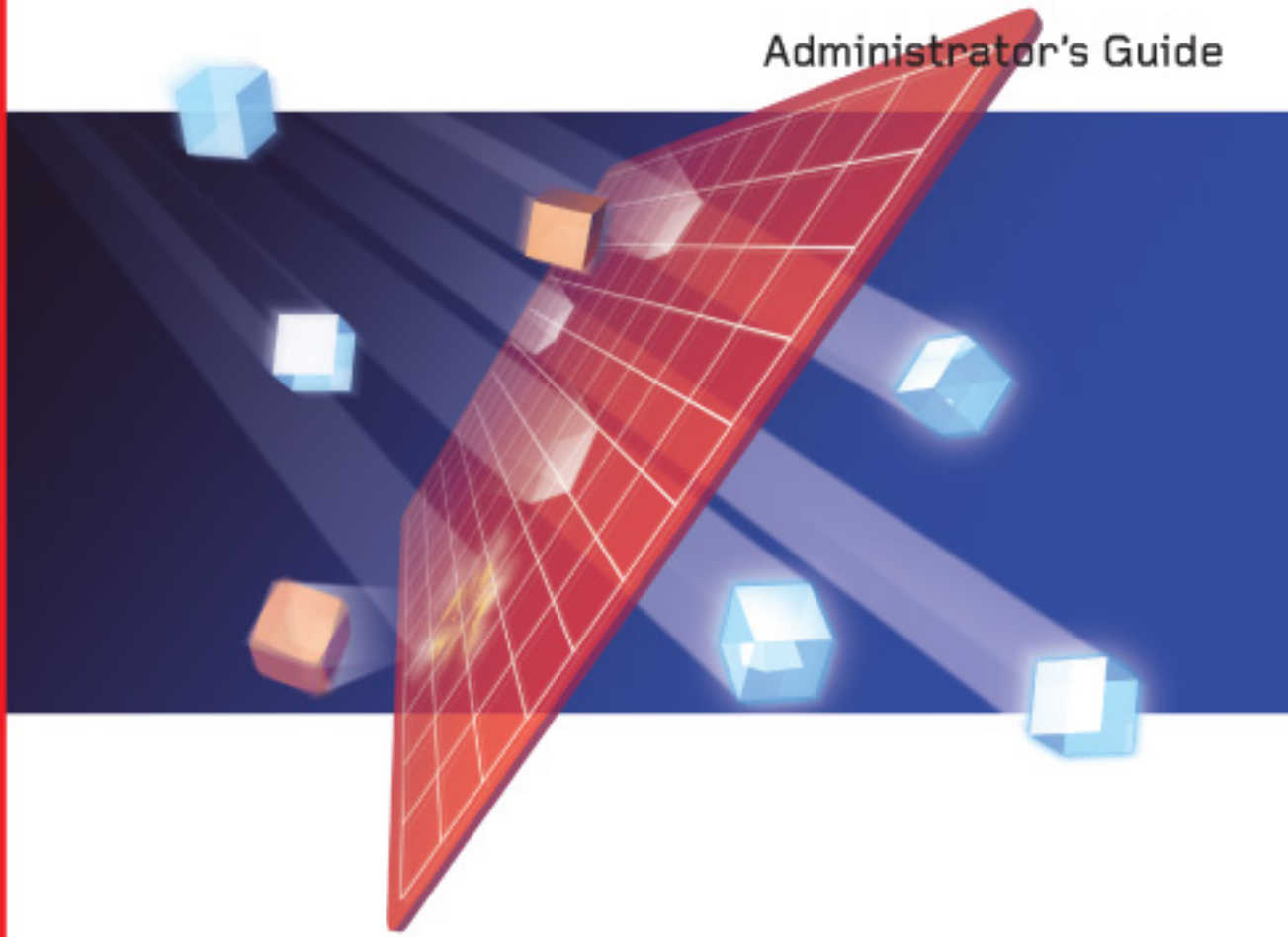
TREND MICRO™
InterScan™ Web Security Suite 3

Antivirus and Content Security at the Web Gateway

for LINUX™

Administrator's Guide



TREND MICRO™

Document Part No. IHEM32859/60920

Release Date: February 2007

Protected by U.S. Patent No. 5,951,698

The Administrator's Guide for Trend Micro is intended to provide in-depth information about the main features of the software. You should read through it prior to installing or using the software.

For technical support, please refer to the Technical Support and Troubleshooting chapter for information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any 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

Preface

Chapter 1: Introducing InterScan Web Security Suite

HTTP and FTP Security Risk Overview 2
Major InterScan Web Security Suite Benefits 2
- Comprehensive Web Security 2
- Centralized Management and Coordination 3
- Scalable and Flexible 3
- Anti-phishing 3
- Anti-spyware 3
- Integration with ICAP 1.0-compliant Caching Devices 4
- Leading Virus Protection 4

Main Features 5
What's New 7
IWSS Architecture 14
- Main Components 14
- Main Services 14
- Scheduled Tasks 15

Chapter 2: Updates

About ActiveUpdate 18
- Updating From the IWSS Console 18

Proxy Settings for Updates 18
Updatable Program Components 20
- Virus Pattern File 21
- PhishTrap Pattern File 22
- Spyware/Grayware Pattern File 22
- Scan Engine 23
- URL Filtering Database 25
- Component Version Information 26

Manual Updates 27
- Forced Manual Updates 27

Scheduled Updates 27

Maintaining Updates 29
Verifying a Successful Update 29
Update Notifications 29
Rolling Back an Update 29
Deleting Old Pattern Files 30
Controlled Virus Pattern Releases 30

Chapter 3: HTTP Settings

Configuring Proxy Scan Settings 34
Proxy Examples 34
Other Proxy-related Settings 41
Configuring Access Control Settings 43
Identifying Clients and Servers 43
Client IP 43
Server IP White List 45
Destination Port Restrictions 46
HTTPS Ports 48
Enabling the HTTP Traffic Flow 50

Chapter 4: Policies and User Identification Method

How Policies Work 52
Default Global and Guest Policies 53
Deploying Policies 54
Configuring the User Identification Method 54
IP Address 55
Host Name 56
User/Group Name Via Proxy Authorization 58
Configuring the Scope of a Policy 65
Using IP Address 66
Using Host Name 67
Using User/group Name via Proxy Authorization 69
Login Accounts 71
About Access Rights 71
Adding a Login Account 71
Changing a Login Account 72
Audit Log File 72

Chapter 5: Configuring HTTP Scanning and Applet/ActiveX Security

Enabling HTTP Scanning and Applets and ActiveX Security 74
HTTP Scanning Performance Considerations 75
Creating and Modifying HTTP Virus Scanning Policies 76
HTTP Virus Scanning Rules 77
Spyware and Grayware Scanning Rules 89
Setting the Scan Action for Viruses 91
Java Applet and ActiveX Security 94
How Applets and ActiveX Security Works 95
Step 1. Filtering Applets & ActiveX at the Server 95
Step 2. Instrumenting Java Applets 96
Step 3. Optionally Re-signing Instrumented Applets 97
Step 4. Monitoring Instrumented Applet Behavior 97
Enabling Applet/ActiveX Security 98
Adding and Modifying Applet/ActiveX Scanning Policies 98
Applet and ActiveX Settings 108
Java Applet Signature Validation 108
Applet Re-signing 110
ActiveX Signature Validation 111
Managing Digital Certificates for Applet Processing 112
Client Side Applet Security Notifications 116

Chapter 6: Access Quotas and URL Access Control

Introduction to Access Quota Policies 120
Managing Access Quota Policies 120
URL Access Control 124
Configuring Trusted URLs 124
Blocking URLs 127
Via Pattern File (PhishTrap) 131

Chapter 7: URL Filtering

Introducing URL Filtering 136
URL Filtering Workflow 137
Managing URL Filtering Policies 139
Enabling URL Filtering 139
Creating a New Policy 139
Modifying and Deleting Policies 142

URL Filtering Settings 144
Requesting URL Re-classification and URL Lookup 144
URL Filtering Exceptions 146
Work and Leisure Schedule Settings 149

Chapter 8: FTP Scanning

Introduction 152
FTP Settings 152
Proxy Settings 152
Passive and Active FTP 153
Client Requests 153
FTP Scanning Options 154
Enabling FTP Traffic and FTP Scanning 154
Scan Direction 155
File Blocking 155
File Scanning 155
Compressed File Handling 156
Large File Handling 156
Encrypting Quarantined Files 157
Scanning for Spyware/Grayware 157
Configuring FTP Scanning Settings 157
Setting Scan Actions on Viruses 160
FTP Access Control Settings 161
By Client IP 161
Via Server IP White List 163
Via Destination Ports 164

Chapter 9: Reports, Logs and Notifications

Introduction to Reports 166
Types of Reports 166
Report Settings 168
Report Scope (Users and Groups) 169
Report Type (Consolidated or Individual) 169
Options 169
Additional Report Settings 169
Generating Reports 170
Real-time Reports 170

Scheduled Reports 175
Customizing Reports 178
Introduction to Logs 180
Querying and Viewing Logs 180
Deleting Logs 186
Log Settings 187
Log File Naming Conventions 189
Exporting Log and Report Data as CSV Files 191
Introduction to Real-time Statistics 191
Virus and Spyware Trend Display 191
Hard Drive Display 192
Bandwidth Usage Display 192
CPU Usage Display 193
Physical Memory Usage Display 194
Introduction to Notifications 194
Email Notification Settings 195
Notification Tokens/Parameters 196
Configuring Notifications 197
SNMP Trap Notifications 208

Chapter 10: IntelliTunnel Security

Protocols Used in Instant Messenging and Authentication Connections 212
About Instant Messenger Protocol 212
About Authentication Connection Protocols 212
Editing an IntelliTunnel Policy 213
Creating a New IntelliTunnel Policy 213

Appendix A: Mapping File Types to MIME Content-types

Appendix B: Configuration Files

Protocol Handlers 222
Scanning Modules 223

Appendix C: OpenLDAP Reference

OpenLDAP Server Side Configuration 226
Software Package Dependencies 226

Configuration Files 226
Tools 231
Customized Attribute Equivalence Table Configuration 234
LDIF Format Sample Entries 236
Sample Configuration 237

Glossary

Index

Preface

Welcome to the *Trend Micro™ InterScan Web Security Suite Administrator's Guide* for release 3.0 of InterScan Web Security Suite (IWSS). This guide provides detailed information about all IWSS configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, configuring scanning, configuring URL blocking and filtering, and using logs and reports.

This preface discusses the following topics:

- *IWSS Documentation* on page x
- *Audience* on page x
- *Document Conventions* on page xi

IWSS Documentation

In addition to the *Trend Micro™ InterScan Web Security Suite Administrator's Guide*, the documentation set for IWSS includes the following:

- Installation Guide (with deployment information)—this guide helps you get "up and running" by introducing IWSS, assisting with installation planning, implementation, and configuration, and describing the main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.
- Online help—the purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the IWSS management console.
- Readme file—this file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.

  The latest versions of the Installation Guide, Administrator's Guide and readme file are available in electronic form at:

  `http://www.trendmicro.com/download/`

- Knowledge Base— the Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://kb.trendmicro.com`

Audience

The InterScan Web Security Suite documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP and POP3 protocols
- Message transfer agents (MTAs)

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

Document Conventions

To help you locate and interpret information easily, the IWSS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Introducing InterScan Web Security Suite

This chapter introduces InterScan Web Security Suite and how it helps to ensure your organization's gateway security.

Topics in this chapter include the following:

- Introducing how InterScan Web Security Suite protects against HTTP and FTP security risks
- Introducing the main InterScan Web Security Suite benefits, its main features and what's new in the latest version
- Explaining the InterScan Web Security Suite program architecture and the main program components, services and scheduled tasks

HTTP and FTP Security Risk Overview

Web traffic exposes corporate networks to many potential security risks. While most computer viruses enter organizations through messaging gateways, Web traffic is an increasingly common infection vector for new security risks. For example, "mixed risks," which take advantage of multiple entry points and vulnerabilities, can use HTTP to spread.

Significant assessment, restoration, and lost productivity costs associated with outbreaks can be prevented. InterScan Web Security Suite is a comprehensive security product that protects HTTP and FTP traffic in enterprise networks from viruses and other risks.

In addition to antivirus scanning, InterScan Web Security Suite also helps with other network security issues. The URL filtering module enables blocking URLs of Web site content prohibited by your organization's acceptable use policies. The PhishTrap™ pattern file helps to protect against phishing, which is the fraudulent collection of personal information through sending counterfeit email messages purportedly from financial institutions or other organizations. Applets and ActiveX security helps to reduce the risk of malicious mobile code by checking digital signatures at the HTTP gateway, and monitoring applets running on clients for prohibited operations.

Major InterScan Web Security Suite Benefits

Trend Micro InterScan Web Security Suite offers powerful protection for your organization's HTTP and FTP gateway traffic.

Comprehensive Web Security

InterScan Web Security Suite is designed to block Web-based risks, including viruses, Trojans, worms, phishing attacks, and spyware. These risks attack corporate networks through Web-based email and Web pages that contain hidden malicious code. IWSS protects against these risks by scanning HTTP and FTP traffic—vectors left vulnerable by SMTP security solutions. This dedicated HTTP/FTP solution delivers better security and faster throughput, for an improved Web browsing experience.

Centralized Management and Coordination

IT administrators can easily manage InterScan Web Security Suite along with other Trend Micro products within a centralized management console, Trend Micro Control Manager™. Control Manager provides a unified view of Trend Micro software installations across the enterprise. Activities can be centrally managed, and policies can be applied to all layers of security at the same time. You can view real-time or scheduled reports with enhanced graphs and charts. The end result: you can deploy an immediate, coordinated response to block any emerging risk.

Scalable and Flexible

InterScan Web Security Suite supports a standalone configuration whereby it acts as a proxy server or integrates with existing proxy servers and ICAP-compliant caching servers from Cisco, Network Appliance, and others. InterScan Web Security Suite also supports several LDAP directories, enabling IT managers to set policies and assign rules for single PCs or groups. You can schedule and automate routine tasks such as virus pattern and URL filtering database updates.

Anti-phishing

Trend Micro anti-phishing technology is designed to block transmission of outbound data to known phishing-related Web sites—an innovative approach to protect against Internet scams. As a result, InterScan Web Security Suite helps stop phishers from stealing personal and confidential corporate information.

Anti-spyware

Trend Micro's anti-spyware technology is designed to block spyware and adware, plus hacking and remote access tools that could harm the network. This added security helps prevent intruders from collecting personal or corporate information, passwords, email addresses, and other data. It also frees system resources and available bandwidth, improving network performance and reducing spyware-associated system failures.

Integration with ICAP 1.0-compliant Caching Devices

Cache servers help moderate Web traffic congestion and save bandwidth. The "retrieve once, serve many" methodology employed by cache servers permits integration with third-party applications such as virus scanning via IWSS. An open protocol, Internet Caching Acceleration Protocol (ICAP), allows seamless coupling of caching and virus protection.

Leading Virus Protection

Built on Trend Micro's award-winning antivirus technology, InterScan Web Security Suite is serviced 24x7 by the advanced technical team at TrendLabs^{SM}. These engineers monitor virus activity, deliver outbreak prevention policies, and provide updated pattern files, which helps companies minimize outbreak-related costs and damage.

Main Features

The following InterScan Web Security Suite features help you maintain HTTP and FTP gateway security.

HTTP Virus Scanning

InterScan Web Security Suite scans the HTTP traffic flow to detect viruses and other security risks in uploads and downloads. HTTP scanning is highly configurable—for example, you can set the types of files to block at the HTTP gateway and how InterScan Web Security Suite scans compressed and large files to prevent performance issues and browser timeouts. In addition, InterScan Web Security Suite scans for many types of spyware, grayware and other risks.

Applets and ActiveX Security

To manage potential security issues in mobile code downloads from the Internet, IWSS can block or allow Java applets and ActiveX controls. InterScan Web Security Suite includes its own certificate store to manage trusted and flagged certificates used to sign Java applets.

In addition, InterScan Web Security Suite can instrument Java applets so their operations are monitored while they run in client browsers. If a prohibited operation is performed, then the client is notified and prompted to allow or deny the operation.

URL Filtering

IWSS compares requested URLs against entries in the URL filtering database. The URL filtering database categorizes Web sites. Policies are then configured to either allow or deny access to these categories during work or leisure time.

If the requested URL cannot be found in the URL filtering database, IWSS supports querying a remote classification server for information about the URL. Exceptions can be configured to allow access even though the URL is classified into a prohibited content category.

Access Quota Policies

To set limits on client Web browsing, InterScan Web Security Suite allows configuring access quota policies. Clients can surf the Web up to their daily, weekly

or monthly limit, after which further browsing is blocked until the configuration interval expires.

URL Access Control

InterScan Web Security Suite can reduce your server's scanning workload by not scanning content trusted URLs. Likewise, InterScan Web Security Suite can refuse requests to access content retrieved from trusted URLs in order to prevent server resources from scanning content that you want to keep out of your organization (URL blocking).

IP Address, Host Name and LDAP Client Identification

InterScan Web Security Suite supports configuring policies for HTTP virus scanning, Applets and ActiveX security, URL filtering and access quotas. The scope of policies can be configured using client IP address, host name or LDAP user or group name.

Server and Port Access Control Restrictions

To increase the security of the InterScan Web Security Suite server, access control lists limit server access to clients that you specify. Likewise, port access can be blocked to reduce the chance of access for malicious purposes.

FTP Scanning

In addition to scanning FTP uploads and downloads, InterScan Web Security Suite can block file types at the FTP gateway. To prevent performance issues, the FTP scanning module supports special configurations for compressed files and large files. Spyware and grayware scanning is also supported.

InterScan Web Security Suite FTP scanning can be deployed into your environment in conjunction with another FTP proxy server or InterScan Web Security Suite can act as its own FTP proxy. And to help ensure the security of the InterScan Web Security Suite server, several security-related configurations are available to control access to the InterScan Web Security Suite server and its ports.

Reports and Logs

To provide current information about your HTTP and FTP gateway security, IWSS is pre-configured to generate many types of blocking-event reports, traffic reports,

spyware/grayware reports and cleanup reports. Reports can be generated on-demand or scheduled on a daily, weekly or monthly basis. Log and report data can be exported to comma-separated value (CSV) files for further analysis. A scheduled task deletes older logs from the server, to prevent logs from consuming excessive disk space.

Notifications

InterScan Web Security Suite can issue several types of notifications in response to program or security events. Administrator notifications are sent via email to the designated administrator contacts. User notifications are presented in the requesting client's browser. Both administrator and user notifications can be customized.

To work with network management tools, InterScan Web Security Suite can also issue notifications as SNMP traps.

Support for Multiple InterScan Web Security Suite Installations

The method to fully administer multiple IWSS servers from a single console is done through TMCM. However, if multiple IWSS servers are configured to access the same database server, then policies (URL, applets and ActiveX, IntelliTunnel, access quota policies, etc.) are shared between all the servers.

The "master"/"slave" designation from the Server Farm page in the Web console only specifies how dynamic data (list of temporarily blocked URLs and list of client IP addresses suspected of spyware infection) is shared between multiple IWSS servers.

Reports and logs show a consolidated view of all IWSS servers on your network.

What's New

This section describes the new features found in InterScan Web Security Suite 3.0.

Easier Collection of System Information for Postmortem Diagnosis

Collection of logging and configuration information for IWSS, as well as general system information for the server on which IWSS is installed, can now be

accomplished through the IWSS Web interface. The **Generate System Information File** button of the **Support (System Information Files)** screen allows you to collect this snapshot of IWSS system information at the click of a button. See the online help for complete details

True File-type Blocking Within Compressed Files

IWSS applies file-type blocking to the contents of a compressed file, such as a zip file. Therefore, a policy meant to block executables will also block any zip file that contains an executable.

IntelliTunnel

IWSS uses IntelliTunnel technology to block undesirable instant messaging (IM) and authentication connection protocols tunneled across port 80. It uses a dynamically, updatable pattern file to distinguish normal browser traffic from other protocols communicating over port 80. Currently, the pattern file can identify three popular types of IM traffic when this traffic is tunneled through port 80.

Direct URL Filter Category Selection

IWSS includes a database that contains URLs in over 60 categories, such as "gambling," "games," and "personals/dating."

Categories are contained in the following logical groups:

- Computers/Bandwidth
- Computers/Harmful
- Computers/Communication
- Adult
- Business
- Social
- General

You can select all the categories of a specific group, or you can browse through the categories that comprise a group and select only certain categories.

Spyware/Grayware Detection and Cleaning

Spyware/grayware presents two main problems to administrators of enterprise networks—it can compromise sensitive company information and reduce employee productivity by causing infected machines to malfunction. In addition to detecting and blocking incoming files that may install spyware, IWSS can prevent installed spyware from sending confidential data via HTTP.

If a client tries to access a URL classified as spyware, disease vector, or virus accomplice by the PhishTrap pattern, or a client PC uploads a virus classified as a worm as a Web mail attachment, IWSS can send a request to Trend Micro™ Damage Cleanup Services (DCS) to clean the infected machine. DCS reports the outcome of the cleaning attempt (either successful or unsuccessful) to the InterScan Web Security Suite server.

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

Note: To avoid excessive cleanup attempts, IWSS only sends requests to cleanup a target IP once every four hours by default. If the client at that IP continues to perform suspicious actions, then no further cleanup requests will be issued until this lockout period has expired. You can modify the length of this lockout period by changing `[Scan-configuration]/infected_url_block_length` in the `intscan.ini` file. The value in this field is interpreted as the number of hours, and partial values (such as 0.5) are supported.

URL Lookup

If you want to know a category of a URL, you can look it up when specifying URL filtering settings.

Note: An *unrated* URL is a Web site that Trend Micro knows about but has not yet put into a filtering category.

An *unknown* URL is a Web site that is one of the following:
- Unknown to Trend Micro

- A Web site that is not in the local database
- The daemon may be down or the remote rating server is inaccessible to give the URL a rating

An *unknown* URL has a rating of zero (0) and cannot be blocked.

Real-time Reports and Alerts

IWSS includes dynamic reports, where the administrator can view the "real-time" statistics of the IWSS system. These reports include the following:

- Hard Drive
- Bandwidth
- Concurrent Connections
- CPU Usage
- Physical Memory Usage

Virus and Spyware Trend is a static report that is generated when you open the Summary (System Dashboard tab) page. This report is not updated over time like the other reports.

These reports are displayed as charts and tables on the new system dashboard within IWSS.

Configurable Threshold Warning

You can now set a warning when the database size exceeds a specified threshold.

FTP Proxy Enhancements

FTP scanning can be optionally configured to scan uploads and/or downloads. In addition FTP traffic can be scanned for spyware/grayware, and access control lists can be configured to control access to FTP servers based upon client IP address, server IP address or destination port.

MIME-type Verification Before Skipping Scanning

To improve data throughput rates, IWSS can be configured to skip scanning files of MIME-types that present a low risk of harboring viruses. However, since MIME types can be easily forged, IWSS verifies that a file really is a certain MIME-type

through true file type checking. Small files that would otherwise not be scanned due to their MIME type are always scanned.

Configurable Deferred Scanning

To scan files passing through the HTTP gateway for security risks, IWSS needs to accumulate data on the server before forwarding it to the ultimate recipient. When scanning large files, or in slow network traffic environments, the delay in fulfilling the browser's request may be long enough to cause a browser timeout. IWSS supports "deferred scanning", whereby part of a requested page is passed to the browser while scanning is in progress to prevent the browser from timing out.

Note: When deferred scanning is enabled, IWSS will drop the connection when it detects malware, resulting in a partial file creation. For binary file types, (example: exe, dll) and most archive file types (example: .zip, .jar, .cab), the partial file will not be executable or extractable, making it harmless.

There is a remote chance that a script file (example: .js, .htm) that contains a malicious script can still be compiled, even though it is only a partial file. In this case, the malware can harm your system. Also, since script files are plaintext, IWSS may detect signatures in these partial files, giving you the impression that there is a virus leak. This condition can trigger other antivirus products to detect the signatures. While IWSS drops the connection once the malicious signature is detected, another antivirus products may scan the partial and signal an alert, even if that partial file is harmless.

Java Applet and ActiveX Security

To help stop malicious Java applets and ActiveX objects at the HTTP gateway, IWSS supports configuring policies to specify the types of mobile code allowed to pass to your clients. Applets and ActiveX objects can either be blocked or allowed to pass to clients based on their certificate status. Java applet instrumentation allows an executing applet to be monitored with precise control. If an applet attempts to perform operations not allowed by policy, a notification message is presented in the client's browser.

User and Group Policy Configuration

IWSS supports flexible policy configuration for all of the HTTP scanning and blocking features. The scope of a policy can be set by specifying the clients' IP address, host name or an LDAP directory's user/group name. Administrators retain precise control and flexibility for setting security policy.

IWSS supports integrating with Microsoft Active Directory 2000 and 2003, Linux OpenLDAP Directory 2.2.17 and Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server). Multiple domains are supported, so users from other trusted domains can authenticate through IWSS.

Trusted and Blocked URL Lists

To improve performance when browsing Web sites, IWSS supports configuring a "trusted URL" list. Trusted URLs can be exempt from scanning and filtering. By default, IWSS scans trusted URLs. However, in the Trusted URLs screen, you can change this default.

IWSS includes the following default list of trusted URLs:

- http://windowsupdate.microsoft.com
- http://v5.windowsupdate.microsoft.com
- http://v4.windowsupdate.microsoft.com
- http://download.windowsupdate.com
- http://windowsupdate.com
- http://update.microsoft.com

IWSS can also block access to specific URLs. Requests to access blocked URLs are rejected, without scanning the content.

SNMP System and Event Notifications

To work with third-party network monitoring tools, InterScan Web Security Suite supports sending several types of notifications as SNMP traps. InterScan Web Security Suite sends traps for security risk detections, security violations, program and pattern file updates and service disruptions.

Reverse Proxy Support

IWSS is usually installed close to clients to protect them from security risks from the Internet. However, InterScan Web Security Suite also supports being installed as a reverse proxy to protect a Web server from having malicious programs uploaded to it. As a reverse proxy, IWSS is installed close to the Web server that it protects. IWSS receives clients requests, scans all content and then redirects the HTTP requests to the real Web server.

Notifications

To keep you informed about the status of your gateway security, InterScan Web Security Suite supports sending notifications in response to a wide variety of security and program events. There are two types of notifications—administrator notifications are sent via email to the designated administrative contact(s) and user notification messages are displayed in the requesting client's browser.

Logs and Reports

IWSS includes many pre-configured reports to provide a summary of your gateway security status. Reports can be run for a specific time period and customized to only provide information about clients that you're interested in. There are four main classes of reports:

- Blocking event reports
- Traffic reports
- Spyware/grayware reports
- Cleanup reports.

Reports are generated from information written to logs. InterScan Web Security Suite writes log information to a database and text log files, or only to the database. To prevent unneeded log information from consuming excessive disk space, old logs are deleted on-demand or on schedule.

X-Authenticated ICAP Headers Support

InterScan Web Security Suite 3.0 supports X-Authenticated ICAP Headers that are provided by supported ICAP clients, such as NetCache (5.6.2R1) and Blue Coat (SGOS 4.2.1.1). The X-Authenticated Headers comes in two forms: X-Authenticated-User and X-Authenticated-Groups. The advantage of using

X-Authenticated Headers is two-fold: first, it reduces LDAP query overhead in IWSS and second, it allows ICAP clients to provide LDAP searches on LDAP servers with different schemas.

IWSS Architecture

InterScan Web Security Suite includes several required and optional modules, depending upon the functions used. The following summarizes the main modules and services. Additionally, many types of scheduled tasks are set up during installation.

Main Components

The following are the main InterScan Web Security Suite modules:

- Main Program: Installs the management console and the basic library files necessary for InterScan Web Security Suite.
- HTTP Scanning: Installs the services necessary for HTTP scanning (either ICAP or HTTP scanning) and URL blocking.
- FTP Scanning: Installs the service that enables FTP scanning.
- URL Filtering: Installs the service necessary for URL filtering.
- Applets and ActiveX Scanning: Installs the service necessary for checking Java applet and ActiveX object digital signatures, and instrumenting applets so their execution can be monitored for prohibited operations.
- SNMP Notifications: Installs the service to send SNMP traps to SNMP-compliant network management software.
- Control Manager Agent for InterScan Web Security Suite: Installs the files necessary for the Control Manager agent to enable monitoring and configuration through Control Manager.

