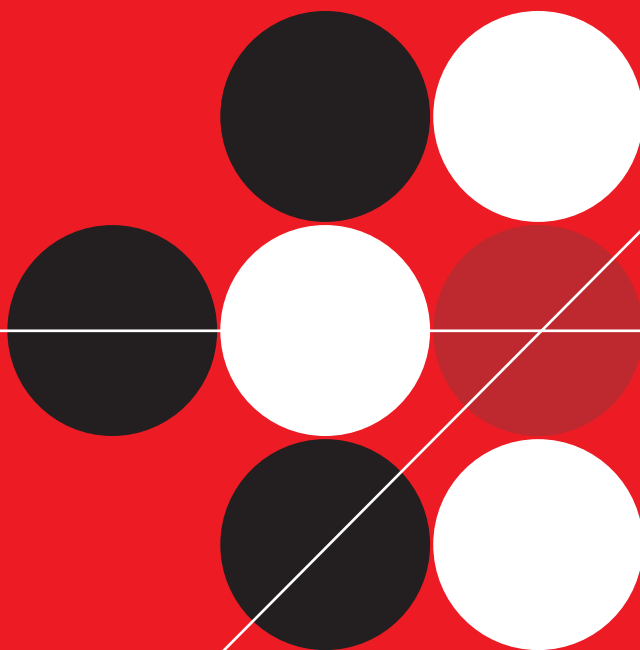


TREND MICRO™

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. 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© 2006-2007 Trend Micro Incorporated. All rights reserved.

Document Part No. SAEM13084/70207

Release Date: February 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

About This Manual

Audience	xiv
About This Administrator's Guide	xiv
Document Conventions	xvi

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
Anti-Pharming	1-8
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	1-16
Activating the Appliance	1-16

Chapter 2: Deployment Options

Overview	2-2
Deployment Topologies	2-4
Deploying in a Single Network Segment	2-4
Deploying in a Network with Multiple Segments	2-5
Basic Deployment	2-8
Advanced Deployment Scenarios	2-9
Operation Modes	2-9
Transparent Proxy Mode	2-10
Fully Transparent Proxy Mode	2-11
Deployment in a DMZ Environment	2-12
Failover Deployment	2-14
Failover Deployment Scenario	2-15
LAN Bypass and Link State Failover Settings	2-16
Deployment Recommendations	2-17
Deployment Issues	2-18
Preconfiguring the Appliance	2-19
Assigning an IP Address	2-19
Connecting to the Network	2-20
Testing the Appliance Connectivity	2-21
Activating the Appliance	2-21

Chapter 3: How InterScan Gateway Security Appliance Works

The Range and Types of Internet Threats	3-2
How InterScan Gateway Security Appliance Protects You	3-3
The Primary Functional Components	3-4
Ethernet Network Interfaces	3-4
Real-Time Scan of SMTP, POP3, HTTP, and FTP Protocols	3-5
The Web Console	3-5
Content Filtering	3-5
Anti-Spam	3-6
The Trend Micro Anti-Spam Engine	3-7
Approved and Blocked Senders Lists	3-8
Using Network Reputation Services	3-10
True File Type and IntelliScan	3-18
Outbreak Defense Services	3-19
Mail Notification	3-21
Logs	3-21
Quarantine	3-21

Chapter 4: Getting Started with InterScan Gateway Security Appliance

Preliminary Tasks	4-2
Accessing the Web Console	4-3
The Summary Screen	4-4
Information Above the Panels	4-4
Outbreak Prevention Service	4-5
Damage Cleanup Service	4-5
Component Version	4-6
Antivirus	4-8
Anti-Spyware	4-9
IntelliTrap	4-9
Anti-Spam: Content Scanning	4-10
Anti-Spam: Network Reputation Services	4-11
Others	4-11
Additional Screen Actions	4-11
Navigating the Web Console	4-12
The Online Help System	4-14

Chapter 5: SMTP Services

SMTP Services	5-2
Enabling Scanning of SMTP Traffic	5-3
Selecting an Alternative Service Port	5-3
Configuring SMTP Virus Scanning	5-4
SMTP Scanning - Target	5-5
SMTP Scanning - Action	5-7
SMTP Scanning - Notification	5-9
Configuring SMTP Anti-Spyware	5-11
SMTP Anti-Spyware - Target	5-11
SMTP Anti-Spyware - Action	5-13
SMTP Anti-Spyware - Notification	5-14
Configuring SMTP IntelliTrap	5-15
SMTP IntelliTrap - Target	5-15
SMTP IntelliTrap - Action	5-16
SMTP IntelliTrap - Notification	5-17

Chapter 5: SMTP Services—continued

Configuring SMTP Anti-Spam: Network Reputation Services ...	5-18
SMTP Anti-Spam: Network Reputation Services - Target	5-18
SMTP Anti-Spam: Network Reputation Services - Action	5-20
Configuring SMTP Anti-Spam: Content Scanning	5-21
SMTP Anti-Spam: Content Scanning - Target	5-22
SMTP Anti-Spam: Content Scanning - Action	5-23
Configuring SMTP Anti-Phishing	5-25
SMTP Anti-Phishing - Target	5-25
SMTP Anti-Phishing - Action	5-26
SMTP Anti-Phishing - Notification	5-27
Configuring SMTP Content Filtering	5-28
SMTP Content Filtering - Target	5-29
SMTP Content Filtering - Action	5-31
SMTP Content Filtering - Notification	5-32

Chapter 6: HTTP Services

HTTP Services	6-2
Enabling Scanning of HTTP Traffic	6-2
Selecting an Alternative Service Port	6-3
Configuring HTTP Virus Scanning	6-4
HTTP Scanning - Target	6-5
Configuring Virus Scanning for HTTP Traffic	6-5
Setting MIME Type Exceptions	6-8
About Deferred Scan for Large File Handling	6-11
HTTP Scanning - Action	6-11
HTTP Scanning - Notification	6-13
Configuring HTTP Anti-Spyware	6-14
HTTP Anti-Spyware - Target	6-14
HTTP Anti-Spyware - Action	6-16
HTTP Anti-Spyware - Notification	6-17
Configuring HTTP Anti-Pharming	6-18
HTTP Anti-Pharming - Target	6-18
HTTP Anti-Pharming - Action	6-18
HTTP Anti-Pharming - Notification	6-19

Chapter 6: HTTP Services—continued

Configuring HTTP Anti-Phishing	6-20
HTTP Anti-Phishing - Target	6-20
HTTP Anti-Phishing - Action	6-21
HTTP Anti-Phishing - Notification	6-22
Configuring HTTP URL Filtering	6-23
HTTP URL Filtering - Rules	6-24
HTTP URL Filtering - Approved Clients List	6-26
HTTP URL Filtering - Settings	6-27
HTTP URL Filtering - Notification	6-29
Configuring HTTP File Blocking	6-30
HTTP File Blocking - Target	6-31
HTTP File Blocking - Notification	6-31

Chapter 7: FTP Services

FTP Services	7-2
Enabling Scanning of FTP Traffic	7-2
Selecting an Alternative Service Port	7-2
Configuring FTP Virus Scanning	7-4
FTP Scanning - Target	7-4
FTP Scanning - Action	7-6
FTP Scanning - Notification	7-7
Configuring FTP Anti-Spyware	7-8
FTP Anti-Spyware - Target	7-9
FTP Anti-Spyware - Action	7-10
FTP Anti-Spyware - Notification	7-11
Configuring FTP File Blocking	7-12
FTP File Blocking - Target	7-12
FTP File Blocking - Notification	7-13

Chapter 8: POP3 Services

POP3 Services	8-2
Enabling Scanning of POP3 Traffic	8-2
Selecting an Alternative Service Port	8-3
Configuring POP3 Virus Scanning	8-4
POP3 Scanning - Target	8-4
POP3 Scanning - Action	8-6
POP3 Scanning - Notification	8-8
Configuring POP3 Anti-Spyware	8-10
POP3 Anti-Spyware - Target	8-10
POP3 Anti-Spyware - Action	8-12
POP3 Anti-Spyware - Notification	8-13
Configuring POP3 IntelliTrap	8-14
POP3 IntelliTrap - Target	8-14
POP3 IntelliTrap - Action	8-15
POP3 IntelliTrap - Notification	8-16
Configuring POP3 Anti-Spam	8-17
POP3 Anti-Spam - Target	8-17
POP3 Anti-Spam - Action	8-19
Configuring POP3 Anti-Phishing	8-19
POP3 Anti-Phishing - Target	8-20
POP3 Anti-Phishing - Action	8-20
POP3 Anti-Phishing - Notification	8-21
Configuring POP3 Content Filtering	8-22
POP3 Content Filtering - Target	8-23
POP3 Content Filtering - Action	8-25
POP3 Content Filtering - Notification	8-26

Chapter 9: Outbreak Defense

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

Chapter 10: Quarantines

Quarantines Screen	10-2
Resending a Quarantined Email Message	10-3
Adding an Inline Notification to Re-Sent Messages	10-3
Querying the Quarantine Folder	10-4
Performing Query Maintenance	10-9
Manual	10-9
Automatic	10-10

Chapter 11: Updating InterScan Gateway Security Appliance Components

Update	11-2
Updating Manually	11-3
Configuring Scheduled Updates	11-4
Configuring an Update Source	11-6

Chapter 12: Analyzing Your Protection Using Logs

Logs	12-2
Querying Logs	12-3
Configuring Log Settings	12-5
Configuring Log Maintenance	12-6
Manual	12-6
Automatic	12-7

Chapter 13: Administration Functions

Administration	13-2
Access Control	13-3
Configuration Backup	13-3
Control Manager Settings	13-5
Registering InterScan Gateway Security Appliance to Control Manager	13-6
Disk SMART Test	13-8
Firmware Update	13-9
IP Address Settings	13-10
Managing IP Address Settings	13-11
Static Routes	13-12
Notification Settings	13-15
Settings	13-16
Events	13-17
Operation Mode	13-18
Password	13-19
Product License	13-20
Proxy Settings	13-24
SNMP Settings	13-26
System Time	13-27
Reboot from Web Console	13-30
World Virus Tracking	13-31

Chapter 14: Technical Support, Troubleshooting, FAQ

Contacting Technical Support	14-2
Readme.txt	14-3
Troubleshooting	14-4
Frequently Asked Questions (FAQ)	14-7
Recovering a Password	14-8
Virus Pattern File	14-9
Spam Engine and Pattern File	14-10
Hot Fixes, Patches, and Service Packs	14-10
Licenses	14-11
Renewing Maintenance	14-12
EICAR Test Virus	14-13
Best Practices	14-14
Handling Compressed Files	14-14
Block compressed files if... ..	14-14
Handling Large Files	14-16
Sending Trend Micro Suspected Internet Threats	14-18

Chapter 15: Updating the InterScan Gateway Security Appliance Firmware

Identifying the Procedures to Follow	15-2
Updating the Device Image Through the Web Console	15-3
Updating the Device Image Using the AFFU	15-4
Preparing InterScan Gateway Security Appliance for the Device Image Update	15-4
The Preconfiguration Console	15-4
Using the LCD Module	15-5
Before the Update	15-5
Backing Up Your Configuration	15-6
Putting the Appliance into Rescue Mode	15-13
Uploading the New Device Image	15-14
Uploading with Existing Configuration (Option 3)	15-15
Uploading with the Restored, Default Configuration (Option 5)	15-21
Completing the Process After the Device Image Is Uploaded	15-29
Reverting to the Previous Version of the Program File	15-30
BMC and BIOS Firmware Updates Using the Appliance Firmware Flash Utility	15-32
Updating the Appliance BMC Firmware	15-32
Preparing to Upload the BMC Firmware	15-32
Uploading the BMC Firmware	15-37
After the BMC Upload	15-40
Updating the InterScan Gateway Security Appliance BIOS Firmware	15-40
Preparing to Upload the Appliance BIOS	15-40
Uploading the Appliance BIOS Firmware	15-41
After the BIOS Firmware Upload	15-44
Troubleshooting BMC or BIOS Firmware Upload	15-45

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: Introducing Trend Micro Control Manager™

Control Manager Basic Features	B-2
Understanding Trend Micro Management Communication	
Protocol	B-3
Reduced Network Loading and Package Size	B-3
NAT and Firewall Traversal Support	B-4
HTTPS Support	B-5
One-Way and Two-Way Communication Support	B-6
One-Way Communication	B-6
Two-Way Communication	B-6
Single Sign-on (SSO) Support	B-6
Cluster Node Support	B-7
Control Manager Agent Heartbeat	B-7
Using the Schedule Bar	B-8
Determining the Right Heartbeat Setting	B-9
Registering InterScan Gateway Security Appliance M-Series to Control Manager	B-9

Appendix B: Introducing Trend Micro Control Manager™ —continued

Managing InterScan Gateway Security Appliances From Control Manager	B-11
Understanding Product Directory	B-11
Accessing a InterScan Gateway Security Appliance	
M-Series Default Folder	B-12
Access Product Directory	B-13
Manually Deploy New Components Using the Product Directory	B-14
View InterScan Gateway Security Appliance M-Series Status Summaries	B-14
Configure InterScan Gateway Security Appliances and Managed Products	B-16
Issue Tasks to InterScan Gateway Security Appliances and Managed Products	B-17
Query and View InterScan Gateway Security Appliance M-Series and Managed Product Logs	B-18
Recovering InterScan Gateway Security Appliances Removed From the Product Directory	B-19
Search for InterScan Gateway Security Appliances, Product Directory Folders or Computers	B-20
Refresh the Product Directory	B-21
Understanding Directory Manager	B-21
Using the Directory Manager Options	B-22
Access Directory Manager	B-23
Create Folders	B-23
Renaming Folders or InterScan Gateway Security Appliances	B-23
Move Folders or InterScan Gateway Security Appliances	B-24
Delete User-Defined Folders	B-24
Understanding Temp	B-25
Using Temp	B-25
Access Temp	B-25
Adding InterScan Gateway Security Appliances to Temp	B-26
Removing InterScan Gateway Security Appliances From Temp	B-29

Appendix B: Introducing Trend Micro Control Manager™ —continued

Download and Deploy New Components From	
Control Manager	B-30
Understanding Update Manager	B-31
Understanding Manual Downloads	B-31
Manually Download Components	B-31
Configure Scheduled Download Exceptions	B-39
Understanding Scheduled Downloads	B-39
Configure Scheduled Downloads and Enable	
Scheduled Component Downloads	B-40
Use Reports	B-47
Local Reports	B-47
Global Reports	B-47
Understanding Report Templates	B-48
Understanding Report Profiles	B-49
Create Report Profiles	B-49
Review Report Profile Settings	B-56
Enable Scheduled Report Profiles	B-56
Generate On-demand Scheduled Reports	B-56
View Generated Reports	B-57

Appendix C: Technology Reference

Deferred Scan	C-2
Diskless Mode	C-2
False Positives	C-3
LAN Bypass	C-3
Link State Failover	C-4
Enabling or Disabling LAN Bypass and Link State Failover	C-5
Scan Engine Technology	C-10
IntelliScan	C-10
IntelliTrap	C-10
MacroTrap	C-11
WormTrap	C-11
Supported DCS Clients	C-11

Appendix C: Technology Reference—continued

Feature Execution Order C-12

SMTP Feature Execution Order C-12

POP3 Feature Execution Order C-12

HTTP Feature Execution Order C-12

FTP Feature Execution Order C-12

Appendix D: Removing the Hard Disk

Appendix E: System Checklist

Appendix F: File Formats Supported

Compression Types F-2

Blockable File Formats F-4

Malware Naming Formats F-6

Appendix G: Specifications and Environment

Hardware Specifications G-2

Dimensions and Weight G-2

Power Requirements and Environment G-3

About This Manual

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 manual 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:

Chapters

Chapter 1, *Introducing Trend Micro InterScan Gateway Security Appliance*

Chapter 2, *Deployment Options*

Chapter 3, *How InterScan Gateway Security Appliance Works*

Chapter 4, *Getting Started with InterScan Gateway Security Appliance*

Chapter 5, *SMTP Services*

Chapter 6, *HTTP Services*

Chapter 7, *FTP Services*

Chapter 8, *POP3 Services*

Chapter 9, *Outbreak Defense*

Chapter 10, *Quarantines*

Chapter 11, *Updating InterScan Gateway Security Appliance Components*

Chapter 12, *Analyzing Your Protection Using Logs*

Chapter 13, *Administrative Functions*

Chapter 14, *Technical Support, Troubleshooting, and FAQs*

Chapter 15, *Updating the InterScan Gateway Security Appliance Firmware*

Appendixes

Appendix A, *Terminology*

Appendix B, *Introducing Trend Micro Control Manager™*

Appendix C, *Technology Reference*

Appendix D, *Removing the Hard Disk*

Appendix E, *System Checklist*

Appendix F, *File Formats Supported*

Appendix G, *Specifications and Environment*

Index

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
	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail 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 about actions or configurations to avoid
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 1-15
- *Testing the Appliance Connectivity* on page 1-16
- *Activating the Appliance* on page 1-16

What Is InterScan Gateway Security Appliance?

Trend Micro™ InterScan™ Gateway Security 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, pharming, 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 out-breaks early. Moreover, because the security features of the appliance are configured to work right out of the box, the appliance starts protecting your network 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 also saves 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, anti-pharming, 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 companywide Internet security policies Web browser support for Microsoft Internet Explorer 6.x and Mozilla Firefox 1.x
Automated maintenance	You can automate maintenance tasks, such as updating InterScan Gateway Security Appliance components and maintaining log files, 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 of known spam sources—the Real-Time Blackhole List (RBL+) and the QIL (Quick IP List).

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.

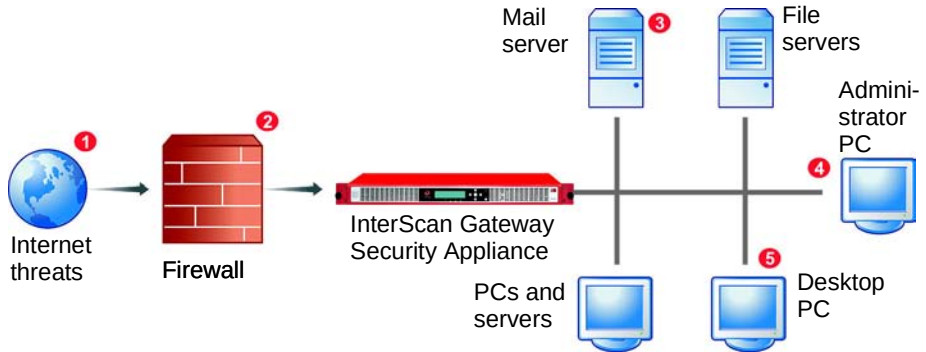


FIGURE 1-1. How InterScan Gateway Security Appliance Works

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. Uses patterns, heuristics, and other innovative technologies to block viruses, worms, and Trojans.
- 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 stops spyware from sending out user data that it has collected. Innovative technology also prevents users from browsing Web sites that install tracking software. If such a site has already installed spyware, 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.

Anti-Pharming

The anti-pharming security function in InterScan Gateway Security Appliance works within the HTTP protocol to block access to known pharming Web sites.

- When enabled, this feature places a warning message in the user's browser upon attempted access of a known pharming site.
- Optionally, you can send customized email notification to the administrator when such an event occurs.

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 the outbreak has reached them—but also repairs malware damage to clients' computers if the outbreak has already affected them.

- Provides defense against outbreaks. When an outbreak occurs anywhere in the world, TrendLabs 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 for InterScan Gateway Security Appliance administrators to take to reduce the threat to clients.
- Provides damage management. Damage Cleanup Services and Damage Cleanup Tools clean any client computers that malware has attacked.
- 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. Use these screws only 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.

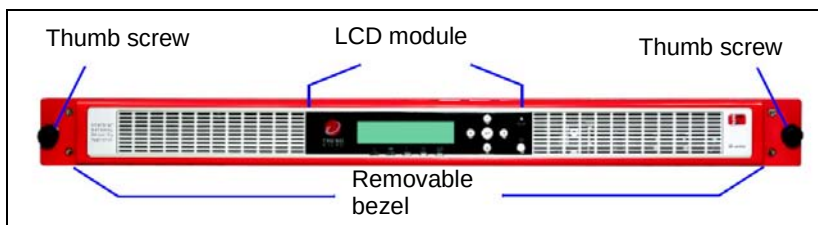


FIGURE 1-2. Front Panel

The following table describes each front panel element.

TABLE 1-2. Front panel elements

Front Panel Elements	Description
LCD Module	The LCD Module comprise 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 two rows of 16 characters each. Displays device status and preconfiguration instructions
Control panel	One five-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 together comprise the LCD Module.

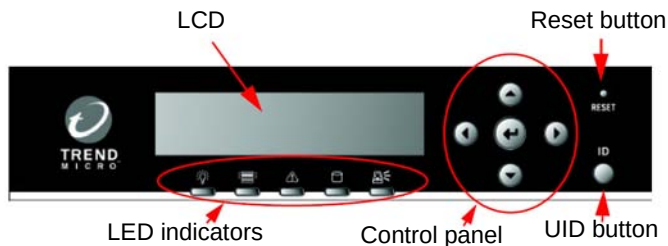


FIGURE 1-3. LCD Module

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 lights up when the 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.

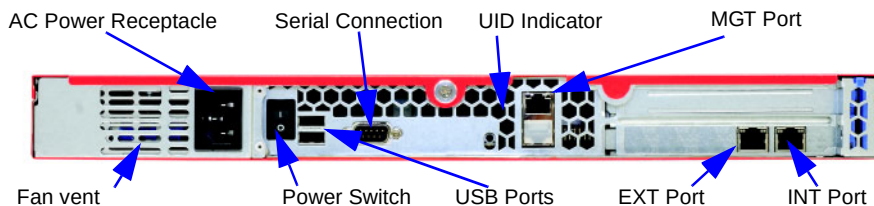


FIGURE 1-4. Back panel

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 located 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.

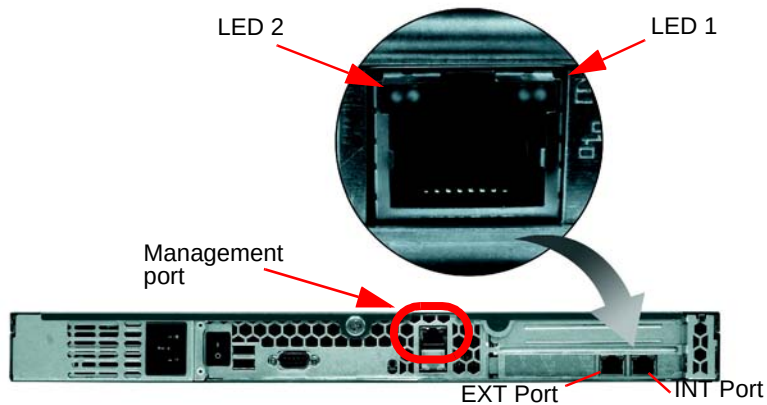


FIGURE 1-5. Port indicators

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	The appliance is not receiving data
		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 automatically resets the appliance to bypass mode, so that all data passes through.

Preconfiguring and Deploying the Appliance

Your InterScan Gateway Security Appliance must have an IP address to operate in your network.

WARNING! *Strictly speaking, this appliance is a [gateway](#) device. Therefore:*

1. Do not place InterScan Gateway Security Appliance in front of your network gateway *(your network firewall, for example).*

2. Do not reconfigure the network firewall to use the IP address of InterScan Gateway Security Appliance as its default gateway address.

Deployment in either of the above ways prevents the appliance from working.

Assign an IP address in any of three ways:

- A DHCP server automatically assigns a dynamic IP address to the appliance during deployment. This is the preferred method. Normally, there is one DHCP server per subnet; however, administrators can use a DHCP relay agent to support multiple subnets.
- Use a terminal communications program, such as HyperTerminal (for Windows) or Minicom (for Linux) to access the appliance Preconfiguration console and manually assign a dynamic or static IP address to the appliance during preconfiguration. If you choose to use a static IP address, you will need to set the netmask address, default gateway address, and primary DNS address.
- Using the LCD module, manually assign a dynamic or static IP address to the appliance after you have mounted it on your network. If you choose to use a static IP address, you will need to use the buttons on the LCD module to set the netmask address, default gateway address, and primary DNS address. You can also designate a host name in this way.

Note: You may also be required to provide a secondary DNS server address. See Chapter 2, *Deployment Options* for full deployment 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 of the appliance, power on the device.

Note: To prevent accidental shutdown of the appliance, the 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**, until the appliance powers off.

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. Visit 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

Deployment Options

This chapter addresses basic and advanced deployment options. For instructions on mounting the physical device, see the *Trend Micro InterScan Gateway Security Appliance M-Series Getting Started Guide*.

This chapter includes the following topics:

- [*Deployment Topologies*](#) on page 2-4
- [*Basic Deployment*](#) on page 2-8
- [*Advanced Deployment Scenarios*](#) on page 2-9
- [*Deployment Recommendations*](#) on page 2-17
- [*Deployment Issues*](#) on page 2-18
- [*Preconfiguring the Appliance*](#) on page 2-19

Overview

This chapter provides guidance on deploying the InterScan Gateway Security Appliance in the most common network topology as well as in more advanced topologies.

Note: InterScan Gateway Security Appliance is not a firewall or a router. Always deploy the appliance behind a firewall or security device that provides adequate NAT and firewall-type protection.

A typical network topology, with no gateway protection is shown in figure 2-1.

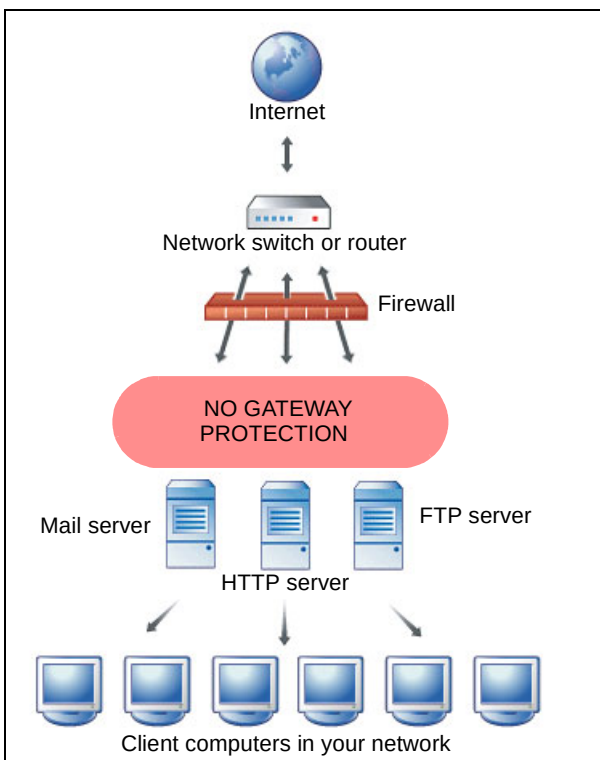


FIGURE 2-1. Typical network topology before deploying InterScan Gateway Security Appliance

In a basic deployment of the appliance in the most common network topology, the appliance sits between the network servers and the firewall, as shown in figure 2-2:

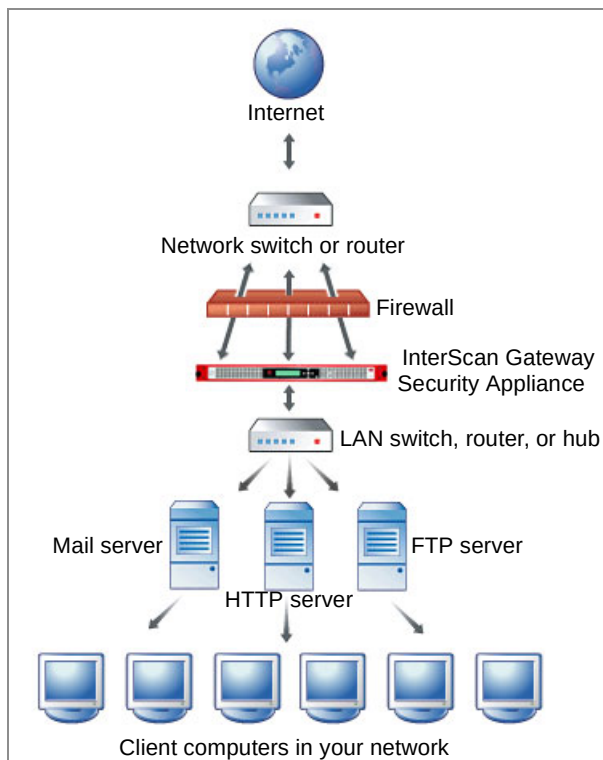


FIGURE 2-2. The most common deployment of InterScan Gateway Security Appliance

Deployment Topologies

This section discusses the following types of deployment topologies:

- Single network segment
- Multiple network segments

Deploying in a Single Network Segment

In [figure 2-3](#) on page 2-4, the network devices all belong in one network segment. All devices, including clients have Class A IP addresses. The core switch is the clients' default gateway. The router is the core switch and the default gateway of the appliance.

Note: If the appliance is not deployed between the router and the core switch, the connection will go through the core switch and then to its default gateway, which is the router. In return, the router redirects traffic to the intended server, thus bypassing the appliance altogether.

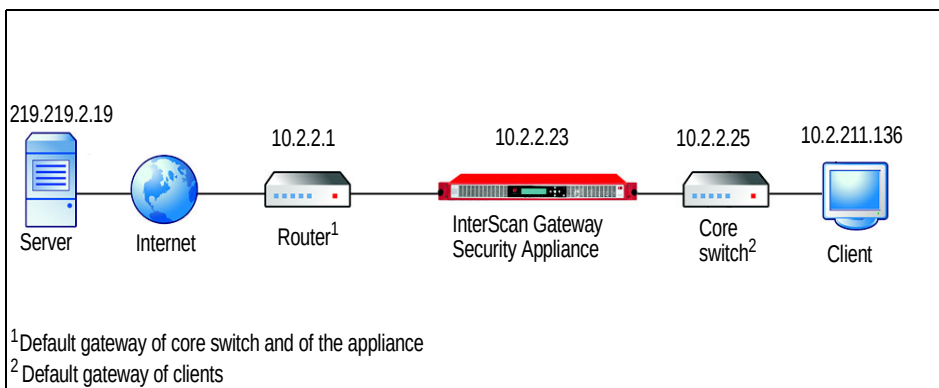


FIGURE 2-3. InterScan Gateway Security Appliance and clients deployed in the same network segment

If the appliance is deployed between a router and core switch within the same network segment, the appliance can directly connect to the router or clients. If a client issues a request to a server, the appliance receives the client's outgoing connection through TCP handshake. Because all devices are in the same segment, there are no problems relaying packets between network devices. The appliance passes the request to the router, which forwards it to the intended server.

Deploying in a Network with Multiple Segments

This section discusses deployment in a multiple-segment environment in which the default gateway of the appliance is a device handling the Internet connection (for example, a router or firewall).

In [figure 2-5](#) on page 2-7, the appliance and clients belong in different network segments. The core switch and the appliance belong in one segment using a Class A IP address. The core switch is the default gateway of the clients. The router is the core switch and is the default gateway of the appliance.

If the clients and the appliance are on different network segments, the router passes traffic to the Internet, but the appliance is unable to connect directly to the client. The packet passes to the default gateway of the appliance, which is the router.

In this topology, the appliance passes the packet to the router. The routing decision depends on the router. The SYN packet will be returned to the client through the router and the core switch. (See [figure 2-4](#) on page 2-6 for an illustration of this problem.)

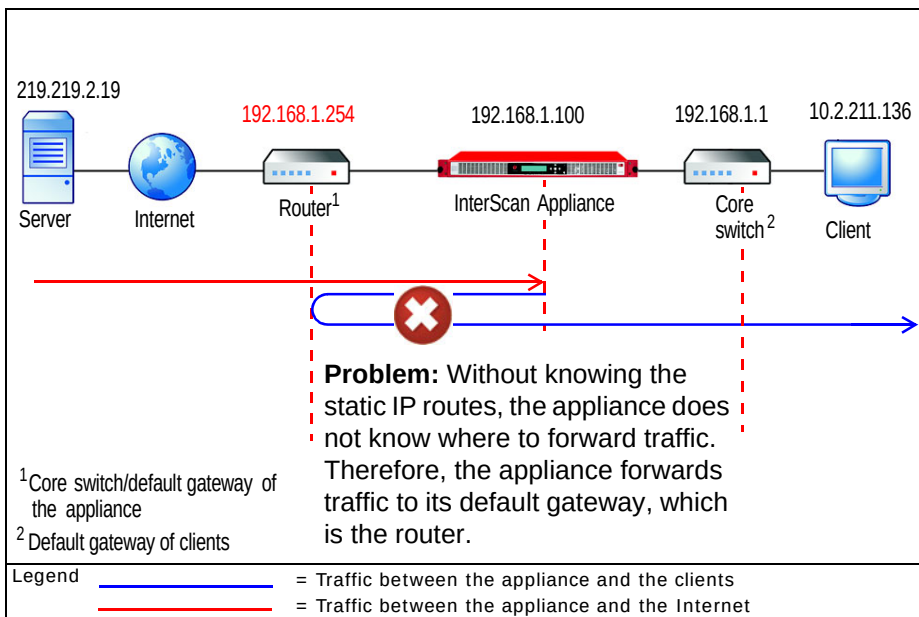


FIGURE 2-4. Problem: The appliance and clients deployed in different network segments, with router as default gateway of the appliance and no static routes set

A routing problem occurs whenever the router performs the following:

- Sending SYN/ACK packet back to clients
- Forwarding data to clients

These transactions lead to a decrease in the network throughput.

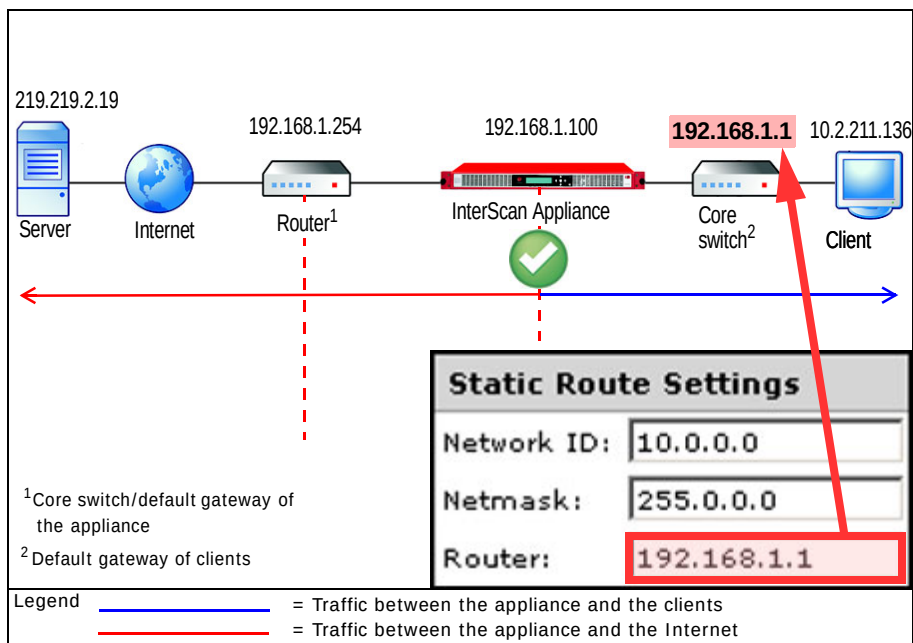


FIGURE 2-5. Solution: Static route settings tell the appliance where to forward traffic from clients deployed, even though they are in a different network segment

As a workaround, add static routing rules in the appliance. See [figure 2-5](#) on page 2-7 for an illustration of the solution to this problem and see [figure 2-6](#) on page 2-8 for instructions on how to add static routes.

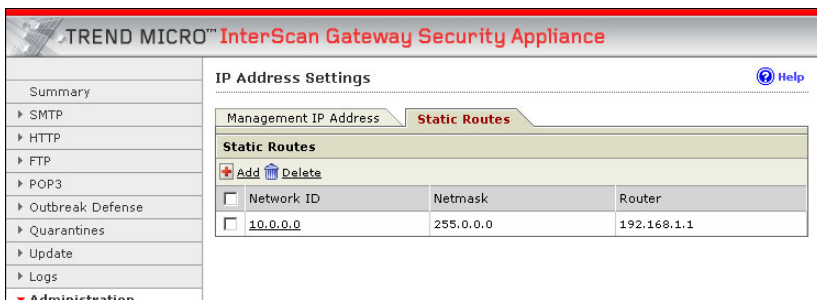


FIGURE 2-6. You can set static routes from the Web console
(Administration > IP Address Settings, Static Routes tab)

Refer to [Deployment Recommendations](#) on page 2-17 for tips to help minimize issues in a multi-segment environment.

Basic Deployment

As shown in figure 2-2, *The most common deployment of InterScan Gateway Security Appliance*, on page 2-3, it is necessary to include a LAN switch, router, or hub after the appliance in the basic deployment scenario. Including a router or switch after the appliance is necessary because the appliance itself is not designed to work as a router or switch.

Advanced Deployment Scenarios

In addition to the basic deployment scenario, administrators can deploy InterScan Gateway Security Appliance:

- In two transparent proxy modes:
 - Transparent proxy mode
 - Fully transparent proxy mode
- In a DMZ environment
- In conjunction with a load-balancing device
- In a single-segment environment
- In a multi segment environment

Note: InterScan Gateway Security Appliance cannot be deployed in a tagged VLAN topology, because the appliance does not support VLAN tags.

Operation Modes

InterScan Gateway Security Appliance implements transparent proxy with bridging.

Note: The appliance can be deployed as an inline (pass-through) device only. It cannot be used as a router or proxy server.

All Ethernet packets are transferred between INT (eth0) and EXT (eth1) ports. In transparent proxy with bridging, the appliance is transparent to other computers (that is, clients, servers, network devices). Other network devices cannot address the appliance directly. However, they can address it at the network layer if an IP address is assigned to the virtual bridge interface (br0).

Bridging is a technique for creating a virtual, wide-area Ethernet LAN, running on a single subnet. A network that uses Ethernet bridging combines an Ethernet interface with one or more virtual tap interfaces and brides them together under the umbrella of a single bridge interface. Ethernet bridges represent the software analog to a physical Ethernet switch. An Ethernet bridge is a kind of software switch that network administrators can use to connect multiple Ethernet interfaces (either physical or virtual) on a single computer while sharing a single IP subnet.

The appliance supports two transparent proxy modes (“operation modes”):

- Transparent proxy mode
- Fully transparent proxy mode

The major difference between transparent and fully transparent proxy modes is the “actual transparency” of the appliance with the destination server. The appliance creates an independent connection to the destination server. In transparent proxy mode, the destination server is aware of the IP address of the appliance.

In neither mode can the appliance keep the client’s MAC address when delivering the request to the server.

Transparent Proxy Mode

InterScan Gateway Security Appliance enforces transparency through the following behavior:

- Clients do not see the presence of additional filters/scanners unless a violation is detected.
- Administrators do not need any additional configuration on the client side.
- The destination servers still see the appliance IP address as the requestor.

For an illustration of how the appliance processes HTTP, FTP, SMTP, or POP3 traffic in transparent proxy mode, see the figure below.

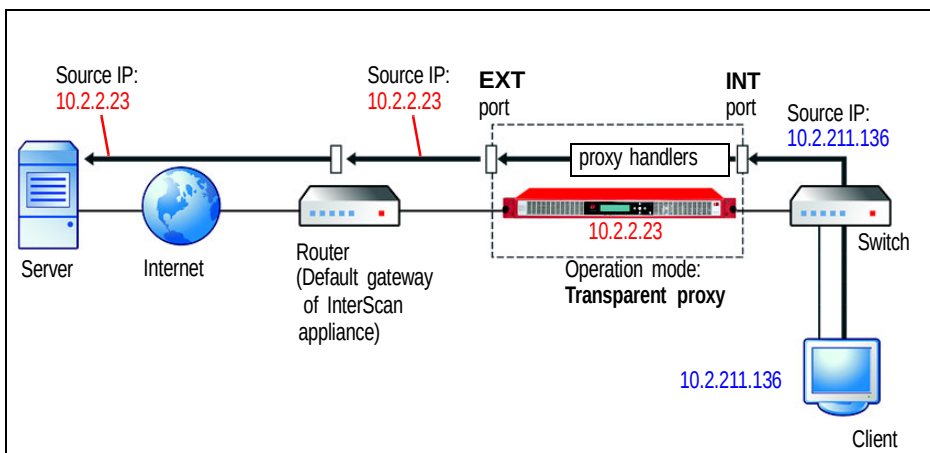


FIGURE 2-7. In transparent proxy mode, the client's IP address becomes that of the appliance

When a client initiates a request, the request passes through the switch that is the default gateway for clients in this segment. The appliance accepts the request through the INT port, which redirects traffic to the corresponding proxy handler. After the proxy handler processes the request, the appliance delivers the packet to the destination server through the router (the default gateway of the appliance).

WARNING! *The connection may be lost if the default gateway IP address of InterScan Gateway Security Appliance is deployed behind the appliance.*

In this mode, the source IP address is that of the InterScan Gateway Security Appliance and the destination IP address is that of the destination server. The appliance works in Layer 3 and has no knowledge of Layer 2 behavior.

Fully Transparent Proxy Mode

The appliance enforces full transparency through the following behaviors:

- Clients/destination servers do not see the presence of additional filters/scanners unless a violation is detected.
- Administrators do not need any additional configuration on the client side.

Figure 2-8 below illustrates how the appliance processes traffic in fully transparent proxy mode.

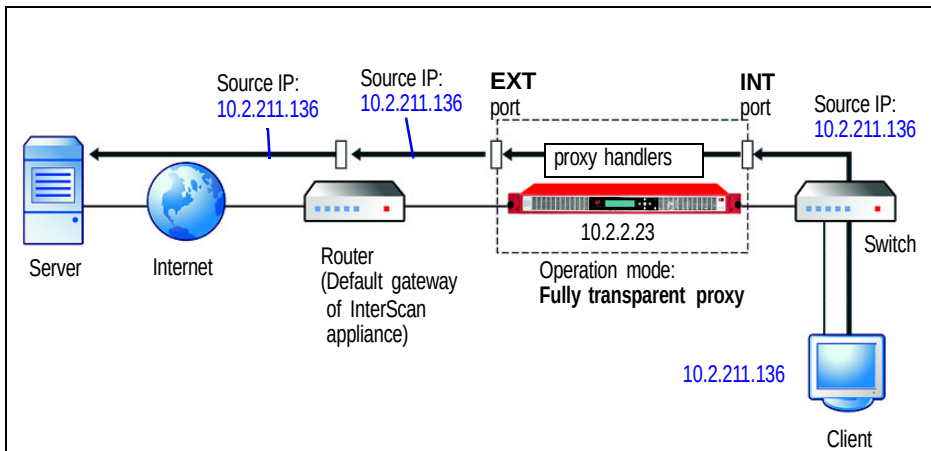


FIGURE 2-8. In fully transparent proxy mode, the IP address of the client is unchanged

When a client initiates a request, the request passes through the switch that is the default gateway for clients in this segment. The appliance accepts the request through the INT port, which redirects traffic to the corresponding proxy handler. After the proxy handler processes the request, the appliance delivers the packet to the destination server by way of the router (the default gateway of the appliance).

