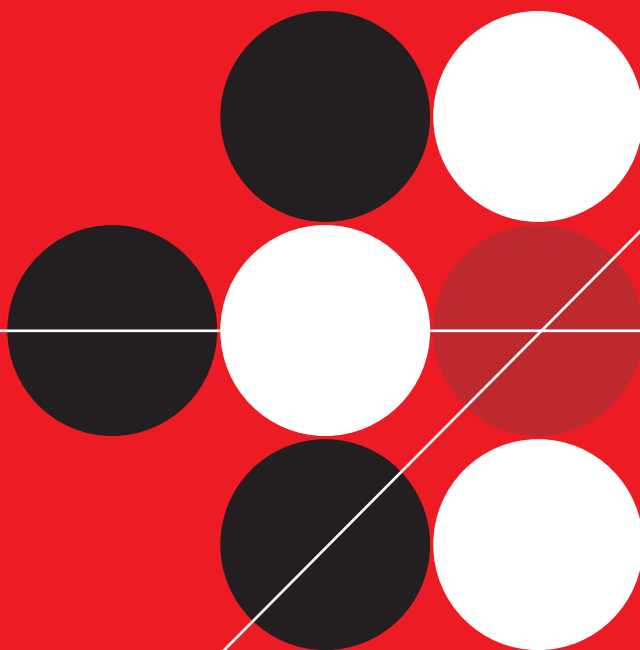


TREND MICRO™

InterScan™ Gateway Security Appliance M-Series

Administrator's Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Should we need to make changes to this document and to the products described herein, we shall however inform you of such changes when they have occurred. Before installing and using the software, please review the readme files, release notes (if any), and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

<http://www.trendmicro.com/download/documentation/>

Trend Micro, the Trend Micro t-ball logo, IntelliTrap, InterScan, ScanMail, MacroTrap, and TrendLabs are trademarks, registered trademarks, or servicemarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2007 Trend Micro Incorporated. All rights reserved.

Document Part No. SAEM12627/60117

Release Date: January 2007

Protected by U.S. Patent No. 5,623,600 and pending patents.

The *Trend Micro InterScan Gateway Security Appliance M-Series Administrator's Guide* is intended to provide detailed information about how to use and configure the features of the hardware device. Read it before using the software.

Additional information about how to use specific features within the software is available in the online help file and the online Knowledge Base at the Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any other Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Contents

Introduction

Audience	xii
About This Administrator's Guide	xii
Document Conventions	xiii

Chapter 1: Introducing Trend Micro InterScan Gateway Security Appliance

What Is InterScan Gateway Security Appliance?	1-2
Important Features and Benefits	1-3
How InterScan Gateway Security Appliance Works	1-5
Antivirus	1-6
Anti-Spyware	1-6
Anti-Spam	1-7
Anti-Phishing	1-7
Content and URL Filtering	1-8
Outbreak Defense	1-8
The Appliance Hardware	1-9
The Front Panel	1-9
LCD Module	1-10
LED Indicators	1-11
The Back Panel	1-12
Port Indicators	1-13
Preconfiguring and Deploying the Appliance	1-14
Connecting to the Network	1-15
Testing the Appliance Connectivity	1-15
Activating the Appliance	1-16

Chapter 2: How InterScan Gateway Security Appliance Works

The Range and Types of Internet Threats	2-2
How InterScan Gateway Security Appliance Protects You	2-3
The Primary Functional Components	2-4
Ethernet Network Interfaces	2-4
Real-Time Scan of SMTP, POP3, HTTP, and FTP Protocols	2-5
The Web Console	2-5
Content Filtering	2-5
Anti-Spam	2-6
Using Trend Micro Anti-Spam Engine	2-7
Using Approved and Blocked Senders Lists	2-8
Approved and Blocked Senders	2-9
Using Network Reputation Services	2-10
The Virus Scan Module	2-19
Outbreak Defense Services	2-20
Mail Notification	2-21
The Log Module	2-22
The Quarantine	2-22
The Delete Function	2-22

Chapter 3: Getting Started with InterScan Gateway Security Appliance

Preliminary Tasks	3-2
Accessing the Web Console	3-3
The Summary Screen	3-4
Information Above the Panels	3-4
Outbreak Prevention Service	3-5
Damage Cleanup Service	3-6
Component Version	3-6
Antivirus	3-8
Anti-Spyware	3-9
IntelliTrap	3-9
Anti-Spam: Content Scanning	3-10
Anti-Spam: Network Reputation Services	3-11
Others	3-11
Additional Screen Actions	3-11
Navigating the Web Console	3-12
The Online Help System	3-13

Chapter 4: SMTP Services

SMTP Services	4-2
Enabling Scanning of SMTP Traffic	4-3
Configuring SMTP Virus Scanning	4-3
SMTP Scanning - Target	4-4
SMTP Scanning - Action	4-6
SMTP Scanning - Notification	4-8
Configuring SMTP Anti-Spyware	4-9
SMTP Anti-Spyware - Target	4-10
SMTP Anti-Spyware - Action	4-12
SMTP Anti-Spyware - Notification	4-13
Configuring SMTP IntelliTrap	4-13
SMTP IntelliTrap - Target	4-14
SMTP IntelliTrap - Action	4-14
SMTP IntelliTrap - Notification	4-15
Configuring SMTP Anti-Spam: Network Reputation Services	4-16
SMTP Anti-Spam: Network Reputation Services - Target	4-17
SMTP Anti-Spam: Network Reputation Services - Action	4-18
Configuring SMTP Anti-Spam: Content Scanning	4-19
SMTP Anti-Spam: Content Scanning - Target	4-20
SMTP Anti-Spam: Content Scanning - Action	4-21
Configuring SMTP Anti-Phishing	4-22
SMTP Anti-Phishing - Target	4-23
SMTP Anti-Phishing - Action	4-23
SMTP Anti-Phishing - Notification	4-24
Configuring SMTP Content Filtering	4-25
SMTP Content Filtering - Target	4-26
SMTP Content Filtering - Action	4-28
SMTP Content Filtering - Notification	4-29

Chapter 5: HTTP Services

HTTP Services	5-2
Enabling Scanning of HTTP Traffic	5-2
Configuring HTTP Virus Scanning	5-2
HTTP Scanning - Target	5-3
Configuring Virus Scanning for HTTP Traffic	5-3
About Deferred Scan for Large File Handling	5-5
HTTP Scanning - Action	5-6
HTTP Scanning - Notification	5-7
Configuring HTTP Anti-Spyware	5-8
HTTP Anti-Spyware - Target	5-8
HTTP Anti-Spyware - Action	5-10
HTTP Anti-Spyware - Notification	5-11
Configuring HTTP Anti-Pharming	5-12
HTTP Anti-Pharming - Target	5-12
HTTP Anti-Pharming - Action	5-12
HTTP Anti-Pharming - Notification	5-13
Configuring HTTP Anti-Phishing	5-14
HTTP Anti-Phishing - Target	5-14
HTTP Anti-Phishing - Action	5-15
HTTP Anti-Phishing - Notification	5-16
Configuring HTTP URL Filtering	5-17
HTTP URL Filtering - Rules	5-17
HTTP URL Filtering - Settings	5-19
HTTP URL Filtering - Notification	5-21
Configuring HTTP File Blocking	5-22
HTTP File Blocking - Target	5-22
HTTP File Blocking - Notification	5-23

Chapter 6: FTP Services

FTP Services	6-2
Enabling Scanning of FTP Traffic	6-2
Configuring FTP Virus Scanning	6-2
FTP Scanning - Target	6-3
FTP Scanning - Action	6-5
FTP Scanning - Notification	6-6

Chapter 6: FTP Services—continued

Configuring FTP Anti-Spyware	6-7
FTP Anti-Spyware - Target	6-8
FTP Anti-Spyware - Action	6-10
FTP Anti-Spyware - Notification	6-11
Configuring FTP File Blocking	6-12
FTP File Blocking - Target	6-12
FTP File Blocking - Notification	6-14

Chapter 7: POP3 Services

POP3 Services	7-2
Enabling Scanning of POP3 Traffic	7-2
Configuring POP3 Virus Scanning	7-3
POP3 Scanning - Target	7-3
POP3 Scanning - Action	7-5
POP3 Scanning - Notification	7-7
Configuring POP3 Anti-Spyware	7-8
POP3 Anti-Spyware - Target	7-9
POP3 Anti-Spyware - Action	7-11
POP3 Anti-Spyware - Notification	7-12
Configuring POP3 IntelliTrap	7-13
POP3 IntelliTrap - Target	7-13
POP3 IntelliTrap - Action	7-14
POP3 IntelliTrap - Notification	7-15
Configuring POP3 Anti-Spam	7-16
POP3 Anti-Spam - Target	7-16
POP3 Anti-Spam - Action	7-18
Configuring POP3 Anti-Phishing	7-18
POP3 Anti-Phishing - Target	7-19
POP3 Anti-Phishing - Action	7-19
POP3 Anti-Phishing - Notification	7-20
Configuring POP3 Content Filtering	7-21
POP3 Content Filtering - Target	7-22
POP3 Content Filtering - Action	7-24
POP3 Content Filtering - Notification	7-25

Chapter 8: Outbreak Defense

The Outbreak Defense Services	8-2
Current Status	8-3
Configuring Internal Outbreak	8-5
Configuring Damage Cleanup	8-6
Potential Threat	8-7
Configuring Settings	8-7
Outbreak Defense - Settings	8-8
Outbreak Defense - Notification	8-9
Yellow Alerts	8-10
Red Alerts	8-10

Chapter 9: Quarantines

Quarantines	9-2
Conducting a Query	9-3
Performing Quarantine Maintenance	9-7
Manual	9-7
Automatic	9-8

Chapter 10: Update

Update	10-2
Executing a Manual Update	10-3
Configuring Scheduled Updates	10-4
Configuring an Update Source	10-6

Chapter 11: Logs

Logs	11-2
Performing a Log Query	11-3
Configuring Log Settings	11-5
Configuring Log Maintenance	11-6
Manual	11-6
Automatic	11-7

Chapter 12: Administration

Administration	12-2
Access Control	12-3
Configuration Backup	12-4
Disk SMART Test	12-5
IP Address Settings	12-6
Management IP Address	12-6
Static Routes	12-8
Notification Settings	12-11
Settings	12-12
Events	12-13
Operation Mode	12-14
Password	12-15
Product License	12-16
Proxy Settings	12-19
SNMP Settings	12-20
System Time	12-22
World Virus Tracking	12-23

Chapter 13: Technical Support, Troubleshooting, FAQ

Contacting Technical Support	13-2
Readme.txt	13-3
Troubleshooting	13-4
Frequently Asked Questions (FAQ)	13-4
Recovering a Password	13-6
Virus Pattern File	13-7
Spam Engine and Pattern File	13-8
Hot Fixes, Patches, and Service Packs	13-8
Patches	13-9
Licenses	13-9
Renewing Maintenance	13-10
EICAR- Test Virus	13-11
Best Practices	13-12
Handling Compressed Files	13-12
Block compressed files if... ..	13-12
Handling Large Files	13-14
Sending Trend Micro Suspected Internet Threats	13-16

Chapter 14: Updating the InterScan Gateway Security Appliance Firmware

Updating the InterScan Gateway Security Appliance	
Device Image	14-2
Preparing InterScan Gateway Security Appliance for the	
Device Image Update	14-2
The Preconfiguration Console	14-2
Using the LCD Module	14-2
Before the Update	14-3
Backing Up Your Configuration	14-3
Putting the Appliance Into Rescue Mode	14-10
Uploading the New Device Image	14-11
Uploading with Existing Configuration (Option 3)	14-12
Uploading with the Restored, Default Configuration	
(Option 5)	14-18
Completing the Process After the Device Image	
Is Uploaded	14-26
BMC and BIOS Firmware Updates Using the	
Appliance Firmware Flash Utility	14-28
Updating the Appliance BMC Firmware	14-28
Preparing to Upload the BMC Firmware	14-28
Uploading the BMC Firmware	14-33
After the BMC Upload	14-36
Updating the Appliance BIOS Firmware	14-36
Preparing to Upload the Appliance BIOS	14-36
Uploading the Appliance BIOS Firmware	14-37
After the BIOS Firmware Upload	14-39
Troubleshooting BMC or BIOS Firmware Upload	14-39

Appendix A: Terminology

BOT	A-2
Grayware	A-2
Macro Viruses	A-2
Mass-Mailing Attacks	A-3
Network Viruses	A-3
Pharming	A-3
Phishing	A-4
Spam	A-4
Spyware	A-4
Trojans	A-5
Viruses	A-5
Worms	A-5

Appendix B: Technology Reference

Deferred Scan	B-2
Diskless Mode	B-2
False Positives	B-3
LAN Bypass	B-3
ScanEngine Technology	B-4
IntelliScan	B-4
IntelliTrap	B-4
MacroTrap	B-5
WormTrap	B-5
Supported DCS Clients	B-6
Feature Execution Order	B-6
SMTP feature execution order is:	B-6
POP3 feature execution order is:	B-6
HTTP feature execution order is:	B-6
FTP feature execution order is:	B-6

Appendix C: Removing the Hard Disk

Appendix D: System Checklist

Appendix E: File Formats Supported

Compression Types	E-2
Blockable File Formats	E-4
Malware Naming Formats	E-5

Appendix F: Specifications and Environment

Hardware Specifications	F-2
Dimensions and Weight	F-2
Power Requirements and Environment	F-3

Introduction

Welcome to the *Trend Micro™ InterScan™ Gateway Security Appliance M-Series Administrator's Guide*. This book contains information about the tasks involved in configuring, administering, and maintaining the Trend Micro InterScan Gateway Security Appliance. Use it in conjunction with the *Trend Micro™ InterScan™ Gateway Security Appliance M-Series Getting Started Guide*, which provides up-front details about initial planning, preconfiguring, and deploying the appliance.

Audience

This book is intended for network administrators who want to configure, administer, and maintain InterScan Gateway Security Appliance (the appliance). It assumes a working knowledge of security systems and devices, as well as network administration.

About This Administrator's Guide

The *InterScan™ Gateway Security Appliance M-Series Administrator's Guide* discusses the following topics:

Chapter 1: Introducing InterScan Gateway Security Appliance

Chapter 2: How InterScan Gateway Security Appliance Works

Chapter 3: Getting Started with InterScan Gateway Security Appliance

Chapter 4: SMTP Services

Chapter 5: HTTP Services

Chapter 6: FTP Services

Chapter 7: POP3 Services

Chapter 8: Outbreak Defense

Chapter 9: Quarantines

Chapter 10: Update

Chapter 11: Logs

Chapter 12: Administration

Chapter 13: Technical Support

Chapter 14: Updating the InterScan Gateway Security Appliance Firmware

Appendixes

Document Conventions

To help you locate and interpret information easily, the *InterScan Gateway Security Appliance M-Series Administrator’s Guide* uses the following conventions:

TABLE 1. Conventions used in the Trend Micro InterScan Gateway Security Appliance M-Series documentation

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
<i>Italics</i>	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided
INT	InterScan Gateway Security Appliance interface connected to the protected network
EXT	InterScan Gateway Security Appliance interface connected to the external or public network (usually the Internet)

Introducing Trend Micro InterScan Gateway Security Appliance

This chapter introduces InterScan Gateway Security Appliance and provides an overview of its technology, capabilities, and hardware connections.

This chapter includes the following topics:

- *What Is InterScan Gateway Security Appliance?* on page 1-2
- *Important Features and Benefits* on page 1-3
- *How InterScan Gateway Security Appliance Works* on page 1-5
- *The Appliance Hardware* on page 1-9
- *Preconfiguring and Deploying the Appliance* on page 1-14
- *Connecting to the Network* on page 1-14
- *Testing the Appliance Connectivity* on page 1-15
- *Activating the Appliance* on page 1-16

What Is InterScan Gateway Security Appliance?

Trend Micro™ InterScan™ Gateway Security Appliance (the appliance) is an all-in-one security appliance that blocks threats automatically, right at the Internet gateway. The appliance provides a critical layer of security against such threats as viruses, spyware, spam, phishing, botnet attacks, harmful URLs, and inappropriate content, while complementing desktop solutions. Because it sits between your firewall and network, the appliance augments existing firewall and VPN solutions to stop outbreaks early. And because the security features of the appliance are configured to work right out of the box, your network is protected from the moment the appliance is connected.

The appliance comes preconfigured with software, making it easy to deploy. Administrators can manage the appliance quickly and easily from a single Web-based console. The appliance can also save time and money by:

- Providing the tools to assist you to more effectively achieve regulatory compliance
- Preserving network resource availability and reducing spam so your employees can be more productive
- Integrating multiple products into one solution
- Using Damage Cleanup Services to dramatically reduce administrative effort, cost, and downtime caused by spyware and viruses
- Using IntelliTrap heuristic detection and Outbreak Prevention Services to provide increased defense against emerging threats

Important Features and Benefits

TABLE 1-1. Important Features and Benefits

Features	Description
All-in-one defense	Antivirus, anti-spam, anti-spyware/grayware, anti-phishing, IntelliTrap™ (Bot threats), content filtering, Outbreak Prevention Services (OPS), URL blocking, and URL filtering IntelliTrap detects malicious code such as bots in compressed files. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap is a real-time, rule-based pattern-recognition scan-engine technology that detects and removes known viruses in files compressed up to 20 layers deep using any of 16 popular compression types.
Automatic threat protection	Outbreak Defense — An integral part of Trend Micro's Enterprise Protection Strategy (EPS), which enables Trend Micro devices to proactively defend against threats in their insurgency before traditional pattern files are available.
Gateway protection	Protection from malware right at the Internet gateway
Flexible configuration	Specify files to scan. Specify the action to take on infected files/messages. Specify who to send notifications to when InterScan Gateway Security Appliance detects a threat.
Centralized management	A Web-based console, accessible from a local or remote computer, that enforces company-wide Internet security policies Web browser support for Microsoft Internet Explorer 6.x and Mozilla Firefox 1.x
Automated maintenance	Maintenance tasks, such as updating InterScan Gateway Security Appliance components and maintaining log files, can be automated to save time.

TABLE 1-1. Important Features and Benefits (Continued)

SMTP, POP3, FTP and HTTP scanning capabilities	SMTP and POP3 scanning support: antivirus, IntelliTrap, spyware/grayware detection, anti-spam, anti-phishing, and content filtering, including notification messages to the administrator and users upon detection of phishing messages FTP scanning support: antivirus and spyware/grayware detection HTTP scanning support: antivirus, spyware/grayware detection, and blocking of pharming and phishing URLs
Anti-spam configuration	Allows an administrator to do the following: Set the spam threshold to high, medium, or low. Specify approved and blocked senders. Define certain categories of mail as spam.
URL filtering	URL filtering for the HTTP protocol Allows the administrator to define and configure URL filtering policies for work time and leisure time Local cache support to reduce network traffic Provides a notification to users if URL filtering disallows the URL they want to access
URL file blocking	URL file blocking for the HTTP protocol Allows the administrator to block selected file types Provides a notification to users when a file type is blocked
Network Reputation Services (NRS)	NRS blocks spam by validating the IP addresses of incoming mail against databases—the Real-Time Blackhole List (RBL+) and the QIL—of known spam sources.

How InterScan Gateway Security Appliance Works

InterScan Gateway Security Appliance sits between your firewall and your network, acting as a multiprotocol security gateway between the Internet and your business. With security features for SMTP, POP3, HTTP, and FTP, InterScan Gateway Security Appliance acts as a one-stop solution for all your security needs.

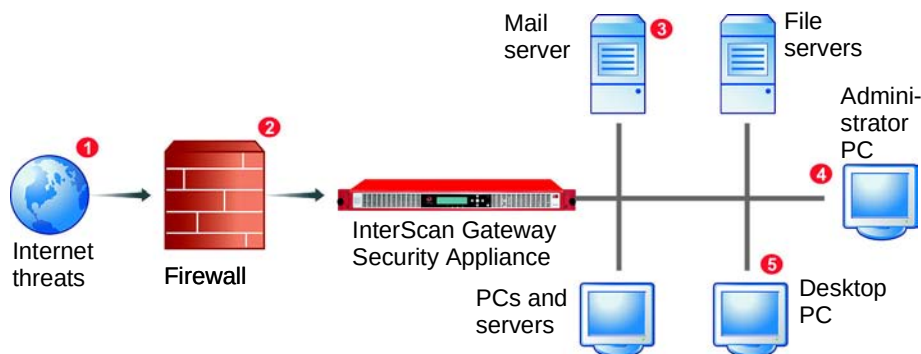


FIGURE 1-1. How InterScan Gateway Security Appliance Works

InterScan Gateway Security Appliance blocks viruses, spyware, spam, phishing, botnet attacks, harmful URLs, and inappropriate content before they enter your network.

- 1** Blocks multiple Internet threats
- 2** Complements existing firewall and VPN
- 3** Decreases spam, email storage, and the cost of regulatory compliance
- 4** Cleans up viruses and spyware at the desktop
- 5** Controls users' Web access with scheduling and policies

InterScan Gateway Security Appliance stops threats at the gateway, using a variety of innovative technologies, including:

Antivirus

The antivirus security in InterScan Gateway Security Appliance guards every network entry point—from the Internet gateway and network perimeter to email and file servers, desktops, and mobile devices.

- Delivers proven virus protection. Blocks viruses, worms, and Trojans using patterns, heuristics, and other innovative technologies.
- Stops file-based viruses, malware, worms, and botnets. Runs inline network scans to detect and block worms and botnets.
- Contains outbreaks. Isolates infected network segments—before threats can spread.
- Blocks malicious mobile code. Screens Web pages for malware hidden in applets, ActiveX controls, JavaScript, and VBScript.
- Automates damage cleanup. Removes malware and spyware from memory of clients and servers including guest devices.
- Detects zero-day threats in real time. IntelliTrap heuristic detection and Outbreak Prevention Services increase defenses against emerging threats.

Anti-Spyware

The anti-spyware feature in InterScan Gateway Security Appliance blocks incoming spyware and the outbound data being collected by spyware. Innovative technology also prevents users from browsing Web sites that install tracking software. If spyware is already installed, end users can automatically clean the infected system by clicking a URL.

- Stops spyware at multiple layers. Delivers end-to-end spyware protection— from the Web gateway to client/server networks.
- Automates cleanup. Removes spyware, unwanted grayware, and remnants from both the server and desktop active memory.

- Prevents “drive by” downloads (downloads of malware through exploitation of a Web browser, e-mail client or operating system bug, without any user intervention whatsoever). Screens Web pages for malicious mobile code and blocks “drive by” spyware installations.
- Blocks URLs known for spyware. Prevents users from browsing Web sites known to harbor malicious spyware.

Anti-Spam

InterScan Gateway Security Appliance stops spam from consuming network resources and wasting employees’ valuable time. The key to its effective protection is the use of adaptable technology that evolves as spamming techniques change and become more sophisticated.

- Blocks spam at the outermost network layer. Stops spam at the IP-connection layer before it can enter your network and burden IT resources.
- Detects known spam sources. Validates IP addresses against the largest reputation database of known spammers.
- Stops spam in real time. Uses dynamic reputation analysis to detect spam, zombies, and botnets in real time.
- Filters messaging traffic. Blocks spam at the Internet gateway before it can get to your mail servers and impact performance.
- Improves spam detection. Combines machine learning, pattern recognition, heuristics, blocked sender lists and approved sender lists for better detection.
- Enables customizing. Gives the flexibility to customize policy and spam tolerance levels.

Anti-Phishing

The anti-phishing security function in InterScan Gateway Security Appliance offers a comprehensive approach to stop identity theft and protect confidential corporate information.

- Filters messaging traffic. Stops fraudulent, phishing-related email at the messaging gateway and mail servers.
- Prevents theft. Protects credit card and bank account numbers, user names, and passwords, and so on.

Content and URL Filtering

The URL filtering security function in InterScan Gateway Security Appliance enables companies to manage employee Internet use and block offensive or non-work-related Web sites. By restricting content, employers can improve network performance, reduce legal liability, and increase employee productivity.

- Manages employee Internet use. Enables IT to set Web-use policies for the company, groups, or individuals.
- Offers flexible filtering options. Filters by category, time, day, bandwidth, key words, file name, true file type, and so on.
- Filters Web content. Blocks inappropriate content from entering your network and prevents sensitive data from going out.
- Categorizes Web sites in real time. Employs dynamic rating technology to categorize Web sites while users browse.

Outbreak Defense

In the event of an Internet outbreak of viruses or malware, the Outbreak Defense function in InterScan Gateway Security Appliance works to protect networks before they have been exposed—but also repairs client's computers if they have been exposed.

- Provides defense against outbreaks. When an outbreak occurs anywhere in the world, TrendLabsSM rapidly responds by developing an Outbreak Prevention Policy (OPP).
- Provides automated policy delivery. Trend Micro ActiveUpdate servers automatically deploy the OPP to InterScan Gateway Security Appliance.
- Provides strategic protective advice. The OPP contains a list of actions that InterScan Gateway Security Appliance administrators should take to reduce the threat to clients.
- Provides damage management. Damage Cleanup Services and Damage Cleanup Tools clean any clients that have been exposed to malware.
- Moves from prevention to cure. The OPP remains in effect until TrendLabs develops a more complete solution to the threat.

The Appliance Hardware

The Front Panel

The front panel of the InterScan Gateway Security Appliance contains two (2) thumb screws and a removable bezel for holding it in a fixed position in a rack cabinet. These screws should only be used in conjunction with the rail mounting kit. (See *Trend Micro InterScan Gateway Security Appliance M-Series Getting Started Guide* for details on mounting the device.) These screws alone will not support the weight of the device. At the center of the bezel is the Liquid Crystal Display (LCD) Module.

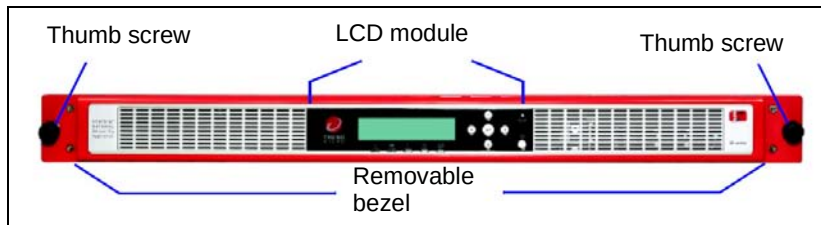


FIGURE 1-2. Front Panel

The following table describes each front panel element.

TABLE 1-2. Front panel elements

Front Panel Elements	Description
LCD Module	The LCD Module is made up of the following items: Liquid Crystal Display (LCD) Control panel Reset button UID button LED indicators The rest of the table contains the descriptions for each item
Liquid Crystal Display (LCD)	A 2.6in x 0.6in (65mm x 16mm) dot display LCD that is capable of displaying messages in 2 rows of 16 characters each. Displays device status and preconfiguration instructions
Control panel	1 5-button control panel that provides LCD navigation. Used for inputting data during preconfiguration
Reset button	Restarts the device
LED Indicators 1 to 5	Indicates the Power, UID, System, Hard Disk, and Outbreak status Power and UID have one color each; System, Hard Disk, and Outbreak have two colors each
UID button	Unique ID button that illuminates a blue LED on the front and rear of the device, which helps administrators locate the device for trouble-shooting or maintenance
Bezel	Detachable casing that covers and protects the front panel
Thumb screws	Used for fixed mounting in any standard 19-inch rack

LCD Module

The LCD and control panel elements are collectively referred to as the LCD Module.

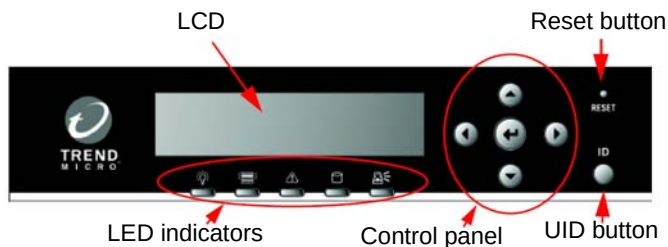


FIGURE 1-3. LCD Module

LED Indicators

The LCD Module has five light-emitting diodes (LEDs) that indicate the **POWER**, **UID**, **SYSTEM**, **HARD DISK**, and **OUTBREAK** status, as shown in the figure below.

TABLE 1-3. Possible behavior for each LED indicator

LED Name	Icon	State	Description
POWER		Yellow, steady	The appliance is operating normally
		Off (no color)	The appliance is off
UID		Blue, steady	The UID LED is illuminated because UID button is pressed
		Off (no color)	The UID LED is not illuminated (default is off)
SYSTEM		Red, flashing	The appliance is booting
		Red, steady	Power-On Self-Test (POST) error
		Yellow, flashing	The appliance OS and applications are booting
		Yellow, steady	The appliance program file (firmware) encountered a critical error
		Green, steady	The appliance program file (firmware) is ready
HARD DISK		Green, steady	The appliance hard disk is operating normally
		Red, steady	Hard disk has failed and the appliance is operating in diskless mode
OUTBREAK		Green, steady	Outbreak Prevention Services (OPS) is disabled
		Red, flashing	OPS is enabled

The Back Panel

The back panel of InterScan Gateway Security Appliance contains a power receptacle, power switch, USB ports, serial connection, fan vent, and LAN ports.

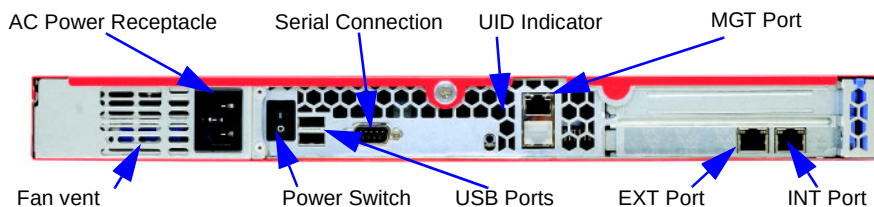


FIGURE 1-4. Back panel

The following table describes each back panel element.

TABLE 1-4. Back panel elements

Element	Description
AC power receptacle	Connects to a power outlet and InterScan Gateway Security Appliance using the power cord (included in the package)
Power switch	Turns the device on and off
DB9 Serial Connection	Connects to a computer's serial port with a DB9 type connection to perform preconfiguration
Ports MGT, EXT, INT	Copper Gigabit LAN port designated as the MANAGEMENT EXTERNAL or INTERNAL port depending on the Operation Mode
Fan Vent	Cooling vent for three (3) system fans
UID LED and UID Button	LED at the back panel of InterScan Gateway Security Appliance. When a user presses the UID button, the UID LED illuminates. The illuminated UID LED allows administrators to easily locate InterScan Gateway Security Appliance for troubleshooting or maintenance
USB Ports	USB ports, reserved for future releases

Port Indicators

InterScan Gateway Security Appliance has three (3) user-configurable copper-based Ethernet ports. Each Ethernet port has two (2) indicator lights that allow you to determine the port's current state and duplex speed.

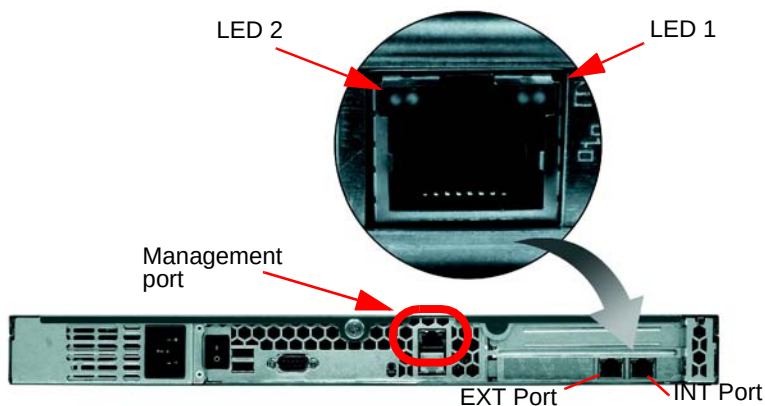


FIGURE 1-5. Port indicators

The following table describes the status of the port indicators when the device is operating normally.

TABLE 1-5. Port indicator status

Indicator Number	Purpose	State	Description
LED 1	Port activity	Light off	No data being received
		Green, flashing	Receiving data
LED 2	Duplex speed	Light off	10mbps LED
		Green, steady	100mbps LED
		Yellow, steady	1000mbps LED

To understand how the port indicators work when InterScan Gateway Security Appliance is operating in LAN bypass mode, see “LAN Bypass” in the InterScan Gateway Security Appliance Online Help.

Note: Loss of power to the InterScan Gateway Security Appliance will automatically reset the appliance, so that all data passes through.

Preconfiguring and Deploying the Appliance

Your InterScan Gateway Security Appliance must be assigned an IP address to operate on your network. This is done in one of three ways:

- Using a DHCP server, InterScan Gateway Security Appliance is automatically assigned a Dynamic IP address during deployment. This is the preferred method. Normally, you have one DHCP server per subnet; however, administrators can use a DHCP relay agent to support multiple subnets.
- Using a Preconfiguration Console—a terminal communications program such as HyperTerminal (for Windows) or Minicom (for Linux)—manually assign a Dynamic or Static IP address to the InterScan Gateway Security Appliance during preconfiguration. If you choose Static, you will be required to set the netmask address, default gateway address, and primary DNS address, as well as a host name.
- Using the LCD Module, manually assign a Dynamic or Static IP address to the InterScan Gateway Security Appliance during preconfiguration. If you choose Static, you will be required to set the netmask address, default gateway address, and primary DNS address, as well as a host name.

Note: You may also be required to provide a secondary DNS server address. See *InterScan Gateway Security Appliance M-Series Getting Started Guide* for full preconfiguration instructions.

Connecting to the Network

With a DHCP server, you can connect InterScan Gateway Security Appliance to your network right out of the box without having to undergo a preconfiguration process. Once connected, InterScan Gateway Security Appliance can handle various interface speeds and duplex mode network traffic.

To connect the InterScan Gateway Security Appliance to your network:

1. Connect one end of the Ethernet cable to the INT port (right side) and the other end to the segment of the network that InterScan Gateway Security Appliance will protect (the Protected Network).
2. Connect one end of another Ethernet cable to the EXT port (left side) and the other end to the part of the network that leads to the public network.
3. Using the Power Switch in the back, power on the device.

Note: To prevent accidental shutdown of the appliance, the InterScan Gateway Security Appliance power switch has been modified from the standard On/Off convention. To power on InterScan Gateway Security Appliance, simply press the Power Switch upward from the 0 to 1 position. To power off InterScan Gateway Security Appliance, press the power switch upward from 0 to 1 and **hold it in that position for a minimum of five seconds**.

Testing the Appliance Connectivity

Perform either of the following tasks to test whether you have successfully configured the InterScan Gateway Security Appliance.

To test if the device is configured properly, do one of the following:

1. Ping the device to verify connectivity; you can obtain the IP address by looking at the LCD panel on the front of the device.
2. Browse the InterScan Gateway Security Appliance Web interface by going to a PC on the protected network and opening an Internet Explorer browser to **https://{the appliance IP Address}**

Activating the Appliance

The Trend Micro sales team or sales representative provides the Registration Key. Use the Registration Key to obtain a full version Activation Code.

To obtain the Activation Code:

1. Go to the Trend Micro Online Registration Web site.
(<https://olr.trendmicro.com/registration>). The Online Registration page of the Trend Micro Web site opens.
2. Perform one of the following:
 - If you are an existing Trend Micro customer, log on using your logon ID and password in the **Returning, registered users** section of the page.
 - If you are a new customer, select your **Region** from the drop-down menu in the **Not Registered** section of the page and click **Continue**.
3. On the **Enter Registration Key** page, type or copy the InterScan Gateway Security Appliance Registration Key, and then click **Continue**.
4. On the **Confirm License Terms** page, read the license agreement, and then click **I accept the terms of the license agreement**.
5. On the **Confirm Product Information** page, click **Continue Registration**.
6. Fill out the online registration form, and then click **Submit**. Trend Micro will send you a confirmation message that you need to acknowledge by clicking **OK**.
7. Click **OK** twice.

After the registration is complete, Trend Micro emails you an Activation Code, which you can then use to activate InterScan Gateway Security Appliance.

A Registration Key has 22 characters (including the hyphens) and looks like this:

xx-xxxx-xxxx-xxxx-xxxx

An Activation Code has 37 characters (including the hyphens) and looks like this:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

How InterScan Gateway Security Appliance Works

This chapter describes in depth how InterScan Gateway Security Appliance works. It provides an overview of the range of Internet security threats, what InterScan Gateway Security Appliance does to protect you, and how it accomplishes its protective tasks. The topics discussed in this chapter include:

- *The Range and Types of Internet Threats* on page 2-2
- *How InterScan Gateway Security Appliance Protects You* on page 2-3
- *The Primary Functional Components* on page 2-4

The Range and Types of Internet Threats

Over the years, as the Internet has developed, so too has the creation of a wide range of Internet threats, collectively known as “malware.” Thousands of viruses are known to exist and virus writers are creating more each day. In addition to viruses, new threats designed to exploit vulnerabilities in corporate email systems and Web sites continue to emerge. Typical types of malware include the following:

TABLE 2-1. Types of Internet threats

Threat Type	Characteristics
Bot	Bots are compressed executable files that are often designed with the intent to cause harm to computer systems and networks. Bots, once executed, can replicate, compress, and distribute copies of themselves. Typical uses of malicious bots are Denial-of-Service attacks, which can overwhelm a Web site and make it unusable.
Pharming	Similar in nature to email phishing, pharming seeks to obtain personal or private information (usually financially related) through domain spoofing.
Phishing	Phishing is the use of unsolicited email to request user verification of private information, such as credit card or bank account numbers, with the intent to commit fraud.
Spam	Unsolicited, undesired bulk email messages that frequently use various tricks to bypass email filtering.
Spyware	Technology that aids in gathering information about a person or organization.
Trojan	Malware that performs unexpected or unauthorized—often malicious—actions. Trojans cause damage and unexpected system behavior and compromise system security, but unlike viruses, they do not replicate.
Virus	A program that carries a destructive payload and that replicates, spreading quickly to infect other systems. Viruses remain one of the most prevalent threats to computing.
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, typically via network connections or email attachments.

How InterScan Gateway Security Appliance Protects You

InterScan Gateway Security Appliance is designed to protect you against such malware and other Internet threats, utilizing software technologies that work in conjunction with the appliance hardware to automate security, while allowing custom management and targeted administration of device settings. The primary functional components in InterScan Gateway Security Appliance include:

- Ethernet network interfaces
- Real-time scan of SMTP, POP3, HTTP, and FTP protocols
- Web console for management and administration
- Security Services: Content Filtering, Anti-spam, Antivirus, IntelliTrap, Anti-spyware, Anti-phishing, Anti-pharming, URL Filtering, File Blocking, Outbreak Defense Services
- Virus Scan Module: True Type File ID, IntelliScan
- Support Functions: Mail Notification, Log, Quarantine, and Delete

The Primary Functional Components

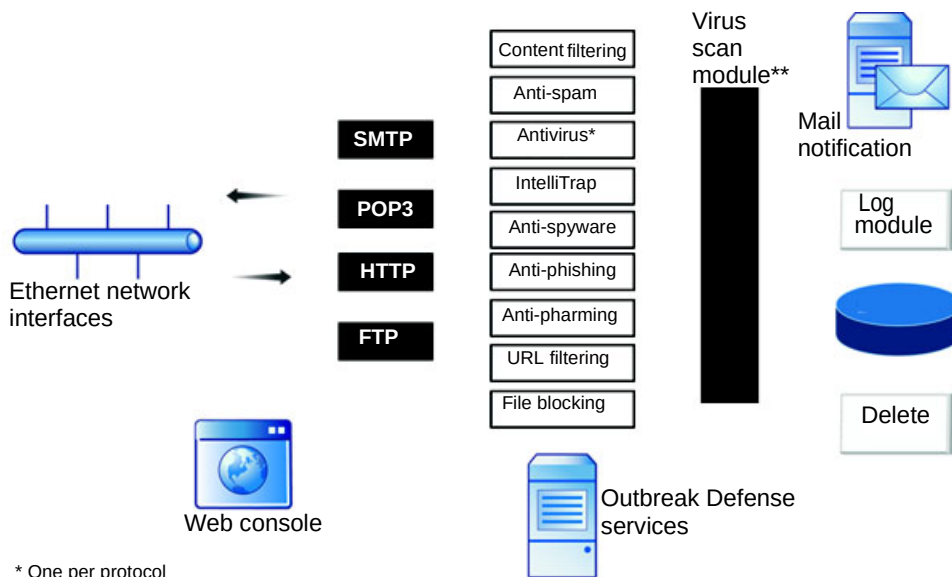


FIGURE 2-1. InterScan Gateway Security Appliance Primary Functional Components

Each of the primary functional components of InterScan Gateway Security Appliance is explained below, along with the underlying processes that are executed by each component.

Ethernet Network Interfaces

InterScan Gateway Security Appliance is an inline device that provides bi-directional support for 10MB, 100MB, and 1GB Ethernet networks through its multi-speed Ethernet Network Interfaces. When InterScan Gateway Security Appliance is attached to your local area network (LAN), its auto-sensing feature automatically adjusts to the speed of your network.

Real-Time Scan of SMTP, POP3, HTTP, and FTP Protocols

Three of the primary types of software tools in use on the Internet are email programs, Web browsers, and file transfer programs, delivered over SMTP/POP3, HTTP, and FTP protocols respectively. Since these programs and protocols are the primary ways that malware can get onto your network and computers, any security solution that wishes to be comprehensive must address each protocol in turn. InterScan Gateway Security Appliance meets this requirement and does so strategically—right at the Internet gateway.

InterScan Gateway Security Appliance performs real-time scans of SMTP, POP3, HTTP, and FTP protocols, providing protocol-specific protection whether you are sending and receiving email, browsing the Web, or transferring files to and from FTP sites. By conducting real-time scans of SMTP, POP3, HTTP, and FTP traffic right at the gateway, InterScan Gateway Security Appliance halts malicious payloads before they can enter your network.

The Web Console

Trend Micro provides easy administration and management of InterScan Gateway Security Appliance through a Web console, accessible from any machine outfitted with a compatible Web browser. Compatible browsers are:

- Microsoft Internet Explorer 6.x
- Mozilla Firefox 1.x

Using the Web console, you have easy access to all InterScan Gateway Security Appliances on the network. The InterScan Gateway Security Appliance Web console lets you configure the appliance, customize settings, and generally manage all your security processes from one convenient interface, accessible anywhere on your local area network (LAN)—or even remotely, from over the Internet, while providing security from unauthorized users. See the sections “Accessing the Web Console” and “Navigating the Web Console” in *Chapter Three: Getting Started with InterScan Gateway Security Appliance* for more details.

Content Filtering

Objectionable content in email is a problem for both inbound and outbound mail. Thus, the content filter in InterScan Gateway Security Appliance provides a means for the administrator to evaluate and control the delivery of email based on the mes-

sage text itself. The content filter helps to monitor inbound and outbound messages to check for the existence of harassing, offensive, or otherwise objectionable message content. Examples of what the content filter can identify include:

- Sexually harassing language
- Racist language
- Spam embedded in the body of an email message

The content filtering function in InterScan Gateway Security Appliance evaluates inbound and outbound messages based on user-defined rules. Each rule contains a list of keywords and phrases. Content filtering evaluates the message size, header and body content, and attachment name. When content filtering finds a word that matches a keyword in one of the keyword lists it takes the action specified by the administrator in the content filtering action screen. InterScan Gateway Security Appliance can send notifications whenever it takes action in response to undesirable content.

InterScan Gateway Security Appliance applies the content filtering rules to email in the same order as displayed in the Content Filtering screen of the Web console. The InterScan Gateway Security Appliance scans each email message. If a message triggers one or more filtering violations, InterScan Gateway Security Appliance takes the action that the administrator has defined in the action section of the Content Filtering screen.

Anti-Spam

Spam email is a mounting problem for businesses, consuming network, computer and human resources by its sheer volume. To address this problem, the anti-spam function in InterScan Gateway Security Appliance helps reduce the occurrence of spam email. Trend Micro anti-spam, using a spam engine, Approved and Blocked Senders lists, spam pattern file, and Network Reputation Services works in conjunction with the InterScan Gateway Security Appliance to scan for and filter spam.

If spam logging is enabled, InterScan Gateway Security Appliance will write spam detections to the Anti-spam: Content Scanning log or the Anti-spam: Network Reputation Services log. You can export the contents of the Anti-spam logs for inclusion in reports.

InterScan Gateway Security Appliance uses the following components to filter email messages for spam:

- Trend Micro Anti-spam engine
- Approved and Blocked senders lists
- Keyword Exceptions list
- The Network Reputation Services databases

InterScan Gateway Security Appliance applies the Anti-spam filtering rules to email messages in the following order: Approved Senders > Blocked Senders > Exception Keywords.

Note: InterScan Gateway Security Appliance can quarantine messages in the user's spam mail folder if the Exchange server has the End User Quarantine tool. When spam messages arrive, the system quarantines them in this folder. End users can access the spam folder to open, read, or delete suspect spam messages.

Using Trend Micro Anti-Spam Engine

The Anti-spam engine in InterScan Gateway Security Appliance uses spam patterns and heuristic rules to filter email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. The Anti-spam engine compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, the Anti-spam engine takes action against the spam. The spam detection levels are as follows:

Low—this is most lenient level of spam detection. InterScan Gateway Security Appliance will filter only the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

Medium—this is the default setting. InterScan Gateway Security Appliance monitors at a high level of spam detection with a moderate chance of filtering false positives.

High—this is the most rigorous level of spam detection. InterScan Gateway Security Appliance monitors all email messages for suspicious files or text, but there is greater chance of false positives.

Administrators cannot modify the method that the Anti-spam engine uses to assign spam scores, but they can adjust the detection levels used by the Anti-spam engine to decide which messages are considered spam.

Example: Spammers sometimes use numerous exclamation marks (!!!!) in their email messages. When the Anti-spam engine detects a message that uses exclamation marks this way, it increases the spam score for that email message.

Tip: In addition to using Anti-spam to screen spam, you can configure content filtering to scan message headers, subject, body, and attachment information for spam and other undesirable content.

Using Approved and Blocked Senders Lists

Use the Web console to set up lists of Approved or Blocked Senders to control how InterScan Gateway Security Appliance filters email messages.

InterScan Gateway Security Appliance does not classify addresses from the Approved Senders list as spam unless it detects a phishing incident. If InterScan Gateway Security Appliance detects a phishing incident in a message from an Approved sender, it will classify the message as phishing and will take the action for phishing.

InterScan Gateway Security Appliance filters addresses from Blocked Senders lists and always classifies them as spam and takes the action set by the administrator.

Note: Administrators set up Approved Senders and Blocked Senders lists in InterScan Gateway Security Appliance. End users can also set up Approved Senders lists using End User Quarantine. If an end user approves a sender, but the sender is on the administrator's Blocked Senders list, InterScan Gateway Security Appliance will block messages from that sender and classify them as spam.

Approved and Blocked Senders

An Approved Senders list is a list of trusted email addresses. InterScan Gateway Security Appliance will not classify messages arriving from these addresses as spam.

A Blocked Senders list is a list of suspect email addresses. InterScan Gateway Security Appliance always categorizes email messages from blocked senders as spam and takes the appropriate action.

The InterScan Gateway Security Appliance administrator uses the Anti-spam page to manage his or her lists. The administrator's Approved Senders list and Blocked Senders list control how InterScan Gateway Security Appliance handles email messages bound for the end users.

Wildcard Matching

InterScan Gateway Security Appliance supports wildcard matching for Approved Senders and Blocked Senders lists. It uses the asterisk (*) as the wildcard character. For more information, refer to the table below:

TABLE 2-2. Wildcard Matching

Pattern	Matched Samples	Unmatched Samples
john@trend.com	john@trend.com john@trend.com	Any address different from the pattern.
@trend.com *@trend.com	john@trend.com mary@trend.com	john@ms1.trend.com john@trend.com.tw mary@trend.com
trend.com	john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com	john@trend.com.tw mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com	john@trend.com john@trend.com.tw mary@ms1.trend.com

TABLE 2-2. Wildcard Matching (Continued)

trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw	john@trend.com john@ms1.trend.com john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com
..*.trend.com *****.trend.com	The same as "*.trend.com"	
trend.com trend.com trend.*.com @*.trend.com	All invalid.	

InterScan Gateway Security Appliance does not support wildcard matching on the username part. However, if you type a pattern such as “*@trend.com”, InterScan Gateway Security Appliance still treats it as “@trend.com”. This feature applies to the user-defined Approved Senders and Blocked Senders.

Using the Keyword Exception List

Use the Keyword Exception list as a way to reduce the chances that the spam engine and pattern file might classify legitimate email as spam.

Use the Web console to set up a list of keywords to control how InterScan Gateway Security Appliance filters email messages.

InterScan Gateway Security Appliance scans the email message body. If the message body contains a word from the Keyword Exception list, InterScan Gateway Security Appliance classifies the message as legitimate email.

Using Network Reputation Services

Anti-Spam Network Reputation Services (NRS) is part of the InterScan Gateway Security Appliance Anti-spam solution. If enabled, NRS can effectively block up to 80% of spam at its source. NRS uses a Real-Time Blackhole List (RBL) and QIL to

identify spam sources. NRS blocks spam at its source by validating the IP address of the SMTP server sending the inbound mail to a list of IP addresses in the RBL and QIL databases.

TABLE 2-3. RBL and QIL databases

NRS Resource	Description
Real-Time Black-hole List (RBL)	RBL is a database that contains the IP addresses of SMTP servers that originate spam or are considered to be spam open-relay hosts. InterScan Gateway Security Appliance categorizes the IP addresses listed in the RBL as permanent sources of spam.
QIL	QIL is a database that contains the IP addresses of SMTP servers that either originate spam or are considered to be spam open-relay hosts. InterScan Gateway Security Appliance categorizes the IP addresses listed in the QIL as impermanent sources of spam. The IP addresses in this list change frequently.

How Network Reputation Services Works

Network Reputation Services (NRS) blocks spam by comparing the IP address of an SMTP server to lists containing the IP addresses of known spam distributors.

For example, user A, in Seattle, sends email to user B in Los Angeles. User B's SMTP server is behind an InterScan Gateway Security Appliance and the NRS service is enabled with the Low setting selected. When InterScan Gateway Security Appliance receives the email sending from user A's SMTP server to user B's SMTP server, it first checks Server A's IP address against the RBL database. If user A's SMTP server IP address is not on the list, InterScan Gateway Security Appliance sends the email to user B's SMTP server. However, if user A's SMTP server IP address is on the list, InterScan Gateway Security Appliance takes the action that the administrator defined in the Action settings screen.

If the administrator chose High setting in the Network Reputation Services screen, InterScan Gateway Security Appliance first checks the IP address of user A's SMTP server against the RBL database. If the SMTP server IP address is not in the RBL database, InterScan Gateway Security Appliance then queries the QIL database. If the SMTP server IP address is not in the QIL database, InterScan Gateway Security Appliance forwards the email to user B's SMTP server. If the QIL database does have

user A's SMTP IP address listed, InterScan Gateway Security Appliance takes the action that the administrator defined in the Action settings screen.

