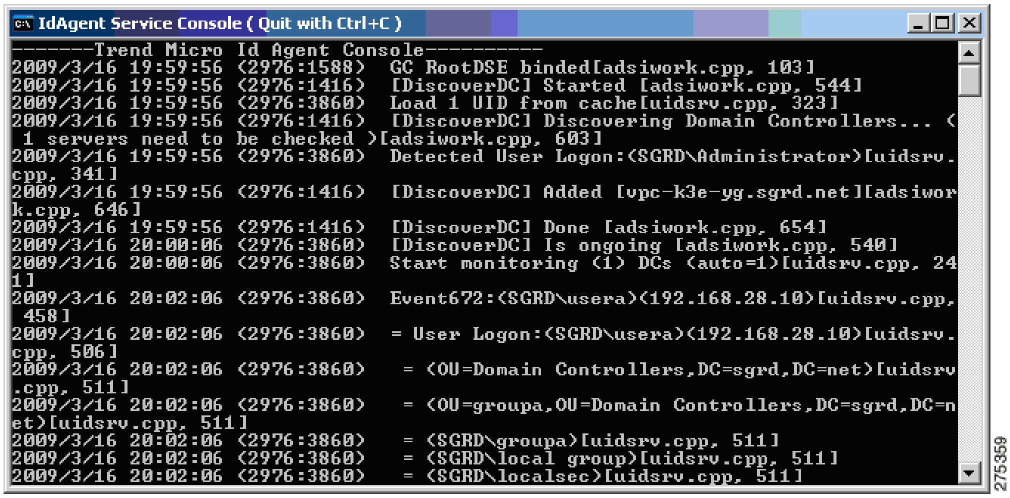
Step 4 Run **services.msc**, choose **TMIdAgent**, and click Restart (■▸) to stop and restart the Domain Controller Agent service.

Step 5 Locate the debugging log file (IdAgentDebug.log) in the Domain Controller Agent installation folder.

Console Mode

In addition to enabling the Domain Controller Agent debugging log, you can run the agent in console mode. When the agent program is running in console mode, it shows the logged-on users and displays debugging messages on the console screen. Console mode can be useful for diagnosing agent connectivity issues. You can see the request and response log immediately. Figure 8-7 shows the console mode interface.

Figure 8-7 Domain Controller Agent Running in Console Mode



```
-------Trend Micro Id Agent Console-----------
2009/3/16 19:59:56 <2976:1588>  GC RootDSE binded[adsiwork.cpp, 103]
2009/3/16 19:59:56 <2976:1416>  [DiscoverDC] Started [adsiwork.cpp, 544]
2009/3/16 19:59:56 <2976:3860>  Load 1 UID from cache[uidsrv.cpp, 323]
2009/3/16 19:59:56 <2976:1416>  [DiscoverDC] Discovering Domain Controllers... (
 1 servers need to be checked )[adsiwork.cpp, 603]
2009/3/16 19:59:56 <2976:3860>  Detected User Logon:<SGRD\Administrator>[uidsrv.
cpp, 341]
2009/3/16 19:59:56 <2976:1416>  [DiscoverDC] Added [vpc-k3e-yg.sgrd.net][adsiwor
k.cpp, 646]
2009/3/16 19:59:56 <2976:1416>  [DiscoverDC] Done [adsiwork.cpp, 654]
2009/3/16 20:00:06 <2976:3860>  [DiscoverDC] Is ongoing [adsiwork.cpp, 540]
2009/3/16 20:00:06 <2976:3860>  Start monitoring (1) DCs (auto=1)[uidsrv.cpp, 24
1]
2009/3/16 20:02:06 <2976:3860>  Event672:<SGRD\usera><192.168.28.10>[uidsrv.cpp,
 458]
2009/3/16 20:02:06 <2976:3860>  = User Logon:<SGRD\usera><192.168.28.10>[uidsrv.
cpp, 506]
2009/3/16 20:02:06 <2976:3860>   = <OU=Domain Controllers,DC=sgrd,DC=net>[uidsrv
.cpp, 511]
2009/3/16 20:02:06 <2976:3860>   = <OU=groupa,OU=Domain Controllers,DC=sgrd,DC=n
et>[uidsrv.cpp, 511]
2009/3/16 20:02:06 <2976:3860>   = <SGRD\groupa>[uidsrv.cpp, 511]
2009/3/16 20:02:06 <2976:3860>   = <SGRD\local group>[uidsrv.cpp, 511]
2009/3/16 20:02:06 <2976:3860>   = <SGRD\localsec>[uidsrv.cpp, 511]
```

To start the console mode, perform the following steps:

Step 1 Stop the running Domain Controller Agent service.

Step 2 In the Trend Micro Domain Controller Agent installation directory, double-click the **DebugMode** shortcut. The default directory is C:\Program Files\Trend Micro\IdAgent\.

Step 3 Click **Ctrl + C** to exit the running console.

CSC SSM Debugging

Enabling CSC SSM debugging syslog messages will also help to diagnose user group policy issues. The daemon debugging log includes information about the user identification results and policy matching information.

To enable the CSC SSM debugging log, perform the following steps:

Step 1 Log on to the CSC SSM web management console.

Step 2 Choose **Logs > Settings > Log Settings** as shown in Figure 8-8.

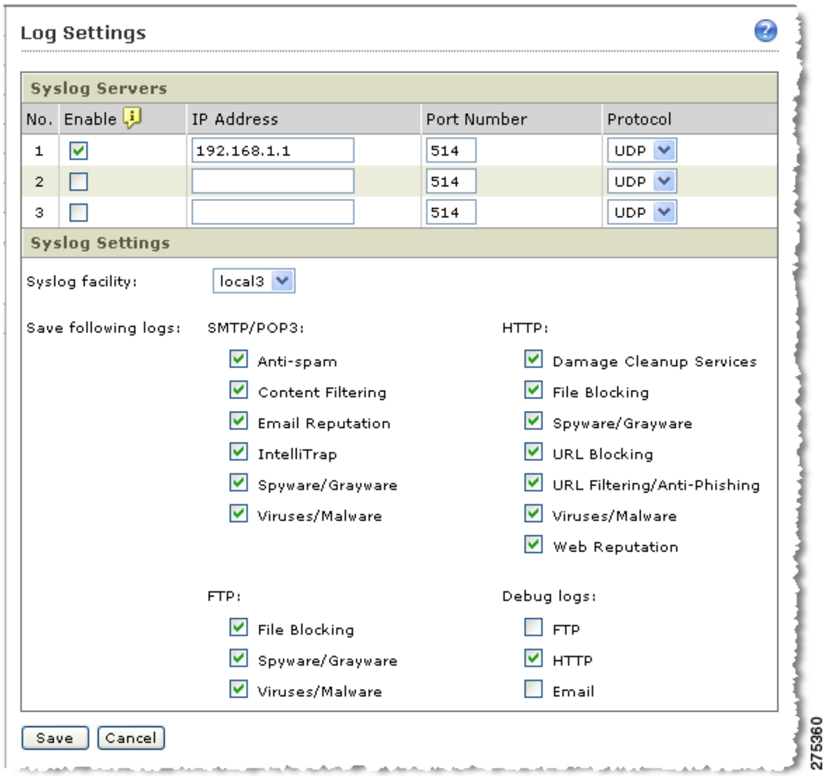
Step 3 Configure at least one syslog server. See the"Configuring Syslog Servers" section on page 5-4 for more information.

Step 4 Choose the applicable **Syslog Facility** from the drop-down list.

Step 5 Under Debug Logs, check the **HTTP** check box.

Step 6 Click **Save**.

Figure 8-8 Viewing the Debugging Log in the Log Settings Screen



Log Settings

Syslog Servers

No.	Enable	IP Address	Port Number	Protocol
1	☑	192.168.1.1	514	UDP
2	□		514	UDP
3	□		514	UDP

Syslog Settings

Syslog facility: local3

Save following logs:

SMTP/POP3:
- ☑ Anti-spam
- ☑ Content Filtering
- ☑ Email Reputation
- ☑ IntelliTrap
- ☑ Spyware/Grayware
- ☑ Viruses/Malware

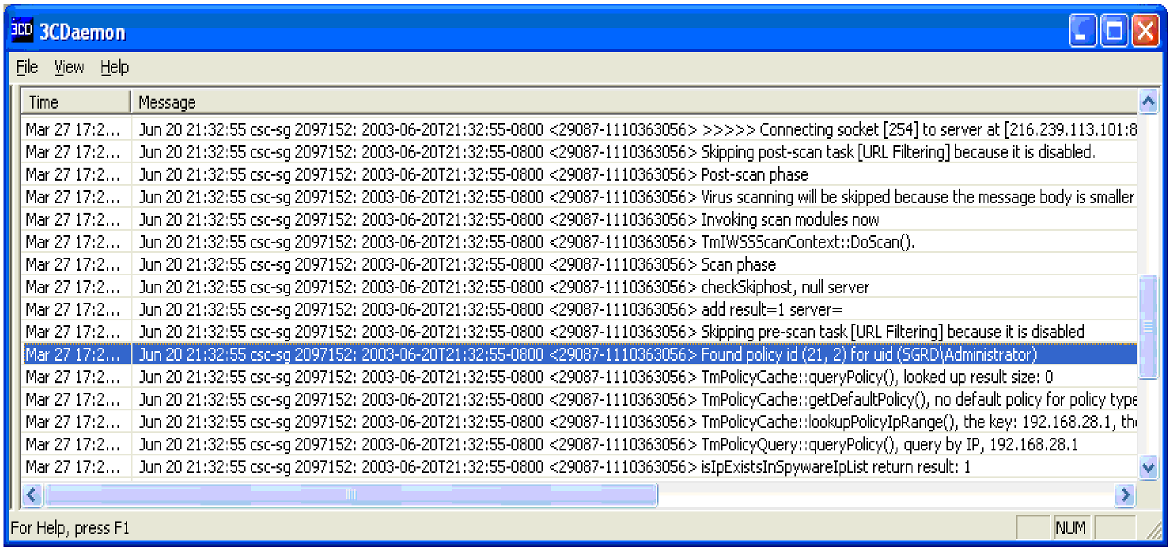
HTTP:
- ☑ Damage Cleanup Services
- ☑ File Blocking
- ☑ Spyware/Grayware
- ☑ URL Blocking
- ☑ URL Filtering/Anti-Phishing
- ☑ Viruses/Malware
- ☑ Web Reputation

FTP:
- ☑ File Blocking
- ☑ Spyware/Grayware
- ☑ Viruses/Malware

Debug logs:
- □ FTP
- ☑ HTTP
- □ Email

When CSC SSM HTTP debugging is enabled, the HTTP daemon will send debugging messages to the syslog server. If you visit a website from the client, the user/group-based policy matching will be logged. The syslog lines shown in Figure 8-9 illustrate the functioning user identification and policy matching. The displayed policy ID is the matched policy ID. The identified username for the incoming connection is given in parentheses.

Figure 8-9 User Identification and Policy Matching in Debugging Syslog



```
Time          Message
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> >>>>> Connecting socket [254] to server at [216.239.113.101:8
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Skipping post-scan task [URL Filtering] because it is disabled.
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Post-scan phase
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Virus scanning will be skipped because the message body is smaller
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Invoking scan modules now
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> TmIWSSScanContext::DoScan().
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Scan phase
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> checkSkiphost, null server
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> add result=1 server=
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Skipping pre-scan task [URL Filtering] because it is disabled
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> Found policy id (21, 2) for uid (SGRD\Administrator)
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> TmPolicyCache::queryPolicy(), looked up result size: 0
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> TmPolicyCache::getDefaultPolicy(), no default policy for policy type
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> TmPolicyCache::lookupPolicyIpRange(), the key: 192.168.28.1, th
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> TmPolicyQuery::queryPolicy(), query by IP, 192.168.28.1
Mar 27 17:2...  Jun 20 21:32:55 csc-sg 2097152: 2003-06-20T21:32:55-0800 <29087-1110363056> isIpExistsInSpywareIpList return result: 1
```

Domain Controller Agent, Active Directory, and User Identification Troubleshooting

This section includes the following topics:

- Domain Controller Agent Installation or Service Failure, page 8-21
- Domain Controller Agent Connectivity, page 8-21
- Domain Controller Server Connectivity, page 8-25

Domain Controller Agent Installation or Service Failure

The Domain Controller Agent must be installed in the domain. The installation also requires administrator privileges. In most cases, the agent is installed on a Domain Controller server, which avoids assigning different credentials for the agent to access Domain Controller server. However, it is also possible to install the agent on another server that belongs to the domain.

Verify that the following items are true before attempting to troubleshoot any agent installation issue:

- Verify that the OS is supported. The agent can be installed on Windows Server® 2000, Windows Server® 2003, Windows Server® 2008. Windows® 2000 Pro, and Window® XP.
- Be sure you have local administrator privileges to launch the agent installation program (MSI).
- Remove any previous version of the agent from the Add or Remove Programs in Control Panel.

Domain Controller Agent Connectivity

The Domain Controller Agent service is displayed as “Trend Micro IdAgent.” The service name is “TMIDAgent.” You will see it running from the **services.msc** command after the agent is installed on the server.

The agent, after it is installed and started, can be contacted by CSC SSM and answer the user identification requests.

To configure the Domain Controller server, perform the following steps:

Step 1 Open the CSC SSM web console.

Step 2 Choose **Administration > Device Settings > User ID Settings**.

Step 3 Use the User Identification Settings page to perform the following tasks:

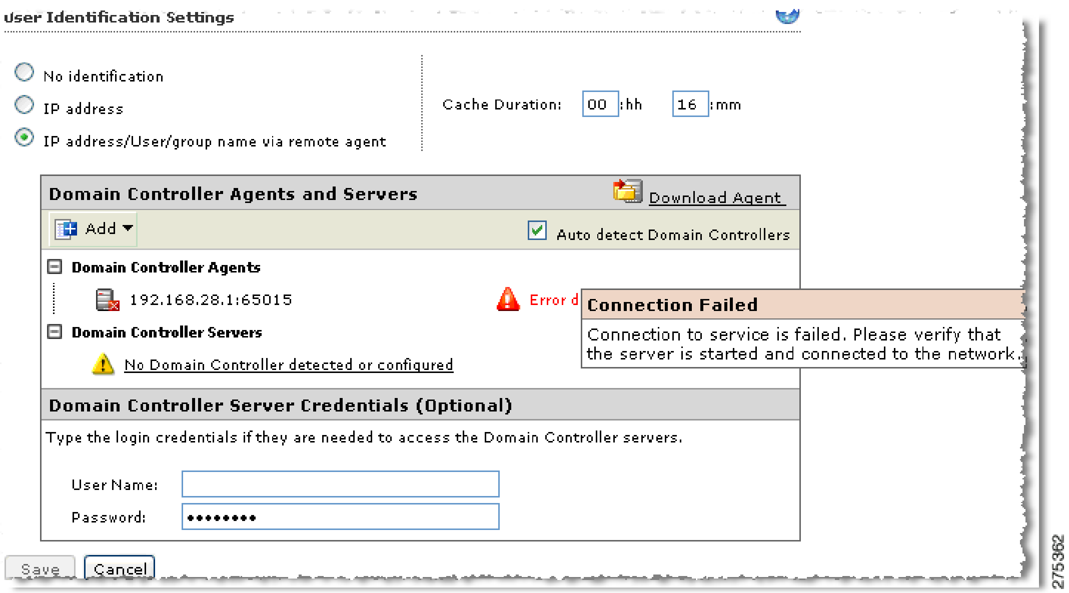
- Add the agent. (See the"Configuring User ID Settings" section on page 6-3 for details.)
- Save the settings.
- View the agent status.

The green icon means the agent is ready for requests.

Note The Domain Controller servers must be configured to allow the agent to identify the logged-on users.

If there is a connectivity error, a detailed message displays in the mouse-over tool tip, as shown in Figure 8-10.

Figure 8-10 Connectivity Error Message



User Identification Settings

○ No identification

○ IP address

● IP address/User/group name via remote agent

Cache Duration: 00 :hh 16 :mm

Domain Controller Agents and Servers

Download Agent

Add ▾

☑ Auto detect Domain Controllers

⊟ Domain Controller Agents

192.168.28.1:65015 Error d

Connection Failed

Connection to service is failed. Please verify that the server is started and connected to the network.

⊟ Domain Controller Servers

No Domain Controller detected or configured

Domain Controller Server Credentials (Optional)

Type the login credentials if they are needed to access the Domain Controller servers.

User Name:

Password: ••••••••

Save Cancel

Table 8-2 lists the possible errors, potential causes, and possible solutions for Domain Controller Agent issues.

Table 8-2 Domain Controller Agent Issues

Error	Potential Cause	Possible Solution or Diagnostic Steps
Invalid host or IP address	Inappropriate agent address is specified.	• Check the agent hostname or IP address and port number. • Verify that the DNS is working for the CSC SSM when the hostname is used.

Table 8-2 Domain Controller Agent Issues (continued)

Error	Potential Cause	Possible Solution or Diagnostic Steps
Version not supported	CSC SSM requires a newer version of the agent.	Download the agent from the CSC SSM web console and re-install it on the target server. See the "Installing the Domain Controller Agent" section on page 6-6 for details.
Connection failed	Critical file is missing, such as the SSL certification file or the configuration file.	Re-install the Domain Controller Agent to resolve this issue. See the "Installing the Domain Controller Agent" section on page 6-6 for details.
	The listening port is occupied. The default agent listening port is 65015.	• Choose another port number and change the port value in the "AgentPort" key in the <Agent installation directory>\IdAgent.ini file. • Restart the agent service.
	Critical OS exceptions, such as memory allocation failure or system handler allocation failure.	• Enable Domain Controller Agent debugging. See the"Enabling Domain Controller Agent Debugging" section on page 8-18. • Check OS environment. • Send the log file to Trend Micro support.
Service status undetermined	The agent is applying new settings; the status is not determined yet.	Refresh the page.
Directory service unavailable	The agent does not have the appropriate privileges to connect to the Active Directory service.	• Log on to the agent-installed PC with the agent's credentials, diagnose the problem with ADSIEditor (see the "Microsoft Active Directory Service Interfaces Editor (ADSI Edit)" section on page 8-16,) and verify that the Active Directory service is accessible. • Change the credentials from the User Identification Settings page in CSC SSM web console. See the "Adding Domain Controller Server Credentials" section on page 6-10 for details.
	The machine that the agent is installed on is not in the Active Directory domain.	Connect the machine to the Active Directory domain.
	The agent is installed on a pre-Vista system, but the Active Directory server is on Windows Server 2008®.	Install the Domain Controller Agent on a Windows Server 2008.