In this mode, the source IP address is the client's address and the destination IP address is that of the server. Bridge netfilter iptables is used to determine the route of the destination server.

Deployment in a DMZ Environment

To protect both a corporate network and a DMZ (*demilitarized zone* or perimeter network), you can deploy two appliances:

- One deployed to protect the corporate network
- One deployed to protect the DMZ

Because a DMZ is a network area (a subnetwork) that sits between an organization's internal network and an external network, two appliances are necessary to protect both areas.

See figure 2-9 for an illustration of a deployment with two appliances deployed as mentioned above. In the illustration, the company LAN is the area with a gray border and the DMZ is the area with a red border.

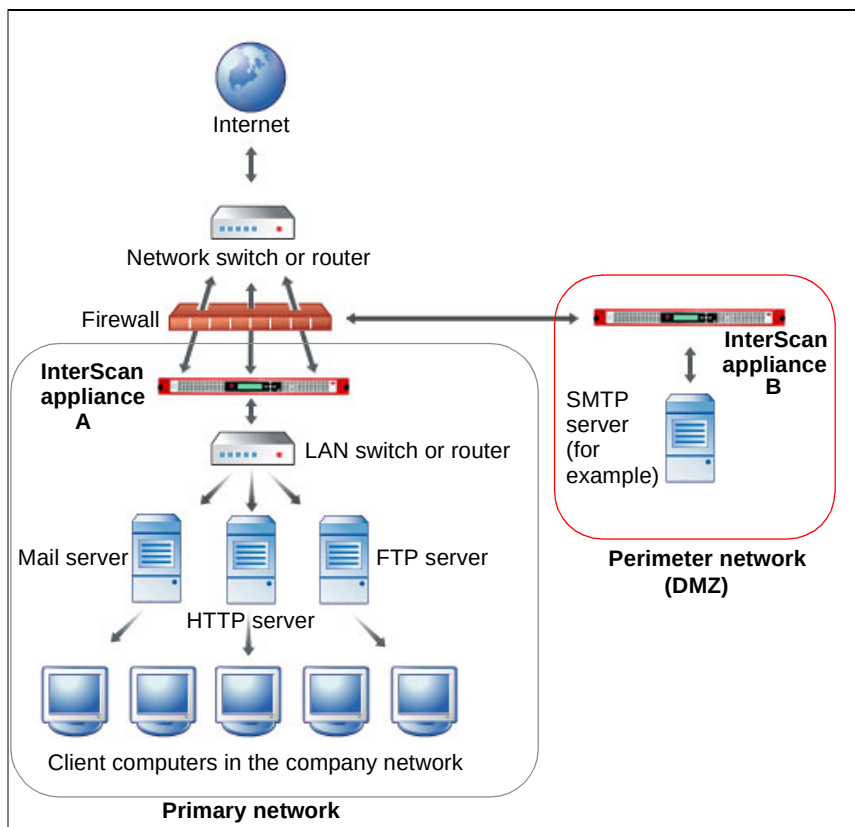


FIGURE 2-9. Deployment in a DMZ environment (requires two appliances)

Failover Deployment

If deploying two InterScan appliances, you can deploy them in such a way that if the connection to one appliance is broken, the second appliance takes over the load of the first appliance.

The basic steps for setting up a failover deployment are:

1. Deploy two appliances in your network (see *Failover Deployment Scenario* on page 2-15)
2. Ensure that **LAN bypass**, an option in the Preconfiguration console, is disabled (disabled by default)
3. Enable **Link state failover**, another option in the Preconfiguration console (disabled by default)

For instructions on how to set these options, see Appendix C. *Technology Reference, Enabling or Disabling LAN Bypass and Link State Failover* on page C-5.

Failover Deployment Scenario

To achieve such a function, deploy two InterScan appliances between two load-balancing devices, as shown in figure 2-10.

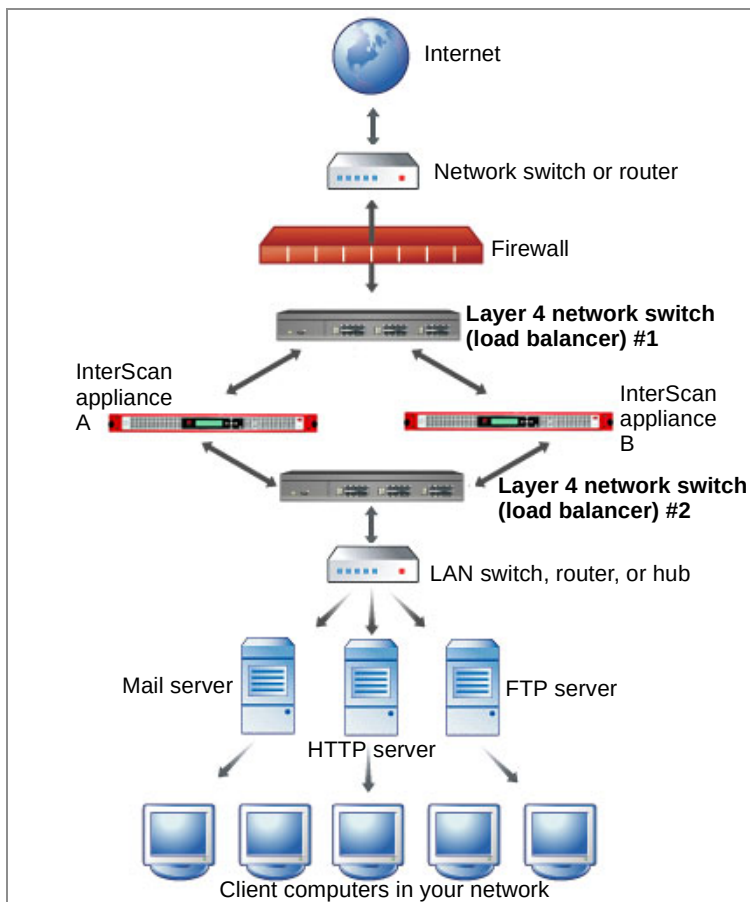


FIGURE 2-10. Two InterScan appliances arranged in a link state failover deployment

WARNING! *In order for this kind of “failover” to work, **LAN bypass** must be disabled and **Link state failover** must be enabled. They are both disabled by default.*

LAN Bypass and Link State Failover Settings

In the Preconfiguration console, **LAN bypass** must be disabled and **Link state failover** must be enabled in order for a load-balancing “failover” deployment to work.

LAN Bypass

LAN bypass is a feature by which, if the appliance encounters an error that causes scanning to stop, network traffic will still flow through the appliance unscanned, so that network traffic is not interrupted (disabled by default).

Link State Failover

Link state failover is a feature by which, if either the **INT** or the **EXT** port stops functioning, both ports are automatically shut down (disabled by default).

Setting LAN Bypass and Link State Failover Options

If you have previously enabled LAN bypass, you can disable it through the InterScan Gateway Security Appliance Preconfiguration console. Likewise, you can enable link state failover on the same screen of the Preconfiguration console. See Appendix C.

[Technology Reference, Enabling or Disabling LAN Bypass and Link State Failover](#) on page C-5 for details.

Deployment Recommendations

Figure 2-11 below shows the recommended deployment setup for the appliance.

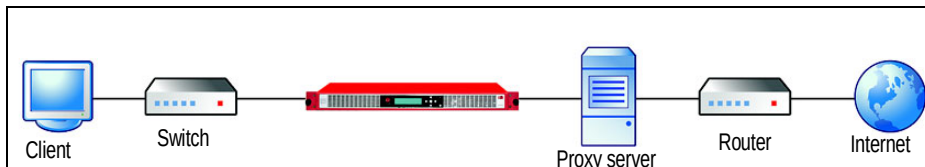


FIGURE 2-11. Recommended position of InterScan Gateway Security Appliance and other network devices in single- or multi-segment environments

To minimize issues and speedily complete deployment, deploy the appliance:

- Between a firewall that leads to the public network and a router, switch, or hub that leads to the protected segment of the local area network.

Connect a router, switch, or hub to the **INT** port, thereby creating a protected network. Connect the **EXT** port to a device that leads to the public network or Internet.

- Before a proxy server leading to the public network.

If deploying in a multi-segment environment, take note of the following recommendations:

- Connect the default gateway to the **EXT** port.
- Use the same default gateway setting for both the appliance and the router that connects the appliance to the segments.
- Using the Web console, add the static routes for each segment to the appliance.
- Disable the proxy settings from the HTTP URL Filtering screen if traffic is not passing through the appliance.

Refer to *Deployment Issues* on page 2-18 to learn about the known deployment issues in this release. For details about single and multi-segment deployment topologies, see *Deploying in a Single Network Segment* on page 2-4 and *Deploying in a Network with Multiple Segments* on page 2-5.

Deployment Issues

This release has the following limitations:

- VLAN is not supported in either transparent or fully transparent proxy mode.
Some network devices use VLAN to separate network layers. This use causes modified VLAN tags. The appliance cannot recognize VLAN tags. If deployed in a VLAN environment, the appliance is unable to scan any of the four protocols, and the Web console is inaccessible.

WARNING! *If the appliance is deployed in a VLAN environment, the LCM LEDs are unable to provide any indication that scanning is not working.*

- MAC address transparency is not supported in any operation mode.
- Original bridge forwarding processing may be disturbed in both operation modes. See [Deployment Issues](#) on page 2-18.
- If the link is broken on the external (Internet-facing) side of the appliance, the appliance cannot alert network devices on the external side. Likewise, if the broken link is on the internal side, the appliance cannot alert devices on that side.
- Packet looping may occur if a proxy server packets pass goes through a proxy server before the appliance.

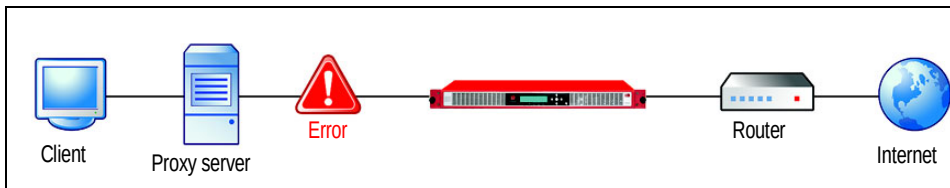


FIGURE 2-12. If the proxy server is deployed on the protected-network side of the appliance, packet looping may occur

Preconfiguring the Appliance

Your InterScan Gateway Security Appliance must have an IP address to operate in your network.

WARNING! *This appliance is a [pass-through](#) device. Therefore:*

1. Do not place InterScan Gateway Security Appliance in front of the network gateway *(the network firewall, for example).*

2. Do not reconfigure the network firewall to use the IP address of InterScan Gateway Security Appliance as its default gateway address.

Deployment in either of the above ways prevents the appliance from working.

Assigning an IP Address

Assign an IP address in any of three ways:

- **[Recommended]** A DHCP server automatically assigns a dynamic IP address to the appliance during deployment. This is the preferred method. Normally, there is one DHCP server per subnet; however, you can use a DHCP relay agent to support multiple subnets.
- Use a terminal communications program, such as HyperTerminal (for Windows) or Minicom (for Linux) to access the appliance Preconfiguration console and manually assign a dynamic or static IP address to the appliance during preconfiguration. If you choose to use a static IP address, you will need to set the netmask address, default gateway address, and primary DNS address.
- Using the LCD module, manually assign a dynamic or static IP address to the appliance after you have mounted it on your network. If you choose to use a static IP address, you will need to use the buttons on the LCD module to set the netmask address, default gateway address, and primary DNS address. You can also designate a host name in this way.

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 of the appliance, power on the device.

Note: To prevent accidental shutdown of the appliance, the 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**, until the appliance powers off.

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. Visit 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

The chapter provides an overview of how the appliance protects your network from a range of Internet-borne security risks.

The topics discussed in this chapter include:

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

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.” There are thousands of known viruses, 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 3-1. Types of Internet threats

Threat Type	Characteristics
Bot	Bots are compressed executable files that are often designed to harm 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 these 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

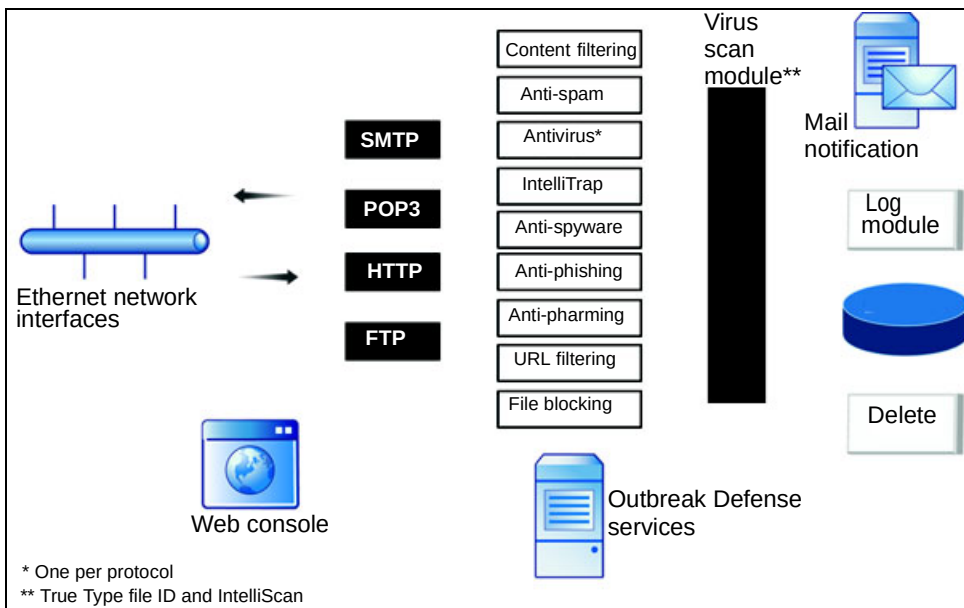


FIGURE 3-1. InterScan Gateway Security Appliance Primary Functional Components

Following is an explanation of each of the primary functional components of the appliance along with the underlying processes that each component executes.

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 [Accessing the Web Console](#) on page 4-3 and [Navigating the Web Console](#) on page 4-12 for more details.

Content Filtering

Objectionable content in email is a problem for both inbound and outbound mail. Therefore, 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

message 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 writes 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.

The 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.

An administrator cannot modify the method that the Anti-spam engine uses to assign spam scores but can adjust the detection levels that the Anti-spam engine uses to decide which messages to treat as 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.

Approved and Blocked Senders Lists

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 screen to manage these 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.

Use the Web console to set up lists of Approved or Blocked Senders to control how the 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.

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 3-2. 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
trend.com	john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com	john@trend.com.tw mary@mytrend.com
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com	john@trend.com john@trend.com.tw
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 a Quick IP List (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 3-3. 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 that NRS considers spam open-relay hosts. InterScan Gateway Security Appliance categorizes the IP addresses listed in the RBL as permanent sources of spam.
Quick IP List (QIL)	QIL is a database that contains the IP addresses of SMTP servers that either originate spam or that NRS considers 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.

Logging in to the Network Reputation Services Site

You can fine-tune NRS settings by logging in to the NRS site and making your changes there.

To fine-tune Network Reputation Services:

1. Visit the following URL:
<https://nrs.nssg.trendmicro.com>
2. Log in to Network Reputation Services with your InterScan Gateway Security Appliance Activation Code.
3. Follow the instructions in the NRS user interface to modify settings.

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.

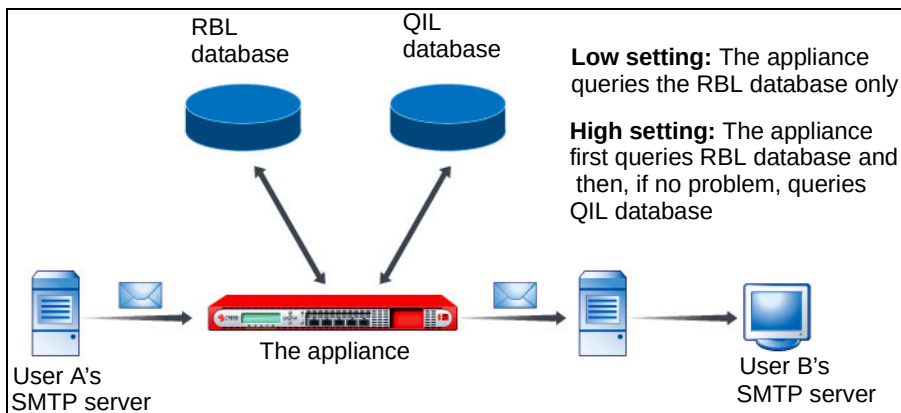


FIGURE 3-2. How the RBL and QIL databases work

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, Trend Micro designed the Anti-phishing function in InterScan Gateway Security Appliance to protect LAN users from inadvertently giving away sensitive information as part of a phishing attack. Anti-phishing monitors:

- Outbound client URL requests
- 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 fraud known as pharming has become an increasingly treacherous way to commit identity theft on the Internet. Therefore, Trend Micro has designed the Anti-pharming feature 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 compares 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 the company considers offensive or in violation of company ethics. Trend Micro has designed the URL filtering function to prevent users from accessing such sites. 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 that malware can arrive on your desktop or network is through files that an HTTP server has sent by streaming or downloading them when a client computer accesses a Web site or an FTP site (FTP over HTTP). It is important to protect your network from this security risk. InterScan Gateway Security Appliance can scan for and block certain file types that originate from HTTP and FTP servers, thereby protecting your network and computers. The appliance can block both predefined and administrator-specified file types.

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 the appliance can block 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.

True File Type and IntelliScan

Virus originators can easily rename a file to disguise its actual type. Programs such as Microsoft Word are “extension independent”; that is, they recognize and open “their” documents regardless of the file name. This security hole poses a danger, for example, if a Word document containing a macro virus has a name such as `benefits_form.pdf`. Word opens the file, but InterScan Gateway Security Appliance may not have scanned it if the appliance is not checking 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 scan for 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 the date of publication of this guide, 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 for the appliance to take to reduce the likelihood that the network that it is protecting will become infected. For example, if the threat's main method of delivery is by email or FTP, the appliance blocks all incoming mail or blocks 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 can send email notifications about any action that it takes on SMTP, POP3, HTTP, and FTP traffic. The appliance can insert inline notification stamps into all scanned message before sending them, and senders, recipients, and administrators can receive standard or customized messages when the appliance performs a particular action. The appliance can also notify TrendLabs of potential threats—for example, a phishing URL—thereby enabling 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.

Logs

Administrators need a way to monitor scanning and detection activity of the appliance over time. Monitoring these activities provides a historical view and enables you to analyze those settings that you may need to modify to optimize security. 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.

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. The appliance can also quarantine email that has triggered the content filtering rules.

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.

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 4-2
- *Accessing the Web Console* on page 4-3
- *The Summary Screen* on page 4-4
- *Navigating the Web Console* on page 4-12
- *The Online Help System* on page 4-14

Preliminary Tasks

The InterScan Gateway Security Appliance is designed to provide good default protection from the moment you install it 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 appliance Web console and the chapters in which you can find descriptions of those functions and settings:

TABLE 4-1. Preliminary tasks

Preliminary Task	See Chapter
Change the default admin password to ensure appliance security	Ch. 13
Schedule default email notifications	Ch. 13
Set up SMTP notifications	Ch. 5
Update the virus pattern, URL Filtering, and scan engine file	Ch. 11
Schedule automatic pattern and engine updates	Ch. 11
Configure HTTP scanning policies	Ch. 6
Set up Access Control (for remote access)	Ch. 13
Create URL Filtering policies and test	Ch. 6
Configure Anti-phishing settings and any specific URL sites to block	Ch. 5, Ch. 6, Ch. 8
URL Blocking (local list)	Ch. 6
URL Blocking (anti-phishing)	Ch. 6
Create FTP scanning policies for inbound and outbound traffic	Ch. 7
Obtain EICAR test file to confirm your installation is working properly	Ch. 14

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.

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.

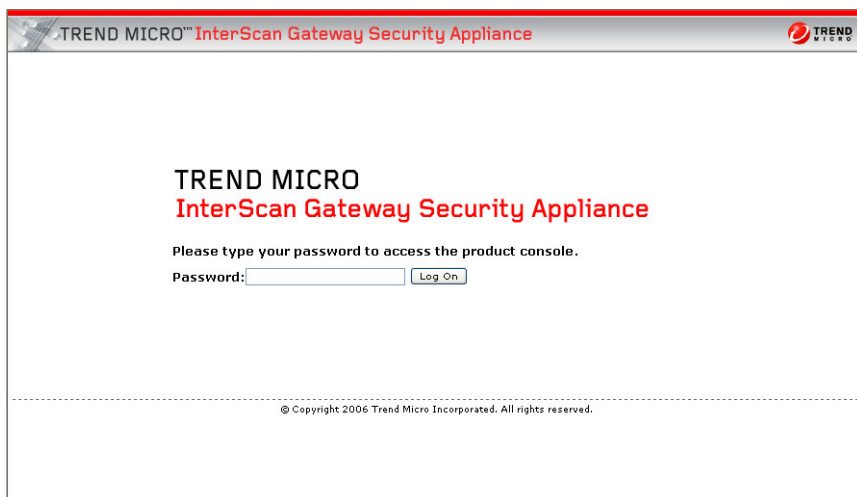


FIGURE 4-1. Web Console Log On Screen

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, the appliance automatically logs you 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 13-27 for more information.)

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

Outbreak Prevention Service

The screenshot shows the 'Summary' page of the Trend Micro InterScan Gateway Security Appliance. The left sidebar contains a navigation menu with items: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'Summary' and includes a status message: 'The InterScan Gateway Security Appliance is valid.' with a green checkmark icon. Below this, it shows 'Last updated: 10/25/2006 12:32:03' and a 'Refresh' button. The 'Outbreak Prevention Service' section shows 'Status: Disabled', 'Risk: N/A', 'Threat: N/A', and 'Description: N/A'. The 'Damage Cleanup Service' section shows '0 infected components.' and a table with columns 'Today', 'Last 7 days', and 'Last 30 days' for 'Infected computers' and 'Cleaned computers'. The 'Component Version' section includes a 'Manual Update' button and a table listing various components, their current versions, and last updated times.

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		
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 4-2. 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.

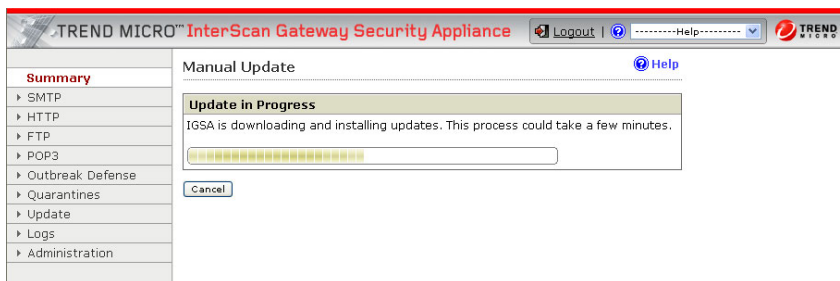


FIGURE 4-3. Update in Progress

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

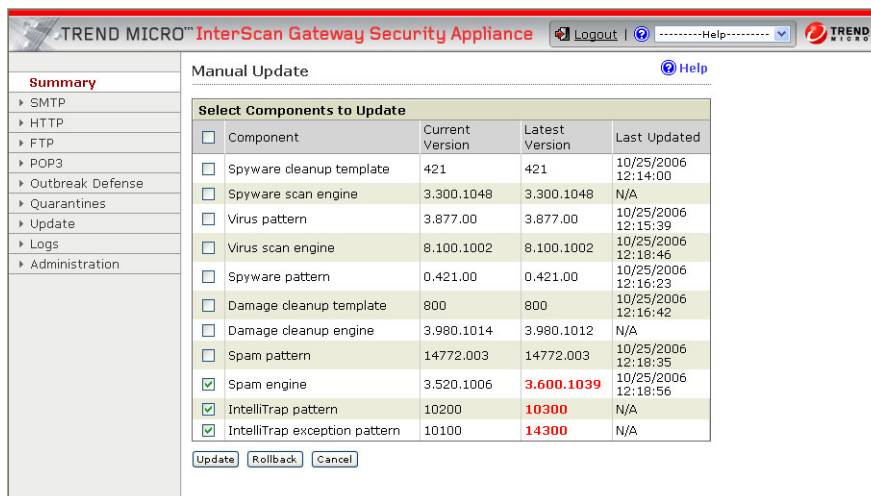


FIGURE 4-4. Manual Update > Select Components to Update

2. Click **Update** to update the appliance. The **Update in Progress** indicator reappears while the appliance updates.
3. [Optional] Click **Rollback** to roll back the 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 4-5. 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 4-6. 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.

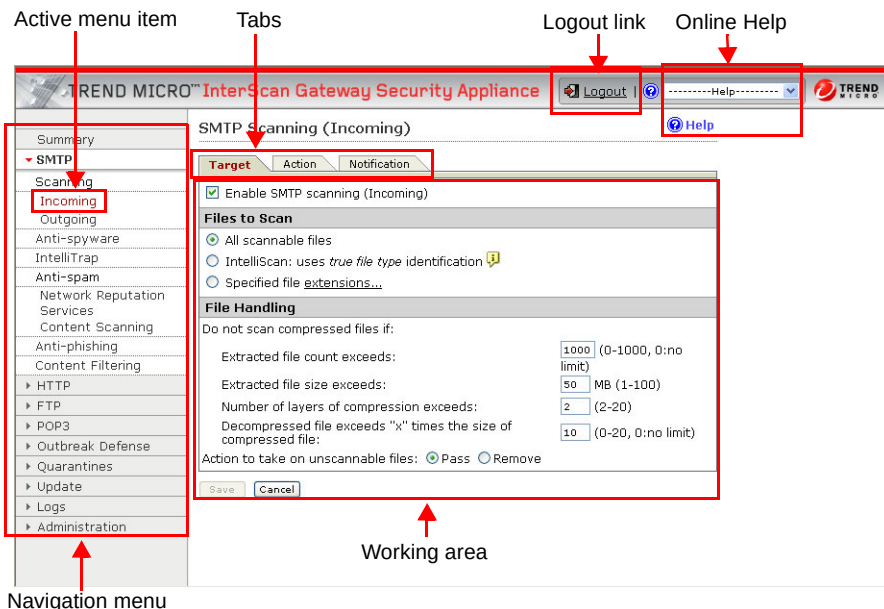


FIGURE 4-7. SMTP > Scanning (Incoming) > Target – Sample Screen

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  **Help** 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

The InterScan Gateway Security Appliance online help system consists three major kinds of help, listed here from the specific to the general:

- Field-specific “embedded help”
- Screen-level, context-sensitive help
- Broader, console-based help, organized in a table of contents

Embedded Help

Embedded help appears in several forms. One form is the “Tooltip,” a yellow icon that displays relevant explanatory material when you mouse-over it, as shown in figure 4-8, below.

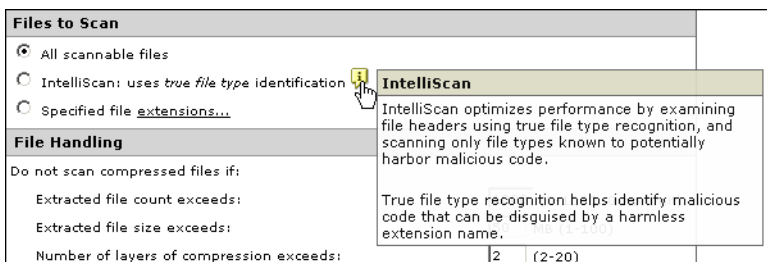


FIGURE 4-8. Sample Tooltip mouseover embedded help

Other embedded help appears under, above, or inside text entry fields, in pop-up windows linked from the user interface, and in explanatory text at the beginning of many sections of the user interface.

Screen-Level Context-Sensitive Help

Context-sensitive help for most screens is available by clicking the blue Help icon at the top right of the screen ( Help).

Console-Based Help

Console-based help includes both screen-level help entries and other, more conceptual information organized in a left-side table of contents. Access this Help system from the Help drop-down menu on the right side of the Web console the title bar, as illustrated in figure 4-9, below.



FIGURE 4-9. Online Help Menu – Contents and Index

To use the online Help system:

1. Select Contents and Index from the Help drop-down menu (figure 4-9). The InterScan Gateway Security Appliance Online Help system displays.

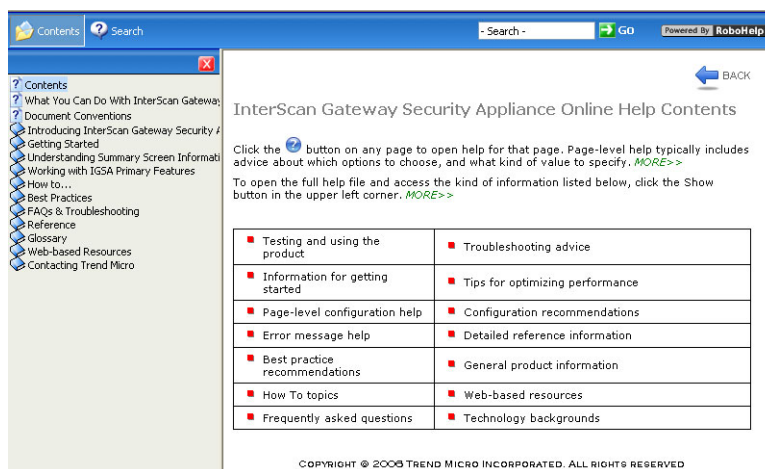


FIGURE 4-10. Online Help System

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

[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 4-11. 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:**FIGURE 4-12. Online Help – MORE> Screen**

4. Back in the Web console, click  **Help** 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 scanning services in InterScan Gateway Security Appliance.

Topics discussed in this chapter include:

- *Enabling Scanning of SMTP Traffic* on page 5-3
- *Configuring SMTP Virus Scanning* on page 5-4
- *Configuring SMTP Anti-Spyware* on page 5-11
- *Configuring SMTP IntelliTrap* on page 5-15
- *Configuring SMTP Anti-Spam: Network Reputation Services* on page 5-18
- *Configuring SMTP Anti-Spam: Content Scanning* on page 5-21
- *Configuring SMTP Anti-Phishing* on page 5-25
- *Configuring SMTP Content Filtering* on page 5-28

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
- The action that InterScan Gateway Security Appliance takes upon detecting the security risk, namely clean, delete, remove, or quarantine.

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

The appliance can only scan SMTP traffic if that feature has been enabled. The feature is not enabled by default. You can enable SMTP scanning on the main SMTP screen.

FIGURE 5-1. SMTP - Enable

To enable scanning of SMTP traffic:

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

Selecting an Alternative Service Port

The default listening port for SMTP services is 25. Administrators whose network security policy requires the use of nonstandard ports for servers may want to change this default.

To select an alternative service port for SMTP services:

1. On the left menu, click **SMTP**. The SMTP screen appears.
2. In the Service Port section, type the desired port in the **SMTP listening service port(s)** field.
3. Click **Save**. A message displays instructing you that the appliance must reboot in order for this change to take effect.

4. Click **OK** to dismiss the message. A countdown screen appears and counts down from 3 minutes while the appliance is rebooting. When the appliance has rebooted, the Web console login screen appears.
5. Log on to the Web console to make any further changes.

Tip: If you are changing the SMTP service port as a security measure against hackers, Trend Micro recommends that you use the less common ports (those above 6,000).

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: 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

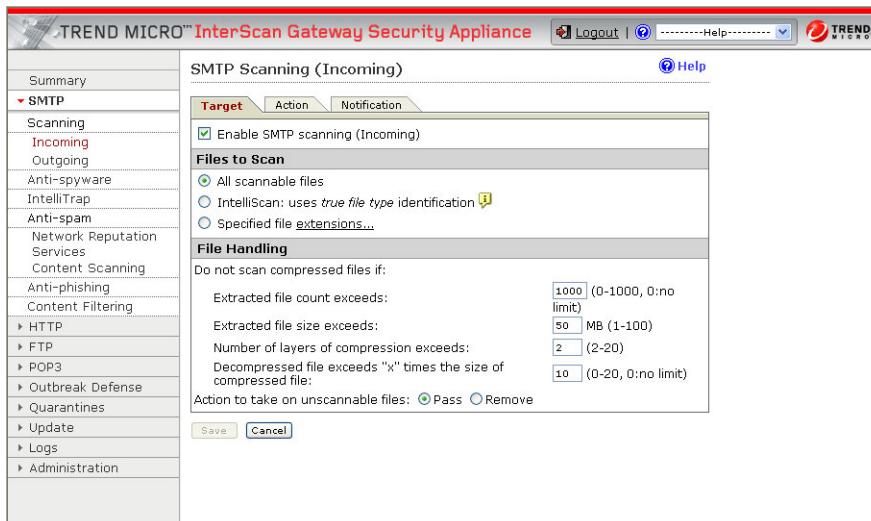


FIGURE 5-2. SMTP > Scanning (Incoming) - Target

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 clicking **Specified file extensions...** and then 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 5-3. 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

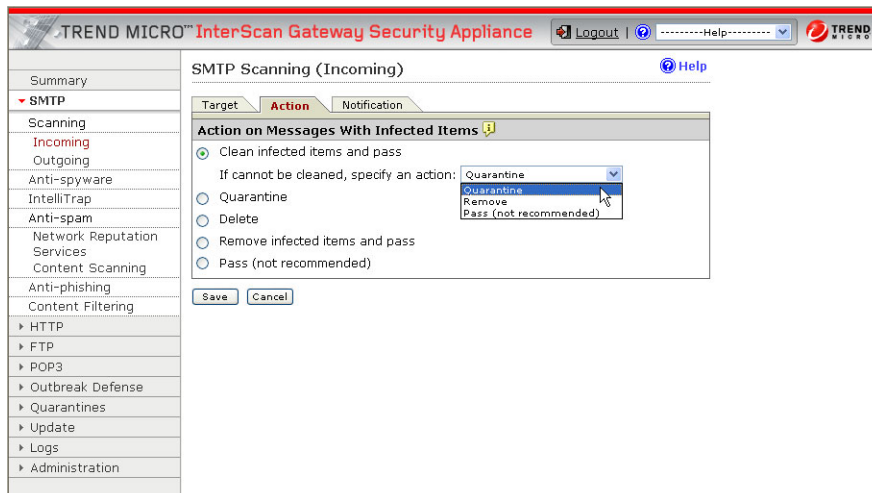


FIGURE 5-4. SMTP > Scanning (Incoming) - Action

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.

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

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 the way in which InterScan Gateway Security Appliance responds to them.

TABLE 5-1. “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.** Alternatively, you can 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

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** [View variable list](#)

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:

Security risk Detected Notifications:

☒ Subject line: Risk Detected:

☒ Message This message contains a possible security risk.

Security risk Free Notifications:

☒ Message Trend Micro InterScan Security Gateway Appliance has scanned this message and found it to be free of known security risks.

Unscannable File Notifications:

☒ Message This message has been scanned and found unscannable files contained.

Save Cancel

FIGURE 5-5. 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.

Unscannable File Notifications

Message - if the appliance is unable to scan one or more files attached to the message, the recipient sees this message appended to the body of the email message.

5. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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

The screenshot displays the 'SMTP Anti-spyware' configuration page in the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar shows a navigation tree with 'SMTP' expanded, and 'Anti-spyware' selected. The main content area has three tabs: 'Target', 'Action', and 'Notification'. The 'Target' tab is active, showing the following configuration:

- Enable SMTP Anti-spyware:** ☒
- Spyware/Grayware Exclusion List:** Includes a search bar and a list box currently showing 'None'. Below the list box, an example shows 'ADW_SLAGENT.A' and 'ADW_BLAZE.B'.
- Scan for Spyware/Grayware:** ☒ Select all
 - ☒ Spyware
 - ☒ Adware
 - ☒ Dialers
 - ☒ Joke Programs
 - ☒ Hacking Tools
 - ☒ Remote Access Tools
 - ☒ Password Cracking Applications
 - ☒ Others

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

FIGURE 5-6. 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.

The screenshot displays the Trend Micro Spyware/Grayware Online Database. At the top, there is a search bar and a dropdown menu for Global Sites. The main navigation bar includes links for Home, Products & Services, Purchase, Support, Security Info, Partners, and About Us. The left sidebar contains a menu with various security resources. The main content area is titled 'Spyware/Grayware' and features a search bar and a dropdown for 'Spyware/Grayware Type'. Below this, a table lists the 'Top 10' spyware/grayware items with their respective report counts. At the bottom, there is a section for 'Spyware/Grayware Advisories' containing a table with columns for Spyware/Grayware, Risk Rating, Advisory Date, and Pattern File.

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 5-7. 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 5-8. 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

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 (selected), Scanning, Incoming, Outgoing, Anti-spyware (selected), IntelliTrap, Anti-spam, Network Reputation Services, Content Scanning, Anti-phishing, Content Filtering, HTTP, FTP, POP3, Outbreak Defense, Quarantines, and Update. The main content area is titled "SMTP Anti-spyware" and has a "Help" icon. Below the title are three tabs: "Target", "Action", and "Notification" (selected). A "View variable list" link is visible. The "Email Notifications" section explains that when a message containing spyware/grayware is detected, email notifications will be sent to selected recipients. Three notification templates are listed, each with a checkbox and a text area for the message content:

Recipient	Notification Message
☒ Administrator	A threat was detected in a message. >Threat type: spyware/grayware >Threat name: %VIRUSNAME% >Sender: %SENDER% >Recipient: %RECIPIENT%
☐ Sender	Warning - a spyware/grayware application was detected in a message sent to %RECIPIENT% from your computer. The message subject is %SUBJECT%. The message may not have been delivered. We suggest scanning your computer for security risks.
☒ Recipient	Warning - a spyware/grayware application was detected in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be deliverable.

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

FIGURE 5-9. 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 notifications(s) will be sent:
 - Administrator
 - Sender
 - Recipient
4. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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

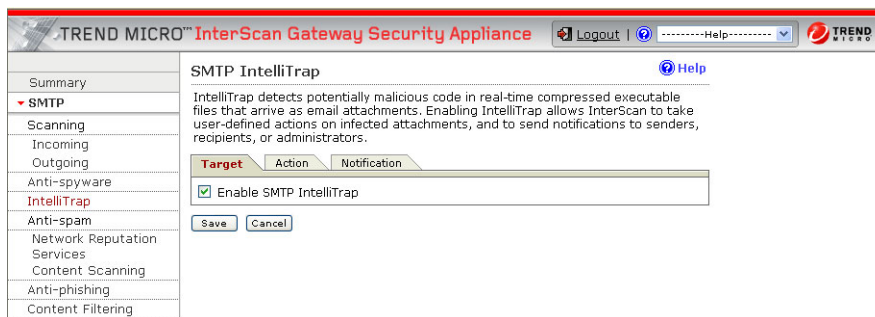


FIGURE 5-10. SMTP > IntelliTrap - Target

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 5-11. 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

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. On the left is a navigation menu with categories like 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, and Administration. The main content area is titled 'SMTP IntelliTrap' and includes a description: 'IntelliTrap detects potentially malicious code in real-time compressed executable files that arrive as email attachments. Enabling IntelliTrap allows InterScan to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.' Below this is a tabbed interface with 'Target', 'Action', and 'Notification' tabs. The 'Notification' tab is active, showing 'Email Notifications' with a 'View variable list' link. It contains three sections for selecting recipients: 'Administrator' (checked), 'Sender' (unchecked), and 'Recipient' (checked). Each section has a text area showing a default notification message with variables like %THREATTYPE%, %THREATNAME%, %INFECTEDFILENAME%, %SENDER%, and %VIRUSNAME%. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 5-12. 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. When IntelliTrap detects a potential threat (such as a bot), the appliance sends the corresponding email notifications(s) to the recipient(s) that you select:
 - Administrator
 - Sender
 - Recipient
4. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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 web interface of the Trend Micro InterScan Gateway Security Appliance. 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 (highlighted), 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, there is a descriptive paragraph about the service. The "Target" tab is active, showing a checkbox for "Enable SMTP Anti-spam (Network Reputation Services)" which is checked. Below this is the "Set Service Level" section with two radio button options: "Low setting" and "High setting". The "High setting" is selected. Below the service level settings is the "Approved IP Address(es)" section, which includes a text input field for "Approved IP:", an "Add >>" button, and a list box for "IP Address(es)" currently showing "None". An example IP address "172.26.240.2" is provided below the input field. At the bottom of the configuration area are "Save" and "Cancel" buttons.

FIGURE 5-13. 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**. The new IP address appears in the IP Address(es) table on the right.
5. Click **Save**.

Logging in to the Network Reputation Services Site

You can fine-tune NRS settings by logging in to the NRS site and making your changes there.

To fine-tune Network Reputation Services:

1. Visit the following URL:
<https://nrs.nssg.trendmicro.com>
2. Log in to Network Reputation Services with your InterScan Gateway Security Appliance Activation Code.
3. Follow the instructions in the NRS user interface to modify settings.

SMTP Anti-Spam: Network Reputation Services - Action



FIGURE 5-14. 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 Quick IP List (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

The screenshot displays the 'SMTP Anti-spam' configuration page in the Trend Micro InterScan Gateway Security Appliance web interface. The left-hand navigation menu is expanded, showing 'SMTP' as the selected category, with 'Content Scanning' highlighted. The main content area is titled 'SMTP Anti-spam' and features a 'Target' tab. Under this tab, there are several configuration sections: 'Enable SMTP Anti-spam' (checked), 'Filter Tuning' (with 'Spam detection level' set to 'Low'), 'Keyword Exceptions' (with a text area for exceptions), 'Approved Senders' (with a text area for approved email addresses), and 'Blocked Senders' (with a text area for blocked email addresses). The interface also includes a 'Summary' link and a 'Help' icon at the top right of the main area. At the bottom of the configuration section are 'Save' and 'Cancel' buttons.

FIGURE 5-15. 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

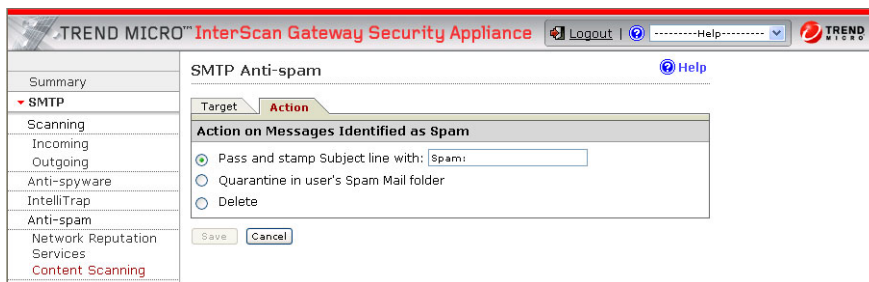


FIGURE 5-16. SMTP > Anti-spam > Content Scanning - Action

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



FIGURE 5-17. 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

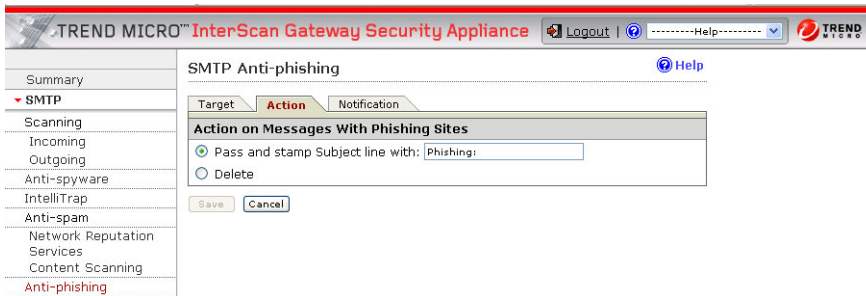


FIGURE 5-18. SMTP > Anti-phishing - Action

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:
 - **Pass 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**—The appliance deletes the message and any attachments.
4. Click **Save**.