Main Services

The following services are used by IWSS:

- Trend Micro InterScan Web Security Suite Console (`java`): This service is the Web server hosting the Web management console.

- Trend Micro InterScan Web Security Suite for FTP (`isftpd`): This service enables the FTP traffic flow and FTP virus scanning.
- Trend Micro InterScan Web Security Suite for HTTP (`iwssd`): This service enables the HTTP traffic flow and HTTP scanning (including FTP over HTTP). It also handles Applets and ActiveX security processing.
- Trend Micro IWSS Log Import (`logtodb`): This service writes logs from text files to the database.
- Trend Micro IWSS Notification Delivery Service (`isdelvd`): This service handles administrator notifications (via email) and user notifications (via browser).
- Trend Micro SNMP Service (`svcmonitor` if using the Linux SNMP agent, `snmpmonitor` if using the IWSS-installed SNMP agent): This service sends SNMP trap notifications to SNMP-capable network monitoring devices.
- Trend Micro Control Manager Service (`En_Main`): This service permits IWSS configuration and status reporting through Trend Micro Control Manager, if you are using Control Manager.
- Trend Micro InterScan Web Security Suite for Dashboard (`ismetricmgmtd`): This service collects system resource data to be used in the display of real-time dashboard metrics.
- Trend Micro InterScan Web Security Suite for URL Filtering (`isurld`): This service enables URL filtering.

Scheduled Tasks

When installing IWSS, the setup program creates several scheduled tasks.

- purgefile: Runs daily at 2:00 A.M. to delete old text log files, subject to the configured time interval to retain logs.
- schedulereport: Runs hourly to check if a scheduled report is configured to run.
- schedulepr_update: Runs daily to check if it is time to update the product registration/license.
- schedule_au: Runs every 15 minutes to check if it is time to update the pattern file or other program components.
- cleanfile: Runs hourly, to remove temporary files downloaded for scan-behind or large file scanning.

- DbOldDataCleanup.sh: Runs daily at 2:05 A.M. to clean up old reporting log data in the database and cleans up the old access quota counters in the database.
- svc_snmpmonitor.sh: Runs every 5 minutes to check if the watchdog/SNMP daemon is up.
- db_reindex.sh: Runs daily at 28 minutes past every other hour to rebuild corrupted database indices containing any invalid data. This maintains optimum database performance.
- db_vacuum.sh: Runs daily at 3:58 A.M. to perform garbage collection to free up unused space from database tables in order to maintain optimum database performance.

Chapter 2

Updates

Because new malicious programs and offensive Web sites are developed and launched daily, it is imperative to keep your software updated with the latest pattern files, scan engine, URL filtering database, and URL filtering database engine.

Topics in this chapter include the following:

- Introducing Trend Micro's ActiveUpdate feature
- Explaining how to update program components via the native IWSS management console or through Trend Micro Control Manager
- Configuring proxy settings to enable Internet connectivity for updates
- Describing program components that need to be updated
- Getting version information about components being used by IWSS
- Invoking manual (on-demand) and scheduled updates
- Forcing a manual update to overwrite components on the IWSS server
- Verifying a successful update
- Rolling back to previous versions of pattern files or the scan engine
- Applying controlled pattern releases

About ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of pattern files, the scan engine, the URL filtering database, and the URL filtering database engine.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on-demand.

Updating From the IWSS Console

If you are not using Trend Micro Control Manager (TMCM) for centralized administration of your Trend Micro products, IWSS will poll the ActiveUpdate server directly. Updated components are deployed to IWSS on a schedule you define, such as:

- Minutes (15, 30, 45, 60)

  These 15-minute interval updates only apply to virus, spyware, PhishTrap, and IntelliTunnel.
- Weekly
- Daily
- Hourly
- On-demand

Note: Trend Micro recommends hourly update of the pattern files, and weekly update of the scan engine and URL filtering database.

Proxy Settings for Updates

If you use a proxy server to access the Internet, you must enter the proxy server information into the IWSS management console before attempting to update. Any proxy information that you enter is used for both updating components from Trend Micro's update servers and for product registration and licensing.

To configure a proxy server for component and license updates:

1. Open the IWSS management console and click **Updates > Connection Settings**.
2. Select **Use a proxy server for pattern, engine, and license update** to specify a proxy server or port.
3. If your proxy server requires authentication, type a user ID and password in the fields provided.

   Leave these fields blank if your proxy server does not require you to authenticate.
4. In the **Pattern File Setting** section, type the number of pattern files to keep on the InterScan Web Security Suite server after updating to a new pattern (default and recommended setting = 3 pattern files).

   Keeping old pattern files on your server allows you to roll back to a previous pattern file in the event of an incompatibility with your environment, for example, excessive false positives. When the number of pattern files on the server exceeds your configuration, the oldest pattern file will be automatically deleted.
5. Click **Save**.

FIGURE 2-1 Configure proxy settings for update and license renewal in the Connection Settings screen

Updatable Program Components

To ensure up-to-date protection against the latest risks, there are several components to update:

- IntelliTunnel signature definition file: This file contains "signatures" of certain HTTP interactions (such as instant messaging protocols tunneled through HTTP and SSL authentication requests) which you may wish to control. New signature definition files are typically released several times a year as the covered protocols evolve or new types of HTTP interactions are added. See Chapter 10, *IntelliTunnel Security*.

  Note: The IntelliTunnel feature is unrelated to VSAPI and uses its own scanning engine, which is not dynamically updatable.

- Virus, spyware/grayware and PhishTrap pattern files: These are the files that contain the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, IWSS is able to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the PhishTrap and grayware/spyware pattern files are updated less frequently.
- Scan engine: This is the module that analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.
- URL filtering database: This is a database that categorizes Web sites according to their content. IWSS compares requested URLs against the URL filtering database to determine whether the page request should be blocked according to the URL filtering policy rules.
- URL filtering database engine: Trend Micro utilizes the TMUFE URL filtering engine to perform categorization based on the TMUFE database. Trend Micro recommends updating the TMUFE URL filtering database frequently in order to have the latest categorization data. The URL filtering database engine uses this data.

Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly pernicious risk is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature (see *About ActiveUpdate* starting on page 18 for details) can detect whenever a new virus pattern is available at the server, and/or can be scheduled to automatically poll the server every hour, day, week, and so on to get the latest file. Virus pattern files can also be manually downloaded from the following Web site:

`http://www.trendmicro.com/download/pattern.asp`

where you can find the current version, release date, and a list of the new virus definitions included in the file.

How it Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary "signature" or string of tell-tale characters that distinguishes it from any other code, the virus experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the virus pattern file looking for a match.

Pattern files use the following naming format:

`lpt$vpn.###`

where ### represents the pattern version (for example, 400). To distinguish a given pattern file with the same pattern version and a different build number, and to accommodate pattern versions greater than 999, the IWSS management console displays the following format:

`roll number.pattern version.build number (format: xxxxx.###.xx)`

- `roll number`—this represents the number of rounds when the pattern version exceeded 999 and could be up to five digits
- `pattern version`—this is the same as the pattern extension of `lpt$vpn.###` and contains three digits

- `build number`—this represents the patch or special release number and contains two digits

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (typically several times per week), and recommends configuring a daily automatic update on the **Updates > Schedule** screen. Updates are available to all Trend Micro customers with valid maintenance contracts.

Note: There is no need to delete the old pattern file or take any special steps to "install" the new one.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire 7 or 8MB pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software and deploy pattern files throughout your environment.

PhishTrap Pattern File

As new "phishing" scams that attempt to steal personal data through counterfeit versions of legitimate Web sites are discovered, Trend Micro collects their URLs and incorporates the information into the PhishTrap pattern file. The PhishTrap pattern file is saved in `/etc/iscan/phishB.ini` and contains an encrypted list of known phishing URLs.

Spyware/Grayware Pattern File

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their telltale signatures and incorporates the information into the spyware/grayware pattern file. The spyware/grayware pattern file, is stored in the following:

`/etc/iscan/ssaptn.###`

where ### represents the pattern version. This format distinguishes a given pattern file with the same pattern version and a different build number. It also accommodates pattern versions greater than 999. The IWSS management console displays the following format:

`roll number.pattern version.build number (format: xxxxx.###.xx)`

- `roll number`—this represents the number of rounds when the pattern version exceeded 999 and could be up to five digits
- `pattern version`—this is the same as the pattern extension of `tmaptn.###` and contains three digits
- `build number`—this represents the patch or special release number and contains two digits

Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. Originally developed in response to the first computer viruses the world had seen, the scan engine today is exceptionally sophisticated. It is capable of detecting Internet worms, mass-mailers, Trojan horse risks, network exploits and other risks, as well as viruses. The scan engine detects the following types of risks:

- "in the wild," or actively circulating
- "in the zoo," or controlled viruses that are not in circulation, but are developed and used for research and "proof of concept"

In addition to having perhaps the longest history in the industry, the Trend Micro scan engine has also proven in test after test to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway. Rather than scan every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where the virus would hide. If a virus is detected, it can be removed and the integrity of the file restored.

The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help minimize bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes and scans common compression formats,

including Zip, Arj, and Cab. Most Trend Micro products also allow administrators to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file.

It is important that the scan engine remain current with the latest risks. Trend Micro ensures this in two ways:

1. Frequent updates to the scan engine's data-file, called the virus pattern file, which can be downloaded and read by the engine without the need for any changes to the engine code itself
2. Technological upgrades in the engine software prompted by a change in the nature of virus risks, such as the rise in mixed risks like SQL Slammer

In both cases, updates can be automatically scheduled, or an update can be initiated on-demand.

The Trend Micro scan engine is certified annually by international computer security organizations, including the International Computer Security Association (ICSA).

About Scan Engine Updates

By storing the most time-sensitive virus information in the virus pattern file, Trend Micro is able to minimize the number of scan engine updates while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- New scanning and detection technologies have been incorporated into the software
- A new, potentially harmful virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:

`http://www.trendmicro.com`

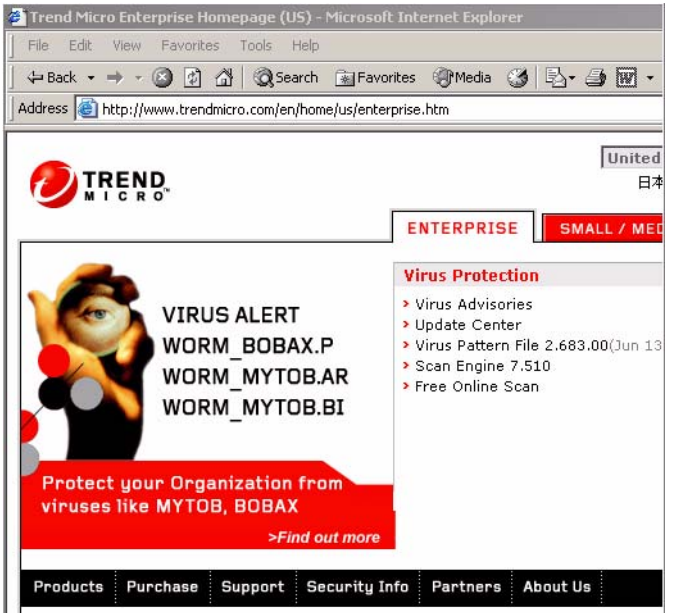


FIGURE 2-2 Current scan engine version on http://www.trendmicro.com

URL Filtering Database

The URL database is updated with the latest categorization of Web pages. IWSS enables you to create URL filtering policies by selecting categories directly, such as "adult content," "games," and "gambling."

To help the administrator manage the categories, IWSS displays them in the following URL groups:

- Computers/Bandwidth
- Computers/Harmful
- Computers/Communication
- Adult
- Business
- Social

- General

You can select all categories in a group or just individual categories within a group.

You can update the URL database manually or automatically (either daily or weekly).

Note: If you feel that a URL has been mis-categorized in the URL filtering database, you can submit the URL for re-classification by choosing **HTTP > URL Filtering > Settings > URL Re-classification & Lookup**.

Component Version Information

To know which pattern file, scan engine, URL filtering database or program build you are running, click **Summary** in the main menu. The version in use is shown in the **Current Version** column on the **Scanning** tab.

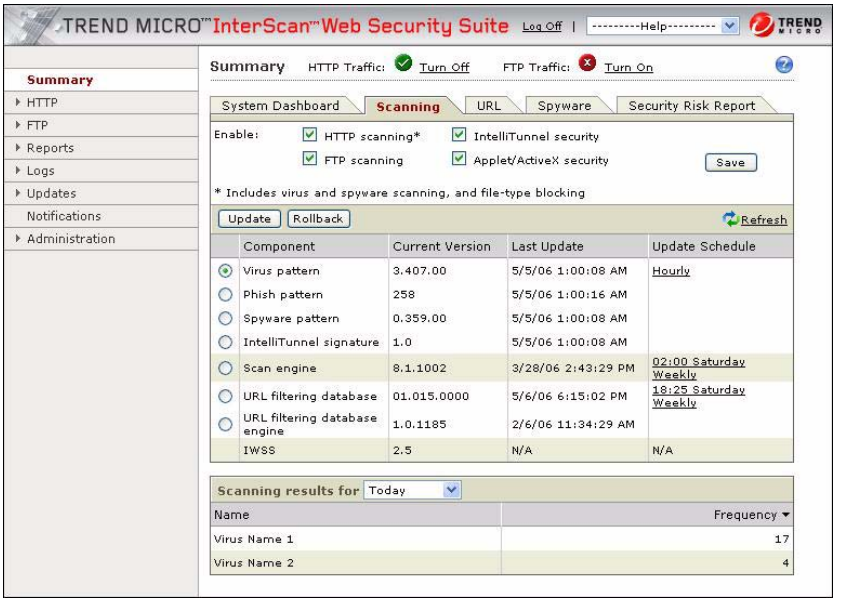


FIGURE 2-3 Pattern file, scan engine and other component version information on the Summary page

Manual Updates

To manually update pattern files, the scan engine or URL filtering database:

1. Click **Summary** in the main menu.
2. On the **Scanning** tab of the **Summary** page, select the component to update and click **Update**. A progress bar displays to indicate the update progress, and a message screen displays the outcome of your update attempt.

Forced Manual Updates

IWSS provides an option to force an update to the pattern file and the scan engine when the version on the IWSS server is greater than or equal to its counterpart on the remote download server (normally IWSS would report that no updates are available). This feature is useful when a pattern file or scan engine is corrupt and you need to download the component again from the update server.

To force an update of a pattern file or scan engine:

1. Click **Summary** in the main menu.
2. Select the component to update and then click **Update**. A message box displays if the version of the pattern file or scan engine on the IWSS server is greater than or equal to the counterpart on the remote download server. If the pattern file on the IWSS server is older than the one on the remote download server, the newer pattern file is downloaded.
3. Click **OK** in the message box to start the forced update.

Scheduled Updates

To schedule automatic pattern file, scan engine and URL filtering database updates:

1. Click **Updates > Schedule** from the main menu.
2. For each type of updatable component, select the update interval. The following are your options:
   - Every *x* minutes (pattern files only; select the number of minutes between update interval)
   - Hourly (pattern files only)

- Daily
- Weekly (select a day from the drop-down menu; this is the recommended setting for scan engine and URL filtering database updates)

Note: Scheduled updates for a given component can be disabled by selecting **Manual updates only** under the components section.

3. For each component, select a **Start time** for the update schedule to take effect.
4. Click **Save**.

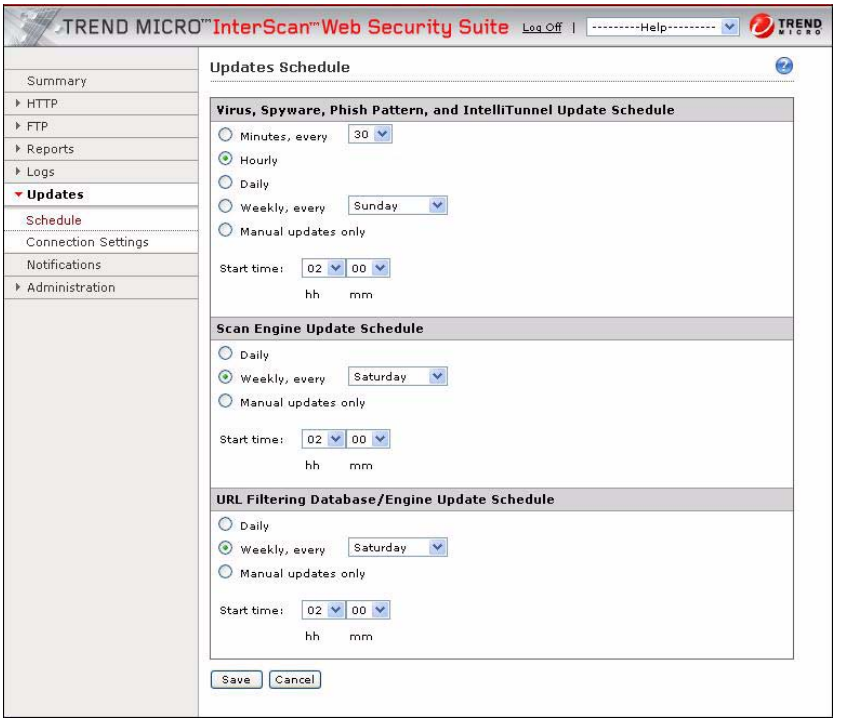


FIGURE 2-4 Configure scheduled updates for the pattern files, scan engine, URL filtering database, and URL filtering database engine

Note: Use the **Summary** screen in the IWSS management console to verify the current version of the virus pattern file. Trend Micro recommends that you flush the cache and reboot the NetCache appliance and Blue Coat Port 80 Security Appliance after updating the virus pattern file to ensure that no viruses are being cached. Consult your Netcache appliance and your Blue Coat Security Appliance documentation for instructions on how to clear the cache and reboot.

Maintaining Updates

Verifying a Successful Update

The **Scanning** tab of the **Summary** page in the IWSS management console displays the version of the component in use, plus the time and date of the last update. Check the Summary page (see Figure 2-3 on page 26) to verify that a manual or scheduled update has completed successfully.

Update Notifications

IWSS can issue notifications to proactively inform an administrator about the status of a pattern file, URL filtering database or scan engine update. For more information about configuring update-related notifications, see *Pattern File Updates* starting on page 206, and *Scan Engine Updates* starting on page 206.

Rolling Back an Update

IWSS checks the program directory and uses the latest pattern file and engine library file (`libvsapi.so`) to scan inbound/outbound traffic. It can distinguish the latest pattern file by its file extension; for example, `lpt$vpn.401` is newer than `lpt$vpn.400`.

Occasionally, a new pattern file may incorrectly detect a non-infected file as a virus infection (known as a “false alarm”). You can revert to the previous pattern file or engine library file.

To roll back to a previous pattern file or scan engine:

1. Click **Summary** in the main menu. The **System Dashboard** tab displays by default.
2. Click the **Scanning** tab.
3. Select the component to roll back and click **Rollback**. A progress bar indicates the rollback progress, and a message screen then displays the outcome of the rollback. After the rollback, you can find the current version and date of the last update on the **Scanning** tab of the **Summary** screen.

Deleting Old Pattern Files

After updating the pattern file, IWSS keeps old pattern files (Virus and Spyware pattern files) on the server so they're available to roll back. The number of pattern files kept on the server is controlled by the **Number of pattern files to keep** setting on the **Updates > Connection Settings** page (see Figure 2-1 on page 19).

If you need to manually delete pattern files, they can be found in the `/etc/iscan/` directory of IWSS.

Controlled Virus Pattern Releases

There are two release versions of the Trend Micro virus pattern file:

- The Official Pattern Release (OPR) is Trend Micro's latest compilation of patterns for known viruses. It is guaranteed to have passed a series of critical tests to ensure that customers get optimum protection from the latest virus risks. Only OPRs are available when Trend Micro products poll the ActiveUpdate server.
- A Controlled Pattern Release (CPR) is a pre-release version of the Trend Micro virus pattern file. It is a fully tested, manually downloadable pattern file, designed to provide customers with advanced protection against the latest computer viruses and to serve as an emergency patch during a virus risk or outbreak.

To apply the latest CPR to IWSS:

1. Open http://www.trendmicro.com/download/pattern-cpr-disclaimer.asp and click **Agree** to signify your agreement with the terms and conditions of using a Trend Micro CPR.

2. Download the CPR to a temporary folder on the IWSS server. The file name will be in the form lptXXX.zip.
3. Stop all the IWSS services.
4. Extract the contents of the files that you downloaded to the `/etc/iscan/`directory of IWSS.
5. Restart all IWSS services.

To verify that the CPR was applied correctly, click **Summary** in the main menu and confirm that the virus pattern version in use corresponds to the version of the CPR that you tried to apply.

Note: Once you apply a CPR, incremental updates will not be possible. This means that subsequent updates will require downloading the entire pattern file rather than just the new patterns, resulting in a slightly longer pattern download time.

In order for IWSS to access the new pattern file, ensure that it has the same permission and ownership as the previous pattern file.

Chapter 3

HTTP Settings

Before you can start using IWSS to scan for malicious HTTP downloads, filter or block URLs and apply access quotas for your clients, you need to configure some HTTP settings that control the HTTP traffic flow. IWSS can be used in conjunction with another proxy server on your network; alternatively, you can configure IWSS to use its native proxy.

Topics in this chapter include:

- Configuring IWSS as a forward proxy to scan content downloaded via HTTP, either stand-alone or in conjunction with another proxy
- Configuring IWSS as a reverse proxy to scan content uploaded to a Web server from clients
- Using IWSS in conjunction with a Layer 4 switch or router to avoid the need to adjust client Internet connection settings
- Configuring access control settings to control HTTP access by the client's IP address
- Adding "trusted" servers to the Server IP White List
- Configuring destination port restrictions
- Enabling the HTTP traffic flow

Configuring Proxy Scan Settings

There are two general ways whereby IWSS can be used to protect your users and network resources from HTTP-borne risks—as a forward proxy and as a reverse proxy. In both configurations, IWSS resides between the clients and a Web server.

- Forward proxy: This configuration is used to protect clients from receiving malicious HTTP-borne risks from a server. This is the most common configuration, and the typical use case is to protect Web users on your network from receiving malicious Internet downloads. In the forward proxy topology, IWSS and the clients that it protects are typically installed within the same LAN.
- Reverse proxy: This configuration interposes IWSS between a Web server and the clients of that server. This is a less common configuration, and a use case is to protect Web servers from having malicious content uploaded to them. In the reverse proxy topology, IWSS is typically installed closer to the Web server that it protects and is separated from the clients by the Internet.

Proxy Examples

There are several types of proxy configurations, as listed below:

- No Upstream Proxy (stand-alone mode)
- Upstream Proxy (dependent Mode)
- Simple transparency
- Reverse proxy

An example of each type of proxy follows.

No Upstream Proxy (Stand-alone Mode)

The simplest configuration is to install IWSS in stand-alone mode, with no upstream proxy. In this case, IWSS acts as a proxy server for the clients. Advantages of this configuration are its relative simplicity and that there is no need for a separate proxy server. A drawback of a forward proxy in stand-alone mode is that each client must configure the InterScan Web Security Suite server as their proxy server in their browser's Internet connection settings. This requires cooperation from your network users, and also makes it possible for users to exempt themselves from your organization's security policies by re-configuring their Internet connection settings.

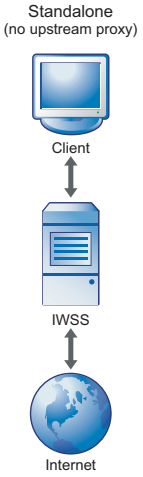


FIGURE 3-1 Forward, no upstream proxy

To configure a stand-alone installation:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Ensure that **Forward proxy** is enabled, and **Enable upstream proxy** and **Enable transparency** are not selected.
3. Click **Save**.

Note: If you configure InterScan Web Security Suite to work in standalone mode, each client on your network needs to configure Internet connection settings to use the IWSS server and port (default 8080) as their proxy server.

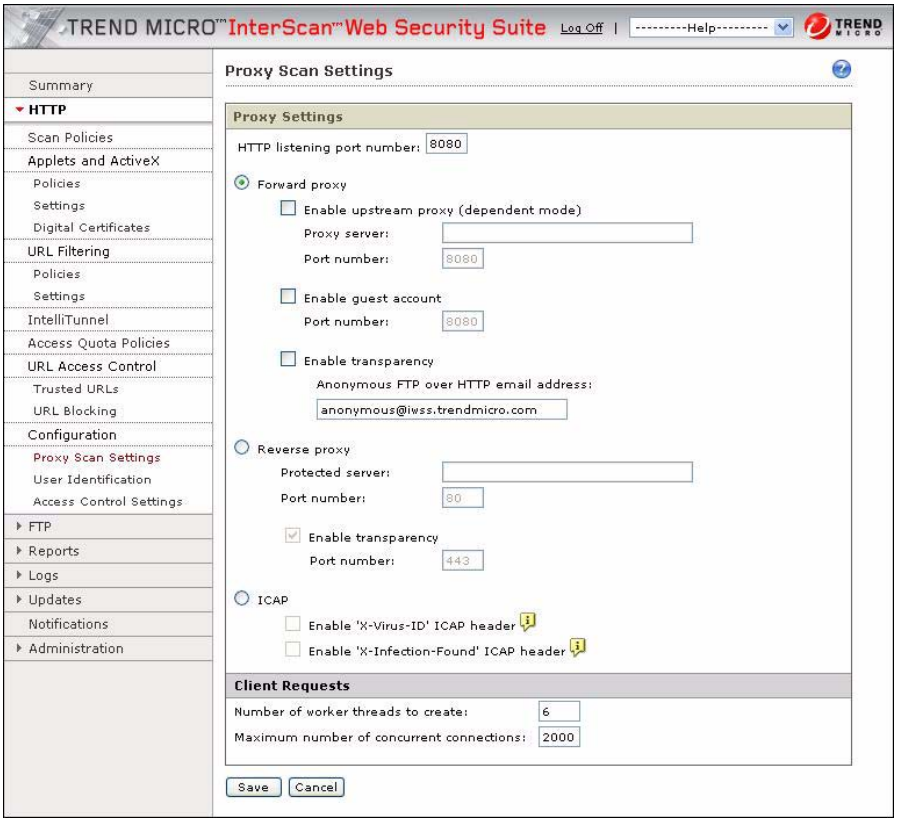


FIGURE 3-2 Configuring the type of proxy and transparency on the Proxy Scan Settings page

Upstream Proxy (Dependent Mode)

IWSS can be configured to work in conjunction with another proxy server on your network. In this configuration, IWSS passes requests from clients to another proxy server, which forwards the requests to the requested server. The upstream proxy is configured in the **Proxy Scan Settings** screen.

Like stand-alone mode, the dependent mode proxy configuration also requires client users to configure the IWSS server as their proxy server in their Internet connection settings. One benefit of using an upstream proxy is improved performance via content caching on the upstream proxy server. IWSS does not perform any content caching, so every client request needs to contact the Internet server to retrieve the content. When using an upstream proxy, pages cached on the proxy server are served more quickly.

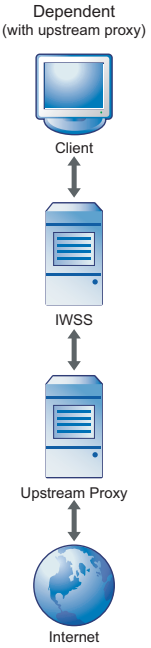


FIGURE 3-3 Forward, upstream proxy

To configure IWSS to work with an upstream proxy:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Check **Forward proxy**.
3. Check **Enable upstream proxy** and enter the IP address or host name of the upstream **Proxy server**, and its **Port**.
4. Click **Save**.

Transparency

Transparency is the functionality whereby client users do not need to change their Internet connection's proxy settings to work in conjunction with IWSS. Transparency is accomplished with a Layer 4 switch that redirects HTTP packets to a proxy server, which then forwards the packets to the requested server.