Table 8-2 Domain Controller Agent Issues (continued)

Error	Potential Cause	Possible Solution or Diagnostic Steps

Agent access denied	The agent denied a request based on the access rule settings.	Agents will not respond to any client if the client's identifier or IP address is not in the access list. When the agent first starts, the agent access list is empty. The first registered client occupies the agent and determines who else is allowed to access this agent. One way to register another CSC SSM is to configure a failover device. However, you can always manually configure the access list on the agent side.
		To manually configure the access list, perform these steps:
		1. Log on to the Domain Controller Agent server machine using an administrator account.
		2. Browse to the agent installation folder, C:\Program Files\Trend Micro\IdAgent\
		3. Locate and open the agent configuration INI file named IdAgent.ini.
		4. In the [ClientList] section, add a new line with a value pair (a key + a value) in the following format:
		`<Your-Temp-ID>=<host:port>|0`
		where
		• <Your-Temp-Id> = any unique key name, such as xxxx. This must be different from any existing string.
		• <host:port>|0 = the Domain Controller Agent server IP address and port number followed by pipe zero (|0).
		Example:
		`[ClientList]`
		`??????=192.168.1.1:65014|0`
		The temporary client ID must be unique, or else it will replace an existing one. The default port is 65014.
		5. Restart the agent service.

Any other error	Unexpected error	• Enable Domain Controller Agent debugging. See the "Enabling Domain Controller Agent Debugging" section on page 8-18. • Send the log file to Trend Micro support.

Domain Controller Server Connectivity

Domain Controller servers must be configured so that user identification can occur on the agent. The Domain Controller server list determines the authentication servers that the Domain Controller Agent will monitor. All the user logon information comes from those servers. If a Domain Controller server is not configured, the Domain Controller Agent will not detect any user information from that server.

To configure a Domain Controller server, perform the following steps:

Step 1 Open the CSC SSM management console.

Step 2 Choose **Administration > User ID Settings**.

Step 3 See the "Adding A Domain Controller Agent or Server to CSC SSM" section on page 6-7.

Auto Detect Domain Controllers

In most cases, the user checks the "Auto detect Domain Controllers" check box on the User Identification Settings page. This setting allows the agent to detect and evaluate the Domain Controller servers at the same site. Auto-detection eliminates errors. The Domain Controller server IP address, if input manually, could be mistyped or not accessible.

The Domain Controller agent needs the appropriate privileges to connect to the Active Directory and to view the Domain Controller event log. You must provide the correct domain credentials to the agent. If the agent does not have the correct privileges, it cannot search though the Active Directory to find the correct Domain Controller server.

For autodetection issues, check the Domain Controller Agent privileges.

Connectivity

If configured correctly, the Domain Controller server list on the User Identification Settings page should show the Domain Controller server as operational. If there is an error, the details display as do the Domain Controller Agent errors shown in Figure 8-10.

Table 8-3 lists the possible errors and potential causes.

Table 8-3 Diagnosing and Solving Domain Controller Server Connectivity

Error	Potential Cause	Possible Solution or Diagnostic Steps
Invalid host or IP address	Invalid host or IP address Inappropriate Domain Controller server address is specified.	• Check the server hostname or IP address. • Verify that DNS is working on the CSC SSM when the hostname is used instead of the IP address.
Connection failed	The server is down or unavailable.	Make sure the Domain Controller server is running and the event log service is enabled.
Logon failed	The username and password provided in the User Identification Settings page is not correct.	• Find the username that the agent is currently using as shown by choosing Administration > User Identification Settings in the Domain Controller server credentials section. • Type the correct username and password.

Table 8-3 Diagnosing and Solving Domain Controller Server Connectivity (continued)

Error	Potential Cause	Possible Solution or Diagnostic Steps
Access denied	The agent does not have the correct access privileges to view the Domain Controller server event log service.	• Find the username that the agent is currently using as shown by choosing Administration > User Identification Settings in the Domain Controller Server Credentials section. • Verify the agent is running with the correct access privileges. • Change the logged-on user if needed. • Use the Event Viewer to determine if access privileges are the problem. See the "Windows Event Viewer" section on page 8-17. To determine if the problem is access privileges, log on to the Domain Controller Agent server using the Domain Controller Agent credentials, open the Event Viewer (eventvwr.msc) and try to connect to the Domain Controller server to see if it can be accessed.
Not initialized	May be caused by the Access Denied error	See the solution for Access Denied error.
Workstation access denied	The client PC disabled the remote registry service.	The agent relies on a remote registry service on the client workstation to verify the user logon. To deploy user group policies, the domain administrator must enforce the remote registry service on each workstation in the domain. This server is turned on by default on most Windows platforms.
	The agent does not have sufficient access privileges.	The agent must have sufficient access privileges to view the remote registry services on other workstations.
	The firewall on the client workstation blocks the request.	*For Windows XP SP2:* The firewall is turned on by default, which will block all the RPC requests. To fix the problem. add a domain policy that enables remote administration. To correct the problem, see the following URL: http://support.microsoft.com/kb/840634
Any other error	Unexpected error	• Enable Domain Controller Agent debugging. See the"Enabling Domain Controller Agent Debugging" section on page 8-18. • Send the log file to Trend Micro support.

AD/LDAP Searching

The Active Directory/Lightweight Directory Access Protocol (AD/LDAP) searching functionality requires correctly configured user identification settings.

To troubleshoot the searching function, perform the following steps:

Step 1 Verify that the "IP address/User/group name via remote agent" method is checked on the Administration > User Identification Settings page. See Figure 8-10 on page 8-22.

Step 2 Verify that the Domain Controller Agent(s) and the Domain Controller server(s) are correctly configured and that they display no error messages on the Administration > User Identification Settings page. If an error appears, match the error message with the correct solution in the previous sections. See Table 8-2 on page 8-22 and Table 8-3 on page 8-25 for a list of solutions.

Step 3 If the Domain Controller Agent(s) and Domain Controller server(s) work, but you still do not obtain search results, enable the Domain Controller Agent debugging log to see if the search request has been correctly handled. See the "Enabling Domain Controller Agent Debugging" section on page 8-18. The ADSI Edit can also be used to verify that the search contains valid results. See the "Microsoft Active Directory Service Interfaces Editor (ADSI Edit)" section on page 8-16.

Step 4 Check the client timeout value. The default timeout value is 10 seconds. To change this value, edit the AcceptTimeoutSecs=10 parameter in the IdLib.ini file located at opt/trend/isvw/config/web/ on CSC SSM. The RecvTimeoutSecs parameter defines how long the CSC SSM waits for the search result.

You must enable debugging on the CSC SSM and, if necessary, send the debugging log to Trend Micro support. For more information, see the "CSC SSM Debugging" section on page 8-19.

User Identification

User identification is critical when using the user /group policy feature. When troubleshooting a user identification issue, the debugging on both CSC SSM side and Domain Controller Agent side should be enabled for more information.

To diagnose user identification problems, perform the following steps:

Step 1 Choose **Administration > User Identification Settings**.

Step 2 Verify that both the Domain Controller Agent(s) and Domain Controller server(s) are configured correctly. If errors exist, see Table 8-2 and Table 8-3 for troubleshooting information.

Step 3 To detect something other than a connectivity or privilege problem, enable the audit account logon events by performing the following steps:

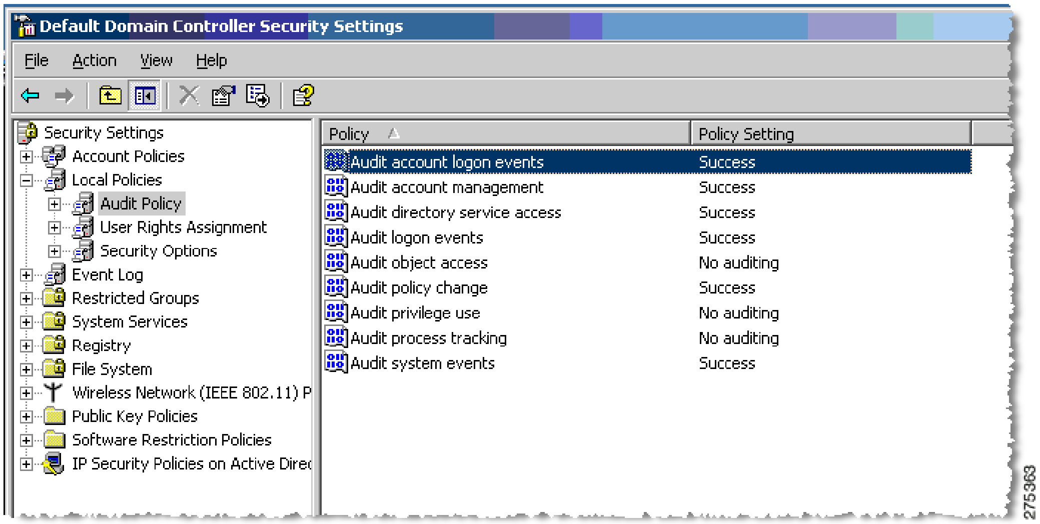
a. Choose **Start > Control Panel > Administrative Tools**.

b. Click **Domain Controller Security Policy**.

c. Expand **Local Policies** on the left pane, and then select **Audit Policy**.

d. Verify that Audit account logon events is enabled. See Figure 8-11.

Figure 8-11 Enabled Audit Logon Account



Policy	Policy Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

Collecting Data for Trend Micro Support

Make sure that you always collect the Domain Controller Agent debugging log and the CSC SSM HTTP daemon debugging log before calling Trend Micro technical support. For more information, see the following sections:

- Enabling Domain Controller Agent Debugging, page 8-18
- CSC SSM Debugging, page 8-19

Known Issues

The following known issues exist in the CSC SSM:

- The CSC SSM does not scan HTTP proxy traffic nor non-HTTP traffic over port 80.

  Workaround: Do one of the following:

  - Use another port as the proxy service,
  - Use the adaptive security appliance modular policyframework to prevent the CSC SSM from scanning the website IP addresses.
  - Deploy a proxy server between the CSC SSM and clients.
- The CSC SSM does not work with certain real-time stock streaming services, such as Yahoo Market Tracker.

  Workaround: Use the adaptive security appliance modular policy framework to prevent the CSC SSM from scanning the website IP addresses for stock streaming services.
- Traffic interruptions may occur during configuration or component updates.

  Workaround: Perform configuration updates or scheduled updates during off-hours.
- The CSC SSM does not scan e-mail traffic between Microsoft Exchange servers that use the EXCH50 protocol.

Workaround: Use the adaptive security appliance modular policy framework to prevent the CSC SSM from scanning the Microsoft Exchange servers' IP addresses.

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

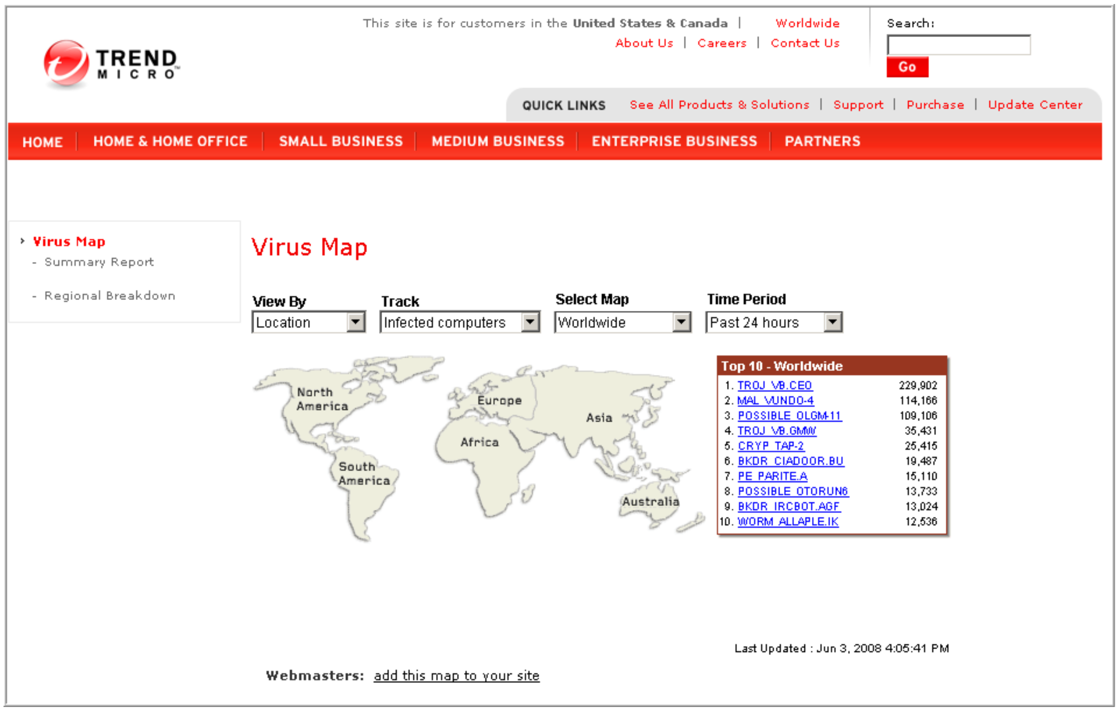
Comprehensive security information is available from the Trend Micro Security Information Center, a free online resource, at the following URL:

http://threatinfo.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 8-12. The virus map is available at the following URL:
  http://wtc.trendmicro.com/wtc/default.asp

Figure 8-12 Virus Map


TREND MICRO
This site is for customers in the United States & Canada | Worldwide
About Us | Careers | Contact Us
Search:
Go
QUICK LINKS See All Products & Solutions | Support | Purchase | Update Center
HOME | HOME & HOME OFFICE | SMALL BUSINESS | MEDIUM BUSINESS | ENTERPRISE BUSINESS | PARTNERS
Virus Map
- Summary Report
- Regional Breakdown
North America
South America
Europe
Africa
Asia
Australia
Webmasters: add this map to your site
250631

Virus Map

View By: Location
Track: Infected computers
Select Map: Worldwide
Time Period: Past 24 hours

Top 10 - Worldwide	
1. TROJ_VB.CEO	229,902
2. MAL_VUNDO-4	114,166
3. POSSIBLE_OLGM-11	109,106
4. TROJ_VB.GMW	35,431
5. CRYP_TAP-2	25,415
6. BKDR_CIADOOR.BU	19,487
7. PE_PARITE.A	15,110
8. POSSIBLE_OTORUN6	13,733
9. BKDR_IRCBOT.AGF	13,024
10. WORM_ALLAPLE.IK	12,536

Last Updated : Jun 3, 2008 4:05:41 PM

- 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

Before Contacting Cisco TAC

Before you contact the Cisco Technical Assistance Center (TAC), check the documentation and online help to see whether it includes 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

CSC SSM Syslog Messages

This appendix lists the syslog messages in numerical order, and includes the following sections:

Messages 181248 - 2392320

Table A-1 shows the variables used by syslog messages in this section.

Table A-1 Messages 181248 - 2392320 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$group	Group name as designated in user/group policy configuration.
$info	Information that explains more about the syslog message
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file-types. • Content filtering uses “Subject,” “Body,” and “Attachment.”
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$proto	Protocol name or value, such as SMTP, POP3, HTTP, FTP
$srcip:$srcport	Source IP address and port number from TCP/IP header
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +–: a plus or minus sign to indicate time zone offset from UTC (+ or –) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$URL	HTTP URL address accessed where spyware was found
$user	Client IP address or username, if username is identified by AD/LDAP integration
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

181248 - Unexpected Connection Loss

Error Message `181248:<$timestamp> A connection was dropped from source $srcip:$srcport to destination $dstip:$dstport via $proto. ($info)`

Example `181248: 2009-03-19T14:23:54-0700 A connection was dropped from source 1.1.1.1:132 to destination 2.2.2.2:25 via SMTP. (network timeout)`

Explanation A connection was not closed normally by the source or the destination. Abnormal closures may be due to timeouts or errors from the source or the destination, or possibly timeouts or errors that occurred in the content security application.

Recommended Action None required unless too many disconnections have been reported or usability issues were discovered.

2113664 - Virus Detected in HTTP but Delivered

Error Message

```
2113664:<$timestamp> Virus - $vname ($vtype) was detected from source
$srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation
was $vip:$vport. The file “$filename” was passed. The URL accessed was “$URL”.
```

Example

```
2113664: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was
detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The
source of violation was 22.22.22.22:80. The file “eicar.com” was passed. The URL
accessed was “http://www.example.com/eicar.com”.
```

Explanation A virus was detected in an HTTP transaction. The infected content was delivered “as-is”.

Recommended Action Perform virus scanning on the source and/or the destination, if they are internal. Consider changing the policy settings to block (not deliver) viruses.

2113792 - Virus Blocked in HTTP

Error Message

```
2113792:<$timestamp> Virus - $vname ($vtype) was detected from source
$srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation
was $vip:$vport. The file “$filename” was blocked. The URL accessed was “$URL”.
```

Example

```
2113792: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was
detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The
source of violation was 22.22.22.22:80. The file “eicar.com” was blocked. The URL
accessed was “http://www.example.com/eicar.com”.
```

Explanation A virus was detected in an HTTP transaction. The infected content was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2113920 - Virus Detected and Cleaned in HTTP

Error Message

```
2113920:<$timestamp> Virus - $vname ($vtype) was detected from source
$srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation
was $vip:$vport. The file “$filename” was cleaned. The URL accessed was “$URL”.
```

Example

```
2113920: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was
detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The
source of violation was 22.22.22.22:80. The file “eicar.com” was cleaned. The URL
accessed was “http://www.example.com/eicar.com”.
```

Explanation A virus was detected in an HTTP transaction. The infected content was cleaned then delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2162816 - Spyware Detected in HTTP but Delivered

Error Message 2162816:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip*:*$srcport* to destination *$dstip*:*$dstport* via HTTP. The source of violation was *$vip*:*$vport*. The file “*$filename*” was passed. The URL accessed was “*$URL*”.

Example 2162816: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file “clickme.com” was passed. The URL accessed was “http://www.example.com/clickme.com”.

Explanation Spyware was detected in an HTTP transaction. The spyware was delivered “as-is.”

Recommended Action Perform spyware scanning on the receiving machine and the violation source, if they are internal. Consider changing the policy settings to block (not deliver) spyware.

2162944 - Spyware Blocked in HTTP

Error Message 2162944:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip*:*$srcport* to destination *$dstip*:*$dstport* via HTTP. The source of violation was *$vip*:*$vport*. The file “*$filename*” was blocked. The URL accessed was “*$URL*”.

Example 2162944: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file “clickme.com” was blocked. The URL accessed was “http://www.example.com/clickme.com”.

Explanation Spyware was detected in an HTTP transaction. The spyware was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2212096 - File Blocked in HTTP

Error Message 2212096:<*$timestamp*> File Blocking- *$pname* (*$prule*) was detected from source *$srcip*:*$srcport* to destination *$dstip*:*$dstport* via HTTP. The source of violation was *$vip*:*$vport*. The file “*$filename*” was blocked. The URL accessed was “*$URL*”.

Example 2212096: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The file “iplayer.zip” was blocked. The URL accessed was “http://www.example.com/iplayer/iplayer.zip”.

Explanation A file blocking violation was detected during HTTP access. The access was blocked.

Recommended Action None required.

2228480 - HTTP URL Blocking Blocked

Error Message `2228480:<$timestamp> URL Blocking - user-defined ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The URL was blocked. The URL accessed was “$URL”. The user identity was “$user” ($group). The policy matched was “$pname”.`

Example `2228480: 2009-03-19T14:23:54-0700 URL Blocking - user-defined (*play*) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was “http://www.example.com/iplayer/index.html”. The user identity was “finance/joek” (US West BU Finance Dept). The policy matched was “Global Policy”.`

Explanation An HTTP access violation was detected based on URL Blocking policy. The access was blocked.