SMTP Anti-Phishing - Notification

The screenshot shows the configuration interface for SMTP Anti-phishing notifications. On the left is a navigation menu with options like Summary, SMTP, Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation Services, Content Scanning, Anti-phishing (selected), Content Filtering, HTTP, FTP, POP3, Outbreak Defense, and Quarantines. The main panel is titled 'SMTP Anti-phishing' and has tabs for Target, Action, and Notification (selected). Below the tabs is a 'View variable list' link. The 'Email Notifications' section explains that notifications are sent when a phishing message is detected and certain items are selected. Two recipients are configured: 'Administrator' and 'Recipient'. The 'Administrator' notification text is: 'A threat was detected in a message. >Threat type: phishing >Sender: %SENDER% >Recipient: %RECIPIENT% >Subject: %SUBJECT%'. The 'Recipient' 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 this is a 'Report Potential Phishing URL' section with a link to 'Submit a Potential Phishing URL to TrendLabs' and 'Save' and 'Cancel' buttons at the bottom.

FIGURE 5-19. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. Click **Save**.

This screen contains 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 web interface. The left sidebar shows a navigation menu with 'SMTP' expanded, highlighting 'Content Filtering'. The main content area is titled 'SMTP Content Filtering' and includes a 'Help' link. The configuration is organized into several sections:

- Target** (selected tab): Contains a checkbox for 'Enable SMTP content filtering' which is checked.
- Filter by Message Size**: A section for filtering messages based on size. It includes a checkbox 'Filter if message size is larger than' which is checked, with a value of '5' and a unit of 'MB'.
- Filter by text in Message Header**: A section for filtering messages based on keywords in the message header (From, To, CC, and Subject fields). It includes a text input field for 'Word to filter from the header:', an 'Add >>' button, a 'Filter List' dropdown menu (currently set to 'None'), and a 'Match case' checkbox.
- Filter by Text in Message Body**: A section for filtering messages with certain words in the body area. It includes a text input field for 'Word to filter from body area:', an 'Add >>' button, a 'Filter List' dropdown menu (currently set to 'None'), and a 'Match case' checkbox.
- Filter by Message Attachment Name**: A section for filtering messages based on attachment file names. It includes 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 for filtering messages based on file types. It includes checkboxes for:
 - 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.)

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

FIGURE 5-20. 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

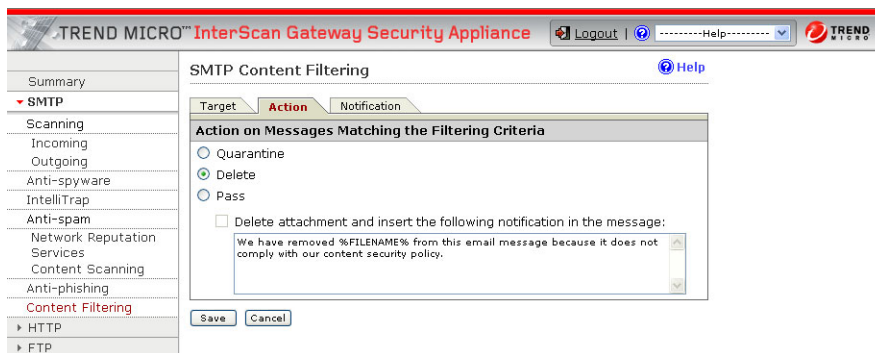


FIGURE 5-21. SMTP > Content Filtering - Action

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

The screenshot shows the Trend Micro InterScan Gateway Security Appliance web interface. On the left is a navigation menu with categories like Summary, SMTP, Scanning, Incoming, Outgoing, Anti-spyware, IntelliTrap, Anti-spam, Network Reputation Services, Content Scanning, Anti-phishing, and Content Filtering. The 'Content Filtering' category is expanded, showing sub-items: HTTP, FTP, POP3, Outbreak Defense, Quarantines, and Update. The main content area is titled 'SMTP Content Filtering' and has three tabs: Target, Action, and Notification. The 'Notification' tab is selected. Below the tabs, there is a 'View variable list' link. The 'Email Notifications' section contains a text box explaining that when a message matches filtering criteria, email notifications will be sent. Below this, there are three checkboxes for recipients: Administrator (checked), Sender (unchecked), and Recipient (checked). Each checkbox has a corresponding text box for customizing the notification message. The 'Administrator' message includes variables like %SENDER%, %RECIPIENT%, %SUBJECT%, and %ACTION%. The 'Sender' and 'Recipient' messages use %SENDER% and %RECIPIENT% variables. At the bottom of the notification area are 'Save' and 'Cancel' buttons.

FIGURE 5-22. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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 6-2
- *Configuring HTTP Virus Scanning* on page 6-4
- *Configuring HTTP Anti-Spyware* on page 6-14
- *Configuring HTTP Anti-Pharming* on page 6-18
- *Configuring HTTP Anti-Phishing* on page 6-20
- *Configuring HTTP URL Filtering* on page 6-23
- *Configuring HTTP File Blocking* on page 6-30

HTTP Services

The HTTP services of InterScan Gateway Security Appliance do the following:

- 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
- 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.

TREND MICRO™ InterScan Gateway Security Appliance

HTTP [Help](#)

You are allowed to enable or disable scanning of HTTP traffic. Enable to allow IGSA to scan for different types of threats originating from HTTP servers. To use the other HTTP scanning functionalities, this feature must be enabled.

Configuration

☒ Enable scanning of HTTP traffic

Service Port

InterScan Gateway Security Appliance listens to the following ports and performs HTTP scanning. Separate multiple entries with a semicolon (;).

HTTP listening service port(s): (1-65535)

[Save](#) [Cancel](#)

FIGURE 6-1. 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**.

Selecting an Alternative Service Port

The default listening port for HTTP services is 80. Administrators whose network security policy requires the use of nonstandard ports for servers may want to change this default.

To select an alternative service port for HTTP services:

1. On the left menu, click **HTTP**. The HTTP screen appears.
2. In the Service Port section, type the desired port in the **HTTP listening service port(s)** field.
3. Click **Save**. A message displays informing you that the appliance must reboot in order for this change to take effect.
4. Click **OK** to dismiss the message. A countdown screen appears and counts down from 3 minutes while the appliance is rebooting. When the appliance has rebooted, the Web console login screen appears.
5. Log on to the Web console to make any further changes.

Tip: If you are changing the HTTP service port as a security measure against hackers, Trend Micro recommends that you use the less common ports (those above 6,000).

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 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

HTTP Scanning

Help

Target

Action

Notification

☒ Enable HTTP 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: 200 (0-1000, 0:no limit)
Extracted file size exceeds: 30 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 ☐ Block

MIME Type Exceptions

Do not scan files of these MIME types:
text/plain
Separate multiple entries with a semicolon (;). For example: text/plain; application/pdf

Large File Handling

Do not scan files larger than 50 MB (1-100)
☒ Enable deferred scan
Start sending parts of the file to the client after: 2 seconds (1-100)
Send unscanned parts of a file to client no faster than: 16 Kbps

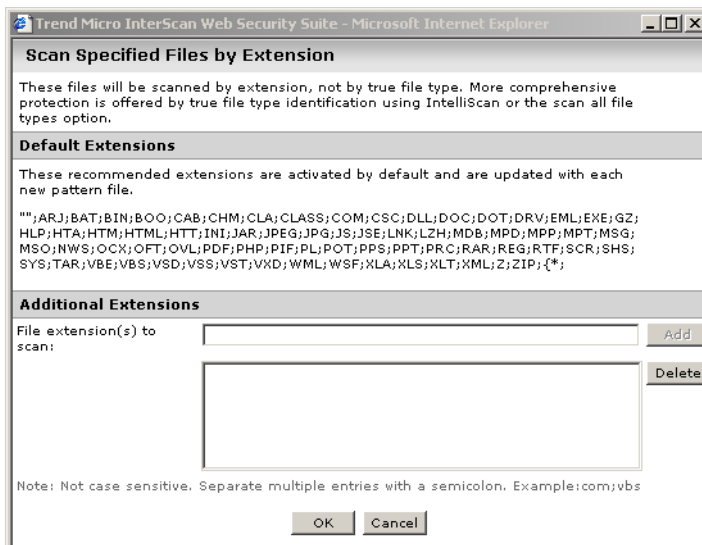
Save

Cancel

FIGURE 6-2. 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: 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 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 clicking **Specified file extensions...** and then clicking the link. A **Scan Specified Files by Extension** window appears.

**FIGURE 6-3. 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. Optionally, in the **MIME Type Exceptions** section, type any MIME types (for example, streaming audio/video) to exclude from scanning. (See [Setting MIME Type Exceptions](#) on page 6-8 for more information.)
 6. Specify how to handle large files.
 - **Do not scan files larger than:** Set size in MB. Default is 50 MB
 - **Start sending parts of the file to the client after:** The appliance starts sending parts of a large file to clients after a specified period so the connection between the client and the appliance will not time out.
 - **Send unscanned parts of a file to client no faster than:** Limit the speed of unscanned data by selecting a transfer rate (in kilobits per second) to suit the bandwidth of your network. (See [About Deferred Scan for Large File Handling](#) on page 6-11 for more information about this option.)
 7. Click **Save**.

Setting MIME Type Exceptions

There are many MIME types. To exclude specific MIME types from scanning, type the exact MIME type in the MIME Type Exceptions section of the HTTP Scanning Target tab.

Common Internet Media Types

To find the MIME type of a certain kind of file to exclude from scanning, the table below for a description of commonly used MIME types.

TABLE 6-1. Common Internet media types and subtypes, by category

Type/Subtype	Description
Type: Audio	
audio/mpeg	MP3 or other MPEG audio
audio/x-ms-wma	Microsoft™ Windows Media Audio file
audio/x-realaudio	RealAudio file
audio/x-wav	WAV audio file
Type: Image	
image/gif	GIF image
image/jpeg	JPEG JFIF image
image/png	Portable Network Graphics
image/tiff	Tagged-Image File Format file
Type: Multipart	
multipart/mixed or multipart/alternative	Archives and other objects made of more than one part
Type: Text	
text/css	Cascading Style Sheets
text/html; charset=UTF-8	HTML in UTF-8 character encoding
text/javascript	Deprecated. RFC 4329 replaces this type with: application/javascript.
text/plain; charset=ISO 8859-1	Textual data in ISO 8859-1 character encoding
text/plain; charset=UTF-8	Textual data in UTF-8 character encoding

TABLE 6-1. Common Internet media types and subtypes, by category (Continued)

Type/Subtype	Description
Type: Video	
video/mpeg	MPEG-1 video with multiplexed audio
video/x-ms-wmv	Microsoft Windows Media Video file
video/x-shockwave-flash	Adobe Flash™ video
Type: Application	
application/javascript	ECMAScript (such as JavaScript)
application/octet-stream	Byte streams that are unspecified. This subtype is the "default" media type, often used to identify executable files or files of unknown type.
application/ogg	Ogg, a multimedia bitstream container format
application/postscript	File formatted in PostScript page description language
application/xhtml+xml; charset=UTF-8	XHTML, a successor to HTML, in UTF-8 encoding

An Internet media type (or MIME type) identifies the kind of file that is traveling through an HTTP stream. This media type is a two-part identifier for file formats on the Internet.

Standard Internet media types have the following format:

`type/subtype`

Nonstandard types have subtype that is prefixed with an `x-`, as follows:

`type/x-subtype`

Vendor-specific types have a subtype with a `vnd.` prefix, as follows:

`type/vnd.subtype`

Capturing Network Traffic for Analysis

If the kind of file that you are looking for is not listed in Table 6-1, “Common Internet media types and subtypes, by category,” on page 6-8, you can determine the MIME type by using a network traffic capture utility (also known as packet sniffers) like Ethereal.

There are both free and commercially available network traffic capture utilities.

Locating the MIME type in Packet Sniffer Data

A typical packet sniffer application can return data on an HTTP stream similar to that shown here:

```
GET /midisong/wma/014223.wma HTTP/1.1
Accept: */*
User-Agent: NSPlayer/9.0.0.2980
Host: sample.some-domain.com
X-Accept-Authentication: NTLM, Digest, Basic
Pragma: version11-enabled=1
Pragma:
no-cache,rate=1.000,stream-time=0,stream-offset=0:0,packet-num=
4294967295,max-duration=0
Pragma: packet-pair-experiment=1
Pragma: pipeline-experiment=1
Supported: com.microsoft.wm.srvppair, com.microsoft.wm.sswitch,
com.microsoft.wm.predstrm
Pragma: xClientGUID={3300AD50-2C39-46c0-AE0A-9B31A4381F20}
Accept-Language: zh-TW, *,q=0.1
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
X-Powered-By: ASP.NET
Date: Tue, 23 Jan 2007 06:42:32 GMT
Content-Type: audio/x-ms-wma
Accept-Ranges: bytes
Last-Modified: Wed, 20 Dec 2006 08:20:06 GMT
ETag: "fcfd33a8f24c71:293f"
Content-Length: 51416
```

Search for the **Content-Type** field (shown in **red bold** above). The MIME type is listed next to this field.

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 a file is completely scanned before the appliance sends the file to the client and the browser loads it. This option can sometimes 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

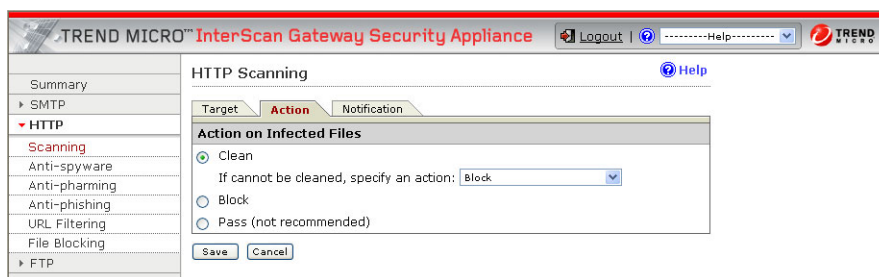


FIGURE 6-4. HTTP > Scanning - Action

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 6-13 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 configuration page for HTTP Scanning - Notification. On the left is 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 three tabs: Target, Action, and Notification (selected). A 'View variable list' link is in the top right. The 'User Notification' section contains a text box with the 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 for 'Administrator' which is checked, and a text box with the message: 'A threat was detected in HTTP traffic. >Threat type: virus/malware >Client IP address: %IPaddress% >Requested URL: %URL% >Date requested: %DATE%'. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 6-5. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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: [Text Input] [Add >>]
 - Exclusion Spyware/Grayware List: [List Box containing '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 [Warning Icon]

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

FIGURE 6-6. 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 options 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 table of 'Top 10 Spyware/Grayware' items. Below this is a section for 'Spyware/Grayware Advisories' with a table listing various advisories.

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 6-7. 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

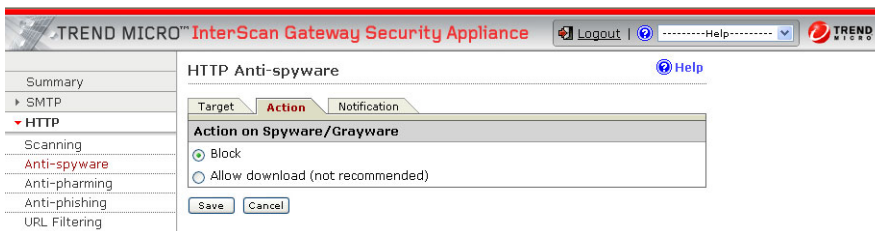


FIGURE 6-8. HTTP > Anti-spyware - Action

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

The screenshot shows the configuration page for HTTP Anti-spyware notifications. On the left is a navigation menu with options: Summary, SMTP, HTTP (selected), Scanning, Anti-spyware (selected), Anti-pharming, Anti-phishing, URL Filtering, File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main panel is titled 'HTTP Anti-spyware' and has three tabs: Target, Action, and Notification (selected). A 'View variable list' link is at the top right of the Notification tab. The 'User Notification' section contains a text box with the message: '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 has a checked 'Administrator' checkbox and a text box with the message: 'A threat was detected in HTTP traffic. >Threat type: spyware/grayware >Client IP address: %IPAddress% >Requested URL: %URL% >Date requested: %DATE%'. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 6-9. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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

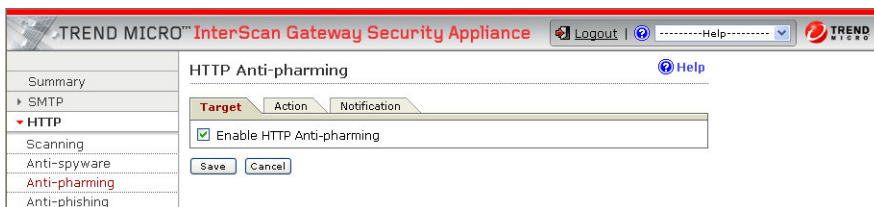


FIGURE 6-10. HTTP > Anti-pharming - Target

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

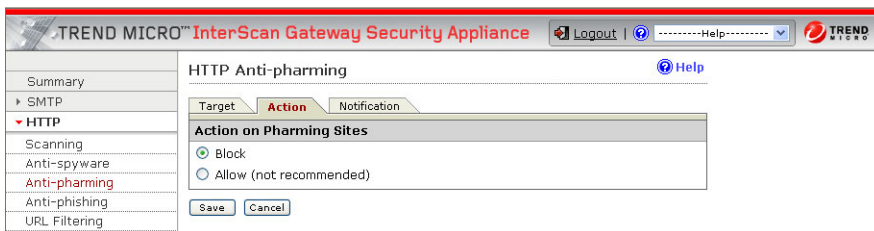


FIGURE 6-11. HTTP > Anti-pharming - Action

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

HTTP Anti-Pharming - Notification

The screenshot shows the configuration page for HTTP Anti-pharming notifications. The left sidebar contains a menu with options like Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-pharming (highlighted), Anti-phishing, URL Filtering, File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'HTTP Anti-pharming' and has three tabs: Target, Action, and Notification (selected). A 'View variable list' link is present. The 'User Notification' section contains a text box with a message to be displayed to the user. The 'Administrator Notification' section includes a checkbox for 'Administrator' and a list of variables to be included in the email notification.

TREND MICRO™ InterScan Gateway Security Appliance	
Summary	HTTP Anti-pharming Help
SMTP	Target Action Notification
HTTP	View variable list
Scanning	User Notification
Anti-spyware	Display the following message on the user's browser when a known pharming site is detected:
Anti-pharming	The URL you are attempting to access may redirect you to a site that collects confidential and personal data. Access to this URL has been blocked for security reasons. If you have any questions, contact your administrator.
Anti-phishing	Administrator Notification
URL Filtering	When a known pharming site is detected and the following item is selected, the corresponding email notification will be sent:
File Blocking	☒ Administrator A threat was detected in HTTP traffic.
FTP	>Threat type: pharming
POP3	>Client IP address: %IPAddress%
Outbreak Defense	>Requested URL: %URL%
Quarantines	>Date requested: %DATE%
Update	Save Cancel
Logs	
Administration	

FIGURE 6-12. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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

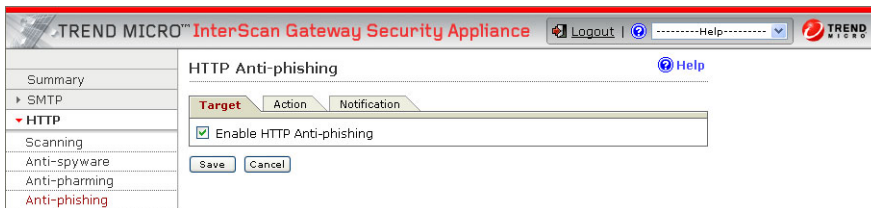


FIGURE 6-13. HTTP > Anti-phishing - Target

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

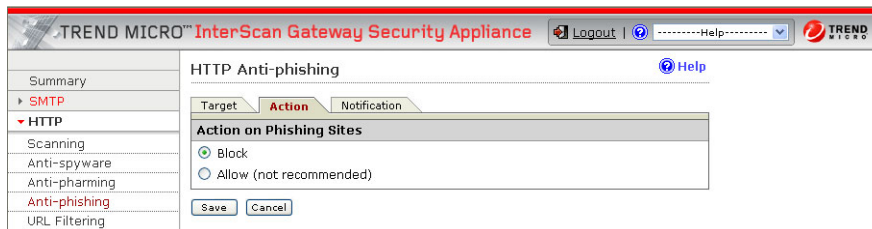


FIGURE 6-14. HTTP > Anti-phishing - Action

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

HTTP Anti-Phishing - Notification

The screenshot shows the configuration page for HTTP Anti-phishing - Notification. On the left is a navigation menu with options: Summary, SMTP, HTTP (selected), Scanning, Anti-spyware, Anti-pharming, Anti-phishing (highlighted in red), URL Filtering, File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'HTTP Anti-phishing' and has three tabs: Target, Action, and Notification (selected). A 'View variable list' link is in the top right. The 'Notification' tab contains sections for 'User Notification' (with a text area for a message), 'Administrator Notification' (with a checked 'Administrator' checkbox and a text area for a message), and 'Report Potential Phishing URL' (with a link to 'Submit a Potential Phishing URL to TrendLabs'). 'Save' and 'Cancel' buttons are at the bottom.

FIGURE 6-15. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. Click **Save**.

This screen contains 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

TREND MICRO™ InterScan Gateway Security Appliance

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 | Approved Clients | Settings | Notification

☒ Enable URL filtering

Filter the Selected Categories

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/Occult	☐	☐
Weapons/Military	☐	☐
Games	☐	☐
Blogs/Web Communications	☐	☐
Personals/Dating	☐	☐
Chat/Instant Messaging	☐	☐
Email	☐	☐
Newsgroups	☐	☐
Shopping/Auction	☐	☐
Software Downloads	☐	☐
Streaming Media/MP3	☐	☐
Job Search	☐	☐
Spyware	☐	☐
Adware/Joke Programs/Cookies	☐	☐
Personal Network Storage/File Download Servers	☐	☐
Photo Searches	☐	☐
Social Networking	☐	☐
Peer-to-Peer	☐	☐

Blocked URL List

FIGURE 6-16. HTTP > URL Filtering – URL Filtering Rules, top half of screen

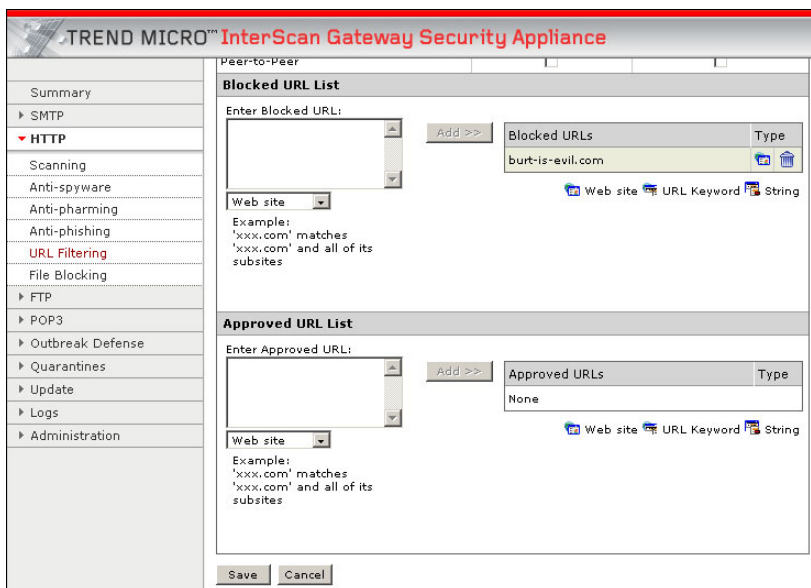


FIGURE 6-17. HTTP > URL Filtering – URL Filtering Rules, bottom half of screen

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 - Approved Clients List

Your organization may want to reserve one or more IP addresses for completely unfiltered access to the Internet. You can exempt one or more IP addresses from URL filtering. You can create another URL filtering rule on top of the existing Global URL policy. Using this rule, you can exclude an IP address from scanning by placing it in an Approved Clients (exception) list.

The appliance does not filter HTTP requests from any IP address in the Approved Clients list.

HTTP URL Filtering [Help](#)

URL Filtering Rules **Approved Clients** Settings Notification

Approved Client IP Addresses

Specify the client IP addresses or IP ranges to exclude from the URL filtering rules:

IP/IP range:

Add >>

Address/Range

10.2.14.171	
244.244.244.244-255.255.255.255	
<ip address>	
<ip address>	
<ip address>	

Example:
IP: 10.1.1.0
IP range: 10.1.1.0-10.1.1.10

Save Cancel

FIGURE 6-18. HTTP URL Filtering > Approved Clients tab

To input IP addresses to exclude from URL filtering:

1. From the left-side menu, select **HTTP > URL Filtering**. The URL Filtering Rules tab appears.
2. Click the **Approved Clients** tab.
3. In the IP/IP range field, type an IP address or range (up to 100 separate entries) and click **Add>>**. The IP address and/or addresses that you typed move over to the Address/Range box on the right.
4. Click **Save**. InterScan Gateway will not filter URLs in HTTP traffic going to those IP addresses and/or ranges.

HTTP URL Filtering - Settings

HTTP URL Filtering Help

URL Filtering Rules | Approved Clients | **Settings** | Notification

Work Time Settings

Work Days:

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

Work Times:

☒ All day (24 hours)

☐ Specify work hours

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

☒ Morning

From: 08:00 To: 12:00

☒ Afternoon

From: 13:00 To: 18:00

URL Rating Server Connection Settings ⓘ

Set timeout for online querying of Trend Micro URL rating server at: 5 seconds

Note: If the query of the URL rating server times out, then the appliance will allow access to the URL.

Connection Settings

☐ Allow URL filtering to use IGSA proxy settings

[View appliance proxy settings ...](#)

Save Cancel

FIGURE 6-19. 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. In the URL Rating Server Connection Settings section, set the timeout (in seconds) for online querying of the Trend Micro URL rating server.

Note: This timeout value applies to two waiting periods—the time that it takes:

- For the appliance to connect to the URL rating server
 - For the URL rating server to analyze the URL and return a rating
-

5. 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.

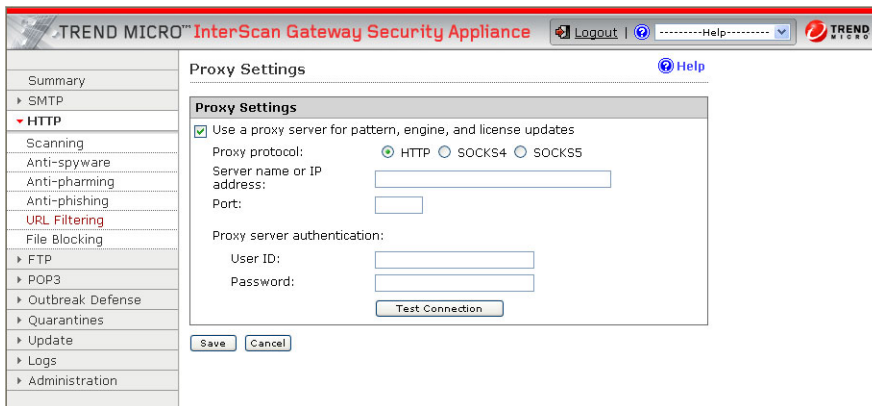


FIGURE 6-20. HTTP > URL Filtering – Proxy Settings

- 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
6. Click **Save**.

HTTP URL Filtering - 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 (selected), Scanning, Anti-spyware, Anti-pharming, Anti-phishing, URL Filtering (highlighted), File Blocking, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'HTTP URL Filtering' and has tabs for 'URL Filtering Rules', 'URL Filtering Rules', 'Settings', and 'Notification' (selected). A 'View variable list' link is present. The 'User Notification' section displays a message template for blocked URLs. The 'Administrator Notification' section includes a checked 'Administrator' checkbox and a text area with variables for client IP, requested URL, date, and time. At the bottom, there is a 'Submit URL to TrendLabs for Reclassification' link and 'Save' and 'Cancel' buttons.

TREND MICRO™ InterScan Gateway Security Appliance

HTTP URL Filtering Help

URL Filtering Rules URL Filtering Rules Settings **Notification** [View variable list](#)

User Notification

Display the following message on the user's browser when user attempts to access a blocked URL:

The URL you are attempting to access has been blocked. Organization policy prohibits accessing this type of site. If you have any questions, contact your administrator.

Administrator Notification

When a site is blocked and the following item is enabled, the corresponding email notification will be sent.

☒ Administrator Access to a restricted site was attempted.
 > Client IP address: %IPAddress%
 > Requested URL: %URL%
 > Date requested: %DATE%
 > Time requested: %TIME%

Submit URL to TrendLabs for Reclassification

<http://www.trendmicro.com/submit-files/index.htm>

FIGURE 6-21. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. Click **Save**.

This screen contains 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).

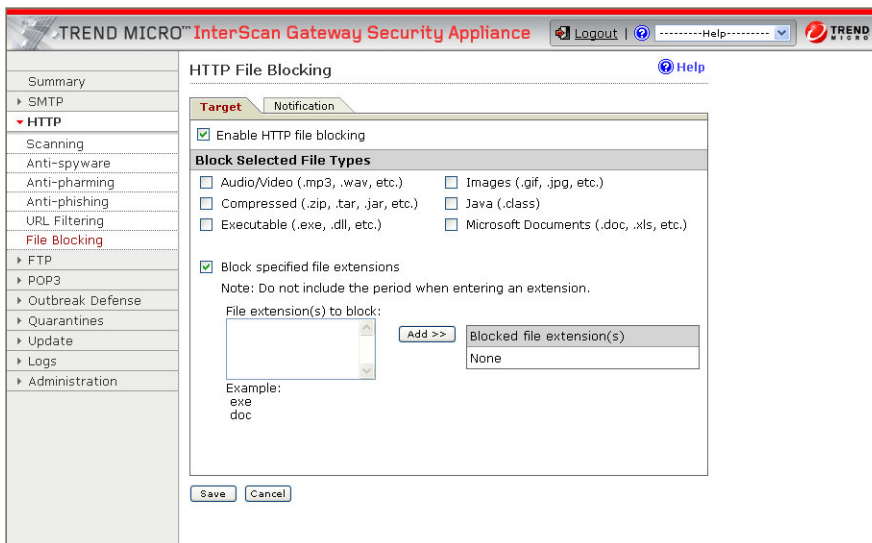


FIGURE 6-22. HTTP > File Blocking - Target

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 web interface of a Trend Micro InterScan Gateway Security Appliance. The left-hand navigation menu is expanded to show 'HTTP' > 'File Blocking'. The main content area is titled 'HTTP File Blocking' and has two tabs: 'Target' and 'Notification'. The 'Notification' tab is active, showing configuration options for user and administrator notifications. The 'User Notification' section includes a text area for a message to be displayed to the user. The 'Administrator Notification' section includes a checkbox for 'Administrator' and a text area for an email notification template with placeholders for client IP, file name, date, and time. At the bottom are 'Save' and 'Cancel' buttons.

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 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 blocked file type is detected and the following item is enabled, 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 6-23. 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 7-4
- *Configuring FTP Anti-Spyware* on page 7-8
- *Configuring FTP File Blocking* on page 7-12

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.

TREND MICRO™ InterScan Gateway Security Appliance

HTTP [Help](#)

You are allowed to enable or disable scanning of HTTP traffic. Enable to allow IGSA to scan for different types of threats originating from HTTP servers. To use the other HTTP scanning functionalities, this feature must be enabled.

Configuration

☒ Enable scanning of HTTP traffic

Service Port

InterScan Gateway Security Appliance listens to the following ports and performs HTTP scanning. Separate multiple entries with a semicolon (;).

HTTP listening service port(s): (1-65535)

FIGURE 7-1. 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**.

Selecting an Alternative Service Port

The default listening port for FTP services is 21. Administrators whose network security policy requires the use of nonstandard ports for servers may want to change this default.

To select an alternative service port for FTP services:

1. On the left menu, click **FTP**. The FTP screen appears.
2. In the Service Port section, type the desired port in the **FTP listening service port(s)** field.

3. Click **Save**. A message displays informing you that the appliance must reboot in order for this change to take effect.
4. Click **OK** to dismiss the message. A countdown screen appears and counts down from 3 minutes while the appliance is rebooting. When the appliance has rebooted, the Web console login screen appears.
5. Log on to the Web console to make any further changes.

Tip: If you are changing the FTP service port as a security measure against hackers, Trend Micro recommends that you use the less common ports (those above 6,000).

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 displays the 'FTP Scanning' configuration page in the Trend Micro InterScan Gateway Security Appliance web interface. The left-hand navigation pane shows a tree structure with 'FTP' selected under the 'Scanning' category. The main content area features three tabs: 'Target', 'Action', and 'Notification'. The 'Target' tab is currently selected, revealing the following settings:

- Enable FTP scanning:** A checked checkbox.
- Files to Scan:** Three radio button options: 'All scannable files' (selected), 'IntelliScan: uses true file type identification', and 'Specified file extensions...'.
- File Handling:** A section titled 'Do not scan compressed files if:' containing four rows of settings:
 - 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:** Radio buttons for 'Pass' (selected) and 'Block'.
- Large File Handling:** A section titled 'Do not scan files larger than' with a value of 50 MB (1-100). It includes a checked checkbox for 'Enable deferred scan' and a text field for 'Start sending parts of the file to the client after' set to 10 (1-100) seconds.

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

FIGURE 7-2. 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 clicking **Specified file extensions...** and then 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 7-3. 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

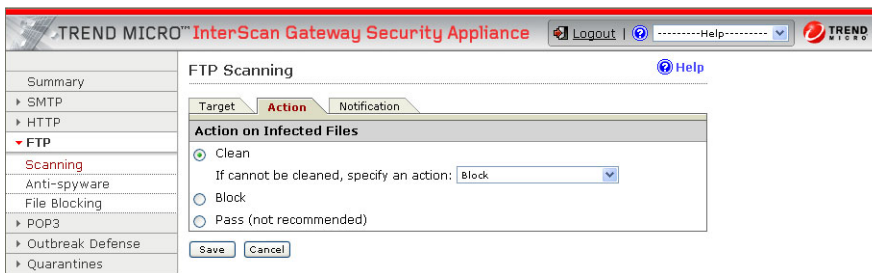


FIGURE 7-4. FTP > Scanning - Action

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
 - **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.
4. Click **Save**.

FTP Scanning - Notification

The screenshot shows the configuration interface for the Trend Micro InterScan Gateway Security Appliance. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP (selected), Scanning (selected), Anti-spyware, File Blocking, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'FTP Scanning' and has three tabs: Target, Action, and Notification (selected). A 'View variable list' link is present. The 'Notification' tab contains two sections: 'User Notification' and 'Administrator Notification'. The 'User Notification' section has a text area for a message to display to the user's browser. The 'Administrator Notification' section has a checkbox for 'Administrator' which is checked, and a text area for the email notification content. At the bottom are 'Save' and 'Cancel' buttons.

TREND MICRO™ InterScan Gateway Security Appliance	
Summary	FTP Scanning Help
▶ SMTP	Target Action Notification View variable list
▶ HTTP	
▼ FTP	
Scanning	
Anti-spyware	
File Blocking	
▶ POP3	
▶ Outbreak Defense	
▶ Quarantines	
▶ Update	
▶ Logs	
▶ Administration	
	User Notification Display the following message on the user's browser when the IGSA detects an infected file: 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.
	Administrator Notification When an infected file is detected and the following item is enabled, the corresponding email notification will be sent: ☒ Administrator A threat was detected in FTP traffic. >Threat type: virus/malware >Threat name: %VIRUSNAME% >Client IP address: %IPAddress% >Action taken: %ACTION%
	Save Cancel

FIGURE 7-5. 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. Select the **Administrator** check box to enable InterScan Gateway Security Appliance to send a notification if it detects a virus or malware.
4. Optionally, customize the text of any email notifications. The appliance provides helpful variables for use in customizing messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab.
5. 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.

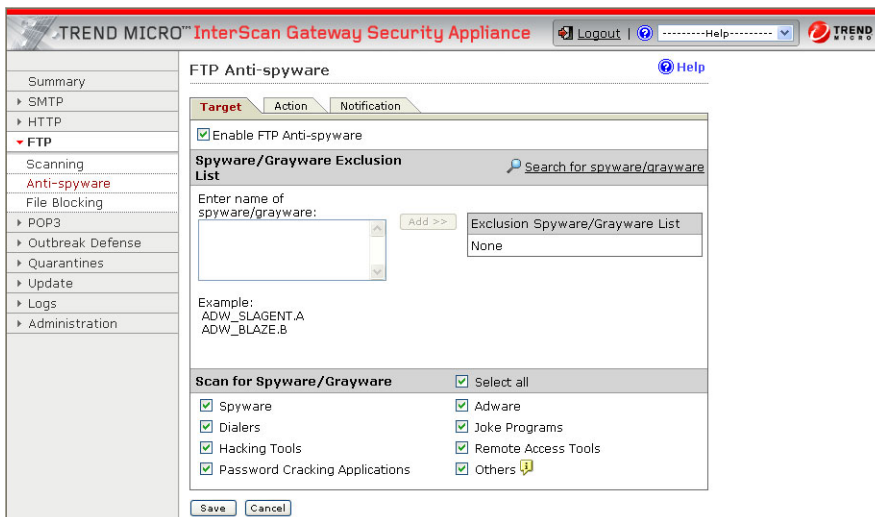


FIGURE 7-6. FTP > Anti-spyware - Target

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.

The screenshot shows the Trend Micro website's Spyware/Grayware section. The left sidebar contains a navigation menu with links like Virus Encyclopedia, Security Advisories, Scams & Hoaxes, Joke Programs, and Spyware/Grayware. The main content area has a search bar and a dropdown for 'Spyware/Grayware Type' set to 'Any Spyware/Grayware Type'. Below the search bar is a table titled 'Top 10 Spyware/Grayware' with columns for the name and reports. At the bottom, there is a section for 'Spyware/Grayware Advisories' with a table listing various spyware types, risk ratings, advisory dates, and pattern files.

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	RISK RATING	ADVISORY DATE	PATTERN FILE
TSPIY_SMALL.DGL	Low	Nov 5, 2006	Scan Pattern: 3.903.00
TSPIY_AGENT.FFE	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSPIY_LINEAGE.CJS	Low	Nov 1, 2006	Scan Pattern: 3.899.00
TSPIY_SMALL.ACF	Low	Oct 29, 2006	Scan Pattern: 3.897.00
TSPIY_LINEAGE.BJK	Low	Oct 21, 2006	Scan Pattern: 3.889.00
TSPIY_LINEAGE.CSJ	Low	Oct 18, 2006	Scan Pattern: 3.853.00
TSPIY_LINEAGE.CKB	Low	Oct 16, 2006	Scan Pattern: 3.897.00
TSPIY_LINEAGE.BYE	Low	Oct 14, 2006	Scan Pattern: 3.903.00
TSPIY_LINEAGE.DAV	Low	Oct 12, 2006	Scan Pattern: 3.851.00
TSPIY_LINEAGE.BDP	Low	Oct 11, 2006	Scan Pattern: 3.889.00

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 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

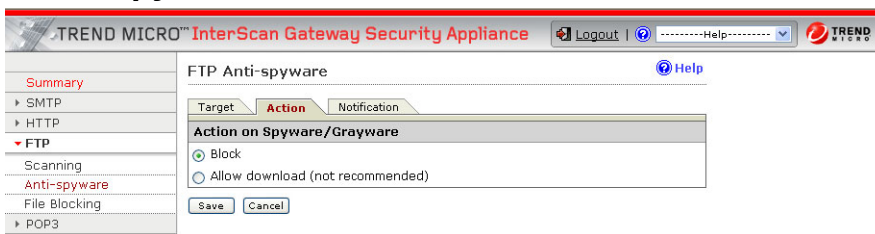


FIGURE 7-8. FTP > Anti-spyware - Action

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 configuration interface for the Trend Micro InterScan Gateway Security Appliance. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP (selected), Scanning, Anti-spyware (selected), File Blocking, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main panel is titled 'FTP Anti-spyware' and has tabs for Target, Action, and Notification (selected). A 'View variable list' link is in the top right of the Notification tab. The 'User Notification' section contains a text box with a message to be displayed to users. The 'Administrator Notification' section has a checked 'Administrator' checkbox and a text box with a customizable message using variables like %VIRUSNAME%, %IPAddress%, and %ACTION%. 'Save' and 'Cancel' buttons are at the bottom.

TREND MICRO™ InterScan Gateway Security Appliance

Summary
 ▶ SMTP
 ▶ HTTP
 ▼ **FTP**
 Scanning
Anti-spyware
 File Blocking
 ▶ POP3
 ▶ Outbreak Defense
 ▶ Quarantines
 ▶ Update
 ▶ Logs
 ▶ Administration

FTP Anti-spyware [Help](#)

Target Action **Notification** [View variable list](#)

User Notification
 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.

Administrator Notification
 When spyware/grayware is detected and the following item is selected, the corresponding email notification will be sent.

☒ Administrator A threat was detected in FTP traffic.
 >Threat type: spyware/grayware
 >Threat name: %VIRUSNAME%
 >Client IP address: %IPAddress%
 >Action taken: %ACTION%

Save Cancel

FIGURE 7-9. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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

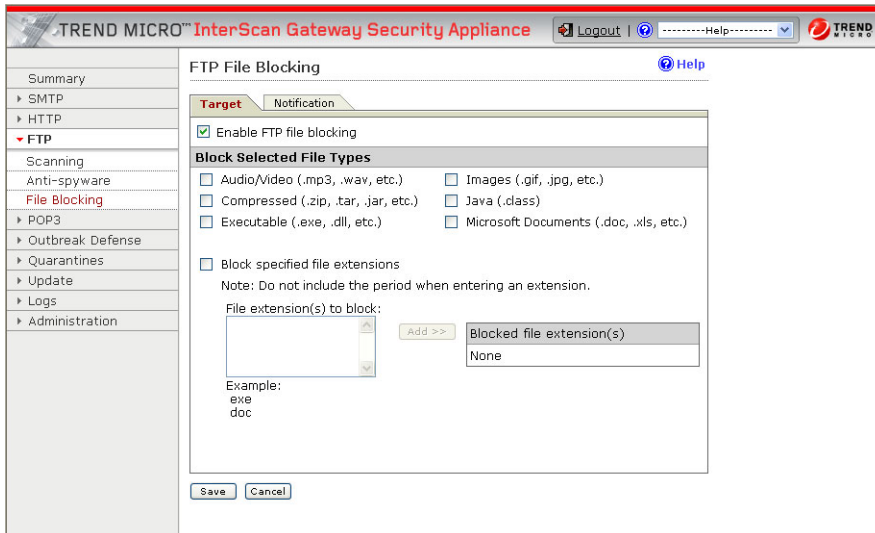


FIGURE 7-10. FTP > File Blocking - Target

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

The screenshot shows the configuration page for FTP File Blocking - Notification. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP (selected), Scanning, Anti-spyware, File Blocking (selected), POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area is titled 'FTP File Blocking' and has two tabs: 'Target' and 'Notification' (selected). A 'View variable list' link is present. Under 'User Notification', there is a text box for the message displayed to the user when a file is blocked. Under 'Administrator Notification', there is a checkbox for 'Administrator' (checked) and a text box for the email notification content, which includes variables like %IPAddress%, %FILENAME%, %DATE%, and %TIME%.