IWSS supports "simple" type transparency. Simple transparency is supported by most Layer 4 switches. While it is compatible with a wide variety of network hardware from different manufacturers, configuring simple transparency does impose several limitations:

- When using simple transparency, the User Identification method to define policies is limited to IP address and/or host name; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available, thus links to ftp:// URLs may not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs may work but the files will not be scanned.
- Simple transparency is not compatible with some older Web browsers when their HTTP requests don't include information about the host.
- HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSS. This means SSL (HTTPS) requests are typically fulfilled but the content is not scanned.
- Do not use any source NAT (IP masquerade) downstream of IWSS, since IWSS needs to know the IP address of the client to clean.
- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

The benefit of enabling transparency is that clients' HTTP requests can be processed and scanned by IWSS without any client configuration changes. This is more

convenient for your end users, and prevents clients from exempting themselves from security policies by simply changing their Internet connection settings.

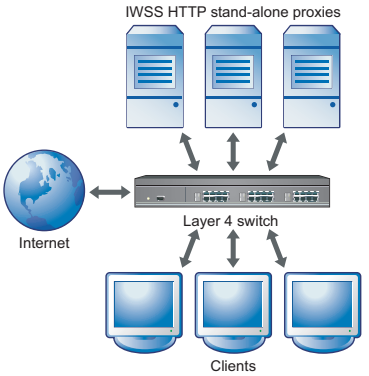


FIGURE 3-4 Forward proxy with transparency

Note: In simple transparency mode, IWSS does not accept SSL (HTTPS) traffic. Configure the router not to redirect port 443 traffic to IWSS.

To configure simple transparency:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Check **Forward proxy**.
3. Check **Enable transparency** and **Use simple transparency**.
4. Under the **Client Requests** section, change the **Listening port number** to the same port that the Layer 4 switch is configured to use.
5. Click **Save**.

Reverse Proxy

IWSS can be used to scan content that clients upload to a Web server. When IWSS is installed using either the forward or reverse proxy scan configuration, traffic of both directions, that is uploading and downloading, is scanned. Since most HTTP requests consist of an empty body, scanning files that are being uploaded is not so useful in the forward proxy configuration. In the reverse proxy configuration, there is more emphasis on scanning than in the forward proxy configuration.

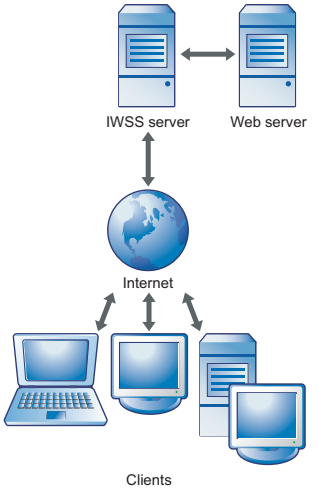


FIGURE 3-5 Reverse proxy protects Web server from clients

To configure IWSS as a reverse proxy:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Select **Reverse proxy**, and enter the IP address or host name of the **Web server** that the reverse proxy will protect.
3. Enter the **Port** (default = 80).
4. If you want to enable HTTPS access, select **Enable SSL Port** and enter the **Port Number**.
5. Click **Save**.

Note: If communication with your internal Web servers will be through SSL, don't forget to configure the HTTPS ports. For more information, see *HTTPS Ports* starting on page 48.

To complete your reverse proxy configuration, the IWSS server's IP address must be registered in the DNS as the host name of the Web server that the reverse proxy is protecting. In this way, the IWSS server appears to be the Web server, as far as the clients are concerned.

Other Proxy-related Settings

HTTP Listening Port

If you enable HTTP scanning, be sure to specify the appropriate listening port number of a given HTTP handler so the traffic will go through.

To configure the listening port number:

1. Open the IWSS management console and click **HTTP > Configuration > Proxy Scan Settings**.
2. In the **Listening port number** text box, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
3. Click **Save**.

Note: IWSS handles HTTPS connections differently than the HTTP connections. Because the data is encrypted, IWSS is not capable of scanning content downloaded via HTTPS. IWSS examines the initial CONNECT request, and rejects it if is does not match the set parameters (such as the target URL is on the Block List or contained in the PhishTrap pattern file, or the port number used is not defined in the `HttpsConnectACL.ini` file).

Anonymous FTP Logon Over HTTP Email Address

FTP over HTTP enables users to access hyperlinks to ftp:// URLs in Web pages and enter a URL starting with ftp:// in the address bar of their browser. If the user omits the user name when accessing this type of URL, anonymous login is used, and the user's email address is conventionally used as a password string that is passed to the FTP server.

To configure the email address to use for anonymous FTP logon over HTTP:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Type the **Email address** to use for anonymous FTP logon.
3. Click **Save**.

Number of Worker Threads to Create

This configuration parameter sets the number of worker threads for the service to launch (default value is 6). In threaded mode, each worker thread can handle many connections, so lowering this number does not directly influence the number of simultaneous connections you can service. Ideally there must be enough threads running so that if one thread is waiting for disk I/O, another can be processing network traffic, but not so many threads that the system gets slowed down with overhead.

Note: Trend Micro recommends setting this value to three times the number of CPUs running on your IWSS machine.

To configure the number of worker threads:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Type the **Number of worker threads to create**.
3. Click **Save**.

Number of Concurrent Connections

In order to prevent the IWSS server from getting overwhelmed with excessive client requests and having clients experience performance issues when browsing, you can configure the maximum number of clients that can connect simultaneously to the IWSS server. When this number is reached, IWSS rejects additional HTTP requests from clients.

To configure the maximum number of concurrent client connections:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Type the **Maximum number of concurrent connections**.
3. Click **Save**.

Configuring Access Control Settings

InterScan Web Security Suite includes several configurations to control your clients' HTTP access. These settings are separate from any scanning or URL filtering policies that you may configure for your user base.

- HTTP access can be selectively enabled for client users with a given IP address, IP range, or IP mask.
- To improve performance when client users request content from "trusted" sites, scanning, URL filtering and URL blocking can be disabled for servers with a given IP address, or servers within a given IP range or IP mask.
- HTTP and HTTP requests to ports or port ranges can be selectively allowed or denied for all users whose Internet access passes through InterScan Web Security Suite. This feature is convenient if you want to prevent certain types of Internet transfers.

Identifying Clients and Servers

For controlling client HTTP access or configuring servers as trusted, there are three ways to identify the client or server:

- IP address: a single IP address, for example, 123.123.123.12
- IP range: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15
- IP mask: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 will identify all machines in the 192.168.1.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32)

Client IP

In addition to the default setting that allows all clients on your network to access the InterScan Web Security Suite proxy, InterScan Web Security Suite can be configured to only allow HTTP access to those clients that you explicitly specify. If your organization does not allow everyone on your network to access the Internet, this is a convenient way to block HTTP access by default.

To allow HTTP access based on client IP:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Ensure that the **Client IP** tab is active.

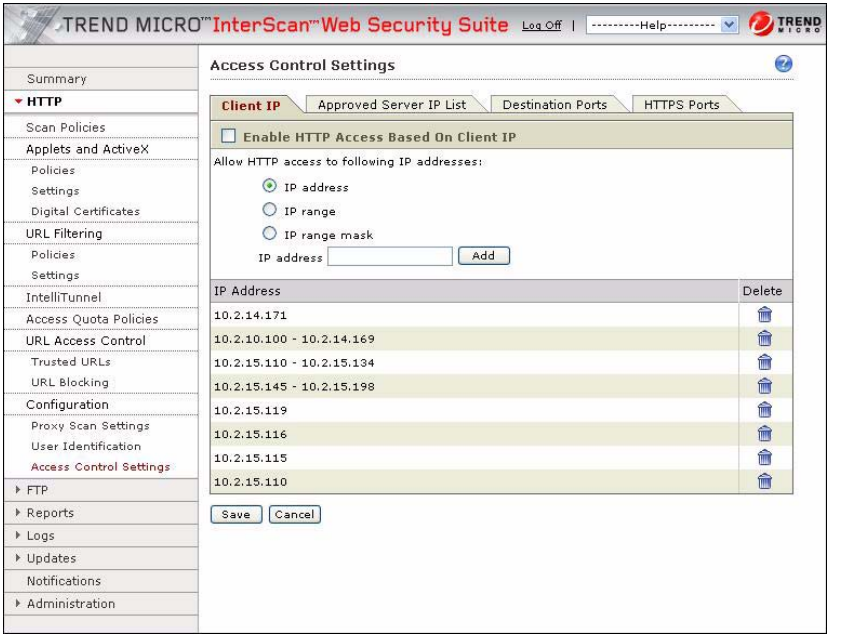


FIGURE 3-6 Configure client IP addresses that are allowed HTTP access

3. Check **Enable HTTP Access Based On Client IP**.
4. Select the radio button that describes how clients are allowed HTTP access—either **IP address**, **IP range**, or **IP range mask**.

   For more information about identifying the clients, see *Identifying Clients and Servers* starting on page 43.
5. Click **Add**.

   The trusted servers that you have configured are added to the list at the bottom of the **Client IP** tab. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Client IP** tab.

6. Click **Save**.

WARNING! *If you specify a single IP address and then an IP address range containing the single IP address, the IP address range is negated if a user attempts to access a URL at the single IP address.*

To delete a client IP or IP range, click the corresponding **Delete** icon next to it.

Server IP White List

To maximize performance of your network, you can configure IWSS to skip scanning and filtering content from specific servers. For example, if you are protecting your intranet server with IWSS in a reverse proxy configuration, you can be reasonably assured that its content is safe and you may want to consider adding your intranet servers to the Server IP White List.

After configuring the IP addresses or ranges of trusted servers, the configurations are saved to the "ServerIPWhiteList.ini" configuration file. Overlapping IP ranges are not allowed.

WARNING! *Content from servers that you configure on the Server IP white list will not be scanned or filtered. Trend Micro recommends only adding servers over which you have close control of their contents.*

In ICAP mode, the server IP white list will only be applied to RESPMOD requests. REQMOD activities (such as URL filtering, Webmail upload scanning and URL blocking) cannot be bypassed by the server IP white list for ICAP installations.

To add servers to the Server IP White List:

1. Select **HTTP >Configuration > Access Control Settings** from the main menu.
2. Ensure that **Server IP White List** tab is active.
3. Check the way to specify trusted servers from which content will not be scanned or filtered—either **IP address**, **IP range**, or **IP range mask**. For more information about identifying the clients, see *Identifying Clients and Servers* starting on page 43.

4. Click **Add**. The trusted servers that you have configured will appear at the bottom of the **Server IP White List** tab.
5. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Server IP White List** tab. To change the order that the Server IP White List is compared to the requested servers, click the up or down arrows in the **Priority** column.
6. Click **Save**.

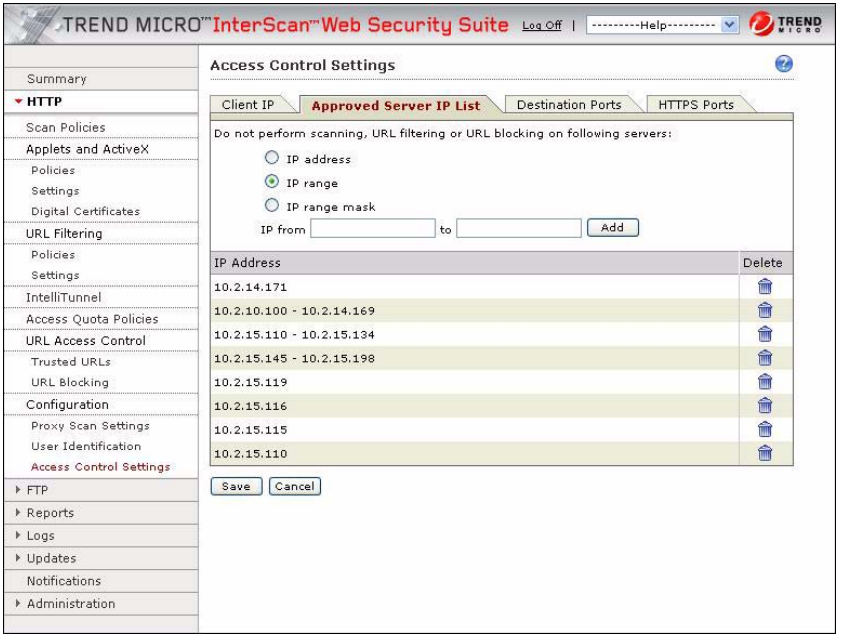


FIGURE 3-7 Content from "trusted" servers configured on the Server IP White List is not scanned or filtered

To delete a trusted server or range, click the corresponding **Delete** icon next to it.

Destination Port Restrictions

IWSS can restrict the destination server ports to which clients can connect. HTTP requests to a denied port are not forwarded. This approach can lock down your server

and prevent clients from using services such as streaming media applications that contravene your network's security policies by denying access to the ports used by these services.

The default post-install configuration is to deny all requests, except for those to ports 80 (HTTP), 70 (Gopher), 210 (TCP), 21 (FTP), 443 (SSL), 563 (NNTPS) and 1025 to 65535.

Note: For a list of ports used by various applications and services, see `http://www.iana.org/assignments/port-numbers`.

To restrict the destination ports to which a client can connect:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Ensure that the **Destination Ports** tab.
3. Choose the **Action** to perform. Choose **Deny** to prevent connections to a specific port or port range on a destination server, or **Allow** to permit connections to a specific port or port range.
4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Click **Add**. The destination port restrictions will be added to the list at the bottom of the **Destination Ports** tab.
6. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Destination Ports** tab. To change the order that ports appear in the list, click the up or down arrows in the **Priority** column.
7. Click **Save**.

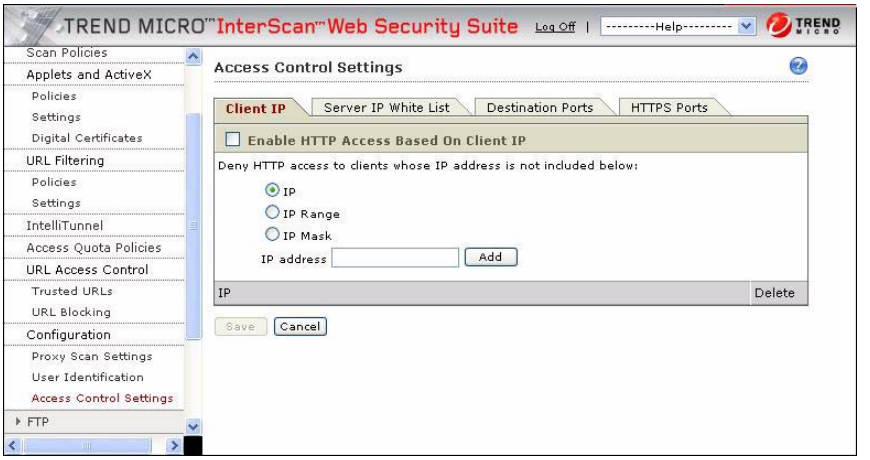


FIGURE 3-8 Port access on destination servers is controlled on the Destination Ports tab

---

Note: To enable FTP over HTTP connections for clients to open FTP links in Web pages, IWSS must be able to open a command connection to the FTP server on port 21. This requires allowing access to port 21 on the HTTP access control settings.

To delete a destination port or port range to which you're allowing or denying access, click the **Delete** icon next to it.

HTTPS Ports

IWSS can restrict which ports can be used to tunnel encrypted HTTP transactions. The default configuration is to allow only HTTPS connections on port 443 (the default HTTPS port) and 563 (the default port for encrypted newsgroups).

Note: If you need to access the management console via HTTPS while connecting through IWSS itself, allow access to the IWSS secure console port number (8443 by default).

To restrict the ports that can be used to tunnel encrypted HTTP transactions:

1. Select **HTTP > Configuration > Access Control Settings** from the main menu.
2. Make the **HTTPS Ports** tab active.
3. Choose the **Action** to perform—either **Deny** or **Allow**.
4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Click **Add**. The destination port restrictions appear at the bottom of the **HTTPS Ports** tab.
6. Access control settings are evaluated according to the order they appear in the list at the bottom of the **HTTPS Ports** tab. To change the order that ports are displayed in the list, click the up or down arrows in the **Priority** column.
7. Click **Save**.

FIGURE 3-9 HTTPS port access can be selectively allowed or denied on the HTTPS Ports tab

To delete any HTTPS port access restrictions that you may have configured, click the **Delete** icon next to the port or port range to remove.

Enabling the HTTP Traffic Flow

In order for your clients to access the Internet, HTTP traffic flow through IWSS must be enabled. Likewise, HTTP access can be turned off from the IWSS management console.

To enable or disable the HTTP traffic flow through IWSS:

1. Select **Summary** in the main menu and then select the **Scanning** tab.

   The state of HTTP traffic flowing through IWSS displays at the top of the Scanning page.

2. Select one of the following:
   - If HTTP traffic is turned off, click the **Turn On** link to enable it.
   - If HTTP traffic is turned on, click the **Turn Off** link to disable it.

When HTTP traffic is turned off, your clients cannot access Web sites or any other services carried through HTTP. To see an example of these links at the top of the **Summary** page, see Figure 2-3 on page 26.

Chapter 4

Policies and User Identification Method

InterScan Web Security Suite is able to apply different HTTP virus scanning, Applets and ActiveX security, URL filtering, IntelliTunnel, and access quota policies to different individuals or groups on your network. In this way, security policies can be customized based on your business need to handle potentially malicious code, view certain categories of Web content or consume bandwidth for Web browsing.

Topics in this chapter include the following:

- Introducing how policies work and the two IWSS default policies—the Global Policy and the Guest Policy
- Enabling the guest port for applying guest policies
- Configuring the user identification method
- Configuring a policy's scope using the three user identification methods

How Policies Work

Different security settings can be configured for different users or groups on your network, based on the type of files or Internet resources they need to access. Some examples of the practical application of different security policies are the following:

- Virus scanning: Your organization's acceptable use policy may generally prohibit clients from downloading audio or video files. However, there may be some groups within your company who have a legitimate business purpose for receiving these types of files. By configuring several virus scanning policies, you can apply different file blocking rules in HTTP virus scanning policies for different groups within your company.
- Applets and ActiveX security: To prevent clients from running applets that could intercept sensitive information and transmit it over the Internet, you may want to configure a policy for most of your company that prevents applets from connecting to their originating servers. However, if there are users in your company who have a legitimate business purpose to run these sorts of applets, for example, to get quotations through a Java applet stock price ticker, another policy could be configured and applied to a sub-set of your client base.
- URL filtering: To discourage your employees from engaging in non-work-related Web surfing, you may want to configure a Global Policy that blocks access to Web sites in the "gambling" category. However, you might need to configure another policy that permits access to these types of sites so your sales organization can learn more about prospects in the gaming industry.
- Access quotas: IWSS allows you to configure access quota policies to limit the volume of files that clients can download during the course of a month, to control the amount of bandwidth that your organization uses. For those employees who have a legitimate business need to browse the Internet extensively, you can configure another policy granting them unlimited Internet access.
- IWSS enables you to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.

In addition to being able to define custom policies that apply to specific users, IWSS is pre-configured with two default policies, the "Global Policy" and the "Guest Policy" to provide a baseline level of HTTP virus scanning, Applets and ActiveX security, IntelliTunnel security, and URL filtering.

Default Global and Guest Policies

InterScan Web Security Suite has three default policies for the HTTP virus scanning: Applets and ActiveX security, URL filtering modules, and IntelliTunnel modules.

- Global Policy—all clients who access IWSS through the **Listening port number** (default port = 8080). This is configured under **HTTP > Configuration > Proxy Scan Settings**.
- Guest Policy—those clients, typically temporary workers, contractors and technicians who access IWSS through a special guest port (default port = 8081). The guest account is disabled by default; enable the guest account and port under **HTTP > Configuration > Proxy Scan Settings**.

Note: By default, there is no access quota control for clients that access IWSS through the default listening port, thus there is no pre-configured Global Access Quota Policy.

About the Guest Policy

The guest port is a feature that's available when the administrator has configured IWSS to run in HTTP proxy mode using LDAP "User/group name via proxy authorization" as the user identification method. The administrator can opt to open the second listening port so that users who don't have accounts in the directory server, for example, contract personnel or visiting vendors, can still access the Web. The default port values are 8080 for users in the directory, and 8081 for guests. The Guest Policy is the only policy applied to guests.

For more information about enabling the "User/group name" user identification method, see *User/Group Name Via Proxy Authorization* starting on page 58.

Enabling the Guest Port

In order to enable Internet connectivity to network users who are not in the LDAP directory and apply guest policies, open a guest port for the client to communicate with IWSS.

To enable the guest port:

1. Select **HTTP > Configuration > User Identification** from the main menu.

2. From the **User Identification** screen, select **User/group name via proxy authorization** and then enter the designated directory server (s) of choice.
3. Click **Save**.
4. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
5. From the **Proxy Scan Settings** screen, check **Enable guest account**.
6. Click **Save**.

Deploying Policies

After configuring a policy, the settings are written to the database after you click **Save**. Clicking **Deploy Policies Now** applies the new policy configuration immediately. Otherwise, the policy changes go into effect when IWSS reads the information from the database after the time intervals specified under **Cache Expiration (TTL in Minutes)** on the **Administration > IWSS Configuration > Database** screen.

Note: When policies are being applied, either after the cache expiration interval or from clicking **Deploy Policies Now**, HTTP and FTP connections will be interrupted for a short time (ten seconds).

Configuring the User Identification Method

In order to define the scope of HTTP virus scanning, URL filtering, Applets and ActiveX security, IntelliTunnel security, and access quota policies, configure how IWSS will identify clients. Your choice of user identification method also determines how security events are traced to the affected systems in the log files and reports.

IWSS provides three user identification methods to identify clients and apply the appropriate policy:

- IP address (default option)
- Host name (modified HTTP headers)
- User/group name via proxy authorization (LDAP)

IP Address

The IP address is the default identification option and requires the following:

- Client IP addresses are not dynamically assigned via DHCP
- Network address translation (NAT) is not performed on the network path between the affected system and IWSS

If the local network meets these conditions, you can configure IWSS to use the IP address user identification method.

When using the IP address identification method, the scope of scanning policies is defined by defining a range of IP addresses, or a specific IP address, when adding or editing a policy.

To enable the IP address user identification method:

1. Select **HTTP > Configuration > User Identification** from the main menu.
2. Under the **User Identification Method** section, check **IP address**.
3. Click **Save**.

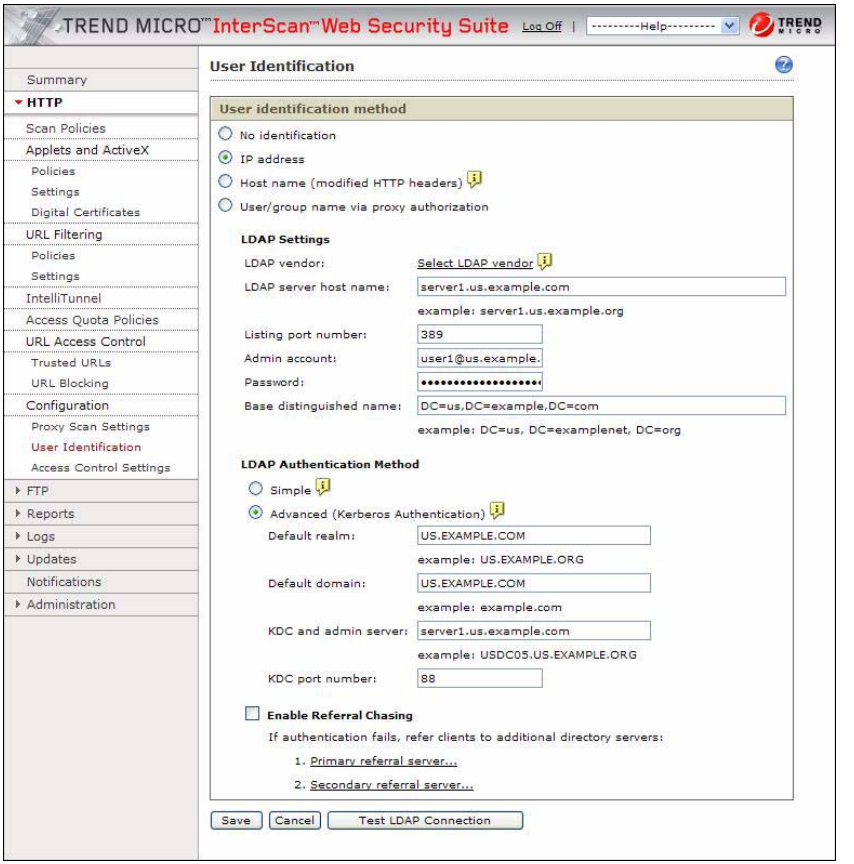


FIGURE 4-1 Identification methods are used to configure the policy's scope and identifying clients in the logs

Host Name

The host name identification method requires that clients use Internet Explorer on the Windows platform. In addition to defining a policy's scope by specifying the user's host name(s) when defining accounts to which a policy applies, the **Host name (modified HTTP headers)** user identification option logs the MAC address and Windows machine name to the security event logs.

Note: By default, only the host name portion of the host name/MAC address combination is stored in IWSS logs and used to match policies.

If you want to use both the host name and MAC address for user identification, then edit `intscan.ini` and change `use_mac_address=no` to `use_mac_address=yes` in the `[user-identification]` section.

Note: Applet-filtering messages show the client IP address (and not the host name) since even when using Internet Explorer, the HTTP request is submitted by the Java plug-in, not the browser; therefore, Internet Explorer cannot add the special header to the request.

To enable the Host name identification method:

1. Select **HTTP > Configuration > User Identification** from the main menu.
2. Check **Host name (modified HTTP headers)**.
3. Click **Save**.

Note: Before your users will be able to access the Internet, and for IWSS to apply the correct policy, clients will have to run the client registration utility.

Client Registration Utility

The **Host name (modified HTTP headers)** user identification option requires that you run a Trend Micro-supplied program on each Windows client before clients connect to IWSS and access the Internet. The program file is `register_user_agent_header.exe` and is located in the installation tar package file. An effective way to deploy this program to your clients is to invoke it from a logon script for the local Windows domain.

The program works by modifying a registry entry (`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform`) that Internet Explorer includes in the User-Agent HTTP header. You can find the identifying information logged under the **User ID** column in various log files. It alters Windows configuration values to include the MAC address of the client system and the

machine name that made the HTTP requests. The MAC address is a unique and traceable identification method and the machine name is an additional and helpful identifier.

After running the `register_user_agent_header.exe` utility, a new registry value is created under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform` key called `IWSS:<host_name>/<MAC address>`, where `<host_name>` and `<MAC address>` correspond to the client that ran the utility.

User/Group Name Via Proxy Authorization

IWSS can integrate with the following LDAP servers, and supports both the LDAP 2 and three protocols:

- Microsoft™ Active Directory 2000 and 2003
- Linux™ OpenLDAP Directory 2.2.17
- Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

LDAP Authentication Method

When you enable the **User/group name via proxy authorization** method, clients are required to enter their network logon credential before accessing the Internet. The following table shows which LDAP authentication methods can be used with each of the supported LDAP servers:

	Kerberos	Simple authentication	NTLM
Microsoft Active Directory 2000 and 2003	yes	yes	yes
Linux OpenLDAP 2.2.17	yes	yes	no
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)	no	yes	no

TABLE 4-1. Authentication methods for supported LDAP servers

Note: To use the Digest-MD5 authentication method with the Sun Java System Directory Server 5.2, all passwords must be stored as cleartext in the LDAP directory.

Choose **Simple** from the **LDAP Authentication Method** area of the **User Identification** page (**HTTP > Configuration > User Identification**) to have IWSS send the user's credential (used in the Admin account) as plain text for the initial LDAP connection only.

For increased security protection, IWSS uses the advance authentication method (Kerberos or Digest-MD5) for all subsequent user logon authentications from IWSS to the LDAP server.

LDAP Communication Flows

When a client requests Internet content, they are prompted to enter their network credential. Simple authentication sends the network credential via clear text. Advanced authentication uses a Kerberos server as a central secure password store, thus the benefit of using Kerberos is a higher degree of security. After the client

authenticates with Kerberos, a special encrypted "ticket" certified by the Kerberos server is used to access IWSS and the Internet.

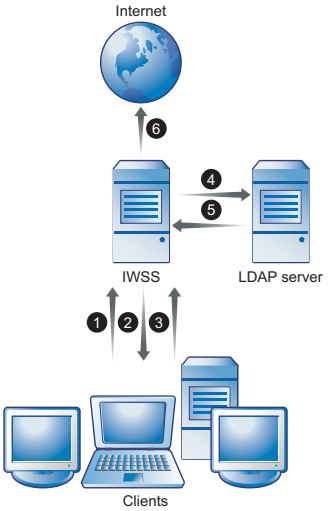


FIGURE 4-2 LDAP communication flow using Kerberos authentication

Configuring LDAP Settings

If you want to use the user/group name via proxy identification method and configure policies that are linked to your network's LDAP server, first configure your LDAP settings.