Recommended Action None required.

2244608 - URL Rating Module Error

Error Message `2244608:<$timestamp> URL Rating Module: $info`

Example `2244608: 2009-03-19T14:23:54-0700 URL Rating Module: Error: Failed to rate URL, rc=-231`

Explanation The URL Rating Module reports operational information.

Recommended Action Verify network setup and connections to the Internet.

2244609 - URL Rating Module Information

Error Message `2244609:<$timestamp> URL Rating Module: $info`

Example `2244609: 2009-03-19T14:23:54-0700 URL Rating Module: Started`

Explanation The URL Rating Module reports operational information.

Recommended Action None required.

2244864 - HTTP URL Filtering Blocked

Error Message 2244864:<*$timestamp*> URL Filtering - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The URL was blocked. The URL accessed was "*$URL*". The user identity was *$user ($group)*. The policy matched was "*$pname*".

Example 2244864: 2009-03-19T14:23:54-0700 URL Filtering - Company Prohibited Sites (Gambling) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was "http://www.example.com/casino/index.html". The user identity was "finance/joek" (Finance Dept). The policy matched was "Global Policy".

Explanation An HTTP access violation was detected based on the URL Filtering policy. The access was blocked.

Recommended Action None required.

2359424 - HTTP Unscanned Content Detected but Delivered

Error Message 2359424:<*$timestamp*> Unscanned - *$unscanexp* (N/A) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file "*$filename*" was passed. The URL accessed was "*$URL*".

Example 2359424: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "broken.zip" was passed. The URL accessed was "http://www.example.com/broken.zip".

Explanation An unscanned attachment was detected during HTTP access. CSC did not scan this content because of a resource or protocol limitation. The original content was delivered anyway.

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

2359552 - Unscanned Content Blocked in HTTP

Error Message `2359552:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The file "$filename" was blocked. The URL accessed was "$URL".`

Example `2359552: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "broken.zip" was blocked. The URL accessed was "http://www.example.com/broken.zip".`

Explanation Unscanned content was blocked in an HTTP transaction.

Recommended Action Blocking unscanned files may break certain applications that use the "resume transfer" function, such as Windows Update. Customers can either deliver the unscanned content or set the ASA Modular Policy Framework policy to avoid scanning traffic to and from the destination IP address.

2392320 -HTTP Web Reputation Blocked

Error Message `2392320:<$timestamp> Web Reputation - Potentially malicious URL was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The URL was blocked. The URL accessed was "$URL". The user identity was $user ($group). The policy matched was "$pname".`

Example `2392320: 2009-03-19T14:23:54-0700 Web Reputation - Potentially malicious URL was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was "http://www.example.com/casino/index.html". The user identity was "finance/joek" (US West BU Finance Dept). The policy matched was "Global Policy".`

Explanation An HTTP access violation was detected based on the Web Reputation policy. The access was blocked.

Recommended Action None required.

Messages 4423808- 6603008

Table A-2 shows the variables used by syslog messages in this section.

Table A-2 Messages 4423808 - 6603008 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types. • Content filtering uses "Subject," "Body," and "Attachment."
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient's e-mail address
$sender	Sender's e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

4423808 - SMTP Spam Detected (Match in ERS Standard Database List)

Error Message `4423808:<$timestamp> Spam (identified by Email Reputation Standard Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `4423808: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Standard Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was passed.`

Explanation An inbound SMTP connection was flagged as potential spam by the ERS Standard Database list. The SMTP connection was allowed. The actual e-mail delivery was still subject to other content scanning.

Recommended Action None required. Consider blocking ERS if too much spam is received.

4423936 - SMTP Spam Blocked (Match in ERS Standard Database List)

Error Message `4423936:<$timestamp> Spam (identified by Email Reputation Standard Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `4423936: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Standard Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was blocked.`

Explanation An inbound SMTP connection was blocked by the ERS Standard Database list. This blocking may prevent one or more potential spam e-mail messages from being delivered.

Recommended Action None required. If this blocking is incorrect, try the following actions:

- Add *$srcip* to the ERS Exception List.
- Visit the ERS Portal to update the configuration or dispute.

4440192 - SMTP Spam Detected (Match in ERS Dynamic Database List)

Error Message `4440192:<$timestamp> Spam (identified by Email Reputation Dynamic Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `4440192: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Dynamic Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was passed.`

Explanation An inbound SMTP connection was flagged as potential spam by the ERS Dynamic Database list. The SMTP connection was allowed. The actual e-mail delivery was still subject to other content scanning.

Recommended Action None required. Consider blocking ERS if too much spam is received.

4440320 - SMTP Spam Blocked (Match in ERS Dynamic Database List)

Error Message `4440320:<$timestamp> Spam (identified by Email Reputation Dynamic Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `4440320: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Dynamic Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was blocked.`

Explanation An inbound SMTP connection was blocked by the ERS Dynamic Database list. This blocking may stop one or more potential spam e-mail messages from being delivered.

Recommended Action None required. If this blocking is incorrect, try the following actions:

- Add *$srcip* to the ERS Exception List.
- Visit the ERS Portal to update the configuration or dispute.

6307968 - POP3 Virus Detected but Delivered

Error Message `6307968:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6307968: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in a POP3 message. The mail was delivered anyway.

Recommended Action Perform virus scanning on the receiving machine to ensure virus removal. Perform virus scanning on the POP3 server, if it is internal. Consider changing the policy settings to block (not deliver) viruses.

6308096 - POP3 Virus Blocked

Error Message 6308096:<*$timestamp*> Virus - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was blocked then the mail was *$msgact*.

Example 6308096: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled “Hello from eicar” from sender “user1@example.com” to recipient “user2@example.com”. The file “eicar.com” was blocked then the mail was passed.

Explanation A virus was detected in a POP3 message. The infected attachment was removed, and the mail was delivered.

Recommended Action Perform virus scanning on the POP3 server, if it is internal.

6308224 - POP3 Virus Cleaned and Delivered

Error Message 6308224:<*$timestamp*> Virus - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was cleaned then the mail was *$msgact*.

Example 6308224: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled “Hello from eicar” from sender “user1@example.com” to recipient “user2@example.com”. The file “eicar.com” was cleaned then the mail was passed.

Explanation A virus was detected in a POP3 message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action Customers should perform virus scanning on the POP3 server, if it is internal.

6357120 - Spyware Detected in POP3 but Delivered

Error Message 6357120:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was passed then the mail was *$msgact*.

Example 6357120: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled “Hello from spy” from sender “user1@example.com” to recipient “user2@example.com”. The file “clickme.exe” was passed then the mail was passed.

Explanation Spyware was detected in a POP3 message. The mail was delivered “as-is.”

Recommended Action Perform spyware scanning on the receiving machine to ensure spyware removal. Consider changing the customer's policy setting to block (not deliver) spyware.

6357248 - Spyware Blocked in POP3

Error Message 6357248:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was blocked then the mail was *$msgact*.

Example 6357248: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled “Hello from spy” from sender “user1@example.com” to recipient “user2@example.com”. The file “clickme.exe” was blocked then the mail was passed.

Explanation Spyware was detected in a POP3 message. The mail was delivered without the detected spyware.

Recommended Action None required.

6373504 - POP3 IntelliTrap Detected by Delivered

Error Message `6373504:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6373504: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.`

Explanation IntelliTrap was detected in a POP3 message. The original mail was delivered "as is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal. Consider changing the policy settings to block (not deliver) IntelliTrap.

6373632 - POP3 IntelliTrap Blocked

Error Message `6373632:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6373632: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation IntelliTrap was detected in a POP3 message. The malware was removed and the mail was delivered.

Recommended Action None required.

6406272 - File Detected in POP3 Message but Delivered

Error Message `6406272:<$timestamp> File Blocking - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6406272: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was passed then the mail was passed.`

Explanation A file blocking violation was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6406400 - File Blocked in POP3 Message

Error Message `6406400:<$timestamp> File Blocking - $pname ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6406400: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was blocked then the mail was passed.`

Explanation A file blocking violation was detected in a POP3 message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6455424 - E-mail Content-filtering Violation Detected in POP3 Message

Error Message `6455424:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `6455424: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A content-filtering violation was detected in POP3 message. The mail was delivered.

Recommended Action None required.

6455552 - E-mail Content-filtering Violation Detected in POP3 Message

Error Message `6455552:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `6455552: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A content-filtering violation was detected in POP3 message. The mail was blocked.

Recommended Action None required.

6553728 - Unscanned Content Detected in POP3 but Delivered

Error Message `6553728:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6553728: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was passed then the mail was passed.`

Explanation An unscanned attachment was detected in a POP3 message, and CSC did not scan this content because of a resource or protocol limitation. The original mail was delivered "as-is."

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

6553856 - Unscanned Content Blocked in POP3

Error Message `6553856:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6553856: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was blocked then the mail was passed.`

Explanation An unscanned attachment was detected in a POP3 message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6602880 - Spam Detected in POP3

Error Message `6602880:<$timestamp> Spam (identified by pattern-recognition technology) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `6602880: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A spam mail was detected in a POP3 message. The mail was delivered "as-is."

Recommended Action None required.

6603008 - Spam Blocked in POP3

Error Message `6603008:<$timestamp> Spam (identified by pattern-recognition technology) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `6603008: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A spam mail was detected in a POP3 message. The mail was blocked.

Recommended Action None required.

Messages 8405120 - 8651008

Table A-3 shows the variables used by syslog messages in this section.

Table A-3 Messages 8405120 - 8651008 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$srcip:$srcport	Source IP address and port number from TCP/IP header
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +–: a plus or minus sign to indicate time zone offset from UTC (+ or –) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

8405120 - Virus Detected in FTP but Delivered

Error Message `8405120:<`*`$timestamp`*`> Virus - `*`$vname`*` (`*`$vtype`*`) was detected from source `*`$srcip:$srcport`*` to destination `*`$dstip:$dstport`*` via FTP. The source of violation was `*`$vip:$vport`*`. The file "`*`$filename`*`" was passed.`

Example `8405120: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was passed.`

Explanation A virus was detected in an FTP transaction. The infected content was delivered.

Recommended Action Customers should perform virus scanning on the source and/or the destination, if they are internal. Consider changing the policy setting to block (not deliver) viruses.

8405248 - Virus Blocked in FTP

Error Message `8405248:<`*`$timestamp`*`> Virus - `*`$vname`*` (`*`$vtype`*`) was detected from source `*`$srcip:$srcport`*` to destination `*`$dstip:$dstport`*` via FTP. The source of violation was `*`$vip:$vport`*`. The file "`*`$filename`*`" was blocked.`

Example `8405248: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was blocked.`

Explanation A virus was detected in an FTP transaction. The infected content was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

8405376 - FTP Virus Cleaned and Delivered

Error Message `8405376:<`*`$timestamp`*`> Virus - `*`$vname`*` (`*`$vtype`*`) was detected from source `*`$srcip:$srcport`*` to destination `*`$dstip:$dstport`*` via FTP. The source of violation was `*`$vip:$vport`*`. The file "`*`$filename`*`" was cleaned.`

Example `8405376: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was cleaned.`

Explanation A virus was detected in a FTP transaction. The infected content was cleaned then delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

8454272 - Spyware Blocked in FTP but Delivered

Error Message 8454272:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via FTP. The source of violation was *$vip:$vport*. The file "*$filename*" was passed.

Example 8454272: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "clickme.com" was passed.

Explanation Spyware was detected in an FTP transaction. The spyware was passed "as-is."

Recommended Action Perform spyware scanning on the receiving machine and the source of violation, if they are internal. Consider changing the policy setting to block (not deliver) spyware.

8454400 - Spyware Blocked in FTP

Error Message 8454400:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via FTP. The source of violation was *$vip:$vport*. The file "*$filename*" was blocked.

Example 8454400: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "clickme.com" was blocked.

Explanation Spyware was detected in an FTP transaction. The spyware was blocked.

Recommended Action Perform spyware scanning on the violation source, if it is internal.

8503552 - File Blocked in FTP

Error Message 8503552:<*$timestamp*> File Blocking - *$pname* (*$prule*) was detected from source $srcip:$srcport to destination *$dstip:$dstport* via FTP. The source of violation was *$vip:$vport*. The file "*$filename*" was blocked.

Example 8503552: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "iplayer.zip" was blocked.

Explanation A file blocking violation was detected during FTP access. The access was blocked.

Recommended Action None required.

8650880 - Unscanned Content Detected in FTP but Delivered

Error Message `8650880:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was passed.`

Example `8650880: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "broken.zip" was passed.`

Explanation An unscanned file was detected during FTP access. CSC did not scan this content because of a resource or protocol limitation. The file was passed "as-is."

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

8651008 - Unscanned Content Blocked in FTP

Error Message `8651008:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was blocked.`

Example `8651008: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "broken.zip" was blocked.`

Explanation Unscanned content was blocked in an FTP transaction.

Recommended Action Blocking unscanned files may break certain applications that use the "resume transfer" function, such as Windows Update. Customers can either deliver the unscanned content or set the ASA MPF policy to avoid scanning traffic to and from the destination IP address.

Messages 16777216 - 18874370

Table A-4 shows the variables used by syslog messages in this section.

Table A-4 Messages 16777216 - 18874370 Section Variables

Variable	Description
$component	Application components, such as Protocol Proxy, Scan Server, Service Module, System Monitor, Event Manager, Config Manager, URL Rating Module, E-mail Notification Module, Virus Scan Engine, Virus Pattern, and Spyware Pattern
$info	Information that explains more about the syslog message
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$version	The product or component version number

16777216 - Update Not Successful

Error Message `16777216:<$timestamp> Component update failed: $component/$version ($info)`

Example
```
16777216: 2009-03-19T14:23:54-0700 Component update failed: 
VirusScanEngine/9.0.1000 (network timeout)
```

Explanation A content security component has failed to be updated.

Recommended Action Verify your network configuration, network connectivity, or ActiveUpdate configuration.

16777217 - Update Status Report

Error Message 16777217:<*$timestamp*> Component successfully updated: *$component*/*$version*

Example 16777217: 2009-03-19T14:23:54-0700 Component successfully updated: VirusScanEngine/8.5.1001

Explanation A content security component has been successfully updated.

Recommended Action None required.

18874368 - License Status Update

Error Message 18874368:<*$timestamp*> The Content Security license has been updated. License Details: *$info*

Example 18874368: 2009-03-19T14:23:54-0700 The Content Security license has been updated. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31

Explanation The Content Security license has been updated because of license activation or license renewal.

Recommended Action None required.

18874369 - License has Expired

Error Message 18874369:<*$timestamp*> The Content Security license has expired. License Details: *$info*

Example 18874369: 2009-03-19T14:23:54-0700 The Content Security license has expired. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31

Explanation The Content Security license has expired and may stop inspecting traffic.

Recommended Action To renew or purchase the license, contact your reseller or visit http://www.cisco.com/go/asa.

18874370 - License Expiration Reminder

Error Message `18874370:<$timestamp> The Content Security license is due to expire. License Details: $info`

Example `18874370: 2009-03-19T14:23:54-0700 The Content Security license is due to expire. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31`

Explanation The Content Security license is going to expire on the specified expiration date.

Recommended Action Renew the Content Security license before the product expires. Contact your reseller or visit http://www.cisco.com/go/asa.

Messages 21151744 - 21184513

Table A-5 shows the variables used by syslog messages in this section.

Table A-5 Messages 21151744 - 21184513 Section Variables

Variable	Description
$info	Information that explains more about the syslog message
$proto	Protocol name or value, such as SMTP, POP3, HTTP, FTP
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

21151744 - System Monitoring Critical Condition Message

Error Message `21151744:<$timestamp> System Monitor: $info`

Example `21151744: 2009-03-19T14:23:54-0700 System Monitor: HTTP service is DOWN.`

Explanation The System Monitor reports critical operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

21151745 - System Monitoring Error Condition Message

Error Message `21151745:<$timestamp> System Monitor: $info.`

Example `21151745: 2009-03-19T14:23:54-0700 System Monitor: Invalid ASA state is received.`

Explanation The System Monitor reports error operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

21151746 - System Monitoring Informational Message

Error Message `21151746:<$timestamp> System Monitor: $info.`

Example `21151746: 2009-03-19T14:23:54-0700 System Monitor: CSC SSM is not activated.`

Explanation The System Monitor reports normal operational information.

Recommended Action None required.

21151747 - System-level Notice

Error Message `21151747:<$timestamp> System Monitor: $info.`

Example `21151747: 2009-03-19T14:23:54-0700 System Monitor: Set CSC SSM Application Status to UP.`

Explanation The System Monitor reports normal operational information.

Recommended Action None required.

21152512 - System is Ready

Error Message `21152512:<$timestamp> Content Security system is ready.`

Example `21152512: 2009-03-19T14:23:54-0700 Content Security system is ready.`

Explanation The content security system is ready to inspect traffic.

Recommended Action None required.

21152513 - System is Reloading

Error Message `21152513:<$timestamp> Content Security system is reloading. ($info)`

Example `21152513: 2009-03-19T14:23:54-0700 Content Security system is reloading. (configuration update)`

Explanation The content security system is reloading for administrative reasons, such as a configuration update or a pattern/engine update.

Recommended Action If the system becomes ready shortly, none required.

21152514 - System is Down

Error Message `21152514:<$timestamp> Content Security system has failed. ($info)`

Example `21152514: 2009-03-19T14:23:54-0700 Content Security system has failed. (Scan Server has failed)`

Explanation The content security system has failed and is unable to inspect traffic.

Recommended Action Check for a valid license or system failure. Reload the system if necessary.

21184512 - Maximum Connections Reached

Error Message `21184512:<$timestamp> The maximum number of connections for $proto has been reached. New connections will be kept in a backlog and may time out.`

Example `21184512: 2009-03-19T14:23:54-0700 The maximum number of connections for SMTP has been reached. New connections will be kept in a backlog and may time out.`

Explanation The device has reached its maximum concurrent scanning for the specific protocol. New connections with the same protocol will be queued and may time out. Network performance may be affected.

Recommended Action If this issue occurs frequently, the device may be underpowered for the amount of traffic being passed. Consider scanning less traffic with ASA MPF skip rules or segmenting the network with more adaptive security appliances.

21184513 - Maximum Connections Returned to Normal

Error Message `21184513:<$timestamp> The maximum number of connections for $proto has returned to normal threshold.`

Example `21184513: 2009-03-19T14:23:54-0700 The maximum number of connections for SMTP has returned to normal threshold.`

Explanation The concurrent connections of the specific protocol have fallen below 80 percent of the maximum capacity. New connections of the specific protocol can be processed normally.

Recommended Action None required.

Messages 33570944 - 33865984

Table A-6 shows the variables used by syslog messages in this section.

Table A-6 Messages 33570944 - 33865984 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file-types. • Content filtering uses “Subject,” “Body,” and “Attachment.”
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient’s e-mail address
$sender	Sender’s e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

33570944 - Incoming Virus Detected in SMTP but Delivered

Error Message `33570944:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `33570944: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The mail was delivered "as-is."