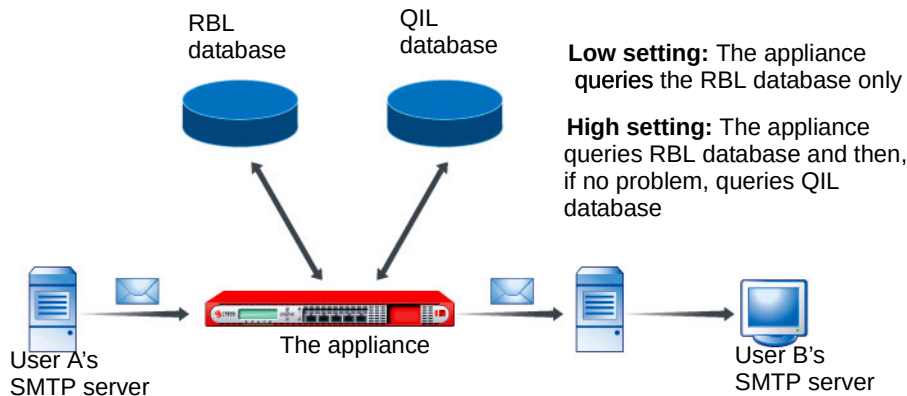


FIGURE 2-2. How the RBL and QIL databases work

Antivirus

Since viruses are still among the most numerous and serious threats on the Internet, virus scanning is a critical and integral part of the set of security services in InterScan Gateway Security Appliance. During a scan, the Trend Micro scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique “pattern” or string of telltale characters that distinguish it from any other code, the virus experts at TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When the scan engine detects a file containing a virus or other malware, it executes an action such as clean, delete, or replace with text/file. You can customize these actions when you set up your scanning tasks.

InterScan Gateway Security Appliance protects you from a wide range of viruses, including:

- HTML viruses
- Macro viruses
- ActiveX malicious code
- COM and EXE file infectors

InterScan Gateway Security Appliance supports virus scanning for SMTP, POP3, HTTP, and FTP protocols, as well as the following features:

- The ability to enable or disable scanning of certain protocols
- The ability to configure scanning for different file types
- Compressed file handling
- Scanning of incoming and outgoing traffic
- The ability to set actions to take when viruses or malware are detected
- The ability to send notifications
- Virus logging

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using different file compression schemes. To deal with this issue, InterScan Gateway Security Appliance uses IntelliTrap, which detects malicious code such as bots in compressed files. IntelliTrap provides heuristic evaluation of compressed files to help reduce the risk that a bot or other malware compressed using these methods will enter the network through email.

IntelliTrap uses the virus scan engine, IntelliTrap pattern, and exception pattern to scan incoming email and attachments to identify bots and other malware applications.

When InterScan Gateway Security Appliance detects a bot or other malware application it takes action according to the action chosen by the administrator under the Action tab. InterScan Gateway Security Appliance will then send a notification email to all persons specified under the Notification tab.

Note: IntelliTrap uses the same scan engine as virus scanning. As a result, the file handling and scanning rules for IntelliTrap will be the same as the ones the administrator defines for virus scanning.

The InterScan Gateway Security Appliance writes bot and other malware detections to the IntelliTrap log. You can export the contents of the IntelliTrap log for inclusion in reports.

IntelliTrap uses the following components when checking for bots and other malicious programs:

- Trend Micro virus scan engine and pattern file
- IntelliTrap pattern and exception pattern

Anti-Spyware

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

The existence of spyware and other types of grayware on your network have the potential to introduce the following:

- Reduced computer performance
- Increased Web browser-related crashes
- Reduced user efficiency
- Degradation of network bandwidth
- Loss of personal and corporate information
- Higher risk of legal liability

To address these problems, the Anti-spyware function in InterScan Gateway Security Appliance helps protect LAN users from inadvertently downloading spyware and grayware, which can collect personal and corporate information, reduce computer

performance, degrade network bandwidth, and more seriously, compromise the security of the network.

Using the spyware scan engine, pattern file, and cleanup template, the Anti-spyware function in InterScan Gateway Security Appliance monitors inbound and outbound SMTP, POP3, HTTP, and FTP traffic for spyware and grayware.

When InterScan Gateway Security Appliance detects spyware or grayware in a specific protocol, it will take the action that the administrator has defined for that protocol. InterScan Gateway Security Appliance will then send a notification email to all persons specified in the Notification section for the specific protocol.

InterScan Gateway Security Appliance writes spyware and grayware detections to the Anti-spyware/grayware log. You can export the contents of the spyware/grayware log for inclusion in reports.

InterScan Gateway Security Appliance uses the following components when scanning for spyware:

- Trend Micro Spyware scan engine and pattern file
- Spyware/Grayware Exclusion List

Anti-Phishing

Because the Internet fraud known as phishing has become an increasing problem on the Internet, the Anti-phishing function in InterScan Gateway Security Appliance has been designed to protect LAN users from inadvertently giving away sensitive information as part of phishing expedition. Anti-phishing works in conjunction with InterScan Gateway Security Appliance to monitor:

- Outbound client URL requests and compare them to a known list of phish sites. Whenever a match occurs, Anti-phishing blocks access to the site.
- Email messages that contain links to phishing sites.

InterScan Gateway Security Appliance writes phishing events to the phishing log. You can export the log for inclusion in reports.

InterScan Gateway Security Appliance uses the following components to check for phishing:

- Trend Micro Anti-spam engine
- URL rating database

Because the incidence of phishing fraud is growing rapidly and the format continues to evolve, it is especially important to keep the spam pattern file up to date. Trend Micro recommends that you schedule frequent updates and set email notifications to let you know the status of scheduled updates. Check the version of the spam pattern file you are running and time of last update on the Summary screen.

From the main InterScan Gateway Security Appliance menu, click **Update > Schedule** and then choose an update frequency. Trend Micro recommends having InterScan Gateway Security Appliance check for updates at least once a day.

Anti-Pharming

As noted in the introduction to this chapter, the Internet fraud known as pharming has become an increasingly treacherous way to commit identity theft on the Internet. Thus, the Anti-pharming feature in InterScan Gateway Security Appliance is designed to protect LAN users from inadvertently giving away sensitive information as part of a pharming event.

The Anti-pharming function in InterScan Gateway Security Appliance monitors outbound client URL requests and compare them to a list of known pharming sites. If the URL of the requested site matches any of the URLs on the list, InterScan Gateway Security Appliance takes the action defined in the Action section of the HTTP Anti-pharming screen. If enabled, InterScan Gateway Security Appliance sends a notification email to the administrator. A notification message also appears on the user's browser explaining that InterScan Gateway Security Appliance has blocked access to the site for security reasons.

InterScan Gateway Security Appliance writes pharming events to the Anti-pharming log. You can export the contents of the log for inclusion in reports.

InterScan Gateway Security Appliance uses a URL rating database to check for pharming.

URL Filtering

Many companies have corporate policies that prohibit access to certain kinds of Web sites that are deemed offensive or in violation of company ethics. The URL filtering function in InterScan Gateway Security Appliance is thus designed to keep users from accessing sites that others might deem offensive or that violates company policy and ethics. URL filtering filters access to Web sites based on administrator-defined settings.

When a user requests access to a URL, InterScan Gateway Security Appliance checks the URL against the Trend Micro URL rating database. After the URL database returns a rating, InterScan Gateway Security Appliance checks the URL against the administrator-defined allowable categories. If the rating returned by the URL rating database matches one of the predefined categories set by the administrator, InterScan Gateway Security Appliance denies access to the Web site.

When InterScan Gateway Security Appliance denies access to a Web site, it sends a notification message to the user's browser informing them that it has denied access to the site based on company policy. InterScan Gateway Security Appliance also sends a notification to the administrator, if he or she has enabled that feature, whenever a user requests access to a prohibited site.

Note: If the rating server does not return a rating result in time, the default action is to allow access to the URL.

Unless the administrator has disabled this feature in the Log Settings screen, InterScan Gateway Security Appliance logs requests to access prohibited sites to the URL filtering log. You can export the contents of the log for inclusion in reports.

The URL filtering function in InterScan Gateway Security Appliance uses the following components when checking a URL:

- Trend Micro URL rating database
- Category filter list
- Blocked and Approved URL lists

InterScan Gateway Security Appliance applies the URL filtering rules according to the order shown in the URL Filtering > Target screen.

File Blocking

One of the ways malware can arrive on your desktop or network is through files that are streamed or downloaded from HTTP servers when a Web site is accessed, or from an FTP site. This is another security threat that must be addressed. InterScan Gateway Security Appliance can scan for and block certain file types that originate from HTTP and FTP servers, thus protecting your network and computers. Both predefined and administrator-specified file types can be blocked.

File Blocking checks the file type (true file type and file extensions) of both inbound and outbound HTTP and FTP files. The File Blocking feature blocks files according to the settings defined by the administrator in the File Blocking screen of the Web console.

The predefined list of file types that can be blocked by InterScan Gateway Security Appliance includes:

- Audio/Video
- Compressed
- Executable
- Java
- Microsoft documents

Note: See “Appendix C: File Blocking - File Formats” for a complete listing of files that can be blocked by InterScan Gateway Security Appliance.

When InterScan Gateway Security Appliance blocks a file, a notification message will appear on the user's browser informing them that InterScan Gateway Security Appliance has blocked the file. InterScan Gateway Security Appliance will send a notification to the administrator, if enabled, whenever it blocks a file.

When InterScan Gateway Security Appliance blocks a file, it will write the incident to the File blocking log. You can export the File blocking log for inclusion in reports.

The Virus Scan Module

True File Type and IntelliScan

Files can be easily renamed to disguise their actual type. Programs such as Microsoft Word are "extension independent"; that is, they will recognize and open "their" documents regardless of the file name. This poses a danger, for example, if a Word document containing a macro virus has been named "benefits form.pdf". Word will open the file, but the file may not have been scanned if InterScan Gateway Security Appliance is not set to check the true file type.

Rather than relying on the file name alone to decide if it should scan a file, InterScan Gateway Security Appliance uses IntelliScan to identify a file's true type.

True file-type detection—IntelliScan first examines the header of the file using true file-type identification and checks if the file is an executable, compressed, or other type of file that may be a threat. IntelliScan examines all files to be sure that the file has not been renamed—the extension must conform to the file's internally registered data type.

File extension checking—IntelliScan also uses extension checking, that is, the file name itself. The list of extension names to be scanned is updated with each new pattern file. For example, when there is a new vulnerability discovered with regard to ".jpg" files, the ".jpg" extension is immediately added to the extension-checking list for the next pattern update.

Only files of the type that are capable of being infected are scanned. For example, .gif files make up a large volume of all Web traffic, but they are not currently able to carry viruses and therefore do not need to be scanned. Similarly, .jpg files are not currently utilized to carry viruses, though there is some concern this may change in the future—which means, IntelliScan would be changed to also scan for this threat. As of date of publication of this manual, however, with true file type selected, once the true type has been determined, these inert file types are not scanned.

Outbreak Defense Services

A virus outbreak can occur on the Internet and spread rapidly. Outbreak Defense is a combination of services designed to protect networks in the event of an outbreak and to repair clients' computers that have been exposed to viruses or malware.

Outbreak Defense uses the following components to protect networks from outbreaks and clean clients exposed to viruses or malware:

- Outbreak Prevention Services and Outbreak Prevention Policy
- Damage Cleanup Services and Damage Cleanup Tool

Outbreak Prevention Services and Outbreak Prevention Policy

Outbreak Prevention Services protects networks by deploying an Outbreak Prevention Policy.

When TrendLabs receives information that a new outbreak is developing anywhere in the world, it quickly develops a response to it called an Outbreak Prevention Policy. Trend Micro ActiveUpdate servers then deploy the Outbreak Prevention Policy to InterScan Gateway Security Appliance. The Outbreak Prevention Policy remains in effect for the administrator-specified amount of time or until TrendLabs develops a complete solution to the threat.

The Outbreak Prevention Policy contains a list of actions that InterScan Gateway Security Appliance should take in order to reduce the likelihood of it or its clients becoming infected. For example, if the threat's main method of delivery is by email or FTP, InterScan Gateway Security Appliance blocks all incoming mail or block ports typically used by FTP.

During an outbreak, InterScan Gateway Security Appliance enacts the instructions contained in the Outbreak Prevention Policy. The Trend Micro Outbreak Prevention Policy is a set of recommended default security configurations and settings designed by TrendLabs to give optimal protection to your computers and network during outbreak conditions. InterScan Gateway Security Appliance downloads the Outbreak Prevention Policy from a Trend Micro ActiveUpdate server.

Damage Cleanup Services and Damage Cleanup Tool

Trend Micro Damage Cleanup Services (DCS) is a comprehensive service that helps assess and cleanup system damage without the need to install software on client computers. DCS helps restore your Windows system after a virus outbreak. Damage Cleanup Services can do the following:

- Removes unwanted registry entries created by worms or Trojans
- Removes memory-resident worms or Trojans
- Removes active spyware/grayware
- Removes garbage and viral files dropped by viruses
- Assesses a system to decide whether it is infected or not
- Returns the system to an active and clean state

Two versions of DCS are available at no charge, one for Trend Micro customers, and one for the general public.

You can download Damage Cleanup Services from the following Web site:

<http://www.trendmicro.com/download/product.asp?productid=48>

Damage Cleanup Services uses the following components to clean clients that have been exposed to viruses, malware, and spyware:

- Damage cleanup engine and template
- Spyware scan engine
- Manual Damage Cleanup tool

Mail Notification

Users and administrators need feedback when InterScan Gateway Security Appliance intervenes to stop viruses, spyware, phishing attempts, access to blocked URLs, and so on. To that end, InterScan Gateway Security Appliance provides a Mail Notification module that operates across the SMTP, POP3, HTTP, and FTP protocols to notify users and administrators when a security action is performed. Inline notification stamps can be inserted into all scanned message before they are sent; and senders, recipients, and administrators can receive standard or custom messages when a particular action is performed. Notification of potential threats can also be sent to

TrendLabs—for example, for a phishing URL—which enables Trend Micro to verify the accuracy of the potential threat, classify it within the TrendLabs databases, and if need be, take systematic action against the threat.

The Log Module

Administrators need a way to monitor scanning and detection activity of InterScan Gateway Security Appliance over time, both to provide an historical view, as well as to analyze those settings that may need to be modified to optimize security in the future. InterScan Gateway Security Appliance assists the administrator in these tasks by tracking all scanning and detection activity that it performs and writing this information to various logs. A log query feature allows you to create reports that show detection activity for the different protocols for the various types of scanning tasks that InterScan Gateway Security Appliance performs. A log maintenance feature allows you to perform log maintenance either manually or according to a schedule. You can also view the event log.

The Quarantine

Sometimes the best strategy for dealing with malware that arrives through email—messages that contain viruses, spyware, or bots—is to quarantine the message and its enclosures for further examination. The InterScan Gateway Security Appliance allows you to quarantine messages, files, or enclosed objects suspected of being malicious in a quarantine folder. Email that has triggered the content filtering rules can also be sent to the quarantine folder.

InterScan Gateway Security Appliance allows you to query the quarantine folder by time, sender, recipient, and subject. You can also perform basic maintenance on the quarantine folder such as manually deleting email messages or setting a schedule to delete email messages; and you can export a query of a set of quarantined files.

The Delete Function

InterScan Gateway Security Appliance can be configured to automatically delete or clean files enclosed in emails (over the SMTP or POP3 protocols) or files that are downloaded (over the HTTP or FTP protocols). InterScan Gateway Security Appliance also provides a delete function for logs and quarantines, so that, as files accumulate, administrators can maintain the log and quarantine databases over time.

Getting Started with InterScan Gateway Security Appliance

This chapter describes how to access InterScan Gateway Security Appliances from the Web console, view system information, deploy system components, and modify device settings.

The topics discussed in this chapter include:

- *Preliminary Tasks* on page 3-2
- *Accessing the Web Console* on page 3-3
- *The Summary Screen* on page 3-4
- *Navigating the Web Console* on page 3-12
- *The Online Help System* on page 3-13

Preliminary Tasks

InterScan Gateway Security Appliance is designed to provide good default protection from the moment it is installed on your network. After installation, however, you should perform a number of tasks to ensure that everything is set up and working optimally and that you are making full use of its many features. Following is a list of preliminary tasks that you can perform using the InterScan Gateway Security Appliance product console and the chapters in which those functions and settings are discussed:

TABLE 3-1. Preliminary tasks

Preliminary Task	See Chapter
Change the default admin password to ensure appliance security	Ch 12
Schedule default email notifications	Ch 12
Set up SMTP notifications	Ch 4
Update the virus pattern, URL Filtering, and scan engine file	Ch 10
Schedule automatic pattern and engine updates	Ch 10
Configure HTTP scanning policies	Ch 5
Set up Access Control (for remote access)	Ch 12
Create URL Filtering policies and test	Ch 5
Configure Anti-phishing settings and any specific URL sites to block	Ch 4, Ch 5, Ch 7
URL Blocking (local list)	Ch 5
URL Blocking (anti-phishing)	Ch 5
Create FTP scanning policies for inbound and outbound traffic	Ch 6
Obtain EICAR test file to confirm your installation is working properly	Ch 13
Test SMTP inbound scanning	Ch 4
Test SMTP outbound scanning	Ch 4
Test POP3 inbound scanning	Ch 7
Test HTTP download scanning	Ch 5
Test HTTP upload scanning	Ch 5
Test FTP scanning	Ch 6
Test URL blocking	Ch 5

Accessing the Web Console

Trend Micro has provided easy access to InterScan Gateway Security Appliance through a Web console, which is accessible from any machine with a compatible Web browser. Using the Web console, you have easy access to all InterScan Gateway Security Appliances on the network.

To access InterScan Gateway Security Appliances:

1. Open a compatible Web browser.
2. In the address field, type the URL (**https://URL or IP Address**) of the target InterScan Gateway Security Appliance Web console. For example, type <https://192.168.1.34>. The Web console Log On screen displays.

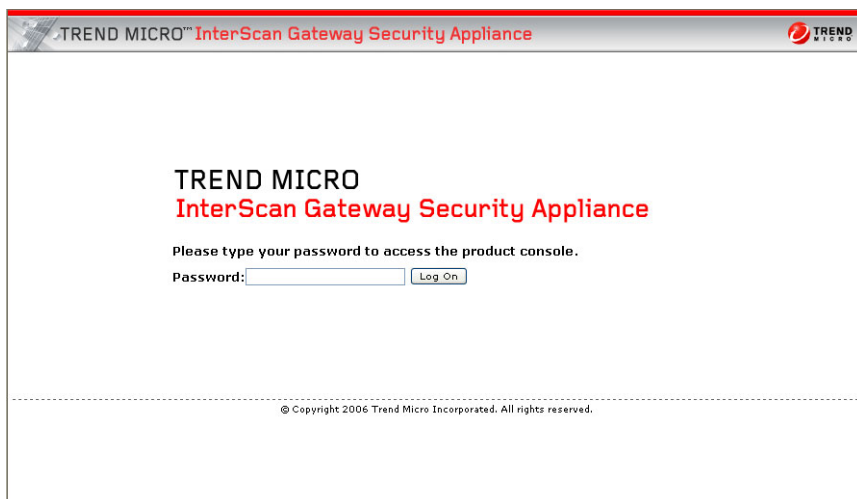


FIGURE 3-1. Web Console Log On Screen

3. Type the default password **admin** in the Password field and click **Log On**. The Summary screen displays.

Note: Once you access the Web console, you have continual access to the InterScan Gateway Security Appliance as long as you are making changes. If there is no activity, you are automatically logged out after 20 minutes to maintain security. To re-access the Web console, simply log on again. To manually log out, click the **Logout** link to the left of the Help menu.

The Summary Screen

The Summary screen is designed to provide all the information you need at-a-glance to easily monitor the status of your InterScan Gateway Security Appliance (the appliance). The Summary screen automatically displays information about the appliance even before you activate the product.

Tip: Action Summaries in the Summary screen panels provide statistics for Today, the Last 7 days, and the Last 30 days, along with totals for all items scanned.

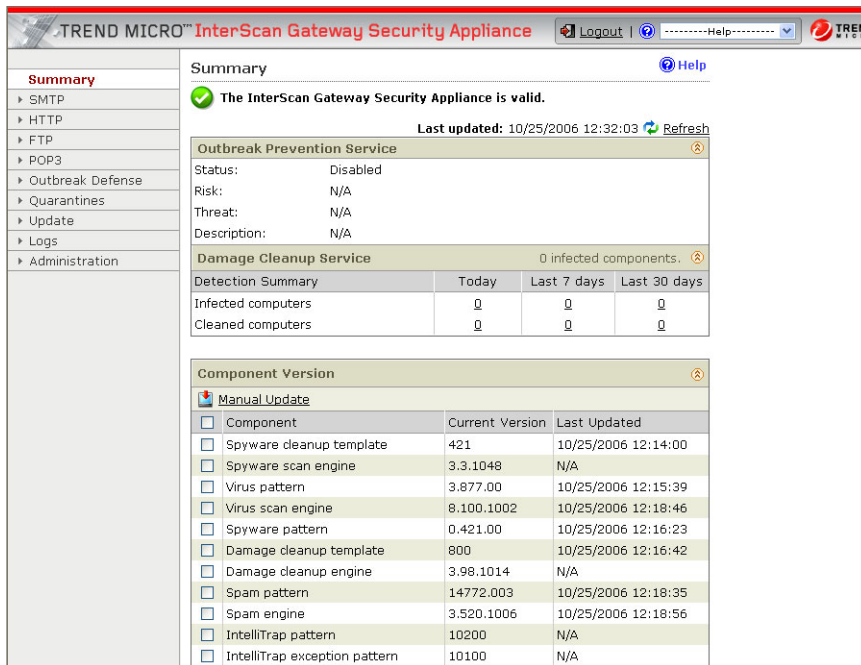
Information Above the Panels

Below the screen title, the first piece of information shown is the license status. If the InterScan Gateway Security Appliance license is current, a green arrow displays, along with the words, “**The InterScan Gateway Security Appliance is valid.**” If the appliance license is not current, a red arrow displays, along with information about how to register (or renew) the license.

Above the first panel, at the top right is a time/date stamp (**Last update:**) showing when the Summary screen was last updated. This time is taken directly from the InterScan Gateway Security Appliance itself when the Web page loads. The administrator can use this time to tell if the appliance is correctly synchronized with an NTP (Network Time Protocol) server and is using the correct time zone setting. The administrator can adjust the time on the appliance from the Web console. (See [System Time](#) on page 12-22 for more information.)

Scroll down the Summary screen to view the list of panels.

Outbreak Prevention Service



TREND MICRO™ InterScan Gateway Security Appliance Logout | Help

Summary Help

✓ **The InterScan Gateway Security Appliance is valid.**

Last updated: 10/25/2006 12:32:03 Refresh

Outbreak Prevention Service

Status: Disabled
Risk: N/A
Threat: N/A
Description: N/A

Damage Cleanup Service 0 infected components.

Detection Summary	Today	Last 7 days	Last 30 days
Infected computers	0	0	0
Cleaned computers	0	0	0

Component Version

Manual Update

Component	Current Version	Last Updated
☐ Spyware cleanup template	421	10/25/2006 12:14:00
☐ Spyware scan engine	3.3.1048	N/A
☐ Virus pattern	3.877.00	10/25/2006 12:15:39
☐ Virus scan engine	8.100.1002	10/25/2006 12:18:46
☐ Spyware pattern	0.421.00	10/25/2006 12:16:23
☐ Damage cleanup template	800	10/25/2006 12:16:42
☐ Damage cleanup engine	3.98.1014	N/A
☐ Spam pattern	14772.003	10/25/2006 12:18:35
☐ Spam engine	3.520.1006	10/25/2006 12:18:56
☐ IntelliTrap pattern	10200	N/A
☐ IntelliTrap exception pattern	10100	N/A

FIGURE 3-2. Summary Screen – First Three Panels

Outbreak Prevention Service displays information about the status of Outbreak Prevention Services (OPS) on your network and about the current threat that OPS is protecting against. Displayed are Status, Risk, Threat, and Description:

To get more information about the status of Outbreak Prevention Service, click **Outbreak Defense > Current Status** in the Main Navigation Menu.

Damage Cleanup Service

Damage Cleanup Service displays a total of all infected components and a summary of infected and cleaned computers.

Component Version

View component version information or manually update components from this section.

To perform a manual update of the InterScan Gateway Security Appliance components:

1. Select all of the components to update and then click the **Manual Update** link. The Manual Update > Update in Progress indicator appears.

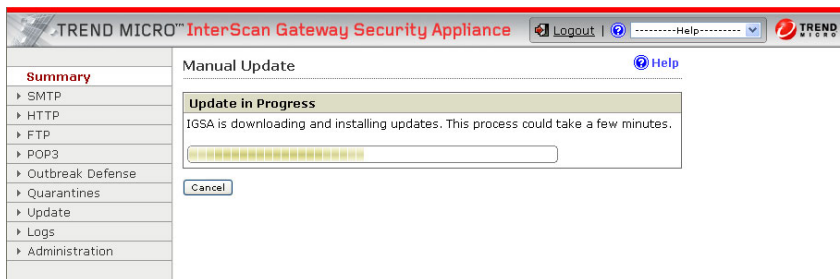


FIGURE 3-3. Update in Progress

When the **Update in Progress** indicator has finished, the **Manual Update > Select Components to Update** screen appears, with its update recommendations pre-selected.

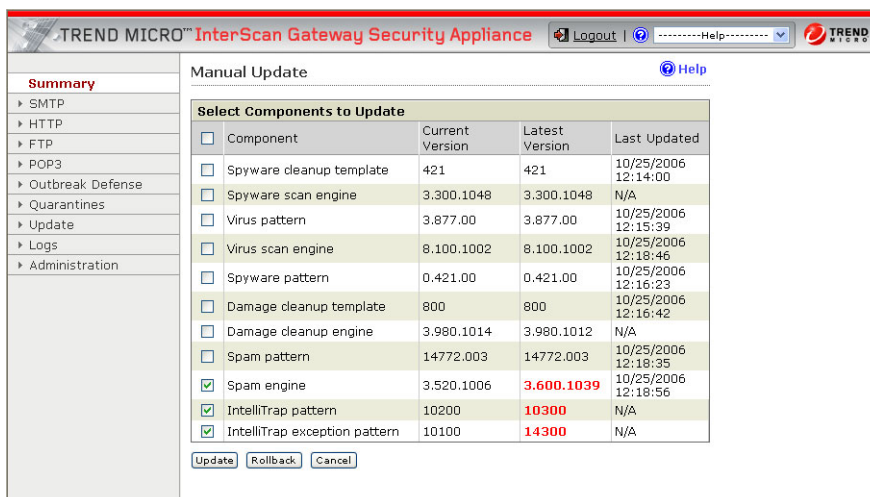


FIGURE 3-4. Manual Update > Select Components to Update

2. Click **Update** to update InterScan Gateway Security Appliance. The **Update in Progress** indicator reappears while InterScan Gateway Security Appliance is updated.
3. [Optional] Click **Rollback** to roll back InterScan Gateway Security Appliance to the last Update.

Note: Rollback allows an administrator to roll InterScan Gateway Security Appliance back to the last Update. Multiple rollbacks are not supported.

Antivirus

Reset All Counters			
Note: Antivirus, Anti-spyware, and IntelliTrap use the same scan engine. Total files scanned is the sum of all scans made by the scan engine.			
Antivirus		0 infected files detected today. ⓘ	
Action Summary	Today	Last 7 days	Last 30 days
Infected files cleaned	0	0	0
Infected files quarantined	0	0	0
Infected files deleted or blocked	0	0	0
Infected files removed	0	0	0
Infected files passed	0	0	0
Total files scanned	85	1407	4955
Anti-spyware		0 spyware/grayware detected today. ⓘ	
Action Summary	Today	Last 7 days	Last 30 days
Spyware/Grayware deleted or blocked	0	0	0
Spyware/Grayware quarantined	0	0	0
Spyware/Grayware removed	0	0	0
Spyware/Grayware passed	0	0	0
Total files scanned	85	1407	4955
IntelliTrap		0 infected files detected today. ⓘ	
Action Summary	Today	Last 7 days	Last 30 days
Infected files deleted or blocked	0	0	0
Infected files quarantined	0	0	0
Infected files removed	0	0	0
Infected files passed	0	0	0
Total files scanned	85	1407	4955

FIGURE 3-5. Summary Screen – Second Three Panels

Antivirus provides virus/malware detection (including IntelliTrap) statistics from SMTP/POP3/HTTP/FTP traffic, including:

- Number of infected files detected today
- Number of infected files cleaned
- Number of infected files quarantined
- Number of infected files deleted or blocked
- Number of infected files removed
- Number of infected files passed
- Total number of files scanned

Anti-Spyware

Anti-spyware provides spyware/grayware detection statistics from SMTP/POP3/HTTP/FTP traffic, including:

- Total number of files InterScan Gateway Security Appliance detected today that contained spyware/grayware
- Spyware/Grayware deleted or blocked
- Spyware/Grayware quarantined
- Spyware/Grayware removed
- Spyware/Grayware passed
- Total files scanned

IntelliTrap

IntelliTrap detects malicious code such as bots in compressed files. IntelliTrap provides detection statistics from SMTP/POP3 traffic, including:

- Infected files deleted or blocked
- Infected files quarantined
- Infected files removed
- Infected files passed
- Total files scanned

Anti-Spam: Content Scanning

Anti-spam: Content Scanning		0 spam messages detected today. ⓘ		
Action Summary	Today	Last 7 days	Last 30 days	
Spam messages deleted	0	0	0	
Spam messages quarantined	0	0	0	
Spam messages tagged	0	0	0	
Total messages received	0	0	0	
Anti-spam: Network Reputation Services		IP addresses filtered today. ⓘ		
Action Summary	Today	Last 7 days	Last 30 days	
IP addresses filtered	0	0	0	
Total IP addresses scanned	0	0	0	
Others ⓘ				
Detection Summary	Today	Last 7 days	Last 30 days	
Pharming incidents detected	0	0	0	
Phishing incidents detected	0	0	0	
Content filtered	0	0	0	
Files blocked	0	0	0	
URLs filtered	0	0	0	

FIGURE 3-6. Summary Screen – Last Three Panels

Anti-spam: Content Scanning provides spam detection statistics from SMTP/POP3 traffic, including:

- Total spam messages detected today
- Spam messages deleted
- Spam messages quarantined
- Spam messages tagged
- Total messages received

Anti-Spam: Network Reputation Services

Anti-spam: Network Reputation Services provides statistics from HTTP traffic, including

- Total number of IP addresses filtered today
- Total IP addresses filtered
- Total IP addresses scanned

Others

Others provides statistics for detected phishing mail, content filtering, and IntelliTrap for SMTP/POP3 traffic, and detected URL filtering for HTTP traffic, including:

- Number of pharming incident detected
- Number of phishing incidents detected
- Number of times that InterScan Gateway Security Appliance filtered content or detected information that met the filtering criteria
- Number of URLs that were filtered based on blocking criteria

Additional Screen Actions

- Click the up and down arrows to expand or collapse different sections of summary information.
- Click **Back** or the Summary link at the top of the screen to return to the Summary screen.
- Click **Reset All Counters** in the upper left corner of the six scanning panels to reset their counters

Navigating the Web Console

Click **SMTP > Scanning > Incoming** in the navigation menu to display the sample screen below. The **Target** tab appears.

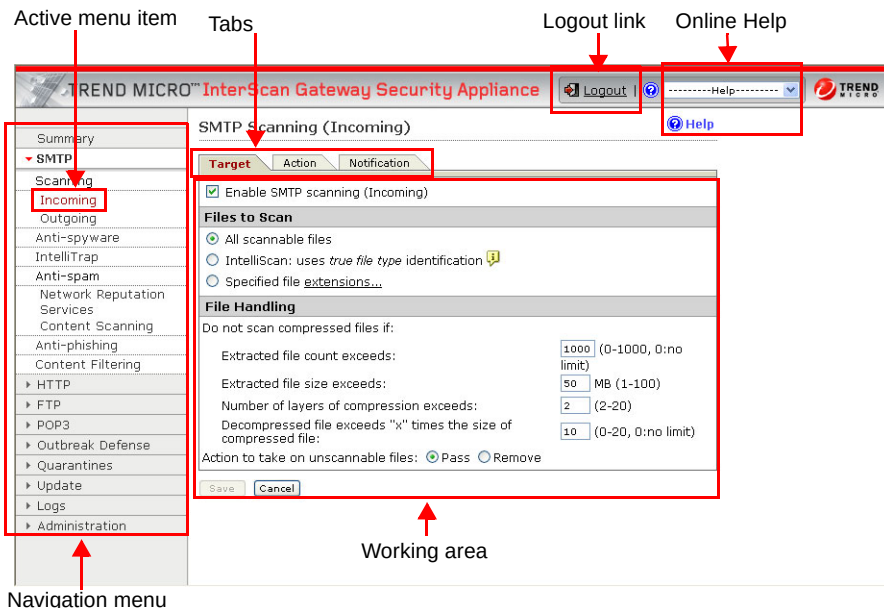


FIGURE 3-7. SMTP > Scanning (Incoming) > Target – Sample Screen

The Web console is designed for easy navigation, providing

- A navigation menu on the left with menu and submenu items that provide access to Settings screens. To access a menu item in the navigation menu, click the name of that item. When you position your cursor over a clickable item, the item turns red.
- A working area on the right with settings screens, often with Target, Action, and Notification tabs that you can click to access additional screens. Separate panels in the screens organize the settings according to functions.

- An online Help system with a drop-down menu, which provides online help organized according to topic. You can also get context-sensitive help at any time by clicking the ? Help icon for that menu item or settings screen.
- A Logout link, which you can click to manually log out of the InterScan Gateway Security Appliance Web console.

Note: Informational pop-ups in Web console screens, indicated by the  icon, provide context-sensitive information about key features of InterScan Gateway Security Appliance.

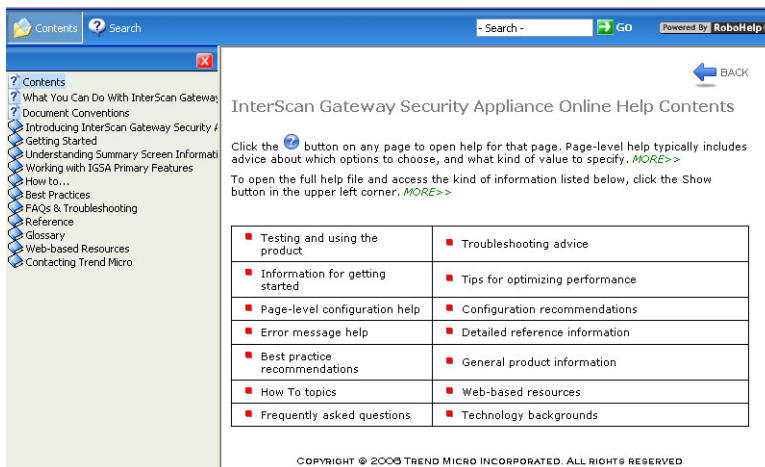
The Online Help System



FIGURE 3-8. Online Help Menu – Contents and Index

To use the online Help system:

1. Select Contents and Index from the Help drop-down menu. (Figure 3-8, “Online Help Menu – Contents and Index,” on page 13) The InterScan Gateway Security Appliance (the appliance) online Help system displays.

**FIGURE 3-9. Online Help System**

2. Click items in the Help system menu on the left for information about using the the appliance Web console to configure settings in the appliance device.

[Show](#)

Configuring Scanning for SMTP

SMTP > Incoming or Outgoing

Configuring virus scanning of SMTP traffic is a three-step process. You must first enable virus scanning and then select what to scan (**Target**). Next, set the action that IGSA should take when it detects a virus or other malware (**Action**). Finally, decide whom to notify when IGSA detects a virus or other malware (**Notification**).

 **NOTE: Infected item** - SMTP infected items are attachments and or the body of an email that contains a virus or other malware.

To configure virus scanning for SMTP traffic:

1. Select **Target**, *MORE>>*
2. Set **Action**, *MORE>>*
3. Select **Notification** recipient, *MORE>>*

See also:

- [About IntelliScan](#)
- [About true file type recognition](#)
- [Configuring Virus Scanning for HTTP](#)
- [Configuring Virus Scanning for FTP](#)
- [Configuring Virus Scanning for POP3](#)

COPYRIGHT © 2008 TREND MICRO INCORPORATED. ALL RIGHTS RESERVED

FIGURE 3-10. Online Help – Configuration Screen

3. Click **MORE>>** to display additional text on any page for more details about that item.

To configure virus scanning for SMTP traffic:

1. Select **Target**, *MORE>>*

SMTP Antivirus - Target:

1. From the left-side menu, click **SMTP > (Incoming or Outgoing)**.
 2. Click the **Target** tab.
 3. Select the **Enable SMTP Scanning (Incoming or Outgoing)** check box.
 4. Specify files to scan:
 - **All scannable files** - scans all files, except password-protected or encrypted files
 - **IntelliScan — True file type identification** - IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible for virus scanning. Scans files by an intelligent combination of true file type scanning and exact extension name filtering.
 - **Specified file extensions...** - manually specify the files to scan based on their extensions.
 5. Select files to exclude from scanning based on different criteria:
 - **Extracted file count exceeds**
 - **Extracted file size exceeds**
 - **Number of layers of compression exceeds**
 - **Extracted file size/compressed file size ratio exceeds**
 - Action to take on all unscannable files:
 - **Pass**
 - **Remove**
 6. Click **Save**.
2. Set **Action**, *MORE>>*
 3. Select **Notification** recipient, *MORE>>*

See also:

[SMTP Antivirus - Target](#)

FIGURE 3-11. Online Help – MORE> Screen

4. Back in the Web console, click the  **Help** icon in any Web console screen to open online context-sensitive Help for that screen. The appliance online Help system displays a Help page for that context.
5. Select other menu items in the online Help drop-down menu to obtain information from the Trend Micro Knowledge Base, to obtain Security Information (for example, current Security Advisories), to contact Sales and Support, or to obtain version, build, and copyright information.

SMTP Services

This chapter describes the SMTP Services in InterScan Gateway Security Appliance.

This chapter includes the following topics:

- *Enabling Scanning of SMTP Traffic* on page 4-3
- *Configuring SMTP Virus Scanning* on page 4-3
- *Configuring SMTP Anti-Spyware* on page 4-9
- *Configuring SMTP IntelliTrap* on page 4-13
- *Configuring SMTP Anti-Spam: Network Reputation Services* on page 4-16
- *Configuring SMTP Anti-Spam: Content Scanning* on page 4-19
- *Configuring SMTP Anti-Phishing* on page 4-22
- *Configuring SMTP Content Filtering* on page 4-25

SMTP Services

InterScan Gateway Security Appliance gives the administrator flexibility in configuring how the SMTP scanning service behaves. For example, you can specify the attachment types to scan, the individuals to notify when a virus is detected, and the action taken by InterScan Gateway Security Appliance—to clean, delete, remove, or quarantine—upon detection.

InterScan Gateway Security Appliance SMTP Services include the following features:

- Real-time scanning of incoming and outgoing SMTP email traffic
- Scanning for viruses/malware, spyware/grayware, bots, spam, inappropriate contents, links to phishing sites
- IntelliScan, which uses true file type identification when scanning (which protects against the "email security flaw")
- Automatic, customizable virus notifications
- Option to clean, delete, remove, pass, or quarantine infected files
- Size filtering
- Ability to insert customized notification stamps in messages

Trend Micro Anti-spam Engine (TMASE) is a built-in anti-spam engine that works even if Network Reputation Services is not enabled.

Enabling Scanning of SMTP Traffic

To allow InterScan Gateway Security Appliance to scan SMTP traffic, enable the feature.

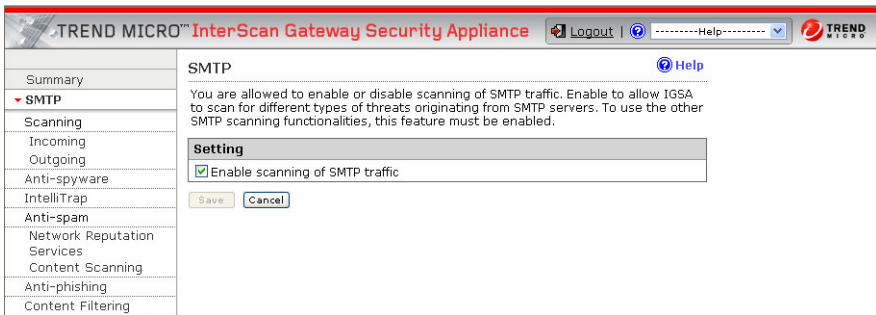


FIGURE 4-1. SMTP - Enable

To enable scanning of SMTP traffic:

1. On the left-side menu, click **SMTP**.
2. Select the **Enable SMTP Traffic** check box.
3. Click **Save**.

Configuring SMTP Virus Scanning

Configuring virus scanning of SMTP traffic is a three-step process. First, enable virus scanning and then select what to scan (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects a virus or other malware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a virus or other malware (Notification tab).

-
- Note:**
1. Infected item - SMTP infected items are attachments and/or the body of an email that contains a virus or other malware.
 2. The procedures for configuring virus scanning for Incoming or Outgoing SMTP traffic are the same, though the examples shown below are for SMTP Incoming mail.
-

SMTP Scanning - Target

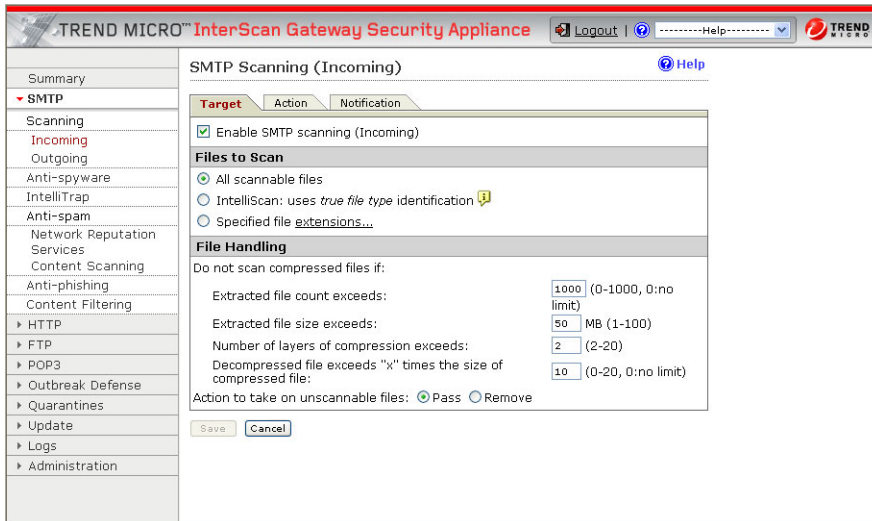


FIGURE 4-2. SMTP > Scanning (Incoming) - Target

To configure the virus scanning Target(s) for SMTP traffic:

1. From the left-side menu, click **SMTP > (Incoming or Outgoing)**. The **Target** tab appears
2. Select the **Enable SMTP Scanning (Incoming or Outgoing)** check box.
3. Specify the files to scan:
 - All scannable files - Scans all files, except password-protected or encrypted files
 - IntelliScan: uses *true file type* identification - IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible for virus scanning. Scans files by an intelligent combination of true file type scanning and exact extension name filtering.
 - Specified file extensions... Manually specify the files to scan based on their extensions by selecting this option and clicking the link. A **Scan Specified Files by Extension** window appears.

Scan Specified Files by Extension

These files will be scanned by extension, not by true file type. More comprehensive protection is offered by true file type identification using IntelliScan or the scan all file types option.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file.

""; ARJ; BAT; BIN; BOO; CAB; CHM; CLA; CLASS; COM; CSC; DLL; DOC; DOT; DRV; EML; EXE; GZ; HLP; HTA; HTM; HTML; HTT; INI; JAR; JPEG; JPG; JS; JSE; LNK; LZH; MDB; MPD; MPP; MPT; MSG; MSO; NWS; OCX; OFT; OVL; PDF; PHP; PIF; PL; POT; PPS; PPT; PRC; RAR; REG; RTF; SCR; SHS; SYS; TAR; VBE; VBS; VSD; VSS; VST; VXD; WML; WSF; XLA; XLS; XLT; XML; Z; ZIP; { *;

Additional Extensions

File extensions to scan:

Note: Not case sensitive. Separate multiple entries with a semicolon. Example: com; vbs

FIGURE 4-3. Scan Specified Files by Extension

- a. Type the file extensions you wish to scan for in the **File extensions to scan** field, separated by a semicolon.
 - b. Click **Add**.
 - c. Finish by clicking **OK**.
4. Back in the main Target screen, select files to exclude from scanning based on different criteria:
 - Extracted file count exceeds
 - Extracted file size exceeds
 - Number of layers of compression exceeds
 - Extracted file size/compressed file size ratio exceeds
 - Action to take on unscannable files:
 - Pass
 - Remove
 5. Click **Save**.

SMTP Scanning - Action

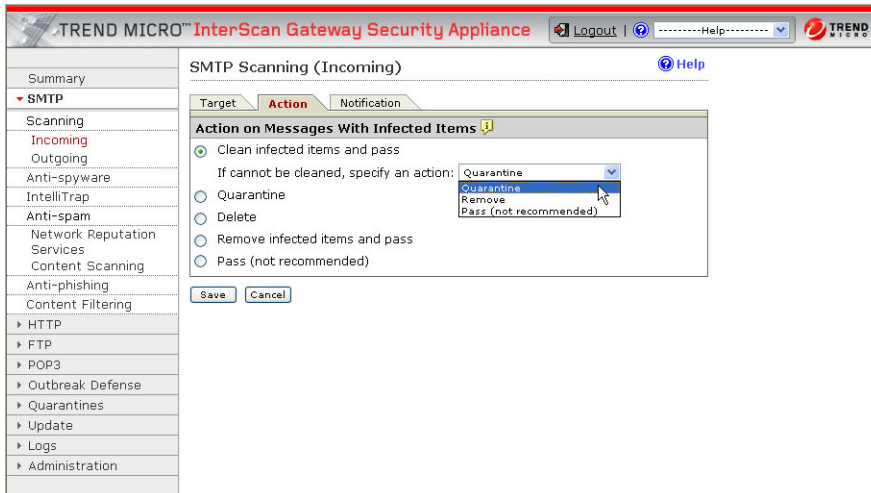


FIGURE 4-4. SMTP > Scanning (Incoming) - Action

To configure the virus scanning Action(s) for SMTP traffic:

1. From the left-side menu, click **SMTP > (Incoming or Outgoing)**.
2. Click the **Action** tab.
3. Choose an action for InterScan Gateway Security Appliance to take when it detects a message containing viruses or malware:
 - a. **Clean infected items and pass** - If InterScan Gateway Security Appliance detects a virus or malware in either the message body or the attachment, it will attempt to clean the item. From the drop-down menu, choose a secondary action for the appliance to take if the item cannot be cleaned:
 - **Quarantine** - InterScan Gateway Security Appliance sends the message and any attachments to the quarantine folder.
 - **Remove** - InterScan Gateway Security Appliance reacts differently depending on what items are infected. The table below describes the

different scenarios and how InterScan Gateway Security Appliance responds to them.

TABLE 4-1. “Remove” Scenarios

Scenarios	Response
Email with infected body	Email delivered with body removed
Email with infected attachment	Email delivered with attachment removed
Email with infected body and infected attachment	Email delivered with body and attachment removed

- **Pass** (not recommended) - InterScan Gateway Security Appliance delivers all items to the recipient.
- b.** Or choose among the following actions for the appliance to take on all messages with infected items:
- **Quarantine** - InterScan Gateway Security Appliance quarantines the message and any attachments.
 - **Delete** - InterScan Gateway Security Appliance deletes the message and any attachments.
 - **Remove** infected items and pass - InterScan Gateway Security Appliance delivers the message and removes only the infected items.
 - **Pass (not recommended)** - InterScan Gateway Security Appliance takes no action on infected items.

4. Click Save.

SMTP Scanning - Notification

TREND MICRO™ InterScan Gateway Security Appliance

Logout | Help

Summary

SMTP

Scanning

Incoming

Outgoing

Anti-spyware

IntelliTrap

Anti-spam

Network Reputation Services

Content Scanning

Anti-phishing

Content Filtering

HTTP

FTP

POP3

Outbreak Defense

Quarantines

Update

Logs

Administration

SMTP Scanning (Incoming)

Help

Target Action Notification

Email Notifications

When an infected incoming message is detected and any of the following items are enabled, the corresponding email notification(s) will be sent:

☒ Administrator

A threat was detected in a message.
 >Threat type: virus/malware
 >Threat name: %VIRUSNAME%
 >Sender: %SENDER%
 >Recipient: %RECIPIENT%

☐ Sender

Warning - the virus, %VIRUSNAME% was detected in a message sent to %RECIPIENT% from your computer. The message subject is %SUBJECT%. The message may not have been delivered.

☐ Recipient

Warning - the virus, %VIRUSNAME% was detected in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be deliverable.

Inline Notification Stamp

Select to insert the following text into all scanned messages before they are sent to recipients:

Virus Detected Notifications:

☒ Subject line: Risk Detected:

☐ Message

This message contains a possible security risk.

Virus Free Notifications:

☐ Message

This message has been scanned by the Trend Micro InterScan Security Module and found to be free of known security risks.

Save Cancel

FIGURE 4-5. SMTP > Scanning (Incoming) - Notification

To select the SMTP Scanning - Notification recipient(s):

1. From the left-side menu, click SMTP > (Incoming or Outgoing).
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when a message matches the scanning criteria, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient

4. Select all options that apply:

Virus Detected Notifications

- Subject line - when InterScan Gateway Security Appliance detects a virus or malware in an email, the recipient sees this message in the subject line of the email.
- Message - when InterScan Gateway Security Appliance detects a virus or malware in an email, the recipient sees this message in the body of the email.

Virus Free Notifications

- Message - after InterScan Gateway Security Appliance scans a message and determines that it is free of viruses or malware, it inserts a “virus free” notification into the body of the email.

5. Click **Save**.

Configuring SMTP Anti-Spyware

Configuring InterScan Gateway Security Appliance to scan SMTP traffic for spyware/grayware is a three-step process. First select what to scan for (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects an item that contains spyware/grayware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects spyware/grayware (Notification tab).

Note: Infected item - SMTP infected items are attachments and or the body of an email that contains spyware/grayware.