To configure IWSS to use the user/group name via proxy identification method:

1. Select **HTTP > Configuration > User Identification** from the main menu.
2. Under the **User Identification Method** section, check **User/group name via proxy authorization**.
3. Click the **Select LDAP vendor** link.

4. In the secondary browser window, select the **LDAP vendor** that you are using from the list of supported LDAP servers.

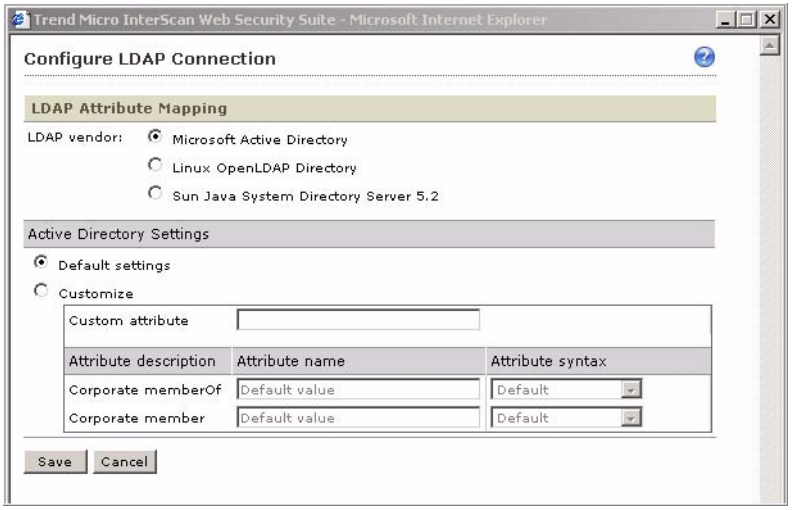


FIGURE 4-3 Choose your directory (LDAP) server's vendor in the Configure LDAP Connection screen

---

Note: In case future versions of Microsoft Active Directory modify the schema, IWSS supports changing the attribute names that make up a user's distinguished name. If you're using either Microsoft Active Directory 2000 or 2003, you should select the **Default settings** option.

---

5. In the **Configure LDAP Connection** secondary window, click **Save** to confirm your choice of LDAP vendor.
6. In the **User Identification** configuration screen, enter the **LDAP server hostname** using its FQDN (Fully Qualify Domain Name).

Note: Entering the LDAP server hostname's IP address is also acceptable, but FQDN format is recommended due to an incompatibility between Kerberos servers and identifying LDAP servers using their IP address.

---

7. Enter the **Listening port number** used by the LDAP server that you have chosen (default = 389). If your network has multiple Active Directory servers and you have enabled the Global Catalog (GC) port, change the listening port to 3268.

   Note: If you enable the Global Catalog in Active Directory, you may need to configure your firewall to allow communication through port 3268.

8. Enter the **Admin account** and **Password** for a credential with at least read authority to the LDAP server. If the domain is *us.example.com*:
   - For Microsoft Active Directory, use the UserPrincipalName for the admin account, for example, *NT_Logon_ID@us.example.com*.
   - For OpenLDAP and the Sun Java System Directory Server 5.2, enter the Distinguished Name (DN) for the admin account, for example, *uid=LOGON_ID,ou=People,dc=us,dc=example,dc=com*.
9. Enter the **Base distinguished name** to specify from level of the directory tree you want IWSS to begin LDAP searches.

   The base DN is derived from the company's DNS domain components, for example, LDAP server us.example.com would be entered as DC=us, DC=example, DC=com.

   Note: If you're using Active Directory servers with the Global Catalog (GC) port enabled, use the root domain of the Global Catalog-enabled Active Directory, for example, use *dc=example,dc=com* instead of *dc=us,dc=example,dc=com*.

10. Select the LDAP authentication method to use - either **Simple** or **Advanced**. If you opt for **Advanced** authentication, the following authentication methods are used:
    - Microsoft Active Directory and OpenLDAP: Kerberos
    - Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server): Digest-MD5

    Additionally, configure the following parameters to use Advanced authentication:
    - Default Realm

- KDC and Admin Server: the hostname of the Kerberos key distribution server. If you're using Active Directory, this is typically the same host name as your Active Directory server
- KDC port number: Default port = 88

Note: When using NTLM to authenticate with KDC(s) on a different forest through Internet Explorer or using IWSS to do referral chasing with Active Directory, Trend Micro recommends enabling "Use HTTP 1.1 through proxy connections." This setting can be found on the Internet Explorer **Tools** menu **>Internet Options > Advanced** tab. Enabling this setting prevents Internet Explorer from cutting off the "Keep-Alive connection" setting. Note that using NTLM is only supported in HTTP Proxy mode with Microsoft Active Directory.

11. In the event a client cannot authenticate using the LDAP and/or Kerberos server that you specify, you can configure IWSS to check other LDAP and/or Kerberos servers on your network. Check **Enable Referral Chasing** and then click the **Primary referral server** and **Secondary referral server** links. Enter the information for the other LDAP servers.

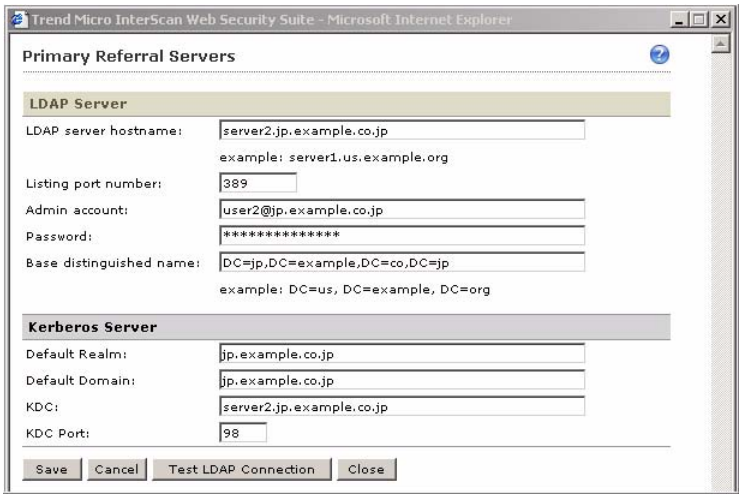


FIGURE 4-4 Configure referral servers

Note: If you are using Active Directory servers and have enabled the Global Catalog port (default = 3268), then IWSS referral chasing configurations are not supported. IWSS uses a different mechanism to query Active Directory servers when the Global Catalog port is enabled, thus configuring referral servers is redundant.

12. To verify the information has been entered correctly and IWSS can communicate with the LDAP servers that you configured, click **Test LDAP Connection** on the **User Identification** page. A message box displays, indicating that you have successfully contacted the LDAP server.
13. Click **Save**.

Note: If you want to apply the Guest Policy for those network users who are not in your LDAP directory, enable the guest account and configure the guest port (default = 8081) that will receive those requests on the IWSS server. For more information about enabling the guest account and configuring the guest port, see *Enabling the Guest Port* starting on page 53. If the guest port is not enabled, only users in the LDAP directory can browse the Internet.

LDAP Query Matching Across Main and Referral Servers

When adding users or groups to a policy's scope using the "User/group name via proxy authorization" identification method, IWSS initially searches in the main LDAP server. If no matching entries are found, the search is extended to the Primary Referral Server and the Secondary Referral Server. However, if entries matching the search string are found in the main LDAP server, the query will not return matches in the Primary and Secondary Referral servers.

For example, assume the following:

- Main LDAP server contains entries "John Smith" and "John Jones"
- Primary referral server contains entry "John Watson"
- Secondary referral server contains "John Carter Rubin"

A query for "John" will only return "John Smith" and "John Jones" since matching entries exist in the main LDAP server and the search will not extend to the referral servers. However, a query for "John Carter" will extend down to the secondary

referral server and return “John Carter Rubin” since no matching entries exist in the main or primary referral servers.

Cross Domain Active Directory Object Queries

Trend Micro recommends using the Global Catalog port (3268) as the IWSS LDAP communication port when using Microsoft Active Directory. Using port 3268 enables cross domain group nesting object queries. This applies when an object's attribute on one domain refers to another object residing on a different domain (for example, cross-domain user or group membership that reside on different domains in a forest).

For retrieving cross-domain group object attribute(s), Trend Micro recommends creating groups with the “Universal” Group Scope to ensure that cross-domain group membership within an Active Directory forest is included in the Global Catalog.

Note: In order to configure IWSS to listen on port 3268, the Microsoft Active Directory server that IWSS uses should have the Global Catalog enabled.

Because the member attribute is not replicated to the Global Catalog for all group types, and because the *memberOf* attribute derives its value by referencing the member attribute (called back links and forward links, respectively), search results for members of groups, and groups in which a member belongs, can vary. Search results depend on whether you search the Global Catalog (port 3268) or the domain (port 389), the kind of groups that the user belongs to (global groups or domain local groups), and whether the user belongs to universal groups outside the local domain.

For more information, search for the article “How the Global Catalog Works” at http://www.microsoft.com.

Configuring the Scope of a Policy

Whether configuring HTTP virus scanning, Applets and ActiveX security, URL filtering, IntelliTunnel security, or access quota policies, the first step is the same—to configure the policy’s scope by identifying the client users to which the policy applies. The following three procedures describe how to select the accounts using the IP address, Host name (modified HTTP headers) and the User/group name via proxy authorization user identification methods.

Note: Even if you configure IWSS to use the Host name (modified HTTP headers) or User/group name via proxy authorization user identification method, you can always specify clients by entering an IP address or IP address range.

Before adding a policy and configuring its scope, set the user identification method. See *Configuring the User Identification Method* starting on page 54 for more information.

Using IP Address

Configuring policies using the clients' IP addresses is the simplest identification method and is always available, regardless of the user identification method that you have configured to use.

To configure a policy's scope using the IP address user identification method:

1. From the main menu, click **HTTP** and then choose the type of policy to create (either **Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, or **Access Quota Policies**).
2. In the screen that corresponds to the type of policy selected, click **Add**.
3. Type a descriptive **Policy name**. Policy names that include references to the users or groups to which they apply, for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers" are easily recognizable.
4. Select the users to which this policy applies by typing the upper and lower bounds of a contiguous range of IP addresses in the **From** and **To** fields. Alternatively, type a single **IP address**. Click the corresponding **Add** button to add the addresses to the policy.
5. When you have named your new policy and defined the IP address(es) to which it applies, click **Next** to proceed with the other policy settings.

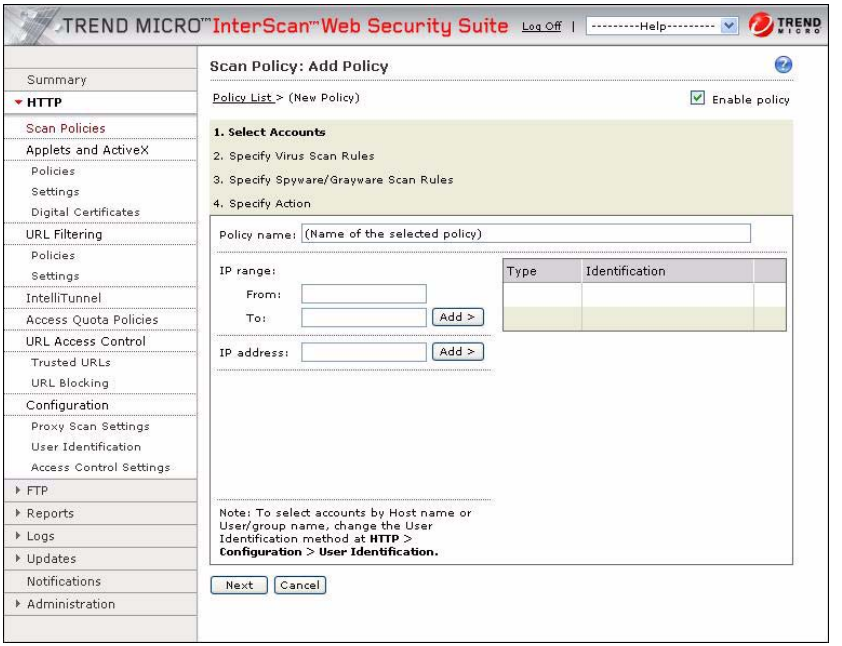


FIGURE 4-5 Configure referral servers if the user credential exists on a different directory server other than the one configured. This is an exception that exists if IWSS is configured to use the Global Catalog port 3268 for Microsoft AD, where referral server configurations do not apply.

Using Host Name

All clients must run a Trend Micro-supplied utility before clients will be subject to a policy that uses the host name (modified HTTP headers) identification method. For more information, see *Client Registration Utility* starting on page 57.

To configure a policy's scope using the client host names:

1. From the main menu, click **HTTP** and then choose the type of policy to create (either **Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, or **Access Quota Policies**).

2. In the screen that corresponds to the type of policy that you selected, click **Add**.
3. Type a descriptive **Policy name**.
4. Select the users to which this policy will apply by typing the **Host name** of the client and clicking **Add**. Repeat typing the host names and clicking **Add** until the Type/Identification table on the right side of the screen shows all the clients to which the policy applies.

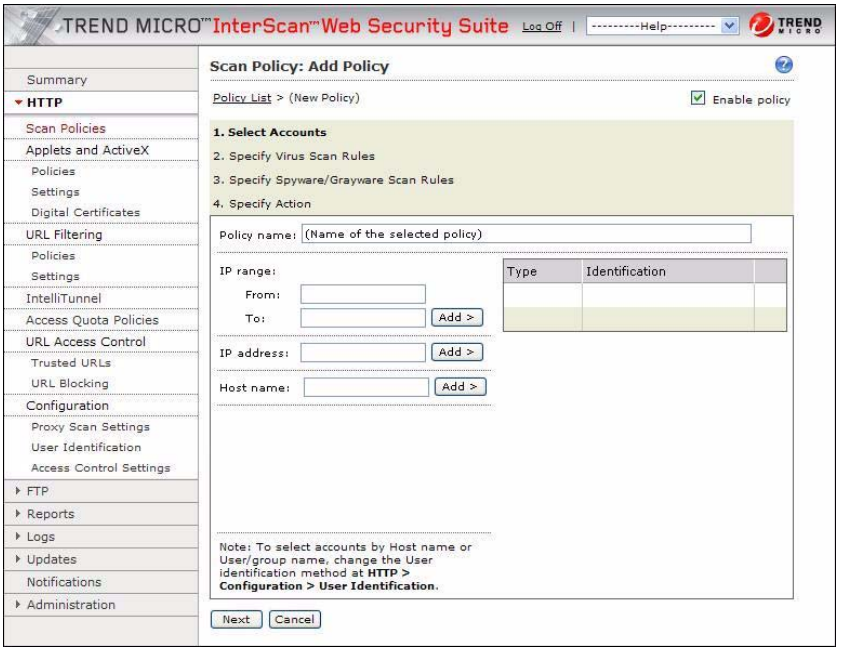


FIGURE 4-6 Configuring a policy's scope using the hostname user identification method (Virus scanning policy shown)

5. When you have named your new policy and defined the account(s) to which it applies, click **Next** to proceed with configuring the rest of the policy.

Using User/group Name via Proxy Authorization

Before configuring a policy using users or groups from your LDAP server, set the user identification method and enter the details of your LDAP server. For more information, see *Configuring LDAP Settings* starting on page 60.

To configure a policy's scope using users and groups from an LDAP server:

1. From the main menu, click **HTTP** and then choose the type of policy to create (either **HTTP Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, or **Access Quota Policies**).
2. In the screen that corresponds to the type of policy that you selected, click **Add**.
3. Type a descriptive **Policy name**.
4. To query your LDAP directory for users or groups to add to your policy:
   a. Check either **User** or **Group**.
   b. Type the first part of the user or group name in the **Name** field and click **Search**.
   c. When the list box displays users or groups that match your search criteria, highlight the user or group to add to the policy and click **Add**.
5. Repeat adding users or groups until your policy's scope is complete.
6. When you have named your new policy and defined the account(s) to which it applies, click **Next** and proceed with configuring the rest of the policy.

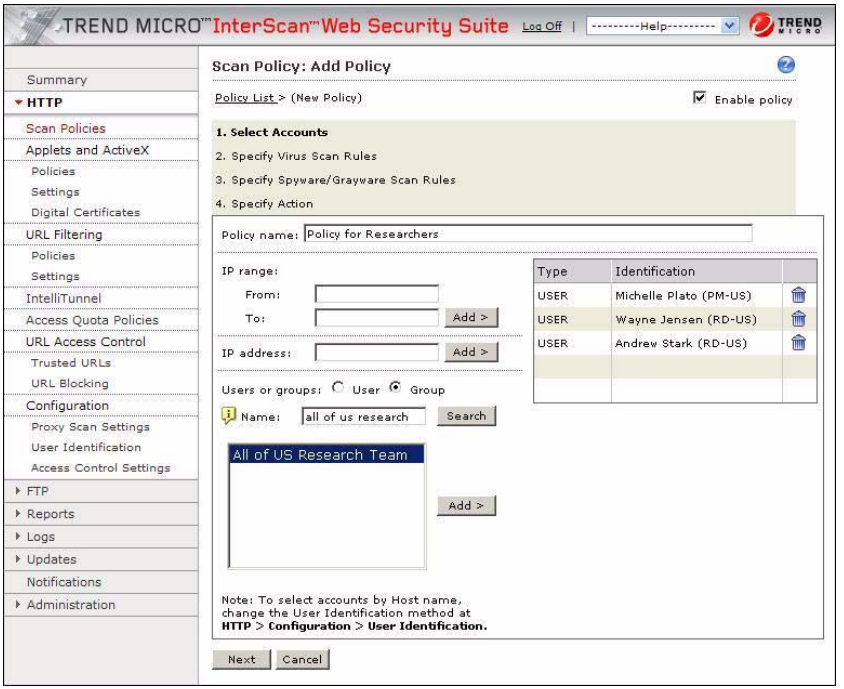


FIGURE 4-7 Configuring a policy's scope using the user/group name identification method (URL Filtering policy shown)

Login Accounts

Up to 128 users can access IWSS using assigned access rights. When in the application, users can make configuration changes that are recorded in the login accounts log.

About Access Rights

If you have a team of security administrators who are responsible for different functions and who may also have help desk privileges, then assigning them access rights can be beneficial to your organization. To manage IWSS, these users can have different logins with different privileges.

Access rights can also give you the ability to audit what is being changed in IWSS. If you have the need to comply with certain government agency standards, then this function is can be critical.

There are three levels of access:

- Full access—Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console including creating, deleting, and modifying user accounts. This is the default access for new users.
- Read only—Users cannot make any configuration changes; they can only view configurations, logs, and reports. They can change their own password.
- Reports only—Users can only view the Summary pages and scheduled reports. They can generate logs and real-time report queries and change their own password.

Adding a Login Account

To add a login account:

1. From the main menu, click **Administration > Login Accounts**.
2. In the Login Accounts page, click **Add**.
3. In the **Add Account** page, complete the necessary information:
   - Username—The name of the user assigned to the login account.

- Password—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
- Description—The field that briefly describes the login account.
- Access Rights—See *About Access Rights* starting on page 71.

4. Click **Save**. The new login account appears in the **Login Accounts** page.

Changing a Login Account

To change a login account:

1. From the main menu, click **Administration > Login Accounts**.
2. Click on the desired username.
3. In the Edit Login Account page, change the necessary information:
   - Username—The name of the user assigned to the login account.
   - Password—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
   - Description—The field that briefly describes the login account.
   - Access Rights—See *About Access Rights* starting on page 71.
4. Click **Save**. The changed login account appears in the **Login Accounts** page.

Audit Log File

The audit log file is where IWSS stores any configuration changes that users make to the application. The log file contains a prefix that you can use to organize your logs.

The log prefix is auto-generated but you can change this in the command line interface (CLI). To change the log prefix, ensure that you have root permission and then from the CLI, open the configuration file (/iscan/intscan.ini) and make the necessary changes. Finally, restart IWSS to activate the change.

Chapter 5

Configuring HTTP Scanning and Applet/ActiveX Security

This chapter describes how to configure HTTP virus scanning and applets and ActiveX security policies. Topics in this chapter include the following:

- Enabling HTTP scanning and applets and ActiveX security
- Understanding HTTP scanning settings and their effect on Web browsing performance
- Creating and modifying HTTP virus scanning, and Applet/ActiveX security policies
- Configuring HTTP virus scanning, including file type blocking, compressed file handling, large file handling, spyware and grayware scanning rules, and scan actions
- Understanding how Applet/ActiveX security works
- Configuring Java applet security, including digital signature and certificate status, applet instrumentation, and re-signing
- Configuring ActiveX security rules
- Configuring applet and ActiveX security settings

Enabling HTTP Scanning and Applets and ActiveX Security

You can enable or disable HTTP scanning from the **Summary** page of the IWSS management console.

To enable HTTP scanning and Applets and ActiveX security:

1. Open the IWSS management console and click **Summary** in the main menu.
2. On the **Scanning** tab, check **HTTP scanning** to enable virus scanning and **Applet/ActiveX security** to scan against malicious mobile code.
3. Click **Save**.

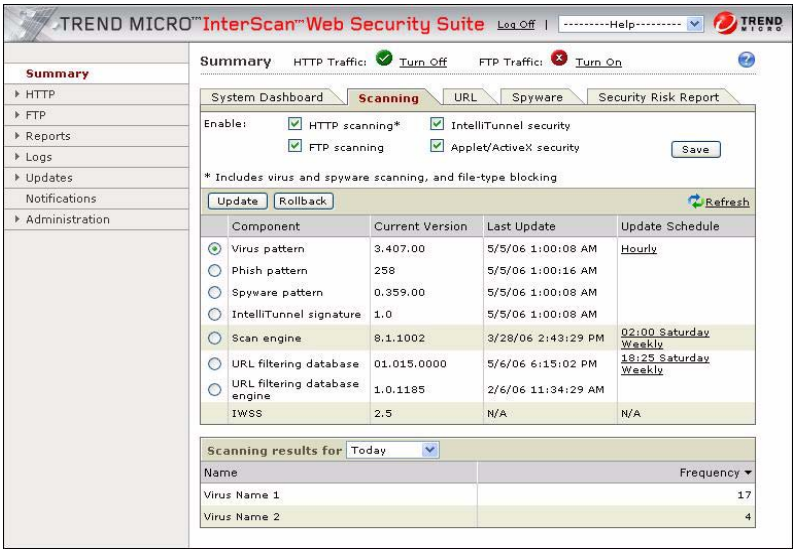


FIGURE 5-1 Enable HTTP scanning on the Summary page

Note: In addition to enabling HTTP scanning and Applet/ActiveX security, ensure that HTTP traffic is turned on (see *Enabling the HTTP Traffic Flow* starting on page 50). Otherwise, clients cannot access the Internet.

HTTP Scanning Performance Considerations

There are trade-offs between performance and security while scanning HTTP traffic for malicious content. When users click a link on a Web site, they expect a quick response. This response, however, may take longer as gateway antivirus software performs virus scanning. Some of the requested files may be large and determining whether the file is safe requires downloading the entire file before it is relayed to the user. Content may also consist of many small files. In this case, the user's wait is the result of the cumulative time needed to scan the files.

One way to improve the user's experience is to skip scanning large files or files that are not likely to harbor viruses. For example, you can skip all files with an extension of ".gif", or all files with a MIME type.

When configured to skip scanning a file due to its MIME content-type, IWSS will attempt to determine the file's true file type and match it to the claimed MIME type before skipping it. If the file's true file type maps to a different MIME type than indicated in the Content-type header attached to the transaction, the file will be scanned. Unfortunately, there is not always a clear mapping between file types and MIME types. If IWSS cannot map the true file type to a MIME type, it will be skipped according to the Content-type header as configured.

You can exclude files from scanning based on extension. Trend Micro recommends that you minimize the list of MIME content-types to skip. In general, relying on the scan engine to decide whether a file should be scanned is safer than trying to pick out which file types you want to skip yourself. Firstly, the content-type HTTP header may not accurately represent the true type of the content to download. Secondly, some types that you may think are safe to skip (for example, text) may not really be safe (since scripts are text, and may possibly be malicious). One more area where you may want to use MIME content-type skipping is where you are consciously making a trade-off in safety versus performance. For example, a lot of Web traffic is text, and the IWSS scan engine will scan all that traffic because the content may contain scripts, which are potentially malicious. But if you are confident that you are browsing an environment that cannot be exploited by Web scripts, you may choose to add text/* to your MIME content-type skip list so IWSS does not scan Web pages.

Malicious code within a small file can quickly spread throughout a network. Malicious code that requires a large file for transport will propagate more slowly, because the file containing malicious code will take longer to transmit. Therefore, it is important to screen small files efficiently and completely.

Note: Performance may be adversely affected if the main policy for ActiveX scanning directs that all PE (windows executable) files must be scanned (not just COM objects, of which ActiveX controls are a subtype), or if all unsigned PE files are to be blocked. The performance impact occurs because the javascan daemon (which enforces policy for these files) is invoked more often.

Creating and Modifying HTTP Virus Scanning Policies

In addition to the default global and guest policies, you can create customized HTTP scanning policies for specified members of your organization.

To create a new virus scan policy:

1. Choose **HTTP > Scan Policies** from the main menu.
2. Select **Enable virus scanning** to turn the policy on.
3. Click **Add**.
4. Type a descriptive **Policy name**. Policy names that include references to the users or groups to which they apply, for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers", are easy to remember.
5. Select the users that this policy will apply to. The options on this page depend upon the user identification method that you are using - either *IP address*, *Host name (modified HTTP headers)* or *User/group name via proxy authorization*. For more information about configuring the user identification method and defining the scope of a policy, see *Configuring the User Identification Method* starting on page 54 and *LDAP Query Matching Across Main and Referral Servers* starting on page 64.

Note: Regardless of the user identification method that you have configured, you can always enter IP addresses of the clients to which the policy will apply.

6. When you have named your new policy and defined the account(s) to which it applies, click **Next** to proceed with defining HTTP virus scanning rules.

To modify an existing HTTP scanning policy:

1. Click **HTTP > Scan Policies** from the main menu.
2. Click the name of the policy to modify.
3. Modify the virus scanning rules, the spyware scanning rules and the scanning action.

To add or remove users from an existing HTTP scanning policy:

1. Click **HTTP > Scan Policies** from the main menu.
2. Click the desired scan policy account.
3. From the **Scan Policy: Edit Policy** (Account tab) screen, either add or remove a user.
   - To add a user, specify a user IP address in the **IP address** field or specify a range of users in the **From** and **To** fields under **IP range.** Click **Add** after specifying a user or range of users.
   - To remove a user, click the trash can icon next to the user.

To enable a HTTP scanning policy:

- In any HTTP scanning policy configuration page, select **Enable policy**.

HTTP Virus Scanning Rules

IWSS administrators can configure which file types to block and scan, and how compressed and large files are handled.

Specifying File Types to Block

You can identify the types of files to block for security, monitoring or performance purposes. Blocked files are not received by the requesting client, nor are they scanned—requests to retrieve a blocked file type are not executed. You have the option of blocking file types such as Java applets, Executables, Microsoft Office documents, Audio/video files, Images or Other files types that you configure.

To specify which file types to block:

1. While adding or editing a policy, under **Block These File Types**, select the file types to block.

2. In the **Other file types** field, type the other file types to block, using a space to delimit multiple entries. See *Mapping File Types to MIME Content-types* starting on page 215 for how to enter other files types that can be blocked, along with their corresponding MIME content-type.

Specifying File Types to Scan

About IntelliScan

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

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

True File Type

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

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

For example, .gif and .jpg files make up a large volume of all Web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. However, this does not mean that they are entirely safe. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan

engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

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

To select which file types to scan:

IWSS can scan all files that pass through it, or just a subset of those files as determined by true file type checking (IntelliScan) or the file extension. In addition, individual files contained within a compressed file can also be scanned.