FIGURE 7-11. 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 the appliance blocks a file.

5. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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 8-4
- *Configuring POP3 Anti-Spyware* on page 8-10
- *Configuring POP3 IntelliTrap* on page 8-14
- *Configuring POP3 Anti-Spam* on page 8-17
- *Configuring POP3 Anti-Phishing* on page 8-19
- *Configuring POP3 Content Filtering* on page 8-22

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.

TREND MICRO™ InterScan Gateway Security Appliance

POP3 [Help](#)

You are allowed to enable or disable scanning of POP3 traffic. Enable to allow IGSA to scan for different types of threats originating from POP3 servers. To use the other POP3 scanning functionalities, this feature must be enabled.

Configuration

☒ Enable scanning of POP3 traffic

Service Port

InterScan Gateway Security Appliance listens to the following ports and performs POP3 scanning. Separate multiple entries with a semicolon (;).

POP3 listening service port(s): (1-65535)

FIGURE 8-1. 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**.

Selecting an Alternative Service Port

The default listening port for POP3 services is 110. Administrators whose network security policy requires the use of nonstandard ports for servers may want to change this default.

To select an alternative service port for POP3 services:

1. On the left menu, click **POP3**. The POP3 screen appears.
2. In the Service Port section, type the desired port in the **POP3 listening service port(s)** field.
3. Click **Save**. A message displays instructing you that the appliance must reboot in order for this change to take effect.
4. Click **OK** to dismiss the message. A countdown screen appears and counts down from 3 minutes while the appliance is rebooting. When the appliance has rebooted, the Web console login screen appears.
5. Log on to the Web console to make any further changes.

Tip: If you are changing the POP3 service port as a security measure against hackers, Trend Micro recommends that you use the less common ports (those above 6,000).

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 Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar contains a navigation menu with the following items: Summary, SMTP, HTTP, FTP, POP3 (selected), Scanning (selected), 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 configuration options:

- ☒ 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

FIGURE 8-2. 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 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;*.CLM;*.CLASS;*.COM;*.CSC;*.DLL;*.DOC;*.DOT;*.DRV;*.EML;*.EXE;*.GZ;*.HLP;*.HTA;*.HTM;*.HTML;*.HTT;*.INI;*.JAR;*.JPEG;*.JPG;*.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:

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

FIGURE 8-3. 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.
 - 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 8-4. 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 the way in which InterScan Gateway Security Appliance responds to them.

TABLE 8-1. “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.
- **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.

4. Click **Save**.

POP3 Scanning - Notification

The screenshot shows the 'POP3 Scanning' configuration page for the 'Notification' tab. The left sidebar contains a navigation menu with 'POP3' selected and expanded, showing 'Scanning' as the active sub-menu. The main content area is titled 'POP3 Scanning' and includes a 'Help' link. Below the title bar, there are tabs for 'Target', 'Action', and 'Notification', with 'Notification' being the active tab. A 'View variable list' link is also present. The 'Email Notifications' section explains that notifications are sent when an infected message is detected and specific items are selected. It lists three notification types: 'Administrator' (checked), 'Sender' (unchecked), and 'Recipient' (checked). Each type has a corresponding text box for the notification message, which includes variables like %VIRUSNAME%, %SENDER%, and %RECIPIENT%. The 'Inline Notification Stamp' section allows selecting text to insert into scanned messages before they are sent to recipients. It includes three sections: 'Security risk Detected Notifications' (with 'Subject line' checked and 'Message' unchecked), 'Security risk Free Notifications' (with 'Message' checked), and 'Unscannable File Notifications' (with 'Message' checked). At the bottom, there are 'Save' and 'Cancel' buttons.

TREND MICRO™ InterScan Gateway Security Appliance

Summary

- SMTP
- HTTP
- FTP
- POP3**
 - Scanning
 - Anti-spyware
 - IntelliTrap
 - Anti-spam
 - Anti-phishing
 - Content Filtering
 - Outbreak Defense
 - Quarantines
 - Update
 - Logs
 - Administration

POP3 Scanning [Help](#)

Target Action **Notification** [View variable list](#)

Email Notifications

When an infected message is detected and any of the following items are selected, 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:

Security risk Detected Notifications:

☒ **Subject line:** Risk detected:

☐ **Message** This message contains a possible security risk.

Security risk Free Notifications:

☒ **Message** Trend Micro InterScan Security Gateway Appliance has scanned this message and found it to be free of known security risks.

Unscannable File Notifications:

☒ **Message** InterScan Gateway Security Appliance has scanned this message and found that one or more unscannable files are attached to it.

Save **Cancel**

FIGURE 8-5. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
6. 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

The screenshot displays the 'POP3 Anti-spyware' configuration page. On the left is a navigation menu with options like Summary, SMTP, HTTP, FTP, POP3 (selected), Scanning, Anti-spyware (selected), IntelliTrap, Anti-spam, Anti-phishing, Content Filtering, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main content area has three tabs: Target, Action, and Notification. The 'Target' tab is active, showing a checked box for 'Enable POP3 Anti-spyware'. Below this is a 'Spyware/Grayware Exclusion List' section with a search bar and a list box currently containing 'None'. An example shows 'ADW_SLAGENT.A' and 'ADW_BLAZE.B'. At the bottom, the 'Scan for Spyware/Grayware' section has a checked 'Select all' box and a grid of checked items: Spyware, Dialers, Hacking Tools, Password Cracking Applications, Adware, Joke Programs, Remote Access Tools, and Others. 'Save' and 'Cancel' buttons are at the bottom left.

FIGURE 8-6. 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 shows 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 'Top 10' list of spyware/grayware items with their names and report counts. At the bottom, there's 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
■ 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.CJS	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 8-7. Trend Micro Spyware/Grayware Online Database

- Search for the spyware 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 8-8. 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

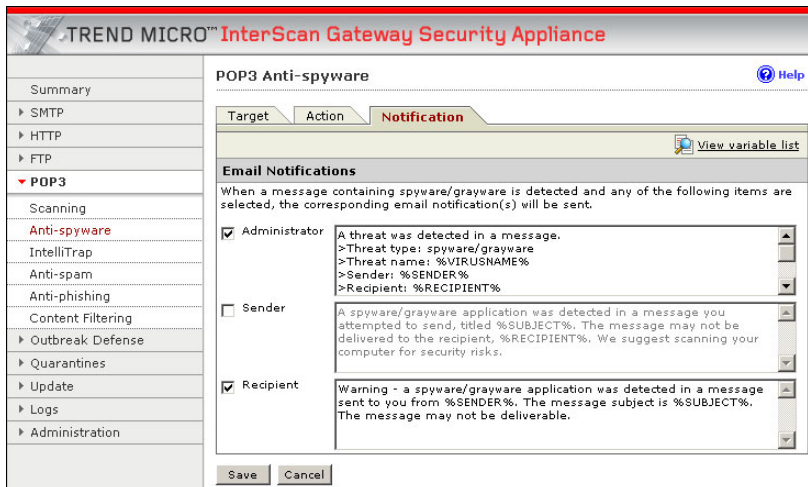


FIGURE 8-9. POP3 > Anti-spyware - Notification

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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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

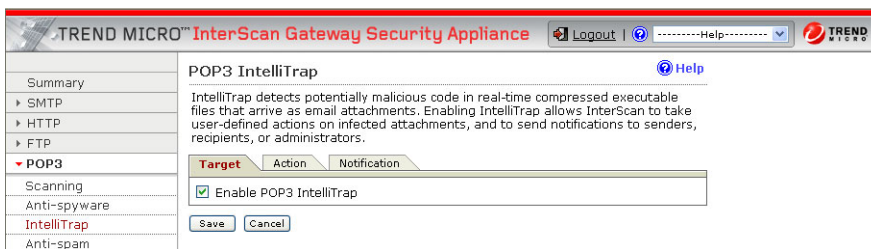


FIGURE 8-10. POP3 > IntelliTrap - Target

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 8-11. 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

TREND MICRO™ InterScan Gateway Security Appliance

Summary

- SMTP
- HTTP
- FTP
- POP3**

Scanning

- Anti-spyware
- IntelliTrap**
- Anti-spam
- Anti-phishing
- Content Filtering
- Outbreak Defense
- Quarantines
- Update
- Logs
- Administration

POP3 IntelliTrap [Help](#)

IntelliTrap detects potentially malicious code in real-time compressed executable files that arrive as email attachments. Enabling IntelliTrap allows InterScan to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Target Action **Notification** [View variable list](#)

Email Notifications

When IntelliTrap detects a potential threat and any of the following items are selected, the corresponding email notification(s) will be sent.

☒ **Administrator** IntelliTrap detected a threat in a message.
 >Threat type: packer
 >Threat name: %VIRUSNAME%
 >Infected file name: %FILENAME%
 >Sender: %SENDER%

☐ **Sender** Warning - a file named %FILENAME%, containing a malicious application named %VIRUSNAME% was detected in a message sent to recipient %RECIPIENT% from your computer. The message subject is %SUBJECT%. The message may not have been delivered.

☒ **Recipient** Warning - a file named %FILENAME%, containing a malicious application named %VIRUSNAME% was detected in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be deliverable.

[Save](#) [Cancel](#)

FIGURE 8-12. POP3 > IntelliTrap - Notification

To select POP3 IntelliTrap – Notification recipient(s):

- From the left-side menu, click POP3 > IntelliTrap.
- Click the **Notification** tab.
- 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
- Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
- 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

TREND MICRO™ InterScan Gateway Security Appliance

Logout | Help

POP3 Anti-spam

Summary

- SMTP
- HTTP
- FTP
- POP3
- Scanning
 - Anti-spyware
 - IntelliTrap
 - Anti-spam
 - Anti-phishing
 - Content Filtering
 - Outbreak Defense
 - Quarantines
- Update
- Logs
- Administration

Target Action

☒ Enable POP3 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 8-13. 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

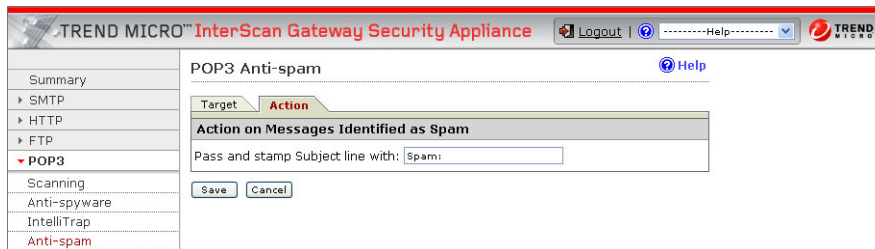


FIGURE 8-14. POP3 > Anti-spam - Action

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

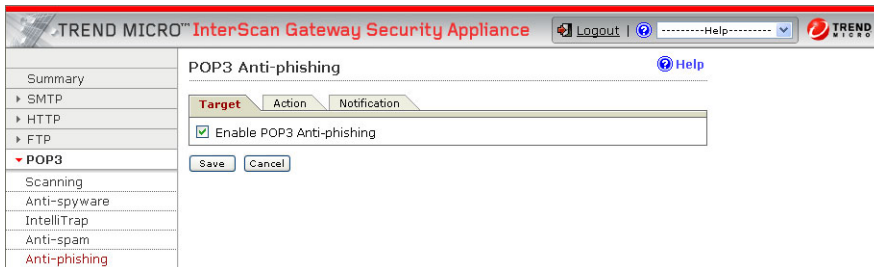


FIGURE 8-15. POP3 > Anti-phishing - Target

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

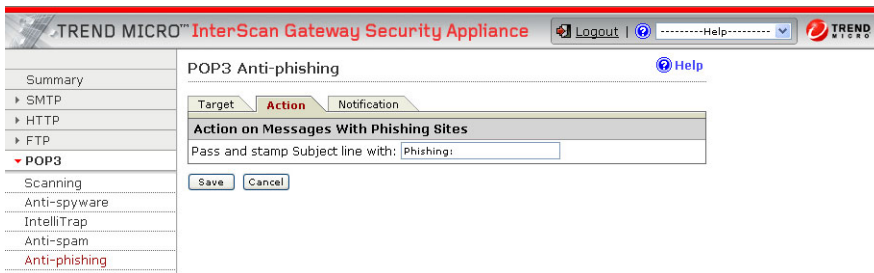


FIGURE 8-16. POP3 > Anti-phishing - Action

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

The screenshot shows the 'POP3 Anti-phishing' configuration page. On the left is a navigation menu with options: Summary, SMTP, HTTP, FTP, POP3 (selected), Scanning, Anti-spyware, IntelliTrap, Anti-spam, Anti-phishing (selected), Content Filtering, Outbreak Defense, Quarantines, Update, Logs, and Administration. The main area is titled 'POP3 Anti-phishing' and has three tabs: Target, Action, and Notification (selected). Below the tabs is a 'View variable list' link. The 'Email Notifications' section explains that when a phishing message is detected, corresponding email notifications will be sent. Two recipients are selected: 'Administrator' and 'Recipient'. The 'Administrator' notification message is: 'A threat was detected in a message. >Threat type: phishing >Sender: %SENDER% >Recipient: %RECIPIENT% >Subject: %SUBJECT%'. The 'Recipient' notification message 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 this is a 'Report Potential Phishing URL' section with a link to 'Submit a Potential Phishing URL to TrendLabs'. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 8-17. 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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. Click **Save**.

This screen contains 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 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

The screenshot displays the 'POP3 Content Filtering' configuration page in the Trend Micro InterScan Gateway Security Appliance web interface. The left sidebar shows a navigation menu with options like 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 Content Filtering' and includes a 'Help' link. It features four tabs: 'Target' (active), 'Action', and 'Notification'. Under the 'Target' tab, there is a checkbox for 'Enable POP3 content filtering'. Below this are three filter sections: 'Filter by Message Size', 'Filter by Text in Message Header', and 'Filter by Text in Message Body'. Each section includes a text input for a word to filter, an 'Add >>' button, and a 'Filter List' dropdown menu. The 'Filter by Message Attachment Name' section includes a text input for a word to filter from attachments, an 'Add >>' button, and a 'Filter List' dropdown menu. At the bottom, there is a 'Filter by True File Type' section with checkboxes for various file types: Audio/Video (.mp3, .wav, etc.), Images (.gif, .jpg, etc.), Compressed (.zip, .tar, .jar, etc.), Java (.class), Executable (.exe, .dll, etc.), and Microsoft Documents (.doc, .xls, etc.). The page concludes with 'Save' and 'Cancel' buttons.

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 5 Mb

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.)

Save Cancel

FIGURE 8-18. 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 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

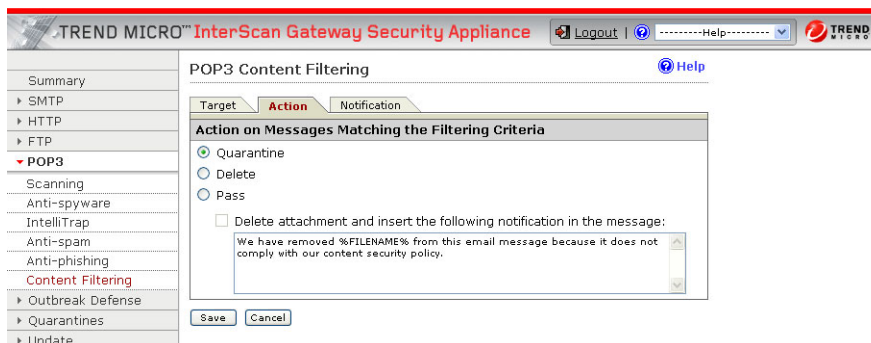


FIGURE 8-19. POP3 > Content Filtering - Action

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

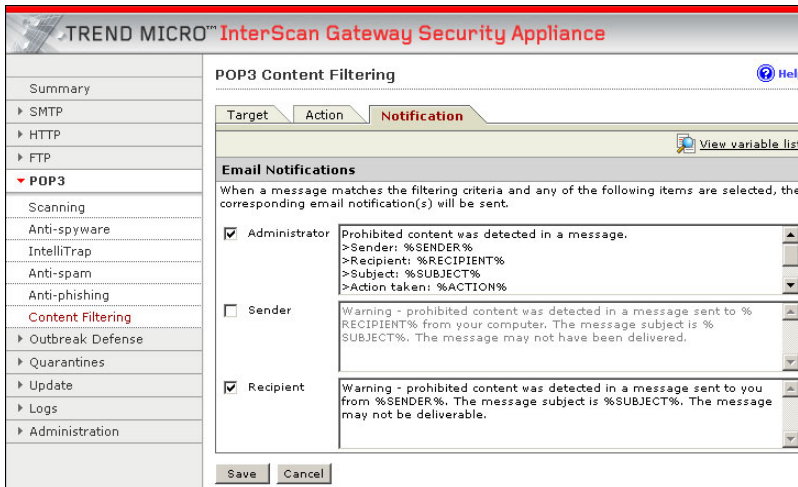


FIGURE 8-20. POP3 > Content Filtering - Notification

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. Optionally, customize the text of any of the email notifications. The appliance supports the use of some helpful variables in customized messages. A list of these variables is accessible from the **View variable list** link at the top right of the Notification tab working area.
5. 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 9-2
- *Current Status* on page 9-3
- *Configuring Internal Outbreak* on page 9-5
- *Configuring Damage Cleanup* on page 9-6
- *Configuring Settings* on page 9-7

The Outbreak Defense Services



FIGURE 9-1. 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 leftover malware and enables users to manually download the Damage Cleanup tool to remove malware.

Current Status

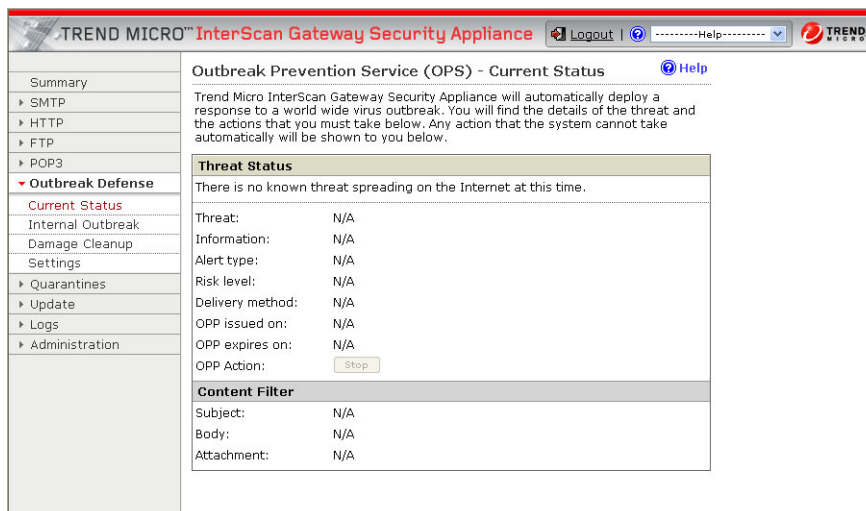


FIGURE 9-2. Outbreak Defense > Current Status

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 9-3. 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.

Note: This screen is disabled (greyed out) if you are managing the appliance using Trend Micro Control Manager. For more information on using Control Manager to manage the appliance, see [Introducing Trend Micro Control Manager™](#) on page B-1.

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, there is a paragraph explaining that Damage Cleanup detects threats and allows users to download a tool from a specific URL. 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: '10.1.1.0-10.1.1.10'. At the bottom, there are 'Save' and 'Cancel' buttons.

FIGURE 9-4. 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 the IP address of your appliance.

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).

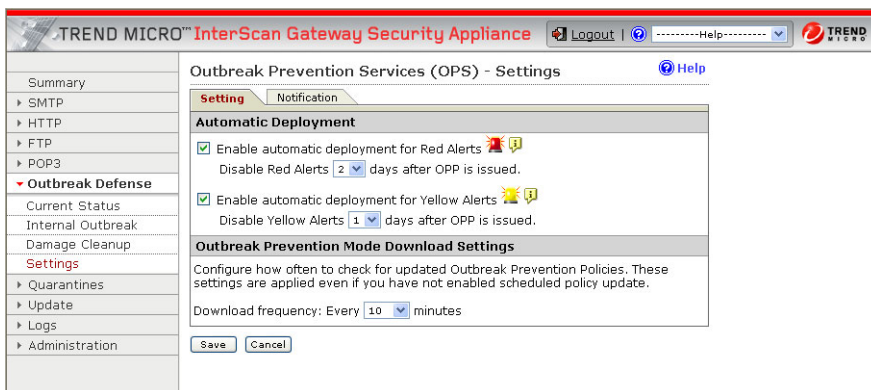


FIGURE 9-5. Outbreak Defense > Settings - Setting

Outbreak Defense - Settings

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**.

Note: This screen is disabled (greyed out) if you are managing the appliance using Trend Micro Control Manager. For more information on using Control Manager to manage the appliance, see *Introducing Trend Micro Control Manager™* on page B-1.

Outbreak Defense - Notification

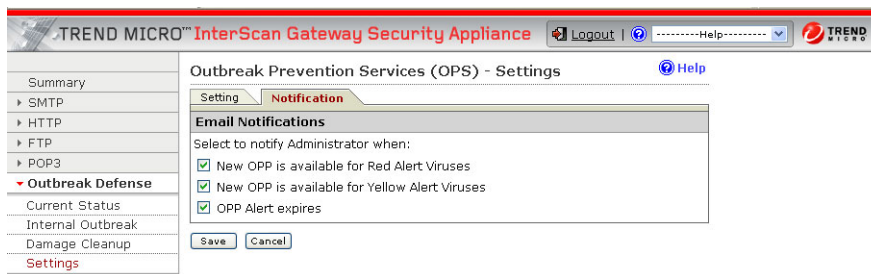


FIGURE 9-6. Outbreak Defense > Settings - Notification

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**.

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. The 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.

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.

Quarantines

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

- *Quarantines Screen* on page 10-2
- *Querying the Quarantine Folder* on page 10-4
- *Performing Query Maintenance* on page 10-9

Quarantines Screen

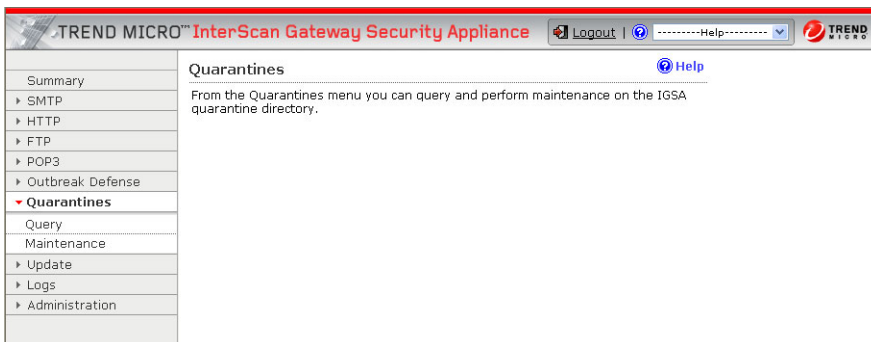


FIGURE 10-1. Quarantines

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.

WARNING! *The maximum limit for the quarantine folder is 1 million email messages. If you allow this 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.*

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.

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

Resending a Quarantined Email Message

Using the Web console, you can resend any email messages that the appliance has quarantined. In order to resend a message from the quarantine folder, query the quarantine folder(s) to produce the Quarantine Query Results screen. From that screen, you can resend the message.

The appliance moves any message selected for resending to a temporary directory. If the message resend succeeds, the appliance permanently removes the message from the quarantine folder. If the message resend fails, the appliance moves the message back to the quarantine folder.

See [Querying the Quarantine Folder](#) on page 10-4 for detailed procedures for resending a quarantined email message.

Adding an Inline Notification to Re-Sent Messages

You can add a notification message to each email message that you resend from the quarantine folder. The default message reads as follow but is customizable:

InterScan Gateway Security Appliance has quarantined this message, and it has been resent without scanning. Therefore, the message could contain a security risk.

To add an inline notification to re-sent email messages:

1. From the left-side menu, click **Quarantines > Settings**. The Quarantine Settings screen appears.
2. In the Inline Message for Resend section, select the **Append the following text in the resend message** check box.
3. Accept the default wording or revise it to suit the needs of your organization.
4. Click **Save**. InterScan Gateway Security Appliance will append this message to all future messages that you resend from the quarantine folder.

Querying the Quarantine Folder

TREND MICRO™ InterScan Gateway Security Appliance

Summary

- SMTP
- HTTP
- FTP
- POP3
- Outbreak Defense
- Quarantines**
 - Query**
- Settings
- Maintenance
 - Update
 - Logs
 - Administration

Quarantine Query [Help](#)

Criteria

Protocol: SMTP and POP3

Reason for quarantine: All

Time period: All

Range

From: 01/22/2007 00:00
mm/dd/yyyy hh mm

To: 01/23/2007 00:00
mm/dd/yyyy hh mm

Sender:

Recipient:

Subject:

☐ Display query results of only those quarantined messages that could not be delivered upon resending

Entries per page: 20

FIGURE 10-2. Quarantines > Query

To query the Quarantine folder:

- From the left-side menu, click **Quarantines > Query**.
- 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

- Click **Search**. The **Quarantine Query Results** screen appears, listing the results of your query.

Quarantine Query Results Help

Date Range: 10/22/02 - 11/15/02 Entries per page: 10

Export
 Delete
 Resend
 Scan and Resend
 1-10 of 20000 14 page 1 of 20000

☐ Date ▼	Protocol	Reason	Sender	Recipient	Subject
☐ 10/22/02 10:25:02	SMTP	Virus Scan	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	SMTP	Virus Scan	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	POP3	Virus Scan	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	POP3	Content Filtering	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	POP3	Spyware	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	SMTP	Spyware	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	SMTP	Spyware	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	SMTP	IntelliTrap	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	POP3	Virus Scan	Mark Lemke	Fred McGriff	Avail for Golf
☐ 10/22/02 10:25:02	SMTP	IntelliTrap	Mark Lemke	Fred McGriff	Avail for Golf

Export
 Delete
 Resend
 Scan and Resend
 1-10 of 20000 14 page 1 of 20000

Done

FIGURE 10-3. 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:

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

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

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

If you think that a legitimate message has ended up in the quarantine folder, you can try modifying the scanning criteria and then resending the message. You have two options in resending such a message:

- Scan and Resend
- Resend (without scanning)

Resending Without Scanning

If you are confident that the message contains no security risks, you can resend it without rescanning it. Follow the procedure below to resend a quarantined message without scanning it.

Scanning and Resending

If you think that the appliance has quarantined a message that is legitimate but are not sure, Trend Micro recommends that you use the Scan and Resend option to safely remove it from the quarantine folder. When you use this option, the appliance first scans the message according to your message scanning settings and then attempts to resend it. Follow the procedure below to scan and resend a quarantined message.

Tip: You can use this feature to fine-tune scan settings for email. Before clicking **Scan and Resend**, modify the scan setting that you think resulted in the quarantining of a legitimate message. Trend Micro recommends using Scan and Resend if there is any doubt as to the safety of the message.

To resend one or more quarantined messages:

1. Select the check box next to each message to resend.
2. To scan the message again before sending it, click the **Scan and Resend** link in the row of action icons and links just below the title row of the query results table. The appliance scans the message again. If the new scan finds no security risk in the message, the appliance resends it. If the new scan again finds a security risk, the appliance takes the action that you have configured in the Action tab for the email protocol (SMTP or POP3) listed for that message in the Quarantine Query Results table.
3. To resend the message without rescanning it, click the **Resend** link in the row of action icons and links just below the title row of the query results table. The appliance resends the message without scanning it.

Tip: Selecting the check box next to the Date heading selects 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 10-1. 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 shown in Table 10-2, “Exported query files – example contents,” on page 10-8, you would first look through the **index.txt** subjects until you found

the one that you were looking for. You would then make note of the file name associated with it and go back to the unzipped folder and double-click the file of the same name. The file would then open in the default text editor.

TABLE 10-2. 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 top right corner of the table to scroll through the list of messages.
- Click the drop-down menu next to **Rows per page** to select the number of entries to display per screen.
- Click **Done** to return to the Quarantine Query screen.

Performing Query 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

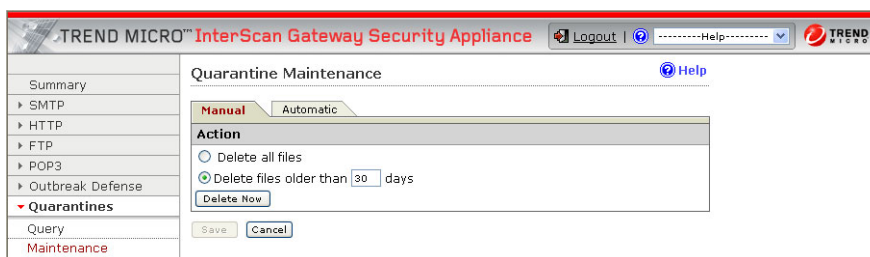


FIGURE 10-4. Quarantine > Maintenance - Manual

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

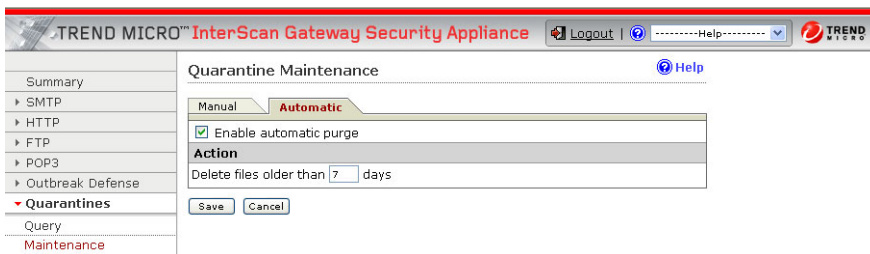


FIGURE 10-5. Quarantine > Maintenance - Automatic

To automatically purge messages from the Quarantine folder:

1. Click the **Maintenance > Automatic** tab.
2. Select the **Enable automatic purge** check box.
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.

Updating InterScan Gateway Security Appliance Components

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

- *Update* on page 11-2
- *Updating Manually* on page 11-3
- *Configuring Scheduled Updates* on page 11-4
- *Configuring an Update Source* on page 11-6

Update

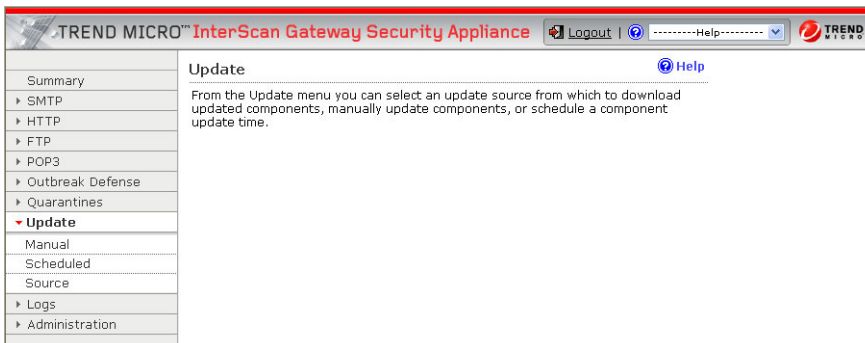


FIGURE 11-1. Update screen

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.

Updating Manually

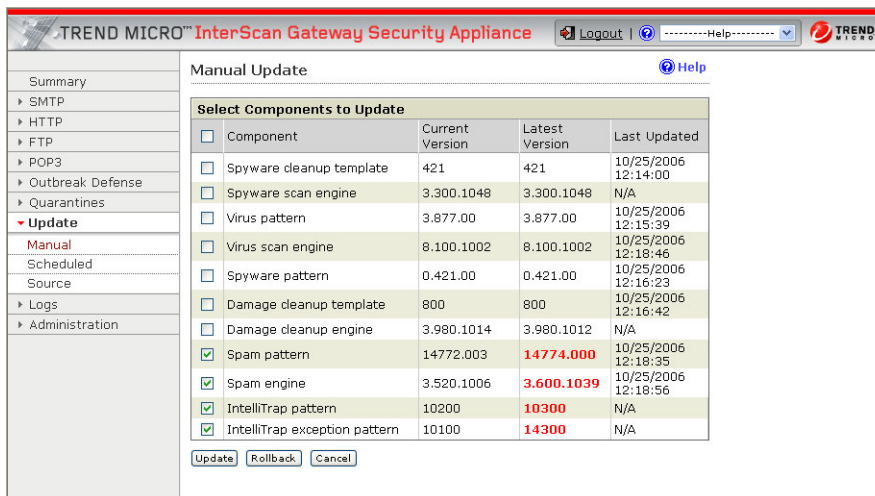


FIGURE 11-2. Update > Manual

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 00:00 (hh:mm)

Save Cancel

FIGURE 11-3. 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**.

Note: This screen is disabled (greyed out) if you are managing the appliance using Trend Micro Control Manager. For more information on using Control Manager to manage the appliance, see *[Introducing Trend Micro Control Manager™](#)* on page B-1.

Configuring an Update Source

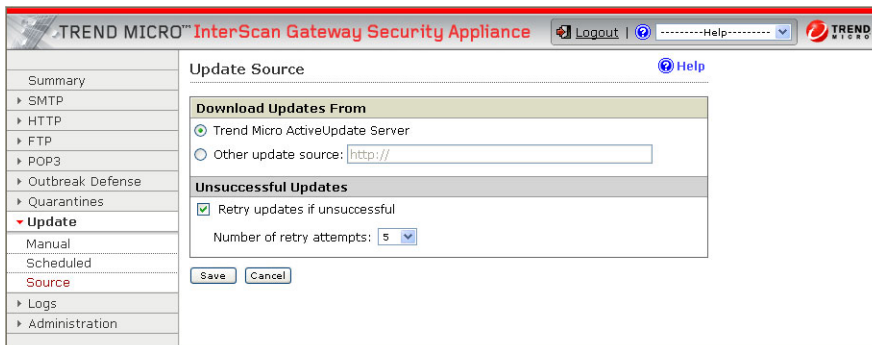


FIGURE 11-4. Update > Source

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**.

Note: This screen is disabled (greyed out) if you are managing the appliance using Trend Micro Control Manager. For more information on using Control Manager to manage the appliance, see *Introducing Trend Micro Control Manager™* on page B-1.

Analyzing Your Protection Using Logs

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

- *Logs* on page 12-2
- *Querying Logs* on page 12-3
- *Configuring Log Settings* on page 12-5
- *Configuring Log Maintenance* on page 12-6

Logs

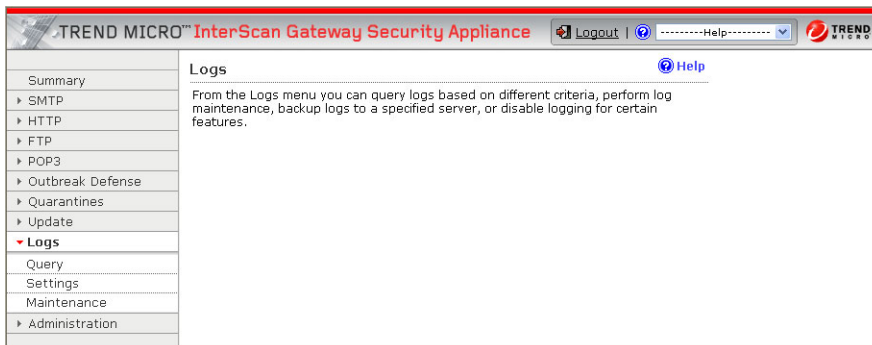


FIGURE 12-1. Logs screen

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.

Querying Logs

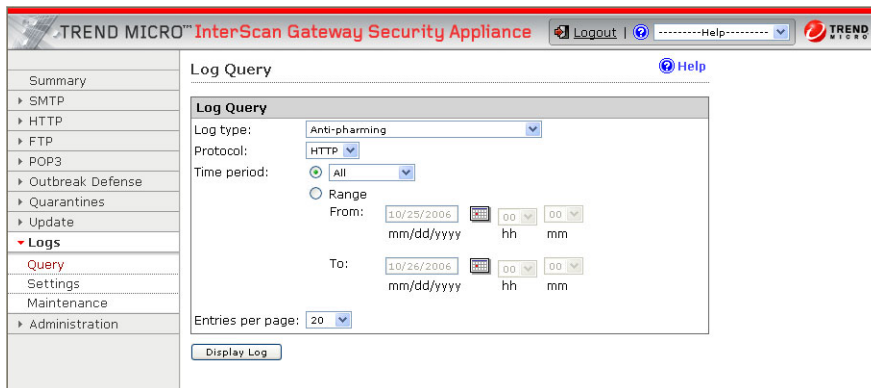


FIGURE 12-2. Logs > Query

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 12-3. 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

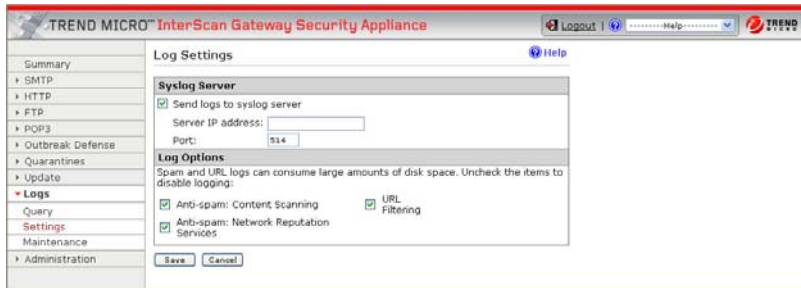


FIGURE 12-4. Logs > Settings

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

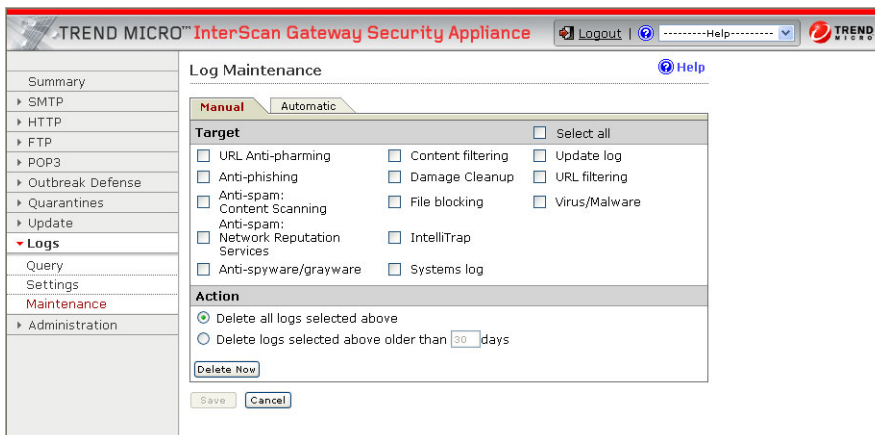
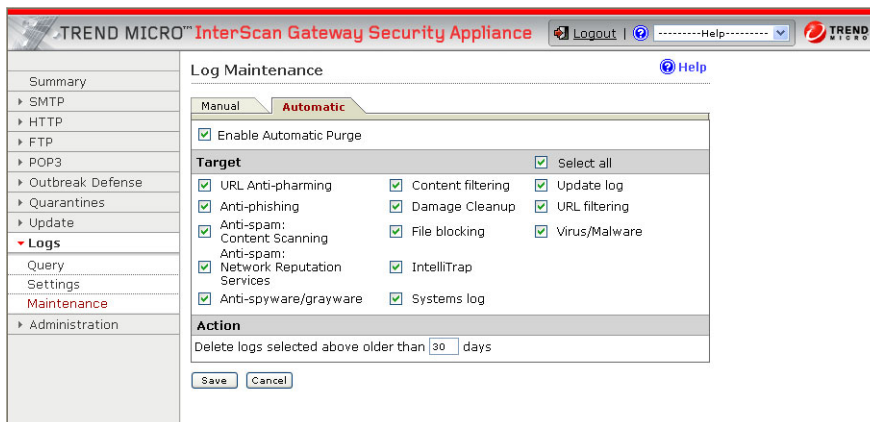


FIGURE 12-5. Logs > Maintenance - Manual

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 12-6. 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.