Recommended Action Perform virus scanning on the receiving machine to ensure virus removal. Consider changing the policy settings to block (not deliver) viruses.

33571072 - Virus Blocked in SMTP (Incoming)

Error Message `33571072:<`*`$timestamp`*`> Virus -` *`$vname`* `(`*`$vtype`*`) was detected from source` *`$srcip:$srcport`* `to destination` *`$dstip:$dstport`* `via SMTP. The source of violation was` *`$vip:$vport`*`. The mail was titled "`*`$subject`*`" from sender "`*`$sender`*`" to recipient "`*`$recipient`*`". The file "`*`$filename`*`" was blocked then the mail was` *`$msgact`*`.`

Example `33571072: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was blocked then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The infected attachment was removed, and the mail was delivered.

Recommended Action None required.

33571200 - Incoming SMTP Virus Cleaned and Delivered

Error Message `33571200:<`*`$timestamp`*`> Virus -` *`$vname`* `(`*`$vtype`*`) was detected from source` *`$srcip:$srcport`* `to destination` *`$dstip:$dstport`* `via SMTP. The source of violation was` *`$vip:$vport`*`. The mail was titled "`*`$subject`*`" from sender "`*`$sender`*`" to recipient "`*`$recipient`*`". The file "`*`$filename`*`" was cleaned then the mail was` *`$msgact`*`.`

Example `33571200: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was cleaned then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action None required.

33620096 - Incoming SMTP Spyware Detected but Delivered

Error Message 33620096:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 33620096: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.

Explanation Spyware was detected in an inbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform spyware scanning on the receiving machine to ensure spyware removal. Consider changing the policy settings to block (not deliver) spyware.

33620224 - Incoming SMTP Spyware Blocked

Error Message 33620224:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 33620224: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.

Explanation Spyware was detected in an inbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action None required.

33636480 - Incoming SMTP IntelliTrap Detected but Delivered

Error Message 33636480:<*$timestamp*> IntelliTrap - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 33636480: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.

Explanation IntelliTrap was detected in an inbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal. Consider changing the policy settings to block (not deliver) IntelliTrap.

33636608- Incoming SMTP IntelliTrap Blocked

Error Message 33636608:<*$timestamp*> IntelliTrap - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 33636608: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.

Explanation IntelliTrap was detected in an inbound SMTP message. The malware was removed and the mail was delivered.

Recommended Action None required.

33669248 - Incoming SMTP File Blocking Detected but Delivered

Error Message 33669248:<*$timestamp*> File Blocking - *$pcat* (*$prule*) was detected from source *$srcip:$srcpor*t to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 33669248: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was passed then the mail was passed.

Explanation Spyware was detected in an outbound SMTP message. The mail was delivered "as-is."

Recommended Action Perform spyware scanning on the sending machine to ensure spyware removal. Consider changing policy settings to block (not deliver) spyware.

33669376 - File Blocked in Incoming SMTP Message

Error Message 33669376:<*$timestamp*> File Blocking - *$pname* (*$prule)* was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 33669376: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was blocked then the mail was passed.

Explanation A file blocking violation was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

33718400 - E-mail Content-filtering Violation Blocked in SMTP - Incoming

Error Message 33718400:<*$timestamp*> Content-Filtering - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The mail was passed.

Example 33718400: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was delivered.

Recommended Action None required.

33718528 - E-mail Content-filtering Violation Blocked in SMTP - Incoming

Error Message 33718528:<*$timestamp*> Content-Filtering - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The mail was blocked.

Example 33718528: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was blocked.

Recommended Action None required.

33816704 - Incoming SMTP Unscanned Content Detected and Delivered

Error Message `33816704:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `33816704: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was passed then the mail was passed.`

Explanation An unscanned attachment was detected in an inbound SMTP message, and CSC did not scan this content because of a resource or protocol limitation. The mail was delivered "as-is."

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

33816832 - Incoming SMTP Unscanned Content Blocked

Error Message `33816832:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `33816832: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was blocked then the mail was passed.`

Explanation An unscanned attachment was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

33865856 - SMTP Spam is Detected but Delivered

Error Message `33865856:<$timestamp> Spam (identified by pattern-recognition technology) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `33865856: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A spam mail was detected in a SMTP message. The mail was delivered "as is."

Recommended Action None required.

33865984 -SMTP Spam Blocked

Error Message `33865984:<$timestamp> Spam (identified by pattern-recognition technology) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `33865984: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A spam mail was detected in a SMTP message. The mail was blocked.

Recommended Action None required.

Messages 35668096 - 48234497

Table A-7 shows the variables used by the syslog messages in this section.

Table A-7 Messages 35668096 - 48234497 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$info	Information that explains more about the syslog message.
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types. • Content filtering uses "Subject," "Body," and "Attachment."
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient's e-mail address
$sender	Sender's e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable (continued)	Description (continued)
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

35668096 - Outgoing SMTP Virus Detected but Delivered

Error Message `35668096:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `35668096: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The mail was delivered "as-is."

Recommended Action Perform virus scanning on the violation source, if it is internal. Consider changing the policy settings to block (not deliver) viruses.

35668224 - Virus Blocked in SMTP-Outgoing

Error Message `35668224:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `35668224: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was blocked then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The infected attachment was removed, and the mail was delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

35668352 - Outgoing SMTP Virus Cleaned and Delivered

Error Message `35668352:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was cleaned then the mail was $msgact.`

Example `35668352: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was cleaned then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

35717248 - Outgoing SMTP Spyware Detected but Delivered

Error Message `35717248:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `35717248: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation Spyware was detected in an inbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action None required.

35717376 - Outgoing SMTP Spyware Blocked

Error Message `35717376:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `35717376: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation Spyware was detected in an outbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action Perform spyware scanning on the sending machine to ensure spyware removal.

35733632 - Outgoing SMTP IntelliTrap Detected but Delivered

Error Message `35733632:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `35733632: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.`

Explanation IntelliTrap was detected in an outbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal.

35733760- Outgoing SMTP IntelliTrap Blocked

Error Message `35733760:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `35733760: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation IntelliTrap was detected in an outbound SMTP message. The malware was removed and the mail was delivered.

Recommended Action Perform malware scanning on the sending machine to ensure malware removal.

35766400 - Outgoing SMTP File Blocking Detected but Delivered

Error Message 35766400:<*$timestamp*> File Blocking - *$pname* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 35766400: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was passed then the mail was passed.

Explanation A file blocking violation was detected in an outbound SMTP message. The mail was delivered with the original attachments.

Recommended Action None required.

35766528 - File Blocked on Outgoing SMTP Message

Error Message 35766528:<*$timestamp*> File Blocking - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 35766528: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was blocked then the mail was passed.

Explanation A file blocking violation was detected in a POP3 message. The mail was delivered with original attachments.

Recommended Action None required.

35815552 - E-mail Content-filtering Violation Detected in SMTP Outgoing

Error Message `35815552:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `35815552: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A content-filtering violation was detected in SMTP-Outgoing message. The mail was delivered.

Recommended Action None required.

35815680 - E-mail Content-filtering Violation Blocked in SMTP Outgoing

Error Message `35815680:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `35815680: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was blocked.

Recommended Action None required.

35913856 - Outgoing SMTP Unscanned Content Detected but Delivered

Error Message 35923856:<*$timestamp*> Unscanned - *$unscanexp* (N/A) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 35923856: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was passed then the mail was passed.

Explanation An unscanned attachment was detected in an outbound SMTP message. CSC did not scan this content because of a resource or protocol limitation. The mail was delivered "as-is."

Recommended Action None required.

35913984 - Unscanned Content Blocked in SMTP (Outgoing)

Error Message 35913984:<*$timestamp*> Unscanned - *$unscanexp* (N/A) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 35913984: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was blocked then the mail was passed.

Explanation An unscanned attachment was detected in an outbound SMTP message. The detected attachment was removed, and the mail was delivered.

Recommended Action None required.

39845888 - Scan Server Error

Error Message 39845888:<*$timestamp*> Scan Server: *$info*

Example 39845888: 2009-03-19T14:23:54-0700 Scan Server: Unable to allocate memory block for scan

Explanation The Scan Server reports abnormal operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

39845889 - Scan Server Information

Error Message `39845889:<$timestamp> Scan Server: $info`

Example `39845889: 2009-03-19T14:23:54-0700 Scan Server: Started`

Explanation The Scan Server reports abnormal operational information.

Recommended Action None required.

44220416 - Service Module Information

Error Message `44220416:<$timestamp> Service Module: $info`

Example `44220416: 2009-03-19T14:23:54-0700 Service Module: Application state: Up`

Explanation The Service Module reports operational information.

Recommended Action None required.

44220419 - Service Module Error

Error Message `44220419:<$timestamp> Service Module: $info`

Example `44220419: 2009-03-19T14:23:54-0700 Service Module: Init CP failed`

Explanation The service module reports abnormal operational information.

Recommended Action If the service module does not recover automatically, reboot theCSC SSM.

46317569 - Failover Module Information

Error Message `46317569:<$timestamp> Failover Module: $info`

Example `46317569: 2009-03-19T14:23:54-0700 Failover Module: Started`

Explanation The Failover Module reports operational information.

Recommended Action None required.

46317570 - Failover Module Error

Error Message `46317570:<$timestamp> Failover Module: $info`

Example `46317570: 2009-03-19T14:23:54-0700 Failover Module: HELLO handler error - The peers do not have the same software and/or hardware version.`

Explanation The Failover Module reports abnormal operational information.

Recommended Action Verify the failover configuration and network setup between the two peers.

48234496- Log Server Information

Error Message `48234496:<$timestamp> Log Server: $info`

Example `48234496: 2009-03-19T14:23:54-0700 Log Server: Unable to allocate memory`

Explanation The Log Server reports abnormal operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

48234497- Log Server Information

Error Message `48234497:<$timestamp> Log Server: $info`

Example `48234497: 2009-03-19T14:23:54-0700 Log Server: Started`

Explanation The Log Server reports operational information.

Recommended Action None required.

Messages 52429184 - 52430720

Table A-8 shows the variables used in the syslog messages in this section.

Table A-8 Messages 52429184 - 52430720 Section Variables

Variable	Description
$component	Application component names, such as: Protocol Proxy, Scan Server, Service Module, System Monitor, Event Manager, Config Manager, URL Rating Module, E-mail Notification Module, Virus Scan Engine, Virus Pattern, and Spyware Pattern
$info	Information that explains more about the syslog message
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$srcip	Source IP address from TCP/IP header

Variable (continued)	Description (continued)
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delay or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$vname	Name of the virus or spyware detected

52429184 - DCS Successful Cleanup

Error Message `52429184:<`*`$timestamp`*`> Damage Cleanup - `*`$vname`*` (`*`$prule`*`) was cleaned successfully at `*`$srcip.`*

Example `52429184: 2009-03-19T14:23:54-0700 Damage Cleanup - WORM_SKA.A (Trojan) was cleaned successfully at 1.1.1.1.`

Explanation An internal machine was cleaned up successfully by the Damage Cleanup Service.

Recommended Action None required.

52430592 - DCS Cleanup Failed

Error Message `52430592:<`*`$timestamp`*`> Damage Cleanup - `*`$vname`*` (`*`$prule`*`) failed to be cleaned at `*`$srcip`*`.`

Example `52430592: 2009-03-19T14:23:54-0700 Damage Cleanup - WORM_SKA.A (Trojan) failed to be cleaned at 1.1.1.1.`

Explanation The Damage Cleanup Service failed to clean up an internal machine.

Recommended Action Perform manual malware cleanup on the machine specified.

52430720 - DCS Service Failed

Error Message `52430720:<$timestamp> Damage Cleanup - DCS server unreachable for cleanup at $srcip.`

Example `52430720: 2009-03-19T14:23:54-0700 Damage Cleanup - DCS server unreachable for cleanup at 1.1.1.1.`

Explanation The DCS server cannot be reached by CSC.

Recommended Action Verify the DCS server installation and configuration.

APPENDIX B

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:

The Trend Micro InterScan for Cisco CSC SSM software is preinstalled on the adaptive 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 the *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 B-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 B-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		❑

Table B-1 Installation Checklist (continued)

Information Requested	Information Entered	Completed
Domain name		❑
Primary DNS IP address		❑
Secondary DNS IP address (optional)		❑
Gateway IP address		❑
Proxy server? (optional) If yes: Proxy server IP address Proxy server port number		❑ ❑ ❑
Domain name for incoming e-mail		❑
Administrator password for the CSC SSM console	Do not record your password.	—
Administrator e-mail address		❑
Notification e-mail server IP address		❑
Notification e-mail server port number		❑
Base License Activation Code		❑
Plus License Activation Code (optional)		❑

Preparing to Reimage the Cisco CSC SSM

You should reimage the CSC SSM under the following conditions:

- No previous image of CSC has been installed on the SSM.
- The CSC image is suspected of being corrupted beyond repair.
- The CSC card is rebooting regularly.
- The CSC card becomes unresponsive or unstable after an upgrade.

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

Note The TFTP server must support files sizes greater than 60 MB. The .bin files are full binary images that are to be uploaded via a TFTP server. The .pkg files are used to upgrade image files from the CSC Admin Console, which are then uploaded through a web browser. Do not upload .bin files using the CSC Admin Console.

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/csc6.2.xxxx.x.bin]:tftp://insidehost/csc6.2.xxxx.x.bin
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
2007
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=csc6.2.xxxx.x.bin
Slot-1 211>   CONFIG=
Slot-1 212> tftp csc6.2.xxxx.x.bin@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 2007
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

hostname# show module 1 details
```

Sample 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 6.2.xxxx.x
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 6.2.xxxx.x
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 6 Open a command session.

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

Step 7 Log in to Trend Micro InterScan for Cisco CSC SSM using the default login name “cisco” and password “cisco.”

```
login: cisco
Password:
```

Step 8 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 B-8
- Viewing or Modifying Network Settings, page B-9
- Viewing Date and Time Settings, page B-9
- Viewing Product Information, page B-9
- Viewing or Modifying Service Status, page B-10
- Using Password Management, page B-10
- Restoring Factory Default Settings, page B-12
- Troubleshooting Tools, page B-13
- Changing the Management Port Console Access Settings, page B-17
- Pinging an IP Address, page B-17
- Exiting the Setup Wizard, page B-18

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

Step 1 Log in to the adaptive 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
---------------------------------------------------------------------------
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] 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 6.2.xxxx.x
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:       6.2.xxxx.x
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 6.2.xxxx.x
```

```
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 8-13.

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:
```

Note Password characters include: ~ ! @ # $ % ^ & * ( ) _ + ` - = { } | [ ] \ : ” ; ’ < > ? , . / . The plus sign is not a valid character if you change the password through the CSC SSM console. This symbol only works through the CLI.

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 B-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 B-13
- Showing System Information, page B-14
- Collecting Logs, page B-16
- Enabling Packet Tracing, page B-16
- Modifying Upload Settings, page B-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. Modify Management Port Console Access Settings
7. Return to Main Menu

Enter a number from [1-7]:
```

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] y
```

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

This warning only appears the first time you enable the root account. After 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 choose 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 B-14
- Uploading System Information, page B-15

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 Jul 24 18:38:01 PST 2007 (-8)

System is: Up

# Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.02.xxxx.x
SSM Model: SSM-10

# Scan Engine and Pattern Information
Virus Scan Engine: 8.500.1002 (Updated: 2007-07-24 14:10:07)
Virus Pattern: 4.613.00 (Updated: 2007-07-23 14:10:39)
Grayware Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)
PhishTrap Pattern: 392 (Updated: 2007-07-23 14:13:28)
AntiSpam Engine: 15320 (Updated: 2007-07-24 14:11:04)
AntiSpam Rule: 3.8.1029 (Updated: 2007-07-24 14:12:53)
IntelliTrap Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)
IntelliTrap Exception Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)

# 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:12/31/2007
Product:Plus License
```

```
Version: Standard
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
Status: Expired within grace period
Expiration date:12/31/2007

Daily Node Count: 0
Current Node Count: 0

# Kernel Information
Linux csc 2.4.26-cscssm #2 SMP Mon Mar 19 11:53:05 PST 2007 (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 B-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**. Upload them via FTP or TFTP to your server, so that Cisco TAC can then obtain them through a pre-arranged method. The logs are sent using the upload settings created by entering **5**, **Modify Upload Settings**. For more information, see Modifying Upload Settings, page B-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.

Enabling Packet Tracing

If you attempt to use the packet tracing command in CSC SSM, you will receive the following message:

“This function is now obsolete. Please use the ‘capture’ command in the ASA CLI for the ‘asa_dataplane’ interface.”

To enable packet tracing between the CSC SSM and adaptive security appliance, use the packet capture command shown in “Performing a Packet Capture” procedure on page 8-7.

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 **7**, **Return to Main Menu**.

Changing the Management Port Console Access Settings

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

Step 1 To reset the management port access control, enter **6.**

When you enter **6**, the following appears:

```
Troubleshooting Tools - Management Port Console Access Settings
---------------------------------------------------------------------

Current Telnet Access : Disabled
Current SSH Access    : Disabled
Modify Telnet Setting [1=Enable 2=Disable]: (default:2) 1
Modify SSH Setting [1=Enable 2=Disable]: (default:2) 1
Saving Management Port Console Access Settings: OK
Press Enter to continue ...
```

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

Step 3 When you are finished, enter **7**, **Return to Main Menu**.

Resetting the Management Port Access Control

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

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:

```
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.

Improving CSC SSM Performance

This section provides information about how to improve CSC SSM performance, and includes the following topics:

- Using the CSC SSM with a Management Network
- Example 1: CSC scanning from all interfaces
- Example 2: CSC scanning on specific ports

When users initially connect to the Internet through the CSC SSM, the CSC SSM contacts the Trend Micro web server using an HTTP request to determine the URL category for URL filtering and blocking. The CSC SSM scans this HTTP request again, which results in two HTTP connections for one initial request.

Note This additional scan is unnecessary. HTTP performance may improve when you prevent CSC SSM packets from being scanned unnecessarily.

Depending on your topology and configuration, you may be able to improve HTTP performance through the CSC SSM by configuring the adaptive security appliance to skip the scanning of management traffic.

To improve HTTP performance, perform the following steps:

Step 1 Collect the following information:

a. Determine the management IP address by executing the **show module 1 details** command on the adaptive security appliance or from the CSC SSM home page in ASDM.