1. Select the files to scan:
   - To scan all file types, regardless of file name extension, select **All scannable files**. IWSS opens compressed files and scans all files within. This is the most secure, and recommended, configuration.
   - To use true file type identification, select **IntelliScan**. This configuration scans file types that are known to harbor viruses by checking the file's true-file type. Since checking the true file type is independent of the filename's extension, it prevents a potentially harmful file from having its extension changed to obscure its true file type.
   - You can explicitly configure the types of files to scan or skip based on their extensions to work around possible performance issues with scanning all HTTP traffic. However, this configuration is not recommended, because the file extension is not a reliable means of determining its content.

     To scan only selected file types (Trend Micro does not recommend this setting), select **Specified file extensions** and then click the list. The **Scan Specified Files by Extension** screen displays. The default extensions list shows all file types that are known to potentially harbor viruses. This list is updated with each virus pattern file release. On the **Scan Specified Files by Extension** screen, add or exclude additional extensions in the **Additional Extensions** and **Extensions to Include** fields. Click **OK** when you are finished. The screen closes.

Note: Enter the extension to scan or exclude from scanning (typically three characters), without the period character. Do not precede an extension with a wildcard (*) character, and separate multiple entries with a semicolon.

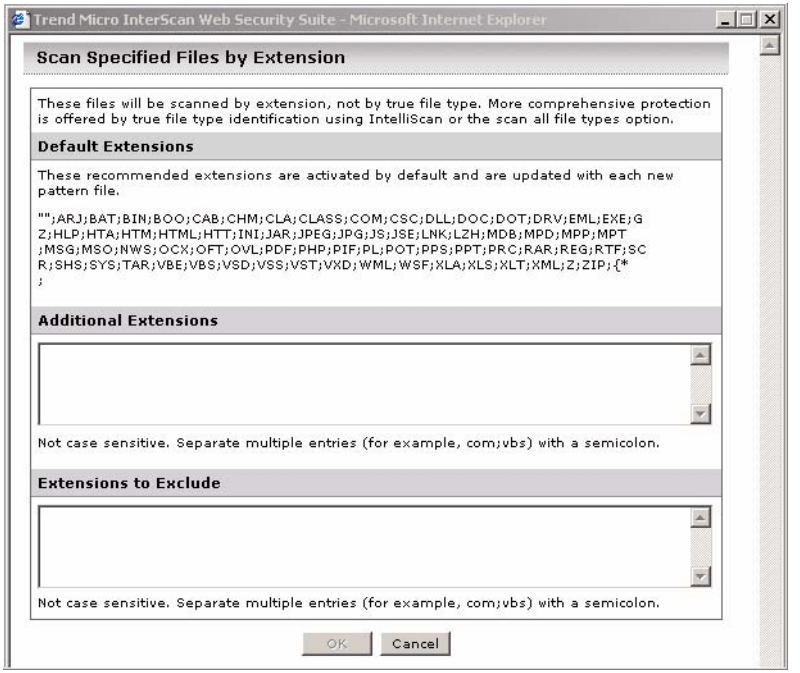


FIGURE 5-2 The recommended extensions to scan are updated with each new pattern file

2. You can configure IWSS to selectively bypass certain MIME content-types. Some file types, such as RealAudio or other streaming content, begin playing as soon as the first part of the file reaches the client machine and will not work properly with the resulting delay. You can have IWSS omit these file types from scanning by adding the appropriate MIME types to the **MIME content-types to skip** list on the **Virus Scan Rule** tab. Type the MIME content-type to bypass in the **MIME content-type to skip** field (for example, image, audio, application/x-director video, and application/pdf).

Note: Trend Micro recommends minimizing the list of MIME content-types to skip to reduce the risk of virus infection. Also, Trend Micro does not recommend skipping any MIME content-types when large file handling is enabled, since it's possible for a MIME content-type to be forged.

Priority for HTTP Scan Configuration

IWSS scans according to the following priority:

1. MIME content-types to skip
2. File types to block
3. File types to scan

Configuring Compressed File Scanning Limits

Compressed file scanning limits can be configured via the **Add** or **Edit** option for the **HTTP > Scan Policies** screen. IWSS opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. IWSS decompresses the files according to the configurable limits (number of files in the compressed archive, size of the compressed file, number of compressed layers and the compression ratio).

To configure the compressed file scanning limits:

Under **Compressed File Handling**, select from the following two options:

- **Block all compressed files**: All requests to download compressed files will not be fulfilled.
- **Block compressed files if...**: Requests to download compressed files that exceed the configured criteria will not be fulfilled. Type values for the following parameters:
  - Decompressed file count exceeds (default is 10000)
  - Size of a decompressed file exceeds (default is 200MB)
  - Number of layers of compression exceeds (range is 0-20; default is 10)
  - Compression ratio of any file in the archive exceeds (*x* %) (range is 1-100; default is 100)

Note: "100" percent file compression ratio means that there is no limit on the compressed files setting; whereas, "0" percent file compression ratio means that all compressed files will be blocked.

A compressed file that meets any of the tests will be blocked at the gateway and not scanned. For example, suppose your settings appear as follows:

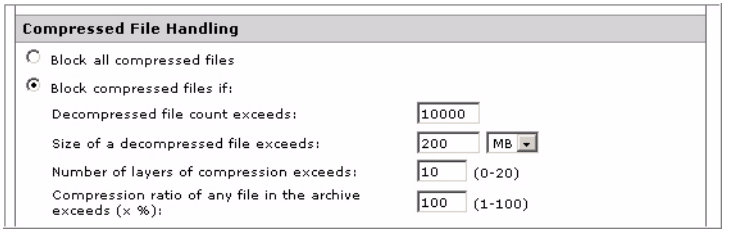


FIGURE 5-3 "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the IWSS server

A compressed file that has more than 10 layers of compression or contains more than 10000 files will not pass through the gateway.

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 transferring the entire file to IWSS, scanning the file, and then transferring 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, 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. The size of file that you should consider "large" varies, depending on the hardware where IWSS is installed, the mix of file types in the particular environment, and so on. Trend Micro recommends that files larger than 512KB (default value) be considered large and files larger than 2048MB do not have to be scanned; however, these values might vary depending on your network speed, server capability, and other factors.

Large file handling can be set via the **Add** or **Edit** option for the **HTTP > Scan Policies** screen.

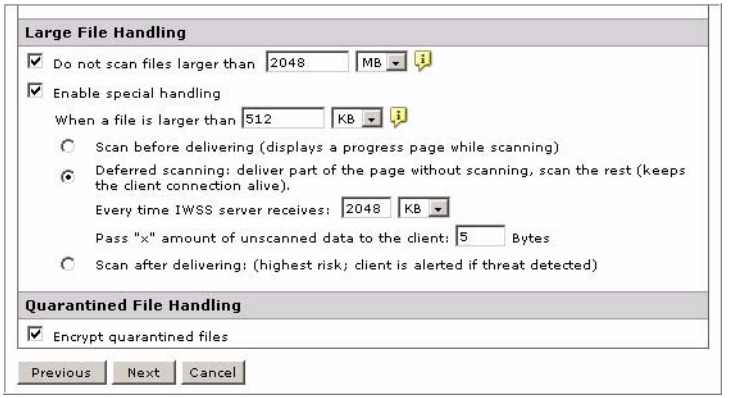


FIGURE 5-4 For special handling of large files, there are three options to choose from: (1) scan before delivering, (2) deferred scanning, or (3) scan after delivering

Once you encounter a large file, IWSS scans it in a manner that will reduce the chance of a browser timeout. Scanning of large files can be turned off by choosing **Do not scan files larger than...** to reduce performance issues when downloading very large files and you have control over their integrity.

To disable scanning large files:

- Under **Large File Handling**, check **Do not scan files larger than...** and configure the file size over which files will not be scanned. The default is 2048MB.

Disabling scanning of any files, even large ones, is not recommended since it introduces a security vulnerability into your network.

To use large file handling for HTTP scanning:

1. Under the **Large File Handling** section, select **Enable special handling**, and then type the file size (in KB or MB) to be considered a large file. The default value is 512KB.
2. Select the type of large file-handling to use:

- **Scan before delivering**: shows progress while scanning, and then loads the page afterwards
- **Deferred scanning**: loads part of the page while scanning; stops the connection if a virus is found (default setting)
- **Scan after delivering**: loads the page first, and then scans afterwards (highest risk of infection)

Note: Large file handling does not work when using the Blue Coat Port 80 Security Appliance in ICAP mode. If IWSS is configured as an HTTP proxy in-line with the Blue Coat appliance, however, large file handling will function.

3. Click **Save**.

Consider configuring large file handling if your users experience browser timeouts when trying to download files. There are three large file scanning options:

Scan Before Delivering (Progress Page)

When IWSS is configured to use the **Scan before delivering** scanning option, requested files are not passed to the client until scanning is finished. A progress page is generated to prevent the browser from timing out and to inform the user that scanning is in progress to prevent them from thinking that the connection is hung.

Note: For large file handling, IWSS uses the progress page. The progress page uses JavaScript and a pop-up window to display the download progress. If your desktop security policy has pop-up blocking enables or JavaScript disabled, then the progress page does not function and scanning is prevented.

In order for the progress page to work, IWSS needs to know to which externally visible IP address the clients will connect. Using 127.0.0.1 causes a problem. If a message about the progress page appears, add the machine IP address to `iscan_web_server` (for example, `iscan_web_server=1.2.3.4:1812`) or modify the `/etc/hosts` file so that the host name does not resolve to 127.0.0.1.

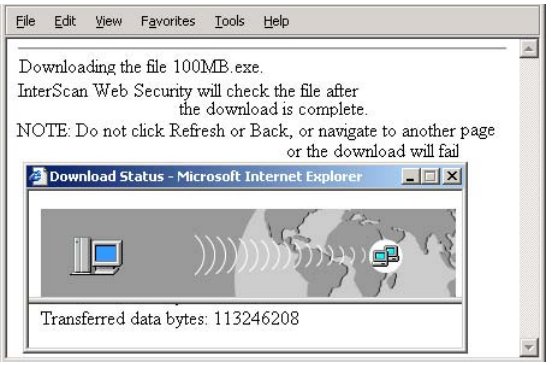


FIGURE 5-5 "Scan before delivering" large file handling progress window

Deferred Scanning

When IWSS is configured to use the **Deferred scanning** option, part of the file is passed to the requesting client while IWSS scans the remainder of the file. The partial file remains in the client's temporary directory until scanning concludes and the last byte of the file is delivered.

If you choose to use the deferred scanning option, there are some parameters to configure:

- **Every time IWSS server receives** controls how often data is passed to the requesting client as a file downloads to the IWSS server. This data prevents the requesting browser from timing out.
- **Pass *x* amount of unscanned data to the client** controls the amount of data released to the requesting client.

For example, assume the following configurations:

- **Every time IWSS server receives** = 2048KB
- **Pass *x* amount of unscanned data to the client** = 512 Bytes

When downloading a large file, 512 bytes of data are released to the requesting client for every 2048KB that is downloaded to the IWSS server.

Scan After Delivering

When IWSS is configured to use the **Scan after delivering** configuration, files are immediately passed to the requesting client without scanning. The file is then scanned by IWSS—if the file is found to contain malicious code, IWSS takes the following actions:

- Sends a notification email message, provided notifications are enabled.
- Logs the event details.
- Automatically blocks the URL from which the malicious content originated from other users for 4 hours after the malicious code detection. Access to the URL is restored after 4 hours elapses, and content from it will be scanned.

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

- Client PC attempts to access a URL classified as Spyware, Disease Vector, or Virus Accomplice by the PhishTrap pattern or
- Client PC uploads a virus classified as a "worm."

DCS connects to the client in order to clean the infected file.

If the affected client has up-to-date antivirus software and security patches, then the antivirus software may also detect the malicious code on the client machine.

The following table summarizes the different program behavior when malicious programs are detected under the three different large file handling configurations.

TABLE 5-1 Comparison between "scan after delivering" and "deferred scanning"

Scanning method for large file	INI setting in intscan.ini [http]/Policy setting in RuleValue database in table tb_Rule	Behavior for first time access	URL in infectedB.ini if virus is found after scanning	Behavior for second and subsequent access to the same URL
Scan after delivering	special_handling=yes deferred_scan=yes	The user always gets the file before virus scanning starts.	IWSS saves the infected URL to the [allow] section if the file is cleaned after scanning. If it is deleted or quarantined, the infected URL is added to the [block] section of the infectedB.ini file.	If the file is cleanable, then IWSS invokes scanning with progress page. However, if the file is non-cleanable, then it is temporarily blocked for four hours. After this time, the file will invoke scanning with progress page
Deferred scanning	special_handling=yes deferred_scan=late	The user gets the file if there is no virus. If a virus is found, IWSS drops the connection.	IWSS saves the infected URL to the [allow] section if the file is cleaned after scanning. If it is deleted or quarantined, the infected URL is added to the [block] section of the infectedB.ini file.	If the file is cleanable, then IWSS invokes scanning with progress page. However, if the file is non-cleanable, then it is temporarily blocked for four hours. After this time, the file will invoke scanning with progress page

Scanning method for large file	INI setting in intscan.ini [http]/Policy setting in RuleValue database in table tb_Rule	Behavior for first time access	URL in infectedB.ini if virus is found after scanning	Behavior for second and subsequent access to the same URL
Scan before delivering (scan-first)	special_handling=yes deferred_scanning=no	The user sees a progress page, and receives the file if there is no risk. If a risk is detected, IWSS drops the connection.	IWSS saves the infected URL to the [allow] section if the file is cleaned after scanning. If it is deleted or quarantined, the infected URL is added to the [block] section of the infectedB.ini file.	If the file is cleanable, then IWSS invokes scanning with progress page. However, if the file is non-cleanable, then it is temporarily blocked for four hours. After this time, the file will invoke scanning with progress page

Important Notes for Large File Handling

- Large file special handling only applies to HTTP scanning, FTP scanning, and FTP over HTTP via the HTTP proxy. It does not apply to FTP over HTTP for ICAP traffic. Users may experience timeout issues while downloading large files using FTP over HTTP.
- When using the scan-after-delivering-large-file-handling method, IWSS does not delete files subsequently found to be infected in the first affected client.

Violations of the large file handling policy will display a user notification in the requesting client's browser.

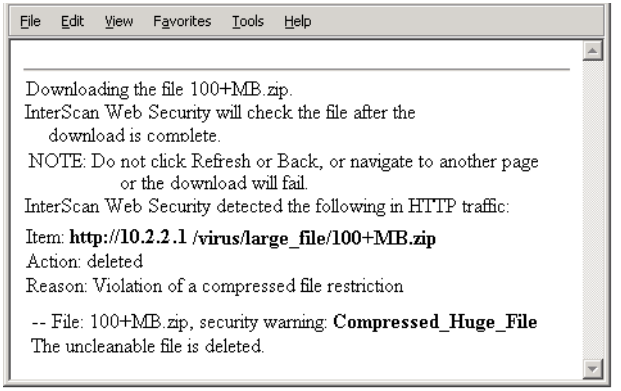


FIGURE 5-6 Notification after completing scanning and downloading the file

Quarantined File Handling

If you choose to quarantine files that IWSS detects as malicious, you can optionally choose to encrypt the files before moving them to the quarantine folder by checking **Encrypt quarantined files**. This will prevent the files from being inadvertently executed or opened. Note that encrypted files can only be decrypted by a Trend Micro Support engineer.

When you've completed configuring the HTTP virus scanning rules on the **HTTP > Virus Scan Add/Edit** policy screen, click **Next** to move on to the spyware/grayware scanning rules.

Spyware and Grayware Scanning Rules

In addition to computer viruses, the IWSS pattern files include signatures for many other potential risks. These additional risks are not viruses since they do not replicate and spread. However, they can perform unwanted or unexpected actions, such as collecting and transmitting personal information without the user's explicit knowledge, displaying pop-up windows, or changing the browser's home page.

IWSS can be optionally configured to scan for the following additional risks:

- Spyware: software that secretly collects and transmits information without the user's explicit knowledge or consent
- Dialers: software that secretly dials a telephone number, typically an international or pay-per call number, through the user's modem
- Hacking tools: software that can be used for malicious hacking purposes
- Password cracking programs: software designed to defeat computer passwords and other authentication schemes
- Adware: software that monitors and collects information about a user's browsing activities to display targeted advertisements in the user's browser or through pop-up windows
- Joke programs: programs that mock computer users or generate some other sort of humorous display
- Remote access tools: programs designed to allow access to a computer, often without the user's consent
- Others: Files that don't fit into the other additional risks classifications. Some of these may be tools or commercial software that have legitimate purposes, in addition to having the potential for malicious actions

To scan for spyware, grayware and other non-virus additional risks:

1. Under **Scan for Additional Threats** on the **HTTP > Scan Policies > Virus Scan Policy Add/Edit** screen or the **Spyware/Grayware Scan Rule** tab on the **FTP > Scan Rules > FTP Scanning** screen, select the types of additional risks to be detected. To scan for all additional risks that have signatures in the pattern file, check **Select all**.

2. Click **Next** to configure the actions against security risks.

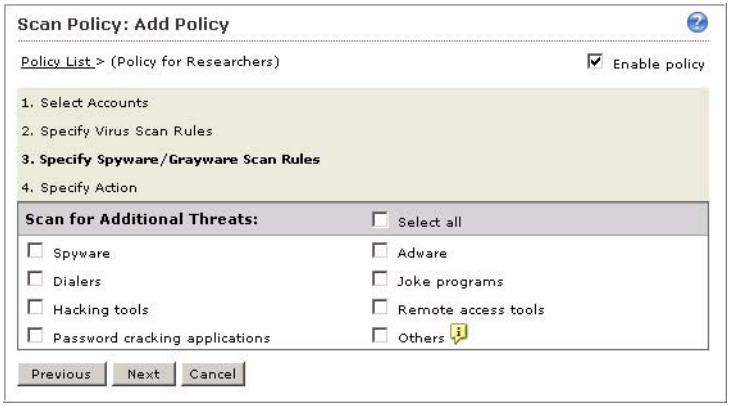


FIGURE 5-7 Spyware, grayware and additional threat scan configuration

Setting the Scan Action for Viruses

After configuring the HTTP virus scanning rules, configure the actions that IWSS will take if an infected file, password-protected or macro-containing file is detected.

Scan Actions

There are four actions that IWSS can take in response to the outcome of virus scanning:

- Choose **Delete** to delete an infected file at the server. The requesting client will not receive the file. This action can be applied to the *Infected files*, *Uncleanable files*, and *Password-protected files* scan events.
- Choose **Quarantine** to move a file (without cleaning) to the quarantine directory (by default):

  `/etc/iscan/Quarantine`

  The requesting client will not receive the file. This scan action can be applied to all four of the scan events. You can optionally choose to encrypt files before sending them to the quarantine directory. For more information, see *Quarantined File Handling* starting on page 89.

- Choose **Clean** to have IWSS automatically clean and process infected files. The requesting client will receive the cleaned file if it is cleanable, otherwise the uncleanable action is taken. This action can be applied to the *Infected files* and *Macros* scan events. For macro-containing files, the Clean action strips the macro from the file, whether the macro is a virus or benign, to protect your network before an updated virus pattern is released and deployed.
- Choose **Pass** to send the file to the requesting user. This action can be applied to the *Uncleanable files*, *Password-protected files* and *Macros* events. The Pass action should always be used for Macros events, unless you want to strip or quarantine all macro-containing files during a virus outbreak.

Note: Trend Micro does not recommend choosing the *Pass* scan action for uncleanable files.

Scan Events

After scanning, you can configure actions for the four possible scanning outcomes:

- **Infected files**: Files determined to be infected with a virus or other malicious code. Available actions are **Delete**, **Quarantine** or **Clean** (recommended and default action).
- **Uncleanable files**: Depending on the type of virus or malicious code infecting a file, the scan engine may not be able to clean some files. Available actions are **Delete** (recommended and default action), **Quarantine** and **Pass**.
- **Password-protected files**: Files that cannot be scanned because they are either password-protected or encrypted. The infection status of these types of files cannot be determined. Available actions are **Delete**, **Quarantine** (recommended and default action) and **Pass**.
- **Macros**: Microsoft Office files that contain macro program code. Since many of the fastest spreading viruses are macro viruses, you can quarantine all macro-containing files during the early stages of a virus outbreak in order to block all files before the new virus pattern is added to the pattern file and deployed to your environment. Available actions are **Quarantine**, **Clean** and **Pass**. Unless there is a need to quarantine or strip macros during a virus outbreak before an updated pattern file is released, the action for Macro should always be set to pass.

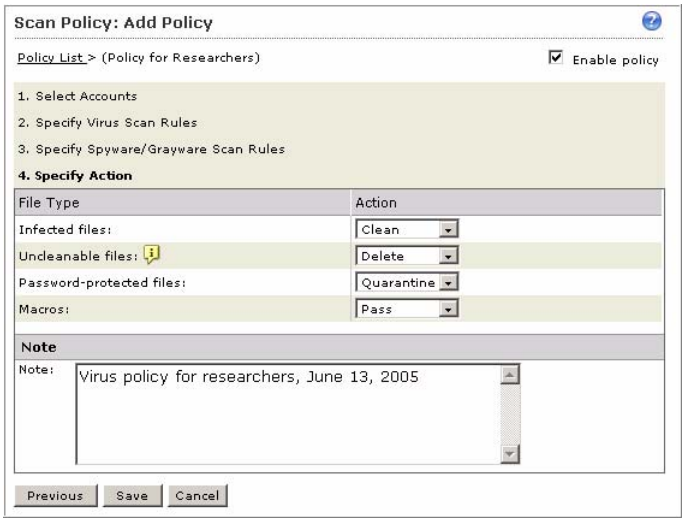


FIGURE 5-8 HTTP virus scanning policy action configuration

Adding Notes to Your Policy

To record notes about your policy, type them into the **Note** field at the bottom after configuring the actions taken against files detected by IWSS.

When you have completed configuring the scan actions to apply to your policy, click **Save**. Click **Deploy Policies** to immediately apply the policy. Otherwise, the policy will be applied after the database cache expires.

Java Applet and ActiveX Security

IWSS Applets and ActiveX scanning blocks malicious Java applets and unsecured ActiveX controls at the Internet gateway—preventing them from infiltrating your network and performing malicious acts on client workstations.

IWSS employs a tiered technology approach that operates on both the Internet gateway server and on desktops.

- On the server, IWSS prefilters Java applets and ActiveX controls based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.
- On client workstations, IWSS code, inserted into Java applets, monitors the behavior of the applets in real time and determines whether their behavior is malicious according to a pre-configured security policy.

Figure 5-9 illustrates how IWSS scans and blocks malicious applets and ActiveX objects.

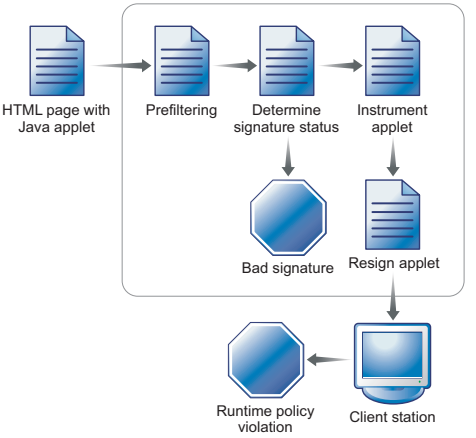


FIGURE 5-9 How Java applet security works

How Applets and ActiveX Security Works

As applets and ActiveX objects pass through the gateway, the validity of their digital signatures are checked. In addition, IWSS monitors applets in real-time on the client workstations and issues an alert if any prohibited operations are attempted.

Step 1. Filtering Applets & ActiveX at the Server

As Java applets and ActiveX controls are downloaded to the proxy server, IWSS filters them according to the following criteria:

For ActiveX Objects...

If ActiveX security is enabled, IWSS checks the signatures of CAB files and executable COM objects (of which ActiveX controls are a type) that are digitally signed. It will then examine the digital certificates contained in the signature and compare them with those in the IWSS-specific certificate database. ActiveX objects not signed, invalidly signed, or signed using an unknown root Certification Authority (CA) certificate can be blocked. In their place, the system creates a new HTML page containing a warning message. This new page is then delivered to client workstations.

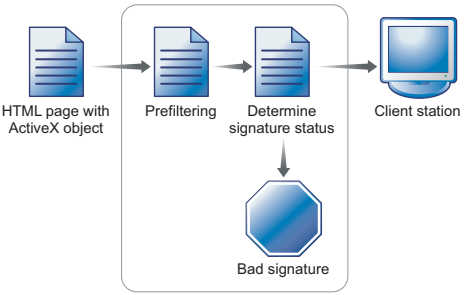


FIGURE 5-10 How ActiveX security works

For Java Applets...

IWSS filters Java applets based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.

If signature verification is enabled, IWSS will verify the signatures of digitally signed applets. Those not signed, signed using an unknown or inactive root Certification Authority (CA) certificate, signed using a flagged certificate, or invalidly signed can be blocked. They are then replaced with a new applet that displays a warning message. If certificate checking is disabled, the system accepts all Java applets regardless of the certificates they carry.

IWSS keeps a database of recognized certificates, which is used in the filtering process. This database is automatically updated to include any unrecognized certificate the system encounters. You can delete entries from the database and enable or disable entries on the **HTTP > Applets and ActiveX > Manage Digital Certificates** screen (see *Managing Digital Certificates for Applet Processing* starting on page 112).

For Java Applets, IWSS first performs Steps 2 and 3 below before sending the applets to the clients.

Step 2. Instrumenting Java Applets

IWSS analyzes the applet code to determine any potentially dangerous actions that it may perform. It then adds instrumentation code, that is, instructions that notify the user of certain programming operations, to monitor and control these actions.

During instrumentation, IWSS inserts monitoring code around suspicious instructions and then attaches the security policy assigned to the intended recipients. Depending on how IWSS is configured, this security policy may vary from one client to another based on the domain they belong to, or their IP addresses. IWSS supports creating multiple policies that can be mapped to different groups of users in your network. IWSS uses the inserted monitoring codes and the attached security policy to monitor the applet's behavior in real-time and to determine whether or not this behavior is malicious.

Note: The process of instrumenting a signed applet renders the signature invalid. Therefore, the signature is stripped, leaving it unsigned. IWSS can optionally re-sign the applet if required by the client browser.

Step 3. Optionally Re-signing Instrumented Applets

If configured to do so, IWSS re-signs the instrumented applets using an imported "private key" before sending them to client workstations. Since applets lose their original signatures during the instrumentation process (due to modifications to their original code), you may want to use this feature to ensure that the clients' Web browsers will run the instrumented applets with the permissions they may require to run correctly.

IWSS supports the import of a "private key", along with the associated certificate that contains the corresponding "public key," for use in the re-signing process. You can purchase this key from any of the well-known Certifying Authorities (CAs). Only one re-signing key may be configured for use at any given time.

Note: Re-signing applies only to validly signed applets. If the system is configured to accept unsigned applets, these applets will bypass this process and will be delivered to client workstations immediately after instrumentation.

Step 4. Monitoring Instrumented Applet Behavior

When the applet executes in the browser, the instrumentation is automatically invoked before any potentially dangerous operation is performed. The instrumentation determines whether an action is permitted by comparing it with the attached security policy. If the action is permitted, IWSS then allows the action to take place. Otherwise, IWSS takes the configured action, which can be one of the following:

- Stop the applet and display a message.
- Notify the users and give them the option to allow the behavior, terminate the behavior, or stop the applet.

Enabling Applet/ActiveX Security

To start scanning your HTTP traffic for malicious applets and ActiveX objects, enable this scanning from either the Applets and ActiveX policy page or Summary > Scanning page.

To enable malicious Applets and ActiveX scanning in HTTP traffic:

1. Select **HTTP > Applets and ActiveX > Policies** from the main menu. Alternatively, you can select **Summary** from the main menu.
2. Check **Enable Applet/ActiveX security**.
3. Click **Save**.

Adding and Modifying Applet/ActiveX Scanning Policies

The first step when configuring a new policy is to set the client accounts to which the policy will apply. See *Configuring the Scope of a Policy* starting on page 65 for more information and procedures for setting a policy's scope using the three different user identification methods.

All configured policies are listed on the **Applets and ActiveX Policies** screen available from **HTTP > Applets and ActiveX > Policies**.