SMTP Anti-Spyware - Target

TREND MICRO™ InterScan Gateway Security Appliance Logout Help

SMTP Anti-spyware Help

Summary

- SMTP
- Scanning
 - Incoming
 - Outgoing
- Anti-spyware
- Anti-trap
- Anti-spam
 - Network Reputation Services
 - Content Scanning
- Anti-phishing
 - Content Filtering
- HTTP
- FTP
- POP3
- Outbreak Defense
 - Quarantines
- Update
- Logs
- Administration

Target Action Notification

☒ Enable SMTP Anti-spyware

Spyware/Grayware Exclusion List Search for spyware/grayware

Enter name of spyware/grayware: Add >> Exclusion Spyware/Grayware List
None

Example:
ADW_SLAGENT.A
ADW_BLAZE.B

Scan for Spyware/Grayware ☒ Select all

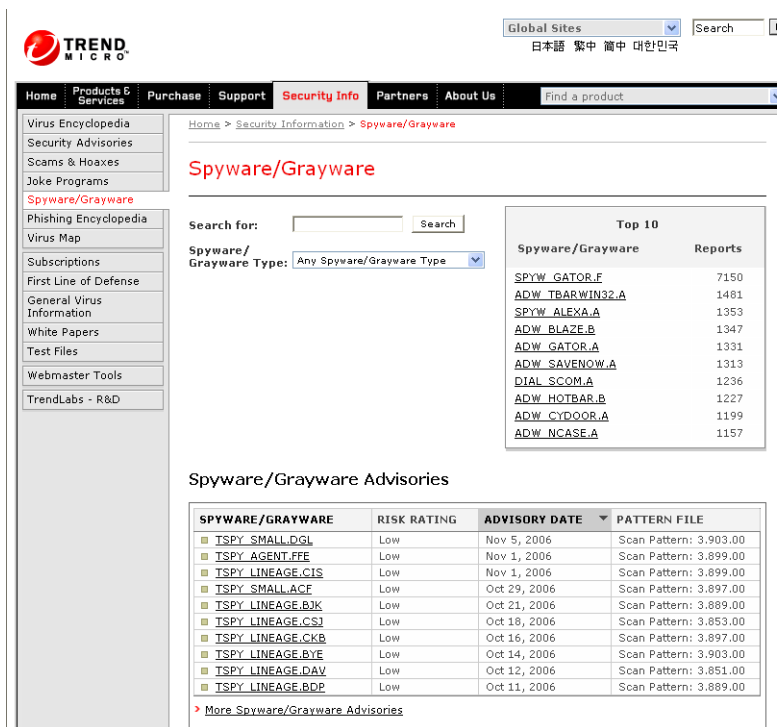
☒ Spyware	☒ Adware
☒ Dialers	☒ Joke Programs
☒ Hacking Tools	☒ Remote Access Tools
☒ Password Cracking Applications	☒ Others

Save Cancel

FIGURE 4-6. SMTP > Anti-spyware - Target

To configure the SMTP Anti-spyware - Target:

1. From the left-side menu, click **SMTP > Anti-spyware**. The **Target** tab appears.
2. Select the **Enable SMTP Anti-spyware** check box.
3. [Optional] Configure the **Spyware/Grayware Exclusion List**:
 - a. Click the **Search for spyware/grayware** link. InterScan Gateway Security Appliance opens a browser window directed to the Trend Micro Web site and displays the Trend Micro Spyware/Grayware online database.



TREND MICRO

Global Sites Search

日本語 繁体 簡中 대한민국

Home Products & Services Purchase Support **Security Info** Partners About Us Find a product

Virus Encyclopedia
Security Advisories
Scams & Hoaxes
Joke Programs
Spyware/Grayware
Phishing Encyclopedia
Virus Map
Subscriptions
First Line of Defense
General Virus Information
White Papers
Test Files
Webmaster Tools
TrendLabs - R&D

Home > Security Information > **Spyware/Grayware**

Spyware/Grayware

Search for: Search

Spyware / Grayware Type:

Top 10	
Spyware/Grayware	Reports
SPYW_GATOR.F	7150
ADW_TBARWIN32.A	1481
SPYW_ALEXA.A	1353
ADW_BLAZE.B	1347
ADW_GATOR.A	1331
ADW_SAVENOW.A	1313
DIAL_SCOM.A	1236
ADW_HOTBAR.B	1227
ADW_CYDOOR.A	1199
ADW_NCASE.A	1157

Spyware/Grayware Advisories

SPYWARE/GRAYWARE	RISK RATING	ADVISORY DATE	PATTERN FILE
☐ TSPY_SMALL.DGL	Low	Nov 5, 2006	Scan Pattern: 3.903.00
☐ TSPY_AGENT.FFE	Low	Nov 1, 2006	Scan Pattern: 3.899.00
☐ TSPY_LINEAGE.CIS	Low	Nov 1, 2006	Scan Pattern: 3.899.00
☐ TSPY_SMALL.ACF	Low	Oct 29, 2006	Scan Pattern: 3.897.00
☐ TSPY_LINEAGE.BJK	Low	Oct 21, 2006	Scan Pattern: 3.889.00
☐ TSPY_LINEAGE.CSJ	Low	Oct 18, 2006	Scan Pattern: 3.853.00
☐ TSPY_LINEAGE.CKB	Low	Oct 16, 2006	Scan Pattern: 3.897.00
☐ TSPY_LINEAGE.BYE	Low	Oct 14, 2006	Scan Pattern: 3.903.00
☐ TSPY_LINEAGE.DAV	Low	Oct 12, 2006	Scan Pattern: 3.851.00
☐ TSPY_LINEAGE.BDP	Low	Oct 11, 2006	Scan Pattern: 3.889.00

[More Spyware/Grayware Advisories](#)

FIGURE 4-7. Trend Micro Spyware/Grayware Online Database

- b. Search for the spyware you wish to exclude.

Note: To determine the formal name of the spyware, review your Spyware logs (**Logs > Query**, Log type = Anti-spyware/grayware).

- c. Returning to the **Target** screen, copy/paste or type the name of the spyware/grayware in the **Enter name of spyware/grayware** field. (The spyware/grayware exclusion list is case sensitive and has exact match capability.)

4. Click **Add**.

5. Select spyware/grayware types to scan for in the **Scan for Spyware/Grayware** section:
 Select all
 Or
 Select specific spyware/grayware types
6. Click **Save**.

SMTP Anti-Spyware - Action

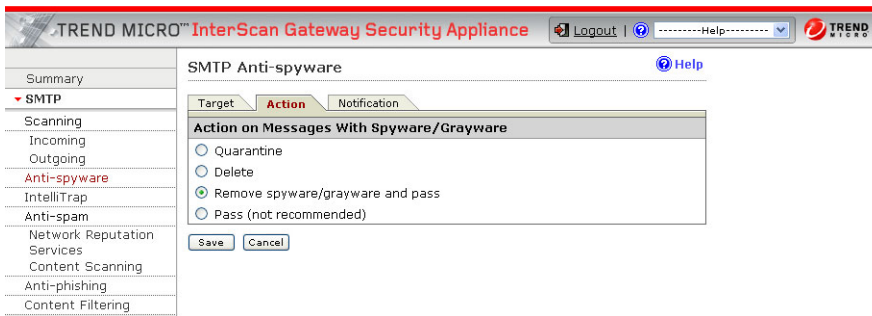


FIGURE 4-8. SMTP > Anti-spyware - Action

To configure SMTP Anti-spyware - Action:

1. From the left side menu, click **SMTP > Anti-spyware**.
2. Click the **Action** tab.
3. Choose an action for InterScan Gateway Security Appliance to take when it detects spyware:
 - **Quarantine** - InterScan Gateway Security Appliance sends the message and any attachments to the quarantine folder.
 - **Delete** - InterScan Gateway Security Appliance deletes the message and any attachments.
 - **Remove spyware/grayware and pass** - InterScan Gateway Security Appliance delivers the message and removes only the infected items.
 - **Pass (not recommended)** - InterScan Gateway Security Appliance takes no action on items that contain spyware/grayware.
4. Click **Save**.

SMTP Anti-Spyware - Notification

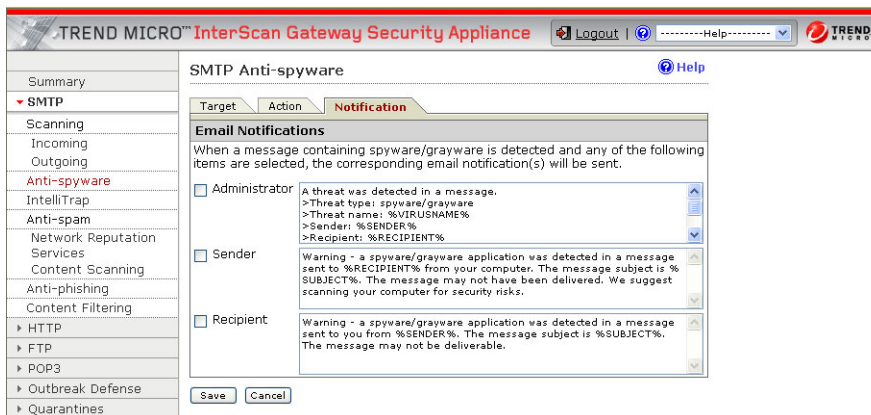


FIGURE 4-9. SMTP > Anti-spyware - Notification

To select SMTP Anti-spyware – Notification recipient(s):

1. From the left-side menu, click **SMTP > Anti-spyware**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when a message containing spyware/grayware is detected, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

Configuring SMTP IntelliTrap

Configuring IntelliTrap to scan SMTP traffic for bots is a three-step process. First, enable InterScan Gateway Security Appliance to scan for bots (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects a bot (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a bot (Notification tab).

SMTP IntelliTrap - Target

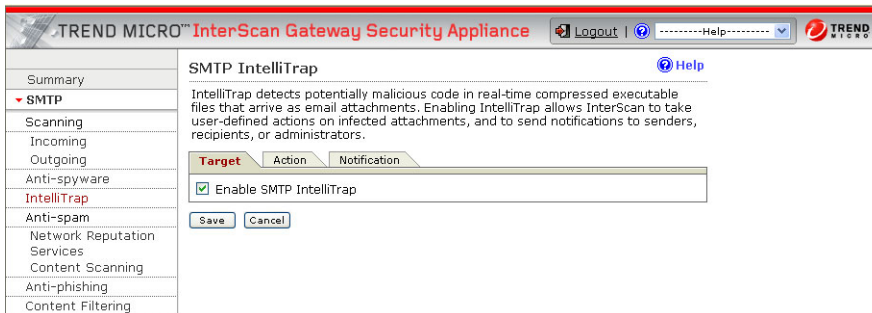


FIGURE 4-10. SMTP > IntelliTrap - Target

To configure IntelliTrap to scan SMTP traffic:

1. From the left-side menu, click **SMTP > IntelliTrap**. The **Target** tab appears
2. Select the **Enable SMTP IntelliTrap** check box.
3. Click **Save**.

SMTP IntelliTrap - Action



FIGURE 4-11. SMTP > IntelliTrap - Action

To configure SMTP IntelliTrap - Action:

1. From the left-side menu, click **SMTP > IntelliTrap**.
2. Click the **Action** tab.
3. Choose an action for InterScan Gateway Security Appliance to take if a bot is detected in an email attachment:
 - Quarantine - InterScan Gateway Security Appliance sends the message and attachment to the quarantine folder.
 - Delete - InterScan Gateway Security Appliance deletes the message and attachment.
 - Remove infected attachments and pass - InterScan Gateway Security Appliance delivers the message and removes the attachment.
 - Record detection and pass (not recommended) - InterScan Gateway Security Appliance records the detection and delivers the message and attachment.
4. Click **Save**.

SMTP IntelliTrap - Notification



FIGURE 4-12. SMTP > IntelliTrap - Notification

To select SMTP IntelliTrap – Notification recipient(s):

1. From the left-side menu, click **SMTP > IntelliTrap**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when IntelliTrap detects a potential threat (such as a bot), the corresponding email notifications(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

Configuring SMTP Anti-Spam: Network Reputation Services

Configuring InterScan Gateway Security Appliance to filter email originating from IP addresses that are known to distribute spam is a two-step process. First, enable InterScan Gateway Security Appliance to scan for spam (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects a message originating from an IP address that is known to distribute spam (Action tab).

SMTP Anti-Spam: Network Reputation Services - Target

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP (selected), Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation Services (selected), Content Scanning, Anti-phishing, Content Filtering, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled "SMTP Anti-spam (Network Reputation Services)" and includes a "Help" link. Below the title is a descriptive paragraph about the service. The "Target" tab is active, showing a configuration form with the following sections: "Enable SMTP Anti-spam (Network Reputation Services)" (checked), "Set Service Level" (with "Low setting" and "High setting" radio buttons, where "High setting" is selected), and "Approved IP Address(es)" (with a text input field containing "Example: 172.26.240.2" and a "Save" button). There is also an "Add >>" button and an "IP Address(es)" dropdown menu.

FIGURE 4-13. SMTP > Anti-Spam (Network Reputation Services) - Target

To configure SMTP Anti-spam (Network Reputation Services) - Target:

1. From the left-side menu, click **SMTP > Network Reputation Services**. The **Target** tab appears
2. Select the **Enable SMTP Anti-spam (Network Reputation Services)** check box.
3. Select a service level:
 Low setting
 Or
 High setting

Note: When clicked, the **Trend Micro RBL+ Service** and **Trend Micro Network Anti-Spam Service** links open a browser to the respective service on the Trend Micro Web site, where you can evaluate the service.

4. Configure Approved IP Address(es):
 - a. Enter one or more IP Addresses for InterScan Gateway Security Appliance to exclude from filtering.
 - b. Click **Add**.
5. Click **Save**.

SMTP Anti-Spam: Network Reputation Services - Action

TREND MICRO™ InterScan Gateway Security Appliance Logout | Help

SMTP Anti-spam (Network Reputation Services) Help

Summary

SMTP

Scanning

Incoming

Outgoing

Anti-spyware

IntelliTrap

Anti-spam

Network Reputation Services

Content Scanning

Anti-phishing

Content Filtering

HTTP

FTP

POP3

Outbreak Defense

Quarantines

Update

Logs

Administration

Low setting - InterScan Gateway Security Appliance queries the RBL+ Service for known sources of spam. Trend Micro recommends that messages from these sources be blocked with a 550 error code, "connection denied".

High setting - InterScan Gateway Security Appliance first queries the RBL+ Service and if the IP address is not a known source of spam, a second query is made to the QIL database of currently active spamming sources. If the messages are from a dynamic source Trend Micro recommends that these connections be blocked with a 450 error code, "server temporarily unavailable, please retry later".

NOTE: For testing purposes, you may want to Pass RBL+ and QIL matches and view your logs for service effectiveness.

Target **Action**

Action for RBL+

☒ Intelligent action - Denial of connection for RBL+ matches
User will receive SMTP error code: (range 400 - 599; default=550)

☐ Connection denied with no error message to user

☐ Pass (not recommended)

Action for QIL

☒ Intelligent action - Denial of connection for QIL matches
User will receive SMTP error code: (range 400 - 599; default=450)

☐ Connection denied with no error message to user

☐ Pass (not recommended)

FIGURE 4-14. SMTP > Anti-spam (Network Reputation Services) - Action

To configure SMTP Anti-spam (Network Reputation Services) - Action:

1. From the left-side menu, click **SMTP > Network Reputation Services**.
2. Click the **Action** tab.
3. Choose the action for InterScan Gateway Security Appliance to take when it detects a message originating from an IP address that is known to be a source of spam:

Action for Real-Time Blackhole List (RBL+) (Applies to both Low and High settings)

- Intelligent action - Permanent denial of connection for RBL+ matches. Error message sent to user
- Connection denied with no error message to user
- Pass (not recommended)

Action for QIL (applies to High settings)

- Intelligent action - Permanent denial of connection for QIL matches. Error message sent to user
- Connection denied with no error message to user
- Pass (not recommended)

4. Click **Save**.

Configuring SMTP Anti-Spam: Content Scanning

Configuring SMTP Anti-Spam Content Scanning to scan SMTP traffic for spam email is a two-step process. First, select a spam detection level and then configure the Approved Senders, Blocked Senders, and Keyword Exception lists (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects a spam email (Action tab).

SMTP Anti-Spam: Content Scanning - Target

TREND MICRO™ InterScan Gateway Security Appliance

Logout | Help

Summary

SMTP

Scanning

Incoming

Outgoing

Anti-spyware

IntelliTrap

Anti-spam

Network Reputation Services

Content Scanning

Anti-phishing

Content Filtering

HTTP

FTP

POP3

Outbreak Defense

Quarantines

Update

Logs

Administration

SMTP Anti-spam

Target

Action

☒ Enable SMTP Anti-spam

Filter Tuning

Spam detection level: Low

Keyword Exceptions

Messages containing identified keywords will not be considered Spam. Separate each entry by a semi-colon.

Approved Senders

Add approved sender email addresses or domain names (for example: abc_company.com.tw; abc@hotmail.com; or @abc_company.com). Separate each entry by a semi-colon.

Blocked Senders

Add blocked sender email addresses or domain names (for example: abc_company.com.tw; abc@hotmail.com; or @abc_company.com). Separate each entry by a semi-colon.

Save Cancel

FIGURE 4-15. SMTP > Anti-spam > Content Scanning - Target

To configure SMTP Anti-spam (Content Scanning) - Target:

1. From the left-side menu, click **SMTP > Content Scanning**. The **Target** tab appears.
2. Select the **Enable SMTP Anti-spam** check box to allow InterScan Gateway Security Appliance to scan email for spam.
3. Select a value from the **Spam detection level** drop-down menu. (Set a spam detection rate to screen out spam. The higher the detection level, the more messages are classified as spam.)
 - Low - This is the default setting. This is the most lenient level of spam detection. InterScan Gateway Security Appliance will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

- Medium - InterScan Gateway Security Appliance monitors at a high level of spam detection with a moderate chance of filtering false positives.
 - High - This is the most rigorous level of spam detection. InterScan Gateway Security Appliance monitors all email messages for suspicious files or text, but there is a greater chance of false positives. False positives are those email messages that InterScan Gateway Security Appliance filters as spam when they are actually legitimate email messages.
4. [Optional]: Keyword Exceptions
Messages containing identified keywords will not be considered spam (separate multiple entries with a semicolon).
 5. [Optional]: Approved Senders
Add approved senders' email addresses or domain names (separate multiple entries with a semicolon).
 6. [Optional]: Blocked Senders
Add blocked senders' email addresses or domain names (separate multiple entries with a semicolon).
 7. Click **Save**.

SMTP Anti-Spam: Content Scanning - Action

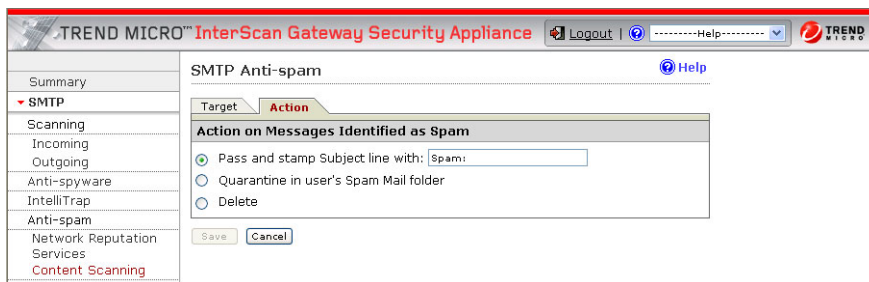


FIGURE 4-16. SMTP > Anti-spam > Content Scanning - Action

To configure SMTP Anti-spam (Content Scanning) - Action:

1. From the left-side menu, click **SMTP > Content Scanning**.
2. Click the **Action** tab.
3. Choose the action for InterScan Gateway Security Appliance to take when it detects spam:
 - **Pass and stamp Subject line with: Spam** - The appliance delivers the message to the recipient and stamps “spam” in the subject line.
 - **Quarantine in user's Spam Mail folder** - The appliance delivers spam to the end user's quarantine folder. Trend Micro End User Quarantine (EUQ) works in conjunction with ScanMail for Exchange to send spam to the end user's quarantine folder.

Note: Alternatively, you can download the End User Quarantine tool from the Trend Micro Update Center, InterScan Gateway Security Appliance page (www.trendmicro.com/download/product.asp?productid=73) in the Related Downloads section.

- **Delete** - InterScan Gateway Security Appliance deletes the message and any attachments.
4. Click **Save**.

Configuring SMTP Anti-Phishing

You can enable InterScan Gateway Security Appliance to scan SMTP email for links to known phishing sites (Target tab). Choose the action for InterScan Gateway Security Appliance to take when it encounters a phishing site (Action tab). When InterScan Gateway Security Appliance detects a phishing site, it sends a message to the recipients that you choose (Notification).

SMTP Anti-Phishing - Target

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a menu with the following items: Summary, SMTP (expanded), Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation Services, Content Scanning, Anti-phishing (highlighted), and Content Filtering. The main content area is titled "SMTP Anti-phishing" and has a "Help" link. Below the title are three tabs: "Target" (selected), "Action", and "Notification". Under the "Target" tab, there is a checkbox labeled "Enable SMTP Anti-phishing" which is checked. Below the checkbox are "Save" and "Cancel" buttons.

FIGURE 4-17. SMTP > Anti-phishing - Target

To configure SMTP Anti-phishing – Target to check for phishing sites:

1. From the left-side menu, click **SMTP > Anti-phishing**. The **Target** tab appears.
2. Select the Enable SMTP Anti-phishing check box.
3. Click **Save**.

SMTP Anti-Phishing - Action

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar is the same as in Figure 4-17, with "Anti-phishing" highlighted. The main content area is titled "SMTP Anti-phishing" and has a "Help" link. Below the title are three tabs: "Target", "Action" (selected), and "Notification". Under the "Action" tab, there is a section titled "Action on Messages With Phishing Sites". This section contains two radio buttons: "Pass and stamp Subject line with:" (selected) and "Delete". The "Pass and stamp Subject line with:" option has a text input field labeled "Phishing:". Below the radio buttons are "Save" and "Cancel" buttons.

FIGURE 4-18. SMTP > Anti-phishing - Action

To configure SMTP Anti-phishing - Action:

1. From the left-side menu, click **SMTP > Anti-phishing**.
2. Click the **Action** tab.
3. Choose the action for InterScan Gateway Security Appliance to take when it detects a known phishing site:
 Deliver and stamp Subject line with: Phishing - leave the default message or type a new message that appears in the subject line of the email if InterScan Gateway Security Appliance detects a known phishing site.
 Or
 Delete - InterScan Gateway Security Appliance deletes the message and any attachments.
4. Click **Save**.

SMTP Anti-Phishing - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP (expanded), Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation, Services, Content Scanning, Anti-phishing (highlighted in red), Content Filtering, HTTP, FTP, POP3, Outbreak Defense, and Quarantines. The main content area is titled "SMTP Anti-phishing" and has a "Help" link. It features three tabs: "Target", "Action", and "Notification" (which is selected). Under the "Notification" tab, there is a section titled "Email Notifications" with the text: "When a phishing message is detected and any of the following items are selected, the corresponding email notification(s) will be sent." Below this text are two checkboxes: "Administrator" and "Recipient". The "Administrator" checkbox is checked, and its corresponding notification text is displayed in a text area: "A threat was detected in a message. >Threat type: phishing >Sender: %SENDER% >Recipient: %RECIPIENT% >Subject: %SUBJECT%". The "Recipient" checkbox is unchecked, and its corresponding notification text is: "Warning - a phishing threat was detected in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be deliverable." Below the notification text areas is a section titled "Report Potential Phishing URL" with the text: "Submit a Potential Phishing URL to TrendLabs". At the bottom of the configuration area are "Save" and "Cancel" buttons.

FIGURE 4-19. SMTP > Anti-phishing - Notification

To select SMTP Anti-phishing – Notification recipient(s):

1. From the left-side menu, click **SMTP > Anti-phishing**.
2. Click the **Notification** tab.
3. Select one or more recipients from the Email Notifications section and InterScan Gateway Security Appliance will send notifications if it detects a known phishing site.
4. Click **Save**.

On this screen is an option to send suspected Phish URLs to TrendLabs for inspection. To send such a URL, click the **Submit a Suspected Phishing URL to TrendLabs** link.

Configuring SMTP Content Filtering

Configuring content filtering for SMTP traffic is a three-step process. First, enable scanning of SMTP traffic and then select what to filter for (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when one or more filters are triggered (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects any filter violations (Notification tab).

SMTP Content Filtering - Target

The screenshot displays the 'SMTP Content Filtering' configuration page in the Trend Micro InterScan Gateway Security Appliance M-Series Administrator's Guide. The page is divided into a left sidebar and a main content area.

Left Sidebar: Contains a navigation menu with the following items: Summary, SMTP (selected), Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation Services, Content Scanning, Anti-phishing, Content Filtering (highlighted), HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration.

Main Content Area: Titled 'SMTP Content Filtering', it features a 'Target' tab and a 'Notification' tab. The 'Target' tab is active, showing the following configuration options:

- Enable SMTP content filtering:** A checkbox that is checked.
- Filter by Message Size:** A section titled 'Filter messages based on their size (including message body and attachment):'. It includes a checkbox 'Filter if message size is larger than' which is checked, followed by a text input field containing '5' and a dropdown menu set to 'MB'.
- Filter by text in Message Header:** A section titled 'Messages can be filtered based on keywords in the message header. The message header includes the From, To, CC, and Subject fields.' It contains a text input field for 'Word to filter from the header:', an 'Add >>' button, and a 'Filter List' dropdown menu currently set to 'None'. There is also a 'Match case' checkbox which is unchecked.
- Filter by Text in Message Body:** A section titled 'Filter messages with certain words in the body area.' It contains a text input field for 'Word to filter from body area:', an 'Add >>' button, and a 'Filter List' dropdown menu currently set to 'None'. There is also a 'Match case' checkbox which is unchecked.
- Filter by Message Attachment Name:** A section titled 'Filter messages based on attachment file names. You can use asterisks (*) as wildcards to define file name filters.' It contains a text input field for 'Word to filter from attachments:', an 'Add >>' button, and a 'Filter List' dropdown menu currently set to 'None'.
- Filter by True File Type:** A section with two columns of checkboxes:
 - Audio/Video (.mp3, .wav, etc.)
 - Compressed (.zip, .tar, .jar, etc.)
 - Executable (.exe, .dll, etc.)
 - Images (.gif, .jpg, etc.)
 - Java (.class)
 - Microsoft Documents (.doc, .xls, etc.)

At the bottom of the main content area, there are 'Save' and 'Cancel' buttons.

FIGURE 4-20. SMTP > Content Filtering - Target

To configure SMTP Content Filtering – Target for SMTP traffic:

1. From the left-side menu, click **SMTP > Content Filtering**. The Target tab appears.
2. Select the **Enable SMTP content filtering** check box.
3. Set any of the following message filters that you need. (They are all optional):
 - **Filter by Message Size.** The Trend Micro recommended size is 5 MB. Larger file sizes can reduce the appliance throughput. If the message exceeds the size set in the filter, it will bypass scanning by the size filter and continue to the next filter.
 - **Filter by Text in Message Header.** Enter one or more words for InterScan Gateway Security Appliance to check for when scanning content in the subject line of email.
 - **Filter by Text in Message Body.** Enter one or more words for InterScan Gateway Security Appliance to check for when scanning content in the body of email.

For the above two filters, Header and Body, you can select **Match case**. InterScan Gateway Security Appliance will identify only items that match the case of the words added to the list.
 - **Filter by Message Attachment Name.** To filter attachments by file name, enter one or more words for InterScan Gateway Security Appliance to check for when scanning attachment names.
 - **Filter by True File Type** - To filter messages based on attachment type, select one or more of the items in the Attachment True File Type box.

Note: The True File Type filter does not support scanning of contents contained within compressed files. For example, if the administrator selects only Microsoft documents from the list, and you receive a message with a compressed (zip) file and the zip file contains a “.doc” or “.xls” file, the filter will not be triggered.

4. Click **Save**.

SMTP Content Filtering - Action

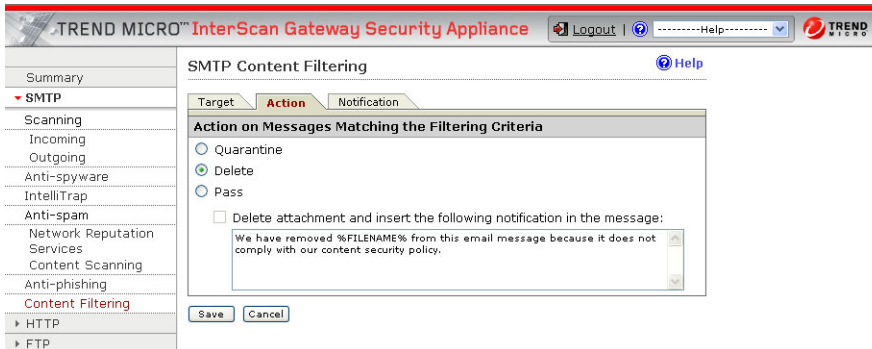


FIGURE 4-21. SMTP > Content Filtering - Action

To configure SMTP Content Filtering - Action:

1. From the left-side menu, click **SMTP > Content Filtering**.
2. Click the **Action** tab.
3. Choose the action for InterScan Gateway Security Appliance to take when email contains content or has an attachment that matches one of the content filtering rules:
 - **Quarantine** - InterScan Gateway Security Appliance sends the email and any attachments to the quarantine folder.
 - **Delete** - InterScan Gateway Security Appliance deletes the email and any attachments.
 - **Pass** - InterScan Gateway Security Appliance delivers the message and the attachment. You have the option of removing the attachment. If you select this option, InterScan Gateway Security Appliance delivers the message with a delete statement inside the body of the message.

Note: The **Delete attachment and insert the following notification in the message:** check box only works with attachments that have triggered the Attachment Name or True File Type filters.

4. Click **Save**.

SMTP Content Filtering - Notification

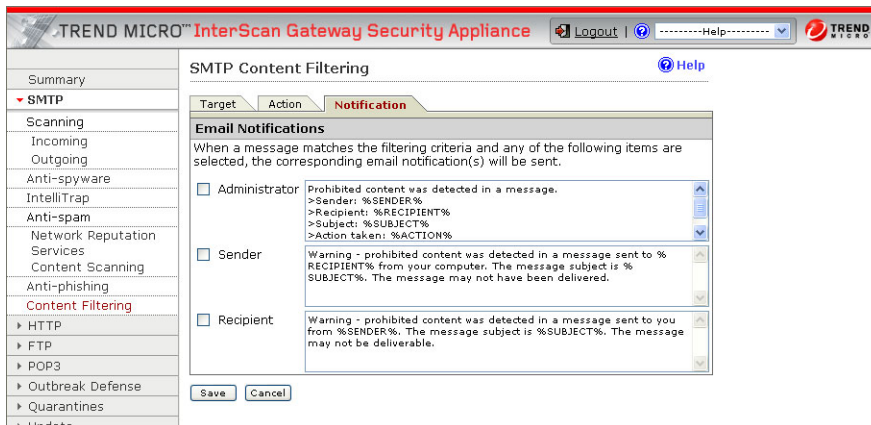


FIGURE 4-22. SMTP > Content Filtering - Notification

To select SMTP Content Filtering – Notification recipient(s):

1. From the left-side menu, click **SMTP > Content Filtering**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when a message matches the filtering criteria, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

HTTP Services

This chapter describes the HTTP Services in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Enabling Scanning of HTTP Traffic* on page 5-2
- *Configuring HTTP Virus Scanning* on page 5-2
- *Configuring HTTP Anti-Spyware* on page 5-8
- *Configuring HTTP Anti-Pharming* on page 5-12
- *Configuring HTTP Anti-Phishing* on page 5-14
- *Configuring HTTP URL Filtering* on page 5-17
- *Configuring HTTP File Blocking* on page 5-22

HTTP Services

The HTTP Services of InterScan Gateway Security Appliance scan incoming and outgoing HTTP traffic for viruses and spyware; protect users from phishing and pharming fraud using the anti-phishing and anti-pharming features; prohibit access, if enabled, to inappropriate Web sites, using URL filtering; and prevent potentially dangerous files or files containing prohibited or privileged information from being transferred, using the file blocking feature.

Enabling Scanning of HTTP Traffic

To allow InterScan Gateway Security Appliance to scan HTTP traffic, enable the feature.

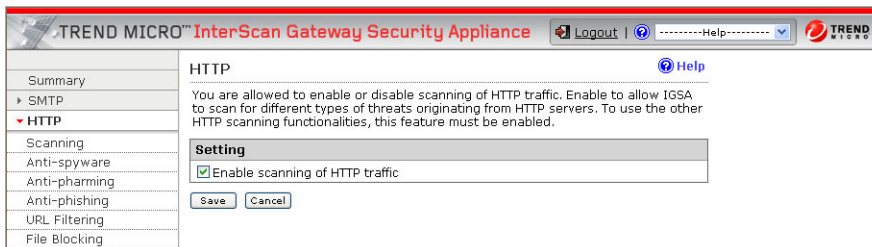


FIGURE 5-1. HTTP - Enable

To enable scanning of HTTP traffic:

1. On the left-side menu, click **HTTP**.
2. Select the **Enable scanning of HTTP traffic** check box.
3. Click **Save**.

Configuring HTTP Virus Scanning

Configuring virus scanning of HTTP traffic is a three-step process. First, select what to scan for (Target tab). Next, choose the action for InterScan Gateway Security Appliance (the appliance) to take when it detects a virus or other malware (Action tab). Finally, decide whom to notify when the appliance detects a virus or other malware (Notification tab).

Note: Infected item - HTTP infected items are virus or malware infected files downloaded using the HTTP protocol.

HTTP Scanning - Target

Configuring Virus Scanning for HTTP Traffic



FIGURE 5-2. HTTP > Scanning - Target

To configure virus scanning for HTTP traffic:

1. From the left-side menu, click **HTTP > Scanning**. The **Target** tab appears.
2. Select the **Enable HTTP Scanning** check box.

3. Specify files to scan:

- All scannable files - scans all files, except password-protected or encrypted files
- IntelliScan — True file type identification - IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus scanning. Scans files by an intelligent combination of true file type scanning and exact extension name filtering.
- Specified file extensions... Manually specify the files to scan based on their extensions by selecting this option and clicking the link. A **Scan Specified Files by Extension** window appears.

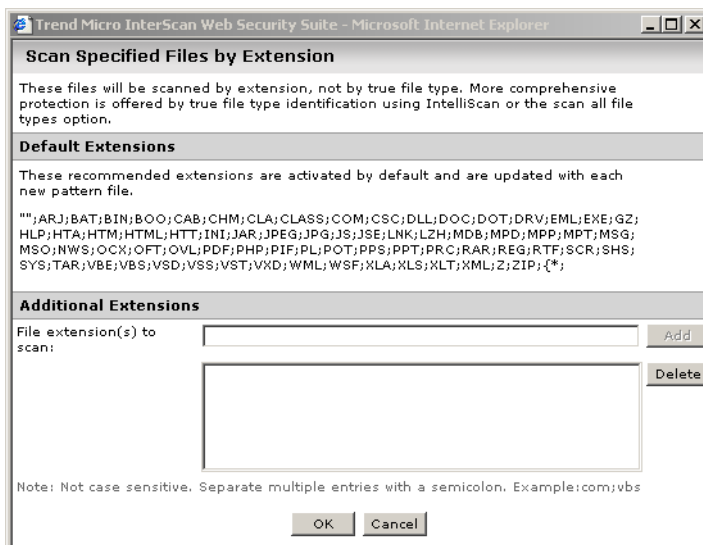


FIGURE 5-3. Scan Specified Files by Extension

- Type the file extensions you wish to scan for in the **File extensions to scan** field, separated by a semicolon.
- Click **Add**.
- Click **OK**.

4. Back in the main **Target** screen, select files to exclude from scanning based on different criteria:
 - Extracted file count exceeds
 - Extracted file size exceeds
 - Number of layers of compression exceeds
 - Extracted file size/compressed file size ratio exceeds
 - Action to take on unscannable files
 - Pass
 - Block
5. Specify a maximum size of file to be scanned.
 - **Do not scan files larger than** - set size in MB. Default is 50 MB
 - **Enable deferred scan** - InterScan Gateway Security Appliance starts sending parts of a large file to clients before the scan begins, so the connection between the client and the appliance will not time out. If the scan detects a virus, the appliance halts the data transfer for that file. (See [About Deferred Scan for Large File Handling](#) on page 5-5 for more information about this option.)
6. Click **Save**.

About Deferred Scan for Large File Handling

Enable deferred scan if your network connection to the appliance is of limited bandwidth and you have experienced delays in the loading of Web pages because of scanning time.

When deferred scan is disabled, end users have to wait until the entirety of each file is both scanned before the appliance sends the file to the client and the browser loads it. This option can result in a noticeable delay before the page loads.

With deferred scan enabled, the appliance increases browser response time, however there is a (relatively low) probability that data in the unscanned part of a file may contain malware, which would reach the client.

Use the **Start sending parts of the file to the client after ____ seconds** field to set a threshold to trigger deferred scanning of a file. This value depends on the speed of your network.

Tip: Trend Micro recommends trying different settings for the **Start sending parts of the file to the client after ____ seconds** field if you enable deferred scan. By fine-tuning this function with the above field, you can arrive at the best setting for your network.

HTTP Scanning - Action

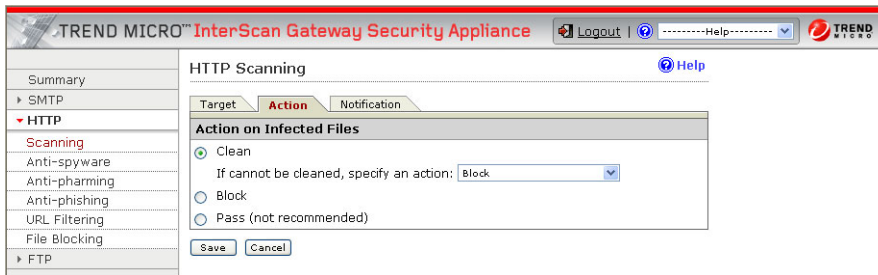


FIGURE 5-4. HTTP > Scanning - Action

To configure HTTP Antivirus - Action:

1. From the left-side menu, click **HTTP > Scanning**.
2. Click the **Action** tab.
3. Choose an action for InterScan Gateway Security Appliance to take when it detects a file containing viruses or malware:
 - **Clean** - if the appliance detects a virus or malware in a file, it first attempts to clean the item. If the item cannot be cleaned, the appliance takes one of the following actions, based on your selection from the drop-down menu:
 - **Block** – The appliance deletes all items
 - **Pass (not recommended)** - The appliance allows all items to be downloaded

- **Block** - When the appliance detects malware in HTTP traffic, it will redirect the browser to a blocking page containing a message that you can customize. (See *To select HTTP Antivirus – Notification recipient(s)*: on page 5-7 for the location and default content of this field.)
- **Pass (not recommended)** - InterScan Gateway Security Appliance takes no action on infected items.

4. Click **Save**.

HTTP Scanning - Notification

The screenshot shows the web interface of the Trend Micro InterScan Gateway Security Appliance. The left sidebar contains a navigation menu with options: Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-phishing, Anti-phishing, URL Filtering, File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'HTTP Scanning' and has a 'Help' link. It features three tabs: 'Target', 'Action', and 'Notification' (selected). Under the 'Notification' tab, there are two sections: 'User Notification' and 'Administrator Notification'. The 'User Notification' section contains a text area with the default message: 'Trend Micro InterScan Gateway Security Appliance has determined that the file you are attempting to transfer is infected. The appliance has taken action on the file.' The 'Administrator Notification' section has a checkbox labeled 'Administrator' which is currently unchecked. Below the checkbox is a text area showing a sample email notification: 'A threat was detected in HTTP traffic. >Threat type: virus/malware >Client IP address: %IPAddress% >Requested URL: %URL% >Date requested: %DATE%'. At the bottom of the page are 'Save' and 'Cancel' buttons.

FIGURE 5-5. HTTP Scanning - Notification

To select HTTP Antivirus – Notification recipient(s):

1. From the left-side menu, click **HTTP > Scanning**.
2. Click the **Notification** tab.
3. For **User Notification**, accept the default text or customize it for your needs. When InterScan Gateway Security Appliance detects malware in HTTP traffic, it will redirect the browser to a blocking page containing this text.
4. Select the **Administrator** check box to enable InterScan Gateway Security Appliance to send a notification to the administrator if it detects a virus or malware.
5. Click **Save**.

Configuring HTTP Anti-Spyware

Configuring InterScan Gateway Security Appliance to scan HTTP traffic for spyware/grayware is a three-step process. First, select what to scan for (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects an item that contains spyware/grayware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects an item containing spyware/grayware (Notification tab).

Note: Infected item - HTTP infected items are files that are spyware/grayware or files that contain spyware/grayware and that are downloaded using the HTTP protocol.

HTTP Anti-Spyware - Target

The screenshot displays the 'HTTP Anti-spyware' configuration page in the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar shows a navigation menu with 'HTTP' selected under 'Scanning'. The main content area has three tabs: 'Target', 'Action', and 'Notification', with 'Target' being the active tab.

Target Tab Configuration:

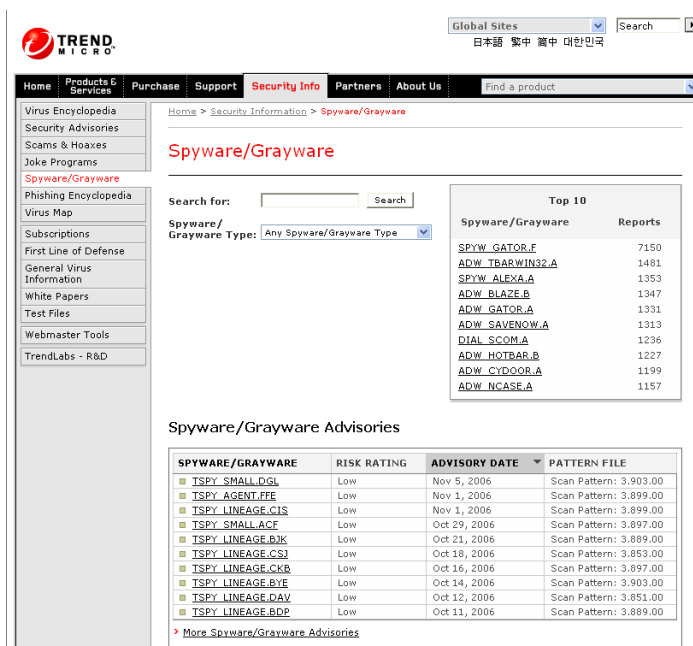
- ☒ Enable HTTP Anti-spyware
- Spyware/Grayware Exclusion List**
 - Search for spyware/grayware
 - Enter name of spyware/grayware:
 - Exclusion Spyware/Grayware List:
 - Example: ADW_SLAGENT.A, ADW_BLAZE.B
- Scan for Spyware/Grayware**
 - ☒ Select all
 - ☒ Spyware
 - ☒ Dialers
 - ☒ Hacking Tools
 - ☒ Password Cracking Applications
 - ☒ Adware
 - ☒ Joke Programs
 - ☒ Remote Access Tools
 - ☒ Others

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

FIGURE 5-6. HTTP > Anti-spyware - Target

To configure HTTP Anti-spyware – Target to scan HTTP traffic:

1. From the left-side menu, click **HTTP > Anti-spyware**. The **Target** tab appears.
2. Select the **Enable HTTP Anti-spyware** check box.
3. [Optional] Configure the **Spyware/Grayware Exclusion List**:
 - Click the **Search for spyware/grayware** link. InterScan Gateway Security Appliance opens a browser window on the Trend Micro Web site and displays the Trend Micro Spyware/Grayware online database.



The screenshot shows the Trend Micro Spyware/Grayware Online Database. The page has a navigation menu on the left with links like Virus Encyclopedia, Security Advisories, Scams & Hoaxes, Joke Programs, and Spyware/Grayware. The main content area is titled 'Spyware/Grayware' and includes a search bar, a dropdown for 'Spyware/Grayware Type', and a 'Top 10' list of spyware/grayware items. Below this is a table of 'Spyware/Grayware Advisories' with columns for Spyware/Grayware, Risk Rating, Advisory Date, and Pattern File.

SPYWARE/GRAYWARE	RISK RATING	ADVISORY DATE	PATTERN FILE
TSFY_SMALL.DGL	Low	Nov 5, 2006	Scan Pattern: 3.903.00
TSFY_AGENT.FFE	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSFY_LINEAGE.CIS	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSFY_SMALL.ACF	Low	Oct 29, 2006	Scan Pattern: 3.897.00
TSFY_LINEAGE.BJK	Low	Oct 21, 2006	Scan Pattern: 3.889.00
TSFY_LINEAGE.CSJ	Low	Oct 18, 2006	Scan Pattern: 3.853.00
TSFY_LINEAGE.CKB	Low	Oct 16, 2006	Scan Pattern: 3.897.00
TSFY_LINEAGE.BYE	Low	Oct 14, 2006	Scan Pattern: 3.903.00
TSFY_LINEAGE.DAV	Low	Oct 12, 2006	Scan Pattern: 3.851.00
TSFY_LINEAGE.BDP	Low	Oct 11, 2006	Scan Pattern: 3.889.00

FIGURE 5-7. Trend Micro Spyware/ Grayware Online Database

- Search for the spyware/grayware you wish to exclude.
 - Returning to the **Target** screen, copy/paste or type the name of the spyware/grayware in the **Enter name of spyware/grayware** field. (The spyware/grayware exclusion list is case sensitive and has exact match capability.)
4. Click **Add**.

5. Select spyware/grayware types to scan for in the **Scan for Spyware/Grayware** section:
 - Select allOr
 - Select specific spyware/grayware types
6. Click **Save**.

HTTP Anti-Spyware - Action

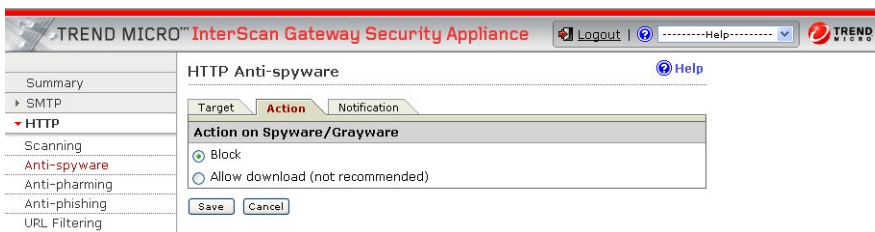


FIGURE 5-8. HTTP > Anti-spyware - Action

To configure HTTP Anti-spyware - Action:

1. From the left-side menu, click **HTTP > Anti-spyware**.
2. Click the **Action** tab.
3. Chose the action for InterScan Gateway Security Appliance to take when it detects spyware:
 - Block - InterScan Gateway Security Appliance deletes the file(s) and notifies recipients with an in-line user notification. InterScan Gateway Security Appliance will send a notification, if enabled, to the administrator.Or
 - Allow download (not recommended) - InterScan Gateway Security Appliance takes no action on items that contain spyware/grayware.
4. Click **Save**.

HTTP Anti-Spyware - Notification



FIGURE 5-9. HTTP > Anti-spyware - Notification

To select HTTP Anti-spyware – Notification recipient(s):

1. From the left-side menu, click **HTTP > Anti-spyware**.
2. Click the **Notification** tab.
3. Review the recipient's notification message.
4. Select the **Administrator** check box to enable the appliance to send a notification to the administrator when it detects spyware.
5. Click **Save**.

Configuring HTTP Anti-Pharming

Configuring HTTP for anti-pharming is a three-step process. First, enable InterScan Gateway Security Appliance to scan Web pages for links to known pharming sites (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it encounters a pharming site (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a known pharming site (Notification tab).

HTTP Anti-Pharming - Target

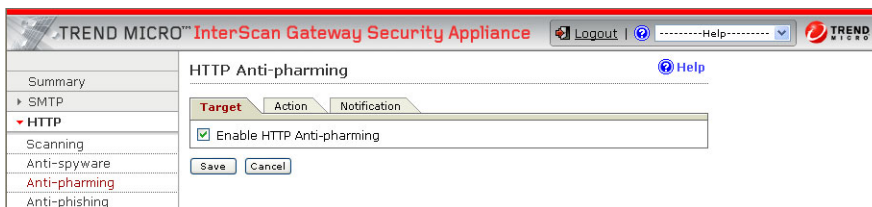


FIGURE 5-10. HTTP > Anti-pharming - Target

To configure HTTP Anti-pharming – Target to check for pharming sites:

1. From the left-side menu, click **HTTP > Anti-pharming**. The **Target** tab appears.
2. Select **Enable HTTP Anti-pharming**.
3. Click **Save**.

HTTP Anti-Pharming - Action

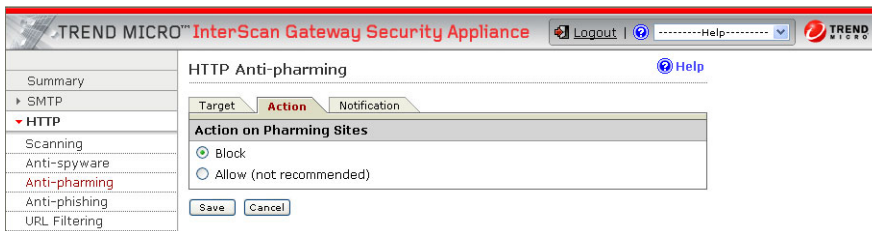


FIGURE 5-11. HTTP > Anti-pharming - Action

To configure HTTP Anti-pharming - Action:

1. From the left-side menu, click **HTTP > Anti-pharming**.
2. Click the **Action** tab.
3. Choose the action for InterScan Gateway Security Appliance to take when it detects a known pharming site.
 - **Block** - InterScan Gateway Security Appliance blocks access to the requested site.

Or

 - **Allow** (not recommended) - InterScan Gateway Security Appliance allows access to the requested site.
4. Click **Save**.

HTTP Anti-Pharming - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left-hand navigation menu is expanded to show the 'HTTP' section, with 'Anti-pharming' selected. The main content area is titled 'HTTP Anti-pharming' and has three tabs: 'Target', 'Action', and 'Notification'. The 'Notification' tab is active, displaying two sections: 'User Notification' and 'Administrator Notification'. The 'User Notification' section contains a text box with a warning message about phishing sites. The 'Administrator Notification' section includes a checkbox for 'Administrator' and a text box with a detailed threat notification template. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

FIGURE 5-12. HTTP > Anti-pharming - Notification

To configure HTTP Anti-pharming - Notification:

1. From the left-side menu, click **HTTP > Anti-pharming**.
2. Click the **Notification** tab.
3. Review the recipient notification.

4. Select the **Administrator** check box to enable the appliance to send a notification to the administrator if it detects a link to a known pharming site.
5. Click **Save**.

Configuring HTTP Anti-Phishing

Configuring InterScan Gateway Security Appliance to scan HTTP traffic for phishing sites is a three-step process. First, enable HTTP Anti-phishing (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it encounters a phishing site (Action tab). Finally, when InterScan Gateway Security Appliance detects a phishing site, it will send a message, if enabled, to the administrator (Notification tab).

HTTP Anti-Phishing - Target

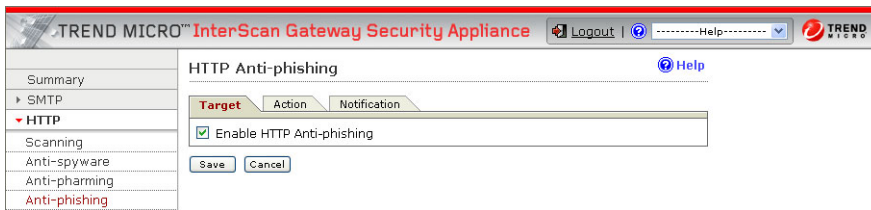


FIGURE 5-13. HTTP > Anti-phishing - Target

To configure HTTP Anti-phishing – Target to check for phishing sites:

1. From the left-side menu, click **HTTP > Anti-phishing**. The **Target** tab appears.
2. Select the **Enable HTTP Anti-phishing** check box to enable scanning of HTTP traffic for known phishing sites.
3. Click **Save**.