Administrative Functions

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

- *Administration* on page 13-2
- *Access Control* on page 13-3
- *Configuration Backup* on page 13-3
- *Control Manager Settings* on page 13-5
- *Disk SMART Test* on page 13-8
- *Firmware Update* on page 13-9
- *IP Address Settings* on page 13-10
- *Notification Settings* on page 13-15
- *Operation Mode* on page 13-18
- *Password* on page 13-19
- *Product License* on page 13-20
- *Proxy Settings* on page 13-24
- *SNMP Settings* on page 13-26
- *System Time* on page 13-27
- *Reboot from Web Console* on page 13-30
- *World Virus Tracking* on page 13-31

Administration

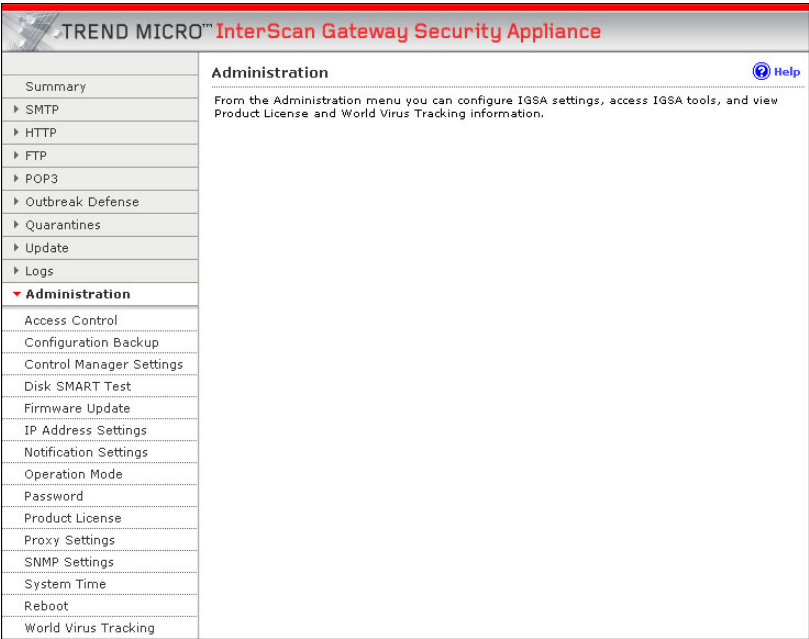


FIGURE 13-1. Administration screen

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

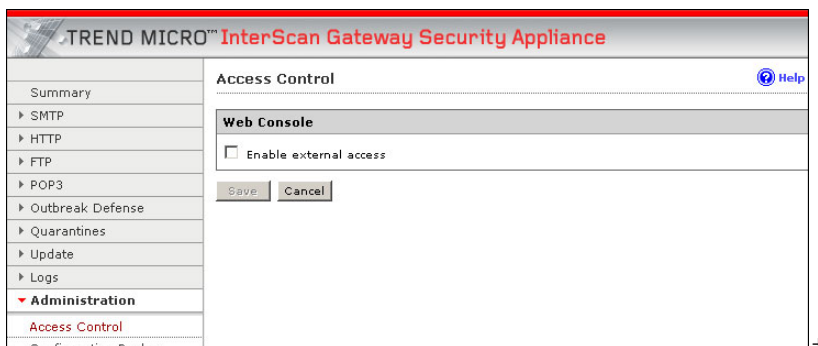


FIGURE 13-2. Administration > Access Control

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

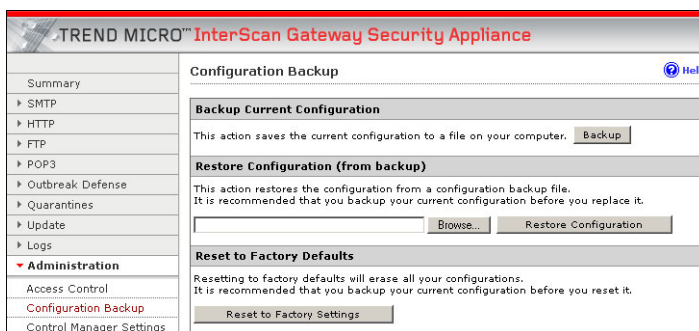
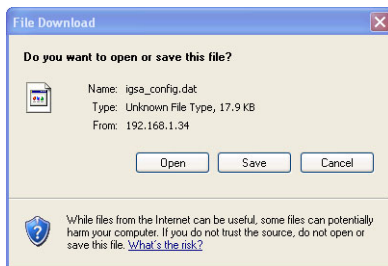


FIGURE 13-3. Administration > Configuration Backup

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 13-4. 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**.

Control Manager Settings

TREND MICRO™ InterScan Gateway Security Appliance	
Summary	Control Manager Settings  Configure the communication between IGSA MCP Agent and the Control Manager server. Connection Status Registered Control Manager server: Last heartbeat: 01/22/2007 18:09:44 Unregister Connection Settings Entity display name: IGSA  Control Manager Server Settings Server FQDN or IP address: Port: ☒ Connect using HTTPS Web server authentication:  Username: Password: ***** MCP Proxy Settings ☐ Use a proxy server for communication with the Control Manager server Proxy protocol: ☒ HTTP ☐ SOCKS4 ☐ SOCKS5 Server FQDN or IP address: Port: Proxy server authentication: User ID: Password: ***** Two-way Communication Port Forwarding ☐ Enable two-way communication port forwarding  IP address: Port: 443 Update Settings Test Connection Cancel
▶ SMTP	
▶ HTTP	
▶ FTP	
▶ POP3	
▶ Outbreak Defense	
▶ Quarantines	
▶ Update	
▶ Logs	
▼ Administration	
Access Control	
Configuration Backup	
Control Manager Settings	
Disk SMART Test	
Firmware Update	
IP Address Settings	
Notification Settings	
Operation Mode	
Password	
Product License	
Proxy Settings	
SNMP Settings	
System Time	
Reboot	
World Virus Tracking	

You can manage multiple InterScan Gateway Security Appliances with Trend Micro Control Manager (sold separately). Control Manager provides aggregate reporting for all managed InterScan Gateway Security Appliances with several new, useful templates.

You must first have the Control Manager product installed and activated in order to add InterScan Gateway Security Appliance as a managed item on a Control Manager

server. For detailed information on how to use Control Manager, see the Trend Micro Control Manager documentation that came with your purchase of Trend Micro Control Manager.

In order to manage InterScan Gateway Security Appliance with TMCM, first register each InterScan Gateway Security Appliance to a TMCM server. The Control Manager Settings screen of the Web changes appearance based on whether InterScan Gateway Security Appliance is registered to a Control Manager server.

Registering InterScan Gateway Security Appliance to Control Manager

InterScan Gateway Security Appliance is a standalone product and you do not need to register the device to Control Manager. However, by registering to Control Manager you gain the benefits mentioned above. All features are managed using the InterScan

Gateway Security Appliance Web console. Before registering InterScan Gateway Security Appliance to a Control Manager server, ensure that both the device and the Control Manager server belong to the same network segment.

To register an InterScan Gateway Security Appliance to a TMCM server:

1. Select **Administration > Control Manager Settings**. The Control Manager Settings screen appears.
2. To verify that the device is not registered to Control Manager, look at the status entry in the Connection Status section. When InterScan Gateway Security Appliance is not registered to Control Manager, the words **Not registered** appear in red.
3. In the Connection Settings section, type the name to display within Control Manager in the **Entity display name** field to identify InterScan Gateway Security Appliance that you are registering. (a required field)

Note: Control Manager uses the name specified in the **Entity display name** field to identify InterScan Gateway Security Appliances. The entity display name appears in the Product Directory of Control Manager.

4. In the Control Manager Server Settings section, type the IP address or FQDN (fully qualified domain name) in the **FQDN or IP address** field. (a required field)
5. Type the port number to use in the **Port** field.
6. If the Web server that serves the Control Manager Web console requires authentication, type the user name and password in the Web server authentication section. Otherwise, leave this section blank.
7. If there is a proxy server between your appliance and the Control Manager server, select the **Use a proxy server for communication with the Control Manager server** check box in the Proxy Settings section. The Proxy protocol options become editable.
 - a. Select the Proxy protocol to use.
 - b. Type the **Server FQDN or IP address** of the proxy server and the Port that it uses.
 - c. If the proxy server uses authentication, type the **User ID** and **Password**.
8. If your InterScan Gateway Security Appliance resides behind an NAT (Network Address Translation) device, select the **Enable two-way communication port forwarding** check box. The **IP address** and **Port** fields become editable.
 - a. Type the IP address of your router or NAT server in the **Port forwarding IP address** field.
 - b. Type the port to forward in the **Port** field.

Note: If the InterScan Gateway Security Appliance M-Series is behind an NAT device, it can use the Port forwarding IP address and Port forwarding port number for two-way communication with Control Manager. Otherwise, port forwarding is not necessary.

9. Click **Test Connection** to verify that your appliance can connect to the Control Manager server.
10. Click **Register**. A progress bar displays the progress of the registration process and when registration is complete, the Control Manager Settings screen changes appearance to reflect the registered status.

To verify that InterScan Gateway Security Appliance has successfully registered to Control Manager:

1. From the Control Manager management console Main Menu, click **Products**.
2. On the leftmost menu, select Managed Products from the list and then click **Go**.
3. Check to see that an icon for InterScan Gateway Security Appliance displays in the product directory.

For more detailed guidance on using InterScan Gateway Security Appliance with Trend Micro Control Manager, see [Appendix B. Introducing Trend Micro Control Manager™](#).

Disk SMART Test



FIGURE 13-5. 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**.

Firmware Update

You can update the program file (device image) of InterScan Gateway Security Appliance through the Web console.

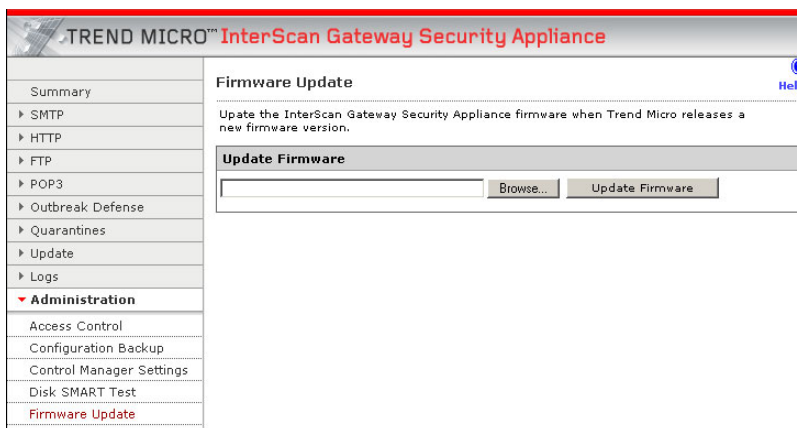


FIGURE 13-6. The Web console Firmware Update screen

To update the device image through the Web console:

1. Obtain the new firmware file in one of two ways:
 - Download the latest firmware from the InterScan Gateway Security Appliance section of the Trend Micro Update Center:
<http://www.trendmicro.com/download/product.asp?productid=73>
 - Insert the InterScan Gateway Security Appliance Solutions Disc containing the new firmware into your CD-ROM drive.
2. Click **Administration > Firmware Update**. The Firmware Update screen appears.

3. Click **Browse**. A navigation window opens.
4. Locate and click the new image file. It will have a file name similar to: `phoenix_image.1.1.1073.en_US.R`. The file name of the new firmware appears in the Browse field.
5. Click **Update Firmware**. A countdown screen appears and counts down from 3 minutes while the appliance is updating its firmware. When the appliance has rebooted, the Web console login screen appears.

Note: This firmware update method enables updating to a new program file while keeping current configuration. For other firmware update alternatives, see *[Updating the Device Image Using the AFFU](#)* on page 15-4.

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.

InterScan Gateway Security Appliance uses the IP address when checking for component and firmware updates. On this screen you can choose either:

- **Dynamic IP address (DHCP)**
- **Static IP address**

Managing IP Address Settings

The screenshot displays the Trend Micro InterScan Gateway Security Appliance web interface. On the left, a navigation menu includes options like Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, and Administration. The Administration section is expanded, showing sub-items like Access Control, Configuration Backup, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings (highlighted), Notification Settings, Operation Mode, Password, Product License, and Proxy Settings. The main content area is titled 'IP Address Settings' and features two tabs: 'Management IP Address' (active) and 'Static Routes'. Under the Management IP Address tab, there is a 'Host Name' field with the placeholder text 'Your Appliance Name'. Below this, the 'IP Address Management' section has two radio button options: 'Dynamic IP address (DHCP)' (selected) and 'Static IP address'. The Dynamic option includes fields for IP Address, Netmask, Gateway, DNS Server 1, and DNS Server 2. The Static option also includes fields for IP Address, Netmask, Gateway, DNS Server 1, and DNS Server 2. At the bottom of the form are 'Save' and 'Cancel' buttons.

FIGURE 13-7. 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 IP Address Settings screen opens, displaying the Management IP Address tab.
2. Type a host name in the **Hostname** field.
This is the network name of the InterScan Gateway Security Appliance. Some mail servers require a host name to accept incoming mail.
3. Select **Dynamic IP address (DHCP)** to use the recommended setting.
4. To use a static IP address, select **Static IP address** and type the following information:
 - **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

5. Click **Save**.

Static Routes

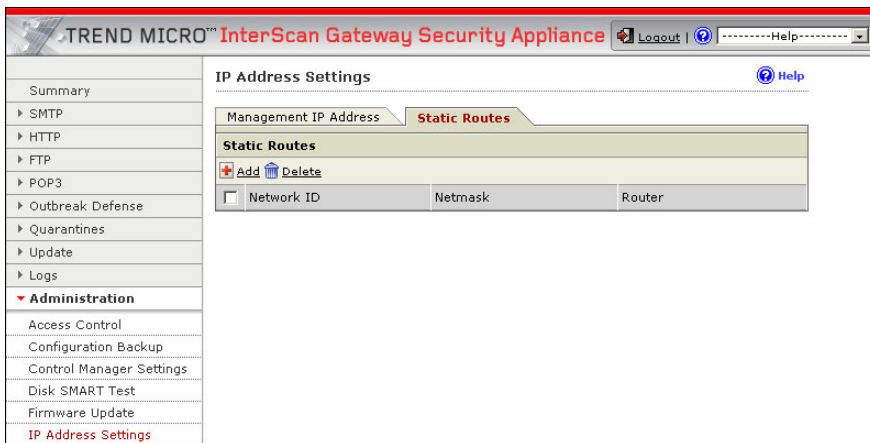


FIGURE 13-8. Administration > IP Address Settings – Static Routes

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 13-9. 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.

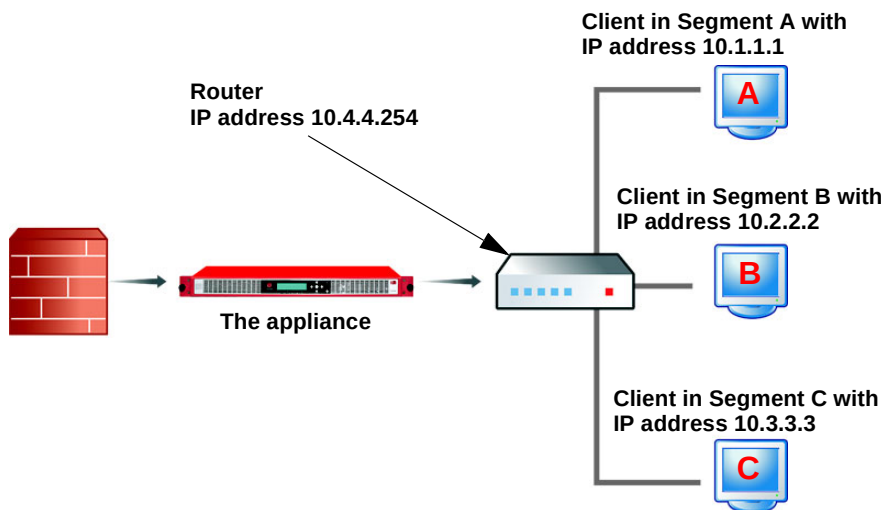


FIGURE 13-10. Static Routes – Multiple Segment Network

TABLE 13-1. 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' web interface. The top navigation bar includes 'Logout' and 'Help' links. The left sidebar contains a tree view of settings categories: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, Administration (expanded), Access Control, Configuration Backup, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, and Notification Settings (selected). The main content area is titled 'Notification' and has a 'Help' link. It features two tabs: 'Settings' (active) and 'Events'. The 'Settings' tab contains the following information:

The following settings will be used when sending email notifications from InterScan Gateway Security Appliance.

SMTP server:

Port:

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

At the bottom of the form are 'Save' and 'Cancel' buttons.

FIGURE 13-11. 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 addresses.
7. Click **Save**.

Events

The screenshot shows the web interface of a Trend Micro InterScan Gateway Security Appliance. The left-hand navigation menu is expanded to the 'Administration' section, which includes options like Access Control, Configuration Backup, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, Notification Settings (highlighted), and Operation Mode. The main content area is titled 'Notification' and contains two tabs: 'Settings' and 'Events' (which is selected). Under the 'Events' tab, there is a text input field labeled 'Maximum notifications per hour:' with the value '50' entered. To the right of the input field is the text '(0: no limit)'. Below the input field are two buttons: 'Save' and 'Cancel'. The top of the interface shows the appliance name, a 'Logout' link, and a 'Help' link.

FIGURE 13-12. 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

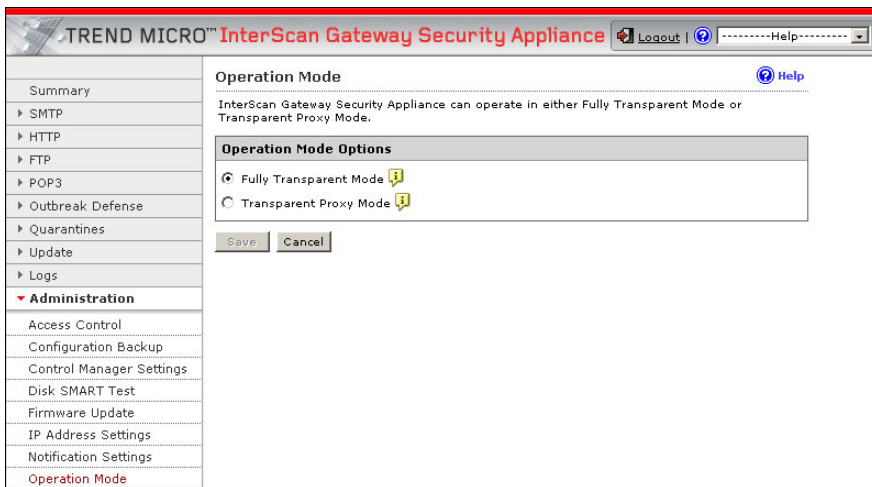


FIGURE 13-13. Administration > Operation Mode

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 Proxy 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

The screenshot shows the 'TREND MICRO™ InterScan Gateway Security Appliance' web interface. The top navigation bar includes 'Logout' and a 'Help' dropdown menu. The left sidebar lists various administrative functions, with 'Administration' expanded to show sub-options like 'Access Control', 'Configuration Backup', 'Control Manager Settings', 'Disk SMART Test', 'Firmware Update', 'IP Address Settings', 'Notification Settings', 'Operation Mode', and 'Password'. The main content area is titled 'Change Password' and features three input fields for 'Old password:', 'New password:', and 'Confirm password:'. A note below the fields states: 'Note: Passwords must be between 4-32 alphanumeric characters.' At the bottom of the form are 'Save' and 'Cancel' buttons.

FIGURE 13-14. 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

The screenshot shows the web console interface for the Trend Micro InterScan Gateway Security Appliance. The left-hand navigation menu is expanded to show the 'Administration' section, which includes options like Access Control, Configuration Backup, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, Notification Settings, Operation Mode, Password, Product License (highlighted), and Proxy Settings. The main content area is titled 'Product License' and features a green checkmark icon with the message 'The InterScan Gateway Security Appliance is valid.' and a link to 'View renewal instructions'. Below this, a yellow box displays 'License information last updated on: 02/01/2007' with an 'Update Information' button. A 'License Information' table follows, showing 'Status: Activated', 'Model: N/A', 'License expires on: 10/15/2007', and 'Activation code: [redacted]'. A 'New Activation Code' button is located at the bottom right of the table. The top of the console shows the 'TREND MICRO™ InterScan Gateway Security Appliance' header, a 'Logout' button, and a help dropdown menu.

License Information	
Status:	Activated
Model:	N/A
License expires on:	10/15/2007
Activation code:	[redacted]

FIGURE 13-15. 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.

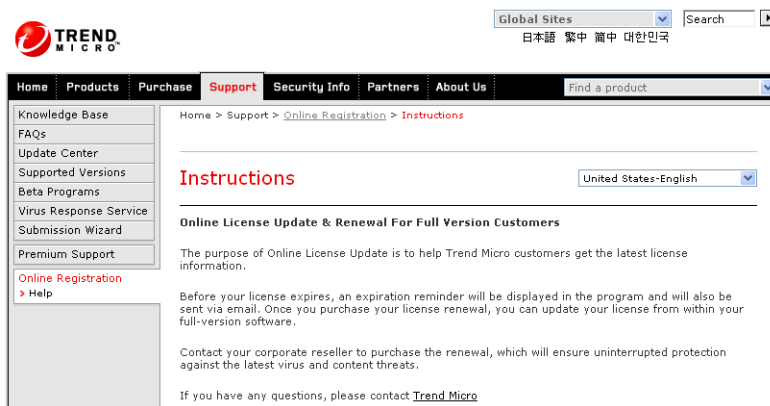


FIGURE 13-16. Online License Update & Renewal

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.

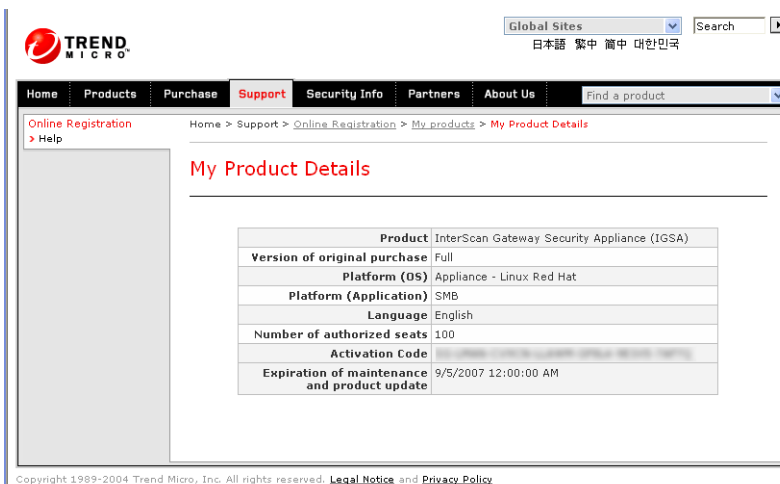


FIGURE 13-17. My Product Details

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 web interface of a 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 administrative functions, with 'Administration' expanded and 'Product License' highlighted. The main content area is titled 'Product License' and includes a 'Help' link. Below the title, there is a breadcrumb trail 'Product License > New Activation Code' and a paragraph explaining that users should register online using the product's registration key. A 'New Activation Code' form is displayed, containing fields for 'Product' (InterScan Gateway Security Appliance), 'Current status' (Activated), 'Current activation code' (a blurred code), and 'New activation code' (an empty input field). At the bottom of the form are 'Save' and 'Cancel' buttons.

FIGURE 13-18. 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 Trend Micro InterScan Gateway Security Appliance Administration web interface. 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, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, Notification Settings, Operation Mode, Password, Product License, and Proxy Settings (highlighted in red). 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:
-
-

FIGURE 13-19. 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 'SNMP Settings' page within the Trend Micro InterScan Gateway Security Appliance Administration interface. 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, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, Notification Settings, Operation Mode, Password, Product License, Proxy Settings, SNMP Settings (highlighted in red), System Time, Reboot, and World Virus Tracking. The main content area is titled 'SNMP Settings' and includes a 'Help' icon. It is divided into three sections: 'SNMP Trap', 'SNMP Agent', and 'Accepted Community Names'. The 'SNMP Trap' section has a checked 'Enable SNMP trap' checkbox, a 'Community name' text field, and a 'Server IP address' text field. The 'SNMP Agent' section has a checked 'Enable SNMP agent' checkbox, a 'System location' text field, and a 'System contact' text field. The 'Accepted Community Names' section features a 'Community name' text field, an 'Add >>' button, and a table with a header 'Community Name' and a single row containing 'None'. Below this is the 'Trusted Network Management IP Address(es)' section, which includes an 'IP address' text field, an 'Add >>' button, and a table with a header 'IP Address' and a single row containing 'None'. At the bottom of the page are 'Save' and 'cancel' buttons.

TREND MICRO™ InterScan Gateway Security Appliance Logout | ?

SNMP Settings Help

SNMP Trap

☒ Enable SNMP trap

Community name:

Server IP address:

SNMP Agent

☒ Enable SNMP agent

System location:

System contact:

Accepted Community Names

Community name: Add >>

Community Name
None

Trusted Network Management IP Address(es)

IP address: Add >>

IP Address
None

Save cancel

FIGURE 13-20. 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

On the Administration > System Time screen, you can:

- View current date and time on the appliance
- Manually change the date and time settings
- Configure the appliance to access a particular Network Time Protocol (NTP) server
- Modify the regional settings to match your region/country

TREND MICRO™ InterScan Gateway Security Appliance

System Time Settings [Help](#)

Synchronize InterScan Gateway Security Appliance with an NTP (Network Time Protocol) server.

Current Date and Time on the Device

Refresh to obtain current date and time on the appliance. If the appliance date and time do not reflect current time zone, check your NTP server connection.

01/22/2007 18:08:50 [Refresh](#)

NTP Setting

To synchronize the appliance with an NTP server, ensure that the appliance is connected to the Internet.

NTP server: [Synchronize Now](#)

Time zone:

Manual Date and Time Setting

The appliance uses the manual date and time setting only if it cannot contact the NTP server. If no NTP server is available, enter date and time settings manually.

mm/dd/yyyy hh mm ss

Regional Setting

Region/Country:

[Save](#) [Cancel](#)

FIGURE 13-21. Administration > System Time

You can configure system time in two ways:

- Manually
- By designating an NTP server for the appliance to synchronize with

Note: If you set both manual and automatic (NTP) settings, the NTP setting takes precedence.

To configure system time manually:

1. From the left-side menu, click **Administration > System Time**. The System Time Settings screen appears.
2. In the Date and Time Setting section, type the current date (in mm/dd/yyyy format) or click the calendar icon to select the date with your mouse pointer.
3. Use the drop-down menus to select hours, minutes, and seconds.
4. Click **Save**. The appliance adjusts its system time to the time and date that you typed.

To configure system time automatically:

1. From the left-side menu, click **Administration > System Time**. The System Time Settings screen appears.
2. In the NTP Setting section, type the domain name or IP address of an NTP server in the **NTP Server** field.
3. Select your time zone from the **Time zone** drop-down menu.
4. Click **Synchronize Now**. The appliance contacts the designated NTP server and synchronizes with it.
5. Select a Region/Country from the **Region/Country** drop-down menu.
6. Click **Save**.

Reboot from Web Console

In this release of InterScan Gateway Security Appliance, you can reboot the appliance directly from the Web console.



FIGURE 13-22. Reboot screen

Note: The Reboot item in the left-side menu is far down the screen under Administration, the second from the bottom. (See Figure 13-23, “Administration > Reboot menu,” on page 30)

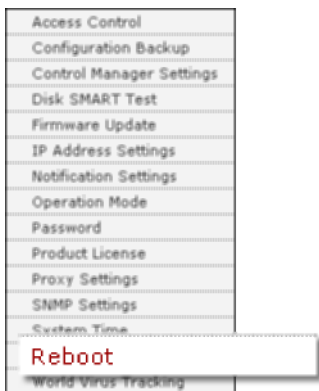


FIGURE 13-23. Administration > Reboot menu

To reboot the appliance from the Web console:

1. On the left-side menu, click **Administration > Reboot**. The Reboot screen appears.
2. Click **Reboot Now**. The appliance reboots.

World Virus Tracking

The screenshot shows the Trend Micro InterScan Gateway Security Appliance administration interface. On the left is a navigation menu with the following items: Summary, SMTP, HTTP, FTP, POP3, Outbreak Defense, Quarantines, Update, Logs, **Administration** (expanded), Access Control, Configuration Backup, Control Manager Settings, Disk SMART Test, Firmware Update, IP Address Settings, Notification Settings, Operation Mode, Password, Product License, Proxy Settings, SNMP Settings, System Time, Reboot, and World Virus Tracking (highlighted in red). The main content area is titled "World Virus Tracking Program" and includes a "Help" link. The text explains that Trend Micro consolidates virus-scanning results from customers worldwide and displays them on the Virus Map. It provides two options: "Yes, I would like to join the World Virus Tracking Program..." (selected with a radio button) and "No, I don't want to participate." (unselected). A note states that sample data is sent to TrendLabs. At the bottom are "Save" and "Cancel" buttons.

FIGURE 13-24. Administration > World Virus Tracking

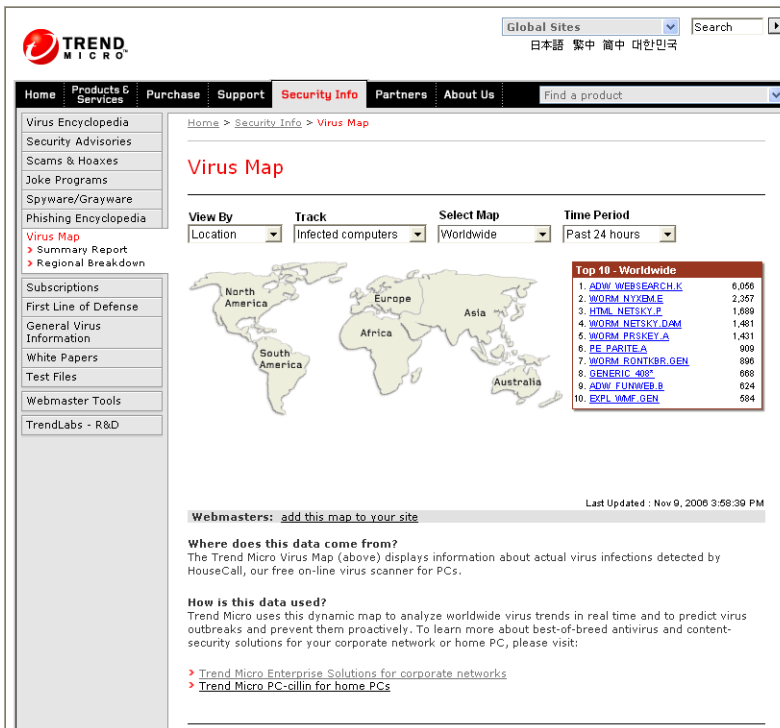
The Trend Micro World Virus Tracking Program collects Internet threat data from tens of thousands of corporate and individual computer systems around the world.

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 13-25. 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, and FAQs

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 14-2
- *Troubleshooting* on page 14-4
- *Frequently Asked Questions (FAQ)* on page 14-7
- *Recovering a Password* on page 14-8
- *Virus Pattern File* on page 14-9
- *Spam Engine and Pattern File* on page 14-10
- *Hot Fixes, Patches, and Service Packs* on page 14-10
- *Licenses* on page 14-11
- *Renewing Maintenance* on page 14-12
- *EICAR Test Virus* on page 14-13
- *Best Practices* on page 14-14

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 file (readme.txt) provided. Trend Micro readme files cover the following 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

Why Is the Summary Screen not Logging Any Events? Why Aren't Any Logs Being Created?

Cause—The appliance requires hard disk initialization and reformat. It is necessary to re-initialize the hard disk under the following conditions:

- When upgrading InterScan Gateway Security Appliance to the latest build version
- When the Hard Disk LED in the front panel of the appliance is red, indicating that the hard disk failed and the unit is already operating in diskless mode

Solution—Follow the procedure below.

To initialize the hard disk:

1. Log on the appliance Preconfiguration console. (See *Interfacing with the Preconfiguration Console for Device Image Updates* on page 15-9.)
2. Select option **4) System Tools** from the Main Menu.
3. On the System Tasks menu, select option **1) Hard Disk Initialization**. The Hard Disk Initialization screen appears, displaying the current status of the hard disk.
4. Press any key. The appliance asks for confirmation.
5. Select **OK**. The appliance removes the contents of the original partition and then reboots.
6. After the appliance has rebooted, repeat steps 1 through 3 above to format the hard disk. The appliance formats the hard disk and then displays the following message:

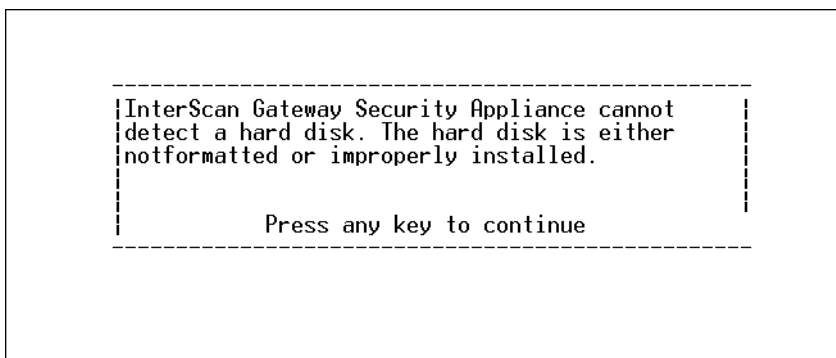


FIGURE 14-1. Preconfiguration console output screen when initializing a hard disk that is not formatted or is improperly installed (the second part of the re-initialization process)

7. Press any key. The appliance formats the hard disk and displays the following screen when the formatting is complete:

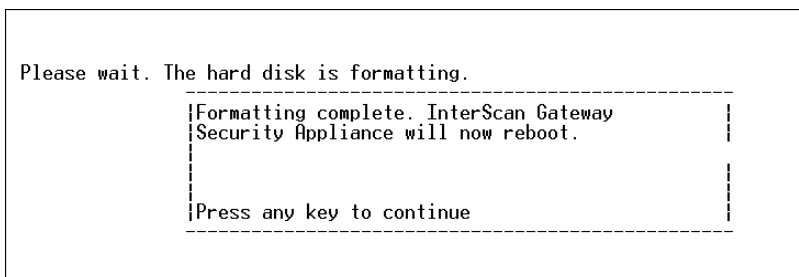


FIGURE 14-2. Preconfiguration console output screen when the appliance has finished formatting the hard disk

8. Press any key. The appliance reboots. The hard disk is ready when the Hard Disk LED in the appliance front panel turns green.

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 5 seconds.** The switch is designed to function in this way to prevent 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** 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 the **DELETE** key. Enable **DC OFF LAN Bypass**. Doing so will allow traffic to pass through the device when there is no direct current. By default, both **DC ON LAN Bypass** and **DC OFF LAN Bypass** are enabled.

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:

- From a backup
- 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 telltale 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.

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 License 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 Agreement 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, 90 days before Maintenance expires, you will start to receive email notifications, alerting you of the pending discontinuation. You can update your Maintenance 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 expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance 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 1,000 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 five 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	71,599	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	148,460	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	1,236	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	433,726	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 14-3. 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 InterScan Gateway Security Appliance program file (device image), the BMC (baseboard management controller) firmware, and the BIOS firmware.

This chapter includes the following topics:

- *Updating the Device Image Using the AFFU* on page 15-4
- *Preparing InterScan Gateway Security Appliance for the Device Image Update* on page 15-4
- *Uploading the New Device Image* on page 15-14
- *Completing the Process After the Device Image Is Uploaded* on page 15-29
- *Updating the Appliance BMC Firmware* on page 15-32
- *Updating the InterScan Gateway Security Appliance BIOS Firmware* on page 15-40

Identifying the Procedures to Follow

There are two main ways to update the InterScan Gateway Security Appliance program file (device image). If you want to update the device image and retain the existing configuration, use the procedure described in [Updating the Device Image Through the Web Console](#) on page 15-3.

If you want to update the device image and restore settings to system defaults, do so using the Trend Micro Appliance Firmware Flash Utility (AFFU).

Consult the table below to determine which instructions to follow for updating firmware, based on what kind of update you want to do.

Type of Update	Tool to Use	Follow These Instructions
Program file, keeping existing configuration	InterScan Gateway Security Appliance Web Console	Updating the Device Image Through the Web Console on page 15-3
Program file, restoring default settings	Appliance Firmware Flash Utility (AFFU)	Uploading with the Restored, Default Configuration (Option 5) on page 15-21
BMC (baseboard management controller) firmware	AFFU	Updating the Appliance BMC Firmware on page 15-32
BIOS firmware	AFFU	Updating the InterScan Gateway Security Appliance BIOS Firmware on page 15-40
Revert to previous firmware	Preconfiguration console	Reverting to the Previous Version of the Program File on page 15-30

Updating the Device Image Through the Web Console

If you want to update the InterScan Gateway Security Appliance program file (device image) and keep the existing configuration, you can easily do it through the appliance Web console. The entire process takes three minutes or less.

To update the device image through the Web console:

1. Obtain the new firmware file in one of two ways:
 - Download the latest firmware from the InterScan Gateway Security Appliance section of the Trend Micro Update Center:
<http://www.trendmicro.com/download/product.asp?productid=73>
 - Insert the InterScan Gateway Security Appliance Solutions Disc containing the new firmware into your CD-ROM drive.
2. Click **Administration > Firmware Update**. The Firmware Update screen appears.
3. Click **Browse**. A navigation window opens.
4. Locate and click the new image file. It will have a file name similar to: `phoenix_image.1.1.1073.en_US.R`. The file name of the new firmware appears in the Browse field.
5. Click **Update Firmware**. A countdown screen appears and counts down from 3 minutes while the appliance is updating its firmware. When the appliance has rebooted, the Web console login screen appears.

Updating the Device Image Using the AFFU

Use the Trend Micro Appliance Firmware Flash Utility (AFFU) to update the program file (device image) and restore the default configuration. You can also use the AFFU to update the firmware and keep current configuration, but doing so is much more complicated than doing it through the Web console. The only reason to use the more complex method would be to ensure that you have the ability to restore the previous configuration through the Preconfiguration console.

Tip: Trend Micro recommends updating the program file through the Web console unless you have a compelling need to maintain the "restore previous configuration" feature.

Preparing InterScan Gateway Security Appliance for the Device Image Update

Before updating the InterScan Gateway Security 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 enables you to configure or view basic (that is, "preconfiguration" settings). 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

Access the Preconfiguration console by physically connecting the serial port on a local computer to the nine-pin serial port on the back of the appliance.

See [Interfacing with the Preconfiguration Console for Device Image Updates](#) on page 15-9 for instructions on accessing the Preconfiguration console.

The Preconfiguration console enables basic preconfiguration of appliance settings. Some, limited preconfiguration is possible through the appliance LCD module.

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:

- ☐ **Back up your configuration** (unless you have not yet configured anything)
(See [Backing Up Your Configuration](#) on page 15-6)
- ☐ **Get the appliance device image file** (See [Getting the Appliance Device Image from the Trend Micro Web site](#) on page 15-7)
- ☐ **Connect the appliance to a local computer** (See [Connecting a Local Computer to the Appliance to Deliver the Update](#) on page 15-7)
- ☐ **Log in to the appliance using terminal software such as HyperTerminal** (See [Interfacing with the Preconfiguration Console for Device Image Updates](#) on page 15-9)
- ☐ **Verify that the local computer IP address matches that of the appliance** (See [Getting the IP Address of the Local PC](#) on page 15-12)
- ☐ **Put the appliance into rescue mode** (See [Putting the Appliance into Rescue Mode](#) on page 15-13)

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 the 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 15-15
- 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 15-21

To connect the local computer to the appliance:

1. Connect an Ethernet cable to the appliance 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 local computer.

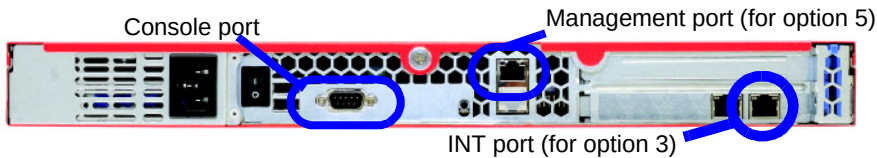


FIGURE 15-1. Back panel of appliance showing console port, management port, and INT port

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 appliance BMC (baseboard management controller) respectively. (See [Getting the IP Address of the Local PC](#) on page 15-12.)
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 15-12.)
4. Connect a serial (RS 232) cable from the local computer to the serial port on the back panel of the appliance. (See figure 15-1 on page 8 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 15-1, *Back panel of 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 terminal emulation to VT100J, as shown below.

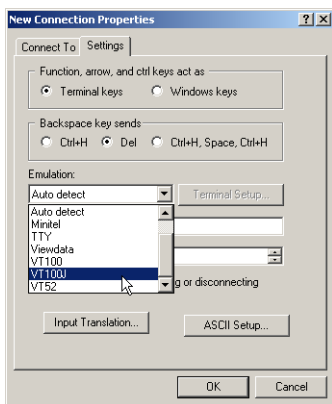


FIGURE 15-2. HyperTerminal display settings

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 15-3. 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.
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

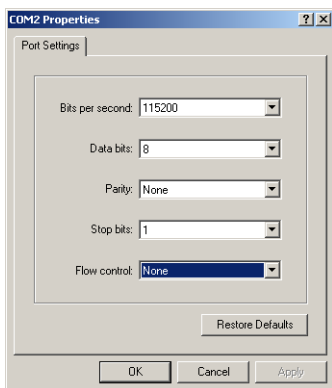


FIGURE 15-4. HyperTerminal COM Properties screen

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.

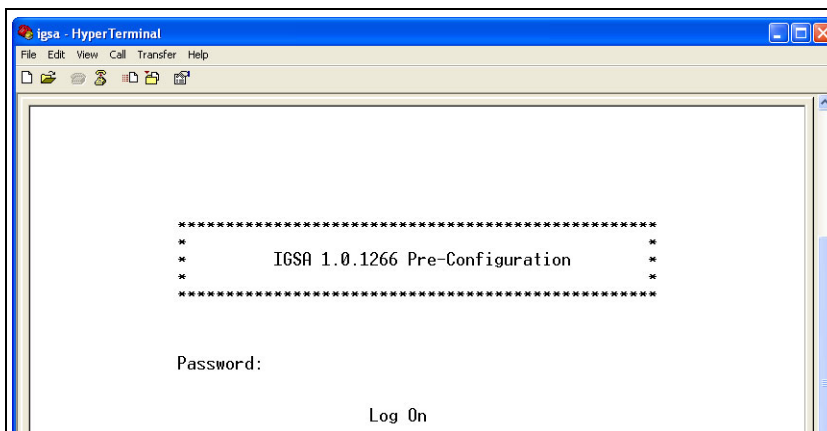


FIGURE 15-5. The appliance Preconfiguration console login screen

8. Press **ENTER** again. The appliance Preconfiguration console Main Menu appears, as shown below.

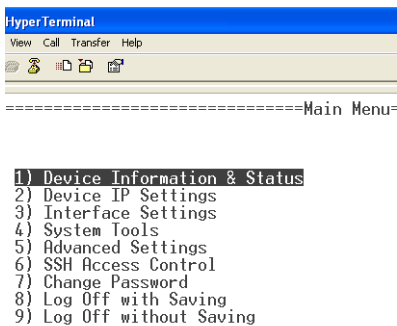


FIGURE 15-6. The appliance Preconfiguration console main menu, accessed via HyperTerminal

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.

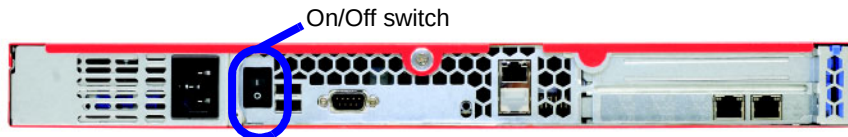


FIGURE 15-7. The appliance back panel showing on/off switch

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 five 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.