FIGURE 5-11 Applets and ActiveX Policy policies

To modify the scope of a policy:

1. Open the **Applets and ActiveX Policy** screen (**HTTP > Applets and ActiveX > Policies** from the main menu).
2. Do one of the following:
   - To remove accounts from a policy's scope, select the users, click **Delete** and then **Save**.
   - To add accounts to a policy's scope, click the **Policy Name**, switch to the **Account** tab, add or delete the accounts to which the policy applies, and click **Save**.
3. Click **Deploy Policies**. Changes to a policy's scope do not take effect until the modified policies are deployed.

After configuring the scope of your policies, configure the applet and ActiveX scanning rules.

Configuring Java Applet Security Rules

On the **HTTP > Applets and ActiveX > Policies** screen, add a new policy or select an existing policy. On the **Java Applets Security Rules** tab, IWSS can be configured to either block all applets, or to accept and process applets using the security settings that you specify.

Signature Status

A digital signature is a way to verify the genuine publisher of an applet. It also allows you to verify that the applet has not been tampered with or otherwise changed since it was published. After analyzing the applet's signature, IWSS makes one of the following determinations:

- Valid signature
- No signature: the applet is unsigned
- Invalid signature: the applet's signature is corrupt or cannot be verified for some reason, for example, no trusted root certificate is found

Checking the signature of an applet is done in two steps. The first is a verification of the integrity of the applet code against data in the signature. The second is a verification of the integrity of the certificates, the "certificate chain", used to create the signature. For the signature to be considered valid, the certificate chain must end

with a certificate known to IWSS that is trusted. The set of these certificates can be viewed and managed by opening the management console to **HTTP > Applets and ActiveX > Digital Certificates > Active Certificates**.

Certificate Status

Java applet security rules can apply different actions to applets that have valid signatures, based on their certificate status.

By default, IWSS trusts its active certificates. However, an active certificate can be "flagged" if you no longer want to trust applets that have a flagged certificate in their certificate chain. Flagged certificates continue to be listed as active certificates, though the flagged status is noted.

Instrumentation and Re-signing

Instrumentation is the process through which IWSS adds monitoring and control code to the applet. Since the instrumentation process breaks the applet's signature, if any, you can alternatively choose to re-sign an applet after instrumentation. This ensures the instrumented applets will execute in the browser and perform operations as expected.

Applet Instrumentation Settings

The purpose of instrumenting applets is to prevent applets from executing prohibited operations on client machines. By default, Java applets processed by IWSS are not allowed to perform the following types of operations:

- Destructive operations: Deleting and renaming files
- Non-destructive operations: Listing files in a directory or retrieving file attribute information
- Write: Writing new or modifying existing files
- Read: Reading file contents

Configuring Exceptions

For each of the types of operations that can be selectively allowed or prohibited, you can configure file or folder exceptions where the security policies will not apply.

- To allow a given type of file operation, except when performed by a subset of files, check the **Enable** button next to the file operation. Click the **Exceptions**

link. The **Exceptions to File Operations** screen displays. Configure the files and folders where the operation is not allowed.

- To generally disallow a given type of file operation, except for a subset of files, check the **Disable** button next to the file operation. Click the **Exceptions** link and then configure the files and folders where the operation is allowed.

To configure Java applet processing settings:

1. After setting the scope of your policy, do one of the following:
   - Select **Process Java applets using the following settings** for IWSS to pass, block or instrument the applet based on its signature and certificate status.
   - Select **Block all Java applets** for IWSS to not allow any applets to pass to the clients. If you choose this setting, proceed to step 3.
2. For each of the following signature and certificate status, choose the processing action to use (* denotes the default Trend Micro-recommended settings):
   - **Valid signature, trusted certificate**: Pass*, Instrument applet (re-sign), Instrument applet (strip signature), Block
   - **Valid signature, flagged certificate**: Pass, Instrument applet (re-sign), Instrument applet (strip signature), Block*
   - **No signature**: Pass, Instrument Applet*, Block
   - **Invalid signature**: Pass, Instrument Applet (strip signature), Block*

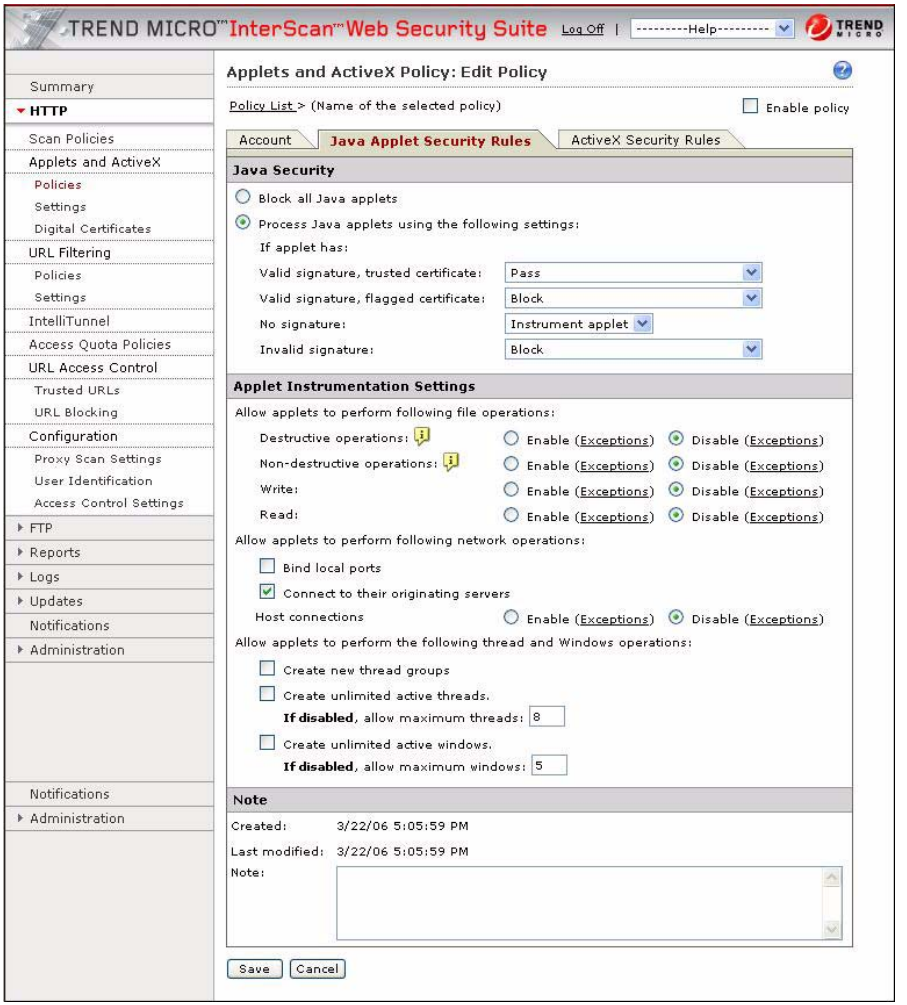


FIGURE 5-12 Java Applet security rule configuration screen

3. For each of the four (destructive, non-destructive, write or read) operations that can be selectively enabled or disabled, click the **Enable** or **Disable** button to configure your security policy.

4. Click the **Exceptions** button, and then configure the files or folders that are exceptions to the security policy:
   a. Enter the **Directory/File Path** of the files that will not apply to the configured security policy.
      - To configure a specific file path, check **Exact file path**.
      - To exclude the entire folder's contents from the security rule, check **Include all files in this directory**.
      - To exclude all of the folder's files, plus those in sub-directories, from the security rule, check **Include files in this and all sub-directories**.

Note: All file paths are those on the client machine, where the applet will run. The file path format should be in the form required by the operating system running on the client.

---

   b. Click the **Add** button to add the exceptions to the given security policy.
   c. Configure other files or directories to exempt from the applet's security settings.

d. When you've completed configuring your file and folder exceptions, click **Save**.

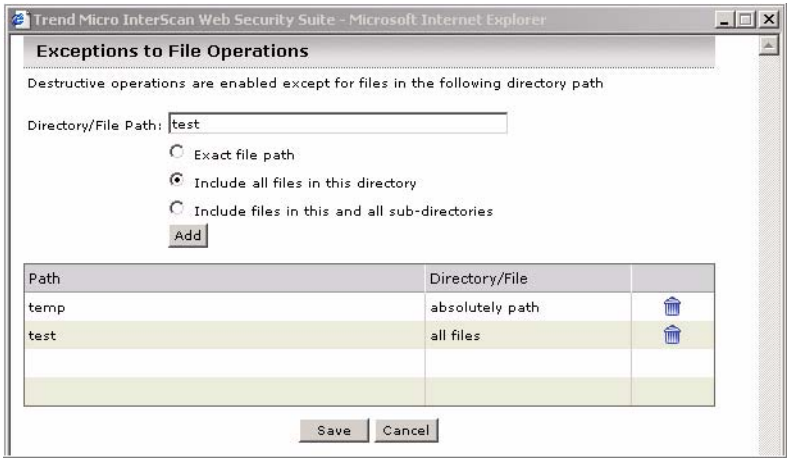


FIGURE 5-13 Java applet instrumentation settings exception files and folders

5. Back on the **Java Applet Security Rules** tab, to allow applets to bind to ports on the client workstation, select **Bind local ports**.
6. To allow applets to connect to their originating servers, select **Connect to their originating servers**.
7. To allow applets to connect to hosts other than the ones they originated from, check **Enable** or **Disable** next to **Host connections**, then configure exceptions to the security policy.
   - **a.** Enter the **Host** that will not apply to the configured security policy.
   - **b.** Click the **Add** button to add the exceptions to the given security policy.
   - **c.** Add others host that will not apply to the security policy.

d. When you've completed configuring the hosts that are exceptions to the policy's security rules, click **Save**.

FIGURE 5-14 Exceptions to the Java applet host connection rules

8. Choose **Create new thread groups** to allow applets to create new thread groups. To disallow this operation, clear it.
9. Choose **Create unlimited active threads** to have IWSA ignore thread activity from applets downloaded to clients on the LAN. Clear the box and specify a limit to restrict the number of threads applets can create at one time.
10. Choose **Create unlimited active windows** to limit the number of active top-level windows applets can open. Enter the number of allowable windows in the provided text box. Clearing this option gives applets the freedom to open as many windows as they want — just like some malicious Java applets do to annoy users.
11. Enter any optional **Note** for future reference about this policy.
12. Click **Next** to continue with configure ActiveX security rules if you are configuring a new Applets and ActiveX policy. If you are modifying an existing policy, click **Save**.
13. Click **Deploy Policies** to immediately apply the policy. Otherwise, the policy will be applied after the database cache expires.

Enter any notes to save pertinent information about this policy, and click **Save**.

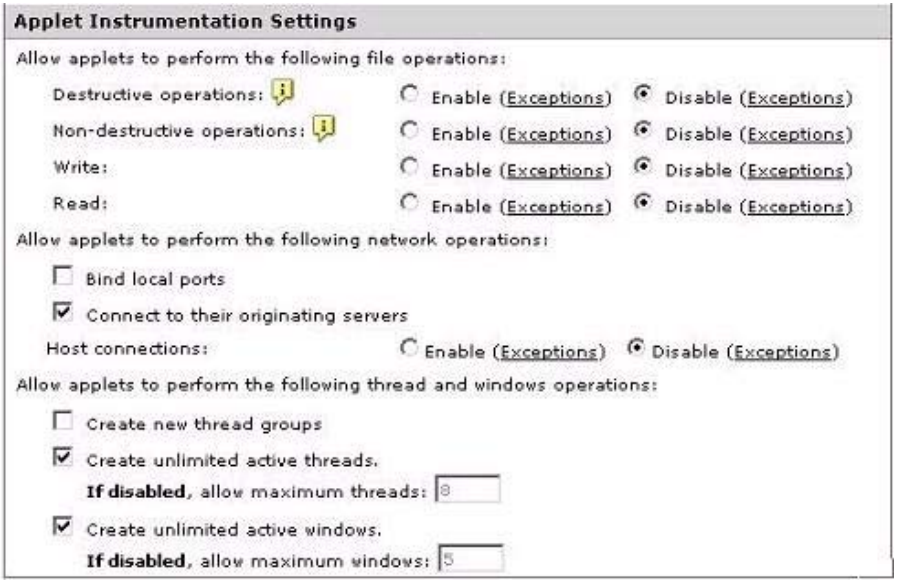


FIGURE 5-15 Applet Instrumentation Settings

Configuring ActiveX Security Rules

ActiveX security rules can be applied to the two different types of ActiveX controls:

- Executable cabinet files (*.cab): An ActiveX control distributed using the Windows native compressed archive format.
- Portable executable (PE) files (*.exe, *.ocx, and so on): An executable file format that has "portability" across all 32-bit and 64-bit versions of Windows.

For each of these two file types, you can configure security policies to:

- Block all ActiveX controls of that type
- Allow all ActiveX controls of that type
- Verify signatures, and alternatively block invalidly signed or unsigned files

Enter any notes about this policy and then click **Save**.

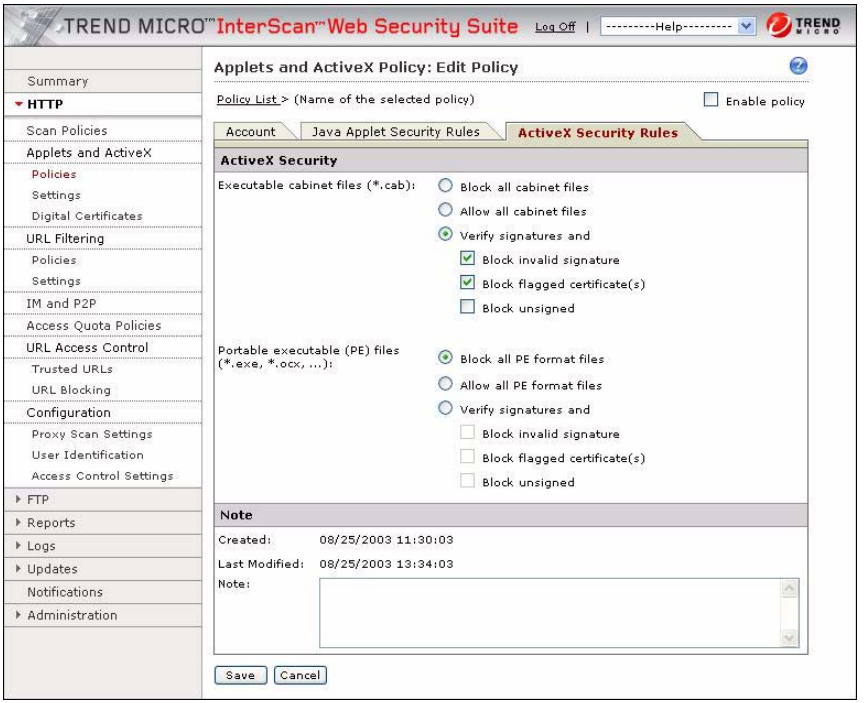


FIGURE 5-16 ActiveX security rules configuration

Applet and ActiveX Settings

Applet and ActiveX security policies determine certificate and signature status as configured on the **Applet and ActiveX Settings** page. For example, IWSS can either attempt to validate signatures, strip the signatures and process all applets as being unsigned, or optionally check the certificate's revocation status. In addition, IWSS can optionally re-sign applets after instrumentation.

To validate the signature of an ActiveX control, IWSS can check the expiration of the signing certificate, check all certificates in the signing chain (exclusive of the signing certificate) and check the revocation status of the certificate (where a revocation information source is available for a certificate).

To configure how IWSS validates Java applet and ActiveX signatures:

1. Click **HTTP > Applets and ActiveX > Settings** from the main menu.
2. Complete the settings on the **Java Applets** and **ActiveX Executable**s tabs.
3. Click **Save**.

Java Applet Signature Validation

When IWSS processes signed applets, it can handle digital signatures in one of two ways:

- Strip signatures and treat all incoming applets as unsigned applets, a restrictive security setting that treats all applets, signed or unsigned, in the same manner. In a normal client browser environment, the unsigned applet will not have access to the client system's resources, but it can still produce annoying behavior such as opening many windows.

- Perform full signature validation on the applets.

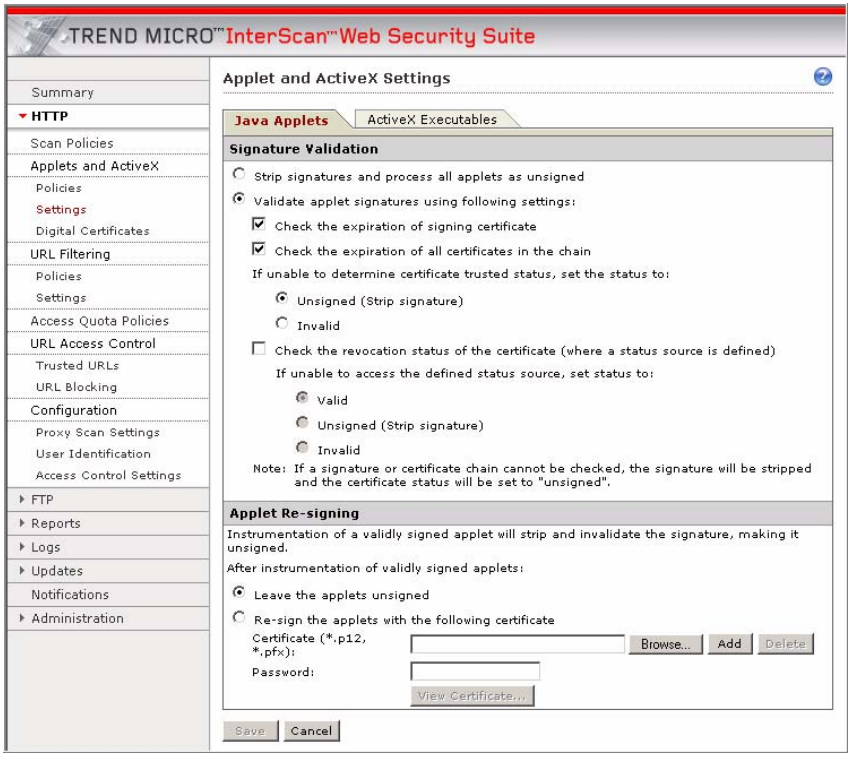


FIGURE 5-17 Applet and ActiveX Settings configuration page

Certificate Expiration

IWSS can be optionally configured to:

- Check that the certificate used to sign the applet has not expired
- Check that the certificates in the certification path are all valid

Untrusted Signature Status

If IWSS is unable to determine whether the certificate should be trusted owing to its certification path, then the applet's signature status can be set to:

- Unsigned (which means the signature is stripped, or
- Invalid

Revocation Status

Digital certificates can be revoked by their issuer. IWSS can check whether a certificate has been revoked when a status source is available.

If IWSS cannot access the defined status source, you can configure IWSS to set the status of the certificate to Valid, Unsigned (Strip signature) or Invalid.

Applet Re-signing

IWSS can re-sign instrumented applets with your company's own "private key" before they are sent to client workstations. Since applets lose their original certificates during instrumentation, you may want to re-sign them to ensure that clients' Web browsers will always accept the applets without any restrictions.

To use the re-signing feature, you need two keys: 1) a "private key" that must be imported into IWSS, and 2) a certificate containing the "public key" equivalent to your "private key" that must be imported into your clients' Web browsers. The certificate enables the browsers to recognize the signature you affix to instrumented applets. Without this certificate, these applets will be treated as another unsigned applet—either blocked by the browser or given limited access to system resources.

IWSS supports the PKCS12 key format. If you do not have a key yet, you can purchase one from any of the well-known Certificate Authorities (CAs).

To re-sign applets after instrumentation:

1. On the **Java Applets** tab of the **Applet and ActiveX Settings** page (**HTTP > Applets and ActiveX Settings**), check **Re-sign the applets with the following certificate**.
2. Type the path or **Browse** to the certificate to use for re-signing.
3. Enter the certificate's **Password**.
4. Click **Add**.
5. Click **Save**.

ActiveX Signature Validation

To verify whether an ActiveX control is validly signed, IWSS can check the control's certificate in several ways—for both a Cab file and PE file. This validation includes checking the expiration of the signing certificate, the expiration of all certificates in the signing chain, or by checking the revocation status of the certificate (when a status source is defined).

To configure how IWSS checks the signature status of a signed ActiveX control:

1. Select **HTTP > Applets and ActiveX > Settings** from the main menu, and click the **ActiveX Executables** tab.
2. Enable the types of signature checking to use for ActiveX controls:
   - Verify that the signing certificate has not expired
   - Check that all of the certificates in the certifying path have not expired
   - When the certificate's issuer is defined, verify whether the certificate has been revoked by the issuer
   - Signature timestamps can be checked. If set, a signature with an expired certificate will be considered valid if it has a valid timestamp countersignature.
3. If IWSS is unable to access the certificate's issuer, then the status of the signature can be set to either **Valid** or **Invalid**.
4. Click **Save**.

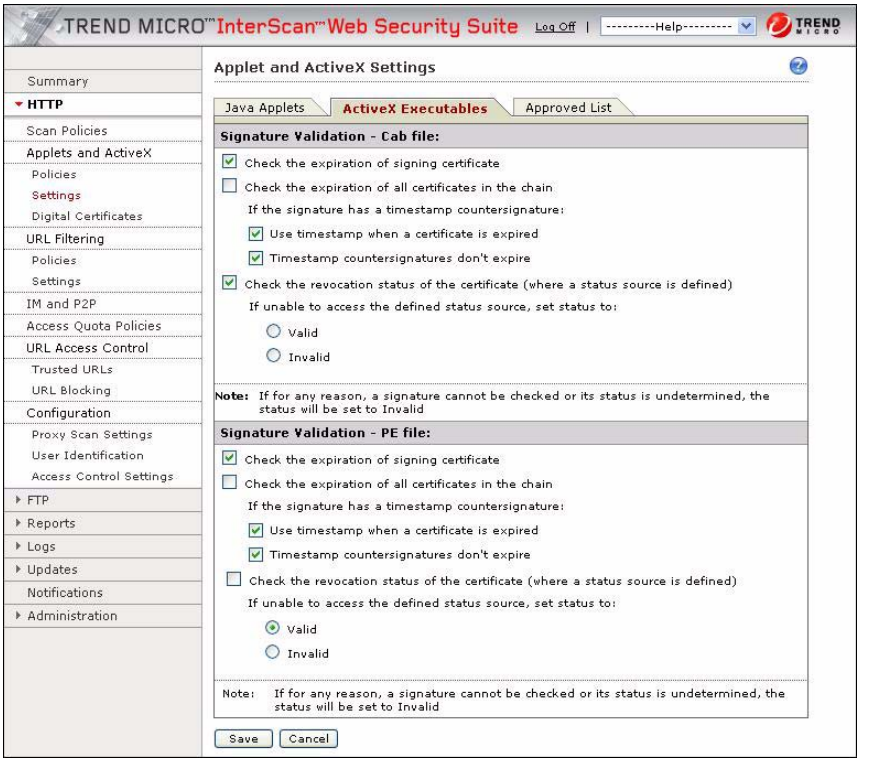


FIGURE 5-18 ActiveX control signature validation configuration

Managing Digital Certificates for Applet Processing

In order for IWSS to determine that an applet's signature is trusted, the root Certification Authority (CA) certificate on which the signature is based must be added to the IWSS certificate store.

There are three types of digital certificates that are involved in producing a digital signature: 1) the "end" or "signing" certificate, which contains the public key to be used to validate the actual applet signature; 2) one or more "intermediate" Certification Authority (CA) certificates, which contain the public keys to validate the signing certificate or another intermediate certificate in the chain; and 3) the

"root" CA certificate, which contains the public key used to validate the first intermediate CA certificate in the chain (or, rarely, the signing certificate directly). An otherwise valid signature will be "trusted" by IWSS if the root CA certificate of the signature is known to IWSS, is active, and is not flagged.

Note: When IWSS encounters an unknown certificate during applet signature processing, it saves the certificate in the "inactive" list along with the URL of the applet that contained the signature. All types of certificates will be collected in this way (signing, intermediate, and root). If required later, a root CA certificate collected this way can be "activated" (made trusted by IWSS) so that the signatures of applets that depend on it can be processed as valid. Intermediate CA and end certificates may be activated, but this will only have an effect if the root certificate is also activated. In other words, activating an intermediate CA or signing certificate does not make them trusted (only root CA certificates can be made trusted), but any certificate may be flagged.

To manage the certificates in the IWSS certificate store, you can perform the following operations:

- Delete a certificate: Removes the selected certificate(s) from the certificate store.
- De-activate a certificate: Keep the certificate in the IWSS certificate store, but do not trust certificates that use it in their certification path.
- Activate a certificate: Make a root CA certificate trusted.
- Flag the certificate: Flag all signatures that use the certificate in its certification path.
- Clear flagged certificate: Re-instate the trusted status of a certificate that was previously flagged, so that certificates that use the certificate in their certification path will be trusted.

To view existing certificates:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. Switch between the **Active Certificates** and **Inactive Certificates** tabs to see which certificates are already known to IWSS.

To add a trusted certificate:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.

2. Ensure the **Active Certificates** tab is active.

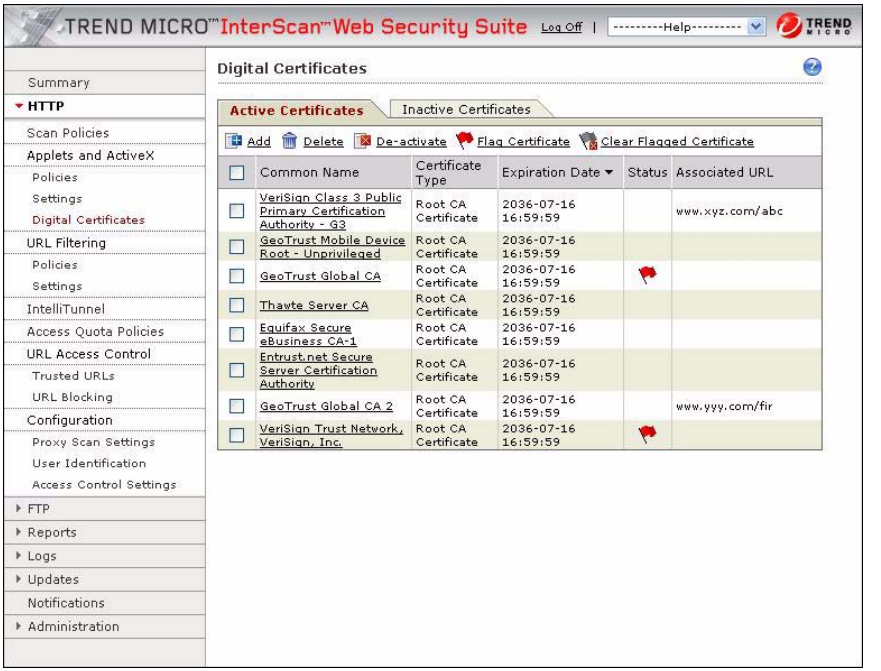


FIGURE 5-19 Active certificates in the IWSS certificate store

3. Click **Add**.

   The **Add Certificates** screen displays.

4. Type the path or **Browse** to the certificate to add and click **Add**.

Note: Certificates are commonly contained in files with the extensions .cer, .der, .crt. Also note that, as stated above, only active root CA certificates are considered trusted, but any active certificate may be flagged.

The screen returns to the **Active Certificates** tab. The certificate that you added should be visible, along with the type of certificate and its expiration date.

To delete a certificate:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. Select the certificate(s) to delete.
3. Click **Delete**.

To de-activate a trusted certificate:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Check the certificate(s) to de-activate.
4. Click **De-activate**.
5. The certificate(s) that you selected moves to the **Inactive Certificates** tab.

To activate a certificate:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. Make sure the **Inactive Certificates** tab is active.
3. Select the certificate(s) to activate.
4. Click **Activate**.
5. The certificate(s) that you selected moves to the **Active Certificates** tab.

To flag a certificate:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Select the certificate(s) to flag.
4. Click **Flag Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, with a red X in the status column.

To remove a certificate from being flagged:

1. Select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.

2. Make sure the **Active Certificates** tab is active.
3. Select the flagged certificate(s) to be cleared (certificates with flagged status have a red X in the **Status** column).
4. Click **Clear Flagged Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, with a red X in the **Status** column.

Client Side Applet Security Notifications

There are several alert messages that may be displayed in the client's browser in response to IWSS Java applet security policies.