HTTP Anti-Phishing - Action

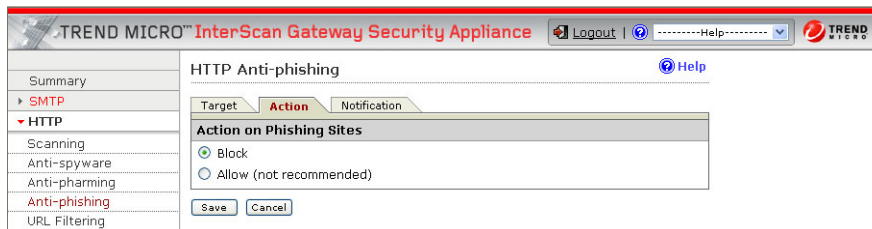


FIGURE 5-14. HTTP > Anti-phishing - Action

To configure HTTP Anti-phishing - Action:

1. From the left-side menu, click **HTTP > Anti-phishing**.
2. Click the **Action** tab.
3. Choose one of the following actions for InterScan Gateway Security Appliance to take when it detects a known phishing site.
 - **Block** - InterScan Gateway Security Appliance blocks access to the requested Web site.

Or

 - **Allow (not recommended)** - InterScan Gateway Security Appliance allows access to requested Web site.
4. Click **Save**.

HTTP Anti-Phishing - Notification

The screenshot displays the 'HTTP Anti-phishing' configuration page within the Trend Micro InterScan Gateway Security Appliance M-Series Administrator's Guide. The page is divided into a left-hand navigation menu and a main content area. The navigation menu includes options like Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-phishing (highlighted), URL Filtering, File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'HTTP Anti-phishing' and features a 'Notification' tab. Under this tab, there are three sections: 'User Notification' (displaying a message to the user's browser), 'Administrator Notification' (with a checkbox for 'Administrator' and a text area for the notification message), and 'Report Potential Phishing URL' (with a link to 'Submit a Potential Phishing URL to TrendLabs'). At the bottom of the main content area are 'Save' and 'Cancel' buttons.

FIGURE 5-15. HTTP > Anti-phishing - Notification

To configure HTTP Anti-phishing - Notification:

1. From the left-side menu, click **HTTP > Anti-phishing**.
2. Click the **Notification** tab.
3. Review the recipient notification.
4. Select the **Administrator** check box to enable the appliance to send a notification to the Administrator if it detects a link to a known phishing site.
5. Click **Save**.

On this screen is an option to send suspected Phish URLs to TrendLabs for inspection. To send such a URL, click the **Submit a Suspected Phishing URL to TrendLabs** link.

Configuring HTTP URL Filtering

InterScan Gateway Security Appliance uses administrator-defined rules to determine if a requested site is prohibited (URL Filtering Rules tab). InterScan Gateway Security Appliance performs URL filtering according to the administrator-set schedule (Settings) tab. If InterScan Gateway Security Appliance blocks access to a prohibited Web site, it sends a notification, if enabled, to the specified recipients (Notifications tab).

HTTP URL Filtering - Rules

The screenshot shows the 'HTTP URL Filtering' configuration page. The left sidebar contains a menu with options like Summary, SMTP, HTTP, Scanning, Anti-spyware, Anti-phishing, URL Filtering (selected), File blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area has three tabs: 'URL Filtering Rules' (active), 'Settings', and 'Notification'. Under the 'URL Filtering Rules' tab, there is a section 'Filter the Selected Categories' with a table of URL categories and checkboxes for filtering during work and leisure time. Below this are sections for 'Blocked URL List' and 'Approved URL List', each with a text input field and a list of URLs.

URL Category	Filter During Work Time	Filter During Leisure Time
All	☐	☐
Adult/Mature Content	☐	☐
Sex	☐	☐
Alcohol/Tobacco	☐	☐
Illegal Drugs	☐	☐
Gambling	☐	☐
Crime	☐	☐
Violence/Hate/Racism	☐	☐
Hacking/Proxy Avoidance	☐	☐
Cult/Ocult	☐	☐
Weapons/Military	☐	☐
Games	☐	☐
Blogs/Web Communications	☐	☐
Personals/Dating	☐	☐
Chat/Instant Messaging	☐	☐
Email	☐	☐
Newsgroups	☐	☐
Shopping/Auction	☐	☐
Software Downloads	☐	☐
Streaming Media/MP3	☐	☐
Job Search	☐	☐
Spyware	☐	☐
Adware/Doke Programs/Cookies	☐	☐
Personal Network Storage/File Download Servers	☐	☐
Photo Searches	☐	☐
Social Networking	☐	☐
Peer-to-Peer	☐	☐

Blocked URL List

Enter Blocked URL: Blocked URLs Type

Example: 'xxx.com' matches 'xxx.com' and all of its subdomains

Approved URL List

Enter Approved URL: Approved URLs Type

Example: 'xxx.com' matches 'xxx.com' and all of its subdomains

FIGURE 5-16. HTTP > URL Filtering – URL Filtering Rules

To configure HTTP – URL Filtering Rules:

1. From the left-side menu, click **HTTP > URL Filtering**. The **Filtering Rules** tab appears.
2. Select the **Enable URL Filtering** check box.
3. Select filtering based on pre-defined categories and times.
 - Filter During Work Time – Check **All** or specific categories
 - Filter During Leisure Time – Check **All** or specific categories
4. Configure the **Blocked URL List**:
 - Type one or more URLs in the **Enter Blocked URL** field.
 - Select a type from the drop-down menu.
 - Web site
 - URL keyword
 - String
 - Click **Add**.
5. Configure the **Approved URL List**:
 - Type one or more URLs in the **Enter Approved URL** field.
 - Select a type from the drop-down menu.
 - Web site
 - URL keyword
 - String
 - Click **Add**.
6. Click **Save**.

HTTP URL Filtering - Settings

TREND MICRO™ InterScan Gateway Security Appliance

Logout | Help

Summary

SMTP

HTTP

Scanning

Anti-spyware

Anti-pharming

Anti-phishing

URL Filtering

File Blocking

FTP

POP3

Outbreak Defense

Quarantines

Update

Logs

Administration

HTTP URL Filtering

Help

URL Filtering Rules Settings Notification

Work Time Settings

Work Days:

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Work Time

☒ All day (24 hours)

☐ Specify work hours

Note: Time not designated as work time will be considered leisure time.

☐ Morning

From: 9:00 AM

To: 12:00 PM

☐ Afternoon

From: 1:30 PM

To: 6:00 PM

Connection Settings

☐ Allow URL Filtering to use the appliance Proxy Settings

Note: Do not select this option if your proxy server is located within the protected network.

[View appliance Proxy Settings...](#)

Save Cancel

FIGURE 5-17. HTTP > URL Filtering - Settings

To configure HTTP URL Filtering - Settings:

1. From the left-side menu, click **HTTP > URL Filtering**.
2. Click the **Settings** tab.
3. Configure **Work Time Settings**:
 - Work Days - select all days that apply.
 - Work Time - select **All day (24 hours)** or **Specify work hours**.
4. Specify Connection Settings:
 - Check **Allow URL filtering to use the appliance Proxy Settings**
 - [Optional] - View appliance proxy settings... - click this link to view the proxy settings screen.

The screenshot displays the web interface of the Trend Micro InterScan Gateway Security Appliance. The top navigation bar includes the product name, a 'Logout' button, a 'Help' dropdown menu, and the Trend Micro logo. On the left, a sidebar menu lists various configuration categories: Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-phishing, URL Filtering (highlighted in red), File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'Proxy Settings' and features a 'Help' icon. Within this section, there is a sub-header 'Proxy Settings' followed by a checkbox labeled 'Use a proxy server for pattern, engine, and license updates', which is checked. Below this, the 'Proxy protocol' is set to 'HTTP' (selected with a radio button), with options for 'SOCKS4' and 'SOCKS5'. The 'Server name or IP address' and 'Port' fields are empty text boxes. The 'Proxy server authentication' section includes 'User ID' and 'Password' text boxes, and a 'Test Connection' button. At the bottom of the settings panel are 'Save' and 'Cancel' buttons.

FIGURE 5-18. HTTP > URL Filtering – Proxy Settings

- a. Check **Use a proxy server for pattern, engine, and license updates**
 - b. Select a proxy protocol
 - c. Type in your server name or IP address
 - d. Designate the port
 - e. Type in your User ID
 - f. Type in your Password
5. Click **Save**.

HTTP URL Filtering - Notification

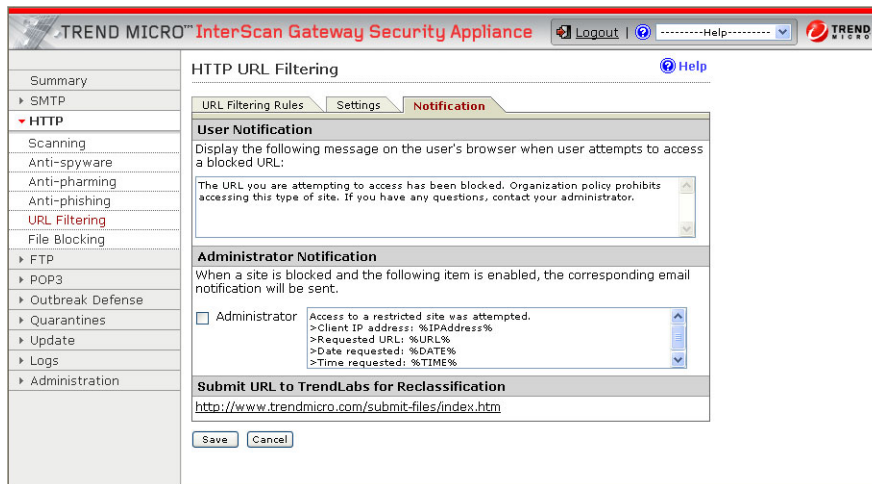


FIGURE 5-19. HTTP > URL Filtering - Notification

To configure HTTP URL Filtering - Notification:

1. From the left-side menu, click **HTTP > URL Filtering**.
2. Click the **Notification** tab.
3. Review the recipient notification.
4. Select the **Administrator** check box to enable the appliance to send a notification to the administrator when a prohibited URL request is detected.
5. Click **Save**.

On this screen is an option to send suspected Phish URLs to TrendLabs for inspection. To send such a URL, click the **Submit a Suspected Phishing URL to TrendLabs** link.

Configuring HTTP File Blocking

InterScan Gateway Security Appliance can scan for and block certain file types that originate from HTTP servers. Enable File Blocking for HTTP traffic and choose the items InterScan Gateway Security Appliance should scan for (Target tab). When InterScan Gateway Security Appliance blocks a file, it sends a notification, if enabled, to the administrator (Notification tab).

HTTP File Blocking - Target

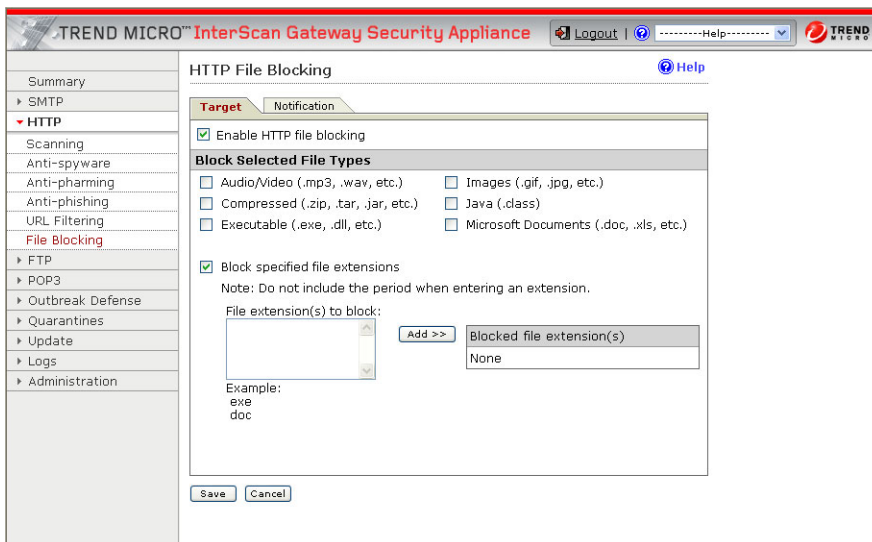


FIGURE 5-20. HTTP > File Blocking - Target

To configure HTTP File Blocking – Target for HTTP traffic:

1. From the left-side menu, click **HTTP > File Blocking**. The **Target** tab appears.
2. Select the **Enable HTTP file blocking** check box.

3. Check one or more items from the predefined list of file types.
 - Audio/Video
 - Compressed
 - Executable
 - Images
 - Java
 - Microsoft documents
4. Enable blocking of specified file extensions.
 - Enter one or more file extensions to block.
5. Click **Add**.
6. Click **Save**.

HTTP File Blocking - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-pharming, Anti-phishing, URL Filtering, File Blocking (highlighted in red), FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled "HTTP File Blocking" and has a "Help" link. It features two tabs: "Target" and "Notification" (selected). Under the "Notification" tab, there are two sections: "User Notification" and "Administrator Notification". The "User Notification" section includes a text area with the message: "The file that you are attempting to transfer has been blocked. Organization policy prohibits transfer of this type of file." The "Administrator Notification" section includes a checkbox for "Administrator" and a text area with the message: "Transfer of prohibited material(s) attempted. >Client IP address: %IPAddress% >File name: %FILENAME% >Date requested: %DATE% >Time requested: %TIME%". At the bottom of the page are "Save" and "Cancel" buttons.

FIGURE 5-21. HTTP > File Blocking - Notification

To select HTTP File Blocking – Notification recipient(s):

1. From the left-side menu, click **HTTP > File Blocking**.
2. Click the **Notification** tab.
3. Review the recipient notification.
4. Select the **Administrator** check box to enable InterScan Gateway Security Appliance to send a notification to the administrator when it blocks a file.
5. Click **Save**.

FTP Services

This chapter describes the FTP services in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Configuring FTP Virus Scanning* on page 6-2
- *Configuring FTP Anti-Spyware* on page 6-7
- *Configuring FTP File Blocking* on page 6-12

FTP Services

The FTP scanning feature in InterScan Gateway Security Appliance scans incoming and outgoing FTP traffic for viruses and spyware. Using file blocking, InterScan Gateway Security Appliance can prevent potentially dangerous files or files containing prohibited or privileged information from being transferred.

Enabling Scanning of FTP Traffic

To allow InterScan Gateway Security Appliance to scan FTP traffic for viruses and other security threats, enable the feature.

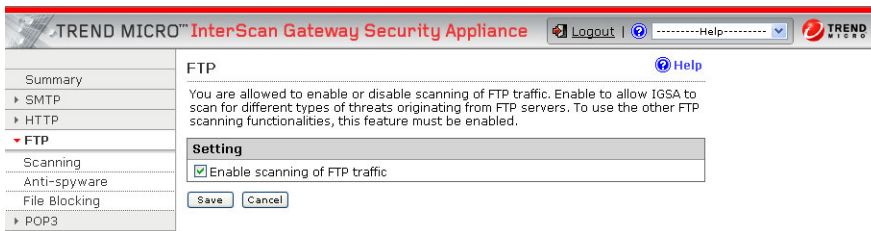


FIGURE 6-1. FTP - Enable

To enable scanning of FTP traffic:

1. On the left-side menu, click **FTP**.
2. Select the Enable FTP Traffic check box.
3. Click Save.

Configuring FTP Virus Scanning

Configuring virus scanning of FTP traffic is a three-step process. First, select what to scan for (Target tab). Next, choose the action for InterScan Gateway Security Appliance to take when it detects a virus or other malware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a virus or other malware (Notification tab).

Note: Infected item - FTP infected items are files downloaded using the FTP protocol that contain viruses or malware.

FTP Scanning - Target

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP (selected), Scanning (expanded), Anti-spyware, File Blocking, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled "FTP Scanning" and includes a "Help" link. The "Target" tab is active, showing the following configuration options:

- ☒ Enable FTP scanning
- Files to Scan**
 - ☒ All scannable files
 - ☐ IntelliScan: uses *true file type* identification
 - ☐ Specified file extensions...
- File Handling**

Do not scan compressed files if:

 - Extracted file count exceeds: (0-1000, 0:no limit)
 - Extracted file size exceeds: MB (1-100)
 - Number of layers of compression exceeds: (2-20)
 - Decompressed file exceeds "x" times the size of compressed file: (0-20, 0:no limit)

Action to take on unscannable files: ☒ Pass ☐ Block
- Large File Handling**

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

 - ☒ Enable deferred scan
 - Start sending parts of the file to the client after (1-100) seconds.

At the bottom of the configuration area are "Save" and "Cancel" buttons.

FIGURE 6-2. FTP > Scanning - Target

To configure the FTP Scanning (Antivirus) - Target:

1. From the left-side menu, click **FTP > Scanning**. The **Target** tab appears.
2. Select the Enable FTP Scanning check box.

3. Specify files to scan:

- All scannable files - InterScan Gateway Security Appliance scans all files, except password-protected or encrypted files
- IntelliScan — True file type identification - IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible for virus scanning. Scans files by an intelligent combination of true file type scanning and exact extension name filtering.
- Specified file extensions... Manually specify the files to scan based on their extensions by selecting this option and clicking the link. A **Scan Specified Files by Extension** window appears.

Scan Specified Files by Extension

These files will be scanned by extension, not by true file type. More comprehensive protection is offered by true file type identification using IntelliScan or the scan all file types option.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file.

.ARJ;.BAT;*.BIN;*.BOO;*.CAB;*.CHM;*.CLA;*.CLASS;*.COM;*.CSC;*.DLL;*.DOC;*.DOT;*.DRV;*.EML;*.EXE;*.GZ;*.HLP;*.HTA;*.HTM;*.HTML;*.HTT;*.INI;*.JAR;*.JPEG;*.JPG;*.JS;*.JSE;*.LNK;*.LZH;*.MDB;*.MPD;*.MPP;*.MPT;*.MSG;*.MSO;*.NWS;*.OCX;*.OFT;*.OVL;*.PDF;*.PHP;*.PIF;*.PL;*.POT;*.PPS;*.PPT;*.PRC;*.RAR;*.REG;*.RTF;*.SCR;*.SHS;*.SYS;*.TAR;*.VBE;*.VBS;*.VSD;*.VSS;*.VST;*.VXD;*.WML;*.WSF;*.XLA;*.XLS;*.XLT;*.XML;*.Z;*.ZIP;*.

Additional Extensions

File extensions to scan:

Note: Not case sensitive. Separate multiple entries with a semicolon. Example:com;vbs

FIGURE 6-3. Scan Specified Files by Extension

- Type the file extensions you wish to scan in the **File extensions to scan** field, separated by a semicolon.
- Click **Add**.
- Finish by clicking **OK**.

4. Back in the main **Target** screen, select files to exclude from scanning based on different criteria:
 - Extracted file count exceeds
 - Extracted file size exceeds
 - Number of layers of compression exceeds
 - Decompressed file size/compressed file size ratio exceeds
 - Action on unscannable files
 - Pass
 - Block
5. Specify a maximum size of file to be scanned.
 - Do not scan files larger than... - set size in MB. Default is 50 MB
 - Enable deferred scanning for files after... - InterScan Gateway Security Appliance starts loading parts of a large file to clients, after a specified period, so the connection between the client and InterScan Gateway Security Appliance will not time out.
6. Click **Save**.

FTP Scanning - Action

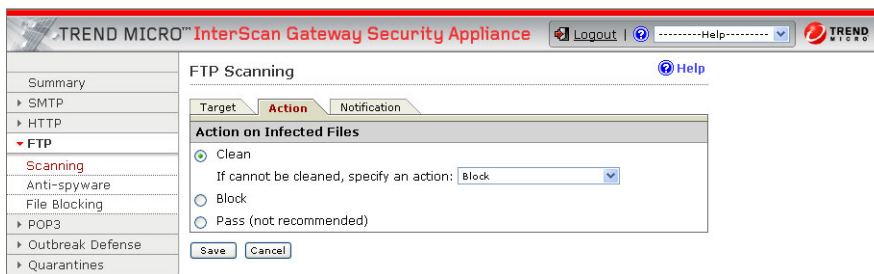


FIGURE 6-4. FTP > Scanning - Action

To configure FTP Scanning (Antivirus) Action:

1. From the left-side menu, click **FTP > Scanning**.
2. Click the **Action** tab.

3. Choose an action for InterScan Gateway Security Appliance to take when it detects a file containing viruses or malware:
 - Clean - if InterScan Gateway Security Appliance detects a virus or malware in the file, it first attempts to clean the item. If the item cannot be cleaned, choose a secondary action from the drop-down menu:
 - Block - InterScan Gateway Security Appliance deletes all items
 - Pass (not recommended) - InterScan Gateway Security Appliance allows all items to be downloaded
4. Or choose among the following options:
 - Block - if more than one file is downloaded, InterScan Gateway Security Appliance deletes only the infected files, and the others will continue downloading.
 - Pass (not recommended) - InterScan Gateway Security Appliance takes no action on infected items.
5. Click **Save**.

FTP Scanning - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP (selected), Scanning (sub-menu), Anti-spyware, File Blocking, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled "FTP Scanning" and has a "Help" link. It features three tabs: "Target", "Action", and "Notification" (selected). The "Notification" tab contains two sections: "User Notification" and "Administrator Notification". The "User Notification" section has a text area for displaying a message to the user's browser when an infected file is detected. The "Administrator Notification" section has a checkbox for "Administrator" and a text area for configuring the email notification message. The email message template includes fields for Threat type, Threat name, Client IP address, and Action taken. At the bottom of the "Administrator Notification" section are "Save" and "Cancel" buttons.

FIGURE 6-5. FTP > Scanning - Notification

To select FTP Scanning (Antivirus) – Notification recipients:

1. From the left-side menu, click **FTP > Scanning**.
2. Click the **Notification** tab.
3. In the **User Notification** text box, type the message that the user will see if the appliance detects an infected file.
4. In the **Administrator Notification** text box, type the message that the administrator will see.
5. Select the **Administrator** check box to enable InterScan Gateway Security Appliance to send a notification if it detects a virus or malware.
6. Click **Save**.

Configuring FTP Anti-Spyware

Configuring InterScan Gateway Security Appliance to scan FTP traffic for spyware/grayware is a three-step process. First, select what to scan for (Target tab). Next, set the action for InterScan Gateway Security Appliance to take when it detects an item infected that contains spyware/grayware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects an item containing spyware/grayware (Notification tab).

Note: Infected item - FTP infected items are files that are spyware/grayware or files that contain spyware/grayware and that are downloaded using the FTP protocol.

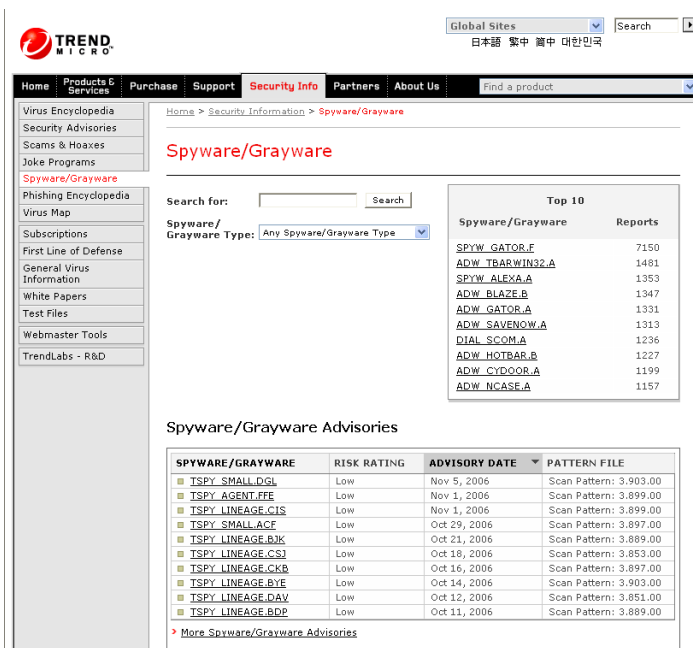
FTP Anti-Spyware - Target



FIGURE 6-6. FTP > Anti-spyware - Target

To configure Anti-spyware to scan FTP traffic:

1. From the left-side menu, click **FTP > Anti-spyware**. The **Target** tab appears.
2. Select the **Enable FTP Anti-spyware** check box.
3. [Optional] Configure the **Spyware/Grayware Exclusion List**:
 - Click the **Search for spyware/grayware** link. InterScan Gateway Security Appliance opens a browser window on the Trend Micro Web site and displays the Trend Micro Spyware/Grayware online database.



TREND MICRO

Global Sites: 日本語 繁体中 简体中文

Home | Products & Services | Purchase | Support | **Security Info** | Partners | About Us | Find a product

Home > Security Information > **Spyware/Grayware**

Spyware/Grayware

Search for: Search

Spyware/Grayware Type:

Top 10	
Spyware/Grayware	Reports
SPYW_GATOR.F	7150
ADW_TBARWIN32.A	1481
SPYW_ALEXA.A	1353
ADW_BLAZE.B	1347
ADW_GATOR.A	1331
ADW_SAVENOW.A	1313
DIAL_SCOM.A	1236
ADW_HOTBAR.B	1227
ADW_CYDOOR.A	1199
ADW_NCASE.A	1157

Spyware/Grayware Advisories

SPYWARE/GRAYWARE	RISK RATING	ADVISORY DATE	PATTERN FILE
☐ TSPY_SMALL.DGL	Low	Nov 5, 2006	Scan Pattern: 3.903.00
☐ TSPY_AGENT.FFE	Low	Nov 1, 2006	Scan Pattern: 3.899.00
☐ TSPY_LINEAGE.CIS	Low	Nov 1, 2006	Scan Pattern: 3.899.00
☐ TSPY_SMALL.ACF	Low	Oct 29, 2006	Scan Pattern: 3.897.00
☐ TSPY_LINEAGE.BJK	Low	Oct 21, 2006	Scan Pattern: 3.889.00
☐ TSPY_LINEAGE.CSI	Low	Oct 18, 2006	Scan Pattern: 3.853.00
☐ TSPY_LINEAGE.CKB	Low	Oct 16, 2006	Scan Pattern: 3.897.00
☐ TSPY_LINEAGE.BVE	Low	Oct 14, 2006	Scan Pattern: 3.903.00
☐ TSPY_LINEAGE.DAV	Low	Oct 12, 2006	Scan Pattern: 3.851.00
☐ TSPY_LINEAGE.BDP	Low	Oct 11, 2006	Scan Pattern: 3.889.00

[More Spyware/Grayware Advisories](#)

FIGURE 6-7. Trend Micro Spyware/Grayware Online Database

- Search for the spyware you wish to exclude:
 - Returning to the Target screen, copy/paste or type the name of the spyware grayware in the **Enter name of spyware/grayware** field. (The spyware/grayware exclusion list is case sensitive and has exact match capability.)
4. Click **Add**.
 5. Select spyware/grayware types to scan for in the **Scan for Spyware/Grayware** section:
 - Select all
 Or
 - Select specific spyware/grayware types
 6. Click **Save**.

FTP Anti-Spyware - Action

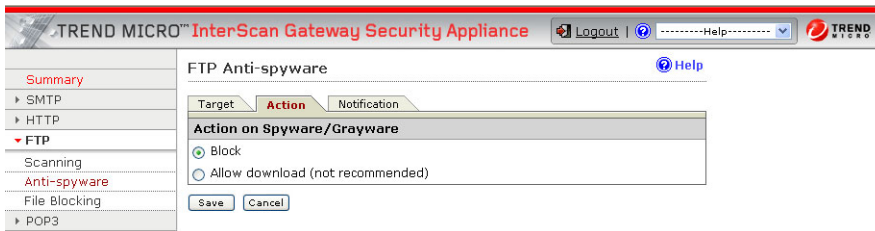


FIGURE 6-8. FTP > Anti-spyware - Action

To configure FTP Anti-spyware Action:

1. From the left-side menu, click **FTP > Anti-spyware**.
2. Click the **Action** tab.
3. Choose one of the following actions for InterScan Gateway Security Appliance to take when it detects a spyware:
 - **Block** - InterScan Gateway Security Appliance blocks the file transfer and then notifies recipients with an in-line user notification. InterScan Gateway Security Appliance also sends a notification, if enabled, to the administrator.
 - or
 - **Pass (not recommended)** - InterScan Gateway Security Appliance takes no action on items that contain spyware/grayware.
4. Click **Save**.

FTP Anti-Spyware - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP (selected), Scanning, Anti-spyware (selected), File Blocking, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled "FTP Anti-spyware" and includes a "Help" link. Below the title is a tabbed interface with "Target", "Action", and "Notification" tabs. The "Notification" tab is active, showing two sections: "User Notification" and "Administrator Notification". The "User Notification" section contains a text box with the message: "Display the following message on the user's browser when spyware/grayware is detected: Trend Micro InterScan Gateway Security Appliance has determined that the file you are attempting to transfer contains spyware/grayware. The appliance has taken action on the file." The "Administrator Notification" section contains a text box with the message: "When spyware/grayware is detected and the following item is selected, the corresponding email notification will be sent." Below this is a checkbox labeled "Administrator" which is currently unchecked. To the right of the checkbox is a text box containing the following information: "A threat was detected in FTP traffic. >Threat type: spyware/grayware >Threat name: %VIRUSNAME% >Client IP address: %IPAddress% >Action taken: %ACTION%". At the bottom of the page are "Save" and "Cancel" buttons.

FIGURE 6-9. FTP > Anti-spyware - Notification

To select FTP Anti-spyware – Notification recipient(s):

1. From the left-side menu, click **FTP > Anti-spyware**.
2. Review the user notification message.
3. Select the **Administrator** check box to enable InterScan Gateway Security Appliance to send the administrator a notification when it discovers spyware/grayware.
4. Click **Save**.

Configuring FTP File Blocking

Configuring InterScan Gateway Security Appliance to scan for and block certain file types in FTP traffic is a two-step process. First, enable FTP file blocking and select what to block (Target tab). Second, when InterScan Gateway Security Appliance blocks a file, it sends a notification, if enabled, to the administrator (Notification tab).

FTP File Blocking - Target

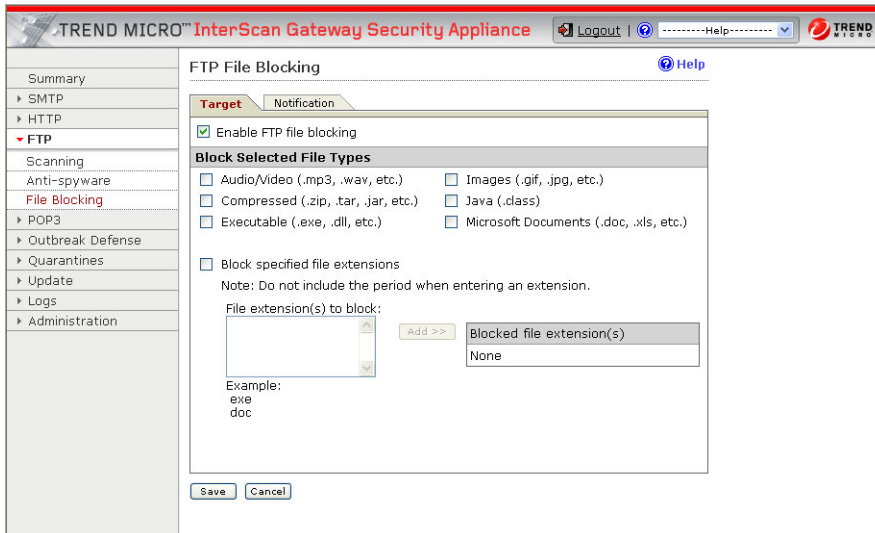


FIGURE 6-10. FTP > File Blocking - Target

To configure FTP File Blocking - Target:

1. From the left-side menu, click **FTP > File Blocking**. The **Target** tab appears.
2. Select the **Enable FTP file blocking** check box.
3. Select the type(s) of files to be blocked.
 - Audio/Video
 - Compressed
 - Executable
 - Images
 - Java

- Microsoft documents
4. Enable blocking of administrator-specified file extensions.
 5. Enter one or more file extensions to block.
 6. Click **Add**.
 7. Click **Save**.

Note: For more information on Blockable File Types, see Appendix C: File Formats: Blockable File Formats

FTP File Blocking - Notification

TREND MICRO™ InterScan Gateway Security Appliance Logout | Help

FTP File Blocking Help

Target **Notification**

User Notification
Display the following message on the user's browser when a blocked file type is detected:

The file that you are attempting to transfer has been blocked. Organization policy prohibits transfer of this type of file.

Administrator Notification
When a blocked file type is detected and the following item is selected, the corresponding email notification will be sent.

☐ Administrator

Transfer of prohibited material(s) attempted.
>Client IP address: %IPAddress%
>File name: %FILENAME%
>Date requested: %DATE%
>Time requested: %TIME%

Save Cancel

FIGURE 6-11. FTP > File Blocking - Notification

To configure FTP File Blocking – Notifications:

1. From the left-side menu, click **FTP > File Blocking**.
2. Click the **Notification** tab.
3. Review the recipient notification.
4. Select the Administrator check box to enable InterScan Gateway Security Appliance to send a notification to the administrator when it blocks a file.
5. Click Save.

POP3 Services

This chapter describes POP3 Services in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Configuring POP3 Virus Scanning* on page 7-3
- *Configuring POP3 Anti-Spyware* on page 7-8
- *Configuring POP3 IntelliTrap* on page 7-13
- *Configuring POP3 Anti-Spam* on page 7-16
- *Configuring POP3 Anti-Phishing* on page 7-18
- *Configuring POP3 Content Filtering* on page 7-21

POP3 Services

Enable POP3 scanning to allow InterScan Gateway Security Appliance to scan traffic originating from POP3 servers for viruses/malware, spyware/grayware, bots, spam, inappropriate content, and links to phishing sites.

Enabling Scanning of POP3 Traffic

To allow InterScan Gateway Security Appliance to scan POP3 traffic, enable the feature.

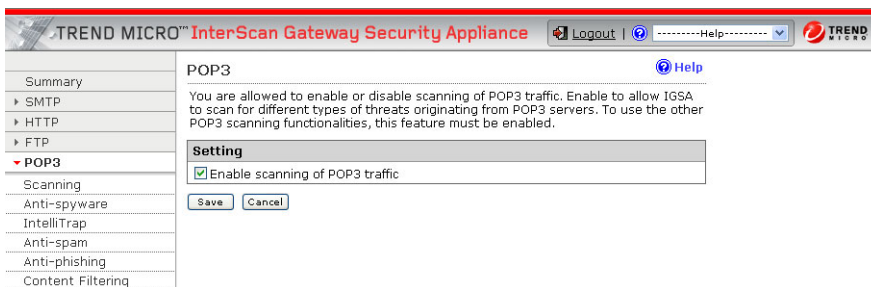


FIGURE 7-1. POP3- Enable

To enable scanning of POP3 traffic:

1. On the left-side menu, click **POP3**.
2. Select the **Enable POP3 Traffic** check box.
3. Click **Save**.

Configuring POP3 Virus Scanning

Configuring virus scanning of POP3 traffic is a three-step process. First, enable virus scanning and then select what to scan (Target tab). Next, set the action for InterScan Gateway Security Appliance to take when it detects a virus or other malware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a virus or other malware (Notification tab).

Note: Infected item - POP3 infected items are attachments and or the body of an email that contains a virus or other malware.

POP3 Scanning - Target

The screenshot shows the configuration interface for POP3 Scanning in the Target tab. The interface includes a left-hand navigation menu with options like Summary, SMTP, HTTP, FTP, POP3, Scanning, Anti-spyware, IntelliTrap, Anti-spam, Anti-phishing, Content Filtering, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'POP3 Scanning' and has three tabs: Target, Action, and Notification. The Target tab is active, showing the following settings:

- Enable POP3 scanning:** ☒
- Files to Scan:**
 - ☒ All scannable files
 - ☐ IntelliScan: uses *true file type* identification
 - ☐ Specified file [extensions...](#)
- File Handling:**

Do not scan compressed files if:

Extracted file count exceeds:	1000 (0-1000, 0:no limit)
Extracted file size exceeds:	50 MB (1-100)
Number of layers of compression exceeds:	2 (2-20)
Decompressed file exceeds "x" times the size of compressed file:	10 (0-20, 0:no limit)

Action to take on unscannable files: ☒ Pass ☐ Remove

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

FIGURE 7-2. POP3 > Scanning - Target

To configure the POP3 Scanning – Target:

1. From the left-side menu, click **POP3 > Scanning**. The **Target** tab appears.
2. Select the Enable POP3 Scanning check box.
3. Specify the files to scan:
 - All scannable files - InterScan Gateway Security Appliance scans all files, except password-protected or encrypted files
 - IntelliScan — True file type identification - IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus scanning. Scans files by an intelligent combination of true file type scanning and exact extension name filtering.
 - Specified file extensions... Manually specify the files to scan based on their extensions by selecting this option and clicking the link. A **Scan Specified Files by Extension** window appears.

Scan Specified Files by Extension

These files will be scanned by extension, not by true file type. More comprehensive protection is offered by true file type identification using IntelliScan or the scan all file types option.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file.

**; ARJ; BAT; BIN; BOO; CAB; CHM; CLA; CLASS; COM; CSC; DLL; DOC; DOT; DRV; EML; EXE; GZ; HLP; HTA; HTM; HTML; HTT; INI; JAR; JPEG; JPG; JS; JSE; LNK; LZH; MDB; MPD; MPP; MPT; MSG; MSO; NWS; OCK; OFT; OVL; PDF; PHP; PIF; PL; POT; PPS; PPT; PRC; RAR; REG; RTF; SCR; SHS; SYS; TAR; VBE; VBS; VSD; VSS; VST; VXD; WML; WSF; XLA; XLS; XLT; XML; Z; ZIP; { *;

Additional Extensions

File extensions to scan: Add

Delete

Note: Not case sensitive. Separate multiple entries with a semicolon. Example:com;vbs

OK
Cancel

FIGURE 7-3. Scan Specified Files by Extension

- a. Type the file extensions you wish to scan in the **File extensions to scan** field, separated by a semicolon.
- b. Click **Add**.
- c. Click **OK**.

4. Back in the main **Target** screen, select files to exclude from scanning based on different criteria:
 - Extracted file count exceeds
 - Extracted file size exceeds
 - Number of layers of compression exceeds
 - Extracted file size/compressed file size ratio exceeds
5. Choose the action on unscannable files:
 - Pass
 - Remove
6. Click **Save**.

POP3 Scanning - Action



FIGURE 7-4. POP3 > Scanning - Action

To configure the POP3 Scanning - Action:

1. From the left-side menu, click **POP3 > Scanning**.
2. Click the **Action** tab.

3. Choose an action for InterScan Gateway Security Appliance to take when it detects viruses or malware:
 - Clean infected items and pass - If InterScan Gateway Security Appliance detects a virus or malware in either the message body or the attachment, it attempts to clean the item. If the item cannot be cleaned, choose a secondary action from the drop-down menu:
 - Quarantine - InterScan Gateway Security Appliance sends the message and any attachments to the quarantine folder and then sends the recipient a quarantine notification.
 - Remove: - InterScan Gateway Security Appliance reacts differently depending on what items are infected. The table below describes the different possible scenarios and how InterScan Gateway Security Appliance responds to them.

TABLE 7-1. "Remove" Scenarios

Scenarios	Response
E-mail w/infected body	Email delivered with body removed
Email w/infected attachment	Email delivered with attachment removed
Email w/infected body and infected attachment	Email delivered with body and attachment removed

- Pass (not recommended) - InterScan Gateway Security Appliance delivers all items to the recipient.
4. Or choose among the following options:
 - Quarantine - InterScan Gateway Security Appliance quarantines the message and any attachments and then sends the recipient a quarantine notification.
 - Delete - InterScan Gateway Security Appliance deletes the message and any attachments and then sends the recipient a delete notification.
 - Remove infected items and pass - InterScan Gateway Security Appliance delivers the message and removes any infected items.
 - Pass (not recommended) - InterScan Gateway Security Appliance takes no action on infected items.
 5. Click **Save**.

POP3 Scanning - Notification

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3 (selected), Scanning, Anti-spyware, IntelliTrap, Anti-spam, Anti-phishing, Content Filtering, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'POP3 Scanning' and has a 'Help' link. It contains three tabs: Target, Action, and Notification (selected). Under the 'Notification' tab, there is a section for 'Email Notifications' which explains that notifications are sent when an infected message is detected. Below this, there are three checkboxes for recipients: Administrator, Sender, and Recipient. Each checkbox has a corresponding text area for the notification message. The 'Administrator' message states: 'A threat was detected in a message. >Threat type: virus/malware >Threat name: %VIRUSNAME% >Sender: %SENDER% >Recipient: %RECIPIENT%'. The 'Sender' message states: 'Warning - the virus, %VIRUSNAME% was detected in a message sent to %RECIPIENT% from your computer. The message subject is %SUBJECT%. The message may not have been delivered.' The 'Recipient' message states: 'Warning - the virus, %VIRUSNAME% was detected in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be deliverable.' Below the 'Email Notifications' section is the 'Inline Notification Stamp' section, which allows inserting text into scanned messages. It has two sub-sections: 'Virus Detected Notifications' and 'Virus Free Notifications'. Under 'Virus Detected Notifications', there are checkboxes for 'Subject line' (with the text 'Risk detected:') and 'Message' (with the text 'This message contains a possible security risk.'). Under 'Virus Free Notifications', there is a checkbox for 'Message' (with the text 'This message has been scanned by the Trend Micro InterScan Security Module and found to be free of known security risks.'). At the bottom of the page are 'Save' and 'Cancel' buttons.

FIGURE 7-5. POP3 > Scanning - Notification

To select POP3 Scanning – Notification recipient(s):

1. From the left-side menu, click **POP3 > Scanning**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when an infected incoming message is detected, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient

4. Select all options that apply:

Virus Detected Notifications

- Subject line - when InterScan Gateway Security Appliance detects a virus or malware in an email, the recipient receives this message in the subject line of the email.
- Message - when InterScan Gateway Security Appliance detects a virus or malware in an email, the recipient receives this message in the body of the email.

Virus Free Notifications

- Message - when an email is scanned and determined to be free of viruses or malware, the recipient receives this message in the body of the email.

5. Click **Save**.

Configuring POP3 Anti-Spyware

Configuring anti-spyware to scan POP3 traffic for spyware/grayware is a three-step process. First, select what to scan for (Target). Next, set the action for InterScan Gateway Security Appliance to take when it detects an item that contains spyware/grayware (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects an item containing spyware/grayware (Notification tab).

Note: Infected item - POP3 infected items are attachments and or the body of an email that contains spyware/grayware.

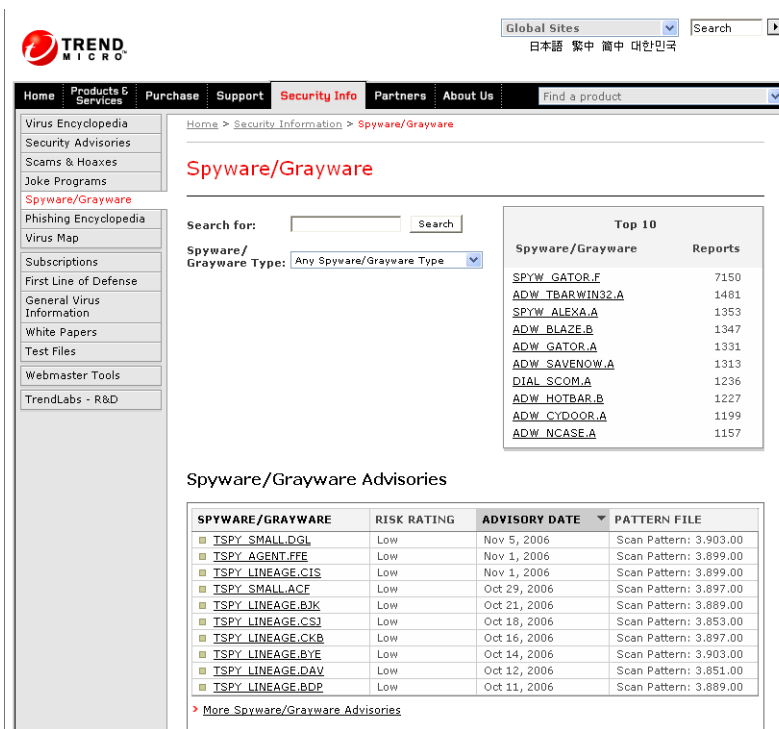
POP3 Anti-Spyware - Target



FIGURE 7-6. POP3 > Anti-spyware - Target

To configure the POP3 Anti-spyware – Target:

1. From the left-side menu, click **POP3 > Anti-spyware**. The **Target** tab appears.
2. Select the **Enable POP3 Anti-spyware** check box.
3. [Optional] Configure the **Spyware/Grayware Exclusion List**:
4. [Optional] Click the **Search for spyware/grayware** link. InterScan Gateway Security Appliance opens a browser window on the Trend Micro Web site and displays the Trend Micro Spyware/Grayware online database.



The screenshot displays the Trend Micro website's 'Spyware/Grayware' section. At the top, there's a navigation bar with links like Home, Products & Services, Purchase, Support, Security Info, Partners, and About Us. A search bar is also present. The main content area is titled 'Spyware/Grayware' and includes a search bar and a dropdown menu for 'Spyware/Grayware Type'. Below this, there's a table titled 'Top 10' showing the most common spyware/grayware types and their report counts. At the bottom, there's a table titled 'Spyware/Grayware Advisories' listing various advisories with their risk ratings, advisory dates, and pattern files.

SPYWARE/GRAYWARE	RISK RATING	ADVISORY DATE	PATTERN FILE
TSPY_SMALL.DGL	Low	Nov 5, 2006	Scan Pattern: 3.903.00
TSPY_AGENT.FFE	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSPY_LINEAGE.CIS	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSPY_SMALL.ACF	Low	Oct 29, 2006	Scan Pattern: 3.897.00
TSPY_LINEAGE.BJK	Low	Oct 21, 2006	Scan Pattern: 3.889.00
TSPY_LINEAGE.CSJ	Low	Oct 18, 2006	Scan Pattern: 3.853.00
TSPY_LINEAGE.CKB	Low	Oct 16, 2006	Scan Pattern: 3.897.00
TSPY_LINEAGE.BYE	Low	Oct 14, 2006	Scan Pattern: 3.903.00
TSPY_LINEAGE.DAV	Low	Oct 12, 2006	Scan Pattern: 3.851.00
TSPY_LINEAGE.BDP	Low	Oct 11, 2006	Scan Pattern: 3.889.00

FIGURE 7-7. Figure 7-7. Trend Micro Spyware/Grayware Online Database

- Search for the spyware you wish to exclude.
 - Returning to the **Target** screen, copy/paste or type the name of spyware/grayware in the Enter name of spyware/grayware field. (The spyware/grayware exclusion list is case sensitive and has exact match capability.)
5. Click **Add**.
 6. Select spyware/grayware types to scan for in the **Scan for Spyware/Grayware** section:
 - Select all
 - Or
 - Select specific spyware/grayware types
 7. Click **Save**.

POP3 Anti-Spyware - Action

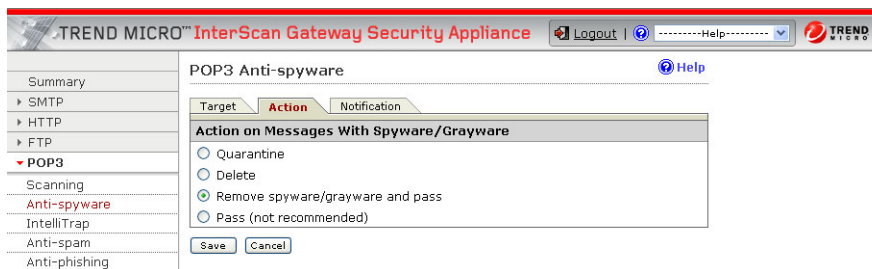


FIGURE 7-8. POP3 > Anti-spyware - Action

To configure POP3 Anti-spyware - Action:

1. From the left-side menu, click **POP3 > Anti-spyware**.
2. Click the **Action** tab.
3. Choose one of the following actions for InterScan Gateway Security Appliance to take when it detects spyware:
 - Quarantine - InterScan Gateway Security Appliance sends the message and any attachments to the quarantine folder and then sends the recipient a quarantine notification.
 - Delete - InterScan Gateway Security Appliance deletes the message and any attachments and then sends the recipient a delete notification.
 - Remove spyware/grayware and pass - InterScan Gateway Security Appliance delivers the message and removes any infected items.
 - Pass (not recommended) - InterScan Gateway Security Appliance takes no action on items that contain spyware/grayware.
4. Click **Save**.

POP3 Anti-Spyware - Notification

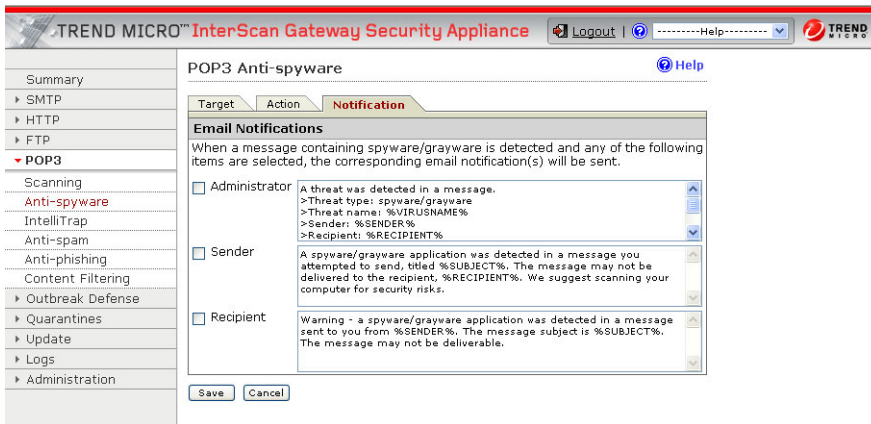


FIGURE 7-9. POP3 > Anti-spyware - Notification

To select POP3 Anti-spyware Notification recipient(s):

1. From the left-side menu, click **POP3 > Anti-spyware**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when a message containing spyware/grayware is detected, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

Configuring POP3 IntelliTrap

Configuring IntelliTrap to scan POP3 traffic for bots is a three-step process. First, enable InterScan Gateway Security Appliance to scan for bots (Target tab). Next, set the action that InterScan Gateway Security Appliance should take when it detects a bot (Action tab). Finally, decide whom to notify when InterScan Gateway Security Appliance detects a bot (Notification tab).

Note: Infected item - POP3 infected items are email attachments that contain compressed executable files that are designed with the intent to cause harm to computer systems and networks. These types of compressed executables are known as bots. Bots, once executed, can replicate, compress, and distribute themselves.