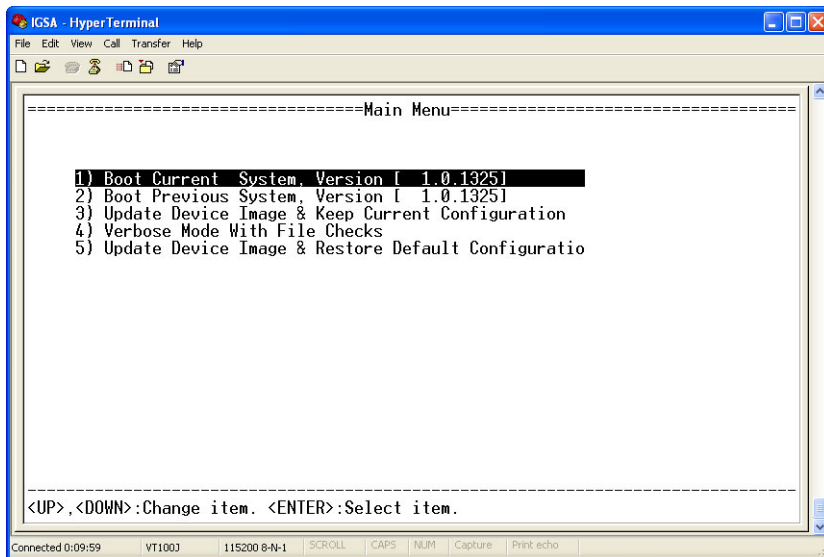


FIGURE 15-8. The appliance rescue mode main menu

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:

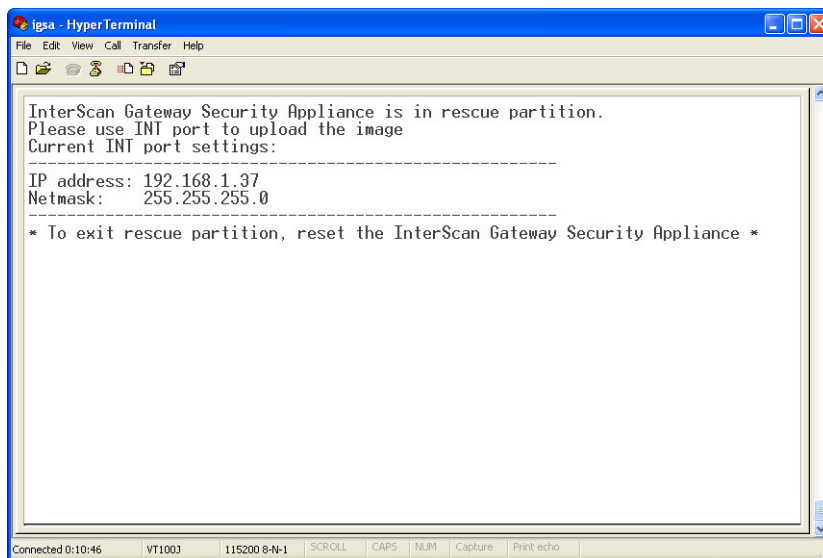


FIGURE 15-9. Preconfiguration console screen that appears when you select option 3 in rescue mode

2. Connect an RJ45 Ethernet cable from your local computer to the **INT** port of the appliance, as shown below.



FIGURE 15-10. 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 15-16.

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 15-9, [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 appliance Solutions CD into the local computer. The following screen appears:

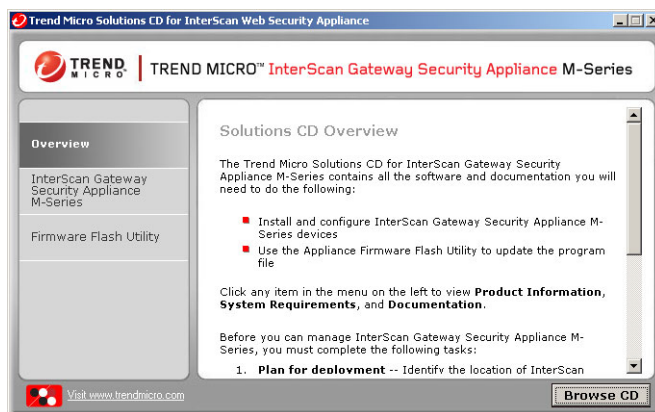


FIGURE 15-11. The appliance Solutions CD splash screen

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:

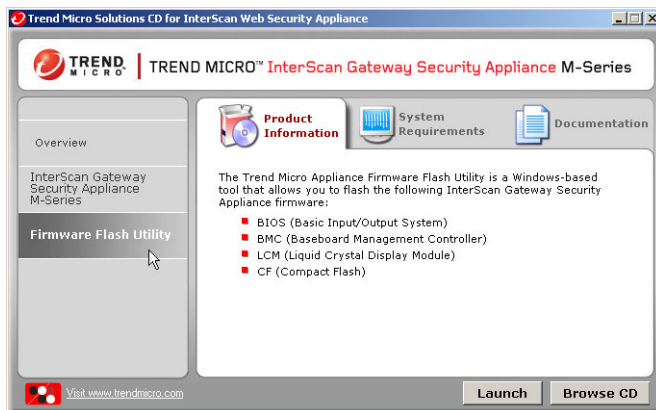


FIGURE 15-12. The appliance Solutions CD Firmware Flash Utility section

3. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

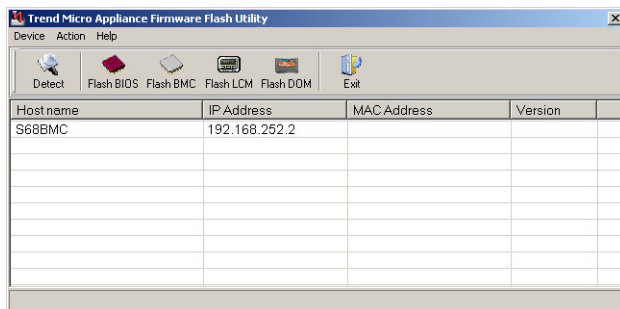


FIGURE 15-13. Trend Micro Appliance Firmware Flash Utility, opening screen, when uploading with option 3

4. Click **Flash DOM** (disk-on-module), as shown below.

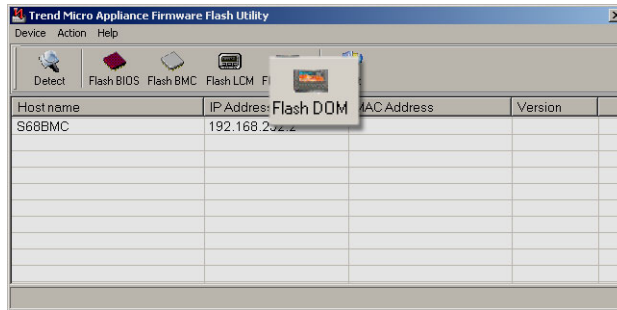


FIGURE 15-14. AFFU opening screen when uploading with option 3, emphasizing Flash DOM

5. After you click **Flash DOM**, the Appliance Firmware Flash Utility - DOM screen appears, as shown below.

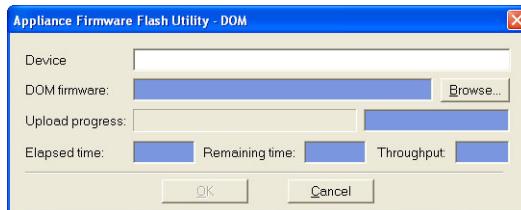


FIGURE 15-15. AFFU DOM screen

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 in the file navigation screen that opens, as shown below.

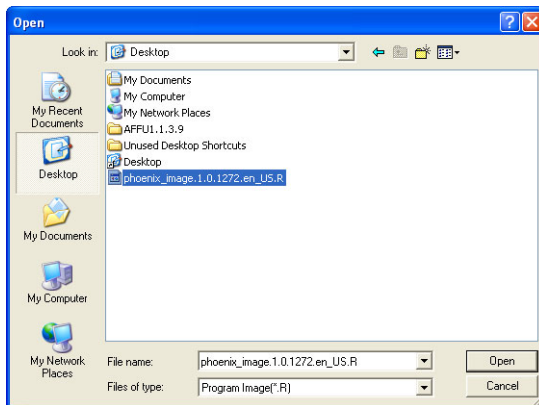


FIGURE 15-16. AFFU - browse to device image

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.

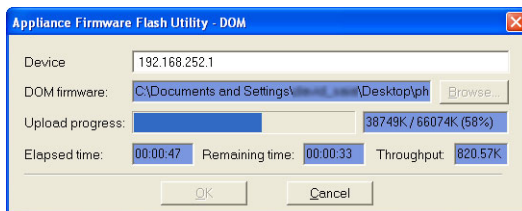


FIGURE 15-17. AFFU DOM screen showing progress of the update

When the update is complete, the AFFU displays a message stating that the device image uploaded successfully.

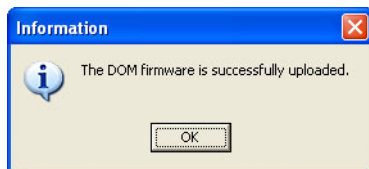


FIGURE 15-18. AFFU “flash DOM successfully uploaded” message

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 15-10, “The appliance back panel showing location of internal (INT) port,” on page 16).
- 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:

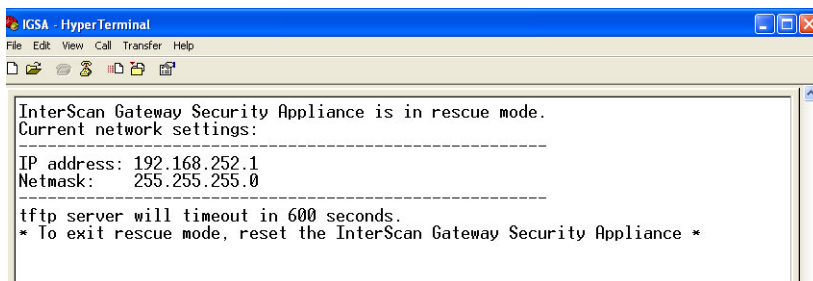


FIGURE 15-19. Preconfiguration console screen that appears when you select option 5 in rescue mode

2. Connect an RJ45 Ethernet cable from your local computer to the Management port of the appliance, as shown below.



FIGURE 15-20. The 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 15-23.

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 15-19, *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 15-12).

To upload the device image update using the Appliance Firmware Flash Utility:

1. Put the appliance Solutions CD into the local computer. The following screen appears:

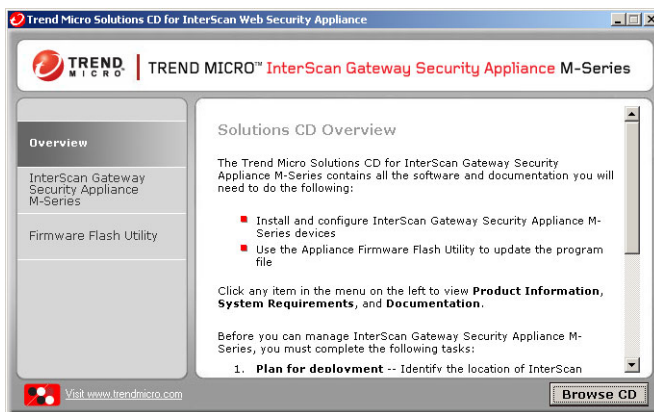


FIGURE 15-21. The appliance Solutions CD splash screen

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:

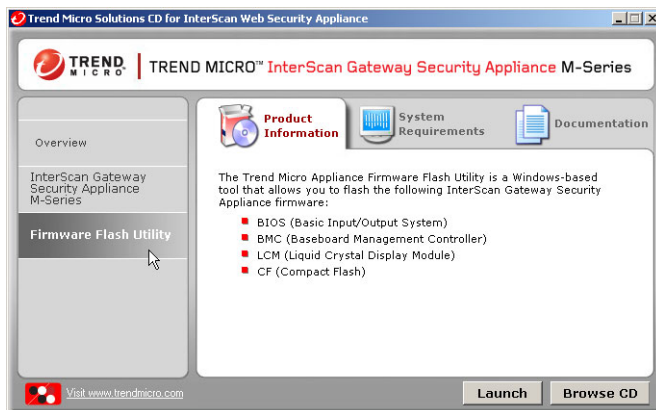


FIGURE 15-22. The appliance Solutions CD Firmware Flash Utility section

3. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

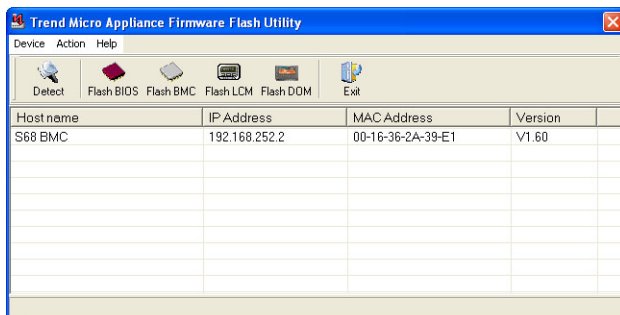


FIGURE 15-23. Trend Micro Appliance Firmware Flash Utility, opening screen when using option 5

4. Click **Flash DOM** (disk-on-module), as shown below.

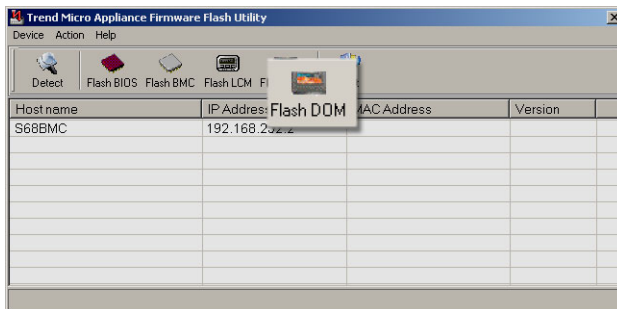


FIGURE 15-24. AFFU opening screen when using option 5, emphasizing Flash DOM

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's 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.

Do not click the row displaying the IP address. That is, do not do the following:

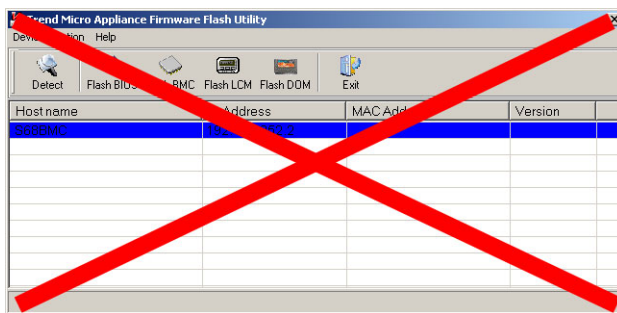


FIGURE 15-25. AFFU - Do not click the row displaying the IP address

5. After you click **Flash DOM**, the Appliance Firmware Flash Utility - DOM screen appears, as shown below.

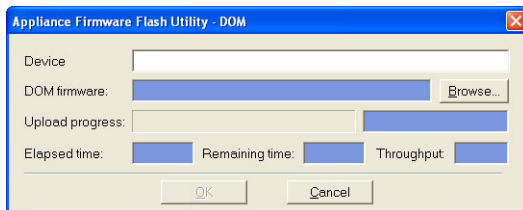


FIGURE 15-26. AFFU DOM screen

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.

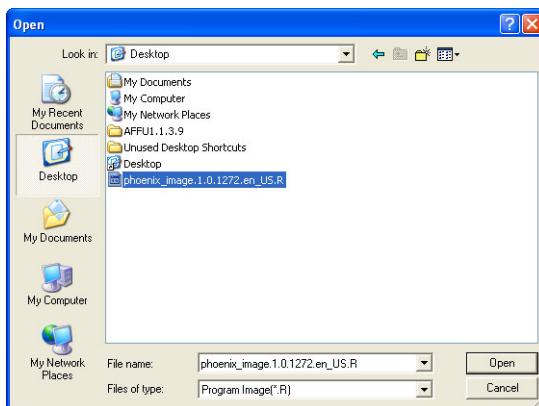


FIGURE 15-27. AFFU - browse to device image file

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.

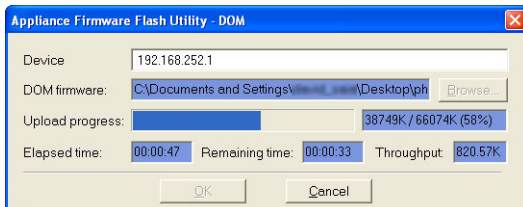


FIGURE 15-28. AFFU DOM screen showing progress of the update

When the update is complete, the AFFU displays a message stating that the device image uploaded successfully.

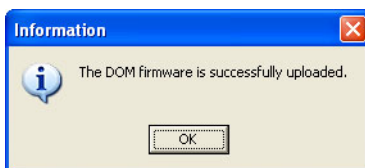


FIGURE 15-29. AFFU “flash DOM successfully uploaded” message

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 15-20, “The appliance back panel showing location of management port,” on page 22.)
- 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 Preconfiguration rescue mode console. (See [Putting the Appliance into Rescue Mode](#) on page 15-13.)

- 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.)

Tip: Many personal firewalls block UDP traffic by default. TFTP uses UDP, so if the local computer you are using has a personal firewall or a local client for a companywide antivirus application, temporarily modify the settings on the local computer to either allow UDP traffic or to allow such traffic from the IP address of the local computer.

Note: It can take two or three minutes for the appliance to finish updating its device image.

lgsa - HyperTerminal

File Edit View Call Transfer Help

Transmission done.
 Image size is 67660161.
 File size of kernel is 796481.
 File size of initrd is 66863660.
 [2142.777670] Starting new kernel

=====
 - Format System Partitions -
 =====
 - Copy System Data -
 =====
_

Connected 0:45:37 VT1003 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

15-29

After the appliance has rebooted, confirm that the appliance 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.

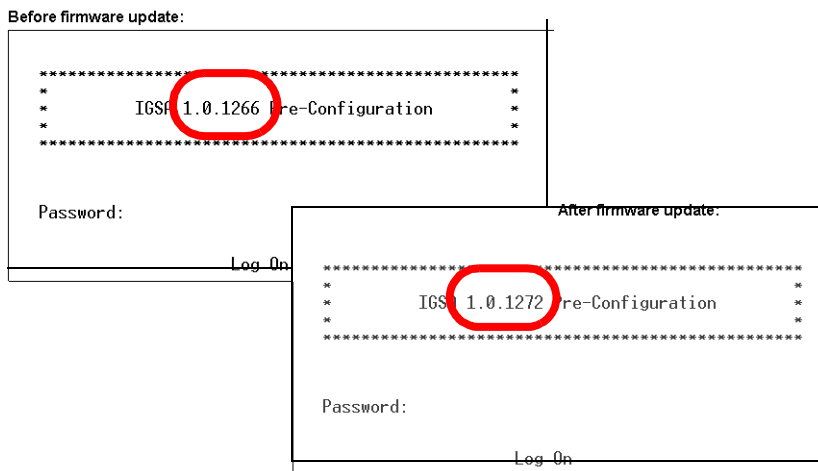


FIGURE 15-31. The appliance preconfiguration console login screens, before and after device image update

Reverting to the Previous Version of the Program File

InterScan Gateway Security Appliance includes a feature by which you can revert to the previous version of the firmware (program file). If for some reason you need to step back to the previous firmware that the appliance was using, you can do so by using the appliance Preconfiguration console.

To revert to the previously installed firmware version:

1. Before beginning, make a note of the build number of the currently installed firmware. You can locate this information by doing one of the following:
 - On the Web console, from the drop-down Help menu on the right side of the top banner, select **About** (the bottom-most item). The About InterScan Gateway Security Appliance pop-up window appears, displaying the release number and build number.
 - Access the Preconfiguration console (as shown in [Interfacing with the Preconfiguration Console for Device Image Updates](#) on page 15-9). The release number and build number are displayed in the middle of the login screen.
2. Follow the procedures for connecting a local computer to the appliance and getting into Rescue mode, as described in [Preparing InterScan Gateway Security Appliance for the Device Image Update](#) starting on page 15-4 and [Putting the Appliance into Rescue Mode](#) starting on page 15-13. The Rescue mode main menu appears, displaying options 1 and 2 with the current and previously installed versions of the program file, as shown in the figure below.

```

=====Main Menu=====

  1) Boot Current System, Version [ 1.1.1073]
  2) Boot Previous System, Version [ 1.1.1068]
  3) Update Device Image & Keep Current Configuration
  4) Verbose Mode With File Checks
  5) Update Device Image & Restore Default Configuration

-----
<UP>,<DOWN>:Change item. <ENTER>:Select item.

```

FIGURE 15-32. Preconfiguration console - Rescue mode main menu

3. Type **2** or select item 2 using the up and down keys, and then press **ENTER**. The appliance reboots and reverts to the previous firmware version.
4. Verify that the appliance has reverted to the previous firmware version by again checking the build number, as described in the first step of this procedure.

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 InterScan Gateway Security Appliance (the 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 appliance Management port on the back of the device, as shown in the figure below, and connect the other end of the cable the local computer.

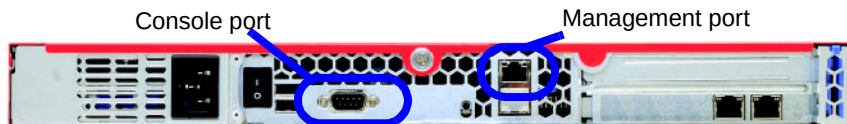


FIGURE 15-33. Back panel of the appliance showing console (serial) port and management port

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 the appliance rescue mode and for the appliance BMC (baseboard management controller) respectively. (See *Getting the IP Address of the Local PC* on page 15-12.)
3. Follow the instructions in *Interfacing with the Preconfiguration Console for Firmware Updates* starting on page 15-34.
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 15-1 on page 8.)

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 terminal emulation to VT100J, as shown below.

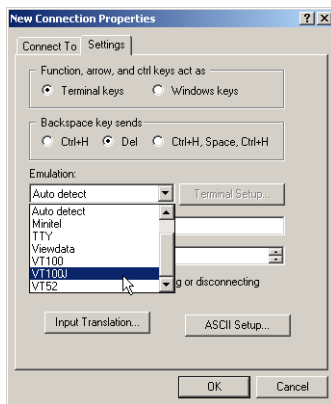


FIGURE 15-34. HyperTerminal display settings

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 15-35. 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.
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

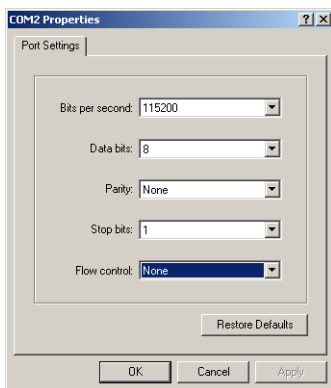


FIGURE 15-36. HyperTerminal COM Properties screen

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.

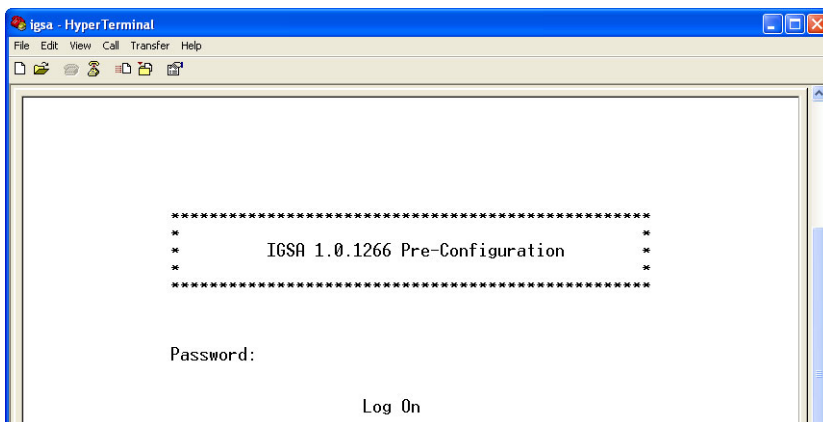


FIGURE 15-37. The appliance Preconfiguration console login screen

8. Press **ENTER** again. The Preconfiguration console Main Menu appears, as shown below.

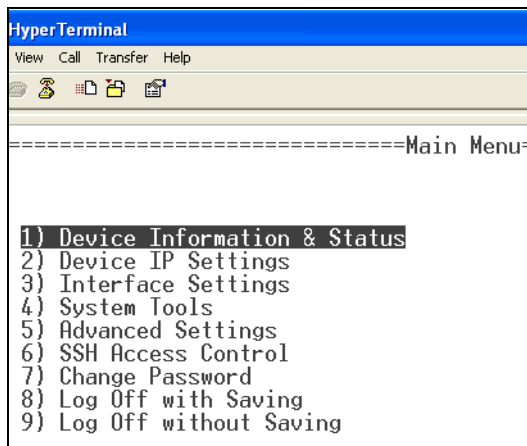


FIGURE 15-38. The appliance Preconfiguration console main menu, accessed via HyperTerminal

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 appliance Solutions CD into the local computer. The following screen appears:

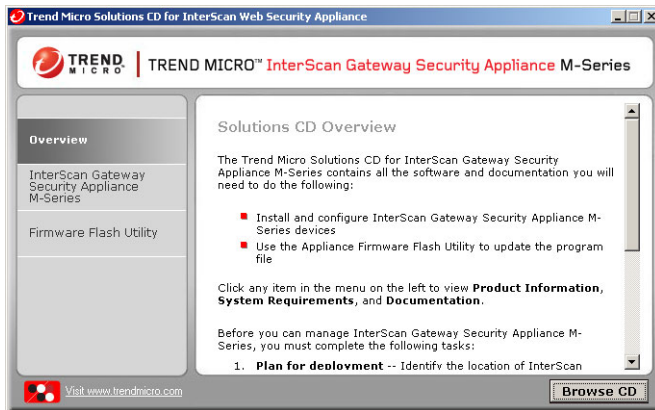


FIGURE 15-39. The appliance Solutions CD splash screen

- On the main menu click **Firmware Flash Utility**. The following screen appears:

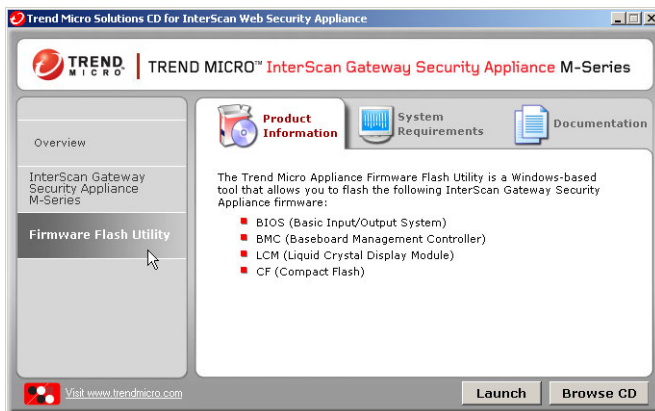


FIGURE 15-40. The appliance Solutions CD Firmware Flash Utility section

4. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

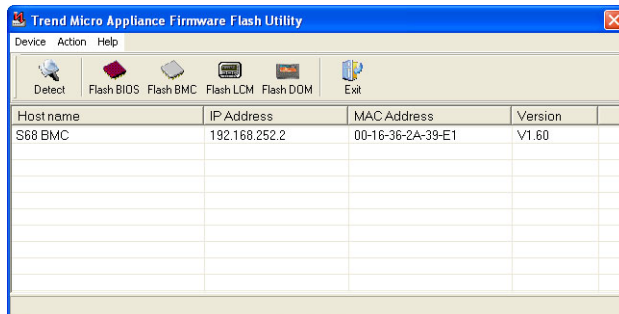


FIGURE 15-41. Trend Micro Appliance Firmware Flash Utility, opening screen

5. 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 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.

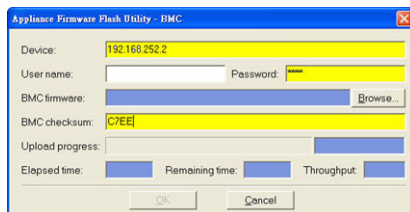


FIGURE 15-42. AFFU - BMC information entry screen

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 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 InterScan Gateway Security Appliance BIOS Firmware

On rare occasions, it may be necessary to update the InterScan Gateway Security Appliance (the appliance) BIOS. Follow the procedures below to complete this kind of update.

Preparing to Upload the Appliance BIOS

Before uploading the appliance 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 15-32), are exactly the same as the procedures for connecting a local computer to the appliance to deliver the update and interfacing with the Preconfiguration console:

1. Follow the instructions in [Preparing to Upload the BMC Firmware](#) starting on page 15-32.
2. Follow the instructions in [Interfacing with the Preconfiguration Console for Firmware Updates](#) starting on page 15-34.

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 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 appliance Solutions CD into the local computer. The following screen appears:

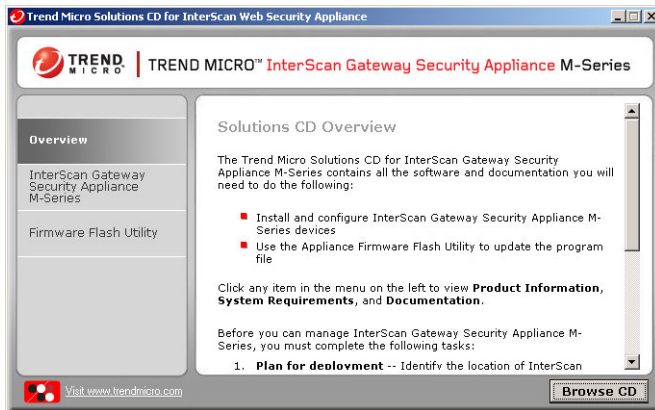


FIGURE 15-43. The appliance Solutions CD splash screen

- On the main menu click **Firmware Flash Utility**. The following screen appears:

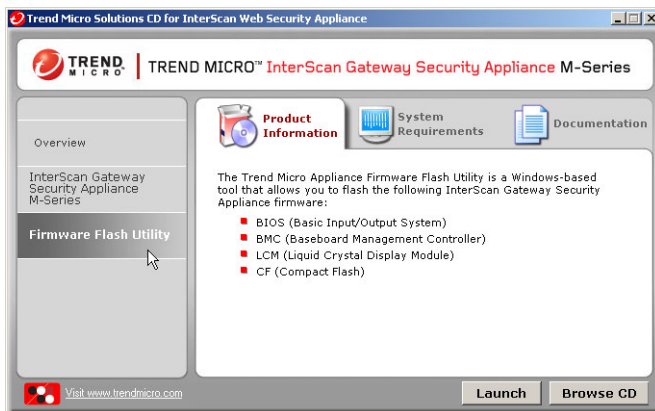


FIGURE 15-44. The appliance Solutions CD Firmware Flash Utility section

4. On the Product Information tab, click **Launch**. The Trend Micro Appliance Firmware Flash Utility opens, and the following screen appears:

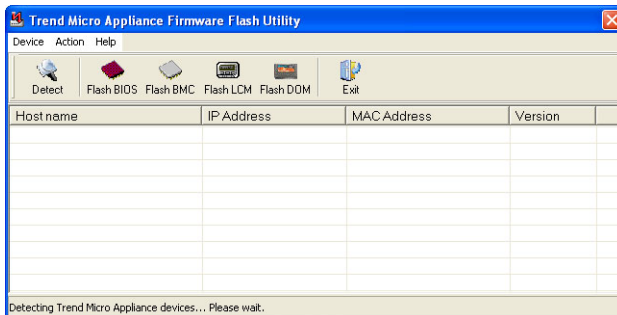


FIGURE 15-45. AFFU screen that appears initially

5. 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.

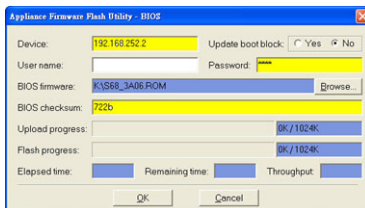


FIGURE 15-46. AFFU BIOS information entry screen

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 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 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:

- That the Ethernet cable is connected to the management port. (See Figure 15-20, "The appliance back panel showing location of management port," on page 22.)
- 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.)
- 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 15-32.)
- 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; therefore, 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. Therefore, the recommended action is that they be deleted—fully supported by InterScan Gateway Security Appliance.

Introducing Trend Micro Control Manager™

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

This chapter discusses the following topics:

- *Control Manager Basic Features* on page B-2
- *Understanding Trend Micro Management Communication Protocol* on page B-3
- *Control Manager Agent Heartbeat* on page B-7
- *Registering InterScan Gateway Security Appliance M-Series to Control Manager* on page B-9
- *Managing InterScan Gateway Security Appliances From Control Manager* on page B-11

Control Manager Basic Features

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

Control Manager is designed to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

FEATURE	Description
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console. This helps ensure consistent enforcement of your organization's virus and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak.
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure management console access and component download.
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage via user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control InterScan Gateway Security Appliances in real-time. Control Manager immediately sends configuration modifications made on the management console to the InterScan Gateway Security Appliances. System administrators can run manual scans from the management console. This command system is indispensable during a virus outbreak.

FEATURE	Description
Centralized update control	Update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed
Centralized reporting	Get an overview of the antivirus and content security product performance by using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with InterScan Gateway Security Appliances. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

XML parsing requires more system resources compared to the other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).

The agent footprint required to transfer information is much larger in XML compared with other data formats.

Data processing performance is slower due to the larger data footprint.

Packet transmissions take longer and the transmission rate is less than other data formats.

With the issues mentioned above, MCP's data format is devised to resolve these issues. The MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility is also been considered since each item is composed of name ID, type, length and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with/or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IPs on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks

when agent sits behind a NAT device (or TMCM server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the TMCM server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

The MCP deals with this issue by introducing a one-way communication model. With one-way communication, only the agent initiates the network connection to the server. The server cannot initiate connection to the agent. This one-way communication works well for log data transfers. However, the server dispatching of commands occurs under a passive mode. That is, the command deployment relies on the agent to poll the server for available commands.

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

- A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues
- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used.

Using MCP, Control Manager has three security levels:

- **Normal security:** Control Manager uses HTTP for communication
- **Medium security:** Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security:** Control Manager uses HTTPS for communication

One-Way and Two-Way Communication Support

MCP supports one-way and two-way communication.

One-Way Communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. In order to address this issue, MCP uses one-way communication. One-way communication has the Control Manager agent initiating the connection to and polling of commands from the server. Each request is a CGI-like command query or log transmission. In order to reduce the network impact, the connection is kept alive and open as much as possible. A subsequent request uses an existing open connection. Even if the connection is dropped, all connections involving SSL to the same host benefit from session ID cache that drastically reduces re-connection time.

Two-Way Communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on HTTP protocol. Two-way communication can improve real time dispatching and processing of commands from the server by the Control Manager agent. The Control Manager agent side needs a Web server or CGI compatible program that can process CGI-like requests to receive notifications from Control Manager server.

Single Sign-on (SSO) Support

Through MCP, Control Manager 3.5 now supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

The following products support SSO with Control Manager 3.5:

- InterScan Gateway Security Appliance
- SeverProtect for Linux version 2.5
- Network VirusWall Enforcer 1200
- Network VirusWall Enforcer 2500

Cluster Node Support

Under varying cases, administrators may like to group certain product instances as a logical unit, or cluster (for example, products installed under a cluster environment

present all installed product instances under one cluster group). However, from the Control Manager server's perspective, each product instance that goes through the formal registration process is regarded as an independent managed unit and each managed unit is no different from another.

Through MCP, Control Manager supports cluster nodes.

Control Manager Agent Heartbeat

To monitor the status of InterScan Gateway Security Appliances, Control Manager agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the InterScan Gateway Security Appliance and to check for commands to the InterScan Gateway Security Appliance from Control Manager. The Control Manager Web console then presents the product status. This means that the InterScan Gateway Security Appliance status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each InterScan Gateway Security Appliance in a sequential manner in the background. Control Manager changes the status of InterScan Gateway Security Appliances to offline, when a fixed period of time elapses without a heartbeat from the InterScan Gateway Security Appliance.

Active heartbeats are not the only means Control Manager has for determining the status of InterScan Gateway Security Appliances. The following also provide Control Manager with the InterScan Gateway Security Appliance status:

- Control Manager receives logs from the InterScan Gateway Security Appliance. Once Control Manager receives any type of log from the InterScan Gateway Security Appliance successfully, this implies that the InterScan Gateway Security Appliance is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the InterScan Gateway Security Appliance to retrieve the pending command. If server connects to the InterScan Gateway Security Appliance successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.
- In one-way communication mode, the Control Manager agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The Control Manager agent heartbeats implement with the following ways:

- **UDP:** If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. In addition, the transmitting client cannot make sure that the server does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the InterScan Gateway Security Appliance applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains InterScan Gateway Security Appliance activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 PM, and from 6:00 P.M. to 12:00 P.M.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend

Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

Registering InterScan Gateway Security Appliance M-Series to Control Manager

The InterScan Gateway Security Appliance is a standalone product and you do not need to register the device to Control Manager. However, by registering to Control Manager you gain the benefits explained earlier in this appendix. All features are managed using the InterScan Gateway Security Appliance Preconfiguration console and Web console. Before registering InterScan Gateway Security Appliance to a Control Manager 3.5 server, you must ensure that both the device and the Control Manager server belong to the same network segment.

To register an InterScan Gateway Security Appliance to Control Manager:

1. Log on to the Preconfiguration console.
2. On the **Main Menu** of the Preconfiguration console, type 2 to select **Device Settings** and press **Enter**. The Device Settings Screen displays.

Note: Control Manager uses the name specified in the Host name field to identify InterScan Gateway Security Appliances. The Host name appears in the Product Directory of Control Manager.

3. Use the down arrow to bring the cursor down to **Register to Control Manager**, and then use the spacebar to change the option to **[yes]**.

4. Type the Control Manager server IP address in the **FQDN or IP address** field.
5. Type the port number and IP address of your router or NAT device server in the **Port forwarding IP address** and **Port forwarding port number** fields.

Note: The InterScan Gateway Security Appliance uses the **Port forwarding IP address** and **Port forwarding port number** for two-way communication with Control Manager.

6. Use the down arrow to bring the cursor down to **Return to main menu** and press **Enter**.
7. On the Main Menu, type A to select **Save and log off** and press **Enter**. A confirmation screen displays.
8. Ensure the cursor is on **OK** and press **Enter**.
9. From the Control Manager management console **Main Menu**, click **Products**.
10. On the left most menu, select **Managed Products** from the list and then click **Go**.
11. Check to see that InterScan Gateway Security Appliance displays.

Managing InterScan Gateway Security Appliances From Control Manager

A managed product refers to an InterScan Gateway Security Appliance, an antivirus, a content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons. These icons represent InterScan Gateway Security Appliances, other Trend Micro antivirus and content security products, as well as third party products.

Indirectly administer the managed products either individually or by groups through the Product Directory. Use the Directory Manager to customize the Product Directory organization.

Understanding Product Directory

Take care when planning the structure of the Product Directory, a logical grouping of managed products, because it affects the following:

- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For example, granting access to the root segment grants access to the entire Directory. On the other hand, granting access to a specific InterScan Gateway Security Appliance only grants access to that specific product.
- **Deployment planning:** Control Manager deploys virus pattern, scan engine, spam rule, and program updates to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory will therefore simplify the designation of recipients.
- **Outbreak Prevention Policy and Damage Control Template deployments:** OPP and DCS deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

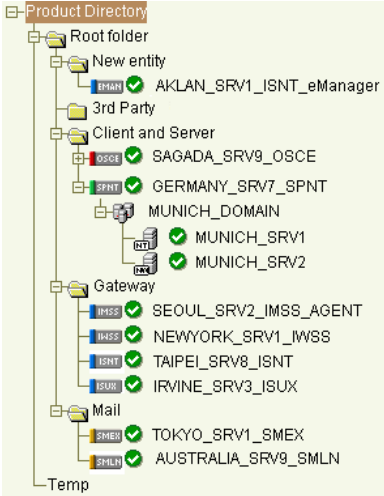
PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
		New entity or user-defined folder name
		
		InterScan VirusWall for Windows
		InterScan VirusWall for Linux
		InterScan Gateway Security Appliance
		
		
		Network VirusWall
		
		
		
		
		
		
		
		NetScreen Global PRO Firewall
		Managed Product connection status icon
		
		

Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your InterScan Gateway Security Appliances according to their protection type and the Control Manager network administration model. For example, grant access rights to mail administrators to configure the Mail folder.

Accessing a InterScan Gateway Security Appliance M-Series Default Folder

Newly registered InterScan Gateway Security Appliances usually appear in the New entity folder depending on the user account specified during the agent installation. Control Manager determines the default folder for the InterScan Gateway Security Appliance by the privileges of the user account specified during the product agent installation. However, Control Manager segregates managed products handled by Trend VCS agents under the Trend VCS agents folder.

The following presents different scenarios for the accessible folders given to the account and the resulting default managed product location:



ACCESSIBLE FOLDER GIVEN TO THE ACCOUNT	DEFAULT MANAGED PRODUCT LOCATION
Root folder	New entity
Mail	Mail
SAGADA_SRV9_OSCE	New entity

User accounts set to access a specific managed product cannot access any newly registered managed products.

FIGURE B-1. Managed Products vs. User Access

Access Product Directory

Use the Product Directory to administer InterScan Gateway Security Appliances registered with the Control Manager server.

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

- 1. Click **Products** on the main menu.
- 2. On the left most menu, select **Managed Products** from the list and then click **Go**.

Manually Deploy New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your InterScan Gateway Security Appliances and other managed products on demand. This is useful especially during virus outbreaks.

Download new components before deploying updates to specific or groups of InterScan Gateway Security Appliances or managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired folder or InterScan Gateway Security Appliance.
4. On the working area, click the **Tasks** tab.
5. Select **Deploy <component>** from the Select task list.
6. Click **Next>>**.
7. Click **Deploy Now** to start the manual deployment of new components.
8. Monitor the progress via Command Tracking.
9. Click the **Command Details** link to view details for the Deploy Now task.

View InterScan Gateway Security Appliance M-Series Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all InterScan Gateway Security Appliances and other managed products present in the Product Directory tree.

There are two ways to view the InterScan Gateway Security Appliances status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system.

This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or InterScan Gateway Security Appliance.
 - If you click an InterScan Gateway Security Appliance or managed product, the Product Status tab displays the InterScan Gateway Security Appliance or managed product's summary
 - If you click the **Root** folder, **New entity**, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configure InterScan Gateway Security Appliances and Managed Products

Depending on the product and agent version:

- You can configure devices or products either individually or in groups according to folder division
Perform group configuration using the folder Configuration tab.

Note: When performing a group configuration, verify that you want all InterScan Gateway Security Appliance in a group to have the same configuration. Otherwise, add devices or managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows either the product's Web console or a Control Manager-generated console

To configure a product:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired InterScan Gateway Security Appliance, managed product or folder.
4. On the working area, click the **Configuration** tab.
5. Select the product to configure from the Select product list.

Note: Step 4 is necessary when you use the folder Configuration tab.

6. At the Select configuration list, select the product feature to access or configure.
7. Click **Next**. The InterScan Gateway Security Appliance or managed product Web-based console or Control Manager-generated console appears.

Issue Tasks to InterScan Gateway Security Appliances and Managed Products

Use the Tasks tab to invoke available actions to a group or specific InterScan Gateway Security Appliance or managed product. You can perform the following tasks on InterScan Gateway Security Appliances:

- Configuration Replication
- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Replicate configuration to entire folder

Deploy the latest pattern file, or scan engine to InterScan Gateway Security Appliances with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to InterScan Gateway Security Appliances:

1. Access the Product Directory.
2. On the left-hand menu, select the desired InterScan Gateway Security Appliance or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the Select task list.
5. Click **Next**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View InterScan Gateway Security Appliance M-Series and Managed Product Logs

Use the Logs tab to query and view logs for a group or specific InterScan Gateway Security Appliance.

To query and view InterScan Gateway Security Appliance logs:

1. Access the Product Directory.
2. On the left-hand menu, select the desired InterScan Gateway Security Appliance or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

Event Logs:

- a. Provide the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

- b. Click **Display Logs** to begin the query and display the query results.

Security Logs:

- a. Select All virus log incidents or a specific security logs type and then click **Query**.
- b. Provide the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

- c. Click **Display Logs** to begin the query.