If an applet is blocked due to its signature or certificate status, the requesting client is presented with a message showing the policy that blocked the applet, along with the reason:

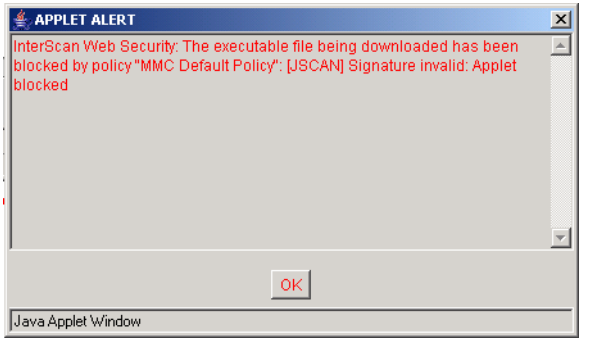


FIGURE 5-20 Blocked applet notification

If an instrumented applet attempts to perform an operation that is not allowed by a policy's configuration, a notification displays the disallowed operation and the user is prompted how to proceed. Available options are:

- **Allow**: The instrumented applet continues to run, including the operations not allowed by the policy.
- **Disallow**: The operation that triggered the Applet security policy is stopped, but the instrumented applet continues to run.

- **Stop Applet**: The instrumented applet is terminated.

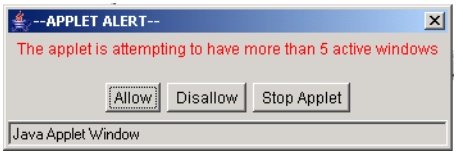


FIGURE 5-21 Applet security violation notification

If the client chooses **Stop Applet**, another notification is displayed to indicate that the applet has terminated.

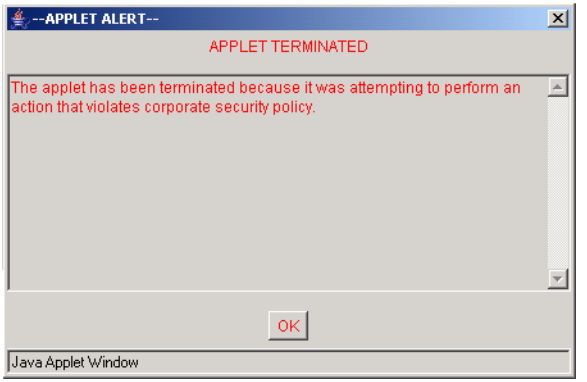


FIGURE 5-22 Applet execution termination notification

Chapter 6

Access Quotas and URL Access Control

Access quotas limit a client's bandwidth consumption to a fixed amount per unit of time. URL trusting can improve browsing performance by exempting trusted URLs from scanning and other IWSS operations. URL blocking refuses requests to URLs that you specify or whose patterns are contained in the PhishTrap pattern file.

Topics in this chapter include:

- Using access quota policies to set a limit on client bandwidth consumption
- Exempting scanning of trusted URLs to improve browsing performance to low-risk sites
- Blocking all access to sites
- Using the PhishTrap pattern file of known phishing sites
- Submitting suspicious URLs to Trend Micro for further analysis

Introduction to Access Quota Policies

The IWSS access quotas Guest Policy limits the HTTP bandwidth used by clients who access the Internet through the IWSS guest port. A policy for other clients can also be defined (there is no access quota Global Policy)—if no policy matches the connection, then the client has unlimited access. After modifying access quota policies and saving the policies to the database, the IWSS service in a multiple server configuration environment reloads the policies according to the time-to-live (TTL) value configured on the **HTTP Configuration** page (**Administration > IWSS Configuration > Database**).

If the quota is exceeded while making a download, the download is allowed to continue. However, succeeding downloads/browsing requests (before the access quota interval expires) are refused. Users are allowed access again after the access quota interval expires.

Note: For a group quota policy, the quota is for each client within the policy's scope, and all clients in the same policy have the same quota.

Managing Access Quota Policies

The clients within the scope of an access quota policy, the bandwidth quota and the time interval for the quota's duration are configurable.

To add an access quota policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. Select **Enable access quota control**.
3. From the drop-down menu, select the access quota interval—either **Daily**, **Weekly**, or **Monthly**.

Note: The value for the access quota interval is globally applied to all access quota policies, including all existing policies.

4. Click **Save**.

FIGURE 6-1 User-defined policies on the Access Quota Policies page

5. Click **Add**.
6. Select **Enable policy** and enter the access quota.
7. Select the users to which the policy applies. The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers)* or *User/group name via proxy authorization*. These settings are configured on the **HTTP > Scan Policies > Virus Scan Policy > Add/Edit Policy** screens. For more information about configuring the user

identification method and defining the scope of a policy, see *Configuring the User Identification Method* starting on page 54.

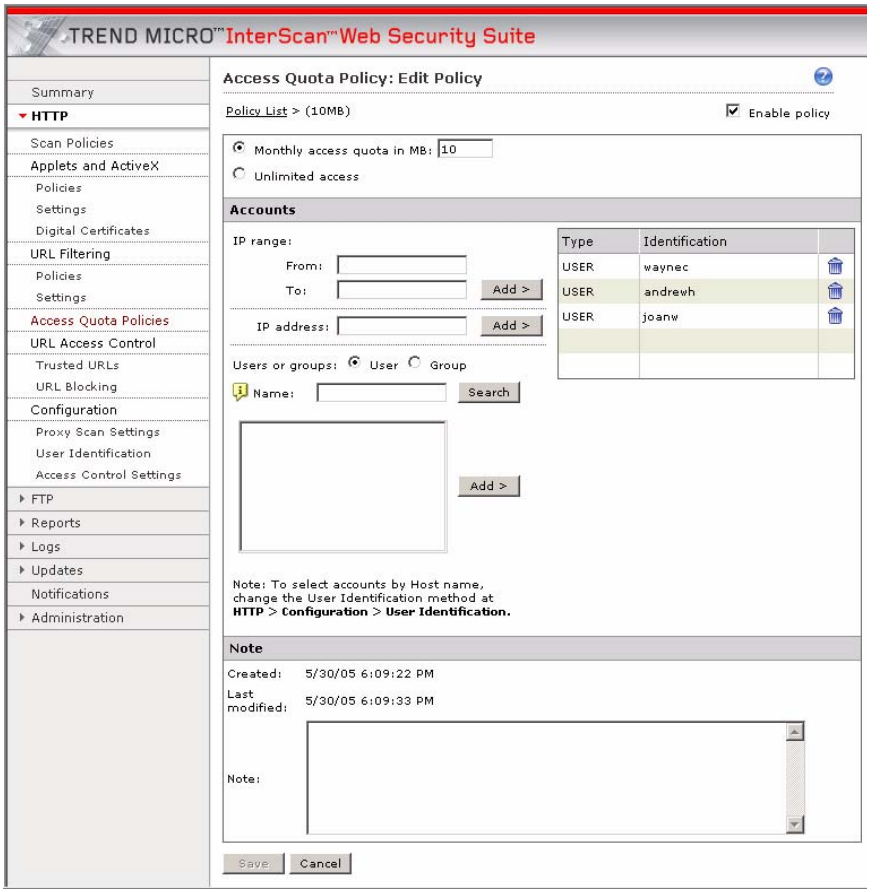


FIGURE 6-2 Access Quota Policy configuration page

Note: Regardless of the user identification method that you have configured, you can always enter IP addresses of the clients to which the policy will apply.

8. Type some optional notes to record any special information about the policy.

9. Click **Save**.
10. When returned to the **Access Quota Policies** page, click **Deploy Policies** to immediately apply the policy. Otherwise, the policy will be applied after the database cache expires.

There may be times when you want to temporarily deactivate a policy, without deleting the settings from the database.

To deactivate a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, click the linked item in either the **Account** or **Access quota** column to take you to the Edit Policy screen.
3. Clear **Enable policy** at the top of the screen and click **Save**.

If you no longer have any need for a policy, for example, if the employee using the client leaves your organization, you can either delete the whole policy or users within the policy's scope from the IWSS database.

To delete a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, select the policy and click **Delete**.

URL Access Control

IWSS can optionally "trust" some URLs and exempt them from scanning and filtering to improve browsing performance to low risk sites. It can also block access to sites via a user-configured list, or by checking requested sites against the PhishTrap pattern file, a compilation of sites associated with "phishing" schemes or other malicious acts.

Configuring Trusted URLs

IWSS can be optionally configured to trust some URLs and exempt them from scanning and filtering. Since this opens a security risk by allowing unchecked content into your network, configuring a URL as "trusted" must be considered carefully. Since trusted URLs are not scanned, browsing performance is improved. Good candidates for trusting are Web sites that are frequently accessed and contains content you can control, for example, your company's intranet sites.

If you installed the HTTP stand-alone proxy handler, trusted URLs are exempted from all IWSS modules. If you installed the ICAP proxy handler, REQMOD activities, for example, URL filtering, Webmail upload scanning and URL blocking, cannot bypass the trusted URLs list.

Trusted URL information is kept in the [URL-trusting], normalLists section of the intscan.ini configuration file.

When configuring trusted URLs, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Exact-match strings within a requested URL

You can apply exceptions to sites that would otherwise match the criteria for the trusted URL list, so IWSS scans or filters them as usual.

A list of trusted URLs and their exceptions can also be imported from a file, in addition to configuring them through the user interface. Write a comment or title (which IWSS will ignore) at the top of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group sites to be blocked under `[block]` as shown in the example, and group exceptions under `[allow]`. For example:

```
URL Blocking Import File {this title will be ignored}

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

Managing your trusted URLs and exceptions:

1. Click **HTTP > URL Access Control > Trusted URLs** from the main menu.
2. In the **Trusted URLs** configuration page, select **Enable URL trusting**.
3. Select how you want to specify the URL to trust:
   - **Web site** match (including all sub-sites)

- **String** match (URL must contain the string)

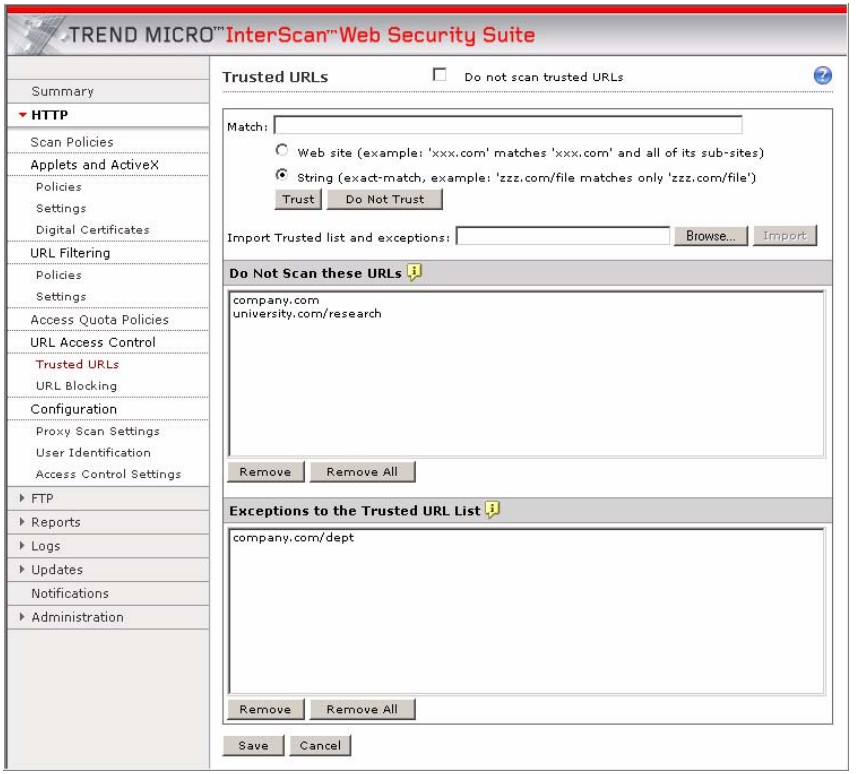


FIGURE 6-3 Enter the URLs that will not be scanned

4. Type the URL string to **Match** and click **Trust** to add it to the Trusted URLs list (shown below the **Do Not Scan these URLs** section). To configure exceptions to the trusted URLs list, click **Do Not Trust** and your entry will be entered under **Exceptions to the Trusted URL List**.
5. To remove a trusted URL or exception from your trusted URLs list, highlight the item and click **Remove**. **Remove All** clears all the respective items.
6. Click **Save**.

To import a list of trusted URLs and their exceptions:

1. Click **HTTP > URL Access Control > Trusted URLs** from the main menu.
2. Browse or type the name of the file that contains the list of trusted URLs and their exceptions into the **Import Trusted list and exceptions** field.
3. Click **Import**. The trusted URLs and their exceptions from the file appear in the appropriate fields on the interface.
4. Click **Save**.

Blocking URLs

IWSS can block Web sites and URL strings in both ICAP and HTTP proxy mode.

Note: If you have installed the ICAP proxy handler, configure the ICAP client to scan files in pre-cache request mode to make this feature work. The stand-alone proxy requires no additional configuration.

When configuring URLs to block, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Keyword matching within a URL
- Exact-match strings within a requested URL

You can apply exceptions to the blocked URL list so IWSS allows requests as usual. Using this feature, you can block a given site yet allow access to some of its sub-sites or files. The URL Blocking list (including exceptions) are maintained in the `/<install_folder>/URLB.ini` file. The path for the `URLB.ini` file is set using the “normalLists” parameter under the [URL-blocking] section in the `intscan.ini` file.

You can also block URLs based on pattern matching with the PhishTrap pattern file, a database of patterns of Web sites associated with phishing or related schemes.

In addition to adding the URLs through the management console, URL block lists can be imported from a text file.

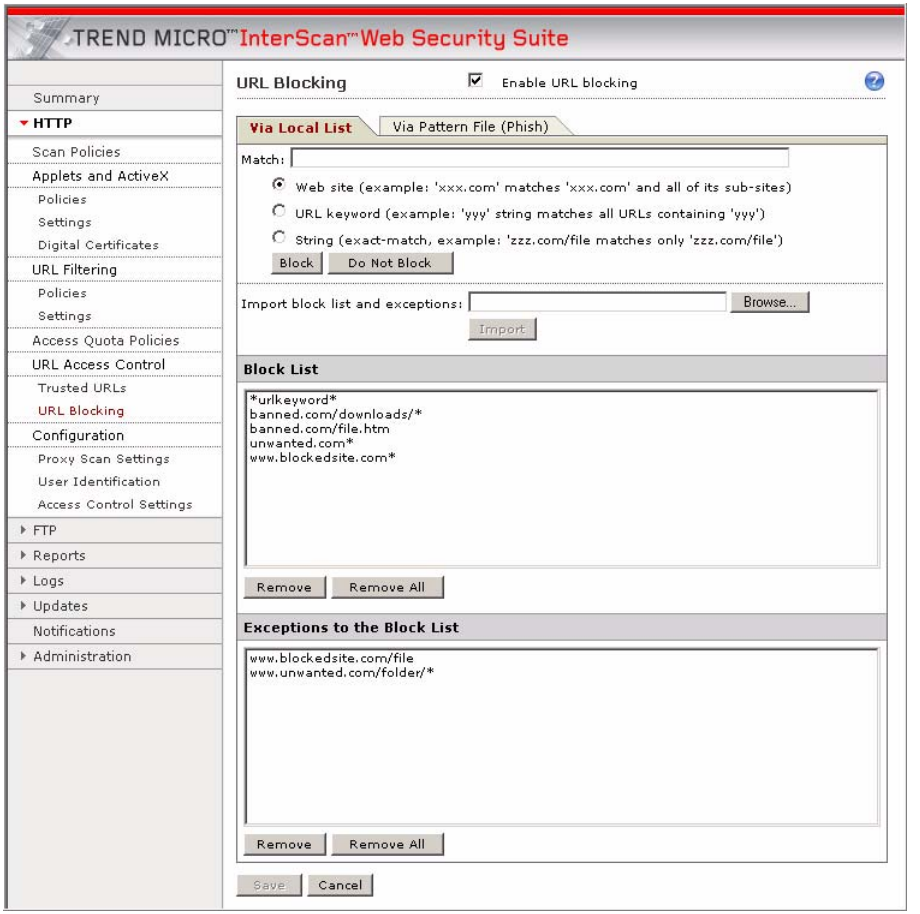


FIGURE 6-4 URL Blocking via Local List configuration screen

Via a Local List

You can configure IWSS to block access to URLs based on a list of blocked sites and exceptions that you maintain for your environment.

Configuring URLs to block:

1. Click **HTTP > URL Access Control > URL Blocking**.
2. Select **Enable URL blocking**.
3. On the **Via Local List** tab, type the full Web address or URL keyword, or exact-match string in the **Match** field.

   To identify a folder or directory in a given Web site, use a forward slash (/) after the last character. For example, if you want to block `www.blockedsite.com` but allow access to its `charity` directory:

   a. Type `www.blockedsite.com` in the **Match** field, and then click **Block**.

   b. Type `www.blockedsite.com/charity/` in the **Match** field, and then click **Do Not Block**. (If you write `charity` without the forward slash, IWSS will consider `www.blockedsite.com/charity` as a file.)
4. Click **Remove** to remove the highlighted entries from the list (or **Remove All** to remove all entries).
5. Click **Save**.

Note: When adding URLs to the **Block List** and **Exceptions to the Block List**, it is best that you first make all additions to one list and then save this configuration before you make additions to the other list. This method will help ensure that the same URL does exists in both lists. If you attempt to add a URL to the **Block List** or **Exceptions to the Block List** and it already exists in the other list, IWSS will prevent the addition and display a warning message stating that the entry already exists in the other list.

Importing a List of Blocked URLs from a File

IWSS can import a list of URLs to block from a file. Write a title or comments on the first line of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group sites to be blocked under `[block]` as shown in the example, and group exceptions under `[allow]`. For example:

```
URL Blocking Import File {this title will be ignored}

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

If importing the list is not successful, verify that you have followed the specified format for the URL Blocking import file before contacting customer support. Be sure you have:

- Listed blocked entries under [block] and exceptions under [allow]
- Formatted entries containing wildcards as described in this document or the online help

To import a list of URLs to block:

1. Format a text file as described above with the URLs to block, along with any exceptions.
2. Click **HTTP > URL Access Control > URL Blocking** from the main menu.
3. Specify the location of the file to import in the **Import block list and exceptions** field by clicking **Browse**, and then click **Import**.
4. Click **Save**.

Note: To include the "*" and "?" characters in a URL blocking string rather than having IWSS consider them as wildcards, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to block `www.example.com/*wildcard` literally, specify the blocking rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

Via Pattern File (PhishTrap)

Phishing is a malicious hacker term that means electronically hunting for a victim. "Phishers" imitate an email message from a company with whom the user has an account. These fraudulent email messages seem authentic, and many recipients are deceived into supplying their personal information, such as a credit card account number, eventually resulting in the user becoming a victim of computer crime.

PhishTrap is a Trend Micro service that leverages:

- the ability of IWSS to block outbound access to a specific URL
- the capability of the Trend Micro antivirus team to collect and analyze customer submissions and distribute a database of known harmful URLs.

PhishTrap can minimize harm from private and confidential information from being sent out from the client. PhishTrap also prevents access to known phishing URLs.

The URL that is determined to maliciously collect user information will be added to the PhishTrap pattern file. The PhishTrap pattern file is a list of URLs that IWSS will block. IWSS periodically retrieves the updated PhishTrap pattern file via ActiveUpdate.

IWSS allows users to submit suspected phishing URLs to TrendLabs for evaluation. TrendLabs evaluates the Web site and determines whether the submitted URL is malicious. The URL is considered malicious if it meets the criteria for one of the categories listed below.

- Phishing: A fraudulent collection of confidential information. This can be done by offering an email message or Web site that poses as a communication from a legitimate business, which requests information for the purpose of identity theft.
- Spyware: A hidden but legal program that secretly collects confidential information. Spyware monitors a user's computing habits and personal information, and then sends this information to third parties without the user's approval.
- Virus accomplice: An outbound HTTP request due to known behavior of malicious code—the malicious code could either send the information out or download further components from a certain URL. These are the symptoms of a spyware or trojan infection.
- Disease vector: A Web site that exists only for a malicious purpose.

Blocking URLs via PhishTrap

To block PhishTrap categories:

1. Open the IWSS management console and click **HTTP > URL Access Control > URL Blocking > Via Pattern File (PhishTrap)**.
2. Make sure that **Enable URL blocking** is enabled.
3. Enable the PhishTrap categories to block.

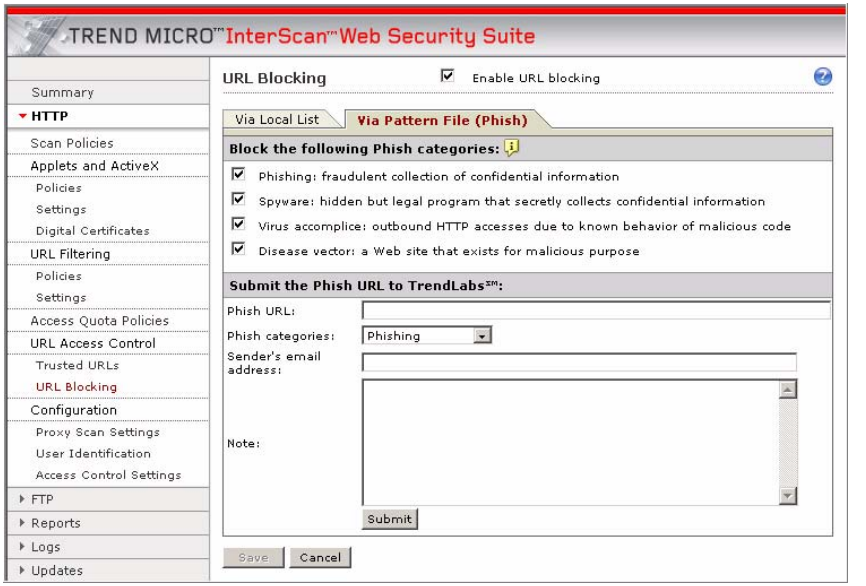


FIGURE 6-5 Block access to URLs in the PhishTrap pattern file

4. Click **Save**.

To submit a suspected phishing URL to TrendLabs:

To report a suspected phishing URL to Trend Micro, use the submission form on the URL Blocking configuration screen. Submissions are investigated, and if associated with malicious behavior, the URL is added to future releases of the PhishTrap pattern file.

1. Open the IWSS management console and click **HTTP > URL Access Control > URL Blocking > Via Pattern File (PhishTrap)**.

2. Type the URL that you want Trend Micro to investigate in the **PhishTrap URL** field.
3. Select the **PhishTrap categories** (either phishing, spyware, virus accomplice, disease vector, and others) that you think the URL is associated with from the drop-down menu under **PhishTrap categories**.
4. Type an email address where you can be contacted, if necessary.
5. Add any observations about the URL that you would like to tell our TrendLabs engineers.
6. Click **Submit**.

Chapter 7

URL Filtering

This chapter presents an overview and workflow of the InterScan Web Security Suite URL filtering module with procedures for creating and configuring policies.

Topics in this chapter include the following:

- Introducing URL filtering and how IWSS URL filtering policies work
- Understanding the URL filtering workflow
- Creating, modifying and deleting URL filtering policies
- Configuring URL filtering settings, including managing URL categories, setting URL filtering exceptions to retain access to blocked sites and setting the work and leisure time schedules
- Requesting reviews of URLs misclassified into the wrong category

Introducing URL Filtering

The default settings for the IWSS URL filtering module assume that your organization's primary interest is to avoid legal liabilities associated with viewing of offensive material. However, because there are instances that require exceptions, additional policies may be created to allow access to restricted category groups for employees whose job function requires broader access. For example, members of the Human Resources or IT departments may need unrestricted Internet access to conduct investigations into violations of your organization's acceptable Internet use policies.

In addition, IWSS also provides enhancement as it combines dynamic filtering with advanced databases. Browsing Web sites related to online trading, shopping, auction bidding, dating, gambling and other non-work related topics during work time reduces employee productivity and decreases bandwidth available for legitimate browsing. IWSS allows Internet access to be customized according to user and workgroup-specific needs, thus optimizing the use of the Internet.

IWSS allows for very flexible application of the URL filtering policy. There are three basic mechanisms for customization:

- IWSS includes a database that contains URLs in over 60 categories, such as "gambling," "games," and "personals/dating."

  Categories are contained in the following logical groups:

  - Computers/Bandwidth
  - Computers/Harmful
  - Computers/Communication
  - Adult
  - Business
  - Social
  - General
- Each category may be blocked or not blocked during time periods designated as work or leisure time.
- Different policies can be configured for different users in your environment.

Access to all identified URLs within a targeted category may be managed according to policy. The database associates each URL with one or more categories. In the

event a URL that your organization needs to access is associated with a prohibited category, Exceptions to URL Filtering can be used to override the database's classification. The patterns specified in the Approved URL List are matched against the URL, not to the content of the document to which the URL refers. IWSS gives you the option to configure a URL filtering approved-list by matching Web site, URL keyword, and exact-string categories.

The following are two rules that you can apply for a given policy in a given time period:

- Block access to configured site categories during work time
- Block access to configured site categories during leisure time

URL Filtering Workflow

The input for the URL filtering module consists of the URL and the user's ID (IP address, IP address range, user name, group name, or host name). A user is identified according to the user identification method that IWSS is configured to use (see *Configuring the User Identification Method* starting on page 54).

The output of the URL filtering module either allows or blocks access to a URL.

The URL filtering module works with the local classification database and the policy management database.

- A local classification database contains the URL classification information; thus, most classifications will be retrieved with a minimum of overhead.
- If the classification information is not available locally, a remote Web-based classification service is contacted.

The remote classification service may have more up-to-date information, or may be able to classify the URL dynamically. The classification service compiles a list of previously unclassified URLs. Once classified, these URLs are added to a master

database, which is distributed as an update to the local classification database. Such updates are periodically retrieved by IWSS via ActiveUpdate.

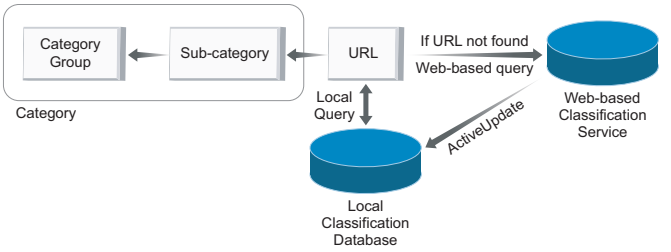


FIGURE 7-1 How URL classification works with the local and remote classification databases

A queried URL is classified into one or more of 60 plus categories, which are contained in 7 groups. With the given category classification and the user ID as input, the query is made to the policy management database. The result of the query is either allowing or blocking access to the requested URL.

Note: Manual updates to the URL filtering database can be invoked from the **Summary** screen.

Remote Classification Server Performance Considerations

Access to the remote Web-based classification service is enabled by default. Although the classification service is designed to provide quick responses to requests from all over the world, accessing it can still impart a significant performance degradation in certain circumstances (particularly if your environment has large throughput requirements and frequently needs to query the classification service).

Before accessing the remote Web-based classification service, Trend Micro recommends installing and configuring IWSS to confirm that the performance for your network is acceptable. When you are ready to enable Remote Service (RS) access, edit the `urlfcIfx.ini` configuration file in the /HTTP folder to set:

```
[network]
no_web_access=no
```

Managing URL Filtering Policies

IWSS is pre-configured with two default URL filtering policies—the Global Policy that applies to all clients on the network, and the Guest Policy that applies to clients that access IWSS through the guest port.

Note: The Guest Policy is not supported if you have installed IWSS in ICAP mode.

Note: The Hacking/Proxy Avoidance category in InterScan Web Security Suite 2.0 release has been split into two separate categories in release 3.0. If you specified this category for an IWSS 2.0 policy, then the migration process will automatically substitute the Proxy Avoidance category in its place. To retain all of the Hacking/Proxy Avoidance category, you must manually select the Hacking category in IWSS 3.0 migrated policies.

Enabling URL Filtering

Make sure that the URL filtering module is enabled before you start.

To enable URL filtering:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Select **Enable URL filtering**.
3. Click **Save**.

Creating a New Policy

Creating a new URL filtering policy is a two-step process:

- Select the accounts to which the policy will apply
- Specify the Web site categories to be blocked during work and leisure time.