POP3 IntelliTrap - Target

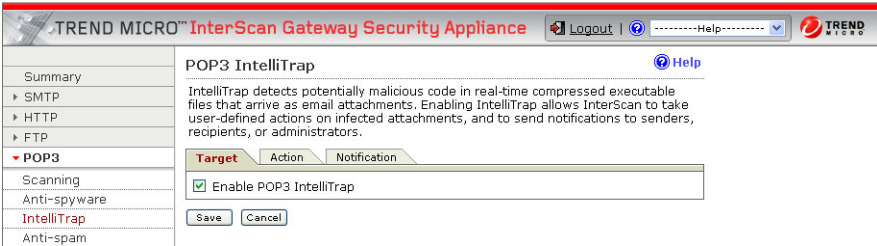


FIGURE 7-10. POP3 > IntelliTrap - Target

To configure POP3 IntelliTrap - Target:

1. From the left-side menu, click **POP3 > IntelliTrap**. The **Target** tab appears.
2. Select the **Enable POP3 IntelliTrap** check box.
3. Click **Save**.

POP3 IntelliTrap - Action



FIGURE 7-11. Figure 7-11. POP3 > IntelliTrap - Action

To configure POP3 IntelliTrap - Action:

1. From the left-side menu, click **POP3 > IntelliTrap**.
2. Click the **Action** tab.
3. Select one of the following actions for InterScan Gateway Security Appliance to take if it detects a bot in an email attachment:
 - **Quarantine**- InterScan Gateway Security Appliance sends the message to the quarantine folder and then sends the recipient a quarantine notification.
 - **Delete**- InterScan Gateway Security Appliance deletes the message and any attachment(s) and then sends the recipient a delete notification.
 - **Remove infected attachments and pass**- InterScan Gateway Security Appliance delivers the message and removes any infected items.
 - **Record detection and pass (not recommended)**- InterScan Gateway Security Appliance records the detection and delivers the message.
4. Click **Save**.

POP3 IntelliTrap - Notification



FIGURE 7-12. POP3 > IntelliTrap - Notification

To select POP3 IntelliTrap – Notification recipient(s):

1. From the left-side menu, click POP3 > IntelliTrap.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when IntelliTrap detects a potential threat, the corresponding email notification(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

Configuring POP3 Anti-Spam

Configuring anti-spam to scan POP3 traffic for spam email is a two-step process. First, select a spam detection level, and then configure the Approved Senders, Blocked Senders, and Keyword Exception lists (Target tab). Next, set the action that InterScan Gateway Security Appliance should take when it detects a spam email (Action tab).

POP3 Anti-Spam - Target

The screenshot displays the 'POP3 Anti-spam' configuration page. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3 (selected), Scanning, Anti-spyware, IntelliTrap, Anti-spam (highlighted), Anti-phishing, Content Filtering, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'POP3 Anti-spam' and includes a 'Help' link. It features two tabs: 'Target' (active) and 'Action'. Under the 'Target' tab, there is a checkbox for 'Enable POP3 Anti-spam' which is checked. Below this is the 'Filter Tuning' section with a 'Spam detection level' dropdown set to 'Low'. The 'Keyword Exceptions' section contains a text area for entering keywords. The 'Approved Senders' section includes a text area for adding approved sender email addresses or domain names. The 'Blocked Senders' section includes a text area for adding blocked sender email addresses or domain names. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 7-13. POP3 > Anti-spam - Target

To configure POP3 Anti-spam – Target:

1. From the left-side menu, click **POP3 > Anti-spam**. The Target tab appears.
2. Select the **Enable POP3 Anti-spam check box** to allow InterScan Gateway Security Appliance to scan POP3 email for spam.
3. Select a value from the Spam detection level drop-down menu. The higher the detection level, the more messages are classified as spam.
 - Low - This is the default setting. This is the most lenient level of spam detection. InterScan Gateway Security Appliance only filters the most obvious and common spam messages, but there is a very low chance that it will filter false positives.
 - Medium - (default) - InterScan Gateway Security Appliance monitors at a high level of spam detection with a moderate chance of filtering false positives.
 - High - This is the most rigorous level of spam detection. InterScan Gateway Security Appliance monitors all email messages for suspicious files or text, but there is a greater chance of false positives. False positives are those email messages that InterScan Gateway Security Appliance filters as spam when they are actually legitimate email messages.
4. [Optional]: Keyword Exceptions
Messages containing identified keywords will not be considered spam (separate multiple entries with a semicolon).
5. [Optional]: Approved Senders
Add approved senders' email addresses or domain names (separate multiple entries with a semicolon).
6. [Optional]: Blocked Senders
Add blocked senders' email addresses or domain names (separate multiple entries with a semicolon).
7. Click **Save**.

POP3 Anti-Spam - Action

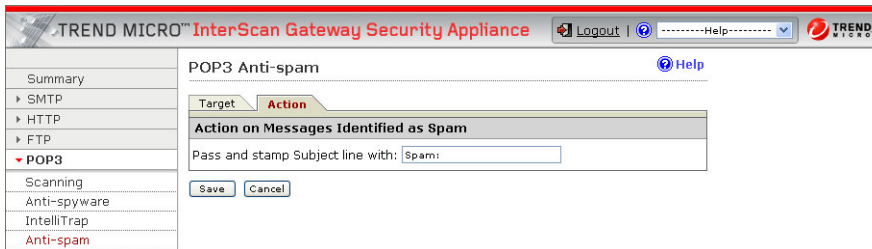


FIGURE 7-14. POP3 > Anti-spam - Action

To configure POP3 Anti-spam - Action:

1. From the left-side menu, click **POP3 > Anti-spam**.
2. Click the **Action** tab.
3. Leave the default message or type a new message in the **Pass and stamp Subject line with** field. The message will appear in the subject line of the email if InterScan Gateway Security Appliance detects spam.
4. Click **Save**.

Configuring POP3 Anti-Phishing

You can enable InterScan Gateway Security Appliance to scan POP3 email for links to known phishing sites (Target tab). Choose the action for InterScan Gateway Security Appliance to take when it encounters a phishing site (Action tab). When InterScan Gateway Security Appliance detects a phishing site, it sends a message, if enabled, to recipients that you choose (Notification tab).

POP3 Anti-Phishing - Target

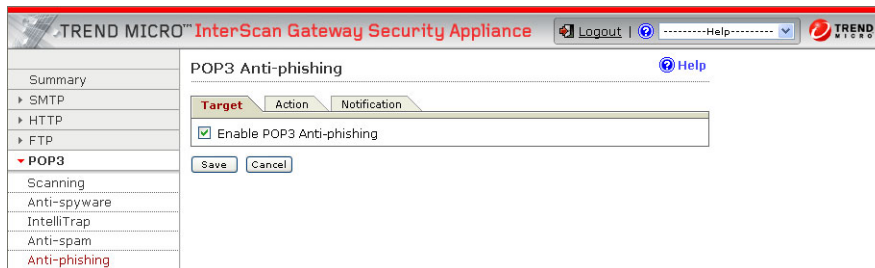


FIGURE 7-15. POP3 > Anti-phishing - Target

To configure POP3 Anti-phishing – Target:

1. From the left-side menu, click **POP3 > Anti-phishing**. The **Target** tab appears.
2. Select the **Enable POP3 Anti-phishing** check box to enable scanning of POP3 traffic for known phishing sites.
3. Click **Save**.

POP3 Anti-Phishing - Action

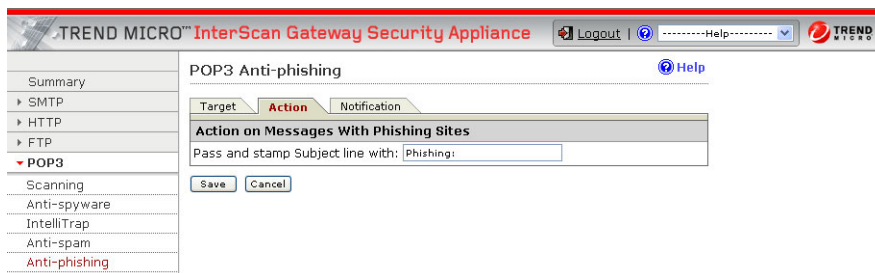


FIGURE 7-16. POP3 > Anti-phishing - Action

To configure POP3 Anti-phishing - Action:

1. From the left-side menu, click **POP3 > Anti-phishing**.
2. Click the **Action** tab.

3. Review the default message or type a new message in the **Pass and stamp Subject line:** field. The message appears in the subject line of the email if InterScan Gateway Security Appliance detects a known phishing site.
4. Click **Save**.

POP3 Anti-Phishing - Notification

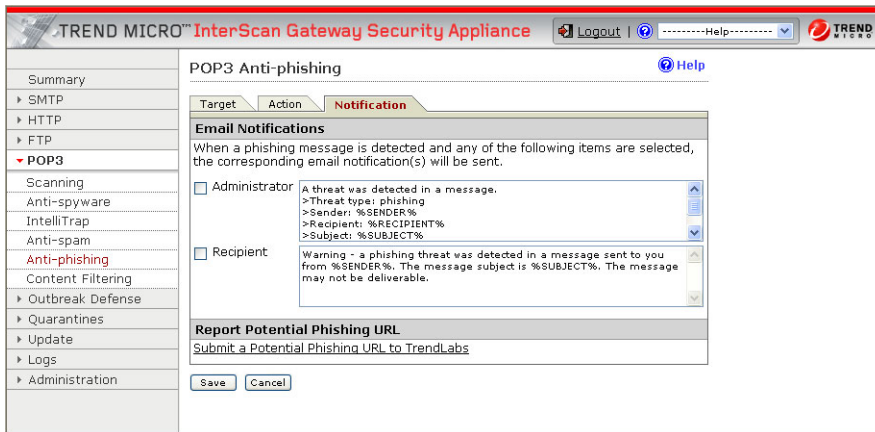


FIGURE 7-17. POP3 > Anti-phishing - Notification

To configure POP3 Anti-phishing - Notifications:

1. From the left-side menu, click **POP3 > Anti-phishing**.
2. Click the **Notification** tab.
3. Select one or more recipients from the Email Notifications section. InterScan Gateway Security Appliance sends notifications to the selected recipients when it detects a known phishing site.
4. Click **Save**.

On this screen is an option to send suspected Phish URLs to TrendLabs for inspection. To send such a URL, click the **Submit a Suspected Phishing URL to TrendLabs** link.

Configuring POP3 Content Filtering

Configuring content filtering for POP3 traffic is a four-step process:

1. Enable scanning of SMTP traffic
2. Select what to filter for (Target tab).
3. Set the action for InterScan Gateway Security Appliance (the appliance) to take when one or more filters is triggered (Action tab).
4. Decide whom to notify when the appliance detects any filter violations (Notification tab).

POP3 Content Filtering - Target

TREND MICRO™ InterScan Gateway Security Appliance Logout | Help

POP3 Content Filtering Help

Target Action Notification

☐ Enable POP3 content filtering

Filter by Message Size

Filter messages based on their size (including message body and attachment):

☒ Filter if message size is larger than

Filter by Text in Message Header

Messages can be filtered based on keywords in the message header. The message header includes the From, To, CC, and Subject fields.

Word to filter from the header:

Filter List

None

☐ Match case

Filter by Text in Message Body

Filter messages with certain words in the body area.

Word to filter from body area:

Filter List

None

☐ Match case

Filter by Message Attachment Name

Filter messages based on attachment file names. You can use asterisks (*) as wildcards to define file name filters.

Word to filter from attachments:

Filter List

None

Filter by True File Type

☐ Audio/Video (.mp3, .wav, etc.) ☐ Images (.gif, .jpg, etc.)

☐ Compressed (.zip, .tar, .jar, etc.) ☐ Java (.class)

☐ Executable (.exe, .dll, etc.) ☐ Microsoft Documents (.doc, .xls, etc.)

FIGURE 7-18. POP3 > Content Filtering - Target

To configure POP3 Content Filtering - Target:

1. From the left-side menu, click **POP3 > Content Filtering**. The **Target** tab appears.
2. Select the **Enable POP3 content filtering** check box.
3. Set any of the following message filters:
 - Filter by Message Size: The Trend Micro recommended size is 5 MB. Larger file sizes can reduce the appliance throughput. If message exceeds size it will not be scanned.
 - Filter by Text in Message Header:
 - i. Enter one or more words for InterScan Gateway Security Appliance to check for when scanning content of the message header, including the Subject, From, To, and CC fields.
 - ii. Click **Add**.
 - iii. [Optional] – if match case is selected, only items that match the case entered in the list will be identified.
 - Filter by Text in Body:
 - i. Enter one or more words for InterScan Gateway Security Appliance to check for when scanning content in the body of email.
 - ii. Click **Add**.
 - iii. [Optional] - If you select match case, only items that match the case entered in the list will be identified.
 - Filter by Message Attachment - Filter attachments by file name:
 - i. Type one or more words for InterScan Gateway Security Appliance to check for when scanning attachment names.
 - ii. Click **Add**.
 - Filter by Attachment True File Type - InterScan Gateway Security Appliance can filter email attachments by type. To have InterScan Gateway Security Appliance filter messages based on attachment type, select one or more of the items in the Attachment True File Type dialog box.
4. Click **Save**.

POP3 Content Filtering - Action

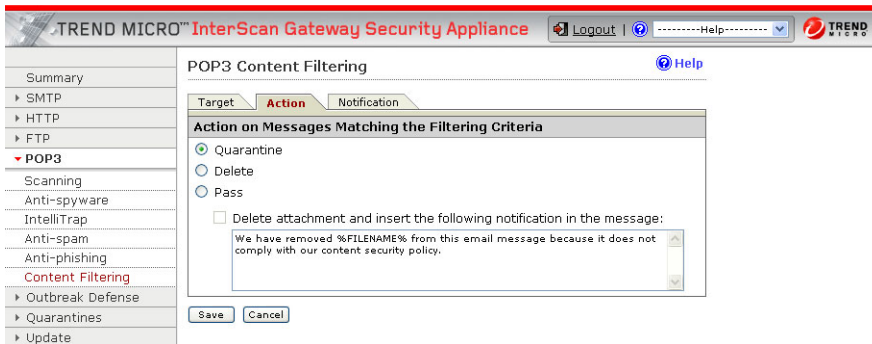


FIGURE 7-19. POP3 > Content Filtering - Action

To configure POP3 Content Filtering - Action:

1. From the left-side menu, click **POP3 > Content Filtering**.
2. Click the **Action** tab.
3. Select one of the following actions for InterScan Gateway Security Appliance to take when the contents of an email message or an attachment triggers one of the content filtering rules:
 - **Quarantine** - InterScan Gateway Security Appliance sends the email and any attachments to the quarantine folder and then sends the recipient a quarantine notification.
 - **Delete** - InterScan Gateway Security Appliance deletes the message and any attachments and then sends the recipient a delete notification.
 - **Pass** - InterScan Gateway Security Appliance delivers the message and the attachment. You have the option of removing the attachment. If you select this option, InterScan Gateway Security Appliance delivers the message with a delete statement inside the body of the message.

Note: The Delete attachment and insert the following notification in the message check box only works with attachments that have triggered the Attachment Name or True File Type filters.

4. Click **Save**.

POP3 Content Filtering - Notification

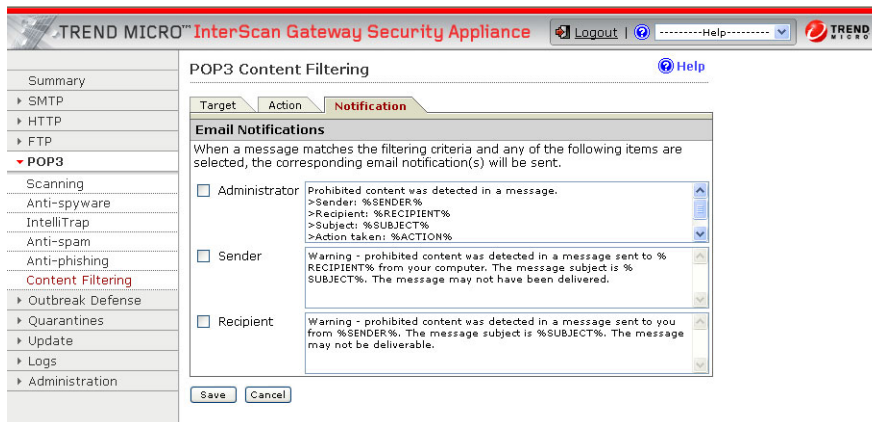


FIGURE 7-20. POP3 > Content Filtering - Notification

To select POP3 Content Filtering – Notification recipient(s):

1. From the left-side menu, click **POP3 > Content Filtering**.
2. Click the **Notification** tab.
3. Select one or more of the following recipients and when a message matches the filtering criteria, the corresponding email notification(s) will be sent.
 - Administrator
 - Sender
 - Recipient
4. Click **Save**.

Outbreak Defense

This chapter describes the Outbreak Defense functions in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *The Outbreak Defense Services* on page 8-2
- *Current Status* on page 8-3
- *Configuring Internal Outbreak* on page 8-5
- *Configuring Damage Cleanup* on page 8-6
- *Configuring Settings* on page 8-7

The Outbreak Defense Services



FIGURE 8-1. Outbreak Defense

Outbreak Defense is a combination of services designed to protect and repair your system in the event of an outbreak. Outbreak Defense consists of the following services:

- **Outbreak Prevention Services** - Outbreak Prevention Services protects your system by deploying Trend Micro Outbreak Prevention Policy
- **Outbreak Prevention Policy** - Outbreak Prevention Policy (OPP) is a set of recommended default security configurations and settings designed by TrendLabs to give optimal protection to your computers and network during outbreak conditions.
- **Damage Cleanup Services** - Damage Cleanup Services detects left-over malware and enables users to manually download the Damage Cleanup tool to remove malware.

Current Status

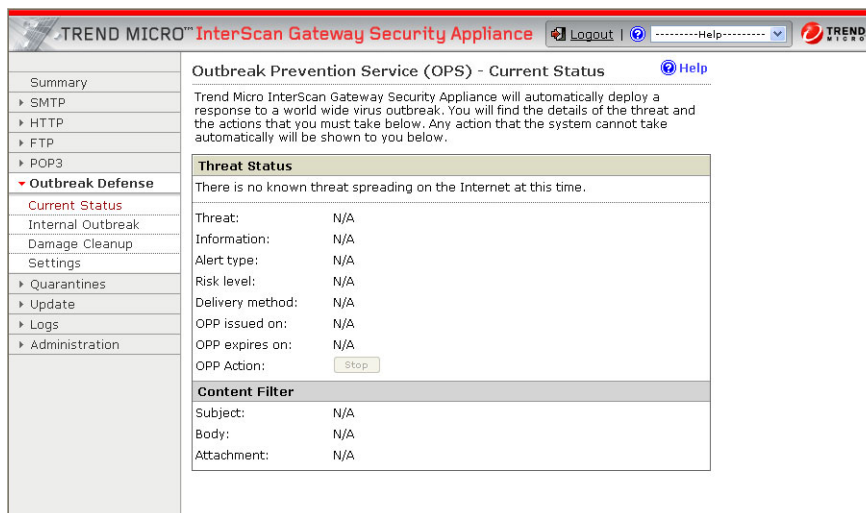


FIGURE 8-2. Outbreak Defense > Current Status

The **Outbreak Defense > Current Status** screen displays information about the status of Outbreak Prevention on the InterScan Gateway Security Appliance. If there is no outbreak, the screen is still viewable, but there is no information regarding the threat, the alert type, or actions for you to take.

The Current Status screen contains the following basic information:

Threat Status - Brief description of the threat

- Threat - Threat name
- Information - Brief description of the vulnerability that the threat exploits
- Alert type - Alert type (Yellow, Red) issued by TrendLabs
- Risk level - Low, Medium, or High
- Delivery method - Brief description about how the threat is propagated
- OPP issued on - When the current Outbreak Prevention Policy was initially deployed

- OPP expires in - Days remaining until the current Outbreak Prevention Policy expires
- OPP action - Click to **Stop** the current OPP
- A list of actions for you to take (in addition to the actions OPP has taken) to protect your device and clients

Content Filter

- Subject – How the threat is labeled in the email Subject field
- Body – The content in the Body of the message lets you create a rule to look for a specific word or words, phrase or sentence
- Attachment – How the threat attachment is usually labeled

Stopping the Outbreak Prevention Policy

Stop the currently deployed Outbreak Prevention Policy when you need to manually deploy a newer Outbreak Prevention Policy or if the actions taken by the policy are having a negative impact on an activity that is critical to your business.

For example, if your business relies heavily on email, the Outbreak Prevention Policy might stop all email traffic if a new outbreak occurs that uses email as the method of delivery. If this situation occurs, you might need to stop the current policy.

Configuring Internal Outbreak



FIGURE 8-3. Outbreak Defense > Internal Outbreak

The **Outbreak Prevention Services (OPS) - Internal Outbreak** screen displays a list of older Outbreak Prevention Policies (OPP). If OPS is not currently running, you can select any one of the OPP items in the list and apply it. If OPS is currently running and TrendLabs issues a new OPP, InterScan Gateway Security Appliance stops the current OPS and moves the OPP to the top of the Outbreak Prevention Policy list. If OPS is currently running and you want to apply an older OPP, you must first manually stop OPS from the Outbreak Defense > Current Status screen.

To apply an older OPP when OPS is not running:

1. From the left-side menu, click **Outbreak Defense > Internal Outbreak**.
2. Select one of the policies to apply. (InterScan Gateway Security Appliance supports running only one policy at a time.)
3. Select how long the policy should be in effect. (The default is 2 days.)
4. Click **Apply Selected OPP**.

Tip: View the Summary screen for the current status of Outbreak Prevention Services.

Configuring Damage Cleanup

The screenshot shows the web interface of the Trend Micro InterScan Gateway Security Appliance. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense (expanded), Current Status, Internal Outbreak, Damage Cleanup (selected), Settings, Quarantines, Update, Logs, and Administration. The main content area is titled 'Potential Threat' and includes a 'Help' link. Below the title is a paragraph explaining that Damage Cleanup detects threats and allows users to download a cleanup tool. The 'Damage Cleanup Setting' section shows 'Enable Damage Cleanup' checked. The 'Damage Cleanup Exception List' section contains a table with columns 'IP/IP range' and 'Address/Range'. An 'Add >>' button is next to the 'IP/IP range' column. Below the table, an example IP range is provided: 'Example: IP range: 10.1.1.0-10.1.1.10'. At the bottom are 'Save' and 'Cancel' buttons.

IP/IP range	Address/Range
	None

Example:
IP range: 10.1.1.0-10.1.1.10

Save Cancel

FIGURE 8-4. Outbreak Defense > Damage Cleanup

InterScan Gateway Security Appliance automatically deploys a response to a worldwide virus outbreak. If a client's outgoing SMTP, FTP, or HTTP traffic contains malware or spyware and InterScan Gateway Security Appliance detects it, the client will be able to download and run the Damage Cleanup Tool to remove the malware or spyware. InterScan Gateway Security Appliance then lists the client in the **Cleaned computers** section of the Summary screen.

You can find the Damage Cleanup Services (DCS) Online Scan at the following URL:

`https://The_appliance_IP/nonprotect/cgi-bin/dcs_manual_cleanup.cgi`

In the URL above, replace **The appliance_IP** with your appliance IP Address.

Potential Threat

A potential threat is any client that has malware or spyware on their computer. As such, they pose a threat to the security of your network.

If InterScan Gateway Security Appliance detects that a client has malware or spyware, it will deploy Damage Cleanup Services on the client's machine.

To configure the Damage Cleanup Setting:

1. From the left-side menu click Outbreak Defense > Damage Cleanup.
2. Select the **Enable Damage Cleanup** check box.
3. Optional - Add non-Windows-based clients to the **Damage Cleanup Exception List** by typing their IP address or the IP address range and clicking **Add**. InterScan Gateway Security Appliance will not deploy Damage Cleanup to clients with IP addresses that are on the **Damage Cleanup Exception List**.
4. Click **Save**.

Note: Damage Cleanup Services only works if the HTTP, SMTP, and FTP protocols and their anti-spyware features are enabled.

Configuring Settings

Configure Outbreak Prevention Policy (OPP) Automatic Deployment and OPP download options (Setting tab). InterScan Gateway Security Appliance sends out a message whenever a new OPP becomes available or an old OPP expires (Notification tab).

Outbreak Defense - Settings

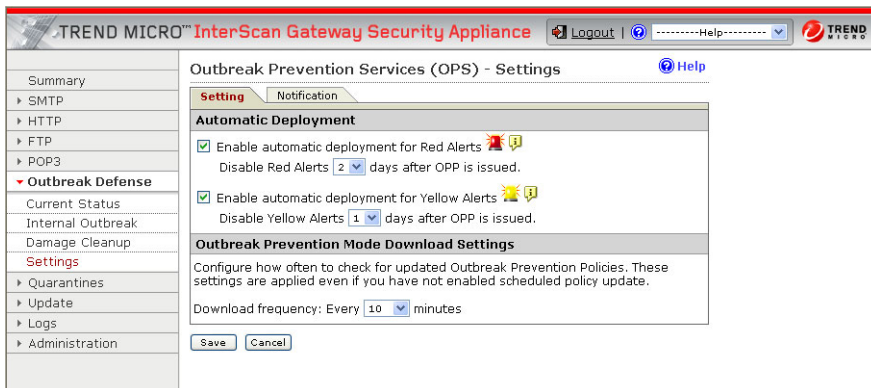


FIGURE 8-5. Outbreak Defense > Settings - Setting

To configure Automatic Deployment and OPP policy download settings:

1. From the left-side menu, click **Outbreak Defense > Settings**. The **Setting** tab appears.
2. Select and configure one or more of the following Automatic Deployment options:
 - Enable automatic deployment for Red Alerts - check to enable automatic deployment of Outbreak Prevention Policies when InterScan Gateway Security Appliance detects an outbreak.
 - Disable OPS alert {number} days after OPP is issued - select the maximum number of days that an OPP is to be in effect. This is useful if the OPP settings are interfering with operations.
 - Enable automatic deployment for Yellow Alerts - check to enable automatic deployment of Outbreak Prevention Policies when InterScan Gateway Security Appliance detects an outbreak.
 - Disable OPS alert {number} days after OPP is issued - select the maximum number of days that an OPP is to be in effect. This is useful if the OPP settings are interfering with operations.

3. Select an OPP download frequency. **Download frequency:** Every {number} minutes - define how often InterScan Gateway Security Appliance checks for updated Outbreak Prevention Policies.
4. Click **Save**.

Outbreak Defense - Notification

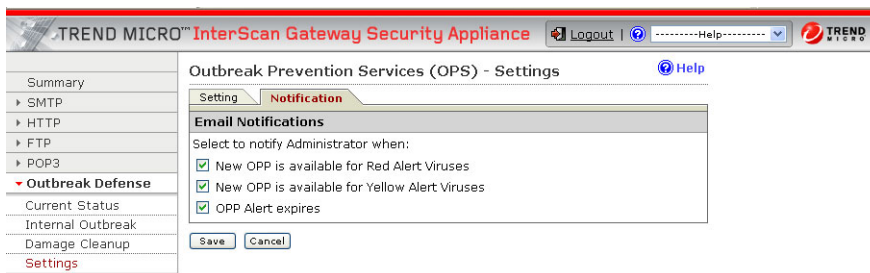


FIGURE 8-6. Outbreak Defense > Settings - Notification

To select OPS – Notification(s):

1. From the left-side menu, click **Outbreak Defense > Settings**.
2. Click the **Notification** tab.
3. Select one or more of the following options:
 - New OPP is available for Red Alert Viruses
 - New OPP is available for Yellow Alert Viruses
 - OPP Alert expires
4. Click **Save**.

Yellow Alerts

Trend Micro issues a Yellow Alert when a threat has been detected “in the wild,” but it is not widespread. TrendLabs then creates and pushes down to deployment servers an official pattern release (OPR). InterScan Gateway Security Appliance can then download the OPR from the deployment servers. Yellow Alerts can trigger Outbreak Defense.

Red Alerts

Trend Micro issues a Red Alert when it receives several reports of virus and malware detection incidents in a short amount of time—that is, the threat is widespread. These reports usually describe a virus or malware threat that is actively circulating on the Internet and spreading to mail servers and computers on local networks. Red Alerts trigger the Trend Micro 45-minute Red Alert solution process. This process includes deploying an official pattern release (OPR) and notifying designated computer security professionals, repressing all other notifications to conserve bandwidth, and posting fix tools and information regarding vulnerabilities to the Trend Micro download pages. Red Alerts can trigger Outbreak Defense.

Quarantines

This chapter describes the Quarantine function in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Quarantines* on page 9-2
- *Conducting a Query* on page 9-3
- *Performing Quarantine Maintenance* on page 9-7

Quarantines



FIGURE 9-1. Quarantines

InterScan Gateway Security Appliance can quarantine email messages that contain viruses, spyware, or bots. Email that has triggered the content filtering rules can also be sent to the quarantine folder.

InterScan Gateway Security Appliance allows you to query the quarantine folder by time, sender, recipient, and subject. You can also perform basic maintenance on the quarantine folder, such as manually deleting email messages or setting a schedule to delete email messages.

WARNING! *The maximum limit for the quarantine folder is 1,000,000 email messages. If you allow the 1,000,000 message quarantine folder limit to be exceeded, InterScan Gateway Security Appliance will not quarantine any new messages that meet the quarantine criteria but instead will apply the Pass action to them.*

Tip: To avoid exceeding the quarantine folder's capacity, perform quarantine maintenance regularly.

Conducting a Query

The screenshot shows the 'Quarantine Query' interface of the Trend Micro InterScan Gateway Security Appliance. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines (selected), Query (highlighted), Maintenance, Update, Logs, and Administration. The main content area is titled 'Quarantine Query' and includes a 'Criteria' section. In the 'Criteria' section, the 'Time period' is set to 'All'. The 'Range' option is selected, with 'From' set to 10/25/2006 and 'To' set to 10/26/2006. Below this, there are input fields for 'Sender:', 'Recipient:', and 'Subject:'. The 'Entries per page' is set to 20. At the bottom of the criteria section are 'Search' and 'Reset' buttons.

FIGURE 9-2. Quarantines > Query

To query the Quarantine folder:

1. From the left-side menu, click **Quarantines > Query**.
2. Under Criteria, set the following options:
 - Time period - select a predefined period of time or specify a range of time
 - Sender - search by sender
 - Recipient - search by recipient
 - Subject - search by subject
 - Entries per page - choose how many entries to display per page

3. Click **Search**. The **Quarantine Query Results** screen appears



FIGURE 9-3. Quarantine Query Results

Note: The Sender, Recipient, and Subject fields are all case insensitive and have partial match capability.

The Quarantine Query Results screen displays a list of quarantined email messages, which can be ordered by Date, Type, Sender, Recipient, and Subject.

To delete messages from the Quarantine Query Results list:

1. Select one or more of the messages to delete.
2. Click the **Delete** link.

To export messages in the list to a comma delimited file:

1. Select one or more of the messages to export.
2. Click the **Export** link.

Tip: Selecting the checkbox next to the Date heading will select all messages.

Viewing the Contents of an Exported Quarantine File

When the user decides to export a query, InterScan Gateway Security Appliance assigns all queried messages a new name and a new “.txt” extension. InterScan Gateway Security Appliance then zips up all the files, including an index file that it creates.

After you unzip the file, you will see a folder that contains a list of files similar to those in the following table. Each file name, except "index.txt", corresponds to a quarantined email message.

TABLE 9-1. Exported query file examples

Example of files displayed in an exported query file
mail_001.txt
mail_002.txt
mail_003.txt
mail_003.txt
mail_004.txt
index.txt

To use the index.txt file to find a specific message:

1. Unzip the exported Quarantine file.
2. Open the unzipped file and double-click **index.txt** to open it.
3. The index.txt file contains a list of file names, similar to those described in the example above, and the corresponding content of the subject line from the original message.
4. Find the subject of the message you wish to open. Next to the subject line content is the name of the file that corresponds to the original message.

In the example below, the user would first look through the index.txt subjects until they found the one they were looking for. They would then make note of the file name associated with it. They would then go back to unzipped folder and

double-click on the file of the same name. The file would then open in whatever text editor program is the default.

TABLE 9-2. Exported query files – example contents

Example of Contents of an index.txt File		Example of Contents of an Exported Quarantine File
File name	Subject line of original message	
mail_003.txt	I'm sick today	mail_001.txt
mail_001.txt	Do you like viruses	mail_002.txt
mail_004.txt	Free spam pizza	mail_003.txt
mail_002.txt	Someone wants to meet you	mail_004.txt
mail_005.txt	This is a virus open it	mail_005.txt

Additional screen actions:

- Click the **Previous** and **Next** arrows in the right-hand corner of the table to scroll through the list of messages.
- Click the drop-down menu next to **Entries per page** to select the number of entries to display per screen.
- Click **Done** to return to the Quarantine Query screen.

Performing Quarantine Maintenance

Performing Quarantine maintenance is very important. The InterScan Gateway Security Appliance Quarantine folder can contain a maximum of 1,000,000 email messages. If you allow the maximum limit to be exceeded, InterScan Gateway Security Appliance applies the pass action to all new messages that meet the quarantine criteria.

Manual

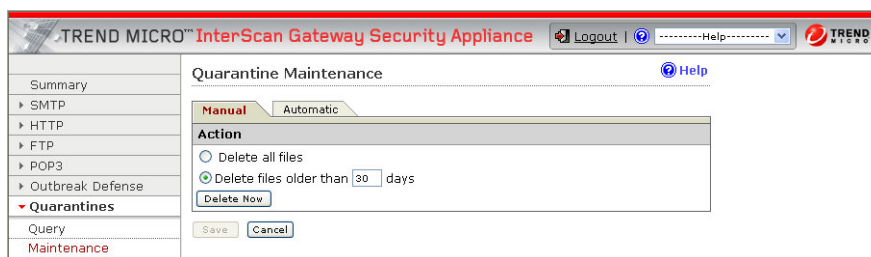


FIGURE 9-4. Quarantine > Maintenance - Manual

To manually delete messages from the Quarantine folder:

1. From the left-side menu, click **Quarantines > Maintenance**. The **Manual** tab appears.
2. Select the email to delete:
 - Delete all files
 Or
 - Type a value in the **Delete files older than {#days}** field (Maximum value is 100).
3. Click **Delete Now**.

Automatic

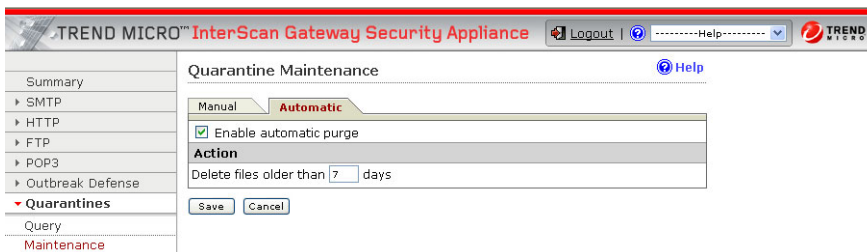


FIGURE 9-5. Quarantine > Maintenance - Automatic

To automatically purge messages from the Quarantine folder:

1. Click the **Maintenance > Automatic** tab.
2. Select the **Enable automatic purge** checkbox.
3. Type a value in the **Delete files older than {#days} days** field.
4. Click **Save**.

Note: The InterScan Gateway Security Appliance will perform an automatic purge every evening at 23:30 local time.

Update

This chapter describes the Update function in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Update* on page 10-2
- *Executing a Manual Update* on page 10-3
- *Configuring Scheduled Updates* on page 10-4
- *Configuring an Update Source* on page 10-6

Update

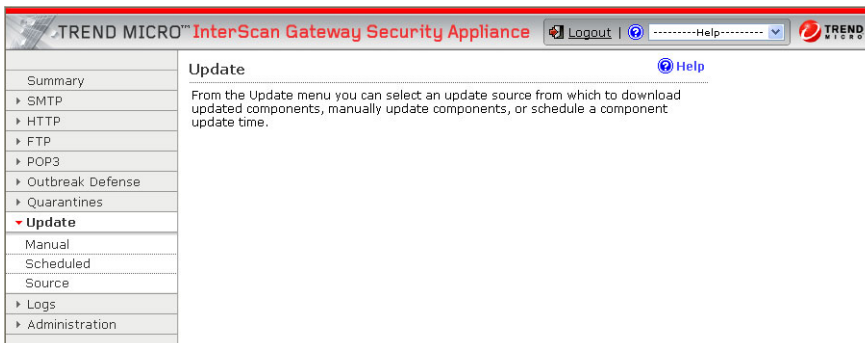


FIGURE 10-1. Update

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

<http://www.trendmicro.com/download/>

When the Update Center screen appears, select your product. Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

From the Update menu you can perform the following tasks:

- Manually update components
- Schedule a time for InterScan Gateway Security Appliance to check for and download updated components
- Designate the Source from which you will receive the updates.

Executing a Manual Update

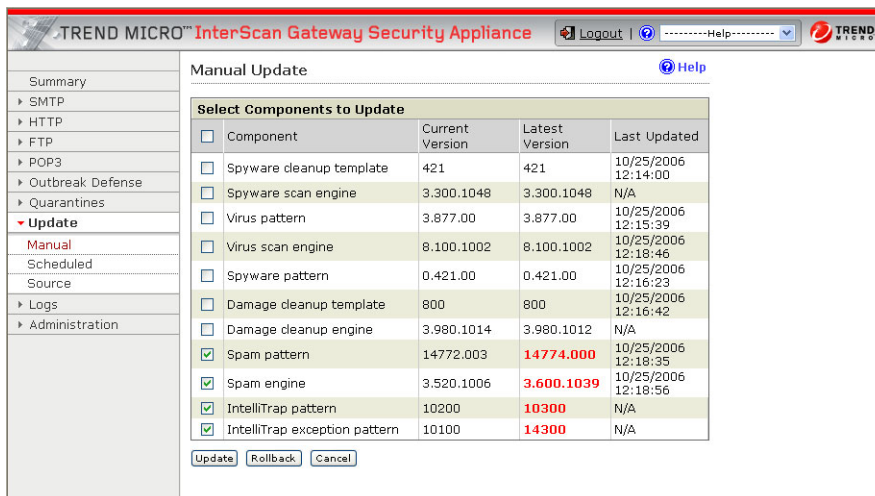


FIGURE 10-2. Update > Manual

To manually update InterScan Gateway Security Appliance components:

1. From the left-side menu, click **Update > Manual**. A progress indicator appears as InterScan Gateway Security Appliance searches for updates, followed by the **Manual Update** screen.
2. Select from the following options for updating components:
 - Component - to select all available components
 Or
 - Select specific components
3. Click **Update**. A progress indicator appears. Depending upon the number of updates selected, InterScan Gateway Security Appliance may take several minutes to update the components.

To roll back components after an Update:

1. From the left-side menu, click **Update > Manual**.
2. Select from the following options for rolling back components:
 - Component - selects all components
 Or
 - Select specific components
3. Click **Rollback**.

Note: Note: You can only roll back components one version. The Rollback feature cannot roll back the device firmware to a previous version.

Configuring Scheduled Updates

TREND MICRO™ InterScan Gateway Security Appliance Logout | Help

Scheduled Update Help

Settings

☒ Enable scheduled updates

Select Components ☒ Select all

☒ Spyware cleanup template ☒ Damage cleanup template

☒ Spyware scan engine ☒ Damage cleanup engine

☒ Virus pattern ☒ Spam pattern

☒ Virus scan engine ☒ Spam engine

☒ Spyware pattern ☒ IntelliTrap pattern

☒ IntelliTrap exception pattern

Update Schedule

Update every: ☐ Minute(s) ☐ Hour(s) ☒ Day(s) ☐ Week, on

1 day(s) at 0 : 00 (hh:mm)

Save Cancel

FIGURE 10-3. Update > Scheduled

To create a schedule for updating InterScan Gateway Security Appliance components:

1. From the left-side menu, click **Update > Scheduled**. The **Scheduled Update** screen appears.
2. Select Enable scheduled updates.
3. Select from the following options for updating components:
 - Select all - selects all componentsOr
 - Select specific components
4. Specify an update duration and frequency.
5. Click **Save**.

Configuring an Update Source

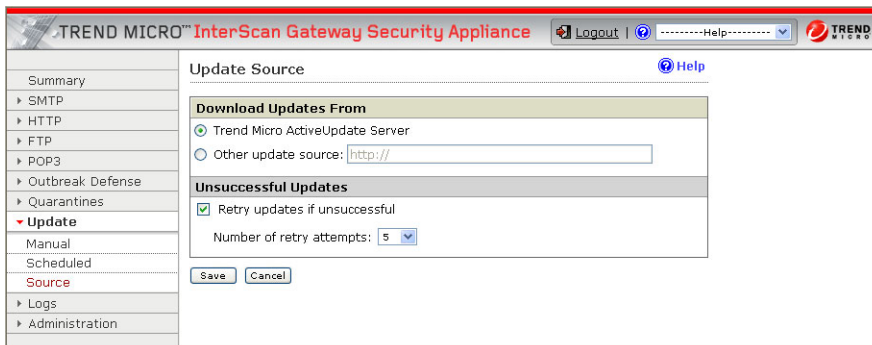


FIGURE 10-4. Update > Source

To configure an Update Source:

1. From the left-side menu, click **Update > Source**. The **Update Source** screen appears.
2. Select and configure one of the following update sources:
 - Trend Micro ActiveUpdate Server (default)Or
 - Other update source: - type the URL for the location of the other update source.
3. Select **Retry updates if unsuccessful** if you want InterScan Gateway Security Appliance to retry the update download.
Number of retry attempts - select the number of times InterScan Gateway Security Appliance should try to download updates.
4. Click **Save**.

Logs

This chapter describes the Log function in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Logs* on page 11-2
- *Performing a Log Query* on page 11-3
- *Configuring Log Settings* on page 11-5
- *Configuring Log Maintenance* on page 11-6

Logs

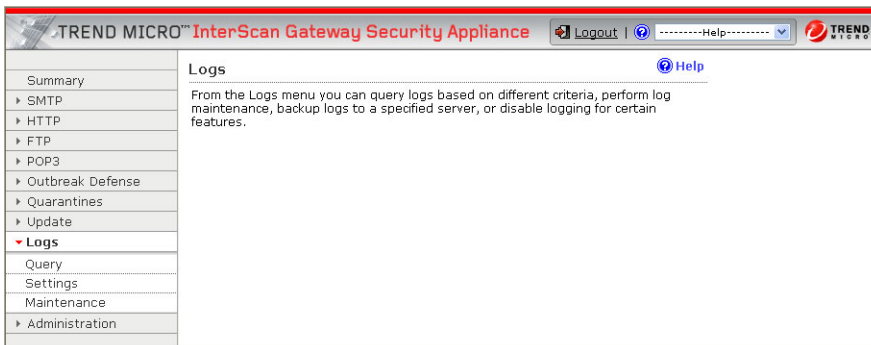


FIGURE 11-1. Logs

InterScan Gateway Security Appliance tracks all scanning and detection activity that it performs and writes this information to various logs. The log query feature allows you to create reports that show detection activity for the different protocols for the various types of scanning tasks that InterScan Gateway Security Appliance performs. The log maintenance feature allows you to perform log maintenance either manually or according to a schedule. You can also view the event log.

Performing a Log Query

The screenshot shows the 'Log Query' interface of the Trend Micro InterScan Gateway Security Appliance. On the left, a navigation menu lists various system functions, with 'Logs' expanded and 'Query' selected. The main content area is titled 'Log Query' and contains a form for configuring a log query. The form includes the following fields and options:

- Log type:** A dropdown menu set to 'Anti-pharming'.
- Protocol:** A dropdown menu set to 'HTTP'.
- Time period:** Radio buttons for 'All' (selected) and 'Range'.
- From:** A date/time picker set to '10/25/2006' at '00:00'.
- To:** A date/time picker set to '10/26/2006' at '00:00'.
- Entries per page:** A dropdown menu set to '20'.
- Display Log:** A button to execute the query.

FIGURE 11-2. Logs > Query

InterScan Gateway Security Appliance tracks all scanning and detection activity that it performs and writes this information to various logs. With the log query feature you can create reports that show detection activity for the different protocols for the various types of scanning tasks that InterScan Gateway Security Appliance performs. You can also view the event log.

To perform a Log Query:

1. From the left-side menu, click **Logs > Query**. The **Log Query** screen appears.
2. Configure the following options:
 - Log type - select the type of log to query
 - Protocol - select a protocol
 - Time period - select one of the predefined query times or specify a range of time to query
 - Entries per page - choose how many entries to display per page

3. Click **Display Log**. The Log screen appears, labeled according to the type of log you have chosen.



FIGURE 11-3. Logs > Query – HTTP Anti-Pharming Log

The column headings displayed in the Query Result screen differ depending on the log type queried.

Additional screen actions

- Click **Export List** on the upper left side of the table to export query results for inclusion in reports.
- Click the log navigation arrows (top and bottom right of the screen) to forward through the list of log entries.
- Click the drop-down menu next to **Entries per page** to select the number of entries to display per screen.
- Click **Done** (bottom left side of the screen) or the **Log Query** link (top left side of the screen) to return to the Log Query screen.

Note: InterScan Gateway Security Appliance does not back up the logs from the device to a remote server. If the send logs to syslog server function is enabled, InterScan Gateway Security Appliance will generate logs on the local log database and send logs to the remote server. If logs are created on the remote server, you will not be able to query them.

Configuring Log Settings



FIGURE 11-4. Logs > Settings

By default InterScan Gateway Security Appliance creates a log for each type of scanning supported. Some scans, such as anti-spam, URL filtering, and NRS can generate a large number of log entries. You can disable logging of these types of scans.

You can configure InterScan Gateway Security Appliance to store log events on a remote device by enabling the Send logs to syslog server feature. The remote device must have syslog software installed. After you have enabled the syslog server feature, logs will be created in both the local log database and the syslog server. Logs generated before enabling the syslog server feature will not be copied to the syslog server.

Note: Log events that are stored on the remote device cannot be queried or maintained from the InterScan Gateway Security Appliance Web console.

When the InterScan Gateway Security Appliance is operating in diskless mode, logs will not be created on the local machine, but if the syslog server feature is enabled, logs will be created on the remote machine.

To configure Log Settings:

1. From the left-side menu, click **Logs > Settings**.
2. Select the Send logs to syslog server check box.

3. Enter the syslog server's IP address and port number in the IP address and Port fields.
4. Click Save.

To configure Log Options (to disable logging):

1. From the left-side menu, click **Logs > Settings**.
2. Clear one or more of the following items to disable logging of those features:
 - Anti-spam: Content Scanning
 - Anti-spam: Network Reputation Services
 - URL filtering
3. Click **Save**.

Configuring Log Maintenance

Configuring log maintenance is a two-step process. First, select the type of logs to delete (Target tab). Next, set the action that InterScan Gateway Security Appliance should take on the selected logs (Action tab). From the Log Maintenance screen you can configure both Manual and Automatic log maintenance.

Manual

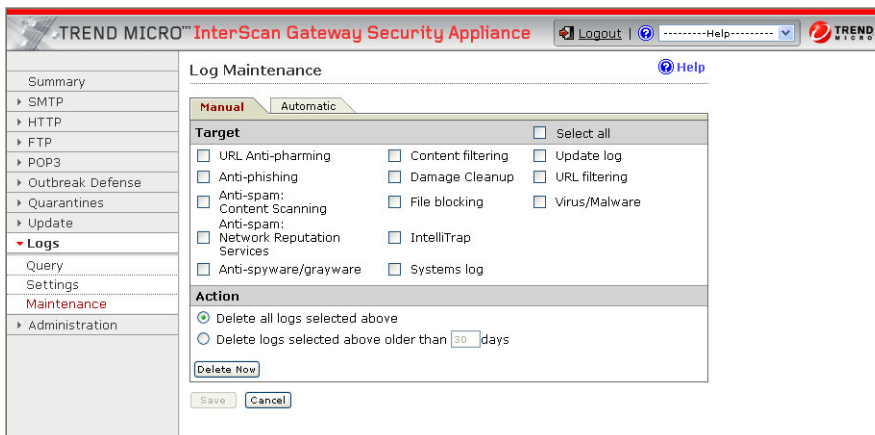


FIGURE 11-5. Logs > Maintenance - Manual

To perform Log Maintenance manually:

1. From the left-side menu, click **Logs > Maintenance**. The **Manual** tab appears.
2. In the **Target** section, select from the following options:
 - Select all - at the far right side of the target section header
 Or
 - Select one or more of the predefined log categories.
3. In the **Action** section, select one of the following options:
 - Delete all logs selected above
 Or
 - Delete logs selected above older than {#days} days - type a value in the {#days} field (Maximum value is 100).
4. Click **Delete Now**.

Automatic

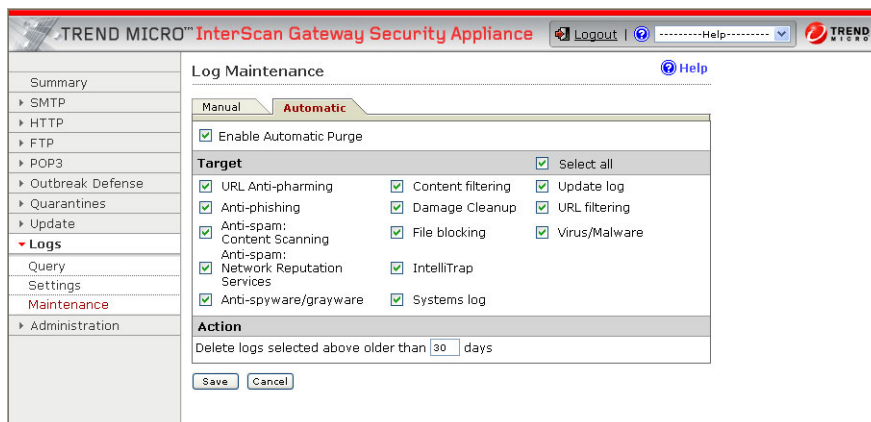


FIGURE 11-6. Logs > Maintenance - Automatic

To perform Log Maintenance automatically:

1. From the left-side menu, click **Logs > Maintenance**. The **Manual** tab appears.
2. Click the **Automatic** tab. The Automatic tab appears.
3. Select the **Enable automatic purge** check box.
4. In the **Target** section, select from the following options:
 - Select all - at the far right side of the target section headerOr
 - Select one or more of the predefined log categories.
5. In the **Action** section, type a value in the **Delete logs selected above older than {#days} days** field (Maximum value is 100).
6. Click **Save**.

Note: Logs that meet the specified purge criteria are deleted nightly at 23:45.

Administration

This chapter describes the Administration functions in InterScan Gateway Security Appliance. Topics discussed in this chapter include:

- *Administration* on page 12-2
- *Access Control* on page 12-3
- *Configuration Backup* on page 12-4
- *Disk SMART Test* on page 12-5
- *IP Address Settings* on page 12-6
- *Notification Settings* on page 12-11
- *Operation Mode* on page 12-14
- *Password* on page 12-15
- *Product License* on page 12-16
- *Proxy Settings* on page 12-19
- *SNMP Settings* on page 12-20
- *System Time* on page 12-22
- *World Virus Tracking* on page 12-23

Administration



FIGURE 12-1. Administration

From the Administration menu you can configure many InterScan Gateway Security Appliance operational settings, access different InterScan Gateway Security Appliance tools, and view Product License and World Virus Tracking details.