```
hostname# show module 1 details
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: JAB093102KY
Firmware version: 1.0(10)0
Software version: CSC SSM 6.2.xxxx.x
MAC Address Range: 0013.c480.b183 to 0013.c480.b183
App. name: CSC SSM
App. Status: Up
App. Status Desc: CSC SSM scan services are available
App. version: 6.2.xxxx.x
Data plane Status: Up
Status: Up
HTTP Service: Up
Mail Service: Up
FTP Service: Up
Activated: Yes
Mgmt IP addr: 10.132.84.251
Mgmt web port: 8443
Peer IP addr: <not enabled>
hostname#
```

b. Determine which adaptive security appliance interface the SSM management port is connected to in the network.

Step 2 Configure service policies.

- To exclude SSM management traffic for scanning, you must use access list-based class maps in service policies. For more information, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*, at the following URL:

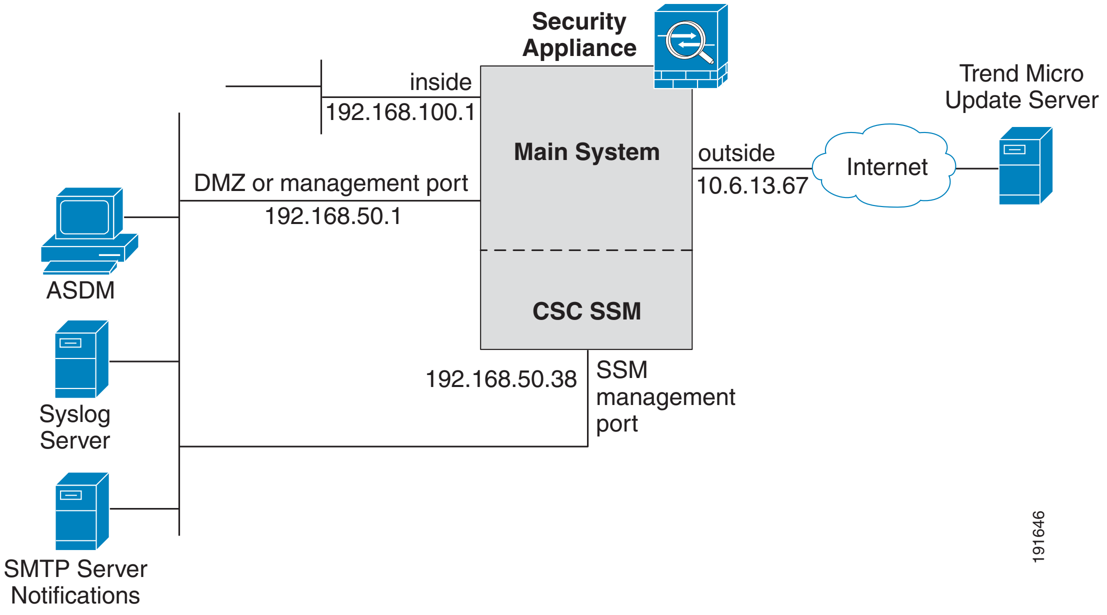
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- Do not configure a class map matched with a port.

Note If a NAT device exists between the SSM management port and the adaptive security appliance interface, be sure you use the applicable NAT device address.

Using the CSC SSM with a Management Network

Figure B-1 shows an example of a CSC SSM deployment with a management network. The SSM IP address is 192.168.50.38, and management traffic goes through the DMZ or management interface before reaching the Trend Micro web server on the Internet.

Figure B-1 CSC SSM Deployment with a Management Network



Example 1: CSC scanning from all interfaces

To perform CSC scanning from all interfaces, perform the following steps:

Step 1 Create an access list that matches all traffic, except traffic for the SSM management IP address, using the following commands:

```
access-list csc-scan line 1 extended deny tcp host 192.168.50.38 any
access-list csc-scan line 2 extended permit tcp any any
```

Note You may have different entries instead of "any any."

Step 2 Create the class map, global-class, with the access list that was created in Step 1, and apply this class map to a global policy for CSC scanning, using the following commands:

```
class-map global-class
   match access-list csc-scan
policy-map global-policy
   class global-class
      csc fail-open
service-policy global-policy global
```

Example 2: CSC scanning on specific ports

To perform CSC scanning on specific ports for SMTP, POP3, HTTP, and FTP traffic from a specific interface (for example, DMZ) and to exclude the SSM management IP address, perform the following steps:

Step 1 Create an access list, using the following commands:

```
access-list csc-scan line 1 extended deny tcp host 192.168.50.38 any
access-list csc-scan line 2 extended permit tcp any any eq smtp
access-list csc-scan line 3 extended permit tcp any any eq pop3
access-list csc-scan line 4 extended permit tcp any any eq http
access-list csc-scan line 5 extended permit tcp any any eq ftp
```

Step 2 Create the class map, dmz-class, with the access list that was created in Step 1, and apply this class-map to an interface (DMZ) for CSC scanning, using the following commands:

```
class-map dmz-class
   match access-list csc-scan
policy-map dmz-policy
    class dmz-class
        csc fail-open
service-policy dmz-policy interface dmz
```

Important Notes

- Your configuration may have an access list with different sources and destinations than the examples shown in this document. If the access list has **deny ACE** for the SSM management IP address, the configuration will still work.

- If you have both global and interface-specific service policies, you must add an access list to exempt the SSM management port IP address from scanning. For any service policy or class map, if the configuration includes URL categorization (HTTP) traffic, you must add an access list with **deny ACE** that exempts the SSM IP address from scanning.
- If the class-map on the SSM-connected interface uses port-matching criteria by means of the **match** command, you must convert these criteria into access list-based matching criteria to ensure that SSM management traffic is not scanned.

APPENDIX C

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

You should have already installed the Control Manager agent and registered CSC SSM with Control Manager using the CSC SSM Administration > Register to TMCM window. Control Manager is a central management console that runs on its own server, separate from CSC SSM. It 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 that 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 Control Manager, 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
- Ad hoc queries and reports

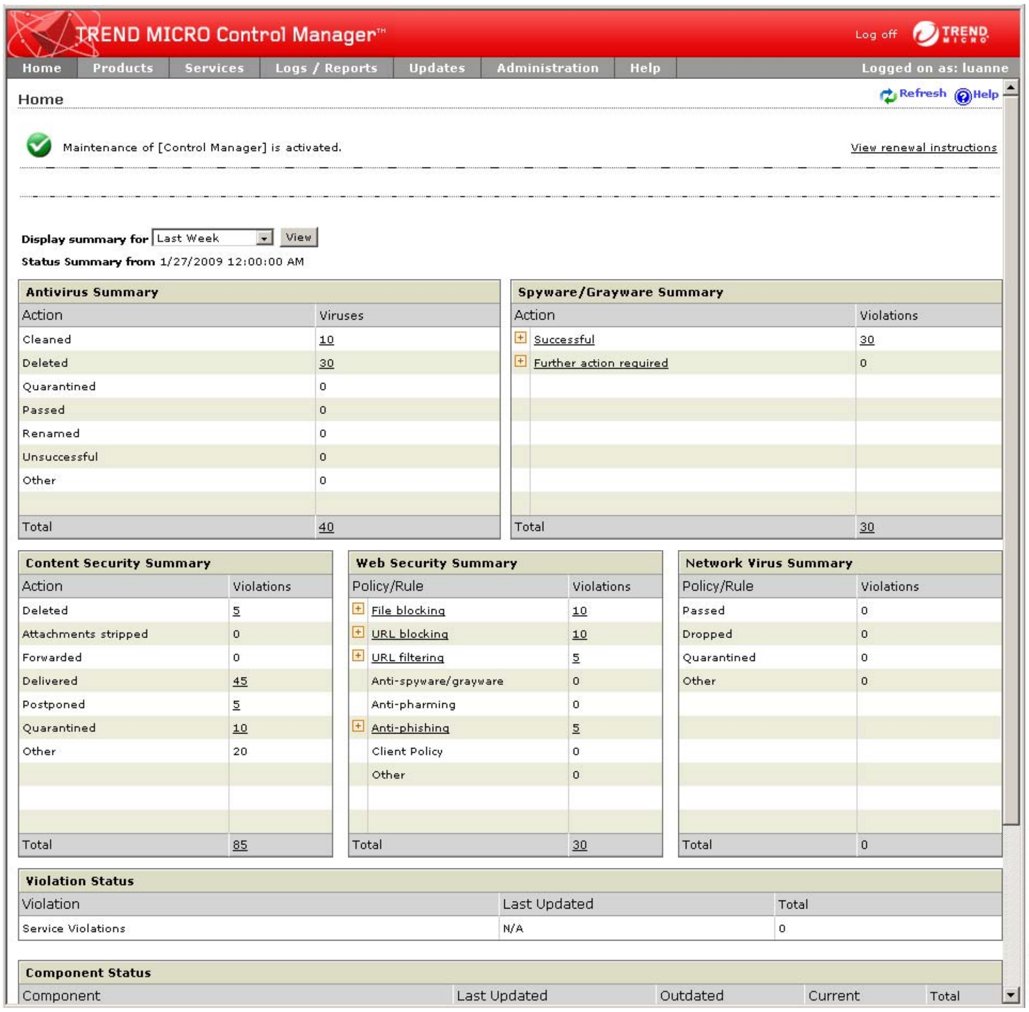
Control Manager Interface

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

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

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

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



Maintenance of [Control Manager] is activated.

Display summary for Last Week

Status Summary from 1/27/2009 12:00:00 AM

Antivirus Summary

Action	Viruses
Cleaned	10
Deleted	30
Quarantined	0
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	40

Spyware/Grayware Summary

Action	Violations
Successful	30
Further action required	0
Total	30

Content Security Summary

Action	Violations
Deleted	5
Attachments stripped	0
Forwarded	0
Delivered	45
Postponed	5
Quarantined	10
Other	20
Total	85

Web Security Summary

Policy/Rule	Violations
File blocking	10
URL blocking	10
URL filtering	5
Anti-spyware/grayware	0
Anti-pharming	0
Anti-phishing	5
Client Policy	0
Other	0
Total	30

Network Virus Summary

Policy/Rule	Violations
Passed	0
Dropped	0
Quarantined	0
Other	0
Total	0

Violation Status

Violation	Last Updated	Total
Service Violations	N/A	0

Component Status

Component	Last Updated	Outdated	Current	Total

Using the Management Console

The management console consists of the following elements:

- The main menu bar contains Home, Products, Services, Logs/Reports, Updates, Administration, and Help, which you use to administer Control Manager and managed products.

  - The Help menu provides links to the Control Manager online help (Content and Index), Trend Micro Knowledge Base, Trend Micro Security Information, Sales, Support, and the About screen for Control Manager.

- When you choose the Products or Services menu item, the navigation menu in the left-hand pane refreshes to display the available options.
- In addition to the navigation menu items, choose **Products** from the main menu to access the following tabs for working with managed products: Advanced Search, Configuration, Tasks, Logs, and Directory Management

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 C-3
- About the Product Directory, page C-4

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

To open the Control Manager console from a remote computer, follow these steps:

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

http://{*hostname***}/ControlManager** (for Control Manager 3.5) or
http://{*hostname***}/WebApp/login.aspx** (for Control Manager 5.0)

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

Step 2 Enter a Control Manager username and password in the field and click **Enter**.

Step 3 When the Control Manager console appears, 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 *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL: http://www.trendmicro.com/download/product.asp?productid=7

To open the Control Manager console using HTTPS, perform the following steps:

Step 1 Enter the URL for encrypted communication (HTTPS) in one of the following formats:

- **https://{***hostname***}:443/ControlManager** (for Control Manager 3.5)
- **https://{***hostname***}:443/WebApp/login.aspx** (for Control Manager 5.0)

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.

Step 2 Press **Enter**.

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 Control Manager 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 Control Manager "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 Control Manager 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 Control Manager Product Directory depends on the account type and folder access rights assigned to your Control Manager log-on credentials. If you cannot see CSC SSM in the Control Manager Product Directory, contact the Control Manager administrator.

Downloading and Deploying New Components

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

- Deploying New Components from the Control Manager Product Directory, page C-5
- Viewing Managed Products Status Summaries, page C-5
- Configuring CSC SSM Products, page C-6
- Issuing Tasks to the CSC SSM, page C-6
- Querying and Viewing Managed CSC SSM Product Logs, page C-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 that you update 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, even if there is no managed product registered on the Control Manager server.

The components to update follow, 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 spam prevention 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 Control Manager 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, follow these steps:

Step 1 From the Control Manager console, click **Products** on the main menu. The Product Directory screen appears.

Step 2 Select a managed CSC SSM or directory from the Product Directory. The managed product or directory highlights.

Step 3 Mouse over **Tasks** from the Product Directory menu. A drop-down menu appears.

Step 4 Choose Deploy <component> from the drop-down menu.

Step 5 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 in the Command Tracking screen 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 Control Manager console, click **Products** on the main menu.

Step 2 On the left-hand navigation tree, click the desired folder or managed product name.

- If you click a managed product name, and then click **Status**, System Information displays for the managed product summary.
- If you click the Root folder, New Entity, or another user-defined folder, and then click **Status**, summaries display for Antivirus, Spyware/Grayware, Content Security, Web Security, and Network Virus summaries.

Configuring CSC SSM Products

You can configure one or more instances of CSC SSM from Control Manager, 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, follow these steps:

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

Step 2 Select the managed CSC SSM from the product tree. The product status appears in the right-hand area of the screen.

Step 3 Mouse over **Configure** from the product tree menu. A drop-down menu appears.

Step 4 Choose **Configure <CSC SSM name>**. The managed product's web-based console or Control Manager-generated console appears.

Step 5 Log in and configure the managed CSC SSM from the web console.

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, follow these steps:

Step 1 From the Control Manager 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 in the response screen.

Querying and Viewing Managed CSC SSM Product Logs

Use the Configure tab to query and view logs for a group or specific managed CSC SSM using the CSC SSM console.

To query and view managed CSC SSM logs, follow these steps:

Step 1 From the Control Manager console, click **Products** to shown the Product Directory.

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

Step 3 Click the **Configure** tab.

Step 4 Log in to the CSC SSM console.

Step 5 Choose **Logs > Query**.

Step 6 Select the log type form the drop-down menu.

Step 7 Select the appropriate protocol and time filter.

Step 8 Select the number of logs to display per page.

Step 9 Click **Display Log**.

To filter information to be more specific, you can use an ad hoc query. For more information, see Creating a New Ad Hoc Query, page C-9.

For additional information and instructions about using Trend Micro Control Manager, see the online help embedded in the application or PDF file documentation available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

Ad Hoc Queries

Trend Micro Control Manager 5.0 supports collecting the data an administrator needs from Control Manager and managed CSC SSM logs. Control Manager supports the display of data through the use of ad hoc queries. Ad hoc queries provide administrators with a quick method of extracting information directly from the Control Manager database. The database contains information collected from all CSC SSMs registered to the Control Manager server. (Log aggregation can affect the data available to query.) Using ad hoc queries to extract data directly from the database provides a very powerful tool for administrators.

When querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis, or save the query for future use. Control Manager also supports the sharing of saved queries, so other users can benefit from useful queries.

An ad hoc query is a direct request to the Control Manager database for information. The query uses data views to narrow the request and improve performance for the information. After specifying the data view, users can further narrow their search by specifying filtering criteria for the request.

When performing an ad hoc query, the user first specifies that the Control Manager server, where the user is currently logged on, should query a CSC SSM that the Control Manager manages.

For more information, see the *Trend Micro Control Manager 5.0 Administrator's Guide* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

System Requirements

Table C-1 shows the system requirements for using ad hoc queries with CSC SSM.

Table C-1 System Requirements for Using Ad Hoc Queries

Language	Version of Control Manager	Version of CSC SSM
English	5.0 + Patch 3	6.3
Japanese	5.0 + Patch 3	6.3

Understanding Ad Hoc Queries

Completing an ad hoc query consists of the following processes:

- Selecting the managed CSC SSM for the query
- Selecting the Data View to query
- Specifying filtering criteria, and the specific information that displays
- Saving and completing the query
- Exporting the data to CSV or XML format

For example, Chris, an CSC SSM Administrator, wants to check the status of pattern files for the CSC SSM. Chris selects Logs/Reports > New Ad Hoc Query, and then selects the managed CSC SSM from the Select Product tree and clicks Next. Under Product Information > Component Information, Chris chooses the data view for Pattern File/Rule Status Summary. Proceeding to the next step, Chris clicks "Change column display" and selects four fields that the query will display: Pattern/File Rule Name, Pattern/File Rule Version, Pattern/File Rule Up-to-Date, and Pattern/File Rule Out-of-Date. Chris returns to the Results Display Settings and unchecks the Custom Criteria check boxes. After clicking Query, the results for the query that Chris created appear. The results can now be exported in CSV or XML format, if needed.

Understanding Data Views

A Data View is a table consisting of clusters of related data cells. Data Views provide the foundation on which users perform ad hoc queries of the Control Manager database. Control Manager separates Data Views into two major categories: Product Information and Security Threat Information.

For more information on Data Views, see Appendix B of the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

The Control Manager web console displays the types of Data Views and the information available from each type of Data View.

Table C-2 Control Manager Major Data View Categories

Major Data View Category	Details
Product Information	Managed Product Information includes: • CSC SSM Distribution Summary • CSC SSM Status Information • CSC SSM Event Information Component Information includes: • CSC SSM Scan Engine Status • CSC SSM Pattern File/Rule Status • CSC SSM Component Deployment • Scan Engine Status Summary • Pattern File/Rule Status Summary
Security Threat Information	Displays the following information about security threats that managed CSC SSMs detect: • Virus/Malware Information • Spyware/grayware Information • Content Violation Information • Spam Violation Information • Web Violation/Reputation Information • Overall Threat Information

Creating a New Ad Hoc Query

After you create and save an ad hoc query, you can run that query as often as needed. This example shows how to create a query that displays a summary of detected web violations.

To create a new ad hoc query, follow these steps:

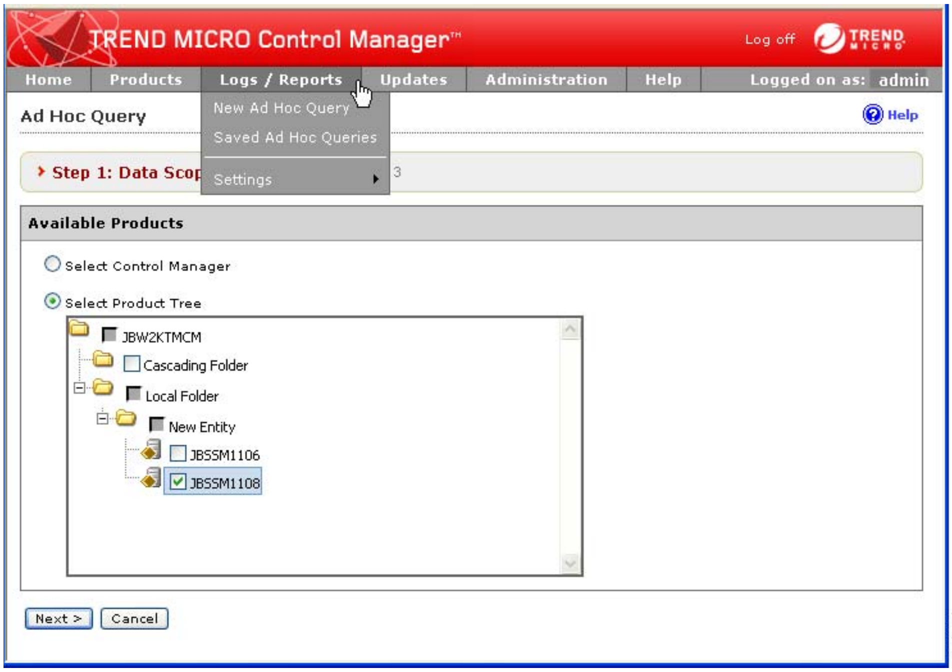
Step 1 Mouse over **Logs/Reports** on the main menu.

Step 2 Click **New Ad Hoc Query**. The Available Products screen appears.

Step 3 Click the **Select Product Tree** radio button to specify that the query data should originate from the managed CSC SSM(s) and not Control Manager. See Figure C-2.

Step 4 Select the check box to designate which managed CSC SSM(s) to query or select a folder to query all the products in that folder.

Figure C-2 Step 1: Data Scope



Ad Hoc Query

› Step 1: Data Scop 3

Available Products

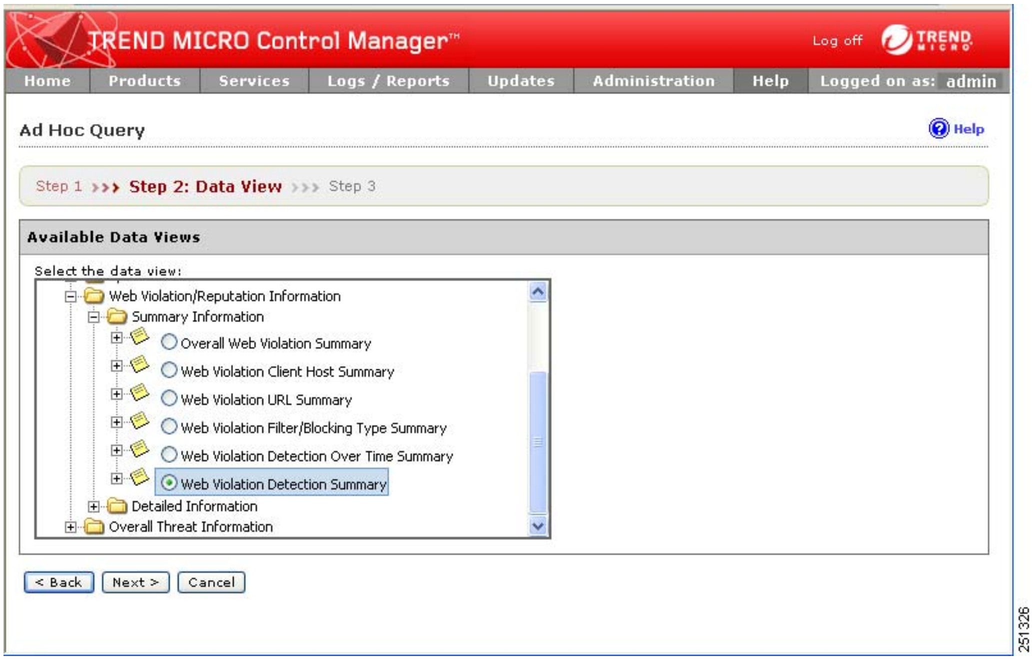
○ Select Control Manager

● Select Product Tree

- ■ JBW2KTMCM
  - □ Cascading Folder
  - ■ Local Folder
    - ■ New Entity
      - □ JBSSM1106
      - ☑ JBSSM1108

Step 5 Click **Next** to select the Data View. The “Ad Hoc Query Step 2: Select Data View” screen appears. See Figure C-3.

Figure C-3 Step 2: Select the Data View



Ad Hoc Query

Step 1 >>> Step 2: Data View >>> Step 3

Available Data Views

Select the data view:

- Web Violation/Reputation Information
  - Summary Information
    - ○ Overall Web Violation Summary
    - ○ Web Violation Client Host Summary
    - ○ Web Violation URL Summary
    - ○ Web Violation Filter/Blocking Type Summary
    - ○ Web Violation Detection Over Time Summary
    - ● Web Violation Detection Summary
  - Detailed Information
- Overall Threat Information

< Back | Next > | Cancel

Step 6 Specify the data view for the log by performing the following steps:

a. Select the data to query from the Available Data Views area.

Select multiple items using the Shift or Ctrl key.

b. Click **Next**. The Step 3: Query Criteria screen appears. See Figure C-5.

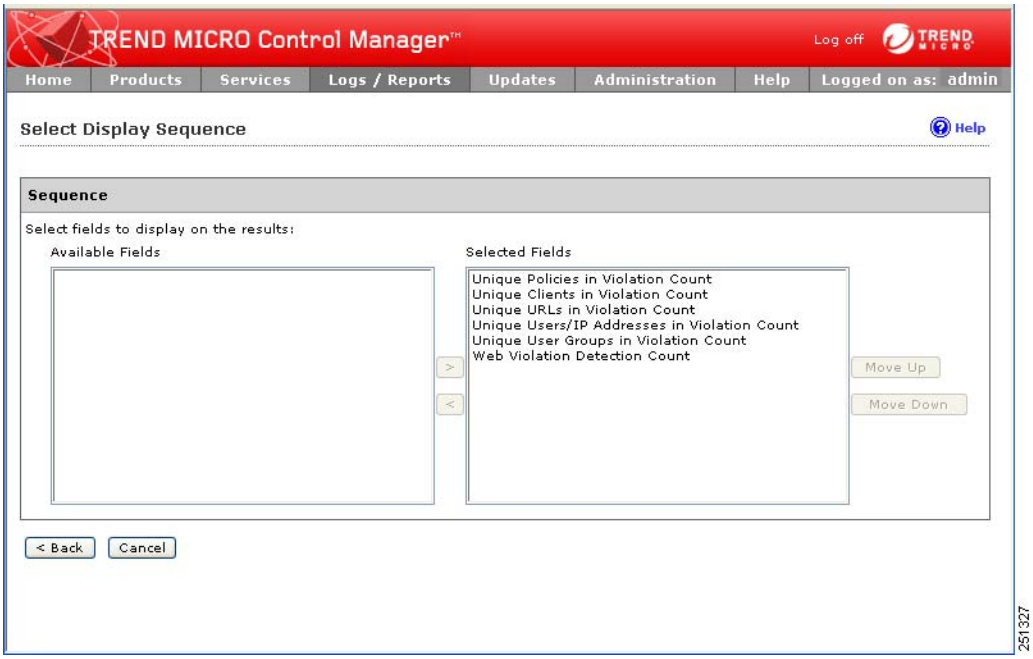
Note Selecting CSC SSM in the managed product/directory dictates the data views that are available in the Data Views list to those associated with CSC SSM. For more information on data views, see Understanding Data Views, page C-9 or the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

Step 7 Specify the data to appear in the log and the order in which the data appears by doing the following:

a. Click **Change column display**. The Select Display Sequence screen appears. See Figure C-4.

Figure C-4 Select Fields to Display and Arrange Order



Select Display Sequence

Sequence

Select fields to display on the results:

Available Fields

Selected Fields

Unique Policies in Violation Count
Unique Clients in Violation Count
Unique URLs in Violation Count
Unique Users/IP Addresses in Violation Count
Unique User Groups in Violation Count
Web Violation Detection Count

b. To remove fields, select them in the Selected Fields list.

Select multiple items using the Shift or Ctrl key.

c. Click the less than sign (<) to remove unnecessary fields.

Note Items appearing at the top of the Selected Fields list appear as the left-most column of the query results table. Removing a field from Selected Fields list removes the corresponding column from the ad hoc query returned table.

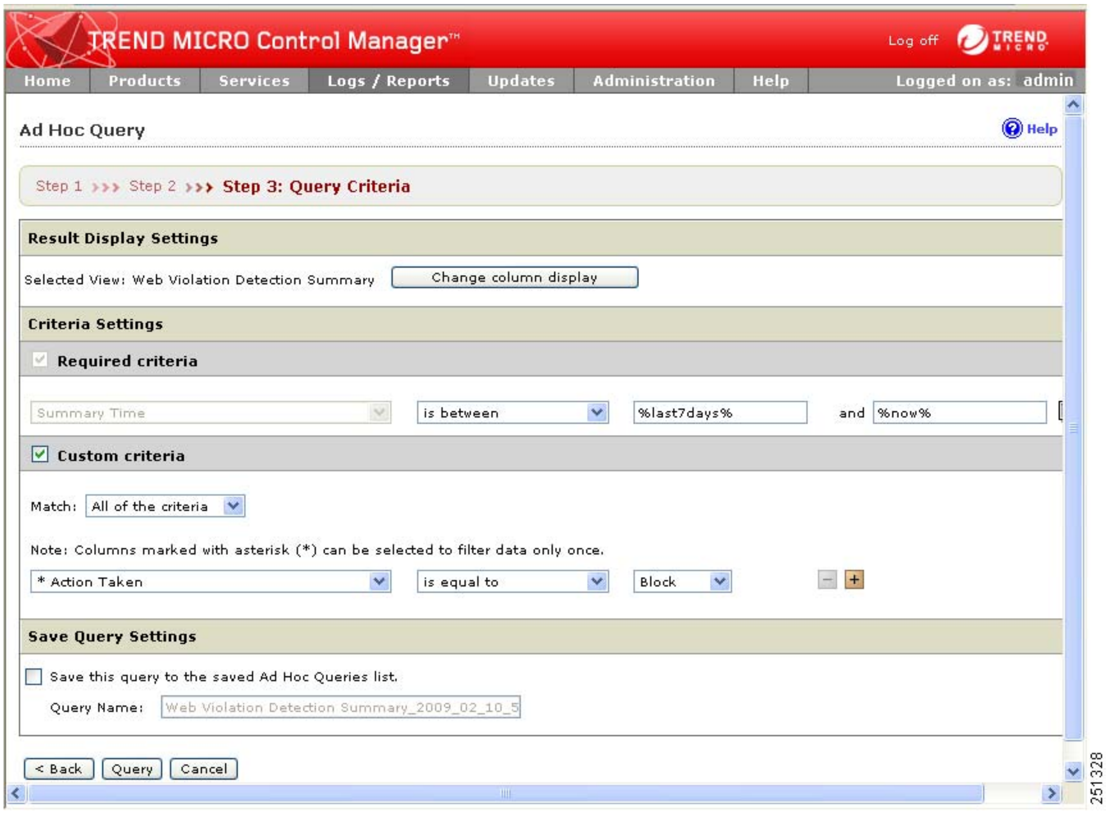
d. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

e. Click **Back** when the sequence fits your requirements.

Step 8 Specify the filtering criteria for the data:

Note When querying for summary data, users must specify the items under Required criteria.

Figure C-5 Setting Required and Custom Criteria



Ad Hoc Query

Step 1 >>> Step 2 >>> **Step 3: Query Criteria**

Result Display Settings

Selected View: Web Violation Detection Summary

Criteria Settings

☑ **Required criteria**

Summary Time | is between | %last7days% | and | %now%

☑ **Custom criteria**

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

* Action Taken | is equal to | Block

Save Query Settings

□ Save this query to the saved Ad Hoc Queries list.

Query Name: Web Violation Detection Summary_2009_02_10_5

Required criteria

- Specify a Summary Time for the data. The default is between the "last 7 days" and "now."

Custom criteria

a. Specify the criteria filtering rules for the data categories:

  – **All of the criteria:** This selection acts as a logical "AND" function. Data appearing in the report must meet all the filtering criteria.

  – **Any of the criteria:** This selection acts as a logical "OR" function. Data appearing in the report must meet any of the filtering criteria.

b. Specify the filtering criteria for the data. Control Manager supports up to 20 criteria for filtering data.

Tip If you do not specify any filtering criteria, the ad hoc query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

Step 9 (Optional) To save the query, perform the following steps:

a. Click the **Save this query to the saved Ad Hoc Queries list** check box.

b. Type a name for the saved query in the Query Name field. The default name is Web Violation Detection Summary_<date>. For example, type "Web Violation Detection Summary_last7days."

Step 10 Click **Query**. The Results screen appears.

Step 11 (Optional) To save the report to CSV format:

- **a.** Click **Export to CSV**. A dialog box appears.
- **b.** Click **Save**. A Save as dialog box appears.
- **c.** Specify the location to save the file.
- **d.** Click **Save**.

Step 12 (Optional) To save the report to XML format:

- **a.** Click **Export to XML**. A dialog box appears.
- **b.** Click **Save**. A Save as dialog box appears.
- **c.** Specify the location to save the file.
- **d.** Click **Save**.

Tip To query for more results on a single screen, select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

Step 13 (Optional and only necessary if not saved in Step 9.) To save the settings for the query:

- **a.** Click **Save query settings**. A confirmation dialog box appears.
- **b.** Accept the default name for the query or type a different name in the **Query Name** field.
- **c.** Click **OK**.

The saved query is now available from **Logs/Report > Saved Ad Hoc Queries > My Queries**.

Performing an Ad Hoc Query

"Creating a New Ad Hoc Query" section on page C-9 shows how to create a sample ad hoc query called "Web Violation Summary_last7days." That query shows a summary of web violations for the last week. That saved query can be run as needed.

This section includes the following topics:

- Available Headings in the Web Violation Query
- Creating an Available Query
- Running an Available Query

Available Headings in the Web Violation Query

The “Web Violation Summary_last7days” sample query created in “Creating a New Ad Hoc Query” section on page C-9 shows the statistics described in Table C-3.

Table C-3 Details Available in the Pre-packaged Ad Hoc Query

Parameter	Shows	Drills Down to
Unique Policies in Violation Count	Number of policies violated	• Name of violated policy • Filter/Blocking Type such as URL Filtering, Web Reputation, or file name • Number of Unique Clients in Violation Count* • Number of Unique URLs in Violation Count* • Number of Web Violation Detection Count*
Unique Clients in Violation Count	Number of clients in violation	• IP address of the host of the client in violation • Number of Unique Policies in Violation* • Number of Unique URLs in Violation* • Number of Web Violation Detection Count*
Unique URLs in Violation Count	Number of URLs in Violation. Drills	• URL in Violation • Filter/Blocking Type such as URL Filtering, Web Reputation, or file name • Number of Unique Clients in Violation* • Number of Web Violation Detection Count*
Unique Users/IP Addresses in Violation Count	Number users in violations	• IP address or user name (if available) involved in the violation • Web Violation Detection Count*
Unique User Groups in Violation Count	Number of user groups in violation	• Name of the group involved in the violations • Number of Unique Users/IP Addresses in Violation Count* • Number of Web Violation Detection Count*

Table C-3 Details Available in the Pre-packaged Ad Hoc Query (continued)

Parameter	Shows	Drills Down to
Web Violation Detection Count	Number of web violations	• Time Received from Entity • Time Generated at Entity • Entity Display Name* • Managed Product Name • Inbound/Outbound Traffic/Connection • Protocol involved (HTTP or FTP) • URL involved in the violation • User name or IP address involved in the violation • User Group involved in the violation • IP address of the client host • IP address of the server host • Filter or blocking type • Name of the blocking rule violated • Name of the policy violated • File in violation (if any) • Web Reputation rating (if applicable) • Action taken: block or pass for example • Number of web violations detected
*Item drills down to further details.		

Creating an Available Query

The Web Violations query created in "Creating a New Ad Hoc Query" section on page C-9 was saved to the saved queries list on the My Queries tab, which means it can only be run by the administrator who created it. Control Manager supports the modification of a personal, saved ad hoc query from the My Queries tab to become an available query, which can be shared with other administrators.

To share a query from My Queries to Available Queries, follow these steps:

Step 1 Access My Queries from **Logs/Reports > Saved Ad Hoc Queries > My Queries** tab.

Step 2 Click the check box beside the name of the query to be shared.

Step 3 Click the **Share** icon.

Step 4 Verify that the query has been shared by clicking the Available Queries tab.

The newly shared query is listed in the Name column. The name of the query creator appears in the Owner column.

Running an Available Query

Queries available through the Available Queries tab have been created and saved as a shared, available query. See "Creating an Available Query" section on page C-16 for more information. Saved queries can run as often as needed.

To run an available ad hoc query, perform the following steps:

Step 1 Mouse over **Logs/Reports** on the main menu. A drop-down menu appears.

Step 2 Click **Saved Ad Hoc Queries**.

Step 3 Click the **Available Queries** tab.

Step 4 Click **View** in the View Results column. The query runs and the results appear.

Working with Reports

Usage of the reporting feature requires an Advanced License for Control Manager.

Control Manager reports consist of two parts: report templates and report profiles.

- Report templates determine the look and feel of the reports.
- Report profiles specify the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 allows administrators to design their own custom report templates.

- User-defined customized report templates that use direct database queries (database views) and report template elements (charts, graphs, and tables).
- Users have greater flexibility in specifying the data that appears in their reports compared to report templates from previous Control Manager versions.

Note For more information on Control Manager 5.0 templates, see "Understanding Control Manager 5.0 Templates" in Chapter 6 of the *Trend Micro Control Manager 5.0 Administrator's Guide,* available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=7

APPENDIX D

Using CSC SSM with Trend Micro Damage Cleanup Services

Trend Micro InterScan for CSC SSM works with Trend Micro Damage Cleanup Services (DCS) as part of an enterprise protection strategy. The CSC SSM works with DCS Versions 3.1 and 3.2.

This appendix includes the following sections:

- About Damage Cleanup Services, page D-1
- Network Scenarios, page D-3
- Getting Started, page D-6
- DCS Interface, page D-10
- Registering DCS with Cisco ICS, page D-11
- Querying and Viewing DCS Logs in the CSC SSM, page D-12
- Troubleshooting DCS Scan Failures, page D-13

About Damage Cleanup Services

This section includes the following topics:

- Who Should Use DCS?, page D-2
- How Does DCS Access Client Machines?, page D-2
- Machines That DCS Can Scan, page D-2
- Web Browser Requirements, page D-3

DCS is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. DCS removes network viruses that can re-attack the network, and performs the following functions:

- Removes unwanted registry entries created by worms or Trojans.
- Removes memory-resident worms or Trojans.
- Removes active spyware and grayware.
- Removes rootkits.
- Removes garbage and viral files dropped by viruses.
- Assesses a system to decide whether it is infected or not.

- Returns a system to a clean state.
- Can register to Cisco Incident Control Server (ICS) and Cisco Security Monitoring, Analysis and Response System (MARS).
- Can act on clean-up requests from the CSC SSM and MARS.
- Detects spyware and grayware.

Who Should Use DCS?

DCS is designed for IT managers and administrators of medium-to-large computer networks. For DCS to find and clean active Trojans, worms, and spyware or grayware in memory, you need to install required software on client machines. A single DCS server can deploy its updated clean-up engine, when needed, to all Windows PCs in the network. Individual users need not even be aware that DCS is doing its job. If DCS is unable to connect to a client machine (because it is running an outdated operating system or because the login information that DCS has is incorrect), you can have users click a URL that activates a special manual damage cleanup tool to scan and clean a particular client, and then return the resulting scan log to the DCS server.

How Does DCS Access Client Machines?

DCS uses several technologies. When preparing DCS for use, you enter the account information for all of the computers on the network into the Account Management Tool. DCS uses this tool when accessing clients. Because no DCS software is installed on client machines, only the DCS server is required to update its components, which are as follows:

- The virus cleanup template, which contains patterns used to identify Trojans and network viruses
- The spyware pattern, which DCS uses to intelligently identify active spyware programs
- The virus cleanup engine, which DCS deploys to each client machine at the time of scanning
- The spyware scan engine, which DCS deploys to each client machine at the time of scanning
- The anti-rootkit driver, which detects and removes rootkit programs

Note DCS uses the NetBIOS protocol to resolve client machine names.

Machines That DCS Can Scan

DCS can deploy cleanup and assessment tasks to the following systems:

- Windows 2000 Professional/Server/Advanced Server
- Windows XP Professional
- Windows Server 2003 (Web, Standard, or Enterprise Edition)
- Windows Server 2003 R2 (Standard or Enterprise Edition)

Web Browser Requirements

DCS uses ActiveX controls and Windows RPC to perform several tasks. For this reason, the machine on which the DCS server is installed must have Microsoft Internet Information Server (IIS) and the browser used for accessing the DCS web console must be Microsoft Internet Explorer.

DCS Documentation

This appendix gives a brief overview of how Damage Cleanup Services works with CSC SSM. To access the full documentation set for DCS, use the documentation that shipped with the product, the online help in the product, or the following link.

The complete set of print documentation for Damage Cleanup Services is available at:

http://www.trendmicro.com/download/product.asp?productid=48

Network Scenarios

This section shows network scenarios in which you can deploy DCS, and includes the following topics:

- Most Common Network Scenario, page D-3
- Network Scenario Alternative 2, page D-4
- Network Scenario Alternative 3, page D-5

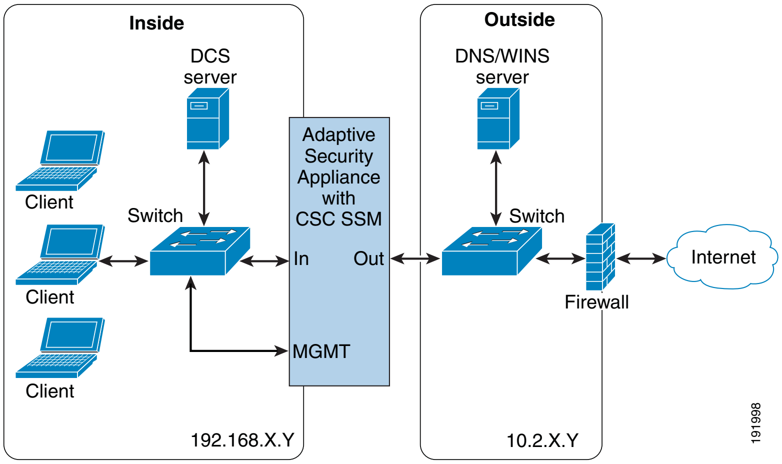
Note HTTP requests must travel through the ASA on Port 80 for CSC SSM to notice suspicious activity. Only clients on the inside network will trigger scans from CSC SSM. For information about how to trigger remote client scans, see DCS Documentation.

Most Common Network Scenario

The network scenario depicted in Figure D-1 has these physical attributes:

- Clients are in the “inside” network.
- The CSC SSM interface is on the “inside” network.
- DCS is on a server in the “inside” network.
- The DNS/WINS server is on the “outside” network.

Figure D-1 Most Common Deployment



In this scenario, note the actions and configurations described in Table D-1.

Table D-1 Common Deployment Actions and Configurations

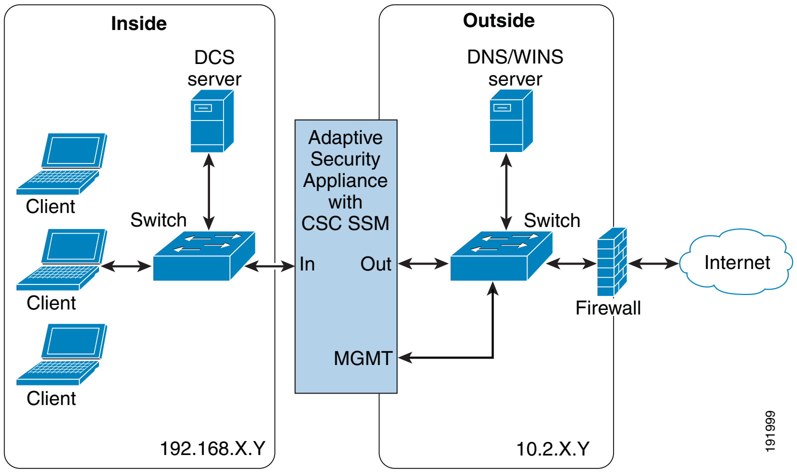
Action	Special Configuration
Registering or unregistering CSC SSM to DCS	None
Remote client cleanup	Requires that the target PCs belong to a Windows domain. An additional configuration file must be manually added to DCS to map client IP addresses to domains. See Adding the ExtraMachineDomainList.ini File, page D-7 for details. In addition, the configuration of the Windows firewall on client PCs must allow file and printer sharing and ICMP echo.
Client redirect to the manual cleanup page	None
DCS transmissions of scan results to the CSC SSM	None

Network Scenario Alternative 2

Network scenario alternative 2, depicted in Figure D-2, has the following physical attributes.

- Clients are in the “inside” network.
- The CSC SSM is “outside.”
- DCS is “inside.”
- The DNS/WINS server is “outside.”

Figure D-2 Alternative #2



In this scenario, note the actions and configurations in Table D-2.

Table D-2 Network Scenario #2 Actions and Configurations

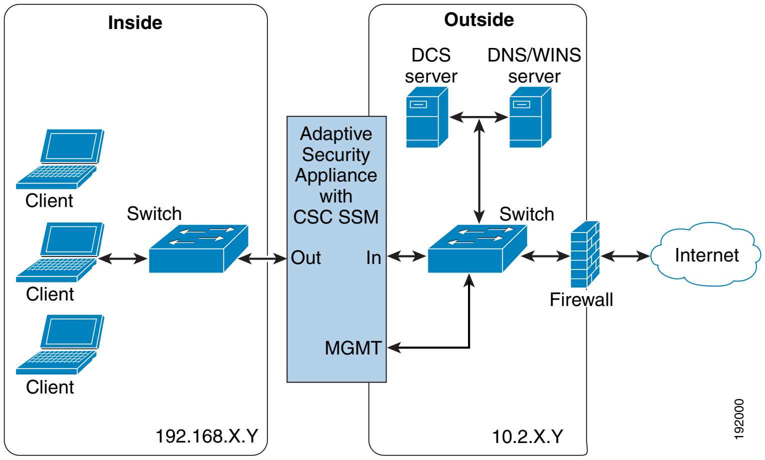
Action	Special Configuration
Registering or unregistering CSC SSM to DCS	A forwarding rule must be added to the security appliance to allow access from outside to DCS GUI on the inside.
Remote client cleanup	A forwarding rule must be set up to allow registration. Has the same restrictions as the most common deployment.
Client redirect to the manual cleanup page	The forwarding rule must be set up to allow registration.
DCS transmissions of scan results to the CSC SSM	The forwarding rule must be set up to allow registration.

Network Scenario Alternative 3

Network scenario alternative 3, depicted in Figure D-3, has the following physical attributes.

- Clients are in the “inside” network.
- The CSC SSM is in the “outside” network.
- DCS is in the “outside” network.
- The DNS/WINS server is in the “outside” network.

Figure D-3 Alternative #3



In this scenario, note the actions and configurations in Table D-3.

Table D-3 Network Scenario #3 Actions and Configurations

Action	Special Configuration
Registering or unregistering CSC SSM to DCS	None
Remote client cleanup	Will not work. The DCS does not see the client IPs at all and cannot use the mapping file to match them to a domain.
Client redirect to the manual cleanup page	None
DCS transmissions of scan results to the CSC SSM	None

Getting Started

The following tasks must be completed for CSC SSM to register to DCS.

- Registration and Activation of DCS, page D-6
- Setting up Accounts, page D-7
- Adding the ExtraMachineDomainList.ini File, page D-7
- Verifying Firewall Security on Target Machines, page D-9
- Registering CSC SSM to DCS, page D-9

Registration and Activation of DCS

DCS is available at the following link:

http://us.trendmicro.com/us/products/enterprise/damage-cleanup-services/

Registration and activation information are available in the DCS product documentation. For information about logging on using the DCS console and querying logs, see DCS Interface, page D-10.

Setting up Accounts

Using the DCS Account Management Tool, add entries for accounts on each domain that has local administrative privileges for machines to be scanned.

To add a domain or machine account, perform the following steps:

Step 1 To open the Account Management Tool, choose **Start > Programs > Trend Micro Damage Cleanup Services > Account Management Tool**.

The Login screen appears.

Step 2 Type your DCS administrative password and click **Log On**.

A list of all existing accounts appears, showing account type and the available descriptions.

Step 3 Click **Add** to add an account.

The Add Account screen appears.

Step 4 Under Select the type of account to add, select what kind of account to add by accepting the default choice of Domain account or by choosing **Machine account**.

Step 5 If the account is a domain account and you would like to use it as the default account, check the **Make this account the default account** check box.

Note If, during a scan, DCS is unable to access a remote machine using the account for that machine, DCS uses the default account to access the machine. Because only a domain account can be a default account, this option is disabled for machine accounts.

Step 6 In the Domain name field, type the name of the domain or machine account.

Step 7 Type the administrator account.

Step 8 Type the password for the administrator account, and then retype it to confirm the entry.

Step 9 (Optional) Type a description for this account (for example, Company domain 1).

Step 10 Click **Verify** to verify that DCS can connect to the domain with the information provided. If DCS can connect to the domain, a **Connectivity to client verified** message appears.

Step 11 Click **OK** to close the verification message, and click **OK** to finish adding the new domain.

The account name appears in the Name column of the Accounts table.

Step 12 Click **Close** to close the Account Management Tool.

Adding the ExtraMachineDomainList.ini File

DCS uses NetBIOS lookups to determine hostnames of PCs that have been targeted for cleanup by external applications (such as TMCM and Cisco ICS) when those applications provide only the target IP address. This method of hostname resolution may fail, particularly if the network WINS server resides on a different network segment with NAT between the WINS server and the clients (both DCS and the target PC).

If your target PCs are part of a Windows domain, you can still use remote cleanup with some additional configuration on both DCS and the clients.

To specify the domain of particular machines by IP address or IP range, place a file named ExtraDomainMachineList.ini into the DCS root folder. DCS uses the domain account type in the Account Management Tool to access those machines and scan them automatically.

Note This file is necessary for deployments using NAT.

To verify that you need to create the ExtraMachineDomainList.ini file, perform the following steps:

Step 1 On your DCS server, to resolve the client machine name using its IP address, issue the **nbtstat** command from a DOS command prompt:

```
c\: nbtstat -A [Client IP Address]
```

Step 2 If the DCS server cannot resolve the client machine name, make sure that the NetBIOS protocol over TCP/IP on the client and DCS server machines is enabled.

Note DCS makes use of the NetBIOS protocol to resolve the machine names. If the NetBIOS protocol is disabled on the server side, the server cannot enumerate any client machines. If the NetBIOS protocol is disabled on the client side, then the client is not enumerated and does not appear in the scan result.

You can also place a file named ExtraDomainMachineList.ini into the DCS root folder to specify the domain of particular machines by IP addresses or IP range.

Step 3 Create a file named ExtraDomainMachineList.ini in the DCS installation directory. For example:

```
[domain_name1}
IP=10.2.2.2
IPRange=10.2.4.1-10.2.4.255
[domain_name2]
IP=10.2.2.1
```

Step 4 In the ExtraDomainMachineList.ini file, specify your Windows domains and the list of machine IP addresses that belong to each domain. Use only the top-level domain name. FQDNs are not supported. Use the format shown in Table D-4:

Table D-4 Elements Used in the ExtraDomainMachineList.ini File

Element	Description
[domain_name1]	The domain name of the IP address or IP range under this section.
IP=10.1.1.1	The IP address that is specified for the domain.
IP=10.2.2.2	Another IP address that is specified for the domain.
IPRANGE=10.1.1.1-10.1.1.255	The IP range that is specified for the domain.
IPRANGE=1.1.1.1-255.255.255.255	Another IP range that is specified for the domain.
[domain_name2]	The second domain name of the IP address or IP range under this section.
IP=10.3.3.3	The IP address that is specified for the second domain.

Table D-4 Elements Used in the ExtraDomainMachineList.ini File (continued)

Element	Description
IPRANGE=10.3.3.3-10.3.3.255	The IP range that is specified for the second domain.
IPRANGE=10.3.3.3-255.255.255.255	Another IP range that is specified for the second domain.

Verifying Firewall Security on Target Machines

DCS uses ICMP echo to verify the route to a target machine, and Windows RPC to log in and clean the targeted PC. Windows Firewall (or other software firewalls) on the target machine may interfere with this process.

To verify firewall security on targets machines, perform the following steps:

Step 1 Verify the firewall applications that are installed on the client or DCS server machine.

Note If a firewall application is installed on the client machine and it is enabled, the firewall may block the scan task and cause scanning to fail.

If a firewall application is installed on the DCS server machine and it is enabled, the firewall may block the scan result that the client machine is sending to the server.

Step 2 Check and open TCP ports 139 and 445 and UDP ports 137 and 138, or enable File and Printer sharing in the exception list on the Exceptions tab in Windows Firewall. DCS makes use of these ports to communicate with clients.

Step 3 If your target PCs have Windows Firewall enabled, be sure that **Allow incoming echo request** check box is checked in the ICMP Settings dialog box on the Advanced tab of the Windows Firewall configuration dialog box.

Registering CSC SSM to DCS

For CSC SSM to acknowledge DCS, the CSC SSM must register to DCS.

To register CSC SSM to DCS, perform the following steps:

Step 1 In the CSC SSM console, go to **Administration > Register to DCS**.

Step 2 Click **Enable**.

Step 3 Enter the DCS server name or IP address in the appropriate field, and then click **Add**.

Step 4 Enter the port number.

Step 5 If a cleanup failure occurs, you can redirect the client to DCS by checking the check box near the bottom of the screen.

Unregistering CSC SSM from DCS

You can unregister from DCS if your DCS server changes or if you no longer need DCS.

To unregister the CSC SSM from DCS, perform the following steps:

Step 1 In the CSC SSM console, go to **Administration > Register to DCS**.

Step 2 In the registration table, click the **Delete** icon beside the registered DCS server name or IP address.

DCS Interface

This section describes the DCS interface, and includes the following topics:

- Managing DCS through TMCM, page D-10
- Accessing DCS, page D-10

Managing DCS through TMCM

During DCS installation, you have the option of enabling DCS to be managed by Trend Micro Control Manager. Choosing this option requires the installation of a Control Manager agent for DCS.

Immediately after you click **Finish** in the InstallShield Wizard Completed screen, a prompt appears, asking if you want to manage DCS by using Trend Micro Control Manager. Click **Yes** to allow Trend Micro Control Manager to manage DCS.

Accessing DCS

DCS can serve as a stand-alone product, and no longer depends on Trend Micro Control Manager for configuration and use. DCS has its own web-based management console.

After you have installed DCS, you can run the DCS console from within Windows.

To log on to the DCS web management console, perform the following steps:

Step 1 Launch the DCS web console in one of the following three ways:

- From the Windows Start menu of the host on which DCS is installed, choose **Start > Programs > Trend Micro Damage Cleanup Services > Trend Micro Damage Cleanup Services**.
- Go to the URL of your installed DCS web console: (http://<Your_DCS_Server_Machine>/DCS/cgiDispatcher.exe)

Tip For convenience, you may want to add this URL to your Favorites list in Microsoft Internet Explorer web browser.

- Double-click the Internet shortcut file created by your installation in the default Destination Folder:

  <OS_drive>\Program Files\Trend Micro\DCS\WebUI\DCS\DCS.url

  or in the folder that you chose during installation, if this is different from the default location:

  <Destination Folder>\WebUI\DCS\DCS.url

The DCS web console opens in a Microsoft Internet Explorer browser window.

Step 2 Type the Administrator password that you chose when installing the program, and press **Enter** or click **Log On**.

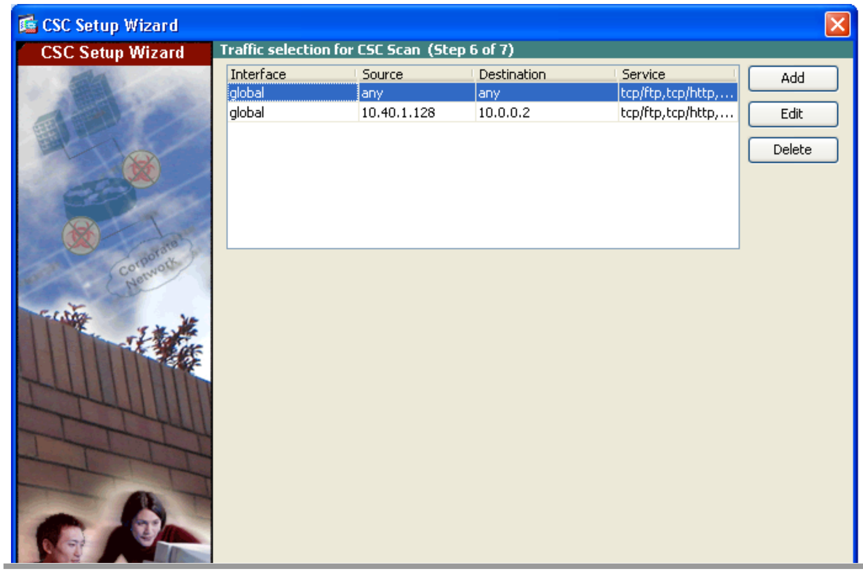
The Trend Micro Damage Cleanup Services web management console opens to the Summary screen.

Note The default system timeout for DCS is 900 seconds (15 minutes). You can change the timeout setting by editing the system registry.

When you log in to DCS, the Home window appears, as shown in Figure D-4.

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

Figure D-4 ***The DCS Console Home Window.***



Traffic selection for CSC Scan (Step 6 of 7)

Interface	Source	Destination	Service
global	any	any	tcp/ftp,tcp/http,...
global	10.40.1.128	10.0.0.2	tcp/ftp,tcp/http,...

Registering DCS with Cisco ICS

You can register DCS with the Cisco ICS from within the DCS management console.

Note For information about how CSC SSM can register with MARS, go to the following URL:

http://www.trendmicro.com/download/product.asp?productid=48

To register DCS with the Cisco ICS, perform the following steps:

Step 1 From the DCS management console, choose **Administration > Cisco ICS Registration**.

The Cisco ICS Registration screen appears.

Step 2 Type the server name or IP address.

Step 3 Select the type of HTTP you would like to use for communication between DCS and Cisco ICS. The available options are HTTP and HTTPS.

Step 4 Choose the port number of the Cisco ICS. The defaults are 8080 for HTTP and 4343 for HTTPS.

Step 5 Type the virtual directory of the Cisco ICS CGI program.

Step 6 Type the update directory for Cisco ICS.

Step 7 Choose the **DCS Notification URL host** from the drop-down list.

Step 8 Click **Register Now**.

DCS registers itself with the Cisco ICS.

Unregistering DCS from the Cisco ICS

You can unregister DCS from eitherthe Cisco ICS or the DCS management console. For instructions about unregistering from Cisco ICS, consult your Cisco ICS documentation.

To unregister DCS from Cisco ICS, perform the following steps:

Step 1 From the DCS management console, choose **Administration > Cisco ICS Registration**.

The Cisco ICS Registration screen appears.

Step 2 Click **Unregister Now**.

DCS unregisters with Cisco ICS.

Querying and Viewing DCS Logs in the CSC SSM

To query and view managed product logs, perform the following steps:

Step 1 From the CSC SSM console, choose **Logs > Query**.

Step 2 Choose **Damage Cleanup Services** from the Log type drop-down list.

Step 3 Choose **HTTP** from the Protocol drop-down list.

Note HTTP is the only supported protocol for DCS logging.

Step 4 Choose the time period, either **All** or a range of dates.

Step 5 Click **Display Log**.

The Damage Cleanup Services Log screen displays the results in a table.

Step 6 Using the links at the top of the screen, you can do the following:

- Initiate a new query.
- Print the current results.
- Export results in a CSV format.
- Refresh the screen.

For additional information and instructions about using DCS, see the DCS online help or the *Damage Cleanup Services Administrator's Guide*.

Troubleshooting DCS Scan Failures

If the scan cannot find a targeted client machine, and the cause is not readily apparent, try the following troubleshooting techniques.

To troubleshoot a scan failure, perform the following steps:

Step 1 Ping the IP address and machine name to determine the connection status between the DCS server and client machine.