Note: eManager managed products records content security violations in the Security Logs, not in the Virus Logs.

5. The Query Result screen displays the results in a table format.
6. The Generated at entity column of the result table indicates the Control Manager server time.

Recovering InterScan Gateway Security Appliances Removed From the Product Directory

The following scenarios can cause Control Manager to delete InterScan Gateway Security Appliances from the Product Directory:

- Reinstalling the Control Manager server and selecting Delete existing records and create a new database option
This option creates a new database using the name of the existing one.
- Replacing the corrupted Control Manager database with another database of the same name
- Accidentally deleting the InterScan Gateway Security Appliance using the Directory Manager

If a Control Manager server's InterScan Gateway Security Appliance records are lost, the agents on the products still "know" where they are registered to. The product agent will automatically re-register itself after eight hours or when the service restarts.

To recover InterScan Gateway Security Appliances removed from the Product Directory:

- Restart the InterScan Gateway Security Appliance.

Search for InterScan Gateway Security Appliances, Product Directory Folders or Computers

Click **Search** to quickly:

- Add a specific or a group of InterScan Gateway Security Appliances to Temp
- Find and locate a specific InterScan Gateway Security Appliance in the Product Directory

To search for a folder or InterScan Gateway Security Appliance:

1. Access Product Directory.
2. On the left menu, click **Search**.

3. On the working area, provide the following search parameters:

PARAMETER	DESCRIPTION
Search for	Select the object of the search from the drop down list Search for managed products or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name Select Case sensitive to narrow down the search results.
Managed product status / Communicator status	Select the appropriate connection status, for the Communicator or managed product The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose All to search for objects regardless of the connection status.
Product	Select the appropriate product from the list. Choose All to search for all products.

4. Click **Begin Search** to start searching.
5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Refresh the Product Directory

To refresh the Product Directory:

- In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Understanding Directory Manager

After the registering to Control Manager, the InterScan Gateway Security Appliance first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs. For example, you can group products by location or product-type messaging security, web security, file storage protection, and so on.

The Directory allows you to create, modify, or delete folders, and move InterScan Gateway Security Appliances between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the InterScan Gateway Security Appliances belonging to each folder. Consider the following factors when planning and implementing your folder and InterScan Gateway Security Appliance structure:

- Product Directory
- User Accounts
- Deployment Plans

Group InterScan Gateway Security Appliances according to geographical, administrative, or product specific reasons. In combination with different access rights used to access InterScan Gateway Security Appliances or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages:

Grouping Type	Pro's	Con's
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

Using the Directory Manager Options

Directory Manager provides seven options: New Folder, Delete, Rename, Undo, Redo, Cut, and Paste.

Use these options to manipulate and organize InterScan Gateway Security Appliances in your Control Manager network.

To use and apply changes in the Directory Manager:

- Right-click a folder or InterScan Gateway Security Appliance to open a pop-up menu that presents a list of actions you can perform
- Click **+** or the folder to display the InterScan Gateway Security Appliances belonging to a folder
- Press **Enter** or click anywhere when you rename a folder
- Click **Save** to apply your changes and update the Directory Manager organization
- Click **Reset** to discard changes that are not yet saved

Access Directory Manager

Use Directory Manager to group InterScan Gateway Security Appliances together.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

Create Folders

Group InterScan Gateway Security Appliances into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If you are building the tree for the first time, right-click the **Root** folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, \$, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, ^, {, |, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming Folders or InterScan Gateway Security Appliances

To rename a folder or InterScan Gateway Security Appliance:

1. Access Directory Manager.
2. On the working area, right-click the folder or InterScan Gateway Security Appliance you want to rename and then select **Rename** from the pop-up menu. The folder/InterScan Gateway Security Appliance name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

Note: Renaming an InterScan Gateway Security Appliance only changes the name stored in the Control Manager database there are no effects to the product.

Move Folders or InterScan Gateway Security Appliances

To transfer or move a folder or InterScan Gateway Security Appliance to another location:

1. Access Directory Manager.
2. On the working area, select the folder or InterScan Gateway Security Appliance you want to move.
3. Do one of the following:
 - Drag-and-drop the folder or InterScan Gateway Security Appliance to the target new location
 - Cut and paste the folder or InterScan Gateway Security Appliance to the target new location
4. Click **Save**.

Delete User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete an InterScan Gateway Security Appliance which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder.

Use caution when deleting user-defined folders, you may accidentally delete an InterScan Gateway Security Appliance.

Understanding Temp

Temp, a collection of InterScan Gateway Security Appliance shortcuts, allows you to focus your attention on specific products without changing the Product Directory organization. Use Temp for deploying updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all InterScan Gateway Security Appliance shortcuts when you log off the management console.
- You can only add the InterScan Gateway Security Appliances to Temp if you can see them in the Product Directory, you cannot make shortcuts to products that you cannot access.

Using Temp

You can manipulate InterScan Gateway Security Appliances in Temp the same way you would with InterScan Gateway Security Appliances in the Product Directory. The folders and InterScan Gateway Security Appliances belonging to Temp have the same folder and InterScan Gateway Security Appliance-level controls. However, Control Manager determines what actions you can perform on the InterScan Gateway Security Appliances according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of InterScan Gateway Security Appliances using folder-level access rights.
- Select a specific InterScan Gateway Security Appliance, and then use the available Product Directory tabs to perform an action.

Access Temp

Use Temp to collect InterScan Gateway Security Appliance shortcuts.

To access Temp:

1. Access Product Directory.
2. On the left most menu, click **Temp**.

Adding InterScan Gateway Security Appliances to Temp

There are three methods to add InterScan Gateway Security Appliances to Temp:

- From the Search results
- From the Product Directory
- Add InterScan Gateway Security Appliances with outdated components based on the Status Summary page

Trend Micro recommends that you add several InterScan Gateway Security Appliances at once to Temp using the last method. The Status Summary screen provides information as to which InterScan Gateway Security Appliances use outdated components. It simplifies virus pattern and scan engine updates on groups of InterScan Gateway Security Appliances belonging to different folder groups.

Note: Adding InterScan Gateway Security Appliances to Temp only allows you to collect InterScan Gateway Security Appliances with outdated components doing so does not trigger automatic deployment.

To add from the Search results

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for InterScan Gateway Security Appliances or folders.

4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the InterScan Gateway Security Appliance shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field. For example, if you specify \pattern\mail, the following Temp structure appears:



-
5. Click **Add**. Control Manager adds InterScan Gateway Security Appliances from the search results to Temp.

To add from the Product Directory

1. Access the Product Directory.
2. On the left-hand menu, select the InterScan Gateway Security Appliance you want to add to Temp.
3. Press "+" on the numeric keypad.

To add InterScan Gateway Security Appliances with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of InterScan Gateway Security Appliances that are outdated. Depending on the link you clicked, the Virus Pattern Status (Outdated), Scan Engine Status (Outdated), Spam Rule Status (Outdated) screen opens displaying the computer name, product name, product version, and outdated component version.
5. Click **Add to Temp** in the status page. Control Manager organizes the InterScan Gateway Security Appliances to Temp using folders named after the page from which they were added. For example, Control Manager places InterScan Gateway Security Appliances added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

Note: Clicking **Add to Temp** only adds the InterScan Gateway Security Appliances shown on the status page. If the list of InterScan Gateway Security Appliances spans more than one screen, click **Add to Temp** on all screens to add all products with outdated component.

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated InterScan Gateway Security Appliances to Temp.

Removing InterScan Gateway Security Appliances From Temp

To remove a InterScan Gateway Security Appliance from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.
3. From the available InterScan Gateway Security Appliances on the Temp list, select the folder or InterScan Gateway Security Appliance shortcut that you want to remove.
4. Press "-" in the numeric keypad.

Note: Control Manager removes InterScan Gateway Security Appliance shortcuts in Temp when you log off from the management console.

Removing InterScan Gateway Security Appliances from Temp will neither disconnect the antivirus or content security product nor uninstall the Control Manager agent from the Control Manager server.

Download and Deploy New Components From Control Manager

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

- **Pattern files/Cleanup templates** - refer to virus pattern files, Damage Cleanup templates, Vulnerability Assessment patterns, network outbreak rules, Pattern Release History, and network virus pattern files
- **Anti-spam rules** - refer to import and rule files used for anti-spam and content filtering
- **Engines** - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux
- **Product program** - these are product specific components (for example, Service Pack releases)

Note: Only registered users are eligible for components update. For more information, see the Control Manager online help [Registering and Activating your Software > Understanding product activation topic](#).

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

Understanding Update Manager

Update Manager provides functions that help you update the antivirus and content security components of your Control Manager network.

Updating the Control Manager network involves two steps:

- Downloading components: You can do this manually or by schedule
- Deploying components: You do this manually or by schedule

Understanding Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Manually Download Components

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

Tip: Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

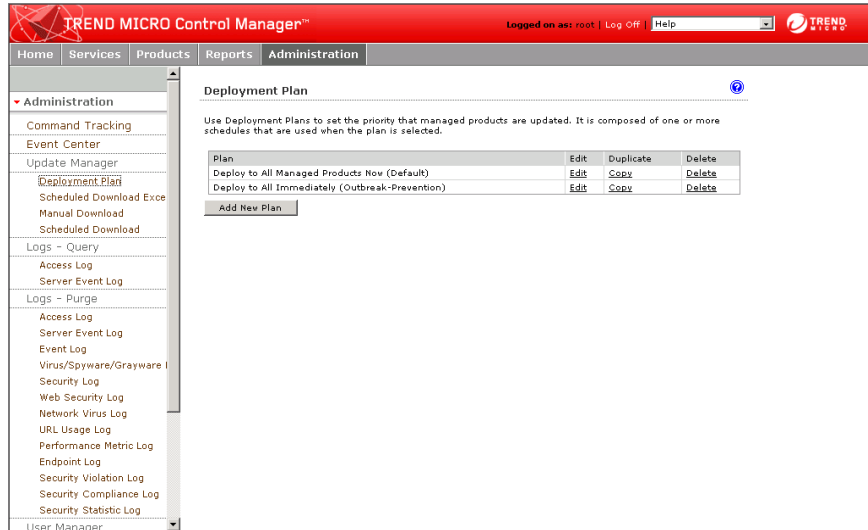
Step 5: Configure the automatic deployment settings

Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.



3. On the working area, click **Add New Plan**.

Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

Schedule(s):

#	Deployment Time	Edit	Delete
Add New Schedule			

Save **Cancel**

Note: After you have added at least one schedule, click Save to save the new plan and schedule(s).

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.

Add New Schedule

Plan name: Schedule 1

Deployment time: ☒ Delay | 0 | hour(s) | 5 | minute(s)
☐ Start at: | 00 | : | 00 | (hh:mm)

Select a folder:
In each schedule, select one folder to apply the deployment. For multiple-folder deployment, create multiple schedules. The folders you see depend on the folder access rights you have been given.

☒ Product Directory
 ☐ Root folder
 ☐ New entity
 ☐ MCP Managed Products

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
 - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify
Use the menus to indicate the duration, in terms of hours and minutes.
 - **Start at** - Performs the deployment at a specific time
Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

System Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

Save

ActiveUpdate settings

☐ Enable HTTPS for the default update download source

Local Windows Authentication

User name:

Password:

Remote UNC Authentication

User name:

Password:

Download component proxy settings

☐ Use a proxy server to download update components from the Internet

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Protocol: ☒ HTTP ☐ Socks

Authentication

Login name:

Password:

Trend VCS agent proxy settings

☐ Use a proxy server to connect to Trend VCS agents

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Protocol: ☒ HTTP ☐ Socks

Authentication

Login name:

Password:

Notification settings

SMTP server

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Sender email address:

Note: The SMTP server may need a sender address to deliver mail.

Pager CDM port

Use ☐ for pagers

SNMP trap notification

Community name:

Server IP address:

Trigger application

☐ Use an specified user to trigger application

User name:

Password:

MSN(TM) Messenger notification

MSN(TM) Messenger email address:

Password:

☐ Use a proxy server to connect to MSN(TM) server

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Protocol: ☒ Socks 4 ☒ Socks 5

Authentication

Login name:

Password:

Save

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
 - **HTTP**
 - **SOCKS**
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Manual Download**. The Manual Download screen appears.

Manual Download

Perform manual downloads to obtain the required update files immediately -- on demand.

Components	
	☐ Pattern files/Cleanup templates
	☐ Anti-spam rules
	☐ Engines
	☐ Product programs

Download settings

Source:

☒ Internet: Trend Micro update server
☐ Other update source

for example, http://DownloadServer.Antivirus.com/AU or c:\ActiveUpdate\ or \\updatesource

Retry frequency: ☐ If the download is unsuccessful, retry time(s), every minute(s)

Proxy: [\(Edit\)](#)

Automatic deployment settings

Configure and select a [Deployment Plan](#) below to schedule automatic deployment by location.

Schedule:

☐ Do not deploy
☐ Deploy immediately
☒ Based on deployment plan
☒ When new updates found

Deployment plan:

2. From the Components area, select the components to download.
 - a. Click the + icon to expand the component list for each component group.
 - b. Select the following components to download:

From Pattern files/Cleanup templates:

- Virus Pattern
- Spyware Pattern
- Spyware Active-monitoring Pattern

- Virus Cleanup Template
- Anti-spam Pattern
- Firmware
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

From Engines:

- Virus Scan Engine (32-bit)
- Spyware Scan Engine (32-bit)
- Virus Cleanup Engine (32-bit)
- Anti-spam Engine

Step 4: Configure the download settings**1.** Select the update source:

- **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
- **Other update source:** Type the URL of the update source in the accompanying field.

After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.

2. Select Retry frequency and specify the number of retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 5: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
 - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
 - Deploying to the managed products individually
 - Testing the updated components before deployment
 - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
 - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
 - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
3. Click **Save**.

Step 6: Complete the manual download

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
2. Click **Command Details** to view details from the Command Details screen.
3. Click **OK** to return to the Manual Download screen.

Configure Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.
3. Do the following:
 - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.
 - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, all downloads for the selected hours are blocked.
4. Click **Save**.

Understanding Scheduled Downloads

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group, downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component is updated
- **Enabled:** Indicates if the schedule for the component is either enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

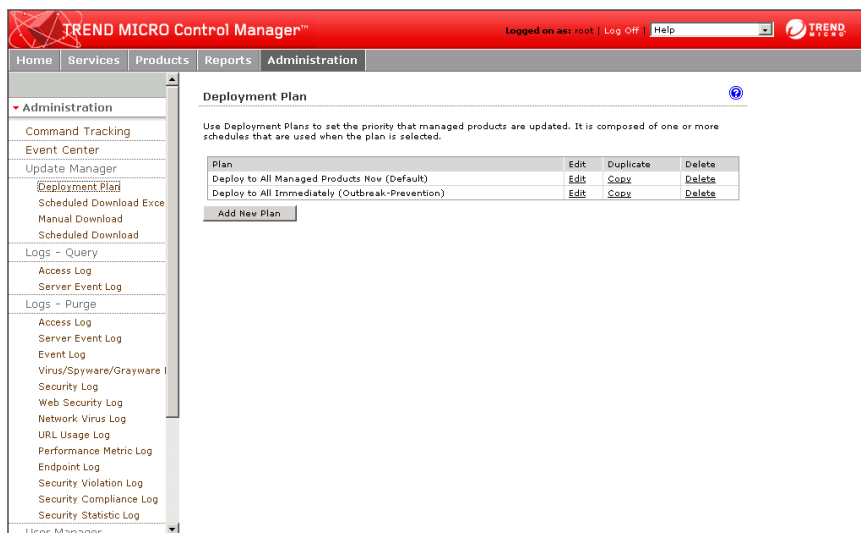
Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

Configure Scheduled Downloads and Enable Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.



3. On the working area, click **Add New Plan**.

Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

Schedule(s):

#	Deployment Time	Edit	Delete
Add New Schedule			

Note: After you have added at least one schedule, click Save to save the new plan and schedule(s).

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
 - **Delay** - After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify
Use the menus to indicate the duration, in terms of hours and minutes.
 - **Start at** - Performs the deployment at a specific time
Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

TREND MICRO Control Manager™ Logged on as: root | Log Off | Help

Home Services Products Reports Administration

System Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

ActiveUpdate settings

☐ Enable HTTPS for the default update download source

Local Windows Authentication

User name:

Password:

Remote UNC Authentication

User name:

Password:

Download component proxy settings

☐ Use a proxy server to download update components from the Internet

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Protocol: ☒ HTTP ☐ Socks

Authentication

Login name:

Password:

Trend VCS agent proxy settings

☐ Use a proxy server to connect to Trend VCS agents

Command Tracking

Event Center

Update Manager

Deployment Plan

Scheduled Download Exceptions

Manual Download

Scheduled Download

Logs - Query

Access Log

Server Event Log

Logs - Purge

Access Log

Server Event Log

Event Log

Virus/Spyware/Grayware Log

Security Log

Web Security Log

Network Virus Log

URL Usage Log

Performance Metric Log

Endpoint Log

Security Violation Log

Security Compliance Log

Security Statistic Log

User Manager

My Account

User Accounts

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
 - HTTP
 - SOCKS
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Scheduled Download**. The Scheduled Download screen appears.

Scheduled Download

Schedule Control Manager automatically search for and download the latest component updates from Trend Micro, to keep your systems up-to-date.

Component	Frequency	Enabled	Update Source
<u>Pattern files/Cleanup templates</u>	Every 1 day(s)		Trend Micro update server.
<u>Anti-spam rules</u>	Every 1 day(s)		Trend Micro update server.
<u>Rule Version</u>	Every 1 day(s)		Trend Micro update server.
<u>Anti-spam Pattern</u>	Every 1 day(s)		Trend Micro update server.
<u>Anti-spam Pattern (Delta)</u>	Every 1 day(s)		Trend Micro update server.
<u>SSAPI Spyware Cleanup Template</u>	Every 1 day(s)		Trend Micro update server.
<u>Engines</u>	Every 1 day(s)		Trend Micro update server.
<u>Product programs</u>	Every 1 week(s)		Trend Micro update server.

Save

2. From the Components area select, the components to download.
 - a. Click the + icon to expand the component list for each component group.
 - b. Select the following components to download:

From Pattern files/Cleanup templates:

- Virus Pattern
- Spyware Pattern
- Spyware Active-monitoring Pattern
- Virus Cleanup Template
- Anti-spam Pattern
- Firmware
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

From Engines:

- Virus Scan Engine (32-bit)
- Spyware Scan Engine (32-bit)
- Virus Cleanup Engine (32-bit)
- Anti-spam Engine

The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.

Pattern files/Cleanup templates

Schedule automatic component download below.

☐ **Enable scheduled download**

Schedule and frequency

Download:

☐ Every 5 minutes
☐ Every hour
☒ Every day
☐ Every week on Sunday

Start time: 00 : 53 (hh:mm)

Download settings

Source:

☒ Internet: Trend Micro update server
☐ Other update source

for example, http://DownloadServer.Antivirus.com/AU or
 c:\ActiveUpdate\ or \\updatesource

Retry frequency: ☐ If the download is unsuccessful, retry time(s), every minute(s)

Proxy: ([Edit](#))

Automatic deployment settings

Configure and select a [Deployment Plan](#) below to schedule automatic deployment by location.

Schedule:

☐ Do not deploy
☐ Deploy immediately
☒ Based on deployment plan
☒ When new updates found

Deployment plan:

Step 4: Configure the download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the download settings

1. Select the update source:
 - **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
 - **Other update source:** Type the URL of the update source in the accompanying field.

After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
 - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
 - Deploying to the managed products individually
 - Testing the updated components before deployment
 - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
 - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
 - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the **Deployment plan** list.
3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click **Status** in the Enabled column.
2. Click **Save**.

Use Reports

A Control Manager **report** is an online collection of figures about virus, spyware/grayware, and content security events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- *Local reports*
- *Global reports*

Note: You can only configure the **Global Report Profile** option through the *parent server management console*.

Local Reports

Local reports are reports about managed products administered by the parent server. Local reports do not include reports generated by child servers. Use the Global Report options to view reports about managed products administered by child servers registered to the parent server.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Local Report Profile**.

Note: When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about managed products administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Global Report Profile**.
3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Understanding Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Trend Micro Control Manager 3.5 adds 3 new report templates to the 77 previously available since Service Pack 3. The reports added in Service Pack 3 fall into five categories: Desktop, Fileserver, Gateway, MailServer and Executive Summary. The new reports in Control Manager 3.5 fall into a new 6th category: Network Products. This category offers reports related to InterScan Gateway Security Appliance.

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses. This change affects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can enter a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the six categories of reports listed below. Clicking a mark into a check box includes the associated report in the final exported report file.

Control Manager 3.5 also provides 18 templates stored in <root>\Program Files\Trend Micro\Control Manager\Reports as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports.

Understanding Report Profiles

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF:** Rich text format; use a word processor (for example, Microsoft Word™) to view *.RTF reports
- **PDF:** Portable document format; use Adobe Reader to view *.PDF reports
- **ActiveX™:** ActiveX documents; use a Web browser to view reports in ActiveX format

Note: Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT:** Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

Create Report Profiles

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

Step 4: Configure the Frequency tab settings

Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

1. Click **Reports** on the main menu.
2. Take one of the following actions:
 - To create a local report profile, click **Local Report Profile** under Reports.
 - To create a global report profile, click **Global Report Profile** under Reports.
3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.

Create Report Profile 

1. Contents 2. Targets 3. Frequency 4. Recipients 5. Summary

Choose a report template to create a new report.

Report Name

Report Title (optional)

Description (optional)

New CM 3.0 Reports		Report Category:
Spyware/Grayware Detection Reports: ☐ Spyware/Grayware Detected ☐ Most Commonly Detected Spyware/Grayware 10 v ☐ Detected Spyware/Grayware List for All Entities		v - Executive summary - Excluded summary - Gateway products - Mail server products - Server based products - Desktop products - Network products
Virus Detection Reports: ☐ Viruses Detected ☐ Most Commonly Detected Viruses 10 v ☐ Virus Infection List for All Entities		☐ Viruses, Grouped by Day v ☐ Damage Cleanups, Grouped by Day v ☐ Spam, Grouped by Day v
		Vulnerability Reports: ☐ Machine Risk Level Assessment ☐ Vulnerability Assessment ☐ Most Commonly Cleaned Infections 10 v ☐ Worst Damage Potential Vulnerabilities 10 v

Step 2: Configure the Contents tab settings

1. In the working area under the Contents tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.
2. Type a title for the report in the **Report Title** field (optional).
3. Type a description of the report profile in the **Description** field (optional).
4. Select **Network Products** from the **Select report template** list.

5. Select the report format.
6. Click **Next >** to proceed to the Targets tab.

Create Report Profile

1. Contents

2. Targets

3. Frequency

4. Recipients

5. Summary

Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

☒ Product Directory

☐ Root folder

☐ New entity

Selected Machines

☒ **All clients**

☐ **IP range**

From :

To :

☐ **Segment**

Example : 10.1.120.122 / 24 : means mask is : 255.255.255.000

Segment : /

< Back

Next >

Cancel

Step 2: Configure the Contents tab settings

1. On the working area under the Targets tab, select the target of the local or global report profile:
 - Select the InterScan Gateway Security Appliances or folders. The profile only contains information about the InterScan Gateway Security Appliances or folders selected.
 - Select the child servers. The profile only contains information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.
2. Select the machines that the report will include:
 - **All clients:** All clients the selected InterScan Gateway Security Appliance protects
 - **IP range:** Select the IP range of the clients you want to include in the report
 - **Segment:** Select the IP range and segment of the clients you want to include in the report

3. Click **Next** > to proceed to the Frequency tab.

Create Report Profile

1. Contents 2. Targets **3. Frequency** 4. Recipients 5. Summary

Define when and how often this report is generated.

☒ One-time only

Contents in the report:

From: February 22 2006

To: February 22 2006

☐ Daily

☐ Weekly, on Sunday

☐ Every first day of the month

☐ Use calendar day

☒ Number of reports to keep 10

Start the scheduler:

☒ Immediately

☐ Start on

February 22 2006

17 : 47 (hh:mm)

< Back Next > Cancel

Step 4: Configure the Frequency tab settings

1. On the working area under the Frequency tab, specify how often Control Manager generates this report. You have the following options:
 - **One-time only:** Provides information you specified in the From and To dates
 - **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time
 - **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
 - **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
 - **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation

- If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs
2. Under Start the scheduler, specify when the Report Server starts collecting information for this report. Select one of the following:
 - **Immediately:** The report server collects information as soon as you save the report profile
 - **Start at:** The report server collects information at the specified date and time
 3. For scheduled reports, click **Number of reports to keep** and then specify the instance Control Manager will maintain on the server.

Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

4. Click **Next >** to proceed to the Recipient tab.

Create Report Profile

1. Contents 2. Targets 3. Frequency **4. Recipients** 5. Summary

Send email notifications to the following recipients whenever Control Manager generates the report:

Users and groups

- Group List ---
- Unexpected_Event
- Update_Event
- Virus_Event
- User List ---
- root

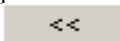
Recipient list

- Group List ---
- User List ---

☒ Send the report as an attachment

< Back Next > Cancel

Step 5: Configure the Recipient tab settings

- On the working area under the Recipients tab, select recipients from the existing Control Manager users and groups.
 - Use  to add recipients from the **Users and groups** list to the Recipient list
 - Use  to remove recipients from the **Recipient** list
- Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report being generated.
- Click **Next >** to proceed to the Summary tab.

Create Report Profile

1. Contents	2. Targets	3. Frequency	4. Recipients	5. Summary
Profile created at: 2/22/2006 5:48:35 PM Created by: root Contents Report name: SPLX Report Template 1 Report title: Report description: Export file format: Rich Text Format Report template: - Overall List of Spyware/Grayware Detected in All Entities - Overall List of Viruses Detected in All Entities - Overall Damage Cleanup Comparison - Overall Spam Comparison - Overall Spyware/Grayware Comparison - Overall Virus Comparison - Overall Most Commonly Detected Spyware/Grayware - Overall Most Commonly Detected Viruses - Overall Summary of Spyware/Grayware Detected - Overall Viruses Detected				
Targets - Product Directory - Root folder - New entity - MCP Managed Products				

- On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

Review Report Profile Settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports
On the working area under the Profile Summary column, click **View Profile**.
- Access Local or Global Scheduled Reports
On the working area under the Profile Summary column, click **View Profile**.

Enable Scheduled Report Profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it via the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, select the profile check box.
Select the check box adjacent to Report Profiles to select or deselect all profiles.
3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available, because Control Manager generates these reports only once.

Generate On-demand Scheduled Reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
 - To create a local report profile, click **Local Report Profile** on the left menu under Reports
 - To create a global report profile, click **Global Report Profile** on the left menu under Reports

3. On the working area under the Available Reports column, click the corresponding **View** link.
4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.
5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

View Generated Reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
 - To create a local report profile, click **Local Report Profile** on the left menu under Reports
 - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time**.
4. Under the Status column, click **View Report**. The default program used to open the file format opens.

Technology Reference

This appendix contains explanations of some of the technologies and terms mentioned most frequently mentioned in this manual.

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 the appliance. The appliance receives the file and starts scanning it. However, if the file is large it can take the 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 the 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, the appliance sends packets to the client one by one. The packets are sent to a temporary folder on the client. If the appliance detects a threat, it immediately stops sending packets, and a notification appears on the user's browser. The user sees a folder on the local 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 D. Removing the 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 C-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

LAN bypass is disabled by default. You can enable the feature through the InterScan Gateway Security Appliance Preconfiguration console. See [Enabling or Disabling LAN Bypass and Link State Failover](#) on page C-5.

Link State Failover

Link state failover is a feature by which, if either the **INT** or the **EXT** port stops functioning, both ports are automatically shut down. This feature is disabled by default. You can enable it through the Preconfiguration console. For instructions on enabling or disabling this feature, see [Enabling or Disabling LAN Bypass and Link State Failover](#) on page C-5.

Enabling or Disabling LAN Bypass and Link State Failover

Accessing the Preconfiguration Console

Follow the procedures below to access the appliance Preconfiguration console.

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 15-1, “Back panel of appliance showing console port, management port, and INT port,” on page 8.)

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 terminal emulation to VT100J, as shown below.

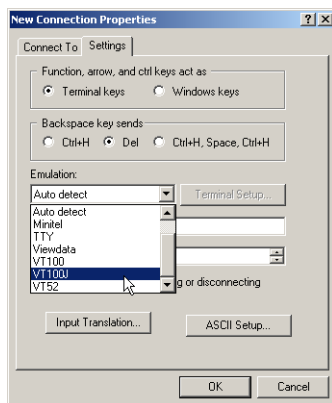


FIGURE C-1. HyperTerminal display settings

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 C-2. 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.
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

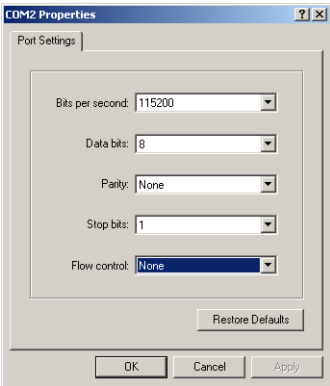


FIGURE C-3. HyperTerminal COM Properties screen

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.

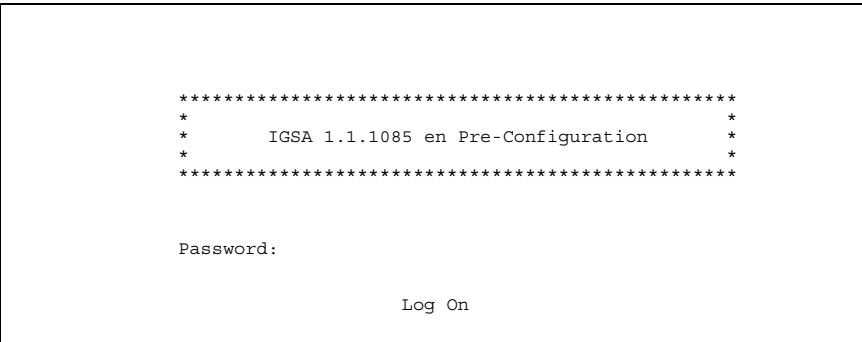


FIGURE C-4. The appliance Preconfiguration console login screen

8. Press **ENTER** again. The appliance Preconfiguration console Main Menu appears, as shown below.

```
====Main Menu====

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

:Change item. <ENTER>:Select item.
```

FIGURE C-5. The appliance Preconfiguration console main menu, accessed via HyperTerminal

To enable or disable LAN bypass and Link state failover:

1. Access the Preconfiguration console as described in [Accessing the Preconfiguration Console](#) on page C-5.
2. Select option **3, Interface Settings**. The following screen appears:

```

                                Interface Settings

Current Interface Setting:

Name           MNG      EXT      INT
=====
speed&duplex   auto      auto      auto

Link state failover: [disable] Use Space to change the value
LAN bypass: [disable] Use Space to change the value

10H: 10 Mbps x half-duplex      1000F: 1000 Mbps x full-duplex
10F: 10 Mbps x full-duplex      auto: automatically select the best
100H: 100 Mbps x half-duplex
100F: 100 Mbps x full-duplex

Return to Main Menu

,<TAB>:Change field. <Space>:Change Value. <ENTER>:Select field.

```

FIGURE C-6. Preconfiguration console Interface Settings screen

3. Use the **TAB** key to select the **LAN bypass** field
4. Press the **SPACE** bar on your keyboard to choose between **disabled** and **enabled**. The **LAN bypass** value toggles between **disabled** and **enabled**.
5. Use the **TAB** key to select the **Link state failover** field
6. Press the **SPACE** bar on your keyboard to choose between **disabled** and **enabled**. The **Link state failover** value toggles between **disabled** and **enabled**.
7. Use the **TAB** key to select the **Return to Main Menu** field and press **ENTER**. The Main Menu screen appears.
8. Select option **8, Log Off with Saving** and press **ENTER**. The system saves your settings and logs you off from the Preconfiguration console.

Scan Engine 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 file types are 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

NRS -> Content Filtering -> Content Scanning + Anti-phishing -> Scanning + Anti-spyware + IntelliTrap

POP3 Feature Execution Order

Content Filtering -> Anti-spam + Anti-phishing -> Scanning + Anti-spyware + IntelliTrap

HTTP Feature Execution Order

File Blocking (Extensions) -> Anti-pharming, Anti-phishing, URL Filtering -> File Blocking (True File type) -> Scanning + Anti-spyware

FTP Feature Execution Order

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.

Follow the procedure in this appendix to remove the InterScan Gateway Security Appliance 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.

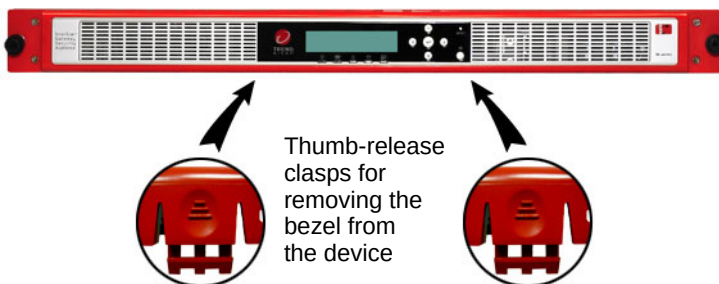


FIGURE D-1. Thumb-release clasps

3. Using both hands, apply pressure to both release clasps until the bottom part of the bezel separates from the device.



While pressing the thumb-release clasps, gently pull the bottom of the bezel away from the device. The top should then release easily.

FIGURE D-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.

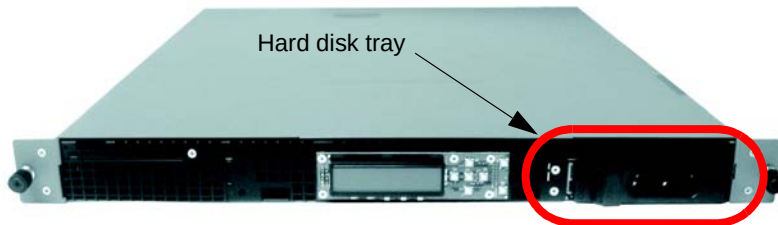


FIGURE D-3. The hard disk tray



FIGURE D-4. Hard disk release lever

6. Gently slide the hard disk tray out of the device.



FIGURE D-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

The following device address information is required during preconfiguration. The settings can be changed after preconfiguration.

TABLE E-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

This appendix includes the following topics:

- *Compression Types* on page F-2
- *Blockable File Formats* on page F-4
- *Malware Naming Formats* on page F-6

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 F-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 F-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 F-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, Convox 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 F-2. Blockable file formats (Continued)

Images	WINDOWS FONT, WINDOWS ICON, SUN GKS, PCX, PPM IMAGE, AUTODESK ANIMATOR (FLI OR FLC) (see subtype VSDT_FL I), PORTABLE NETWORK GRAPHICS, PAIN SHOP PRO, TARGA IMAGE, MACINTOSH BITMAP, ENCAPSULATED POSTSCRIPT, ANI-MATED CURSOR, TERRAGEN ATMOSPHERE, SGI IMAGE, CIN-EMA 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, TER-RAGEN 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 docu-ments	WORD FOR WINDOWS, WINDOWS POWERPOINT, EXCEL FOR WINDOWS, WINDOWS WRITE (see subtype VSDT_WRT), WIN-DOWS 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 F-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

TABLE F-3. Malware naming (Continued)

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
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

TABLE F-3. Malware naming (Continued)

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

This appendix includes the following topics:

- *Hardware Specifications* on page G-2
- *Dimensions and Weight* on page G-2
- *Power Requirements and Environment* on page G-3

Hardware Specifications

InterScan Gateway Security Appliance uses the following components:

TABLE G-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 G-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 G-1. Appliance power requirements and environmental specifications

Element	Specification
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 13-3, 15-4

 enable external access 13-3

 enabling 13-3

Access control 4-2

Activation Code

 new 13-23

 obtaining 1-16, 2-21

Activation code

 entering a new AC 13-23

ActiveX malicious code 3-12

Add Static Routes 13-13

Administration

 Access Control 13-3

 Figures

 fig. 13-01. Administration screen 13-2

 fig. 13-02. Administration > Access Control 13-3

 fig. 13-03. Administration > Configuration Backup 13-3

 fig. 13-04. Windows Save Dialog 13-4

 fig. 13-05. Administration > Disk SMART Test 13-8

 fig. 13-06. The Web console Firmware Update screen 13-9

 fig. 13-07. Administration > IP Address Settings – Management IP Address 13-11

 fig. 13-08. Administration > IP Address Settings – Static Routes 13-12

 fig. 13-09. Add Static Routes 13-13

 fig. 13-10. Static Routes – Multiple Segment Network 13-14

 fig. 13-11. Administration > Notification Settings - Settings 13-16

 fig. 13-12. Administration > Notification Settings - Events 13-17

 fig. 13-13. Administration > Operation Mode 13-18

 fig. 13-14. Administration > Password 13-19

 fig. 13-15. Administration > Product License 13-20

 fig. 13-16. Online License Update and Renewal 13-21

 fig. 13-17. My Product Details 13-22

 fig. 13-18. Administration > Product License - New Activation Code 13-23

 fig. 13-19. Administration > Proxy Settings 13-24

 fig. 13-20. Administration > SNMP Settings 13-26

 fig. 13-21. Administration > System Time 13-28

 fig. 13-22. Reboot screen 13-30

 fig. 13-23. Administration > Reboot menu 13-30

 fig. 13-24. Administration > World Virus Tracking 13-31

 fig. 13-25. Virus Map 13-32

 World Virus Tracking 13-31

Administration > Access Control 13-3

Administration > Configuration Backup 13-3

Administration > Disk SMART Test 13-8

Administration > IP Address Settings – Management IP Address 13-11

Administration > IP Address Settings – Static Routes 13-12

Administration > Notification Settings - Events 13-17

Administration > Notification Settings - Settings 13-16

Administration > Operation Mode 13-18

Administration > Password 13-19

Administration > Product License 13-20

Administration > Product License - New Activation Code 13-23

Administration > Proxy Settings 13-24

Administration > SNMP Settings 13-26

Administration > System Time 13-28

Administration > World Virus Tracking 13-31

Administration screen 13-2

AFFU

- “Flash DOM successfully uploaded” message 15-21, 15-27
- BIOS information entry screen 15-43
- BMC information entry screen 15-39
- browse to device image 15-20
- browse to device image file 15-26
- Do not click the row displaying the IP address 15-25
- DOM screen 15-19, 15-26
- DOM screen showing progress of the update 15-20, 15-27
- opening screen when uploading with option 3, emphasizing Flash DOM 15-19
- opening screen when using option 5, emphasizing Flash DOM 15-25
- screen that appears initially 15-43

AFFU. See Appliance Firmware Flash Utility.

AFFU.exe 15-40

Analyzing Your Protection

Figures

- fig. 12-01. Logs screen 12-2
- fig. 12-02. Logs > Query 12-3
- fig. 12-03. Logs > Query – HTTP Anti-Pharming Log 12-4
- fig. 12-04. Logs > Settings 12-5
- fig. 12-05. Logs > Maintenance - Manual 12-6
- fig. 12-06. Logs > Maintenance - Automatic 12-7

Anti-pharming

- Anti-pharming log 3-16

Anti-phishing

- Anti-phishing services 1-7
- approved and blocked senders lists 3-8
- email links 3-15
- outbound URL requests 3-15
- URL rating database 3-15

Anti-spam

- Anti-spam engine 3-7
- Anti-spam services 1-7
- approved and blocked senders lists 3-7
- configuration 1-4
- Content Scanning log 3-6
- Keyword Exception List 3-10
- Keyword Exceptions List 3-7
- Network Reputation Services 3-11
 - log 3-6
- Quick IP List 3-10
- Real-Time Blackhole List (RBL) 3-10
- spam detection levels 3-7
- wildcard matching 3-9

Anti-spyware

- Anti-spyware services 1-6
- cleanup template 3-14
- pattern file 3-14
- scan engine 3-14

Antivirus

- ActiveX malicious code 3-12
- Antivirus services 1-6
- COM and EXE file infectors 3-12
- HTML viruses 3-12
- Macro viruses 3-12

Appliance Firmware Flash Utility 15-2

- baseboard management controller 15-1
- BMC 15-1
- detecting an IP address 15-39
- launching from the Solutions CD 15-39
- opening screen 15-39
- user name and password 15-39

Appliance Firmware Flash Utility, opening screen when using option 5 15-24

Appliance Firmware Flash Utility, opening screen, when uploading with option 3 15-18

Appliance Firmware Flash Utility. Also see AFFU.