Access Control



FIGURE 12-2. Administration > Access Control

The Access Control screen allows administrators to access the InterScan Gateway Security Appliance Web console from the Internet.

To enable Access Control:

1. From the left-side menu, click **Administration > Access Control**.
2. Select the **Enable external access** check box.
3. Click **Save**.

Configuration Backup

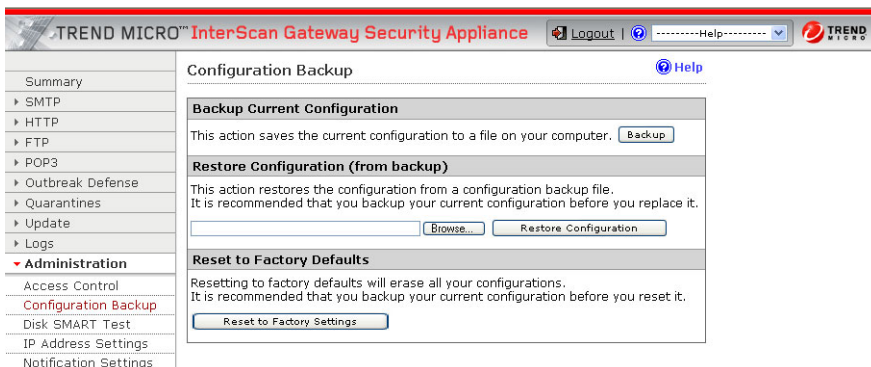


FIGURE 12-3. Administration > Configuration Backup

To back up current Configuration settings:

1. From the left-side menu, click **Administration > Configuration Backup**.
2. In the Backup Current Configuration section, click **Backup**. A Windows dialog appears, asking if you want to open or save the current configuration file onto your computer.

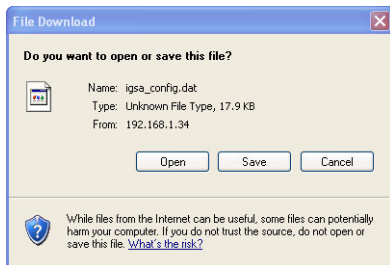


FIGURE 12-4. Windows Save Dialog

3. Click **Save** to open a Save window.
4. Navigate to the folder in which you wish to save the file and click **Save**.

To restore Configuration settings from a backup file:

1. From the left-side menu, click **Administration > Configuration Backup**.
2. From the **Restore Configuration (from backup)** section, click **Browse** to find a configuration file.
3. Click **Restore Configuration**.

To reset Configuration to factory default settings:

1. From the left-side menu, click **Administration > Configuration Backup**.
2. Click **Reset to Factory Settings**.

Disk SMART Test

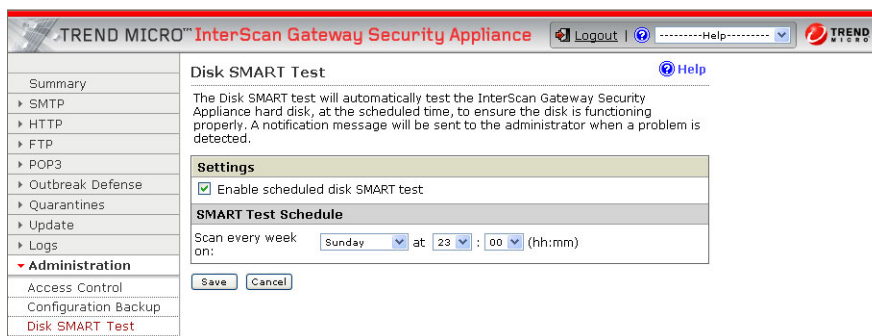


FIGURE 12-5. Administration > Disk SMART Test

The Disk SMART Test scans the device hard disk to ensure that it is functioning properly. If the SMART test detects a problem with the hard disk, InterScan Gateway Security Appliance will automatically reboot and begin operating in diskless mode. The Disk SMART Test runs automatically when InterScan Gateway Security Appliance is started. A Disk SMART Test can also be scheduled from the left-side menu Administration menu item. The results of a Disk SMART test can be viewed in the system logs.

To configure the Disk SMART Test utility:

1. From the left-side menu, click **Administration > Disk SMART Test**.
2. Select the Enable scheduled disk SMART test check box.
3. Configure the SMART Test Schedule.
4. Click **Save**.

IP Address Settings

InterScan Gateway Security Appliance uses the IP address and host name when communicating with other computers or servers and when checking for component and firmware updates. Anti-spam, content filtering, and URL filtering are dependent on the settings in this screen.

Management IP Address

TREND MICRO™ InterScan Gateway Security Appliance

Logout | Help

Summary

- SMTP
- HTTP
- FTP
- POP3
- Outbreak Defense
- Quarantines
- Update
- Logs
- Administration**
 - Access Control
 - Configuration Backup
 - Disk SMART Test
 - IP Address Settings**
 - Notification Settings
 - Operation Mode
 - Password
 - Product License
 - Proxy Settings
 - SNMP Settings
 - System Time
 - World Virus Tracking

IP Address Settings

Management IP Address | Static Routes

Host Name

Hostname: dheppc1

IP Address Management

☒ Dynamic IP address (DHCP)

IP Address: 192.168.1.34

Netmask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server 1: 192.168.1.1

DNS Server 2: N/A

☐ Static IP address

IP Address:

Netmask:

Gateway:

DNS Server 1:

DNS Server 2:

Save Cancel

FIGURE 12-6. Administration > IP Address Settings – Management IP Address

To configure the IP address that InterScan Gateway Security Appliance uses to check for component and firmware updates:

1. From the left-side menu, click **Administration > IP Address Settings**. The Management IP Address tab appears.

Host Name

2. Type a Host name in the **Hostname** field.

This is the name of the InterScan Gateway Security Appliance. Some mail servers require a host name to accept incoming mail.

IP Address Management

InterScan Gateway Security Appliance uses the IP address when checking for component and firmware updates.

- Dynamic IP address (DHCP)

Or

- Static IP address

3. If you choose to use a Static IP Address, select **Static IP address** and enter the following:
 - IP Address – the IP address that InterScan Gateway Security Appliance uses
 - Netmask - Required
 - Gateway - Required
 - DNS Server 1 - primary - Required
 - DNS Server 2 - secondary - Optional

4. Click **Save**.

Static Routes

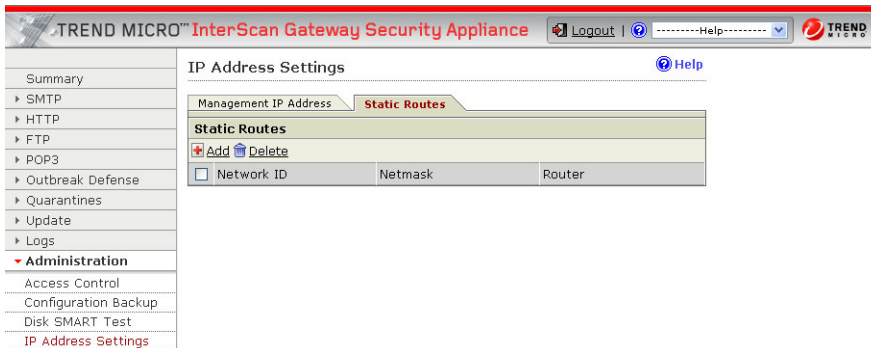


FIGURE 12-7. Administration > IP Address Settings – Static Routes

Static routes are special routes that the network administrator manually enters into the InterScan Gateway Security Appliance configuration. Static routes help InterScan Gateway Security Appliance route traffic to clients or segments within the protected network. The IP Address Settings - Static Routes screen displays a list of InterScan Gateway Security Appliance static routes. From the Static Routes screen, administrators can add, delete, or modify static routes.

To add a Static Route:

1. From the left-side menu, click Administration > IP Address Settings.
2. Click the **Static Routes** tab.

3. Click **Add**. The **Add Static Route** screen appears.

FIGURE 12-8. Add Static Routes

4. Enter a value for the Network ID - The network address.
5. Enter a value for the Netmask - Netmask for the network ID.
6. Enter a value for the Router – This is the IP address of the router used to route traffic to a specific network segment as specified by the Network ID and Netmask.
7. Click **Save**.

To modify a Static Route:

1. From the left-side menu, click Administration > IP Address Settings.
2. Click the **Network ID** link, the **Modify Static Route** screen appears with the current values.
3. Enter a value for the Network ID.
4. Enter a value for the Netmask.
5. Enter a value for the Router.
6. Click **Save**.

To delete a Static Route:

1. From the left-side menu, click **Administration > IP Address Settings**.
2. Select one or more static routes from the **Static Routes** table.
3. Click **Delete**.

An example of InterScan Gateway Security Appliance static routes settings for a multiple segment network is given below. The example below also applies to single segment networks.

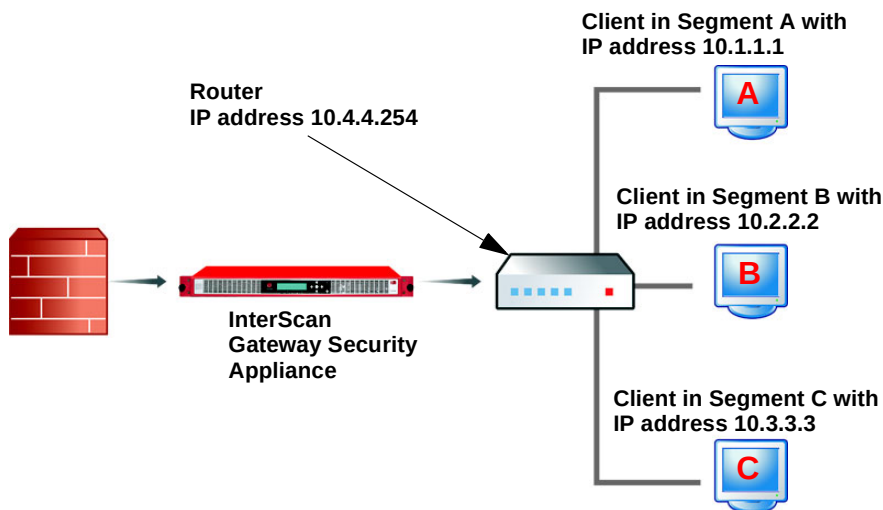


FIGURE 12-9. Static Routes – Multiple Segment Network

TABLE 12-1. Static routes – example settings

Static Route Fields for Segment A	Example Settings
Network ID	10.1.1.0
Netmask	255.255.255.0
Router	10.4.4.254
Static Route Fields for Segment B	Example Settings
Network ID	10.2.2.0
Netmask	255.255.255.0
Router	10.4.4.254
Static Route Fields for Segment C	Example Settings
Network ID	10.3.3.0
Netmask	255.255.255.0
Router	10.4.4.254

Notification Settings

Configure the settings InterScan Gateway Security Appliance is required to use when sending out notifications (Settings tab). InterScan Gateway Security Appliance will send notifications each time an event occurs, up to the number specified by the administrator in the Events screen (Events tab).

Settings

The screenshot shows the Trend Micro InterScan Gateway Security Appliance Administration web interface. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, Administration (highlighted with a red arrow), Access Control, Configuration Backup, Disk SMART Test, IP Address Settings, Notification Settings (highlighted in red), and Operation Mode. The main content area is titled 'Notification' and has a 'Help' link. It contains two tabs: 'Settings' (active) and 'Events'. The 'Settings' tab displays instructions for email notifications and fields for SMTP server, port, user name, and password. Below these is a section for 'Administrator Email Address(es)' with a text input field and a note to use semicolons for multiple addresses. 'Save' and 'Cancel' buttons are at the bottom.

TREND MICRO™ InterScan Gateway Security Appliance	
- Summary ▶ SMTP ▶ HTTP ▶ FTP ▶ POP3 ▶ Outbreak Defense ▶ Quarantines ▶ Update ▶ Logs ▼ Administration - Access Control - Configuration Backup - Disk SMART Test - IP Address Settings Notification Settings - Operation Mode	Notification Help Settings Events The following settings will be used when sending email notifications from InterScan Gateway Security Appliance. SMTP server: 127.0.0.1 Port: 25 Enter the user name and password to be used when sending notification from InterScan Gateway Security Appliance. SMTP user name: SMTP password: Administrator Email Address(es) Email address: Use a semicolon ";" to separate multiple addresses Save Cancel

FIGURE 12-10. Administration > Notification Settings - Settings

To configure the settings that InterScan Gateway Security Appliance will use when sending notifications:

1. From the left-side menu, click **Administration > Notification Settings**. The **Settings** tab appears.
2. SMTP server - Type the SMTP server name or IP address in the **SMTP Server** field.
3. Port - Type the SMTP server port number in the **Port** field.
4. SMTP user name - Type the SMTP server user name in the **SMTP user name** field. Depending on the SMTP server requirements, this could be optional.
5. SMTP password - Type the SMTP server password in the **SMTP password** field. Depending on the SMTP server requirements, this could be optional.
6. Type one or more administrator email addresses in the **Email address** field. Use a semicolon to separate multiple address.
7. Click **Save**.

Events

The screenshot shows the Trend Micro InterScan Gateway Security Appliance Administration web interface. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, Administration (expanded), Access Control, Configuration Backup, Disk SMART Test, IP Address Settings, and Notification Settings (highlighted in red). The main content area is titled 'Notification' and contains two tabs: 'Settings' and 'Events' (selected). Under the 'Events' tab, there is a form with the label 'Maximum notifications per hour:' followed by a text input field containing the value '50' and a note '(0:no limit)'. At the bottom of the form are 'Save' and 'Cancel' buttons. The top of the interface includes a header with 'TREND MICRO™ InterScan Gateway Security Appliance', a 'Logout' link, a help icon, a 'Help' dropdown menu, and the Trend Micro logo.

FIGURE 12-11. Administration > Notification Settings - Events

To configure the maximum number of notifications InterScan Gateway Security Appliance will send out per hour:

1. From the left-side menu, click Administration > Notification Settings.
2. Click the **Events** tab.
3. In the **Maximum notifications per hour** field type the maximum number of notification per hour that InterScan Gateway Security Appliance can send (default is 50).
4. Click **Save**.

Operation Mode

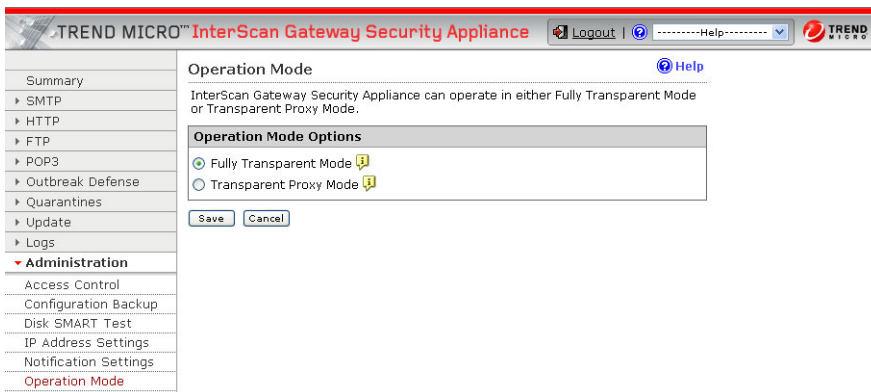


FIGURE 12-12. Administration > Operation Mode

InterScan Gateway Security Appliance can be configured to act as a bridge or a router.

To configure what mode InterScan Gateway Security Appliance should operate in:

1. From the left-side menu, click Administration > Operation Mode.
2. Select a mode:
 - Fully Transparent Mode - destination server sees the client's IP address

Or

 - Transparent Proxy Mode - destination server sees the IP address of InterScan Gateway Security Appliance
3. Click **Save**.

Note: If you have a firewall in your network, you may need to modify the firewall rules to allow InterScan Gateway Security Appliance to access the Internet. If you use Transparent Proxy Mode, you will not be able control Internet access on a per user basis.

Password

FIGURE 12-13. Administration > Password

The default InterScan Gateway Security Appliance console password was chosen at the time of installation. After logging on to the InterScan Gateway Security Appliance Web console, you can change the password at any time. Only one password is supported (there are no multiple accounts).

Note: Passwords should be a mixture of alphanumeric characters from 4 to 32 characters long. Avoid dictionary words, names, and dates.

To change the InterScan Gateway Security Appliance Web console password:

1. From the left-side menu, click **Administration > Password**.
2. In the **Old password** field, type the console's current password.
3. In the **New password** field, type a new password.
4. In the **Confirm password** field, type the same password as entered in the **New password** field.
5. Click **Save**.

Product License

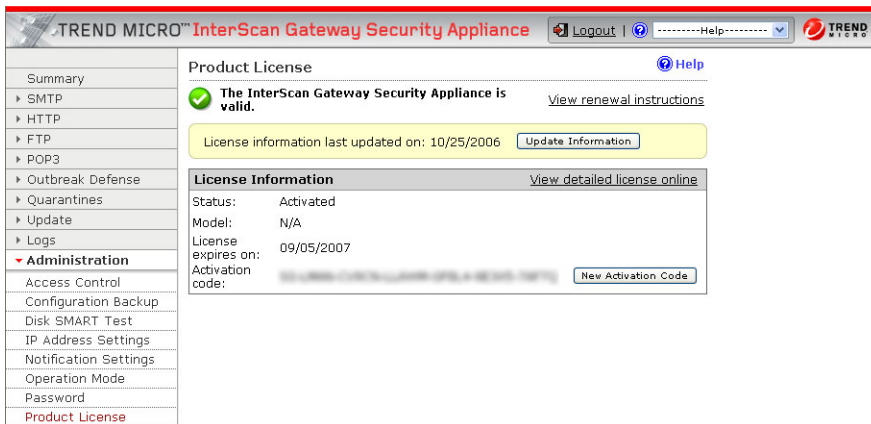


FIGURE 12-14. Administration > Product License

To view license renewal instructions:

1. Select **Administration > Product License** to display the Product License screen.
2. Click **View renewal instructions**. InterScan Gateway Security Appliance opens a browser window on the Renewal Instructions screen.

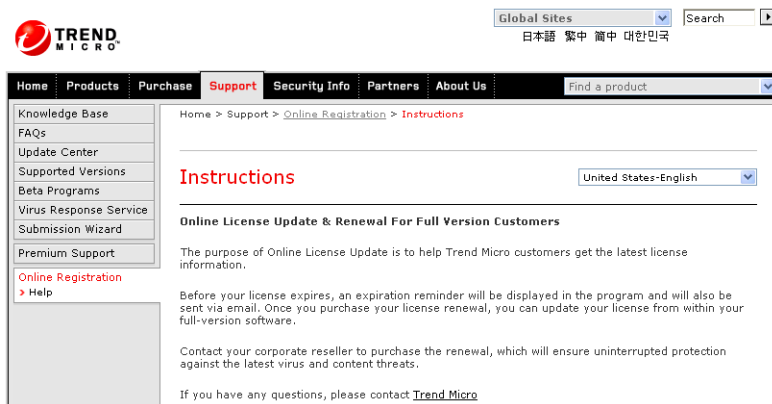


FIGURE 12-15. Online License Update & Renewal

3. Follow the instructions that appear.

To view detailed information about your license:

1. Select **Administration > Product License** to display the Product License screen.
2. To the right of License Information, click **View detailed license online**. A **My Product Details** browser window opens, displaying your license information.

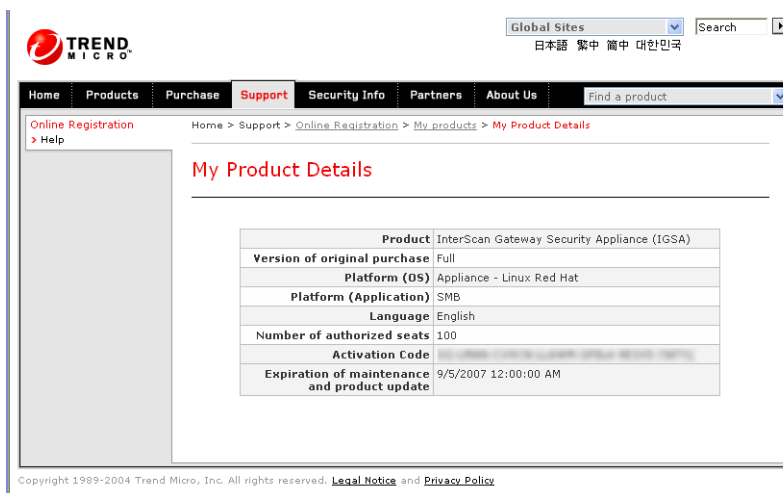


FIGURE 12-16. My Product Details

Note: InterScan Gateway Security Appliance supports automatic online updates as long as the Activation Code has not expired.

To perform online Updates for the product license manually:

1. Check the network status, and proxy settings.
2. Select **Administration > Product License** to display the Product License screen.
3. Click **Update Information**.

To enter a new activation code:

1. Select **Administration > Product License** to display the Product License screen.
2. Click **New Activation Code**. The **New Activation Code** screen appears.



The screenshot shows the Trend Micro InterScan Gateway Security Appliance M-Series Administrator's Guide. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, Administration (highlighted with a red arrow), Access Control, Configuration Backup, Disk SMART Test, IP Address Settings, Notification Settings, Operation Mode, Password, Product License (highlighted with a red box), Proxy Settings, SNMP Settings, System Time, and World Virus Tracking. The main content area is titled 'Product License' and includes a 'Help' link. Below the title, there is a section for 'New Activation Code' with the following fields: Product (Interscan Gateway Security Appliance), Current status (Activated), Current activation code (a blurred field), and New activation code (a text input field). The 'New activation code' field is highlighted with a red box. At the bottom of the form, there are 'Save' and 'Cancel' buttons.

FIGURE 12-17. Administration > Product License - New Activation Code

3. Type the new activation code in the **New activation code** field
4. Click **Save**.

Proxy Settings

The screenshot shows the 'Proxy Settings' page within the Trend Micro InterScan Gateway Security Appliance Administration interface. The left sidebar contains a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, Administration (selected), Access Control, Configuration Backup, Disk SMART Test, IP Address Settings, Notification Settings, Operation Mode, Password, Product License, and Proxy Settings (highlighted). The main content area is titled 'Proxy Settings' and includes a 'Help' link. The settings are as follows:

- ☒ Use a proxy server for pattern, engine, and license updates
- Proxy protocol: ☒ HTTP ☐ SOCKS4 ☐ SOCKS5
- Server name or IP address:
- Port:
- Proxy server authentication:
 - User ID:
 - Password:
 -

At the bottom of the settings area are 'Save' and 'Cancel' buttons.

FIGURE 12-18. Administration > Proxy Settings

If you use a proxy server to connect to the Internet, specify the proxy settings. InterScan Gateway Security Appliance needs the proxy information to:

- Update pattern/engine files
- Update license information
- Send virus logs to the World Virus Tracking (WTC) server
- Download Outbreak Prevention Services (OPS) rules from the OPS server

To configure Proxy Settings:

1. From the left-side menu, click Administration > Proxy Settings.
2. Select the Use a proxy server for pattern, engine, and license updates check box to enable.
3. Choose a proxy protocol by selecting one of the following options:
 - HTTP
 - SOCKS4
 - SOCKS5
4. Specify the proxy server name or IP address and port number.

5. If your proxy server needs authentication, type a valid user ID and password.
6. Click **Test Connection**. If the settings are correct, you will receive a verification notice.
7. Click **Save**.

SNMP Settings

The screenshot displays the 'Administration > SNMP Settings' page of the Trend Micro InterScan Gateway Security Appliance. The left sidebar contains a navigation menu with options like Summary, SMTP, HTTP, FTP, POP3, Outbreak: Defense, Quarantines, Update, Logs, and Administration (which is expanded to show sub-options like Access Control, Configuration Backup, Disk SMART Test, IP Address Settings, Notification Settings, Operation Mode, Password, Product License, Proxy Settings, **SNMP Settings**, System Time, and World Virus Tracking). The main content area is titled 'SNMP Settings' and includes a 'Help' link. It is divided into three sections: 'SNMP Trap' with a checked 'Enable SNMP trap' option and fields for 'Community name' and 'Server IP address'; 'SNMP Agent' with an unchecked 'Enable SNMP agent' option and fields for 'System location' and 'System contact'; and 'Accepted Community Names' and 'Trusted Network Management IP Address(es)' sections, each featuring a list box for adding entries and a table with 'Community Name' or 'IP Address' and 'None' as the default value. At the bottom are 'Save' and 'cancel' buttons.

FIGURE 12-19. Administration > SNMP Settings

InterScan Gateway Security Appliance sends Notifications to one or more administrators or other specified recipients using Simple Network Management Protocol (SNMP).

To configure SNMP Settings:

1. From the left-side menu, click Administration > SNMP Settings.
2. Enable and configure SNMP Trap.
 - Select the **Enable SNMP trap** check box to enable the SNMP Trap.
 - Community name - type the SNMP server community name.
 - Server IP address - type the SNMP server IP address.
3. Enable and configure an SNMP agent.
 - Select the **Enable SNMP agent** check box to enable the SNMP Agent.
 - System location - physical location of the computer/server that contains the SNMP agent (software module). For example, Bottom Floor of building, room 44
 - System contact - email address of person responsible for maintenance of the computer/server that contains the SNMP agent (software module). For example, Admins@email.address.
 - [Optional]: Accepted Community Names - type the community name of a trusted SNMP server.
 - [Optional]: Trusted Network Management IP Address(es) - type the IP address of a trusted SNMP server.
4. Click **Save**.

System Time

TREND MICRO™ InterScan Gateway Security Appliance Logout | ? Help

System Time Settings [Help](#)

Synchronize InterScan Gateway Security Appliance time with an NTP server.

NTP Setting

NTP Server:

Time zone:

Regional Setting

Region/Country:

Left-side menu:

- Summary
- SMTP
- HTTP
- FTP
- POP3
- Outbreak Defense
- Quarantines
- Update
- Logs
- Administration**
 - Access Control
 - Configuration Backup
 - Disk SMART Test
 - IP Address Settings
 - Notification Settings
 - Operation Mode
 - Password
 - Product License
 - Proxy Settings
 - SNMP Settings
 - System Time**
 - World Virus Tracking

FIGURE 12-20. Administration > System Time

To configure System Time:

1. From the left-side menu, click **Administration > System Time**.
2. Enter the IP address of an NTP server in the **NTP Server** field.
3. Select a time zone from the **Time zone** drop-down menu.
4. Select a Region/Country from the **Region/Country** drop-down menu.
5. Click **Save**.

World Virus Tracking

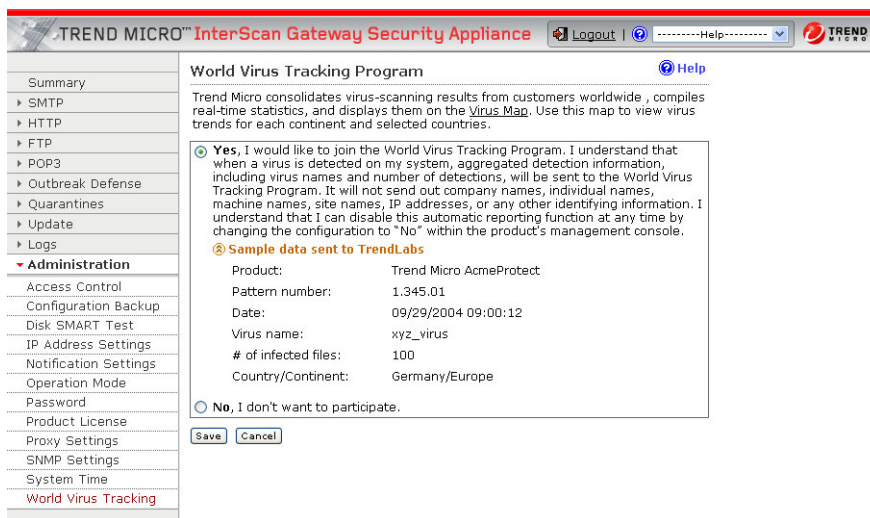


FIGURE 12-21. Administration > World Virus Tracking

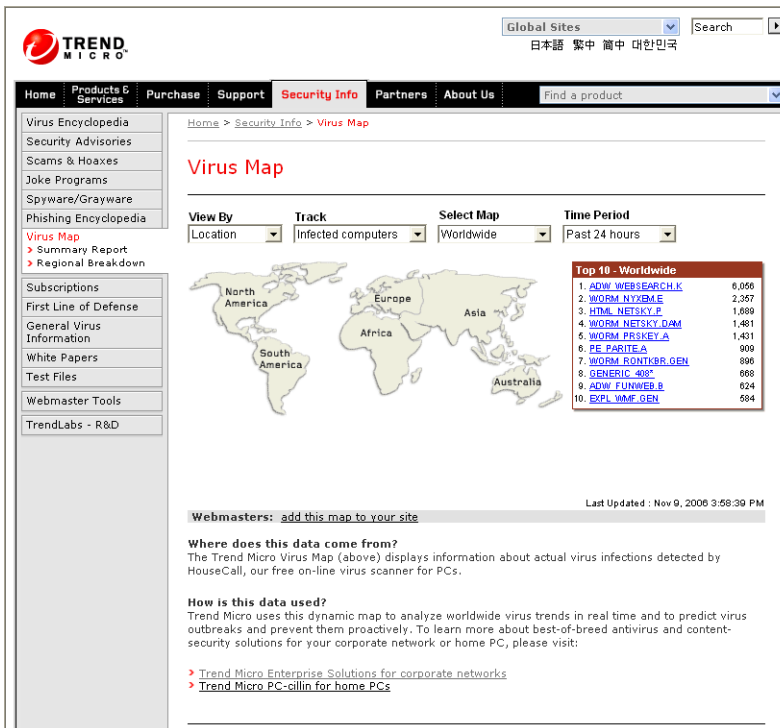
The Trend Micro World Virus Tracking Program collects Internet threat data from tens of thousands of corporate and individual computer systems around the world.

To participate in the World Virus Tracking Program:

1. From the left-side menu, click **Administration > World Virus Tracking**.
2. Choose “Yes, I would like to join....”
Or
Choose “No, I don’t want to participate.”
3. Click **Save**.

To view the Trend Micro Virus Map:

1. From the left-side menu, click **Administration > World Virus Tracking**.
2. Click the **Virus Map** link. A browser opens, showing the Trend Micro Virus Map, with the **Top 10 - Worldwide** viruses listed.

**FIGURE 12-22. Virus Map**

3. Position your mouse over a region to see the top 10 viruses for that region.
4. Use the **View By**, **Track**, **Select Map** and **Time Period** pop-ups to obtain various views of the Virus Map.

Technical Support, Troubleshooting, FAQ

This chapter provides a set of technical resources for the InterScan Gateway Security Appliance administrator. Topics discussed in this chapter include:

- *Contacting Technical Support* on page 13-2
- *Troubleshooting* on page 13-4
- *Frequently Asked Questions (FAQ)* on page 13-4
- *Recovering a Password* on page 13-6
- *Virus Pattern File* on page 13-7
- *Spam Engine and Pattern File* on page 13-8
- *Hot Fixes, Patches, and Service Packs* on page 13-8
- *Licenses* on page 13-9
- *Renewing Maintenance* on page 13-10
- *EICAR- Test Virus* on page 13-11
- *Best Practices* on page 13-12

Contacting Technical Support

Trend Micro provides virus pattern downloads and program updates for one year to all registered users, after which you must renew your license to continue receiving these downloads and updates. Trend Micro also provides technical support (collectively "Maintenance") in certain regions. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users.

Get a list of the worldwide support offices:

<http://esupport.trendmicro.com/>

Get the latest Trend Micro product documentation:

<http://www.trendmicro.com/download>

In the United States, you can reach the Trend Micro representatives via phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.
Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email: support@trendmicro.com

Contact Links

<mailto:virusresponse@trendmicro.com>

<mailto:support@trendmicro.com>

<https://olr.trendmicro.com/registration/>

<http://www.trendmicro.com/vinfo/>

<http://www.trendmicro.com/support>

<http://www.trendmicro.com/download/engine.asp>

<http://esupport.trendmicro.com/support/>

<http://www.trendmicro.com/download/>

<http://www.trendmicro.com>

<http://subwiz.trendmicro.com/subwiz>

Readme.txt

When you install a new product, upgrade an existing product, or apply a patch or hot fix for an existing product, be sure to review the information in the readme provided. Trend Micro readme documents are written using the following outline of topics:

1. **Overview**—Brief description of the product
2. **What's New**—Summary of changes available with this release, upgrade, or patch/hot fix
3. **Documentation Set**—Summary of documentation available for the product
4. **System Requirements**—List of hardware and software required to install and use the product
5. **Installation**—High-level steps for installing the software, upgrade, or patch/hot fix
6. **Post-Installation Configuration**—Steps required after installation is complete, if any
7. **Known Issues**—Description of known issues and work-arounds, if any
8. **Release History**—List of previous releases of this product
9. **Contact Information**—Information about how to contact Trend Micro
10. **About Trend Micro**—Brief description of Trend Micro and a list of copyrights
11. **License Agreement**—Where to find information about your license agreement with Trend Micro (omitted from beta readme.txt)

Troubleshooting

I Can See the Console Output on the HyperTerminal but Some Keystrokes Do Not Work

Cause—The HyperTerminal settings are incorrect or need refreshing.

Solution—Change the HyperTerminal emulation setting to something other than VT100J and then change it back. If the problem persists, you can close HyperTerminal and connect again.

The LCM Displays “[Error] No Connection”

Cause—InterScan Gateway Security Appliance is having a problem connecting to the DHCP server.

Solution—First check that the Ethernet cables are connected. By default, InterScan Gateway Security Appliance uses a dynamic IP address from a DHCP server. Make sure that InterScan Gateway Security Appliance can connect to the DHCP server to get a valid IP address. Use another device and try to obtain an IP from the DHCP server, or change the InterScan Gateway Security Appliance IP address to static.

The Device Does Not Turn off When I Press the Power Switch

Cause—The power switch is not being held down long enough.

Solution—**The power switch has to be pressed for at least 4 seconds.** This is designed so as to avoid an accidental shutdown.

Frequently Asked Questions (FAQ)

Review these frequently asked questions for insight into issues that many users ask about.

What Is the Purpose of the “ID” LED?

The ID LED helps users identify a specific InterScan Gateway Security Appliance in a rack containing many devices. There are two ID LEDs. One is at the front of the device, and the other is at the back of the device.

Can I Use the USB Ports to Transfer Files to and from InterScan Gateway Security Appliance?

No, the USB ports are not enabled in this version. They are for future hardware extensibility.

Will InterScan Gateway Security Appliance Still Operate If the Hard Disk Is Not Working?

Yes, when the hard disk is not working or not working properly, InterScan Gateway Security Appliance will reboot into diskless mode. In diskless mode, InterScan Gateway Security Appliance still scans for threats, but some features are disabled, for example, product updates, event logging, version rollbacks, item quarantine, and Outbreak Prevention Services. Additionally, InterScan Gateway Security Appliance scanning performance is decreased.

Does the “RESET” Pinhole Reset InterScan Gateway Security Appliance to the Factory Default Settings?

No, the “RESET” pinhole just restarts the device and does not modify any configuration settings.

Is a Crossover Network Cable Needed to Connect InterScan Gateway Security Appliance to Another Network Device?

No, a common RJ-45 Ethernet cable is enough because the device has an auto-switching/sensing capability.

Can I Ping InterScan Gateway Security Appliance?

Yes, InterScan Gateway Security Appliance accepts ping packets.

Why Am I Not Receiving Email Notifications?

Using the Web console left navigation menu, go to **Administration > Notification Settings** and verify that the information is complete and correct.

Why Is Traffic Not Passing Through the Device When the Power Is Off?

It is possible that the "DC OFF LAN Bypass Configuration" setting in the BIOS is "disabled." To enable "DC OFF LAN Bypass" prepare a computer with terminal communications software such as HyperTerminal. Connect the computer to the device. Reboot the device and, during the initialization process, enter the BIOS configuration by pressing "Delete." Enable "DC OFF LAN Bypass." This will allow traffic to pass

through the device when there is no direct current. InterScan Gateway Security Appliance comes with "DC ON LAN Bypass" and "DC OFF LAN Bypass" enabled by default.

Why Does the Quarantine Action Fail?

There are three (3) situations that will cause the quarantine action to fail:

- The number of quarantined messages exceeds 1,000,000
- The message that is being quarantined is larger than 100MB
- The total size of all quarantined messages is larger than 16GB

The InterScan Gateway Security Appliance will apply the pass action if the quarantine action fails.

Recovering a Password

How Can I Recover a Lost or Forgotten Password?

There is currently no way to recover a lost or forgotten password without reinstalling the InterScan Gateway Security Appliance “image” to a previous configuration—one in which the password was known. This may be done

1. From a backup
Or
2. By restoring the default configuration, which eliminates all user-customized settings and returns the password to “admin”.

Administrators are therefore encouraged to periodically back up the device configuration.

To backup the device configuration:

1. From the left-side menu, click **Administration > Configuration Backup**.
2. Click **Backup**. A dialog appears, letting you save the backup file to your computer.

To restore a configuration from a backup:

1. From the left-side menu, click Administration > Configuration Backup.
2. Click **Browse** to locate the backup file.
3. Click **Restore Configuration** to restore the device to your backup.
4. Change the password to one that users prefer.

To restore the default configuration:

Please refer to the [InterScan Gateway Security Appliance M-Series Getting Started Guide](#) for details on the procedure.

Virus Pattern File

As new viruses and other Internet threats are written, released to the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the virus and other pattern files.

Trend Micro updates the file as often as several times a week, and sometimes several times a day when people release multiple variants of a widespread threat. By default, InterScan Gateway Security Appliance checks for updates no less often than once a week. If a particularly damaging virus is discovered “in the wild,” or actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available (usually within a few hours).

Note: Pattern file and scan engine updates are only available to registered InterScan Gateway Security Appliance users with active maintenance.

Spam Engine and Pattern File

The InterScan Gateway Security Appliance (the appliance) uses the Trend Micro Anti-spam Engine and Trend Micro spam pattern files to detect and take action against spam messages. Trend Micro updates both the engine and pattern file frequently and makes them available for download. The appliance can download these components through a manual or scheduled update.

The anti-spam engine uses spam signatures and heuristic rules to filter email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. The appliance compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, the appliance takes action against the spam.

For example, spammers sometimes use numerous exclamation marks (! ! ! !) in their email messages. When the appliance detects a message that uses exclamation marks in this way, it increases the spam score for that email message.

Note: Rules in spam pattern differ from pattern to pattern; so, a mail judged as spam in a previous pattern may not be treated as spam in current or later patterns.

Administrators cannot modify the method that the anti-spam engine uses to assign spam scores, but they can adjust the detection levels that the appliance uses to decide if messages are spam.

Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address outstanding issues, enhance product performance, and add new features.

The following is a summary of the items Trend Micro may release:

- **Hot Fix**—a work-around or solution to customer-reported issues. Trend Micro develops and releases hot fixes to specific customers only.
- **Security Patch**—a single hot fix or group of hot fixes suitable for deployment to all customers
- **Patch**—a group of security patches suitable for deployment to all customers
- **Service Pack**—significant feature enhancements that upgrade the product

Your vendor or support provider may contact you when these items become available. Check the Trend Micro Web site for information on new hot fix, patch, and service pack releases:

<http://www.trendmicro.com/download>

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Patches

For patches listed below, replace **the appliance_IP** with your appliance's IP Address.

Non-port 80 configuration (only for patch 2):

`https://the_appliance_IP/nonprotect/confport.htm`

Deferred scan setup:

`https://the_appliance_IP/nonprotect/trickling.htm`

Licenses

A license to the Trend Micro software usually includes the right to product updates and pattern file updates. In certain regions, Trend Micro also offers basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Maintenance is your right to receive pattern file updates and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the licensethat you receive with the product describes the terms of the maintenance for that product.

Note: Maintenance expires. Your License Agreement does not. If the Maintenance expires, scanning can still occur, but you will not be able to update the virus pattern file, scan engine, or program files (even manually). Nor will you be entitled to receive technical support from Trend Micro where applicable.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

<https://olr.trendmicro.com/registration/>

Renewing Maintenance

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

- To purchase renewal maintenance, you may contact the same vendor from whom you purchased the product. A License Agreement extending your Maintenance protection for a further year will be sent to the primary company contact listed in your company's Registration Profile.
- To view or modify your company's Registration Profile, log in to the account at the Trend Micro online registration Web site:

<https://olr.trendmicro.com/registration/us/en-us/>

EICAR- Test Virus

The European Institute for Computer Antivirus Research (EICAR) has developed a test "virus" you can use to test your appliance installation and configuration. This file is an inert text file whose binary pattern is included in the virus pattern file from most antivirus vendors. It is not a virus and does not contain any program code.

Obtaining the EICAR Test File:

You can download the EICAR test virus from the following URLs:

www.trendmicro.com/vinfo/testfiles/

www.eicar.org/anti_virus_test_file.htm

Alternatively, you can create your own EICAR test virus by typing the following into a text file, and then naming the file "eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!  
$H+H*
```

Note: Flush the cache in the cache server and local browser before testing.

Best Practices

Handling Compressed Files

Compressed files provide a number of special security concerns. In short, compressed files can be password-protected or encrypted, they can harbor so-called "zip-of-death" threats, and they can contain within them numerous layers of compression.

To balance security and performance, Trend Micro recommends that you read the following before choosing compressed file settings:

Block compressed files if...

Decompressed file count exceeds:

Set the number of files within a compressed archive at which InterScan Gateway Security Appliance should stop extracting.

For example have InterScan Gateway Security Appliance abandon the extraction after 1000 files.

Whenever the limit is reached, the original archive, and any decompressed files, is deleted. In addition to benefiting overall scan efficiency, setting an upper limit for decompression can prevent "zip of death" attacks designed to crash vulnerable virus scanning programs.

Size of a decompressed file exceeds:

Set the maximum size that files being extracted from a compressed archive are allowed to reach.

Once the limit is reached, the original archive, and any decompressed files, is deleted. As with "Number of files", setting an upper size limit for decompression can help prevent the "zip of death" attack.

Number of layers of compression exceeds:

Set the maximum number of layers (compressed file within a compressed file) you want InterScan Gateway Security Appliance to scan down through. The system maximum is 20.

Scanning multiple layers of compression can slow down overall system performance, which is why the default for this parameter is 10. After detecting 10 layers of compression, InterScan Gateway Security Appliance abandons the scan task and blocks the file.

Although InterScan Gateway Security Appliance can detect viruses in even the 20th layer of compression, it will only clean an infected file if it is detected in the first compression layer.

Decompressed file exceeds “x” times of compressed:

x: Default setting is 10

The InterScan Gateway Security Appliance provides this feature as a guard against so-called “zip of death” threats, where one or more files of a particular nature have been “super compressed.” For example, to block a file that is 10MB before being compressed but is only 2 MB after being compressed, type 5 in this field, because 10MB is 5 times larger than 2MB.

In a compressed archive comprised of multiple files, if the compression factor of one or more files exceeds the number specified here, the appliance blocks the compressed file.

WinZip - IGSA_M-Series_GSG_SRC_GM_06092006.zip

Name	Type	Modified	Size	Ratio	Packed	Path
002.tif	Microsoft Office ...	5/9/2006 11:52 PM	100,003	2%	98,219	IGSA_M-Series_GSG_...
009.tif	Microsoft Office ...	5/9/2006 11:52 PM	169,292	2%	166,679	IGSA_M-Series_GSG_...
010.tif	Microsoft Office ...	5/9/2006 11:52 PM	178,331	2%	174,863	IGSA_M-Series_GSG_...
022.tif	Microsoft Office ...	5/9/2006 11:52 PM	442,538	2%	434,652	IGSA_M-Series_GSG_...
036.tif	Microsoft Office ...	5/9/2006 11:52 PM	364,962	2%	357,430	IGSA_M-Series_GSG_...
Back Panel.tif	Microsoft Office ...	5/9/2006 11:52 PM	119,036	2%	116,607	IGSA_M-Series_GSG_...
Front panel.tif	Microsoft Office ...	5/9/2006 11:52 PM	71,559	2%	69,848	IGSA_M-Series_GSG_...
IGSA attached rail n rail lock.tif	Microsoft Office ...	5/9/2006 11:52 PM	152,364	2%	149,931	IGSA_M-Series_GSG_...
IGSA Content Items.tif	Microsoft Office ...	5/11/2006 3:19 PM	291,627	2%	285,699	IGSA_M-Series_GSG_...
IGSA_GSG.book	Adobe FrameMa...	6/9/2006 6:45 PM	43,008	81%	8,094	IGSA_M-Series_GSG_...
IGSA_GSG.log	Text Document	3/24/2006 5:30 PM	1,031	82%	189	IGSA_M-Series_GSG_...
IGSA_GSG_AppendixA_system_checklist.fm	Adobe FrameMa...	6/9/2006 6:45 PM	115,712	71%	33,909	IGSA_M-Series_GSG_...
IGSA_GSG_AppendixB_Hardware_Specs_Environmental_Factors.fm	Adobe FrameMa...	6/9/2006 6:45 PM	121,856	70%	36,158	IGSA_M-Series_GSG_...
IGSA_GSG-deploying.fm	Adobe FrameMa...	6/9/2006 6:45 PM	148,480	68%	47,426	IGSA_M-Series_GSG_...
IGSA_GSG-intro.fm	Adobe FrameMa...	6/9/2006 6:45 PM	156,672	68%	50,782	IGSA_M-Series_GSG_...
IGSA_GSGIX.fm	Adobe FrameMa...	6/9/2006 6:45 PM	214,016	70%	64,233	IGSA_M-Series_GSG_...
IGSA_GSG-Legal.fm	Adobe FrameMa...	6/9/2006 6:45 PM	340,992	70%	102,489	IGSA_M-Series_GSG_...
IGSA_GSG-pre_config.fm	Adobe FrameMa...	6/9/2006 6:45 PM	160,768	68%	50,825	IGSA_M-Series_GSG_...
IGSA_GSGTOC.fm	Adobe FrameMa...	6/9/2006 6:45 PM	220,160	71%	64,397	IGSA_M-Series_GSG_...
IGSA_GSG-troubleshooting.fm	Adobe FrameMa...	6/9/2006 6:45 PM	116,736	71%	34,383	IGSA_M-Series_GSG_...
IGSA_Preface.fm	Adobe FrameMa...	6/9/2006 6:45 PM	117,760	70%	35,723	IGSA_M-Series_GSG_...
LCM_Closeup.tif	Microsoft Office ...	5/9/2006 11:52 PM	36,340	1%	36,094	IGSA_M-Series_GSG_...
LED-1.tif	Microsoft Office ...	5/9/2006 11:52 PM	1,579	4%	1,519	IGSA_M-Series_GSG_...
LED-2.tif	Microsoft Office ...	5/9/2006 11:52 PM	1,491	4%	1,424	IGSA_M-Series_GSG_...
LED-3.tif	Microsoft Office ...	5/9/2006 11:52 PM	1,367	5%	1,303	IGSA_M-Series_GSG_...
LED-4.tif	Microsoft Office ...	5/9/2006 11:52 PM	1,286	5%	1,222	IGSA_M-Series_GSG_...
LED-5.tif	Microsoft Office ...	5/9/2006 11:52 PM	2,011	3%	1,949	IGSA_M-Series_GSG_...
mountpost.tif	Microsoft Office ...	6/8/2006 3:19 PM	319,197	0%	318,455	IGSA_M-Series_GSG_...
mountslot.tif	Microsoft Office ...	6/8/2006 3:19 PM	156,429	0%	156,134	IGSA_M-Series_GSG_...
MultiSegment.tif	Microsoft Office ...	6/9/2006 10:38 AM	433,728	1%	431,517	IGSA_M-Series_GSG_...
RackKitContents.tif	Microsoft Office ...	6/8/2006 3:16 PM	168,647	1%	167,377	IGSA_M-Series_GSG_...

Selected 0 files, 0 bytes Total 41 files, 61,210KB

FIGURE 13-1. Compression Ratio

Action on unscanned files:

Unscanned or unscannable files include files that are password protected.

Handling Large Files

For larger files, a trade-off must be made between the user's experience and expectations and maintaining security. The nature of virus scanning requires doubling the download time (that is, the time to transfer the entire file to InterScan Gateway Security Appliance, scan the file, and then transfer the entire file to the client) for large files.

In some environments, the doubling of download time may not be acceptable. There are other factors such as network speed and server capability that must be considered.

If the file is not big enough to trigger large-file handling settings, the file will be scanned as a normal file.

When downloading a large file, the time to download the file and scan it for viruses may be long enough to cause the browser to time out.

Tip: Trend Micro recommends not scanning uncompressed files larger than 50 MB (default value); however, these values may vary depending on your network speed, server capability, and security requirements.

InterScan Gateway Security Appliance provides the following methods to address large-file scan lag when downloading HTTP and FTP files:

- **Do not scan files larger than** sets the maximum file size for scanning. InterScan Gateway Security Appliance will not scan files larger than the size specified. The default is 50MB.

WARNING! *This option effectively allows a hole in your Web security—large files will not be scanned. Trend Micro recommends that you choose this option only on a temporary basis.*

Deferred scan: (moderate risk) InterScan Gateway Security Appliance receives a file and begins scanning while it loads part of the page. To keep the connection with the client alive for the time it takes to scan the large file, InterScan Gateway Security Appliance "trickles", or delivers a small amount of the file to the requesting client. InterScan Gateway Security Appliance will stop the connection if it finds a virus.

Note: This option is considered "moderate risk" because it is possible that malicious code will be delivered to the client machine as part of the unscanned delivery.

Most files, however, are unreadable until the entire file is reconstructed.

Sending Trend Micro Suspected Internet Threats

You can send Trend Micro the URL of any Web site you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

1. From the InterScan Gateway Security Appliance console menu, click {**SMTP, HTTP, or POP3**} > **Anti-phishing**.
2. Click the **Notification** tab.
3. Click the **Submit a Potential Phishing URL to TrendLabs** link.
4. Type the suspicious URL in the mail body area and mail to antifraud@support.trendmicro.com.

From outside the InterScan Gateway Security Appliance console, you can:

- Send an email to: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject
- Use the Web-based submission form: <http://subwiz.trendmicro.com/>

Updating the InterScan Gateway Security Appliance Firmware

This chapter provides step-by-step instructions for updating the InterScan Gateway Security Appliance image, the BMC (baseboard management controller) firmware, and the BIOS firmware using the Trend Micro Appliance Firmware Flash Utility.

Topics included in this chapter include:

- *Updating the InterScan Gateway Security Appliance Device Image* on page 14-2
- *Preparing InterScan Gateway Security Appliance for the Device Image Update* on page 14-2
- *Uploading the New Device Image* on page 14-11
- *Completing the Process After the Device Image Is Uploaded* on page 14-26
- *Updating the Appliance BMC Firmware* on page 14-28
- *Updating the Appliance BIOS Firmware* on page 14-36

Updating the InterScan Gateway Security Appliance Device Image

Preparing InterScan Gateway Security Appliance for the Device Image Update

Before updating the InterScan Gateway Security Appliance (appliance) device image, ensure that you are familiar with some basic information about your device, as explained below.

The Preconfiguration Console

The Preconfiguration console is a terminal communications program that allows you to configure or view any preconfiguration setting. These settings include:

- Device Information & Status
- Device IP Settings
- Interface Settings
- System Tools
- Advanced Settings
- SSH Access Control
- Change Password
- Log off with saving
- Log off without saving

Examples of a terminal interface are HyperTerminal for Windows and Minicom for Linux.

The terminal interface allows basic preconfiguration of appliance settings. If you do not have access to a computer with terminal communications software, use the appliance LCD module to perform preconfiguration.

Using the LCD Module

Use the LCD and control panel on the front of the device to configure appliance network settings, such as the IP address, host name, netmask, gateway, and primary and secondary DNS addresses.

Before the Update

Before updating the device image, ensure that you have followed these steps:

TABLE 14-1. Pre-update checklist

- ☐ **Back up your configuration** (unless you have not yet configured anything) (See [Backing Up Your Configuration](#) on page 14-3)
- ☐ **Get the appliance image file** (See [Getting the Appliance Device Image from the Trend Micro Web site](#) on page 14-4)
- ☐ **Connect the appliance to a local computer** (See [Connecting a Local Computer to the Appliance to Deliver the Update](#) on page 14-5)
- ☐ **Log in to the appliance using terminal software such as HyperTerminal** (See [Interfacing with the Preconfiguration Console for Device Image Updates](#) on page 14-6)
- ☐ **Verify that the local computer IP address matches that of the appliance** (See [Getting the IP Address of the Local PC](#) on page 14-9)
- ☐ **Put the appliance into rescue mode** (See [Putting the Appliance Into Rescue Mode](#) on page 14-10)

Backing Up Your Configuration

When the device image updates, all information stored on the Compact Flash (CF) card will be overwritten. Therefore, if you wish to preserve your existing configuration, it is essential that you back up the appliance configuration before updating the appliance device image. This information is stored in a variety of logs, as listed below:

- Anti-pharming
- Anti-phishing
- Anti-spam: content scanning
- Anti-spam: Network Reputation Services
- Anti-spyware/grayware
- Content filtering
- Damage Cleanup
- File blocking
- IntelliTrap
- System
- Update
- URL filtering
- Viruses/malware

To back up the appliance configuration information:

1. Log on to the appliance Web console by pointing an Internet Explorer Web browser to the IP address that you assigned to your appliance when you installed it.
(For example, <https://10.1.151.5>)

Note: Remember to use secure http, that is `https://` and not `http://`.

2. From the main menu, click **Administration > Configuration Backup**. The Configuration Backup screen appears.
3. In the Backup Current Configuration section, click **Backup**. A screen appears asking you where to save the file (on your network or on the PC you are using to access the Web console). The default configuration file name is ***igsa_config.dat***, but you can change it to anything you like.
4. Click **Save**. A Save As screen opens. Navigate to the directory where you wish to store the configuration backup file.
5. Click **Save**. Internet Explorer downloads the configuration backup file to your chosen location.

Getting the Appliance Device Image from the Trend Micro Web site

You can download the appliance device image from the Trend Micro Web site.

To download the file:

1. Visit the following URL:
<http://www.trendmicro.com/download/product.asp?productid=73>
2. Click the link for **Appliance Firmware Flash Utility (AFFU)**. The file will have a name similar to:
phoenix_image_XXXXX.R

A screen appears asking where to store the file.

3. Save the file locally.

Connecting a Local Computer to the Appliance to Deliver the Update

Before you upload the device image to the appliance, designate a computer to interface with the appliance console port. Use a computer that has terminal configuration software such as HyperTerminal for Windows and a DB9 port.

You will be uploading the new device image using this computer that is physically connected to the appliance by means of the (serial) console port.

The port that you connect to on the back panel of the appliance depends on which option you are planning on choosing:

- Uploading the device image and keeping the existing configuration (option 3 on the appliance Preconfiguration rescue mode main menu), as detailed in [Uploading with Existing Configuration \(Option 3\)](#) on page 14-12
- Uploading the device image and restoring the default appliance configuration (option 5 on the appliance Preconfiguration rescue mode main menu), as detailed in [Uploading with the Restored, Default Configuration \(Option 5\)](#) on page 14-18

To connect the local computer to the Appliance:

1. Connect an Ethernet cable to the Management port (for option 5) or the INT port (for option 3) on the back of the device, as shown in the figure below, and connect the other end of the cable the the local computer.

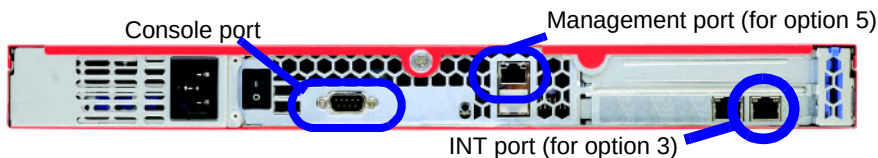


FIGURE 14-1. Back panel of the appliance showing console port, management port, and INT port

2. If uploading with option 5, change the IP address of the local computer to 192.168.252.x and the subnet mask to 255.255.255.0, while being careful to avoid the IP addresses 192.168.252.1 and 192.168.252.2 to avoid an IP conflict, as these are the default IP addresses for the appliance rescue mode and for the BMC (baseboard management controller) respectively. (See [Getting the IP Address of the Local PC](#) on page 14-9.)

3. If uploading with option 3, ensure that the IP address of the local computer is in the same segment as the appliance IP address. (See [Getting the IP Address of the Local PC](#) on page 14-9.)
4. Connect a serial (RS 232) cable from the local computer to the serial port on the back panel of the appliance. (See Figure 14-1 on page 5 for location of the serial port.)

Interfacing with the Preconfiguration Console for Device Image Updates

To access the preconfiguration console:

1. Connect one end of the included console cable to the **CONSOLE** port on the back panel of the device and the other end to the serial port (COM1, COM2, or any other available COM port) on a computer. (See figure 14-1, [Back panel of the appliance showing console port, management port, and INT port.](#))

Tip: Trend Micro recommends that you configure HyperTerminal properties so that the backspace key is set to delete and that you set the emulation type to VT100J for best display results.

2. Open HyperTerminal (**Start > Programs > Accessories > Communications > HyperTerminal**). For best display results, set the the terminal emulation to VT100J, as shown below.

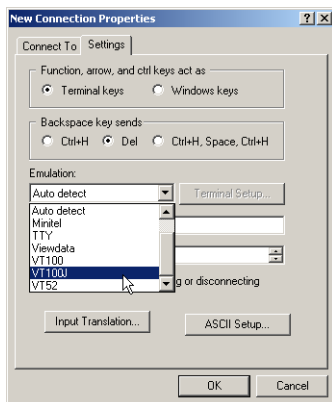


FIGURE 14-2. HyperTerminal display settings

3. Click **File > New Connection**. The Connection Description screen appears. Type a name for the connection profile and click **OK**. The Connect To screen appears:



FIGURE 14-3. The HyperTerminal Connect To screen

4. In the **Connect To** screen, using the drop-down menu, choose the COM port that your local computer has available and that is connected to the appliance box.
5. Click **OK**. The COM Properties screen appears. Use the following communications properties:
 - **Bits per second:** 115200
 - **Data Bits:** 8
 - **Parity:** None
 - **Stop bits:** 1
 - **Flow control:** None

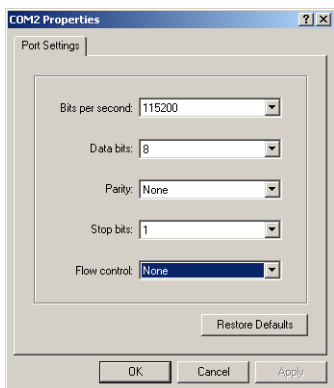


FIGURE 14-4. HyperTerminal COM Properties screen

6. Click **OK**. The COM Properties screen disappears and the screen is blank.
7. At the blank HyperTerminal screen, type the appliance Preconfiguration console password, or, if this is the first time you use the device, use the default password *admin* and press **ENTER**. The console accepts the password, displays the Login screen, and moves the cursor to the **Login** prompt.

Tip: Trend Micro recommends that you change the default password upon first use. You can do so through the Preconfiguration console.

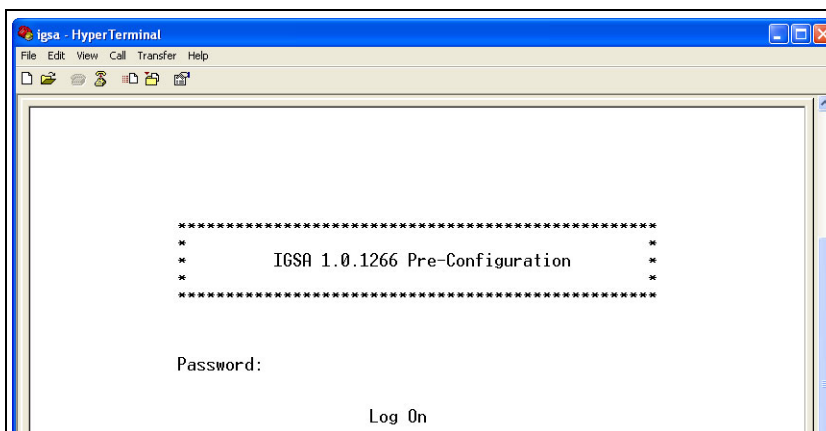
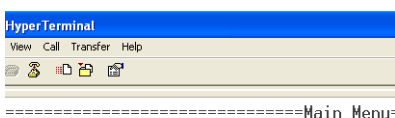


FIGURE 14-5. Appliance Preconfiguration console login screen

8. Press **ENTER** again. The appliance Preconfiguration console Main Menu appears, as shown below.