```
c\: ping [Client IP Address or Machine Name]
```

If the DCS server cannot connect to the machine, the DCS server cannot scan the machine. Correct the network problem, and then try scanning again.

Step 2 Verify whether firewall applications are installed on the client or DCS server machine. For details, see Verifying Firewall Security on Target Machines, page D-9.

Step 3 Use the following command to resolve the client machine name using its IP address.:

```
c\: nbtstat -A [Client IP Address]
```

Step 4 If the command cannot resolve the client machine name, make sure that the following items have been completed:

- The NetBIOS protocol over TCP/IP on the client and DCS server machines is enabled.
- DCS makes use of the NetBIOS protocol to resolve machine names. If the NetBIOS protocol is disabled on the server side, the server cannot enumerate any client machines. If NetBIOS is disabled on the client side, then the client will not be enumerated and will not appear in the scan result.
- Aside from enabling the NetBIOS protocol over TCP/IP, you can also place a file named ExtraDomainMachineList.ini into the DCS root folder to specify the domain of particular machines by IP address or IP range. For details, see Adding the ExtraMachineDomainList.ini File, page D-7.

Note If your system uses NAT, you must create an ExtraMachineDomainList.ini file.

Step 5 Verify that the WINS server in the network is working correctly.

Step 6 Verify that the DNS server in the network is working correctly.

Step 7 Use the UNC path to log on to the client machine and access the default shared folder, and then copy a file to that machine:

```
c\: \\[Client Machine Name]\c$
```

If the DCS server cannot log on to the client machine and copy a file, check the account privilege and the security policy settings of the machine or domain.

Step 8 Enable ICMP. DCS uses ICMP to detect the existence of a client machine. If ICMP has been blocked, then DCS cannot find the client.

APPENDIX E

Open Source License Acknowledgments

Trend Micro InterScan for CSC SSM uses the following open source licenses:

Notices

Some components of CSC SSM may be covered under one or more of the open source licences printed in this appendix. However, the Cisco warranty for the product shall remain in effect to its full extent and shall apply to the entire product.

The following notices pertain to these software licenses.

OpenSSL/Open SSL Project

Open SSL, version 0.9.6L, owner: n/a

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Module License Acknowledgments

Tomcat, xerces, and APR Modules

Tomcat, version 6.0.14, owner: Apache Software Foundation

xerces, version 1.7.0, owner: Apache Software Foundation

The Apache Software License, Version 1.1

Copyright (c) 1999, 2000 The Apache Software Foundation.

All rights reserved

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following

   "This product includes software developed by the Apache Software Foundation <http://www.apache.org/>."

   Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.
4. The names "The Jakarta Project", "Tomcat", and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <apache@apache.org>.
5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

JRE Module

JRE, version 1.5.0, owner: Sun Microsystems

Sun Microsystems, Inc. Binary Code License Agreement for the JAVATM 2 RUNTIME ENVIRONMENT (J2RE), STANDARD EDITION, VERSION 1.4.2_X

SUN MICROSYSTEMS, INC. (“SUN”) IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY “AGREEMENT”). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE “ACCEPT” BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE “DECLINE” BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. **DEFINITIONS**. “Software” means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. “Programs” mean Java applets and applications intended to run on the Java 2 Platform, Standard Edition (J2SETM platform) platform on Java-enabled general purpose desktop computers and servers.
2. **LICENSE TO USE.** Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.
3. **RESTRICTIONS**. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.
4. **LIMITED WARRANTY.** Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided “AS IS”. Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.
5. **DISCLAIMER OF WARRANTY.** UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.
6. **LIMITATION OF LIABILITY**. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES,

HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. **SOFTWARE UPDATES FROM SUN.** You acknowledge that at your request or consent optional features of the Software may download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun (“Software Updates”), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

8. **SOFTWARE FROM SOURCES OTHER THAN SUN.** You acknowledge that, by your use of optional features of the Software and/or by requesting services that require use of the optional features of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun (“Other Software”). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

9. **TERMINATION.** This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

10. **EXPORT REGULATIONS.** All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

11. **TRADEMARKS AND LOGOS.** You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations (“Sun Marks”), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

12. **U.S. GOVERNMENT RESTRICTED RIGHTS.** If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13. **GOVERNING LAW.** Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14. **SEVERABILITY**. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.
15. **INTEGRATION.** This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

a. S**oftware Internal Use and Development License Grant.** Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

b. **License to Distribute Software.** Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

c. **License to Distribute Redistributables.** Subject to the terms and conditions of this Agreement, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software “README” file (“Redistributables”) provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (v) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

d. **Java Technology Restrictions.** You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

e. **Source Code.** Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

f. **Third Party Code.** Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution. For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#135003/Form ID#011801)

SQLite Module

SQLite, version 3.5.8, owner: Public Domain

SQLite is public domain and does not require a license.

STLport Module

STLport, version 4.5.3, owner: n/a

License Agreement

Boris Fomitchev grants Licensee a non-exclusive, non-transferable, royalty-free license to use STLport and its documentation without fee.

By downloading, using, or copying STLport or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of the United States of America, and to all of the terms and conditions of this Agreement.

Licensee shall maintain the following copyright and permission notices on STLport sources and its documentation unchanged:

Copyright 1999,2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The Licensee may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions.

The Licensee may distribute original or modified STLport sources, provided that:

The conditions indicated in the above permission notice are met;

The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met:

Copyright 1994 Hewlett-Packard Company

Copyright 1996,97 Silicon Graphics Computer Systems, Inc.

Copyright 1997 Moscow Center for SPARC Technology.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

zlib General Purpose Compression Library Module

zlib, version 1.2.1, owner engelen

zlib.h -- interface of the 'zlib' general purpose compression library

version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

gSOAP Module

gSOAP, version2.7.11, owner: engelen

gSOAP Public License

Version 1.3a

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

1 DEFINITIONS.

sep 0mm

1.0.1.

1.1. “Contributor”

means each entity that creates or contributes to the creation of Modifications.

1.2. “Contributor Version”

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. “Covered Code”

means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. “Electronic Distribution Mechanism”

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. “Executable”

means Covered Code in any form other than Source Code.

1.6. “Initial Developer”

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. “Larger Work”

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. “License”

means this document.

1.8.1. “Licensable”

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. “Modifications”

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

sep 0mm

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code, or previous Modifications.

1.10. “Original Code”

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. “Patent Claims”

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. “Source Code”

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. “You” (or “Your”)

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, “You” includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2 SOURCE CODE LICENSE.

sep 0mm

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

sep 0mm

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell (“offer to sell and import”) the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

sep 0mm

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell (“offer to sell and import”) the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

3 DISTRIBUTION OBLIGATIONS.

sep 0mm

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

sep 0mm

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled “LEGAL” which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6 VERSIONS OF THE LICENSE.

sep 0mm

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF

HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8 TERMINATION.

sep 0mm

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10 U.S. GOVERNMENT END USERS.

11 MISCELLANEOUS.

12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

EXHIBIT A.

“The contents of this file are subject to the gSOAP Public License Version 1.3 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.cs.fsu.edu/~engelen/soaplicense.html

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code of the gSOAP Software is: stdsoap.h, stdsoap2.h, stdsoap.c, stdsoap2.c, stdsoap.cpp, stdsoap2.cpp, soapcpp2.h, soapcpp2.c, soapcpp2_lex.l, soapcpp2_yacc.y, error2.h, error2.c, symbol2.c, init2.c, soapdoc2.html, and soapdoc2.pdf, httpget.h, httpget.c, stl.h, stldeque.h, stllist.h, stlvector.h, stlset.h.

The Initial Developer of the Original Code is Robert A. van Engelen. Portions created by Robert A. van Engelen are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contributor(s):

“________________________.”

[Note: The text of this Exhibit A may differ slightly form the text of the notices in the Source Code files of the Original code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

EXHIBIT B.

“Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

HyperSonic SQL Module

HSQLDB, version 1.7.1, owner: Hypersonic/HSQLDB

Copyright (c) 2001-2002, The HSQL Development Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyrights and Licenses

This product includes Hypersonic SQL.

Originally developed by Thomas Mueller and the Hypersonic SQL Group.

Copyright (c) 1995-2000 by the Hypersonic SQL Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes Hypersonic SQL.”

- Products derived from this software may not be called “Hypersonic SQL” nor may “Hypersonic SQL” appear in their names without prior written permission of the Hypersonic SQL Group.

- Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes Hypersonic SQL.”

This software is provided “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the Hypersonic SQL Group or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption). However caused any on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

This software consists of voluntary contributions made by many individuals on behalf of the Hypersonic SQL Group.

For work added by the HSQL Development Group:

Copyright (c) 2001-2002, The HSQL Development Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer, including earlier license statements (above) and comply with all above license conditions.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution, including earlier license statements (above) and comply with all above license conditions.

Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ICU Module

ICU, version 1.8.1, owner: IBM

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2006 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

PCRE Module

PCRE, version 4.2, owner: Philip Hazel

PCRE LICENSE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the “BSD” licence, as specified below. The documentation for PCRE, supplied in the “doc” directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE “BSD” LICENCE

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

bash, binutils, busybox, diffutils, e2fsprogs, Grub, iptables, kysmoops, libncurses, libol, Linux-PAM, mod-utils, procfs, syslog-ng, systat, termcap, and util-linux Modules

bash, version 3, owner: Free Software Foundation

binutils, version 2.15, owner: Free Software Foundation

busybox, version 1.10.1, owner: Denis Vlasenko

diffutils, version 2.8.1, owner: Free Software Foundation

e2fsprogs, version 1.40.2, owner: Free Software Foundation

Grub, version 0.95, owner Free Software Foundation

iptables, version 1.3.8, owner: netfilter core team

kysmoops, version 2.4.11, owner: Free Software Foundation

libncurses, 5.4, owner: Free Software Foundation

libol, version 0.3.14, owner: bazis

Linux-PAM, version 0.77, owner: Andrew Morgan

mod-utils, version 2.4.27, owner: Keith Owens

procfs, version 3.2.7, owner: Procfs Project

syslog-ng, version 1.6.5, owner: bazis

systat, version 8.0.0, owner: Sebastien Goddard

termcap, version 1.3.1, Free Software Foundation

util-linux, version 2.21r, owner: Adrian Bunk

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

The Free Software Foundation has exempted Bash from the requirement of Paragraph 2c of the General Public License. This is to say, there is no requirement for Bash to print a notice when it is started interactively in the usual way. We made this exception because users and standards expect shells not to print such messages. This exception applies to any program that serves as a shell and that is based primarily on Bash as opposed to other GNU software.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the

program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and

modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at leas the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type “show w”. This is free software, and you are welcome to redistribute it under certain conditions; type “show c” for details.

The hypothetical commands “show w” and “show c” should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than “show w” and “show c”; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Curl Module

Curl, version 7.17, owner: The cURL Project

libxml Module

libxml, version 2.2.6, owner: n/a

The MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

libuuid Module and glibc Module

libuuid, version 1.2.7, Theodore Y. T’so

glibc, version 2.3.4, owner Free Software Foundation

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”). Each licensee is addressed as “you”.

   A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

   “Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

      (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

   When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

      For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

      It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

    This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

Platform Support License Acknowledgements

Linux Kernel

Linux Kernal, v2.6.17.8, owner Linus Torvalds

NOTE! This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of “derived work”. Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the linux kernel) is copyrighted by me and others who actually wrote it.

Linus Torvalds

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in

themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

   associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail. If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type “show w”.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands “show w” and “show c” should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than “show w” and “show c”; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

tftp-hpa Support

tftp-hpa, version 0.48, owner: H. Peter Anvin

The Berkeley copyright poses no restrictions on private or commercial use of the software and imposes only simple and uniform requirements for maintaining copyright notices in redistributed versions and crediting the originator of the material only in advertising.

For instance:

Copyright (c) 1982, 1986, 1990, 1991, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

1. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Berkeley rescinded the 3rd term (the advertising term) on 22 July 1999. Verbatim copies of the Berkeley license in the OpenBSD tree have that term removed. In addition, many 3rd-party BSD-style licenses consist solely of the first two terms.

Because the OpenBSD copyright imposes no conditions beyond those imposed by the Berkeley copyright, OpenBSD can hope to share the same wide distribution and applicability as the Berkeley distributions. It follows however, that OpenBSD cannot include material which includes copyrights which are more restrictive than the Berkeley copyright, or must relegate this material to a secondary status, i.e. OpenBSD as a whole is freely redistributable, but some optional components may not be.

cracklib License

cracklib, version 2.7, owner Alec Muffett

This document is freely plagiarized from the 'Artistic Licence', distributed as part of the Perl v4.0 kit by Larry Wall, which is available from most major archive sites

This documents purpose is to state the conditions under which these Packages (See definition below) viz: "Crack", the Unix Password Cracker, and "CrackLib", the Unix Password Checking library, which are held in copyright by Alec David Edward Muffett, may be copied, such that the copyright holder maintains some semblance of artistic control over the development of the packages, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

So there.

Definitions:

A "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification, or segments thereof.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when AND WHY you changed that file, and provided that you do at least ONE of the following:
    a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
    b. use the modified Package only within your corporation or organization.

   c. rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide separate documentation for each non-standard executable that clearly documents how it differs from the Standard Version.
   d. make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
   a. distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
   b. accompany the distribution with the machine-readable source of the Package with your modifications.
   c. accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
   d. make other distribution arrangements with the Copyright Holder.
5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. YOU MAY NOT CHARGE A FEE FOR THIS PACKAGE ITSELF. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that YOU DO NOT ADVERTISE this package as a product of your own.
6. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
7. THIS PACKAGE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

tcpdump License

tcpdump, version 3.8.3, owner The Tcpdump Group

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS ORIMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

libncurses License

libncurses, version 5.4, owner: Free Software Foundation

Copyright (c) 1998,2000 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESSOR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

OpenSSH

OpenSSH, version 3.9p1, owner: OpenBSD

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

1)

OpenSSH contains no GPL code.

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licensed software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library

- IDEA is no longer included, its use is deprecated

- DES is now external, in the OpenSSL library

- GMP is no longer used, and instead we call BN code from OpenSSL

- Zlib is now external, in a library

- The make-ssh-known-hosts script is no longer included

- TSS has been removed

- MD5 is now external, in the OpenSSL library

- RC4 support has been replaced with ARC4 support from OpenSSL

- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>

<http://www.core-sdi.com>

3)

ssh-keygen was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. *

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

HIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE.

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Per Allansson

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom

Tim Rice

Andre Lucas

Chris Adams

Corinna Vinschen

Cray Inc.

Denis Parker

Gert Doering

Jakob Schlyter

Jason Downs

Juha Yrj÷lS

Michael Stone

Networks Associates Technology, Inc.

Solar Designer

Todd C. Miller

Wayne Schroeder

William Jones

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8)

Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

“THE BEER-WARE LICENSE” (Revision 42):

<phk@login.dknet.dk> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995

This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.

Todd C. Miller

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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, IntelliTrap pattern and exception pattern files, 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.”

ad hoc query A quick method of extracting information directly from the Control Manager database. The database contains information collected from all CSC SSMs registered to the Control Manager server.

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 B-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 Choosing options for how Trend Micro InterScan for Cisco CSC SSM functions, for example, choosing 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 Dialers, as the name implies, dial to predefined numbers to connect to certain sites. Many users run dialers without knowing that some of these programs actually dial long distance numbers or connect to pay-per-call sites; and that they are being charged for the calls. Dialers are often offered as programs for accessing adult sites.

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.

Email Reputation (ER) technology

Email Reputation (formerly Network Reputation) 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.

Email Reputation Services (ERS)

Email Reputation Services (formerly Network Reputation Services) are services offer by Trend Micro that stops over 80% of spam at its source. Before it reaches your network, the IP address of incoming mail is verified against the world's largest reputation database managed by the Trend Micro Threat Prevention Network that catches not only spam but stops new techniques involving botnets and zombies.

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

ICMP Internet Control Message Protocol. This protocol is used to handle error and control messages at the IP layer. ICMP is actually part of the IP protocol.

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.

imssd The process that implements the scanning of SMTP traffic.

IMSS InterScan Messaging Suite™, Trend Micro's stand-alone SMTP/POP3 anti-virus product on which the Mail Scanner module of CSC was based.

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.

IntelliTrap IntelliTrap is heuristic-based technology that works in real-time to detect potentially malicious code in compressed files that arrive as e-mail attachments. Enabling IntelliTrap allows CSC SSM to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

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 anti-virus 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.

IWSS InterScan Web Security Suite™, Trend Micro's stand-alone HTTP anti-virus product, on which the Web Scanner module of CSC was based.

iwss-process The IWSS process that implements the scanning of HTTP traffic.

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.

KIPF

Kelkea IP Filter, which is part of the Mail Scanner module that implements the Email Reputation Service feature.

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.

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.

MTA Mail Transfer Agent software that transfers e-mail from one host to another (for example, Sendmail and Postfix).

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 Service (see ERS), the CSC anti-spam feature whose filter checks the sending MTA IP addresses with a database of “Spammer” 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.

PID The process ID, a number that is used by the operating system to uniquely identify a running process.

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 B-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.

Q

QIL One of the two databases that the ERS feature queries to check whether or not an IP address is a spammer.

R

RBL One of the two databases that the ERS feature queries to check whether or not an IP address is a spammer.

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.

RPC Remote Procedure Call. A protocol governing the method with which an application activates processes on other nodes and retrieves results.

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 B-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.

TMASE Trend Micro™ Anti-Spam Engine, a heuristic engine that examines the header and body of e-mails to determine whether they are spam.

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, cleans or deletes the message, and sends a notification to the system administrator, message sender, and/or 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 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.

VSAPI Virus Scan API and the main virus scanner engine for Trend Micro.

W

web The World Wide Web, also called the web or the Internet.

Web Reputation Web Reputation is a technology that guards end-users against emerging Web threats by assigning reputation scores (or rating) to URLs.

Web Reputation Services Web Reputation Services are offered by Trend Micro to detect and block Web-based security risks, including phishing attacks.

web server A server process running at a Web site 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