Auto-switching/sensing capability 14-7

B

- Back panel 1-12
 - AC power receptable 1-12
 - elements 1-12
 - fan vent 1-12
 - port indicator status 1-14
 - port indicators 1-13
 - power switch 1-12
 - showing console (serial) port and management port 15-33
 - showing console port, management port, and INT port 15-8
 - showing location of internal (INT) port 15-16
 - showing location of management port 15-22
 - showing on/off switch 15-13
 - UID LED and UID button 1-12
 - USB ports 1-12
- Backup
 - configuration 13-4, 15-5
 - configuration information 15-6
- Baseboard management controller 15-1
- Bezel
 - front panel 1-9
 - releasing the D-3
- BIOS 15-43
 - checksum field 15-44
 - DC OFF LAN Bypass Configuration 14-8
 - flashing 15-43
 - update 15-40
 - IP range 15-45
 - preparing to upload IGSA BIOS 15-40
 - troubleshooting 15-45
 - uploading the IGSA BIOS firmware 15-41
- BIOS firmware
 - after the upload, IGSA will auto-restart 15-44
 - name of file 15-40
 - upload 15-44
- Blockable file formats F-4
- BMC 15-1, 15-39
 - firmware
 - troubleshooting 15-45
 - update
 - auto-restart of IGSA 15-40
 - CPU fans run at full speed 15-40
 - IP range 15-45
 - troubleshooting 15-45

Bot

- defined 3-2
 - threats 1-3
- Browser support
- Internet Explorer 6.x 1-3
 - Mozilla Firefox 1.x 1-3

C

- CF. See Compact Flash.
- Checklist
 - appliance IP addresses E-1
 - getting started 4-2
- Common Internet media types and subtypes, by category 6-8
- Compact Flash card 15-6
- Components
 - primary functional 3-4
- Compression ratio 14-16
- Compression types, supported F-2
- Configuration Backup 15-5
 - back up current configuration 13-4
 - restore configuration from backup 13-4
 - restore configuration to default settings 13-4
- Configuration Backup screen 15-6
- Connecting to the network
 - EXT port 1-15, 2-20
 - INT port 1-15, 2-20
- CONSOLE port 15-34
- Contact us 1-2
- Contacting Technical Support 14-2
- Content and URL filtering (HTTP traffic) 1-8
- Content filtering in SMTP 5-32
- Control Manager B-1
 - antivirus and content security components B-29
 - Anti-spam rules B-29
 - engines B-29
 - Pattern files/Cleanup templates B-29
 - basic features B-2
 - cluster node B-6
 - components
 - downloading B-29
 - configuring
 - managed products B-15
 - Scheduled Download Exceptions B-38
 - Scheduled Downloads B-39

- creating
 - folders B-22
- Directory Manager B-20
- download components
 - manually B-30
- downloading and deploying components B-29
- enable Scheduled Component Downloads B-39
- folders
 - creating B-22
 - moving B-23
 - renaming B-22
- generating on-demand scheduled reports B-55
- global reports B-46
- local reports B-46
- managed products
 - configuring B-15
 - issue tasks B-16
 - moving B-23
 - renaming B-22
 - searching for B-19
 - viewing logs B-17
 - viewing status B-14
- manually download components B-30
- MCP
 - communication, one-way B-6
 - one-way communication B-5–B-6
 - two-way communication B-5–B-6
- moving
 - folders B-23
 - managed products B-23
- on-demand scheduled reports B-55
- Product Directory B-11
 - deploying components B-14
- renaming
 - folders B-22
 - managed products B-22
- report profiles
 - ActiveX B-48
 - contents B-49
 - creating B-48
 - frequency B-52
 - PDF B-48
 - recipient B-54
 - RPT B-48
 - RTF B-48
 - targets B-51

- report templates B-47
- report types B-46
- reports B-46
 - global B-46
 - local B-46
 - on-demand scheduled B-55
 - report profiles B-48
 - viewing generated reports B-56
- Scheduled Download Exceptions
 - configuring B-38
- Scheduled Downloads
 - configuring B-39
- scheduled reports B-55
- searching
 - managed products B-19
- Temp B-24
- Update Manager B-29
- viewing
 - managed products logs B-17
 - managed products status B-14
 - viewing generated reports B-56
- Control Manager profiles. See Control Manager report profiles.
- Controlling access to the appliance 13-3
- Crossover network cable 14-7

D

- Damage Cleanup 9-7
 - configuring 9-6
- Damage Cleanup Services
 - supported DCS clients C-11
- Databases
 - QIL 3-12
 - RBL 3-12
- DC OFF LAN Bypass Configuration 14-8
- Deferred Scan C-2
- Deployment 2-1
 - Figures
 - fig. 2-01. Typical network topology before deploying InterScan Gateway Security Appliance 2-2
 - fig. 2-02. The most common deployment of InterScan Gateway Security Appliance 2-3
 - fig. 2-03. InterScan Gateway Security Appliance and clients deployed 2-4

-
- fig. 2-04. Problem: The appliance and clients deployed in different network segments, with router as default gateway of the appliance and no static routes set 2-6
 - fig. 2-05. Solution: Static route settings tell the appliance where to forward traffic from clients deployed, even though they are in a different network segment 2-7
 - fig. 2-06. You can set static routes from the Web console (Administration > IP Address Settings, Static Routes tab) 2-8
 - fig. 2-07. In transparent proxy mode, the client's IP address becomes that of the appliance 2-10
 - fig. 2-08. In fully transparent proxy mode, the client's IP address becomes that of the appliance 2-12
 - fig. 2-09. Deployment in a DMZ environment (requires two appliances) 2-13
 - fig. 2-10. Two InterScan appliances arranged in a link state failover deployment 2-15
 - fig. 2-11. Recommended position of InterScan Gateway Security Appliance and other network devices in single- or multi-segment environments 2-17
 - InterScan Gateway Security Appliance is not a firewall or a router 2-2
 - most common deployment scenario 2-3
 - options 2-1
 - Description of InterScan Gateway Security Appliance 1-2
 - Device
 - address checklist E-1
 - connectivity
 - ping 1-16, 2-21
 - testing 1-16, 2-21
 - dimensions and weight G-2
 - image 15-4
 - downloading it from the Trend Micro Web site 15-7
 - update 15-4
 - Device image. See Firmware.
 - Dimensions and weight G-2
 - Disk SMART Test
 - Scheduled disk SMART test, enable 13-8
 - DMZ environment, deploying in 2-13
 - Documentation feedback 1-2
 - E**
 - Email "Remove" Scenarios 8-7
 - Email notifications 14-8
 - Ethernet cable 14-7
 - European Institute for Computer Antivirus Research (EICAR)
 - EICAR test virus 14-13
 - Exported query file examples 10-7
 - EXT port 1-15, 2-20
 - F**
 - Factory default settings 14-7
 - False positives C-3
 - FAQs
 - Can I ping the appliance? 14-7
 - Can I use the USB ports to transfer files? 14-7
 - Is a crossover network cable needed? 14-7
 - RESET Pinhole 14-7
 - What is the purpose of the "ID" LED? 14-7
 - Why am I not receiving email notifications? 14-8
 - Why does quarantine action fail? 14-8
 - Why is traffic not passing through the appliance when power is off? 14-8
 - Will the Appliance still work if the hard disk is not working? 14-7
 - Feature execution order C-12
 - Features and benefits 1-3
 - Feedback, documentation 1-2
 - File Blocking
 - types 3-18
 - File formats, blockable F-4
 - File Handling
 - handling compressed files 14-14
 - handling large files 14-16
 - Firefox 1.x, support for 1-3
 - Firewall
 - InterScan Gateway Security Appliance is not a firewall or a router 2-2
 - traversal support B-4
 - Firmware 15-4
 - update 15-4
 - Firmware Flash Utility 15-38

Firmware Flash Utility. See Appliance Firmware Flash Utility.

Firmware Update

Figures

- fig. 15-01. Back panel of appliance showing console port, management port, and INT port 15-8
- fig. 15-02. HyperTerminal display settings 15-9
- fig. 15-03. The HyperTerminal Connect To screen 15-10
- fig. 15-04. HyperTerminal COM Properties screen 15-11
- fig. 15-05. The appliance Preconfiguration console login screen 15-12
- fig. 15-06. Preconfiguration console main menu, accessed via HyperTerminal 15-12
- fig. 15-07. The appliance back panel showing on/off switch 15-13
- fig. 15-08. The appliance rescue mode main menu 15-14
- fig. 15-09. Preconfiguration console screen that appears when you select option 3 in rescue mode 15-15
- fig. 15-10. The appliance back panel showing location of internal (INT) port 15-16
- fig. 15-11. The appliance Solutions CD splash screen 15-17
- fig. 15-12. The appliance Solutions CD Firmware Flash Utility section 15-18
- fig. 15-13. Trend Micro Appliance Firmware Flash Utility, opening screen, when uploading with option 3 15-18
- fig. 15-14. AFFU opening screen when uploading with option 3, emphasizing Flash DOM 15-19
- fig. 15-15. AFFU DOM screen 15-19
- fig. 15-16. AFFU - browse to device image 15-20
- fig. 15-17. AFFU DOM screen showing progress of the update 15-20
- fig. 15-18. AFFU “flash DOM successfully uploaded” message 15-21
- fig. 15-19. Preconfiguration console screen that appears when you select option 5 in rescue mode 15-22
- fig. 15-20. The appliance back panel showing location of management port 15-22
- fig. 15-21. The appliance Solutions CD splash screen 15-23
- fig. 15-22. The appliance Solutions CD Firmware Flash Utility section 15-24
- fig. 15-23. Trend Micro Appliance Firmware Flash Utility, opening screen when using option 5 15-24
- fig. 15-24. AFFU opening screen when using option 5, emphasizing Flash DOM 15-25
- fig. 15-25. AFFU - Do not click the row displaying the IP address 15-25
- fig. 15-26. AFFU DOM screen 15-26
- fig. 15-27. AFFU - browse to device image file 15-26
- fig. 15-28. AFFU DOM screen showing progress of the update 15-27
- fig. 15-29. AFFU “flash DOM successfully uploaded” message 15-27
- fig. 15-30. HyperTerminal window display as the appliance reboots 15-29
- fig. 15-31. The appliance preconfiguration console login screens, before and after device image update 15-30
- fig. 15-32. Preconfiguration console - Rescue mode main menu 15-31
- fig. 15-33. Back panel of the appliance showing console (serial) port and management port 15-33
- fig. 15-34. HyperTerminal display settings 15-34
- fig. 15-35. The HyperTerminal Connect To screen 15-35
- fig. 15-36. HyperTerminal COM Properties screen 15-36
- fig. 15-37. The appliance Preconfiguration console login screen 15-36
- fig. 15-38. The appliance Preconfiguration console main menu, accessed via HyperTerminal 15-37

-
- fig. 15-39. The appliance Solutions CD splash screen 15-38
 - fig. 15-40. Solutions CD Firmware Flash Utility section 15-38
 - fig. 15-41. Trend Micro Appliance Firmware Flash Utility, opening screen 15-39
 - fig. 15-42. AFFU - BMC information entry screen 15-39
 - fig. 15-43. The appliance Solutions CD splash screen 15-42
 - fig. 15-44. The appliance Solutions CD Firmware Flash Utility section 15-42
 - fig. 15-45. AFFU screen that appears initially 15-43
 - fig. 15-46. AFFU BIOS information entry screen 15-43
 - Firmware update
 - acquiring IP address of appliance BMC 15-39
 - avoiding an IP conflict 15-8
 - back up your configuration 15-5
 - Baseboard Management Controller (BMC) 15-8
 - before updating the device image 15-5
 - BIOS
 - after the upload, IGSA will auto-restart 15-44
 - BIOS update 15-40
 - preparing to upload IGSA BIOS 15-40
 - uploading the IGSA BIOS firmware 15-41
 - BMC 15-37
 - changing the IP address of the local computer 15-8
 - checklist 15-5
 - connecting a local computer to deliver the update 15-7
 - CONSOLE port 15-34
 - getting IP address of local PC 15-12
 - Rescue mode 15-8
 - uploading BMC firmware 15-40
 - uploading device image and keeping existing configuration 15-7
 - uploading device image and restoring default appliance configuration 15-7
 - uploading the BMC firmware 15-37
 - uploading with option 3
 - ensuring that local computer is in same segment 15-8
 - serial port 15-8
 - uploading with option 5 15-8
 - using the LCD module 15-5
 - Flash BIOS 15-43
 - Frequently Asked Questions (FAQ) 14-7
 - Front Panel 1-9
 - 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 7-10
 - configure action 7-10
 - configure spyware/grayware exclusion list 7-9
 - configure target 7-9
 - enable 7-9
 - pass spyware files 7-10
 - scan for all types 7-10
 - scan for specific types 7-10
 - search online for spyware/grayware 7-9
 - select notification recipients 7-11
 - Antivirus
 - allow infected files to pass 7-7
 - block infected files 7-7
 - clean infected files 7-7
 - configure action 7-6
 - configure target 7-4
 - do not scan 50MB+ files 7-6
 - enable 7-2
 - enable deferred scanning 7-6
 - scan all files 7-5
 - scan based on different criteria 7-6
 - scan specified files by extension 7-5
 - scan using IntelliScan 7-5
 - select notification recipients 7-7
 - specify files to scan 7-5

File Blocking

- block selected file types 7-12
- block specified file extensions 7-13
- configure notifications 7-13
- configure target 7-12

scanning support 1-4

FTP - Enable 7-2

FTP > Anti-spyware - Action 7-10

FTP > Anti-spyware - Notification 7-11

FTP > Anti-spyware - Target 7-8

FTP > File Blocking - Notification 7-13

FTP > File Blocking - Target 7-12

FTP > Scanning - Action 7-6

FTP > Scanning - Notification 7-7

FTP > Scanning - Target 7-4

FTP Services

Figures

- fig. 7-01. FTP - Enable 7-2
- fig. 7-02. FTP > Scanning - Target 7-4
- fig. 7-03. Scan Specified Files by Extension 7-5
- fig. 7-04. FTP > Scanning - Action 7-6
- fig. 7-05. FTP > Scanning - Notification 7-7
- fig. 7-06. FTP > Anti-spyware - Target 7-8
- fig. 7-07. Trend Micro Spyware/Grayware Online Database 7-9
- fig. 7-08. FTP > Anti-spyware - Action 7-10
- fig. 7-09. FTP > Anti-spyware - Notification 7-11
- fig. 7-10. FTP > File Blocking - Target 7-12
- fig. 7-11. FTP > File Blocking - Notification 7-13

Fully transparent proxy mode 2-12

G

Getting Started

Figures

- fig. 4-01. Web Console Log On screen 4-3
- fig. 4-02. Summary Screen – First Three Panels 4-5
- fig. 4-03. Update in progress 4-6
- fig. 4-04. Manual Update > Select Components to Update 4-7
- fig. 4-05. Summary Screen – Second Three Panels 4-8

fig. 4-06. Summary Screen – Last Three Panels 4-10

fig. 4-07. SMTP > Scanning (Incoming) > Target – Sample Screen 4-12

fig. 4-10. Online Help system 4-15

fig. 4-11. Online Help – Configuration Screen 4-16

fig. 4-12. Online Help – MORE> Screen 4-17

fig. 4-14. Sample ToolTip mouseover embedded help 4-14

fig. 4-9. Online Help Menu – Contents and Index 4-15

Getting started

Preliminary task list 4-2

Getting started checklist of preliminary tasks 4-2

Getting Started Guide 2-1

H

Hard disk D-5

diskless mode C-2

release lever D-4

releasing the bezel D-3

the hard disk tray D-3

thumb-release clasps D-2

Hardware specifications G-2

Help system 4-15, 4-17

Hot Fixes 14-10

How InterScan Gateway Security Appliance Works 1-5

How the Appliance Works

Figures

fig. 3-01. InterScan Gateway Security Appliance Primary Functional Components 3-4

fig. 3-02. How the RBL and QIL databases work 3-12

HTML viruses 3-12

HTTP

Anti-pharming

allow access to Web site 6-19

block access to Web site 6-19

configure action 6-19

configure Notification 6-19

configure target 6-18

enable 6-18

- Anti-phishing
 - allow access to Web site 6-21
 - block access to Web site 6-21
 - configure action 6-21
 - configure notification 6-22
 - configure target 6-20
 - enable 6-20
- Anti-spyware
 - allow download of spyware 6-16
 - block files with spyware 6-16
 - configure Action 6-16
 - configure Spyware/Grayware Exclusion List 6-15
 - configure target 6-15
 - enable 6-15
 - scan for spyware/grayware 6-16
 - search online for spyware/grayware 6-15
 - select Notification recipients 6-17
- Antivirus
 - block infected files 6-12
 - clean infected files 6-12
 - configure action 6-12
 - configure target 6-6
 - enable 6-3
 - exclude files from scan 6-7
 - maximum file size to scan 6-7
 - pass infected files 6-12
 - scan all files 6-6
 - scan specified files by extension 6-6
 - scan using IntelliScan 6-6
 - select notification recipients 6-13
 - specify files to scan 6-6
- Content and URL filtering 1-8
- File Blocking
 - block selected file types 6-31
 - block specified file extensions 6-31
 - configure target 6-31
 - enable 6-31
 - select notification recipients 6-32
- scanning support 1-4
- URL Filtering
 - configure notification 6-29
 - configure proxy settings 6-28
 - configure settings 6-28
 - configure work time settings 6-28
 - enable proxy settings 6-28
- URL filtering
 - filter selected categories 6-24
- URL Filtering Rules
 - configure Approved URL List 6-26
 - configure Blocked URL List 6-25
 - enable 6-25
 - filter during leisure time 6-25
 - filter during work time 6-25
- HTTP - Enable 6-2
- HTTP > Anti-pharming - Action 6-18
- HTTP > Anti-pharming - Notification 6-19
- HTTP > Anti-pharming - Target 6-18
- HTTP > Anti-phishing - action 6-21
- HTTP > Anti-phishing - Notification 6-22
- HTTP > Anti-phishing - Target 6-20
- HTTP > Anti-spyware - Action 6-16
- HTTP > Anti-spyware - Notification 6-17
- HTTP > Anti-spyware - Target 6-14
- HTTP > File Blocking - Notification 6-31
- HTTP > File Blocking - Target 6-30
- HTTP > Scanning - Action 6-11
- HTTP > Scanning - Target 6-5
- HTTP > URL Filtering - Notification 6-29
- HTTP > URL Filtering – Proxy Settings 6-28
- HTTP > URL Filtering - Settings 6-27
- HTTP > URL Filtering – URL Filtering Rules , bot-
tom half of screen 6-25
- HTTP > URL Filtering – URL Filtering Rules , top
half of screen 6-24
- HTTP Scanning - Notification 6-13

HTTP Services

Figures

- fig. 6-01. HTTP - Enable 6-2
 - fig. 6-02. HTTP > Scanning - Target 6-5
 - fig. 6-03. Scan Specified Files by Extension 6-6
 - fig. 6-04. HTTP > Scanning - Action 6-11
 - fig. 6-05. HTTP Scanning - Notification 6-13
 - fig. 6-06. HTTP > Anti-spyware - Target 6-14
 - fig. 6-07. Trend Micro Spyware/Grayware Online Database 6-15
 - fig. 6-08. HTTP > Anti-spyware - Action 6-16
 - fig. 6-09. HTTP > Anti-spyware - Notification 6-17
 - fig. 6-10. HTTP > Anti-pharming - Target 6-18
 - fig. 6-11. HTTP > Anti-pharming - Action 6-18
 - fig. 6-12. HTTP > Anti-pharming - Notification 6-19
 - fig. 6-13. HTTP > Anti-phishing - Target 6-20
 - fig. 6-14. HTTP > Anti-phishing - Action 6-21
 - fig. 6-15. HTTP > Anti-phishing - Notification 6-22
 - fig. 6-16. HTTP > URL Filtering – URL Filtering Rules , top half of screen 6-24
 - fig. 6-17. HTTP > URL Filtering – URL Filtering Rules , bottom half of screen 6-25
 - fig. 6-18. HTTP URL Filtering > Approved Clients tab 6-26
 - fig. 6-19. HTTP > URL Filtering - Settings 6-27
 - fig. 6-20. HTTP > URL Filtering – Proxy Settings 6-28
 - fig. 6-21. HTTP > URL Filtering - Notification 6-29
 - fig. 6-22. HTTP > File Blocking - Target 6-30
 - fig. 6-23. HTTP > File Blocking - Notification 6-31
- HTTP URL Filtering > Approved Clients tab 6-26
- HyperTerminal 15-34, 15-37
- COM Properties screen 15-11, 15-35–15-36, C-7
- Connect To screen 15-10, 15-35, C-6
- display settings 15-9, 15-34
- window display as the appliance reboots 15-29

I

- INT port 1-15, 2-20, 15-8
- IntelliScan 3-18, 6-6, 7-5
- IntelliScan defined C-10
- IntelliTrap 1-3, 5-16–5-17
 - defined C-10
 - detecting bots in compressed files 3-13
 - Log 3-13
 - virus scan engine 3-13
- Internal outbreak 9-5
- Internet Explorer 6.x, support for 1-3
- Internet threats, types of 3-2
- InterScan Gateway Security Appliance
 - described 1-2
 - features and benefits 1-3
 - How it works 1-5
- InterScan Gateway Security Appliance M-Series Getting Started Guide 2-1
- Introducing
 - Figures
 - fig. 1-1. How InterScan Gateway Security Appliance Works 1-5
 - fig. 1-02. Front Panel 1-9
 - fig. 1-03. LCD Module 1-10
 - fig. 1-04. Back panel 1-12
 - fig. 1-05. Port indicators 1-13
- IP address
 - Anti-spam, exclude from filtering 5-19
 - dynamic or static 1-15, 2-19
 - LCD Module, assigning using 1-15
 - LCD Module, assigning using a 2-19
 - Preconfiguration console, assigning using a 2-19
 - Preconfiguration console, assigning using a terminal communications program 1-15
- IP address of appliance BMC 15-39
- IP address of local PC, obtaining 15-12
- IP address settings
 - add Static route
 - Static route 13-12
 - configure IP address for updates 13-11
 - delete Static route 13-14
 - example of static routes 13-14
 - modify static route 13-13
- IP addresses, checklist E-1
- IP conflict, avoiding while accessing the Preconfiguration console 15-8

L

- LAN bypass 1-14
 - passing traffic if failure occurs C-3
- LCD Module 1-10, 15-5
- LED indicators, behavior of 1-11
- License 13-20, 14-11
 - update manually 13-22
 - view detailed license online 13-21
 - view info about your license 13-21
 - view license renewal instructions 13-21
- Link state failover
 - deployment, illustrated 2-15
- Logs 12-2
 - backing up your configuration 15-6
 - log query, additional screen actions 12-4
 - log settings, configuring 12-5
 - logs in diskless mode, remote machine 12-5
 - Maintenance, automatic 12-7
 - maintenance, manual 12-6
 - querying 12-3
- Logs > Maintenance - Automatic 12-7
- Logs > Maintenance - Manual 12-6
- Logs > Query 12-3
- Logs > Query – HTTP Anti-Pharming Log 12-4
- Logs > Settings 12-5
- Logs screen 12-2

M

- Macro viruses 3-12
- MacroTrap defined C-11
- Malware naming F-6
- Malware naming formats F-6
- Malware types 3-2
- Management port 15-8
- Management port, appliance back panel 15-22
- Manual update 4-6
- Manual Update > Select Components to Update 4-7
- MCP
 - communication
 - two-way B-6
 - understanding B-3

MCP benefits

- HTTPS support B-5
- NAT and firewall traversal B-4
- one-way and two-way communication B-5
- reduced network loading and package size B-3
- MCP. See Management Communication Protocol.
- Management Communication Protocol. See also MCP.
- MIME types, list of common types 6-8
- Mozilla Firefox 1.x, support for 1-3
- My Product Details 13-22

N

- Naming of malware F-6
- NAT 2-2
 - deploy the appliance behind a firewall or security device that provides adequate NAT and firewall-type protection 2-2
- NAT traversal support B-4
- Network Reputation Services
 - Quick IP Lookup (QIL) database 1-4
 - RBL and QIL databases 3-10
 - Real-Time Blackhole List (RBL) 1-4
- Network topology
 - most common 2-2
 - typical network topology before deploying InterScan 2-2
 - typical, with no gateway protection 2-2
- Notification Settings
 - Events, maximum notifications per hour 13-17
 - settings, SMTP administrator email address 13-16
 - settings, SMTP server and Port 13-16
 - settings, SMTP user name and password 13-16
- Notifications
 - inline virus stamp 5-10
 - inline virus-free stamp 5-10
- NRS. See Network Reputation Services.

O

- Obtaining Activation Code 1-16, 2-21
- Obtaining Registration Key 1-16, 2-21
- On/off switch
 - turning off the device 15-37, 15-41
- Online Help – Configuration Screen 4-16
- Online Help – MORE> Screen 4-17

Online Help system 4-15

context-sensitive Help 4-17

Online License Update and Renewal 13-21

Operation modes

fully transparent 2-12

fully transparent or transparent proxy mode 13-18

transparent proxy 2-10

OPP. See Outbreak Prevention Policy.

OPS

red alerts 9-10

yellow alerts 9-10

OPS. See Outbreak Prevention Services.

Outbreak Defense 1-3, 9-2

Current Status screen 9-3

Damage Cleanup Exception List, add
non-Windows clients 9-7

Damage Cleanup Services 9-2

Damage Cleanup, configuring 9-6

Figures

fig. 9-01. Outbreak Defense 9-2

fig. 9-02. Outbreak Defense > Current Status
9-3

fig. 9-03. Outbreak Defense > Internal Out-
break 9-5

fig. 9-04. Outbreak Defense > Damage Clean-
up 9-6

fig. 9-05. Outbreak Defense > Settings - Set-
ting 9-8

fig. 9-06. Outbreak Defense > Settings - Noti-
fication 9-9

internal outbreak 9-5

Internal Outbreak, apply older Outbreak

Prevention Policy 9-5

Outbreak Defense services 1-8

Outbreak Prevention Policy 9-2

Outbreak Prevention Policy, stopping 9-4

Outbreak Prevention Services 9-2

Potential Threat 9-7

Potential Threat, enable Damage Cleanup 9-7

red alerts 9-10

settings

automatic deployment 9-8

configure download frequency 9-9

configure notifications 9-9

enable auto deployment for red alerts 9-8

enable auto deployment for yellow alerts 9-8

yellow alerts 9-10

Outbreak Defense > Current Status 9-3

Outbreak Defense > Damage Cleanup 9-6

Outbreak Defense > Internal Outbreak 9-5

Outbreak Defense > Settings - Notification 9-9

Outbreak Defense > Settings - Setting 9-8

Outbreak Defense Services

ActiveUpdate servers 3-19

Damage Cleanup Services (DCS) 3-20

Outbreak Prevention Policy 3-19

Outbreak Prevention Policy 9-2

P

Password

changing the password 13-20

default password 4-3

entering the password 4-3

recovering a password 14-8

Patches 14-10

Pattern Files

Spam Engine and Pattern File 14-10

Virus Pattern File 14-9

Pharming 6-19

defined 3-2

log 3-16

URL rating database 3-16

Phish

approved and blocked senders lists 3-8

configure action 5-26

defined 3-2

email links 3-15

enable scanning of SMTP traffic for 5-25

notify recipients of 5-27

outbound URL requests 3-15

URL rating database 3-15

Ping 14-7
Ping the appliance 1-16
POP3
 Anti-phishing
 configure action 8-20
 configure target 8-20
 enable 8-20
 select notification recipients 8-21
 stamp subject line 8-21
 Anti-spam
 add approved senders 8-18
 add blocked senders 8-18
 configure action 8-19
 configure target 8-18
 enable 8-18
 select detection level 8-18
 set keyword exceptions 8-18
 Anti-spyware 8-12
 configure action 8-12
 configure spyware/grayware exclusion list 8-11
 configure target 8-10
 delete message and attachment 8-12
 enable 8-10
 pass items 8-12
 remove spyware and pass 8-12
 scan all types 8-12
 scan specific types 8-12
 search online for spyware/grayware 8-11
 select notification recipients 8-13
 send message and quarantine attachment 8-12
 Antivirus
 clean infected items and pass 8-6
 configure action 8-6
 configure target 8-4
 enable 8-2
 exclude by different criteria 8-5
 Quarantine 8-6
 remove infected items 8-6–8-7
 scan all files 8-5
 scan specified files by extension 8-5
 scan using IntelliScan 8-5
 select Notification recipients 8-8
 specify files to scan 8-5
 virus detected notification 8-9
 virus free notification 8-9
 Content Filtering
 configure action 8-25
 configure target 8-24
 delete message and attachments 8-25
 deliver message and attachments 8-25
 enable 8-24
 filter by attachment True Type 8-24
 filter by message attachment 8-24
 filter by message size 8-24
 filter by text in body 8-24
 filter by text in header 8-24
 Quarantine email and attachments 8-25
 select notification recipients 8-26
 IntelliTrap
 configure action 8-15
 delete message and attachment 8-15
 deliver message and deleted infected item 8-15
 detect and pass 8-15
 enable 8-14
 Quarantine 8-15
 select notification recipients 8-16
 scanning support 1-4
POP3 > Anti-phishing - Action 8-20
POP3 > Anti-phishing - Notification 8-21
POP3 > Anti-phishing - Target 8-20
POP3 > Anti-spam - Action 8-19
POP3 > Anti-spam - Target 8-17
POP3 > Anti-spyware - Action 8-12
POP3 > Anti-spyware - Notification 8-13
POP3 > Anti-spyware - Target 8-10
POP3 > Content Filtering - Action 8-25
POP3 > Content Filtering - Notification 8-26
POP3 > Content Filtering - Target 8-23
POP3 > IntelliTrap - Action 8-15
POP3 > IntelliTrap - Notification 8-16
POP3 > IntelliTrap - Target 8-14
POP3 > Scanning - Action 8-6
POP3 > Scanning - Notification 8-8
POP3 > Scanning - Target 8-4
POP3- Enable 8-2

POP3 Services

Figures

- fig. 8-01. POP3- Enable 8-2
- fig. 8-02. POP3 > Scanning - Target 8-4
- fig. 8-03. Scan Specified Files by Extension 8-5
- fig. 8-04. POP3 > Scanning - Action 8-6
- fig. 8-05. POP3 > Scanning - Notification 8-8
- fig. 8-06. POP3 > Anti-spyware - Target 8-10
- fig. 8-07. Trend Micro Spyware/Grayware On-line Database 8-11
- fig. 8-08. POP3 > Anti-spyware - Action 8-12
- fig. 8-09. POP3 > Anti-spyware - Notification 8-13
- fig. 8-10. POP3 > IntelliTrap - Target 8-14
- fig. 8-11. POP3 > IntelliTrap - Action 8-15
- fig. 8-12. POP3 > IntelliTrap - Notification 8-16
- fig. 8-13. POP3 > Anti-spam - Target 8-17
- fig. 8-14. POP3 > Anti-spam - Action 8-19
- fig. 8-15. POP3 > Anti-phishing - Target 8-20
- fig. 8-16. POP3 > Anti-phishing - Action 8-20
- fig. 8-17. POP3 > Anti-phishing - Notification 8-21
- fig. 8-18. POP3 > Content Filtering - Target 8-23
- fig. 8-19. POP3 > Content Filtering - Action 8-25
- fig. 8-20. POP3 > Content Filtering - Notification 8-26

Port indicator status 1-14

Port indicators 1-13

Ports

- console (serial) port 15-33
- console port 15-8
- EXT port 1-13, 1-15
- INT 1-15
- INT port 1-13, 15-8
- management port 1-13, 15-8, 15-22, 15-33
- serial 15-33
- status indicators 1-14

Power requirements and environmental specifications G-3

Power switch

- turning off the device 15-41

Preconfiguration console 15-4

- change default password 15-36
- default password 15-36
- Interface Settings screen C-9
- login screen 15-12, 15-36, C-7
- login screens, before and after device image update 15-30
- main menu, accessed via HyperTerminal 15-12, 15-37, C-8
- output screen when initializing a hard disk that is not formatted or is improperly installed (the second part of the re-initialization process) 14-5
- output screen when the appliance has finished formatting the hard disk 14-5
- preparing 15-9, 15-34, C-5
- Rescue mode main menu 15-31
- screen that appears when you select option 3 in rescue mode 15-15
- screen that appears when you select option 5 in rescue mode 15-22

Preconfiguration console output screen when the appliance has finished formatting the hard disk 14-5

Preliminary tasks 4-2

Primary Functional Components

- Anti-pharming URL rating database 3-16
- Anti-phishing Services 3-15
- Anti-spam Services 3-6
- anti-spyware services 3-14
- Antivirus Services 3-12
- Content Filtering Services 3-6
- Ethernet Network Interfaces 3-4
- File Blocking 3-17
- IntelliTrap Services 3-13
- Outbreak Defense Services 3-19
- quarantine 3-21
- Real-Time Scan of protocols 3-5
- URL filtering 3-16
- Web console 3-5

Product License 13-20

- enter new activation code 13-23
- update license manually 13-22
- view detailed license online 13-21
- view info about your license 13-21
- view license renewal instructions 13-21

Product License - New Activation Code 13-23

Product License screen 13-20

Program file 15-4

update 15-4

Program file. See Firmware.

Proxy modes 13-18

fully transparent 2-12

Proxy settings 13-24

configure proxy settings 13-24

use a proxy server 13-24

Q

QIL database 3-12

QIL. See Quick IP List.

Quarantine

maximum number of messages in 14-8

maximum size of message in 14-8

total size of 14-8

Quarantine > Maintenance - Automatic 10-10

Quarantine > Maintenance - Manual 10-9

Quarantine query files – example contents 10-8

Quarantine Query Results 10-5

Quarantine query, exported files 10-7

Quarantines

exporting query results list to comma-delimited

file 10-5

Figures

fig. 10-01. Quarantines screen 10-2

fig. 10-02. Quarantines > Query 10-4

fig. 10-03. Quarantine Query Results 10-5

fig. 10-04. Quarantine > Maintenance - Manual
10-9

fig. 10-05. Quarantine > Maintenance - Auto-
matic 10-10

maintenance

automatic 10-10

delete all files 10-9

delete files older than x days 10-9

enable automatic purge 10-10

manual 10-9

maximum message limit 10-2

quarantine query 3-21

query

delete messages from query results list 10-5

example of exported query file 10-8

execute query 10-5

select criteria 10-4

query results list 10-5

viewing contents of exported file 10-7

Quarantines > Query 10-4

Quarantines screen 10-2

Query logs 12-3

Quick IP List (QIL) 3-10

R

RBL and QIL databases 3-10

RBL database 3-12

RBL. See Real-Time Blackhole List.

Readme.txt

reading enclosed readme documents 14-3

Real-Time Blackhole List (RBL) 3-10

Reboot

HyperTerminal window display as the appliance

reboots 15-29

Reboot screen 13-30

Red Alerts 9-10

Reference

Figures

fig. C-02. The HyperTerminal Connect To
screen C-6

fig. C-03. HyperTerminal COM Properties
screen C-7

fig. C-04. The appliance Preconfiguration con-
sole login screen C-7

fig. C-05. The appliance Preconfiguration con-
sole main menu, accessed via HyperTermi-
nal C-8

Registration Key

obtaining 1-16, 2-21

Removing the Hard Disk

Figures

- fig. D-01. Thumb-release clasps D-2
- fig. D-02. Releasing the bezel D-3
- fig. D-03. The hard disk tray D-3
- fig. D-04. Hard disk release lever D-4
- fig. D-05. InterScan Gateway Security Appliance hard disk D-5

Rescue mode

- main menu 15-14

Reset 14-7

RESET Pinhole 14-7

RJ-45 14-7

Router

- InterScan Gateway Security Appliance is not a firewall or a router 2-2

S

Sample ToolTip mouseover embedded help 4-14

Scan Engine Technology C-10

- IntelliScan defined C-10
- IntelliTrap defined C-10
- MacroTrap defined C-11
- WormTrap defined C-11

Scan Specified Files by Extension 5-6, 6-6, 7-5, 8-5

Scheduled Downloads B-38

Segments

- deploying in multisegment network 2-17
- deploying in single-segment network 2-17

Service Packs 14-10

Simple Network Management Protocol (SNMP)

- SNMP Settings, enable 13-26

SMTP

Anti-phishing

- configure action 5-26
- enable 5-25
- select notification recipients 5-27

Anti-spam

- enable 5-22
- exclude IP address from filtering 5-19
- select detection level 5-22

Anti-spam (content scanning)

- configure action 5-24
- configure target 5-22

Anti-spam Network Reputation Services (NRS)

- configure action 5-20
- configure target 5-19
- QIL 5-21
- Real-Time Blackhole List (RBL) 5-20

Anti-spyware

- choose action when spyware detected 5-14
- configure Action 5-14
- configure exclusion list 5-12
- configure Target 5-12
- delete 5-14
- enable 5-12
- pass 5-14
- quarantine 5-14
- remove spyware/grayware and pass 5-14
- select notification recipients 5-15

Antivirus

- clean infected items and pass 5-7
- configure action 5-7
- configure targets 5-5
- enable 5-3, 5-5
- files to exclude 5-6
- inline virus notification stamps 5-10
- inline virus-free notifications stamp 5-10
- pass all items 5-8
- quarantine 5-7
- remove infected items 5-8
- scan all files 5-5
- scan files by extension 5-5
- select notification recipients 5-10
- use IntelliScan 5-5

content filtering

- configure action 5-31
- configure target 5-30
- select notification recipients 5-32

IntelliTrap

- configure action 5-16
- configure target 5-16
- select notification recipients 5-17

scanning support 1-4

SMTP services described 5-2

Spyware/grayware, online search 5-12

SMTP - Enable 5-3

SMTP > Anti-phishing - Action 5-26

SMTP > Anti-phishing - Notification 5-27

SMTP > Anti-phishing - Target 5-25

SMTP > Anti-spam (Network Reputation Services) - Action 5-20

SMTP > Anti-Spam (Network Reputation Services) - Target 5-18

SMTP > Anti-spam > Content Scanning - Action 5-23

SMTP > Anti-spam > Content Scanning - Target 5-22

SMTP > Anti-spyware - Action 5-13

SMTP > Anti-spyware - Notification 5-14

SMTP > Anti-spyware - Target 5-11

SMTP > Content Filtering - Action 5-31

SMTP > Content Filtering - Target 5-29

SMTP > Contenting Filtering - Notification 5-32

SMTP > IntelliTrap - Action 5-16

SMTP > IntelliTrap - Notification 5-17

SMTP > IntelliTrap - Target 5-15

SMTP > Scanning (Incoming) - Action 5-7

SMTP > Scanning (Incoming) - Notification 5-9

SMTP > Scanning (Incoming) - Target 5-5

SMTP > Scanning (Incoming) > Target – Sample Screen 4-12

SMTP email "Remove" scenarios 5-8

SMTP Services

Figures

- fig. 5-01. SMTP - Enable 5-3
- fig. 5-02. SMTP > Scanning (Incoming) - Target 5-5
- fig. 5-03. Scan Specified Files by Extension 5-6
- fig. 5-04. SMTP > Scanning (Incoming) - Action 5-7
- fig. 5-05. SMTP > Scanning (Incoming) - Notification 5-9
- fig. 5-06. SMTP > Anti-spyware - Target 5-11
- fig. 5-07. Trend Micro Spyware/Grayware Online Database 5-12
- fig. 5-08. SMTP > Anti-spyware - Action 5-13
- fig. 5-09. SMTP > Anti-spyware - Notification 5-14
- fig. 5-10. SMTP > IntelliTrap - Target 5-15
- fig. 5-11. SMTP > IntelliTrap - Action 5-16
- fig. 5-12. SMTP > IntelliTrap - Notification 5-17

- fig. 5-13. SMTP > Anti-Spam (Network Reputation Services) - Target 5-18
- fig. 5-14. SMTP > Anti-spam (Network Reputation Services) - Action 5-20
- fig. 5-15. SMTP > Anti-spam > Content Scanning - Target 5-22
- fig. 5-16. SMTP > Anti-spam > Content Scanning - Action 5-23
- fig. 5-17. SMTP > Anti-phishing - Target 5-25
- fig. 5-18. SMTP > Anti-phishing - Action 5-26
- fig. 5-19. SMTP > Anti-phishing - Notification 5-27
- fig. 5-20. SMTP > Content Filtering - Target 5-29
- fig. 5-21. SMTP > Content Filtering - Action 5-31
- fig. 5-22. SMTP > Contenting Filtering - Notification 5-32

SNMP settings 13-26

- configure SNMP settings 13-27

Solutions CD 15-38, 15-42

Firmware Flash Utility 15-38

Firmware Flash Utility section 15-18, 15-24, 15-38, 15-42

splash screen 15-17, 15-23, 15-38, 15-42

Spam

- anti-spam engine 3-7
- approved and blocked senders lists 3-7
- configure scanning of SMTP for 5-24
- configure target (SMTP traffic) 5-22
- defined 3-2
- detection levels 3-7
- excluding IP address from filtering (SMTP) 5-19
- Keyword Exceptions List 3-7
- Network Reputation Services 5-21
- real-time blackhole list 5-20
- scan SMTP traffic for 5-22
- select detection level for SMTP traffic 5-22
- wildcard matching 3-9

Spam. See Anti-spam.

Specifications, hardware G-2

Spyware 6-16–6-17

- allowing it through 5-14
- block files with spyware 6-16
- cleanup template 3-14
- configure SMTP exclusion list 5-12
- configure target for (SMTP) 5-12
- consequences 3-14
- defined 3-2
- enable scanning of SMTP traffic for 5-12
- exclusion list 6-15
- grayware 3-14
- pattern file 3-14
- quarantine 5-14
- removing (SMTP traffic) 5-14
- scan engine 3-14
- scan HTTP for spyware/grayware 6-16
- select people to notify of 5-15

Spyware. See Anti-spyware.

Spyware/Grayware Online Database 7-9, 8-11

Spyware/grayware, online search 5-12

SSO. See Single Sign-on.

Static route settings, illustrated 2-7

Static route settings, Web console 2-8

Static routes 13-13–13-14

Static Routes – Multiple Segment Network 13-14

Submit potential threat URL to TrendLabs 14-18

Summary Screen 4-4

- Anti-spam Content Scanning 4-10
- Anti-spam Network Reputation Services 4-11
- Anti-spyware 4-9
- Antivirus 4-8
- component version 4-6
- components, manually updating 4-6
- Damage Cleanup Services 4-5
- IntelliTrap 4-9
- others 4-11
- Outbreak Prevention Services (OPS) 4-5
- reset all counters 4-11

Summary Screen – First Three Panels 4-5

Summary Screen – Last Three Panels 4-10

Summary Screen – Second Three Panels 4-8

Switch

- turning off the device 15-37, 15-41

System Time 13-28

- configure NTP Server 13-27

T

Tasks, preliminary 4-2

Technical Support, contacting 14-2

Technology Reference

Figures

fig. C-01. Preconfiguration console Interface

Settings screen C-9

Testing device connectivity

browse the Web 1-16, 2-21

ping 1-16, 2-21

Thumb-release clasps D-2

ToolTip, sample 4-14

Topology

most common network topology 2-2

typical network topology before deploying

InterScan 2-2

Transparent proxy mode 2-10, 13-18

Traversal support

NAT and firewall B-4

Trend Micro InterScan Gateway Security Appliance

M-Series Getting Started Guide 2-1

Trend Micro Spyware/Grayware Online Database

5-12, 6-15, 7-9, 8-11

TrendLabs

submitting potential threat URL to 14-18

Trojans defined 3-2

Troubleshooting

[Error] No Connection 14-4

Figures

fig. 14-01. Preconfiguration console output screen when initializing a hard disk that is not formatted or is improperly installed (the second part of the re-initialization process) 14-5

fig. 14-02. Preconfiguration console output screen when the appliance has finished formatting the hard disk 14-5

fig. 14-03. Compression ratio 14-16

HyperTerminal 14-4

power switch 14-4

quarantine 14-8

True File Type Identification (IntelliScan) 7-5

True File Type identification (IntelliScan) C-10

U

Update

- configure Update Source 11-6
- manual update 11-3
- manual update, select components to update 11-3
- manually 4-6
- rollback 11-4
- rollback, select components for rollback 11-4
- scheduled update, enable 11-5
- scheduled update, select components to update 11-5
- scheduled, specify update duration and frequency 11-5
- select components to update 4-6

Update > Manual 11-3

Update > Scheduled 11-4

Update > Source 11-6

Update Appliance Components

Figures

- fig. 11-01. Update screen 11-2
- fig. 11-02. Update > Manual 11-3
- fig. 11-03. Update > Scheduled 11-4
- fig. 11-04. Update > Source 11-6

Update in progress 4-6

Update screen 11-2

Update source 11-6

URL

- allowable categories 3-16
- Content and URL filtering 1-8
- file blocking 1-4
- filtering log 3-17
- Website filtering 1-4

URL filtering 1-4

V

Virus map 13-32

Virus Scan Module

IntelliScan 3-18

Virus tracking 13-32

Virus. See Antivirus.

Viruses defined 3-2

VT100J 15-34

W

Web console

- accessing the console 4-3
- interface components 4-13
- Log On screen 4-3
- logout link 4-13
- navigating the console 4-12
- navigation menu 4-13
- Online Help 4-13
- password, entering the 4-3
- working area 4-13

Web console Firmware Update screen 13-9

Web Console Log On screen 4-3

Wildcard matching 3-9

Windows 13-4

Windows Save Dialog 13-4

World Virus Tracking 13-31

- participating in program 13-31
- viewing Trend Micro Virus Map 13-32

Worms defined 3-2

WormTrap defined C-11

Y

Yellow Alerts 9-10