```

1) Device Information & Status
2) Device IP Settings
3) Interface Settings
4) System Tools
5) Advanced Settings
6) SSH Access Control
7) Change Password
8) Log Off with Saving
9) Log Off without Saving

```

FIGURE 14-6. Appliance Preconfiguration console main menu, accessed via HyperTerminal

Getting the IP Address of the Local PC

For Windows, you can either use the **ipconfig** command to verify the IP address of your PC or you can ping the appliance IP address that is displayed in HyperTerminal.

Putting the Appliance Into Rescue Mode

In order to update the device image, first put the appliance into rescue mode. With the local PC still connected to the appliance, and with the Preconfiguration console still displaying in HyperTerminal, do the following.

1. Turn off the device by pressing and holding the on/off switch in the ON position for at least 4 seconds. The device powers down.

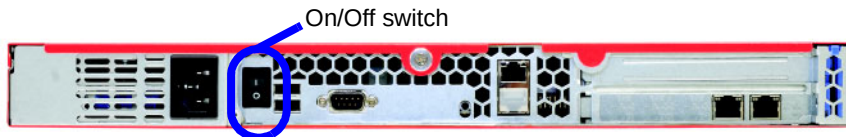


FIGURE 14-7. Appliance back panel showing on/off switch

2. Turn the appliance back on, by pressing the on/off switch in the ON position for only a second. The device begins to reboot, displaying the boot-up sequence on the HyperTerminal screen of your local computer.
3. Closely watch this display in the HyperTerminal window. As soon as you see the **Press ESC to enter the menu...** prompt, firmly press **ESC** (the Escape key). The appliance goes into rescue mode, and the rescue mode main menu displays, as shown below.

About the Appliance On/Off Switch

The appliance on/off switch is designed using industry standards that safeguard against the accidental shutdown of such devices. Although the rocker switch is marked with the international symbols for "on" and "off," it always appears to be in the "off" position when the appliance is running.

To turn the appliance off, press and hold down the "on" side of the switch *for at least four seconds*. When you see the lights for any ports turn off, you know that the device has powered down.

To turn the appliance on, press and hold down the "on" side of the switch for about one second. The appliance powers on.

Tip: The **Press ESC to enter the menu...** prompt displays for only a very short time, so you must be quick. Be sure to firmly press **Esc** as soon as you see the prompt.

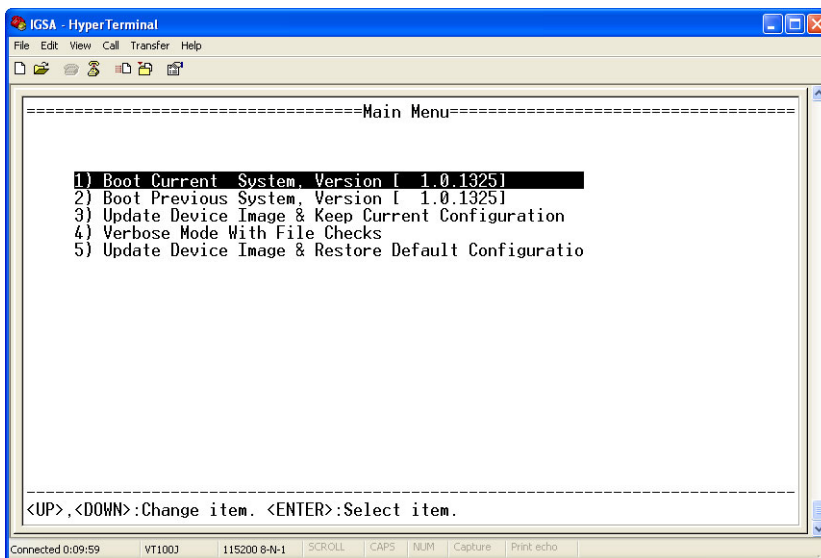


FIGURE 14-8. Appliance rescue mode main menu

Uploading the New Device Image

The steps for uploading the new device image vary based on whether you plan to keep the existing appliance configuration (option 3) or to restore the default configuration (option 5).

Depending on which option you are using, you will see different data in the appliance Preconfiguration console and in the Appliance Firmware Flash Utility (AFFU).

Uploading with Existing Configuration (Option 3)

You can either use up and down arrow keys on your keyboard to move to the choice that you want, or you can simply press the number of that option. The option for uploading with the existing configuration is:

3 - Update Device Image & Keep Current Configuration

When using this option, only the system partition will be updated.

To upload the new device image using existing configuration:

1. Choose option 3, Update Device Image & Keep Current Configuration. The following screen appears:

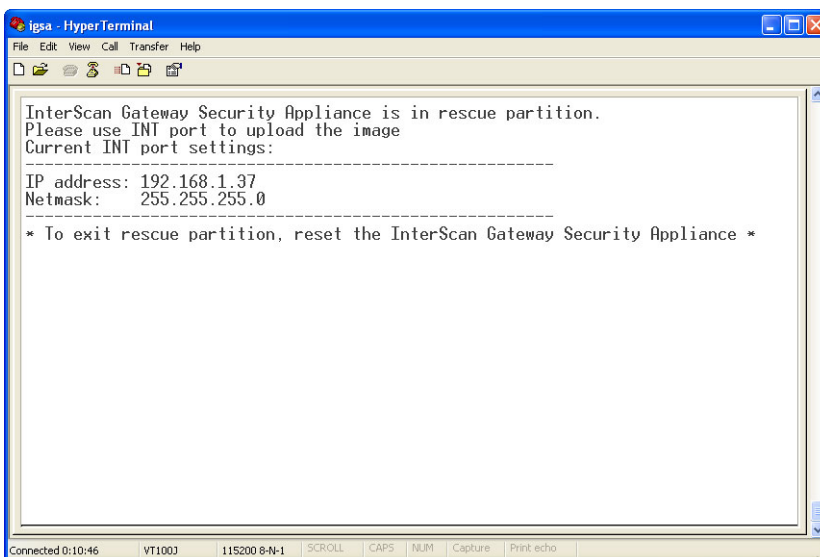


FIGURE 14-9. Preconfiguration console screen that appears when you select option 3 in rescue mode

2. Connect an RJ45 Ethernet cable from your local computer to the **INT** port of the appliance, as shown below.



FIGURE 14-10. The appliance back panel showing location of internal (INT) port

3. Upload the new device image by using the Trend Micro Appliance Firmware Flash Utility as described in *Using the Appliance Firmware Flash Utility with Option 3* on page 14-13.

Using the Appliance Firmware Flash Utility with Option 3

Before launching the Appliance Firmware Flash Utility (AFFU), ensure that the IP of your PC is within the same segment as the IP of the appliance. The appliance IP address appears on the preconfiguration console screen that appears when you select option 3 - Update Device Image & Keep Current Configuration (see figure 14-9, *Preconfiguration console screen that appears when you select option 3 in rescue mode*).

To upload the device image update with option 3 using the AFFU:

1. Put the InterScan Gateway Security Appliance Solutions CD into the local computer. The following screen appears:

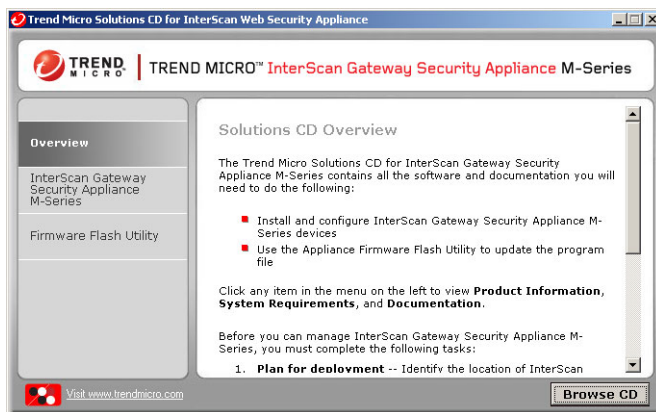


FIGURE 14-11. InterScan Gateway Security Appliance Solutions CD splash screen

Note: If for some reason the above screen does not appear after you put the CD in the CD-ROM drive, locate the file **setup.exe** and click it. The screen will appear.

- On the main menu click **Firmware Flash Utility**. The following screen appears:

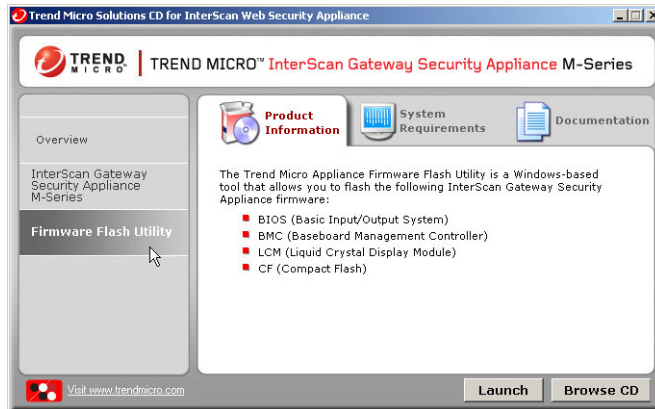


FIGURE 14-12. The appliance Solutions CD Firmware Flash Utility section

- On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

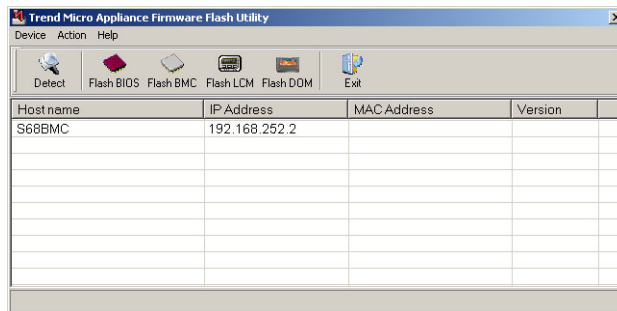


FIGURE 14-13. Trend Micro Appliance Firmware Flash Utility, opening screen, when uploading with option 3

- Click **Flash DOM** (disk-on-module), as shown below.

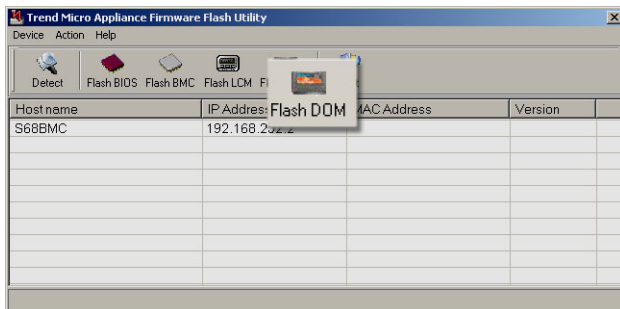


FIGURE 14-14. AFFU opening screen when uploading with option 3, emphasizing Flash DOM

- After you click **Flash DOM**, the Appliance Firmware Flash Utility - DOM screen appears, as shown below.

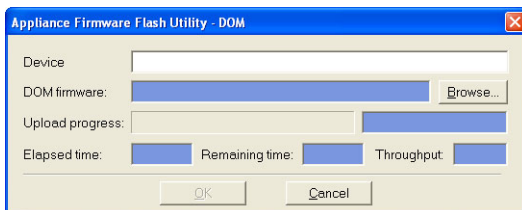


FIGURE 14-15. AFFU DOM screen

- Because the appliance uses the 192.168.252.1 as the default rescue mode IP address, type `192.168.252.1` in the **Device** field.

7. Click **Browse** (next to the DOM firmware field) and browse to the device image in the file navigation screen that opens, as shown below.

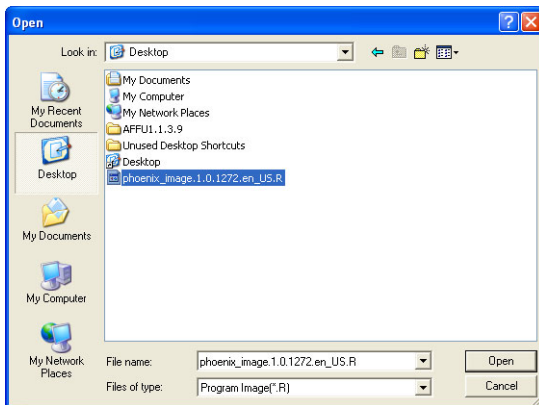


FIGURE 14-16. AFFU - browse to device image

8. Click **Open** to select the device image. The AFFU DOM screen reappears, with the full path to the device image in the **DOM firmware** field.
9. Click **OK** to start the device image update. The AFFU begins uploading the new device image to the appliance, and the AFFU DOM screen displays the progress of the update.

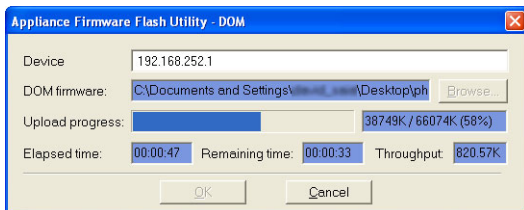


FIGURE 14-17. AFFU DOM screen showing progress of the update

When the update is complete, the AFFU displays a message stating that the device image uploaded successfully.



FIGURE 14-18. AFFU "flash DOM successfully uploaded" message

Troubleshooting Device Image Upload with Option 3

If you are unable to upload the appliance device image in rescue mode using option 3, verify the following:

- Make sure that the appliance can get an IP address dynamically from your DHCP server or that you have assigned a static IP address.
- Make sure that the Ethernet cable is connected to the **INT** (internal) port (see Figure 14-10, “The appliance back panel showing location of internal (INT) port,” on page 13).
- Make sure that the uploading client is in the same IP segment as the appliance IP address, which you can see on the appliance rescue mode console. You can use the **ping** command to check the appliance connection.
- Make sure that TFTP traffic is not being blocked by an application on the uploading client or by some intermediate device. (TFTP is the protocol that the appliance uses to communicate with the uploading client.)

Uploading with the Restored, Default Configuration (Option 5)

You can either use up and down arrow keys on your keyboard to move to the choice that you want, or you can simply press the number of that option. The option for uploading with the existing configuration is:

5 - Update Device Image & Restore Default Configuration

When using this option, all the partitions on the Compact Flash (CF) card will be erased. Upload the image to the management port, and not the INT port, as with option 3.

Note: If you are using this option and have already entered your appliance Activation Code (AC), you will need to re-enter your AC in the Web console after the appliance image upload is complete and the device has rebooted.

To upload the new image file and restore the default configuration:

1. Choose option 5, Update Device Image & Restore Default Configuration. The following screen appears:

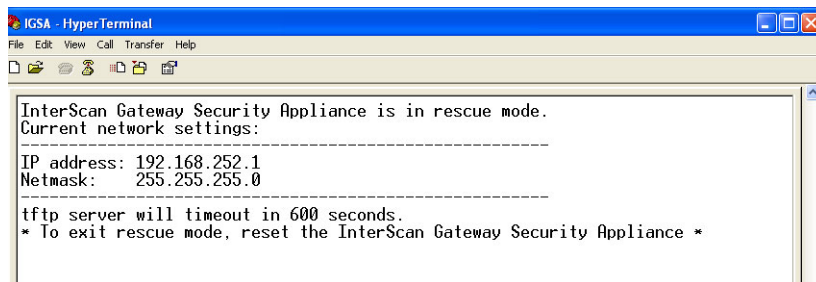


FIGURE 14-19. Preconfiguration console screen that appears when you select option 5 in rescue mode

2. Connect an RJ45 Ethernet cable from your local computer to the Management port of the appliance, as shown below.



FIGURE 14-20. Appliance back panel showing location of management port

3. Upload the new image file by using the Trend Micro Appliance Firmware Flash Utility as described in [Using the Appliance Firmware Flash Utility with Option 5](#) on page 14-20.

Note: After you select the upload option, the appliance waits for the upload for up to 10 minutes, at which point it times out.

Using the Appliance Firmware Flash Utility with Option 5

Before launching the Appliance Firmware Flash Utility (AFFU), ensure that the IP of your PC is within the same segment as the IP of the appliance. The appliance IP address appears on the preconfiguration console screen that appears when you select option 5 - Update Device Image & Restore Default Configuration (see figure 14-19, *Preconfiguration console screen that appears when you select option 5 in rescue mode*). (For more information on how to get the IP address of the local computer, see *Getting the IP Address of the Local PC* on page 14-9).

To upload the device image update using the Appliance Firmware Flash Utility:

1. Put the InterScan Gateway Security Appliance Solutions CD into the local computer. The following screen appears:

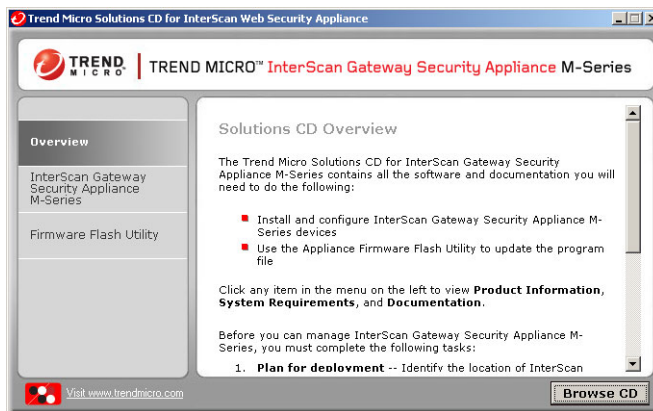


FIGURE 14-21. InterScan Gateway Security Appliance Solutions CD splash screen

Note: If for some reason the above screen does not appear after you put the CD in the CD-ROM drive, locate the file **setup.exe** and click it. The screen will appear.

2. On the main menu click **Firmware Flash Utility**. The following screen appears:

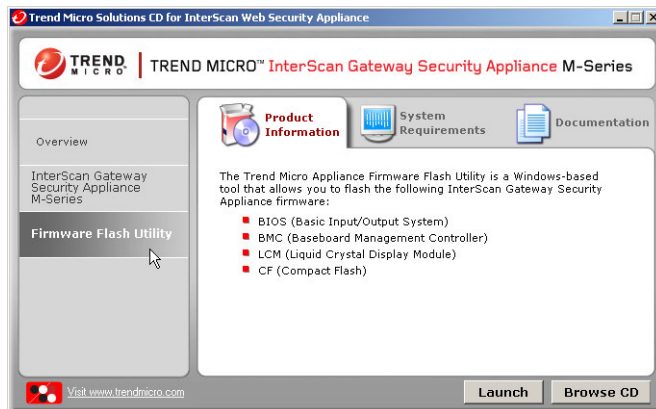


FIGURE 14-22. The appliance Solutions CD Firmware Flash Utility section

3. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

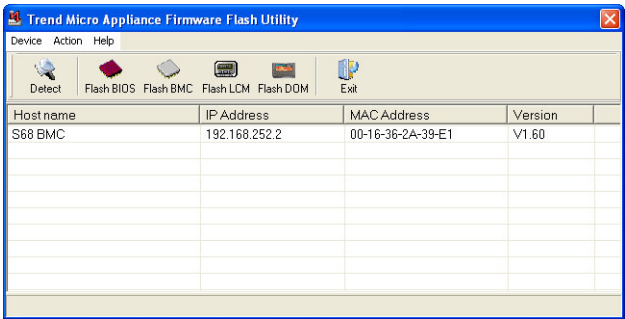


FIGURE 14-23. Trend Micro Appliance Firmware Flash Utility, opening screen when using option 5

4. Click **Flash DOM** (disk-on-module), as shown below.

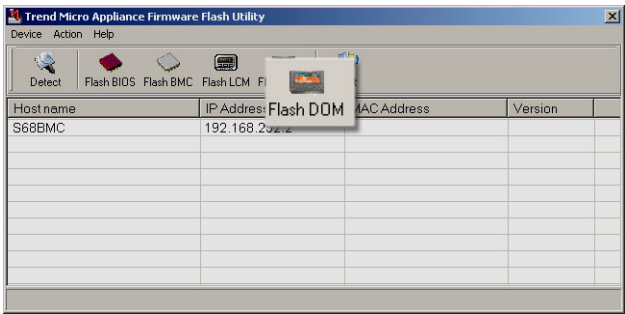


FIGURE 14-24. AFFU opening screen when using option 5, emphasizing Flash DOM

WARNING! Do not click on the table row containing the IP address. If you do, AFFU will connect to the IP address of that entry, which is the IP address of the appliance BMC, and an IP conflict will result. To upload the device image, the appliance needs to use the rescue mode IP address, which is always 192.168.252.1.

That is, do not do the following:

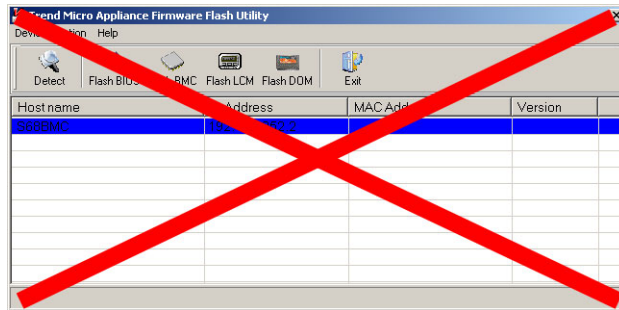


FIGURE 14-25. AFFU - Do not click the row displaying the IP address

5. After you click **Flash DOM**, the Appliance Firmware Flash Utility - DOM screen appears, as shown below.

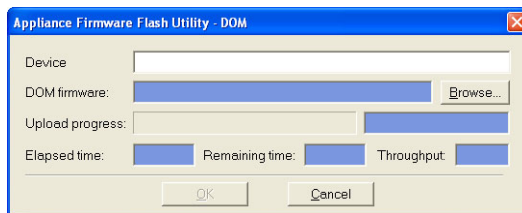


FIGURE 14-26. AFFU DOM screen

6. Because the appliance uses the 192.168.252.1 as the default rescue mode IP address, type `192 . 168 . 252 . 1` in the **Device** field.

7. Click **Browse** (next to the DOM firmware field) and browse to the device image file in the file navigation screen that opens.

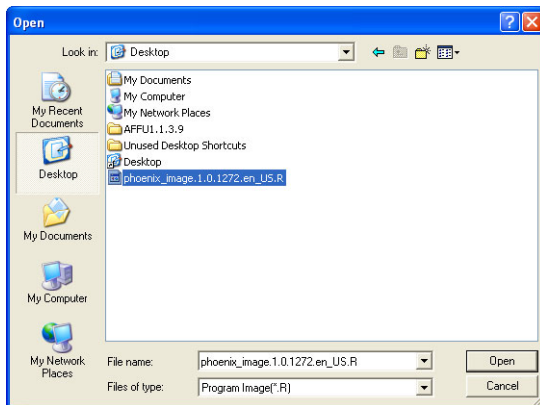


FIGURE 14-27. AFFU - browse to device image file

8. Click **Open** to select the device image file. The AFFU DOM screen reappears, with the full path to the device image in the **DOM firmware** field.
9. Click **OK** to start the device image update. The AFFU begins uploading the new device image to the appliance, and the AFFU DOM screen displays the progress of the update.

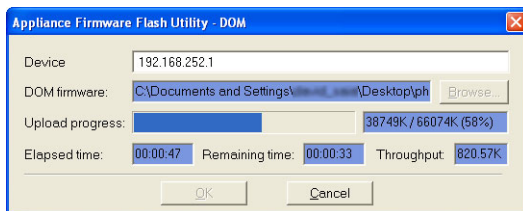


FIGURE 14-28. AFFU DOM screen showing progress of the update

When the update is complete, the AFFU displays a message stating that the device image uploaded successfully.

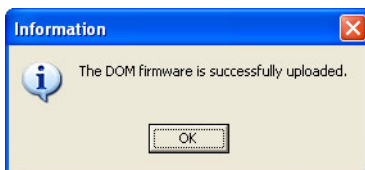


FIGURE 14-29. AFFU "flash DOM successfully uploaded" message

Troubleshooting Device Image Upload with Option 5

If you are unable to upload the appliance device image in rescue mode using option 5, verify the following:

- Make sure that the Ethernet cable is connected to the appliance management port. (See Figure 14-20, “Appliance back panel showing location of management port,” on page 19.)
- Make sure that the uploading client is in IP range 192.168.252.x / 255.255.255.0. You can use the **ping** command to check the appliance connection.
- Make sure that the appliance is still in rescue mode. You can verify that by viewing the appliance Preconfiguration rescue mode console. (See [Putting the Appliance Into Rescue Mode](#) on page 14-10.)
- Make sure that TFTP traffic is not being blocked by an application on the uploading client or by some intermediate device. (TFTP is the protocol that the appliance uses to communicate with the uploading client.)

Completing the Process After the Device Image Is Uploaded

After receiving the image, the appliance automatically reboots.

Note: It can take 2 or 3 minutes for the appliance to finish updating its device image.

The Preconfiguration console display in the HyperTerminal window on the local computer displays the progress of the reboot, as shown below.

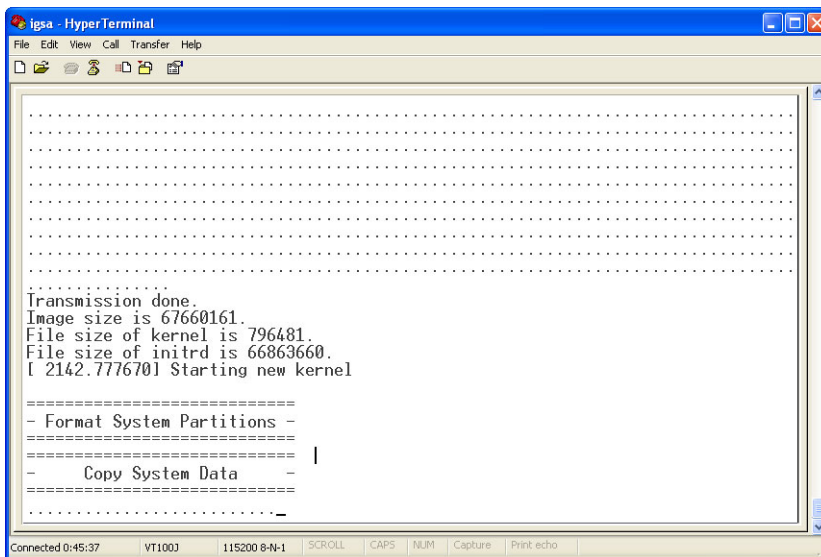


FIGURE 14-30. HyperTerminal window display as the appliance reboots

After the appliance has rebooted, confirm that it has the new device image. You can do so by comparing the build number on the new Preconfiguration console opening screen to the previous build number, as shown below.

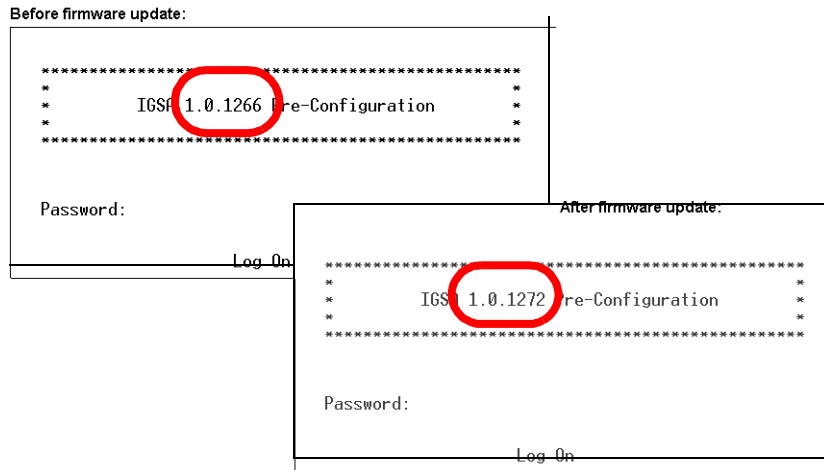


FIGURE 14-31. Appliance preconfiguration console login screens, before and after device image update

BMC and BIOS Firmware Updates Using the Appliance Firmware Flash Utility

Updating the Appliance BMC Firmware

The BMC (baseboard management controller) is a foreground/background embedded system. The current appliance BMC implements the Intelligent Platform Management Interface specification v1.5 (IPMI 1.5), using all mandatory commands and some Trend Micro OEM (original equipment manufacturer) commands. BMC firmware provides the functionality and the communication interfaces between the physical hardware and the software system.

For firmware updates, that is, updates for BIOS, BMC, and LCM (LCD module), the appliance uses the IP address 192.168.252.2.

Preparing to Upload the BMC Firmware

Before uploading the BMC firmware, ensure that you have the following:

- Trend Micro Appliance Firmware Flash Utility (AFFU . exe)
- The BMC firmware file, which will have a name similar to S68FWxxx . BIN

Preparing the Local Computer for Uploading to the Appliance

Before you upload the device image to the appliance, designate a computer to interface with the appliance console port. Use a computer that has terminal configuration software such as HyperTerminal for Windows and a DB9 port.

You will be uploading the new device image using this computer that is physically connected to the appliance by means of the (serial) console port.

To connect the local computer to the appliance:

1. Connect an Ethernet cable to the Management port on the back of the device, as shown in the figure below, and connect the other end of the cable the the local computer.

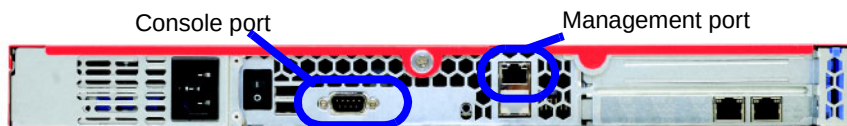


FIGURE 14-32. Back panel of the appliance showing console (serial) port and management port

2. Change the IP address of the local computer to 192.168.252.x and the subnet mask to 255.255.255.0, while being careful to avoid the IP addresses 192.168.252.1 and 192.168.252.2 to avoid an IP conflict, as these are the default IP addresses for appliance rescue mode and for the BMC (baseboard management controller) respectively. (See [Getting the IP Address of the Local PC](#) on page 14-9.)
3. Follow the instructions in [Interfacing with the Preconfiguration Console for Firmware Updates](#) starting on page 14-29.
4. Connect a serial (RS 232) cable from the local computer to the serial port on the back panel of the appliance.

Interfacing with the Preconfiguration Console for Firmware Updates**To access the preconfiguration console:**

1. Connect one end of the included console cable to the **CONSOLE** port on the back panel of the device and the other end to the serial port (COM1, COM2, or any other available COM port) on a computer. (See Figure 14-1, “Back panel of the appliance showing console port, management port, and INT port,” on page 5.)

Tip: Trend Micro recommends that you configure HyperTerminal properties so that the backspace key is set to delete and that you set the emulation type to VT100J for best display results.

2. Open HyperTerminal (**Start > Programs > Accessories > Communications > HyperTerminal**). For best display results, set the the terminal emulation to VT100J, as shown below.

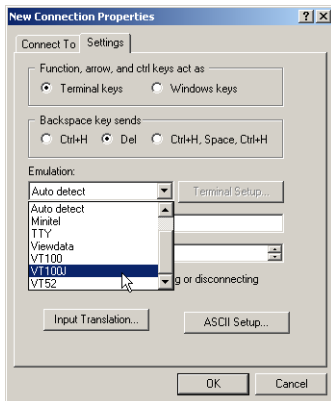


FIGURE 14-33. HyperTerminal display settings

3. Click **File > New Connection**. The Connection Description screen appears. Type a name for the connection profile and click **OK**. The Connect To screen appears:



FIGURE 14-34. The HyperTerminal Connect To screen

4. In the **Connect To** screen, using the drop-down menu, choose the COM port that your local computer has available and that is connected to the appliance box.

5. Click **OK**. The COM Properties screen appears. Use the following communications properties:
 - **Bits per second:** 115200
 - **Data Bits:** 8
 - **Parity:** None
 - **Stop bits:** 1
 - **Flow control:** None

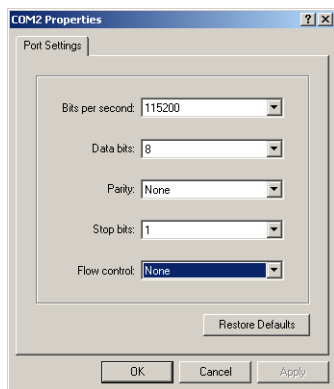


FIGURE 14-35. HyperTerminal COM Properties screen

6. Click **OK**. The COM Properties screen disappears and the screen is blank.
7. At the blank HyperTerminal screen, type the appliance Preconfiguration console password, or, if this is the first time you use the device, use the default password *admin* and press **ENTER**. The console accepts the password, displays the Login screen, and moves the cursor to the **Login** prompt.

Tip: Trend Micro recommends that you change the default password upon first use. You can do so through the Preconfiguration console.

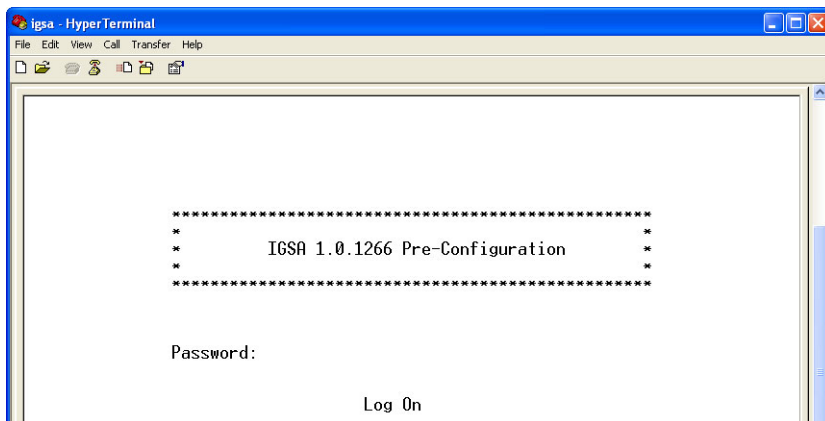


FIGURE 14-36. Appliance Preconfiguration console login screen

8. Press **ENTER** again. The appliance Preconfiguration console Main Menu appears, as shown below.

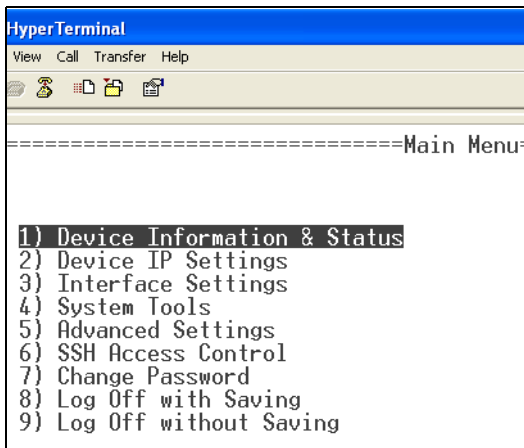


FIGURE 14-37. Appliance Preconfiguration console main menu, accessed via HyperTerminal

Getting the IP Address of the Local PC

For Windows, you can either use the **ipconfig** command to verify the IP address of your PC or you can ping the appliance IP address that is displayed in HyperTerminal.

Uploading the BMC Firmware

To upload the BMC firmware to the appliance:

1. Power off the appliance, but keep the power cord plugged in. (DC off, AC on)

Note: Turn off the device by pressing and holding the on/off switch in the ON position for at least 4 seconds.

- Put the InterScan Gateway Security Appliance Solutions CD into the local computer. The following screen appears:

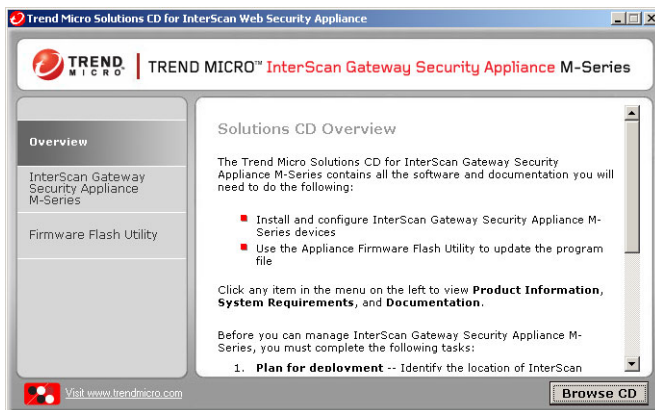


FIGURE 14-38. InterScan Gateway Security Appliance Solutions CD splash screen

- On the main menu click **Firmware Flash Utility**. The following screen appears:

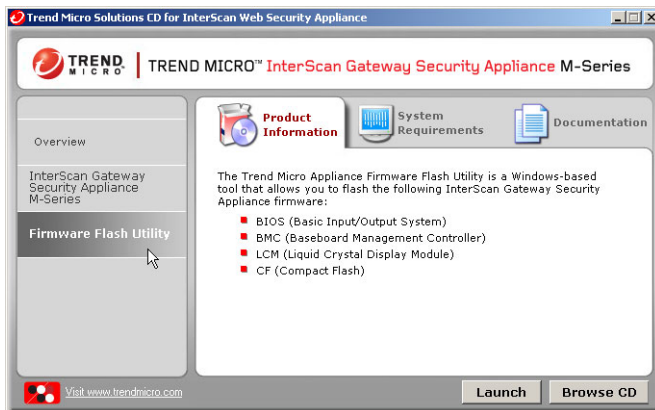


FIGURE 14-39. The InterScan Gateway Security Appliance Solutions CD Firmware Flash Utility section

4. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

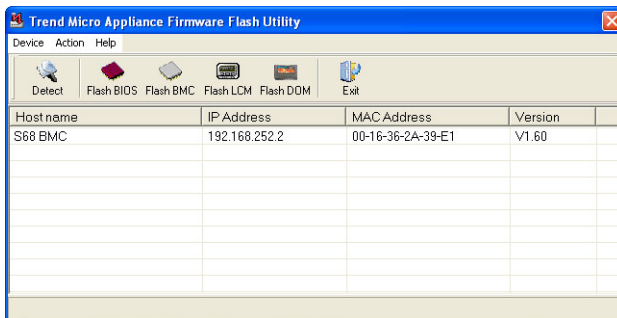


FIGURE 14-40. Trend Micro Appliance Firmware Flash Utility, opening screen

5. Click **Detect** to acquire the IP address of the BMC.

Note: For successful detection, configure the IP address of the local computer to be in the same segment as that of the BMC.

6. Select the detected entry by clicking the table row with the detected information.
7. Click **Flash BMC**. The Appliance Firmware Flash utility (AFFU) prompts you for a user name and password.
8. Leave the user name field empty and type `root` in the password field. The AFFU-BMC screen appears as shown below.

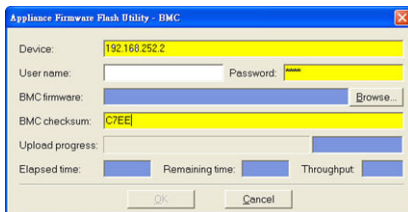


FIGURE 14-41. AFFU - BMC information entry screen

9. Click **Browse** (next to the BMC firmware field) and browse to the BMC firmware file in the file navigation screen that opens.
10. In the BMC checksum field, type the checksum value that you got from the the firmware release note.
11. Click **OK**. AFFU auto-powers on the appliance to begin to upload the BMC firmware and when the upload is complete, displays an information message stating that the BMC firmware uploaded successfully.

Note: During the BMC update, the appliance CPU fans run at full speed.

After the BMC Upload

After the BMC has upgraded, BMC will auto-restart the appliance to re-flash the BMC.

Updating the Appliance BIOS Firmware

On rare occasions, it may be necessary to update the appliance BIOS. Follow the procedures below to complete this kind of update.

Preparing to Upload the Appliance BIOS

Before uploading the BIOS, ensure that you have the following:

- Trend Micro Appliance Firmware Flash Utility (AFFU . exe)
- The BIOS firmware, which will have a name similar to S68_3AXX . ROM

Preparing the Local Computer for Uploading to the Appliance

The first two tasks when uploading new BIOS firmware (as detailed in [Updating the Appliance BMC Firmware](#) on page 14-28), are exactly the same as the procedures for connecting a local computer to the appliance to deliver the update and interfacing with the appliance Preconfiguration console:

1. Follow the instructions in [Preparing to Upload the BMC Firmware](#) starting on page 14-28.
2. Follow the instructions in [Interfacing with the Preconfiguration Console for Firmware Updates](#) starting on page 14-29.

Note: When connecting the Ethernet cable from the local computer to the Management port, that port should be lit up green.

Uploading the Appliance BIOS Firmware

To upload the appliance BIOS:

1. Power off the appliance, but keep the power cord plugged in. (DC off, AC on)

Note: Turn off the device by pressing and holding the on/off switch in the ON position for at least 4 seconds.

2. Put the InterScan Gateway Security Appliance Solutions CD into the local computer. The following screen appears:

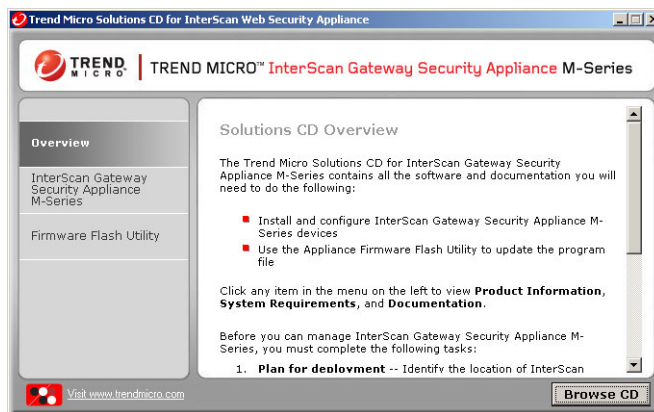


FIGURE 14-42. InterScan Gateway Security Appliance Solutions CD splash screen

- On the main menu click **Firmware Flash Utility**. The following screen appears:

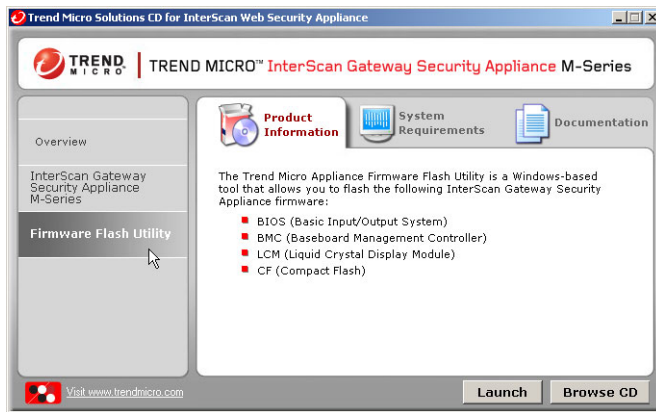


FIGURE 14-43. The appliance Solutions CD Firmware Flash Utility section

- On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

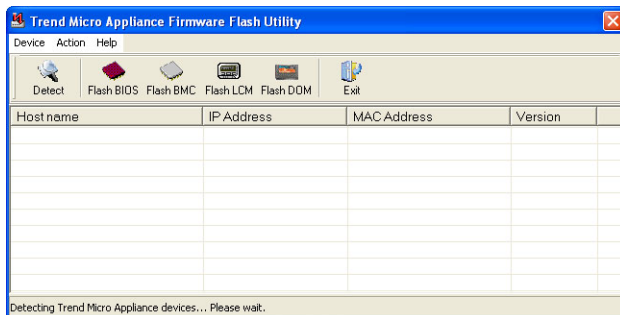


FIGURE 14-44. AFFU screen that appears initially

- Click **Detect** to acquire the IP address of the appliance BMC.

Note: For successful detection, configure the IP address of the local computer to be in the same segment as that of the appliance BMC.

6. Select the detected entry by clicking the table row with the detected information.
7. Click **Flash BIOS**. AFFU prompts you for a user name and password.
8. Leave the user name field empty and type `root` in the password field. The AFFU-BIOS screen appears as shown below.

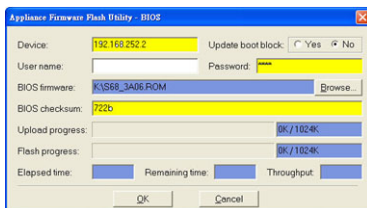


FIGURE 14-45. AFFU BIOS information entry screen

9. Click **Browse** (next to the BIOS firmware field) and browse to the BIOS firmware file in the file navigation screen that opens.
10. In the BIOS checksum field, type the checksum value that you got from the the BIOS release note.
11. Click **OK**. AFFU auto-powers on the appliance to begin to upload the BIOS firmware and, when the upload is complete, displays an information message stating the the BIOS firmware upgraded successfully.

After the BIOS Firmware Upload

After the BIOS has upgraded, the appliance will auto-restart and will then re-flash the BIOS.

Troubleshooting BMC or BIOS Firmware Upload

If the AFFU tool produces an error message saying "Can't log in to device, or user privilege level is not administrator," verify the following:

- Make sure that the Ethernet cable is connected to the management port. (See Figure 14-20, "Appliance back panel showing location of management port," on page 19.)
- Make sure that the uploading client is in IP range
192.168.252.x / 255.255.255.0 (You can use the AFFU detect

function to verify the connection status between the appliance and the uploading client.)

- Make sure that you follow the correct update procedure to shut down the appliance before attempting to update the BMC/BIOS firmware. (See [*Preparing to Upload the BMC Firmware*](#) on page 14-28.)
- Verify that the IP address of the appliance is 192 . 168 . 252 . 2 and that the authenticated password information is correct.

Terminology

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a brief discussion of these terms and their meanings as used in this document.

BOT

The term "BOT" is derived from the word "robot." In common usage, a BOT is a software agent that interacts with network services intended for people (for example, Web, email, etc.) as if it were a real person. A typical use of a BOT is to simply gather information (such as on a Web page), though common malicious uses include using a BOT to commit click fraud or installing a BOT behind the scenes on people's computers to coordinate such things as a distributed denial-of-service attack. InterScan Gateway Security Appliance protects against these kinds of BOTs using IntelliTrap™, particularly when they're enclosed as compressed or multi-compressed files attached to email messages.

Grayware

Grayware is a general classification for application behavior that is undisclosed, annoying, or undesirable. Grayware includes spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and any other unwelcome files and programs (apart from viruses) that may harm the performance of computers on your network. InterScan Gateway Security Appliance can detect both malware and grayware during its real-time scans and can respond in a variety of ways.

Macro Viruses

Macro viruses are application-specific but can cross operating systems, for example, from Windows to Linux. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro-capable applications such as .doc, .xls, and .ppt. Macro viruses travel between data files in the application and can eventually infect hundreds of files if undeterred. InterScan Gateway Security Appliance detects malicious macro code by using heuristic scanning. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature. Trend Micro MacroTrap™, one of the underlying technologies in InterScan Gateway Security Appliance, is specifically designed to detect, clean, delete and/or quarantine malicious macro code.

Mass-Mailing Attacks

Email-aware viruses have the ability to spread by email by automating the infected computer's email client. Mass-mailing behavior describes a situation when an infection spreads rapidly between clients and servers in an email environment. Trend Micro has designed the scan engine in InterScan Gateway Security Appliance to detect behaviors that mass-mailing attacks usually demonstrate. The behaviors are recorded in the virus pattern file that is updated using the Trend Labs ActiveUpdate servers. The action set for mass-mailing behavior takes precedence over all other actions, and the recommended action against mass-mailing attacks is that such email be deleted.

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the threats mentioned in this section, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols such as SMTP and POP3 to replicate. InterScan Gateway Security Appliance works with a network virus pattern file to identify and block network viruses.

Pharming

Similar in nature to email phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous email requests for you to visit spoofed Web sites that appear legitimate, pharming "poisons" a DNS server by infusing it with false information, resulting in your request's being redirected elsewhere. However, your browser will indicate that you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to defraud people one at a time with an email, whereas pharming allows the scammers to target large groups of people at one time through domain spoofing.

Phishing

A phish is an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click on a link that will redirect their browsers to a fraudulent Web site. Once there, the user is asked to update personal information such as passwords, social security numbers, and credit card numbers, which will be used for identity theft. InterScan Gateway Security Appliance provides tools for handling known phishing sites and for adding others to a list of offenders.

Spam

Spamming is the misuse of electronic communications media to send unsolicited bulk messages. The most common form of spam is delivered in email as a form of commercial advertising. In practice, however, people use spam for many purposes other than commercial ones and in many media other than email, including instant messaging, Usenet newsgroups, Web search engines, Web logs, and mobile phone messaging. InterScan Gateway Security Appliance protects you against unwanted spam in email and on the Web using a database of known spammers and content filters.

Spyware

Spyware refers to that broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of its owner or user. While the term suggests software that secretly monitors the user, it more broadly refers to software that subverts the computer's operation for the benefit of a third party, usually for commercial gain. Typical uses of spyware include the delivery of unsolicited pop-up advertisements, the theft of personal information (including financial information such as credit card numbers), the monitoring of Web-browsing activity for marketing purposes, and the routing of HTTP requests to advertising sites.

Trojans

A Trojan is a malicious program that masquerades as a harmless application. Unlike viruses, Trojans do not replicate, but they can be just as destructive. An application that claims to rid your computer of viruses when it actually introduces viruses onto your computer is an example of a Trojan. Trojans do not infect files; thus, they cannot be cleaned and Trend Micro recommends that they be deleted—a strategy fully supported by InterScan Gateway Security Appliance.

Viruses

Computer viruses are programs that have the unique ability to replicate. They can attach themselves to just about any type of executable file and are spread as files that are copied and sent from individual to individual. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. InterScan Gateway Security Appliance can detect and delete or quarantine viruses during its real-time scans.

Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. Unlike viruses, worms do not need to attach themselves to host programs. Worms cannot be cleaned, because they are self-contained programs. Thus, the recommended action is that they be deleted—fully supported by InterScan Gateway Security Appliance.

Technology Reference

Deferred Scan

Deferred scan ensures that the connection between the client and InterScan Gateway Security Appliance remains open while large file scanning takes place. A client requests a file from an FTP or HTTP server, and the server sends the file to the client located behind InterScan Gateway Security Appliance. InterScan Gateway Security Appliance receives the file and starts scanning it. However, if the file is large it can take InterScan Gateway Security Appliance some time to complete the scan. If the time it takes to scan the file is too long, the connection between the client and InterScan Gateway Security Appliance will be lost, and the client will not receive the file.

To ensure that the connection with the client remains open while file scanning occurs, InterScan Gateway Security Appliance sends packets to the client one by one. The packets are sent to a temporary folder on the client. If InterScan Gateway Security Appliance detects a threat, it immediately stops sending packets and a notification appears on the user's browser. When this happens the user will see a folder on their computer with a partial file in it. Because the file is incomplete, it presents no danger.

Diskless Mode

InterScan Gateway Security Appliance can operate in diskless mode when there is a problem with the device hard disk. InterScan Gateway Security Appliance uses the disk SMART system test feature to determine if there is a problem with the device hard disk. If disk SMART Test detects a problem, InterScan Gateway Security Appliance will reboot and begin operating in diskless mode.

- When InterScan Gateway Security Appliance is in diskless mode the following features are disabled:
- Manual and Scheduled Update - InterScan Gateway Security Appliance will not download updates
- Logging - InterScan Gateway Security Appliance will not log events
- Quarantining - InterScan Gateway Security Appliance will not quarantine specified items
- World Virus Tracking Program - InterScan Gateway Security Appliance will not track virus information for the World Virus Tracking Program

Another effect of diskless mode is a reduction in InterScan Gateway Security Appliance scanning capability. InterScan Gateway Security Appliance is usually capable of scanning four items concurrently, but when in diskless mode, it can only scan one item at a time, resulting in reduced scanning performance, and possibly, dropped traffic.

When InterScan Gateway Security Appliance is in diskless mode the hard disk LED turns red and become static. InterScan Gateway Security Appliance notifies the administrator, by email, if there is a problem with the system hard disk.

See “Appendix C: Removing the Device Hard Disk”

False Positives

A false positive occurs when a Web site, URL, “infected” file, or email message is incorrectly determined by filtering software to be of an unwanted type. For example, a legitimate email between colleagues may be detected as spam if a job-seeking filter does not distinguish between *resume* (to start again) and *résumé* (a summary of work experience)

You can reduce the number of future false positives in the following ways:

1. Update to the latest pattern file (phishing, virus, spam, and so on).
2. Exempt the item from scanning by adding it to an Approved List.
3. Report the false positive to Trend Micro.

LAN Bypass

LAN bypass is a fault-tolerance solution that allows InterScan Gateway Security Appliance to continue to pass traffic if a software, hardware, or electrical failure occurs.

InterScan Gateway Security Appliance has three (3) user-configurable Copper-based Ethernet ports. Each Ethernet port has two (2) indicator lights that allow you to determine the port’s current state and duplex speed. View the port indicator lights to determine if LAN bypass is currently active.

The following table describes the different LAN bypass triggers and the associated LED indicator status.

TABLE B-1. LED indicator status

Trigger	LED 1 Status	LED 2 Status
Software problems or system rebooting	Yellow	OFF
Power cord is plugged in but device is shutdown	Yellow	OFF
Power cord unplugged	OFF	OFF

ScanEngine Technology

IntelliScan

IntelliScan is a feature in Trend Micro products that allows optimization of scanning time by enabling the product to skip file types that are safe from virus infection.

It is a safe compromise between performance and detection. Users can enable IntelliScan at the gateway or in the desktop so that their product scans only scannable file types. Scannable file types are those that can contain malicious code, such as those known to be used by malware authors.

IntelliScan identifies true file type, such that it detects even renamed Win32 executable files.

IntelliTrap

IntelliTrap scans SMTP and POP3 traffic to catch packed malicious executables sent as attachment to email messages. It is the Scan Engine technology that heuristically catches packed malware at the gateway.

IntelliTrap evaluates attachments by checking for characteristics of compressed Win32 files. It is based on the concept that average users do not usually pack program files and send them through email. On the other hand, malware authors

usually use packers to change the binary image of their programs, and then spam them via email or give them malware mass-mailing capability.

It is designed specifically to catch possibly malicious packed Win32 executable files. It uses the detection name PAK_GENERIC.XXX. To minimize the possibility of false positives, IntelliTrap uses exception patterns for normal software.

As with Trend Micro's other heuristics technologies, IntelliTrap detection is superseded by specific detection.

MacroTrap

MacroTrap is a technology for heuristic detection of MS Office macro viruses. It inspects macro scripts and for tokens that signify malicious nature. It works using rules and exception patterns.

As with Trend Micro's other heuristics technologies, MacroTrap detection is superseded by specific detection.

WormTrap

WormTrap is a technology for heuristic detection of Win32 worms. It checks files for the import table. By doing API matching, it can check if a program calls functions that are commonly used by worms, such as APIs used for mass-mailing and network propagation.

It uses a pattern file that contains the list of APIs to check. To minimize false positives, which may be due to the fact that the APIs it checks for are likely used by legitimate programs such as mailing applications, it uses exception patterns.

As with Trend Micro's other heuristics technologies, WormTrap detection is superseded by specific detection.

Supported DCS Clients

The Trend Micro Damage Cleanup Service (DCS) supports assessment and repair of the following clients:

- Windows 2003 Web, Standard and Enterprise server
- Windows XP Professional
- Windows 2000 Professional/Server/Advanced Server
- Windows NT Server and Workstation

Feature Execution Order

InterScan Gateway Security Appliance executes its features in a particular order for each protocol as follows.

SMTP feature execution order is:

NRS -> Content Filtering -> Content Scanning + Anti-phishing -> Scanning + Anti-spyware + IntelliTrap

POP3 feature execution order is:

Content Filtering -> Anti-spam + Anti-phishing -> Scanning + Anti-spyware + IntelliTrap

HTTP feature execution order is:

File Blocking (Extensions) -> Anti-pharming, Anti-phishing, URL Filtering -> File Blocking (True File type) -> Scanning + Anti-spyware

FTP feature execution order is:

File Blocking (Extensions) -> File Blocking (True File type) -> Scanning + Anti-spyware

Removing the Hard Disk

The InterScan Gateway Security Appliance hard disk needs to be removed only if it develops a problem or fails.

To remove the InterScan Gateway Security Appliance Hard Disk:

1. Remove the bezel from the front of the device.
2. To remove the bezel, locate the two (2) bezel release clasps on the bottom of the bezel.

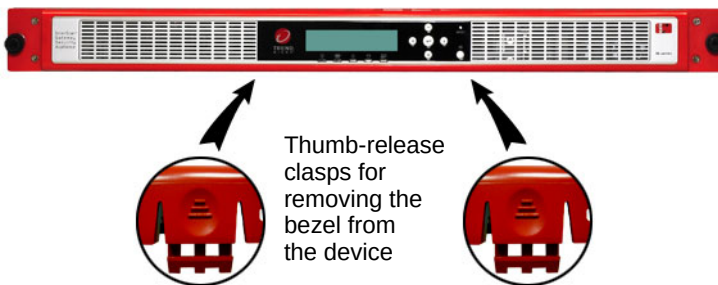


FIGURE C-1. Thumb-release clasps

3. Using both hands, apply pressure to both release clasps until the bottom part of the bezel separates from the device.



FIGURE C-2. Releasing the bezel

4. Gently pull the bezel away from the device paying attention to the clasps at the top of the bezel.
5. Pull the hard disk release lever outward and towards the right to unlock the hard disk tray.

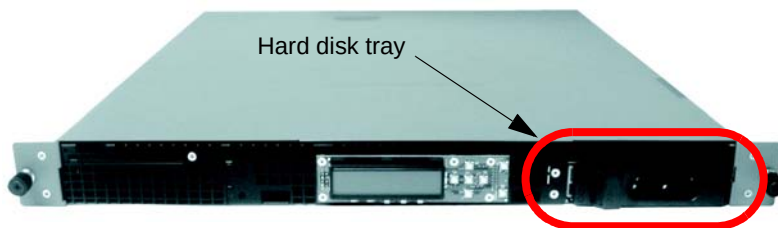


FIGURE C-3. The hard disk tray



FIGURE C-4. Hard disk release lever

6. Gently slide the hard disk tray out of the device.

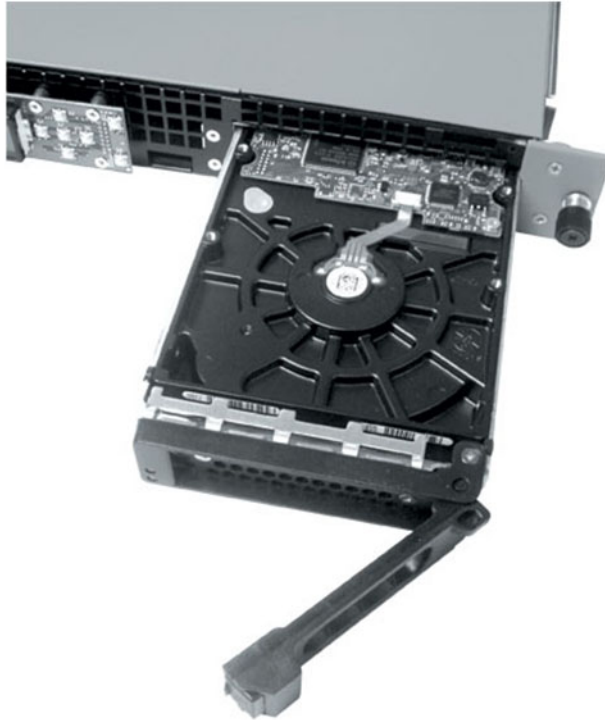


FIGURE C-5. InterScan Gateway Security Appliance hard disk

Note: The InterScan Gateway Security Appliance hard disk needs to be equal to or greater than 80GB. InterScan Gateway Security Appliance only uses 80GB of hard disk space. Additional drive space will be unused.

System Checklist

You must provide the following device address information during preconfiguration. The settings can be changed after preconfiguration.

TABLE D-1. Device address checklist

Information required	Sample	Your value
InterScan Gateway Security Appliance Information	Device Address	
IP address	10.1.104.50	
Subnet mask	255.255.254.0	
Host name	name.domain.com	
Gateway	10.1.104.60	
Primary DNS	10.1.107.40	
Secondary DNS	10.1.107.50	

File Formats Supported

Compression Types

The InterScan Gateway Security Appliance scan engine can extract and scan files compressed using any of the most popular compression types (listed below). InterScan Gateway Security Appliance can also check for viruses being "smuggled" within nested compressions, for example, an infected file that is zipped, ARJ-compressed, MS-compressed, and zipped again.

The maximum number of recursive scan layers is 20. You can set this limit from the **Scanning > Target** pages of the Web console, for all four protocols.

Support Compression Types include the following:

TABLE E-1. Supported compression types

Supported Compression Types
ZIP
ZIP to EXE
Cabinet (.cab)
ARJ
ARJ to EXE
TAR
GZIP (.gz)
BZIP and BZIP2
ASPAC
UPX
LHA
LHA to EXE

TABLE E-1. Supported compression types (Continued)

MSCOMP
LZEXE
PKLite
Diet
UNIX LZW compress(.Z)
UNIX pack(.z)

Blockable File Formats

InterScan Gateway Security Appliance can scan for and block certain types of files that originate from FTP servers. You can configure File Blocking from the **FTP > File Blocking** menu of the Web console.

Blockable File Formats include the following:

TABLE E-2. Blockable file formats

File Type	Formats
Audio/Video	Advanced Streaming Format, Quick Time Media, MPEG, Apple Sound, Audio InterChange File Format from Apple/SGI, Nullsoft AVS Files, BAR CDA Music Track File Format, CHL File, Macromedia Director Cast, Diamondware Digitized Sound, Amiga 8SVX Audio InterChange File Format, InterVoice Files, Mathlab Sound, MAUD Sample Format, Multiple-image Network Graphics, Gravis Patch Files, Real Audio, Lotus ScreenCam Movie, MIDI Sample Sound, IRCAM, Sonic Foundry File, SampleVision Sound, Sndtool Sound File, Yamaha tx-16w, Con-vox V8 File, Psion Audio Files, Audio, Microsoft RIFF, Creative Lab CMF, MIDI, MP3, Real Media, Creative Voice Format (VOC)
Compressed	MSCOMP, unix cpio archive, LHA, unix ar archive, ARC, TAR, RAR, TeleDisk Image, Macintosh MacBinary, GNU BZIP2, Fujitsu AMG compressed type, ARJ, GNU ZIP, LZW, MS Cabinet, PKZIP
Executable	COM (see subtype VSDT_COM), EXE (see subtype VSDT_EXE), NT/95 SHORTCUT(*.lnk), MAC, MACROMEDIA DIRECTOR SHOCK-WAVE MOVIE, UNINSTALL SCRIPTS, SHORTCUT TO MICROSOFT PROGRAM, TREND MICRO DEFINED TYPE, SCRIPT CUSTOMER - DEFINED TYPE MATCH, COREL GLOBAL MACRO, COMPILED TERMINFO ENTRY, UNIX CORE FILE, WINDOWS GROUP, PA-RISC EXECUTABLE, PA-RISC DEMAND-LOAD EXECUTABLE, PA-RISC SHARED EXECUTABLE, PA-RISC DYNAMIC LOAD LIBRARY, PA-RISC SHARED LIBRARY, COMPILED LISP, HP s800 EXECUTABLE, HP s800 SHARED EXECUTABLE, 4016 HP s800 DEMAND-LOAD EXECUTABLE, 4017 HP S800 SHARED LIBRARY, 4018 HP s800 DYNAMIC LOAD LIBRARY, 4019 PA-RISC RELOCATABLE OBJECT, 6002 BINHEX, 6006 NETWARE LOADABLE MODULE, 6011 NOVELL SYSTEM PRINTDEF DEVICE DEFINITION, 6012 NOVELL HELP LIBRARIAN DATA FILE, 6013 NETWARE UNICORE RULE TABLE FILE

TABLE E-2. Blockable file formats (Continued)

Images	WINDOWS FONT, WINDOWS ICON, SUN GKS, PCX, PPM IMAGE, AUTODESK ANIMATOR (FLI OR FLC) (see subtype VSDT_FLI), PORTABLE NETWORK GRAPHICS, PAIN SHOP PRO, TARGA IMAGE, MACINTOSH BITMAP, ENCAPSULATED POSTSCRIPT, ANIMATED CURSOR, TERRAGEN ATMOSPHERE, SGI IMAGE, CINEMA 4D, COMPUTER GRAPHICS METAFILES, CALIGARI TRUESPACE FILE, AUTOCAD DWG (see subtype VSDT_DWG), FREE HAND DOCUMENT, SOFTIMAGE, INTERLEAF IMAGE, GEM IMAGE, IMAGINE 3D OBJECT, LIGHTWAVE 3D OBJECT, MAGICK IMAGE FILE FORMAT, ATARI NEOCHROME, PALMPILOT IMAGE, ADOBE FONT FILE, WAVEFRONT RLA, SCULPT 3D/4D SCENE, SOLITAIRE IMAGE RECORDER, TERRAGEN SURFACE, TERRAGEN TERRAIN, TERRAGEN WORLD, BITMAP IMAGE YUV12, WEBSHOTS COLLECTION, WINDOWS METAFILE, COREL PHOTO-PAINT, WINDOWS BMP, JPEG, HP-WINDOWS FONT, MICROSOFT PAINT v1.x, MICROSOFT PAINT v2.x, TIFF, SUN RASTER(RAS), ADOBE PHOTOSHOP(PSD), TRUE TYPE COLLECTION, GIF
Java	JAVA Applets
Microsoft documents	WORD FOR WINDOWS, WINDOWS POWERPOINT, EXCEL FOR WINDOWS, WINDOWS WRITE (see subtype VSDT_WRT), WINDOWS CALENDAR, MICROSOFT ACCESS (MDB) (see subtype VSDT_MDB), PROJECT FOR WINDOWS, COREL PRESENTATION EXCHANGE, WINDOWS CLIPBOARD, WORDPERFECT, MS WORD/DOS 4.0/5.0, HLP, ADOBE FONT (see subtype VSDT_ADB), WINDOWS CARDFILE, FRAMEMAKER (see subtype VSDT_FM), POSTSCRIPT, MICROSOFT RTF, ADOBE PORTABLE DOCUMENT FORMAT FILE (see subtype VSDT_PDF), MACROS IN MS OFFICE COMPRESSED BY ACTIVEMIME

Malware Naming Formats

Malware, with the exception of boot sector viruses and some file infectors, is named according to the following format:

`PREFIX_THREATNAME_SUFFIX`

The suffix used in the naming convention indicates the variant of the threat. The suffix assigned to a new threat (meaning the binary code for the threat is not similar to any existing threats) is the alpha character “A.” Subsequent strains are given subsequent suffixes, for example, “B”, “C”, “D”. Occasionally a threat is assigned a

special suffix, (.GEN, for generic detection or.DAM if the variant is damaged or malformed).

TABLE E-3. Malware naming

Prefix	Description
No prefix	Boot sector viruses or file infector
1OH	File infector
ADW	Adware
ALS	Auto-LISP script malware
ATVX	ActiveX malicious code
BAT	Batch file virus
BHO	Browser Helper Object - A non-destructive toolbar application
BKDR	Backdoor virus
CHM	Compiled HTML file found on malicious Web sites
COOKIE	Cookie used to track a user's Web habits for the purpose of data mining
COPY	Worm that copies itself
DI	File infector
DIAL	Dialer program
DOS, DDOS	Virus that prevents a user from accessing security and antivirus company Web sites
ELF	Executable and Link format viruses
EXPL	Exploit that does not fit other categories
FLOODER	Tool that allows remote malicious hackers to flood data on a specified IP, causing the target system to hang
FONO	File infector
GCAE	File infector
GENERIC	Memory-resident boot virus
HKTL	Hacking tool
HTML	HTML virus
IRC	Internet Relay Chat malware

TABLE E-3. Malware naming (Continued)

JAVA	Java malicious code
JOKE	Joke program
JS	JavaScript virus
NE	File infector
NET	Network virus
PALM	Palm PDA-based malware
PARITY	Boot virus
PE	File infector
PERL	Malware, such as a file infector, created in PERL
RAP	Remote access program
REG	Threat that modifies the system registry
SPYW	Spyware
SYMBOS	Trojan that affects telephones using the Symbian operating system
TROJ	Trojan
UNIX	Linux/UNIX script malware
VBS	VBScript virus
WORM	Worm
W2KM, W97M, X97M, P97M, A97M, O97M, WM, XF, XM, V5M	Macro virus

Specifications and Environment

Hardware Specifications

InterScan Gateway Security Appliance uses the following components:

TABLE F-1. Hardware specifications

Component	Specification
CPU	LGA 775 Pentium 3.0GHz
Chipset	915GV
Memory	1GB (512MB x 2)
Compact Flash	512MB
HDD	80GB SATA I hard disk
LAN Devices	PCI LAN card x 1 (supports LAN Bypass) onboard LAN: (management port)

Dimensions and Weight

The following specifications apply to InterScan Gateway Security Appliance:

TABLE F-2. InterScan Gateway Security Appliance dimensions and weight

Element	Measurement
Chassis dimension with bezel (D x W x H)	Depth: 505 mm Width: 430 mm Height: 42.4 mm
System weight	9Kg (19.8lbs)

Power Requirements and Environment

The following power requirements and environmental specifications apply to InterScan Gateway Security Appliance::

TABLE F-1. The appliance power requirements and environmental specifications

Element	Specification
DC power receptacle	Connects to the power cable.
Power switch	Turns the device on and off.
AC input voltage	90 to 264VAC (100 to 240 nominal)
AC input current (90VAC)	8.0A
AC input current (180VAC)	4.0A
Frequency	47 to 63Hz (50/60 nominal)
NORMAL OPERATING AMBIENT TEMPERATURE (AT SEA LEVEL)	
Minimum (operating and idle)	32°F (0°C)
Maximum (operating, power supply on)	104°F (40°C)
Maximum rate of change	50°F per hour (10°C per hour)
STORAGE TEMPERATURE (AT SEA LEVEL)	
Minimum	-4°F (-20°C)
Maximum	158°F (70°C)
Maximum rate of change	68°F per hour (15°C per hour)
HUMIDITY	
Maximum (operating)	80% non-condensing
Maximum (non-operating)	95% non-condensing

Index

A

- Access Control 3-2, 12-3, 14-2
 - enable external access 12-3
 - enabling 12-3
- Activation Code
 - obtaining 1-16
- Activation code
 - entering a new AC 12-17
- ActiveX malicious code 2-13
- Administration
 - Access Control 12-3
 - World Virus Tracking 12-23
- AFFU.exe 14-36
- Anti-pharming
 - Anti-pharming log 2-16
- Anti-phishing
 - Anti-phishing Services 1-7
 - approved and blocked senders lists 2-8
 - email links 2-15
 - outbound URL requests 2-15
 - URL rating database 2-16
- Anti-spam
 - Anti-spam engine 2-7
 - Anti-spam Services 1-7
 - approved and blocked senders lists 2-7, 2-9
 - configuration 1-4
 - Content Scanning log 2-6
 - Keyword Exception List 2-10
 - Keyword Exceptions List 2-7
 - Network Reputation Services (NRS) 2-11
 - Network Reputation Services log 2-6
 - Network Reputation Services QIL 2-10
 - Network Reputation Services Real-Time Blackhole List (RBL) 2-11
 - spam detection levels 2-7
 - wildcard matching 2-9
- Anti-spyware
 - Anti-spyware Services 1-6
 - cleanup template 2-15
 - pattern file 2-15
 - scan engine 2-15

Antivirus

- ActiveX malicious code 2-13
- Antivirus Services 1-6
- COM and EXE file infectors 2-13
- HTML viruses 2-13
- Macro viruses 2-13
- Appliance Firmware Flash Utility 14-1
 - baseboard management controller 14-1
 - BMC 14-1
 - detecting an IP address 14-35
 - launching from the Solutions CD 14-35
 - user name and password 14-35
- Auto-switching/sensing capability 13-5

B

- Back Panel
 - AC power receptable 1-12
 - elements 1-12
 - fan vent 1-12
 - port indicator status 1-13
 - port indicators 1-13
 - power switch 1-12
 - UID LED and UID button 1-12
 - USB ports 1-12
- Backup
 - configuration 12-4–12-5, 14-3
 - configuration information 14-4
- Baseboard management controller 14-1
- Bezel
 - front panel 1-9
- BIOS
 - checksum field 14-39
 - DC OFF LAN Bypass Configuration 13-5
 - flashing 14-39
- BIOS firmware upload
 - after the upload, IGSA will auto-restart 14-39
- BIOS firmware, name of file 14-36
- BIOS update 14-36
 - preparing to upload IGSA BIOS 14-36
 - troubleshooting 14-39
 - uploading the IGSA BIOS firmware 14-37
- Blockable file formats E-4
- BMC 14-1

BMC update

- auto-restart of IGSA 14-36
- troubleshooting 14-39

BOT defined 2-2

Browser support

- Internet Explorer 6.x 1-3
- Mozilla Firefox 1.x 1-3

C

CF card 14-3

Compact Flash card 14-3

Compression Types scanned E-2

Configuration

- backup 14-3

Configuration Backup

- back up current configuration 12-4
- restore configuration from backup 12-5
- restore configuration to default settings 12-5

Configuration Backup screen 14-4

Connecting to the network

- EXT port 1-15
- INT port 1-14

CONSOLE port 14-29

Contact us 1-2

Contacting Technical Support 13-2

Content and URL filtering (HTTP traffic) 1-8

Content filtering in SMTP 4-29

Controlling access to the device 12-3

Crossover network cable 13-5

D

Damage Cleanup 8-7

- configuring 8-6

Damage Cleanup Services

- supported DCS clients B-6

DC OFF LAN Bypass Configuration 13-5

Deferred Scan B-2

Device

- dimensions and weight F-2

Device connectivity

- ping 1-15
- testing 1-15

Device Image 14-2

- update 14-2

Device image

- downloading it from the Trend Micro Web site 14-4

Device image. See Firmware.

Dimensions and weight F-2

Disk SMART Test

- Scheduled disk SMART test, enable 12-5

Document conventions -xiii

Documentation feedback 1-2

E

Email notifications 13-5

Troubleshooting

- 13-4

Ethernet cable 13-5

European Institute for Computer Antivirus Research (EICAR)

- EICAR test virus 13-11

EXT port 1-15

F

Factory default settings 13-5

False Positives B-3

FAQs 13-4

- can I ping IGSA? 13-5

- Can I use the USB ports to transfer files? 13-5

- Is a crossover network cable needed? 13-5

- RESET Pinhole 13-5

- What is the purpose of the "ID" LED? 13-4

- Why am I not receiving email notifications? 13-5

- Why does quarantine action fail? 13-6

- Why is traffic not passing through device when power is off? 13-5

- Will IGSA still work if hard disk is not working? 13-5

Feature execution order B-6

File Blocking

- types 2-18

File Handling

- handling compressed files 13-12

- handling large files 13-14

Firefox 1.x, support for 1-3

Firmware 14-2

- update 14-2

Firmware Flash Utility 14-34

Firmware Flash Utility. See Appliance Firmware
Flash Utility.

Firmware update

- acquiring IP address of IGSA BMC 14-35

- avoiding an IP conflict 14-5

- back up your configuration 14-3

- baseboard management controller 14-5

- before updating the device image 14-3

- BIOS

 - after the upload, IGSA will auto-restart 14-39

- BIOS update 14-36

 - IP range 14-39

 - preparing to upload IGSA BIOS 14-36

 - uploading the IGSA BIOS firmware 14-37

- BMC 14-33

- BMC firmware

 - troubleshooting 14-39

- BMC update

 - auto-restart of IGSA 14-36

 - CPU fans run at full speed 14-36

 - IP range 14-39

- changing the IP address of the local computer 14-5

- checklist 14-3

- connecting a local computer to deliver the update
14-5

- CONSOLE port 14-29

- getting IP address of local PC 14-9

- rescue mode 14-5

- uploading BMC firmware 14-36

- uploading device image and keeping existing
configuration 14-5

- uploading device image and restoring default

 - IGSA configuration 14-5

- uploading the BMC firmware 14-33

- uploading with option 3

 - ensuring that local computer is in same seg-
ment 14-6

 - serial port 14-6

- uploading with option 5 14-5

- using the LCD module 14-2

Flash BIOS 14-39

Frequently asked questions 13-4

Frequently Asked Questions (FAQ) 13-4

Front Panel

- control panel 1-10

- LCD Module 1-9–1-10

- LED indicators 1-10

- removable bezel 1-9

- reset button 1-10

- thumb screws 1-9

- UID button 1-10

FTP

- Anti-spyware

 - block all spyware files 6-10

 - configure Action 6-10

 - configure spyware/grayware exclusion list 6-8

 - configure Target 6-8

 - enable 6-8

 - pass spyware files 6-10

 - scan for all types 6-9

 - scan for specific types 6-9

 - search online for spyware/grayware 6-8

 - select Notification recipients 6-11

- Antivirus

 - allow infected files to pass 6-6

 - block infected files 6-6

 - clean infected files 6-6

 - configure Action 6-5

 - configure Target 6-3

 - do not scan 50MB+ files 6-5

 - enable 6-2

 - enable deferred scanning 6-5

 - scan all files 6-4

 - scan based on different criteria 6-5

 - scan specified files by extension 6-4

 - scan using IntelliScan 6-4

 - select notification recipients 6-7

 - specify files to scan 6-4

- File Blocking

 - block selected file types 6-12

 - block specified file extensions 6-13

 - configure notifications 6-14

 - configure Target 6-12

- scanning support 1-4

G

Getting started

- Preliminary task list 3-2

H

Hard Disk

- Diskless mode B-2

Hardware specifications F-2

Help system 3-14, 3-16

Hot Fixes 13-8

HTML viruses 2-13

HTTP

Anti-pharming

- allow access to Website 5-13
- block access to Website 5-13
- configure Action 5-13
- configure Notification 5-13
- configure Target 5-12
- enable 5-12

Anti-phishing

- allow access to Website 5-15
- block access to Website 5-15
- configure Action 5-15
- configure notification 5-16
- configure Target 5-14
- enable 5-14

Anti-spyware

- allow download of spyware 5-10
- block files with spyware 5-10
- configure Action 5-10
- configure Spyware/Grayware Exclusion List 5-9
- configure Target 5-9
- enable 5-9
- scan for spyware/grayware 5-10
- search online for spyware/grayware 5-9
- select Notification recipients 5-11

Antivirus

- block infected files 5-7
- clean infected files 5-6
- configure Action 5-6
- configure Target 5-3
- enable 5-2
- exclude files from scan 5-5
- maximum file size to scan 5-5
- pass infected files 5-7
- scan all files 5-4
- scan specified files by extension 5-4

- scan using IntelliScan 5-4

- select notification recipients 5-7

- specify files to scan 5-4

Content and URL Filtering 1-8

File Blocking

- block selected file types 5-23
- block specified file extensions 5-23
- configure Target 5-22
- enable 5-22
- select notification recipients 5-24

scanning support 1-4

URL Filtering

- configure notification 5-21
- configure Proxy Settings 5-20
- configure Settings 5-19
- configure work time settings 5-19
- enable Proxy Settings 5-19
- filter selected categories 5-17

URL Filtering Rules

- configure Approved URL List 5-18
- configure Blocked URL List 5-18
- enable 5-18
- filter during leisure time 5-18
- filter during work time 5-18

HyperTerminal 14-2, 14-29

- COM Properties screen 14-31

I

- INT port 1-14, 14-5

- IntelliScan 2-19, 5-4, 6-4

- IntelliScan defined B-4

- IntelliTrap 1-3, 4-14–4-16

- defined B-4

- detecting bots in compressed files 2-13

- Log 2-14

- virus scan engine 2-13

- Internal outbreak 8-5

- Internet Explorer 6.x, support for 1-3

- InterScan Gateway Security Appliance

- described 1-2

- features and benefits 1-3

- How it works 1-5

- IP Address

- Anti-spam, exclude from filtering 4-18

-
- IP address
 - DHCP server, assigning using a 1-14
 - dynamic or static 1-14
 - LCD Module, assigning using a 1-14
 - Preconfiguration console, assigning using a 1-14
 - IP Address Settings
 - add Static route
 - Static route 12-8
 - configure IP Address for updates 12-7
 - delete Static route 12-10
 - modify static route 12-9
 - IP Address settings
 - example of static routes 12-10

L

- LAN Bypass
 - passing traffic if failure occurs B-3
- LAN bypass 1-14
- LCD Module 14-2
- License 12-16
 - update manually 12-17
 - view detailed license online 12-17
 - view info about your license 12-17
 - view license renewal instructions 12-16
- Licenses 13-9
- Log module
 - log query 2-22
- Logs 11-2
 - backing up your configuration 14-3
 - log query, additional screen actions 11-4
 - log query, performing a 11-3
 - log settings, configuring 11-5
 - logs in diskless mode, remote machine 11-5
 - Maintenance, automatic 11-7
 - maintenance, manual 11-6

M

- Macro viruses 2-13
- MacroTrap defined B-5
- Malware naming formats E-5
- Malware types 2-2
- Management port 14-5
- Manual update 3-6
- Minicom 14-2
- Mozilla Firefox 1.x, support for 1-3

N

- Network Reputation Services
 - QIL database 1-4
 - Real-Time Blackhole List (RBL) 1-4
- No Connection 13-4
- Notification Settings
 - Events, maximum notifications per hour 12-13
 - settings, SMTP administrator email address 12-12
 - settings, SMTP server and Port 12-12
 - settings, SMTP user name and password 12-12
- Notifications
 - inline virus stamp 4-9
 - inline virus-free stamp 4-9
- NRS. See Network Reputation Services.

O

- Obtaining Activation Code 1-16
- Obtaining Registration Key 1-16
- On/off switch
 - turning off the device 14-33, 14-37
- Online Help System 3-14
 - context-sensitive Help 3-16
- Operation Mode
 - fully transparent or transparent proxy mode 12-14
- OPP. See Outbreak Prevention Policy.
- OPS
 - red alerts 8-10
 - yellow alerts 8-10

Outbreak Defense 1-3

- Current Status screen 8-3

- Damage Cleanup Exception List, add non-Windows clients 8-7

- Damage Cleanup Services 8-2

- Damage Cleanup, configuring 8-6

- internal outbreak 8-5

- Internal Outbreak, apply older Outbreak

 - Prevention Policy 8-5

- Outbreak Defense Services 1-8

- Outbreak Prevention Policy 8-2

- Outbreak Prevention Policy, stopping the 8-4

- Outbreak Prevention Services 8-2

- Potential Threat 8-7

- Potential Threat, enable Damage Cleanup 8-7
- red alerts 8-10

- settings, automatic deployment 8-8

- settings, configure download frequency 8-9

- Settings, configure notifications 8-9

- settings, enable auto deployment for red alerts 8-8
- settings, enable auto deployment for yellow alerts 8-8

- yellow alerts 8-10

Outbreak Defense Services

- ActiveUpdate servers 2-20

- Damage Cleanup Services (DCS) 2-21

- Outbreak Prevention Policy 2-20

Outbreak Prevention Policy 8-2

P

Password

- changing the password 12-15

- default password 3-3

- entering the password 3-3

- recovering a password 13-6

Patches 13-8

Pattern Files

- Spam Engine and Pattern File 13-8

- Virus Pattern File 13-7

Pharming 5-13

- defined 2-2

- log 2-16

- URL rating database 2-16

Phish

- approved and blocked senders lists 2-8

- configure action 4-24

- defined 2-2

- email links 2-15

- enable scanning of SMTP traffic for 4-23

- notify recipients of 4-25

- outbound URL requests 2-15

- URL rating database 2-16

Ping 13-5

POP3

Anti-phishing

- configure Action 7-19

- configure Target 7-19

- enable 7-19

- select Notification recipients 7-20

- stamp subject line 7-20

Anti-spam

- add approved senders 7-17

- add blocked senders 7-17

- configure Action 7-18

- configure Target 7-17

- enable 7-17

- select detection level 7-17

- set keyword exceptions 7-17

Anti-spyware 7-11

- configure Action 7-11

- configure spyware/grayware exclusion list 7-9

- configure Target 7-9

- delete message and attachment 7-11

- enable 7-9

- pass items 7-11

- remove spyware and pass 7-11

- scan all types 7-10

- scan specific types 7-10

- search online for spyware/grayware 7-9

- select Notification recipients 7-12

- send message and quarantine attachment 7-11

-
- Antivirus
 - clean infected items and pass 7-6
 - configure Action 7-5
 - configure Target 7-4
 - enable 7-2
 - exclude by different criteria 7-5
 - Quarantine 7-6
 - remove infected items 7-6
 - scan all files 7-4
 - scan specified files by extension 7-4
 - scan using IntelliScan 7-4
 - select Notification recipients 7-7
 - specify files to scan 7-4
 - virus detected notification 7-8
 - virus free notification 7-8
 - Content Filtering
 - configure Action 7-24
 - configure Target 7-23
 - delete message and attachments 7-24
 - deliver message and attachments 7-24
 - enable 7-23
 - filter by attachment True Type 7-23
 - filter by message attachment 7-23
 - filter by message size 7-23
 - filter by text in body 7-23
 - filter by text in header 7-23
 - Quarantine email and attachments 7-24
 - select Notification recipients 7-25
 - IntelliTrap
 - configure Action 7-14
 - delete message and attachment 7-14
 - deliver message and deleted infected item 7-14
 - detect and pass 7-14
 - enable 7-13
 - Quarantine 7-14
 - select Notification recipients 7-15
 - scanning support 1-4
 - Power requirements and environment F-2
 - Power switch
 - turning off the device 14-37
 - Preconfiguration console 14-2
 - change default password 14-32
 - default password 14-31
 - preparing 14-6, 14-29
 - Primary Functional Components
 - Anti-pharming URL rating database 2-16
 - Anti-phishing Services 2-15
 - Anti-spam Services 2-6
 - anti-spyware services 2-14
 - Antivirus Services 2-12
 - Content Filtering Services 2-6
 - Ethernet Network Interfaces 2-4
 - File Blocking 2-18
 - IntelliTrap Services 2-13
 - log module 2-22
 - mail notification module 2-21
 - Outbreak Defense Services 2-20
 - quarantine 2-22
 - Real-Time Scan of protocols 2-5
 - The Delete Function 2-22
 - URL filtering 2-17
 - Virus Scan Module, True File Type 2-19
 - Web console 2-5
 - Product License 12-16
 - enter new activation code 12-17
 - update license manually 12-17
 - view detailed license online 12-17
 - view info about your license 12-17
 - view license renewal instructions 12-16
 - Program file 14-2
 - update 14-2
 - Program file. See Firmware.
 - Proxy settings
 - configure proxy settings 12-19
 - use a proxy server 12-19

Q

Quarantine

- maximum number of messages in 13-6
- maximum size of message in 13-6
- total size of 13-6

Quarantines

- exporting query results list to comma-delimited file 9-4
- maintenance
 - automatic 9-8
 - delete all files 9-7
 - delete files older than x days 9-7
 - enable automatic purge 9-8
 - manual 9-7
- maximum message limit 9-2
- quarantine query 2-22
- query
 - delete messages from query results list 9-4
 - example of exported query file 9-6
 - execute query 9-4
 - select criteria 9-3
- query results list 9-4
- viewing contents of exported file 9-4

Query logs 11-3

R

Readme.txt

- reading enclosed readme documents 13-3

Red Alerts 8-10

Registration Key

- obtaining 1-16

Reset 13-5

RESET Pinhole 13-5

RJ-45 13-5

S

Scan Engine Technology B-4

IntelliScan defined B-4

IntelliTrap defined B-4

MacroTrap defined B-5

WormTrap defined B-5

Service Packs 13-8

Simple Network Management Protocol (SNMP)

SNMP Settings, enable 12-20

SMTP

Anti-phishing

- configure action 4-24
- enable 4-23
- select notification recipients 4-25

Anti-spam

- enable 4-20
- exclude IP address from filtering 4-18
- select detection level 4-20

Anti-spam (Content Scanning)

- configure target 4-20

Anti-spam (content scanning)

- configure action 4-22

Anti-spam Network Reputation Services (NRS)

- configure action 4-19
- configure target 4-17

QIL 4-19

Real-Time Blackhole List (RBL) 4-19

Anti-spyware

- choose action when spyware detected 4-12
- configure Action 4-12
- configure exclusion list 4-10
- configure Target 4-10
- delete 4-12
- enable 4-10
- pass 4-12
- Quarantine 4-12
- remove spyware/grayware and pass 4-12
- select notification recipients 4-13

-
- Antivirus
 - clean infected items and pass 4-6
 - configure Action 4-6
 - configure Targets 4-4
 - enable 4-3–4-4
 - files to exclude 4-5
 - inline virus notification stamps 4-9
 - inline virus-free notifications stamp 4-9
 - pass all items 4-7
 - quarantine 4-6
 - remove infected items 4-7
 - scan all files 4-4
 - scan files by extension 4-4
 - select notification recipients 4-8
 - use IntelliScan 4-4
 - content filtering
 - configure action 4-28
 - configure target 4-27
 - select notification recipients 4-29
 - IntelliTrap
 - configure action 4-15
 - configure target 4-14
 - select notification recipients 4-16
 - scanning support 1-4
 - SMTP services described 4-2
 - Spyware/grayware, online search 4-10
 - SNMP Settings
 - configure SNMP settings 12-21
 - Solutions CD 14-34, 14-37
 - Firmware Flash Utility 14-34
 - Firmware Flash Utility section 14-34
 - Spam
 - anti-spam engine 2-7
 - approved and blocked senders lists 2-7, 2-9
 - configure scanning of SMTP for 4-22
 - configure target (SMTP traffic) 4-20
 - defined 2-2
 - detection levels 2-7
 - excluding IP address from filtering (SMTP) 4-18
 - Keyword Exceptions List 2-7
 - Network Reputation Services 4-19
 - real-time blackhole list 4-19
 - scan SMTP traffic for 4-20
 - select detection level for SMTP traffic 4-20
 - wildcard matching 2-9
 - Spam. See Anti-spam.
 - Spyware 5-10–5-11
 - allowing it through 4-12
 - block files with spyware 5-10
 - cleanup template 2-15
 - configure SMTP exclusion list 4-10
 - configure target for (SMTP) 4-10
 - consequences 2-14
 - defined 2-2
 - enable scanning of SMTP traffic for 4-10
 - exclusion list 5-9
 - grayware 2-14
 - pattern file 2-15
 - quarantine 4-12
 - removing (SMTP traffic) 4-12
 - scan engine 2-15
 - scan HTTP for spyware/grayware 5-10
 - select people to notify of 4-13
 - Spyware. See Anti-spyware.
 - Spyware/grayware, online search 4-10
 - Static route 12-9–12-10
 - Static routes 12-10
 - Submit potential threat URL to TrendLabs 13-16
 - Summary Screen 3-4
 - Anti-spam Content Scanning 3-10
 - Anti-spam Network Reputation Services 3-11
 - Anti-spyware 3-9
 - Antivirus 3-8
 - Component Version 3-6
 - Components, manually updating 3-6
 - Damage Cleanup Service 3-5
 - IntelliTrap 3-9
 - others 3-11
 - Outbreak Prevention Service (OPS) 3-5
 - reset all counters 3-11
 - Switch
 - turning off the device 14-37
 - Switch, turning off the device 14-33
 - System Time
 - configure NTP Server 12-22
 - select Region/Country 12-22
 - set time zone 12-22

T

- Technical Support, contacting 13-2
- Terminal interface 14-2
- Testing device connectivity
 - browse the Web 1-15
 - ping 1-15
- Transparent proxy mode 12-14
- TrendLabs
 - submitting potential threat URL to 13-16
- Trojans defined 2-2
- Troubleshooting
 - frequently asked questions 13-4
 - HyperTerminal 13-4
 - power switch 13-4
 - quarantine 13-6
- True File Type 2-19

U

- Update
 - configure Update Source 10-6
 - Manual Update 3-6
 - manual update 10-3
 - manual update, select components to update 10-3
 - Rollback 3-7
 - rollback 10-4
 - rollback, select components for rollback 10-4
 - scheduled update, enable 10-5
 - scheduled update, select components to update 10-5
 - scheduled, specify update duration and frequency 10-5
 - select components to update 3-6
- Update source 10-6

URL

- allowable categories 2-17
 - Content and URL Filtering 1-8
 - file blocking 1-4
 - filtering log 2-17
 - Website filtering 1-4
- URL See HTTP listings

V

- Virus map 12-24
- Virus Scan Module
 - IntelliScan 2-19
- Virus tracking 12-24
- Virus. See Antivirus.
- Viruses defined 2-2
- VT100J 14-29

W

- Web console
 - accessing the console 3-3
 - interface components 3-12
 - Log On screen 3-3
 - logout link 3-13
 - navigating the console 3-12
 - navigation menu 3-12
 - Online Help 3-13
 - password, entering the 3-3
 - working area 3-12
- World Virus Tracking
 - participating in program 12-23
 - viewing Trend Micro Virus Map 12-24
- Worms defined 2-2
- WormTrap defined B-5

Y

- Yellow Alerts 8-10