To create a new policy:

1. Open the IWSS management console and click **HTTP > URL Filtering > Policies** from the main menu.
2. Click **Add**.

The **URL Filtering Policy: Add Policy** screen opens.

3. Type a descriptive **Policy name**.

   Policy names that include references to the users or groups to which they apply, for example, "URL Filtering Policy for Researchers" are easy to remember.

4. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers)* or *User/group name via proxy authorization (LDAP)*. For more information about configuring the user identification method and defining the scope of a policy, see *Configuring the User Identification Method* starting on page 54.

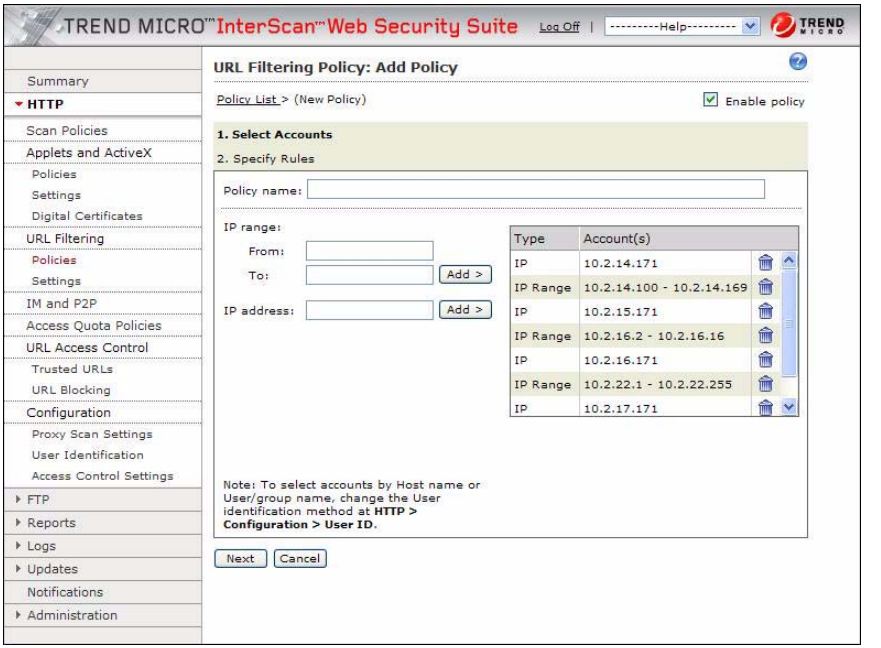


FIGURE 7-2 Specifying the user or group IP address

5. Click **Next**.
6. From the **Specify Rules** screen, ensure that **Enable policy** is selected.

7. Select the URL categories to which you want to restrict access.
   - Select the check box of the category that you want to blocked during work time. To select all the categories of a group, click **Select All** for the group. The group does not need to be expanded for you to select all categories in a group. Restricted days and hours are defined in the URL Filtering Settings (Schedule tab) page.
   - Select the check box of the category that you want to blocked during leisure time. To select all the categories of a group, click **Select All** for the group. The group does not need to be expanded for you to select all categories in a group. Unspecified times are considered "leisure" times.

   The list of groups is not configurable.
8. Type an optional **Note** to include useful information about this policy for future reference.
9. Click **Save**.
10. In the **URL Filtering Policies** screen, set the priority of the new policy (under the **Priority** column) by clicking on the up or down arrows.

Note: The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.

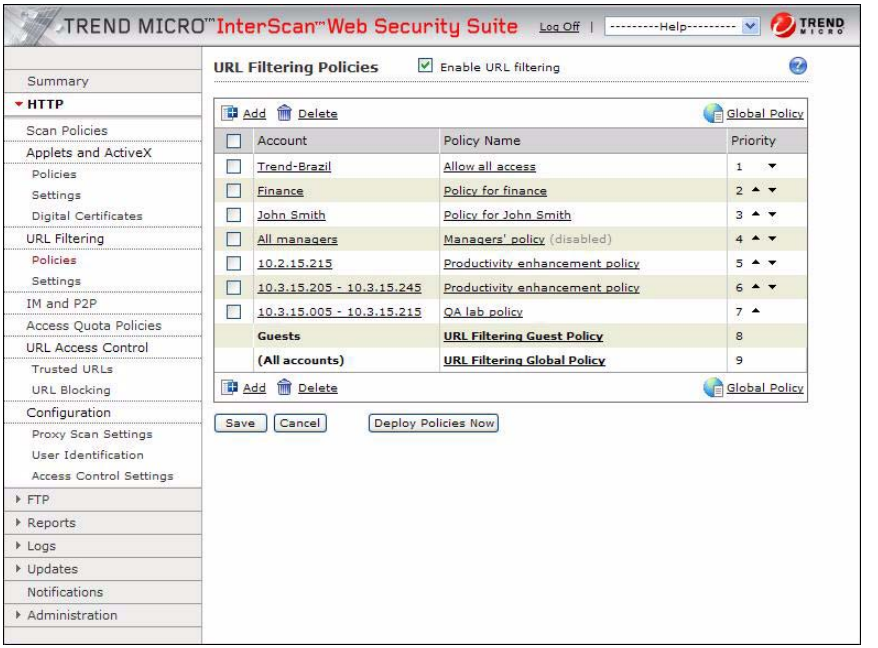


FIGURE 7-3 URL Filtering Policies screen

11. Click **Save**.
12. To immediately apply the policy, click **Deploy Policies Now**. Otherwise, the policy will be applied after the database cache expires.

Modifying and Deleting Policies

IWSS gives you the option of editing any existing policy to better suit your current environment. You can also delete unnecessary account(s) from a policy.

To modify an existing policy:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Click the **Account Name** or **Policy Name** links of the policy to be modified.
3. The **URL Filtering Policy: Edit Policy** screen displays:

- Change the scope of your policy by adding or deleting clients on the **Account** tab.
- From the **Rule** tab, modify the URL categories that clients are allowed to access.

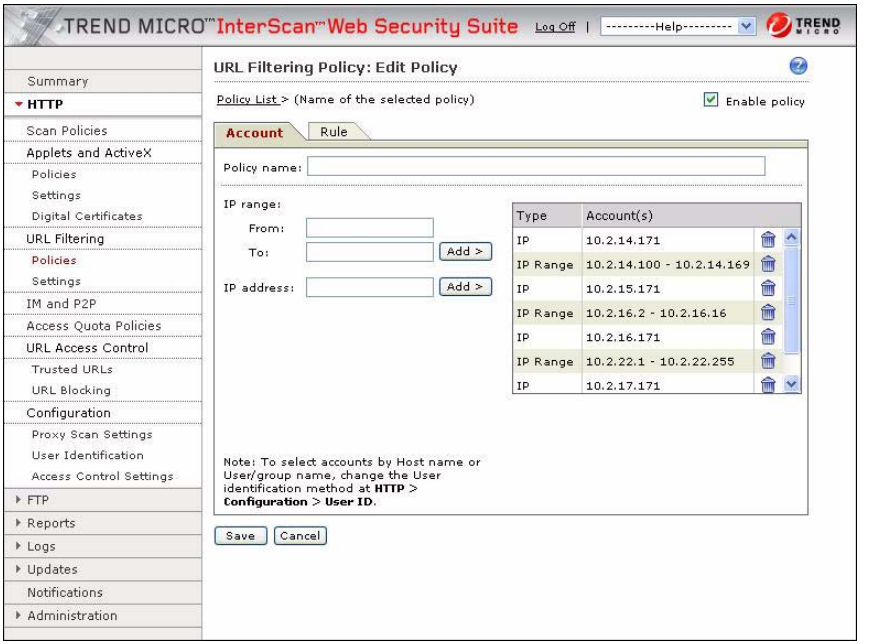


FIGURE 7-4 URL Filtering Policy: Edit Policy

4. Click **Save**.
5. Go to **HTTP** > **URL Filtering > Policies** and set the priority of your policies using the arrows. The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.
6. Click **Save**.
7. Click **Deploy Policies** to immediately apply the policy. Otherwise, the policy will be applied after the database cache expires.

URL Filtering Settings

There are several settings related to URL filtering that you can modify to reflect the realities of your work environment:

- Over 60 Web site categories which are contained in 7 logical groups
- Configuring exceptions to allow access to specific Web sites that would otherwise be blocked by a URL filtering rule
- Setting "work time" and "leisure time" schedule

Additionally, if you believe a URL is classified in the wrong category, you can send a request to Trend Micro to consider re-classifying the URL. You can also look up the category of a URL that you are not sure of.

Requesting URL Re-classification and URL Lookup

Organized in seven logical groups, IWSS includes default categories that provide a baseline level of URL filtering. For example, Web sites related to humor and jokes would be found in the "Joke Programs" category, which is located in the *Computers/Bandwidth* group. Where you do not agree with the default classification of a URL, Trend Micro enables you to suggest a re-classification.

Before rolling out URL filtering policies, Trend Micro recommends verifying that the default categorizations are appropriate for your organization. For example, a clothing retailer might need to remove a swimsuit Web site from the "Intimate Apparel/Swimsuit" category located in the *Adult* group in order to allow legitimate market and competitor research.

If you want to know a category of a URL, you can also look it up from the **URL Lookup and Re-classification** tab.

To re-classify a URL:

1. Click **HTTP > URL Filtering > Settings** from the main menu.
2. Click the **URL Lookup and Re-classification** tab.

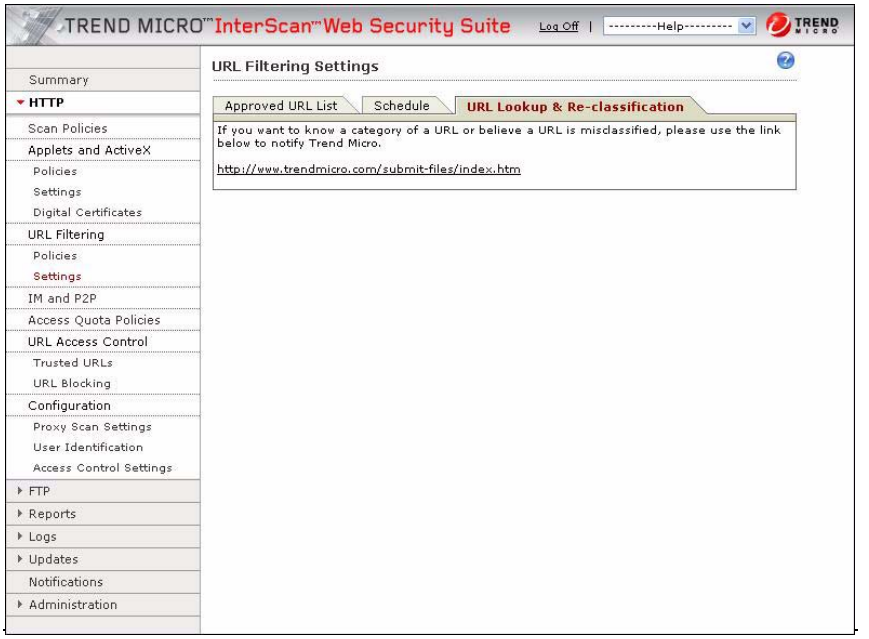


FIGURE 7-5 Re-classify URL categories in the URL Filtering Settings page

3. Click on the URL.

   The Trend Micro Online URL Query - Feedback System screen opens.

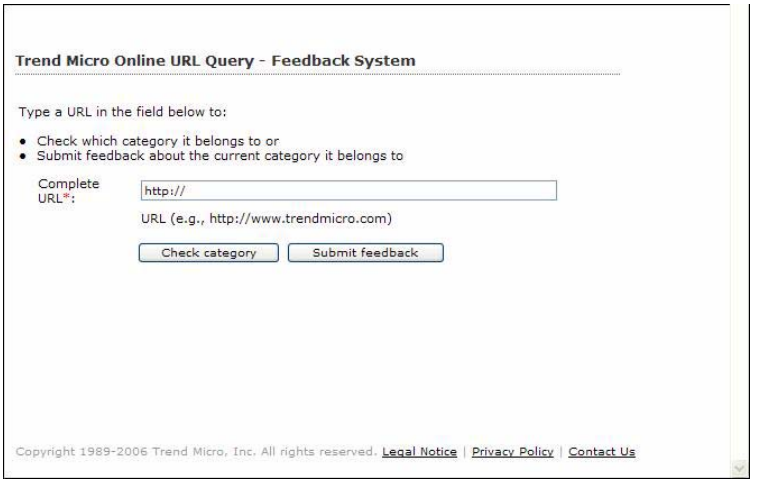


FIGURE 7-6 Trend Micro Online URL Query - Feedback System screen

4. Complete all the necessary information and then click **Submit**.

URL Filtering Exceptions

InterScan Web Security Suite gives you the option to configure exceptions to URL filtering policies to allow access to Web sites that would otherwise be blocked. If your clients have a legitimate need to view Web sites that are being blocked by URL filtering, enter the site as a URL filtering exception. In addition to entering a URL, you can also enter one of the following:

- Specific string to match within a URL
- Exact-match string to allow access to a specific file from an otherwise blocked site

The URL Filtering Exception list is maintained in the <install path> URLFilteringExceptions.ini file. The path for the URLFilteringExceptions.ini file is set using the filtering_exception_list parameter under the [url-filtering] section of the <install path> IWSSPIUrlFilter.dsc file.

To configure the URL filtering approved list:

1. Open the IWSS management console and click **HTTP > URL Filtering > Settings**.
2. In the **Approved URL List** tab, type the Web address, URL keyword, or exact-match string in the **Match** field. Identify this entry by selecting one of the three options:
   - Web site
   - URL keyword
   - String

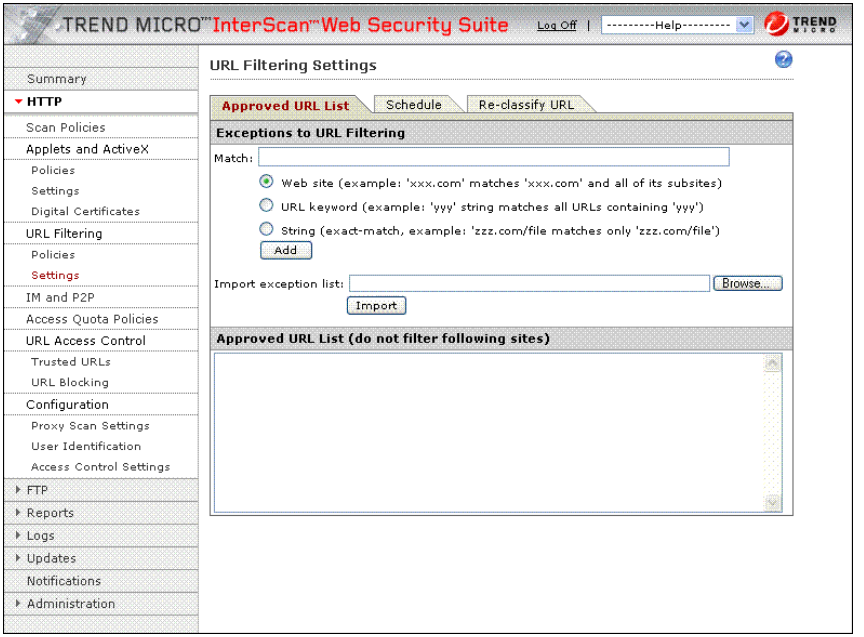


FIGURE 7-7 URL Filtering Exceptions exempt specific URLs and files from filtering

3. Click **Add** to include this entry in **Do not filter the following sites**.

   Click **Remove** to remove highlighted entries from the list (or **Remove All** to remove all entries).
   To import a list of URL filtering exceptions from a file, type or **Browse** to the location of the file in the **Import approved list** field, and then click **Import**.

Note: Format the URL filtering exceptions text file as follows:
line 1 = URL Filtering Import File
line 2 = [approved]
line 3 and so on:
Web sites, URL keywords, and strings, in the format `*information*`
For example:

```
URL Filtering Import File
[approved]
*www.trendmicro.com*
*www.antivirus.com*
```

To include the "*" and "?" wildcards literally, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to filter the site `www.example.com/*wildcard` literally, specify the filtering rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

---

4. Click **Save**.

Work and Leisure Schedule Settings

InterScan Web Security Suite enables you to specify two sets of work times: Work Time 1 and Work Time 2. Both of these work times include 24-hour selections.

When creating URL filtering policies, you can set the policy to be in effect for both Work Time 1 and Work Time 2 and/or during "leisure" time. When you set a policy for Work Time 1, it is also in effect for Work Time 2.

InterScan Web Security Suite policies permit or block access to the various URL categories during work and leisure time. By default, InterScan Web Security Suite uses the following default work time settings:

- Work days: Monday to Friday
- Work hours: 8:00 to 12:00 (Work Time 1) and 13:00 to 17:00 (Work Time 2).

Time not defined as work hours is considered “leisure.”

Before implementing URL filtering policies in your organization, Trend Micro recommends verifying that the work and leisure time settings are appropriate for your environment.

To configure the URL filtering policy schedule:

1. Open the InterScan Web Security Suite management console and click **HTTP > URL Filtering > Settings > Schedule**.
2. Under **Work Time Settings**, select the work days and work hours in the fields provided.

   From the Work Time 1 and/or Work Time 2 areas, specify the hours during which you want to restrict access to selected URL categories.

Note: It is assumed that all InterScan Web Security Suite servers in a cluster are within the same time zone.

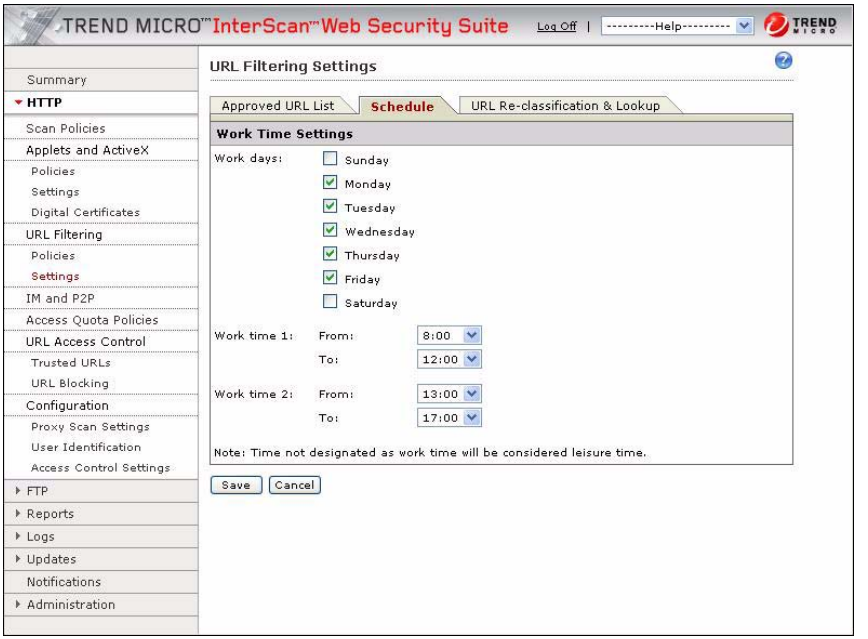


FIGURE 7-8 Define work and leisure time settings for your organization

3. Click **Save**.

To specify no work time or all work time:

- If you do not want to use work times, then uncheck all of the work days. All time will then be leisure time.
- If you want all time to be work time, then select all days and specify the following:
  - For Work time 1, choose "0:00" in the From drop-down list and "11:59" in the To drop-down list.
  - For Work time 2, choose "12:00" in the From drop-down list and "23:59" in the To drop-down list.

Chapter 8

FTP Scanning

This chapter describes FTP virus scanning and the different ways FTP scanning can be deployed and configured for your environment.

Topics in this chapter include:

- Understanding similarities and differences between FTP and HTTP virus scanning
- Configuring FTP scanning proxy options (stand-alone vs. FTP proxy)
- Understanding data connection options (passive FTP vs. active FTP)
- Configuring FTP scanning options
- Setting FTP access control settings

Introduction

InterScan Web Security Suite can scan FTP uploads and downloads for viruses and other malicious code in a similar manner to how it processes HTTP traffic. Unlike HTTP scanning, however, a single configuration is applied to all clients on your network—user or group-based policies are not supported for FTP scanning.

InterScan Web Security Suite FTP scanning uses either a stand-alone proxy or works in conjunction with another FTP proxy on the network. To deploy FTP scanning into your environment, first configure the FTP settings that control the type of proxy and the type of data connection (either passive or active FTP, see *Passive and Active FTP* starting on page 153). The next step is to configure the scanning rules that control the traffic direction that is scanned, the type of files to block or scan, how compressed and large files are handled and the actions taken when malicious code is detected.

After setting the FTP scanning settings, there are optional security and performance settings to consider modifying. Access control lists can be configured to selectively allow client FTP access based on the client's IP address. To improve performance when frequently accessing FTP sites over which you have direct control of the content, specific FTP servers can be added to a white list so that downloads from them will not be scanned. Moreover, to further lock down the InterScan Web Security Suite server, FTP access to specific ports can either be allowed or denied.

FTP Settings

InterScan Web Security Suite FTP scanning settings include options for using either the IWSS native (stand-alone) proxy or a separate FTP proxy, two options for how data connections are made (active FTP vs. passive FTP) and performance-related settings that control the maximum number of concurrent client connections and processing threads.

Proxy Settings

InterScan Web Security Suite FTP scanning provides two proxy options—a "stand-alone" mode whereby clients connect to the native IWSS proxy that later connects with the FTP server, and an "FTP proxy" mode whereby IWSS passes requests through a separate FTP proxy that in turn connects to the FTP server.

- In stand-alone mode, the client needs to use "<username>@<FTP server name>" as the FTP username to indicate which FTP server IWSS should connect to.
- In FTP proxy mode, no username is required because InterScan Web Security Suite always connects to the FTP proxy and server designated in the configuration settings.

FTP proxy mode can also be used to protect a single FTP server by specifying the FTP server's hostname/IP address and port number in the FTP proxy configuration. In this case, the InterScan Web Security Suite FTP scanning module is dedicated to the specified FTP server, in a similar manner to a reverse proxy for HTTP scanning. For more information about InterScan Web Security Suite FTP proxy options, consult the *IWSS Installation Guide*.

Passive and Active FTP

InterScan Web Security Suite uses either active or passive FTP for data connections, depending on your firewall setting. FTP uses two ports, a data port and a command port. In *active* FTP, the server connects to the client to establish the data connection. In *passive* FTP, the client connects to the server.

When passive FTP is selected in the InterScan Web Security Suite configuration, InterScan Web Security Suite converts "active" mode on the client side into passive mode on the server side. Mode conversion is performed only when the IWSS configuration is passive and the client uses active mode. If the IWSS configuration is active, no conversion is performed, so passive requests from the client are still passive requests on the server side.

Client Requests

To configure FTP settings, you need to specify the proxy settings and the data connection.

To configure FTP settings:

1. Click **FTP > Configuration > General** from the main menu.
2. Under the **Proxy Settings** section, select the appropriate FTP setting based on your topology, either **Use stand-alone mode** if you want the native IWSS proxy to connect to FTP sites, or **Use FTP proxy** for the FTP service to work with an existing FTP proxy (specify the host name of the **Proxy server** and the **Port**).

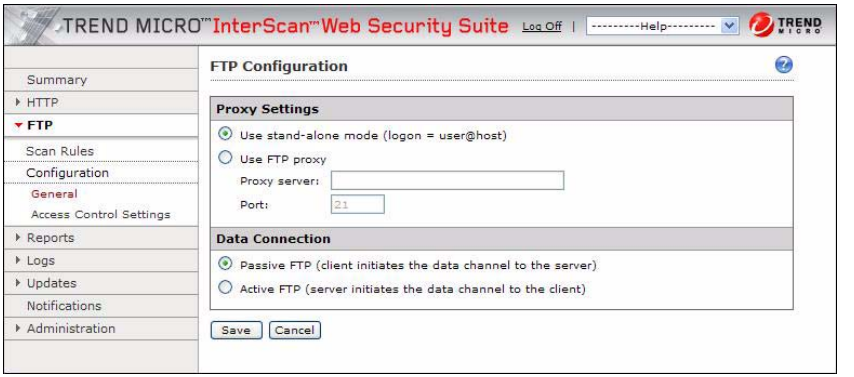


FIGURE 8-1 Configuring your FTP connection

3. Choose the type of data connection to use—either **Passive FTP** or **Active FTP**. For more information on choosing between these options, see *Passive and Active FTP* starting on page 153 or consult the *IWSS Installation Guide*.
4. Click **Save**.

FTP Scanning Options

The FTP virus scanning settings are similar to the HTTP scanning settings, with two differences:

- FTP scanning does not support user or group-based policies, thus one configuration is applied to all clients that access FTP sites through IWSS
- The traffic direction to scan can be configured—either uploads, downloads, or both

Enabling FTP Traffic and FTP Scanning

Before your clients can access FTP sites through IWSS, FTP traffic must be enabled.

To turn on FTP traffic:

1. Click **Summary** in the main menu (see Figure 2-3).
2. Click **Turn On** or **Turn Off** (at the top of the screen) to start or stop the FTP traffic flow.

Turn Off means the FTP service on the IWSS server is shut down, thus clients cannot connect to any FTP servers through the IWSS FTP proxy. The default setting is **On**.

Once the FTP traffic is enabled, FTP scanning must be turned on.

To enable or disable FTP scanning:

1. Open the IWSS management console and click **FTP > Scan Rules**. (see Figure 8-2 on page 158).
2. Select **Enable FTP scanning**.
3. Click **Save**.

Scan Direction

Depending on how you want to use IWSS FTP scanning, you can selectively configure the FTP scanning module to scan uploads, downloads or both. For example, if you have deployed antivirus software to all of the workstations in your organization, disabling uploads may be justified to achieve a performance benefit since the files should already be scanned on the client.

File Blocking

You can identify the types of files to block for security, monitoring or performance purposes. You can block file types such as Java applets, Microsoft Office documents, audio/video files, executables, images or other types that you manually configure. If your organization has policies that prohibit certain types of files in your network, IWSS FTP file blocking can stop them at the FTP gateway.

File Scanning

When configuring the types of files to be scanned, there are three options:

- All scannable files: All files are scanned (the safest option).
- IntelliScan: Only file types known to harbor viruses are scanned (file type is determined by checking the file header). See *About IntelliScan* starting on page 78 for more information.
- Specified file extensions: Only files with specified file extensions are scanned.

Trend Micro recommends scanning all files, unless performance considerations require choosing one of the other options.

Priority for FTP Scan Configuration

If the configurations on the **FTP Virus Scan** screen conflict with each other, the program will scan according to the following priority:

1. Block these file types.
2. Scan these file types (if not blocked).

Compressed File Handling

Compressed files can pose special challenges to antivirus software performance, because they must be decompressed before the individual files within the archive can be scanned. IWSS provides the option to block all compressed files at the gateway. Alternatively, compressed files can be accepted at the gateway but blocked when you specify one of the following:

- Decompressed file count exceeds a given threshold
- Cumulative decompressed file size exceeds a configured maximum
- Recursively compressed file exceeds a certain number of compressed layers
- Uncompressed file size exceeds a configured maximum percentage
- Certain file type within the compressed file is not permitted; therefore, the whole compressed file is blocked

Note: IWSS can also block specified file types within a compressed file during HTTP scanning as well.

Large File Handling

If the delay when downloading large files is unacceptable, IWSS can be configured to skip scanning of files larger than a configured threshold. Additionally, the FTP scanning module can use the "deferred scanning" method for large files to prevent the client connection from timing out. For more information, see *Deferred Scanning* starting on page 85. The FTP scanning module does not support the "scan before

delivering" and "scan after delivering" large file handling methods used by the HTTP scanning module.

Encrypting Quarantined Files

If IWSS is configured to quarantine files as a scan action, it can optionally encrypt the files to prevent them from being accidentally executed by someone browsing the quarantine folder. Note that once encrypted, the files can only be decrypted by a representative from Trend Micro's Support department.

Scanning for Spyware/Grayware

IWSS can scan for many additional non-virus risks for which patterns are contained in the spyware/grayware pattern file. For a summary of these risks, see *Spyware and Grayware Scanning Rules* starting on page 89.

Configuring FTP Scanning Settings

To configure FTP scanning:

1. Click **FTP > Scan Rules** from the main menu.
2. Select **Enable FTP scanning**.
3. Select the types of FTP transfers to scan—either **Upload**, **Download** or both.

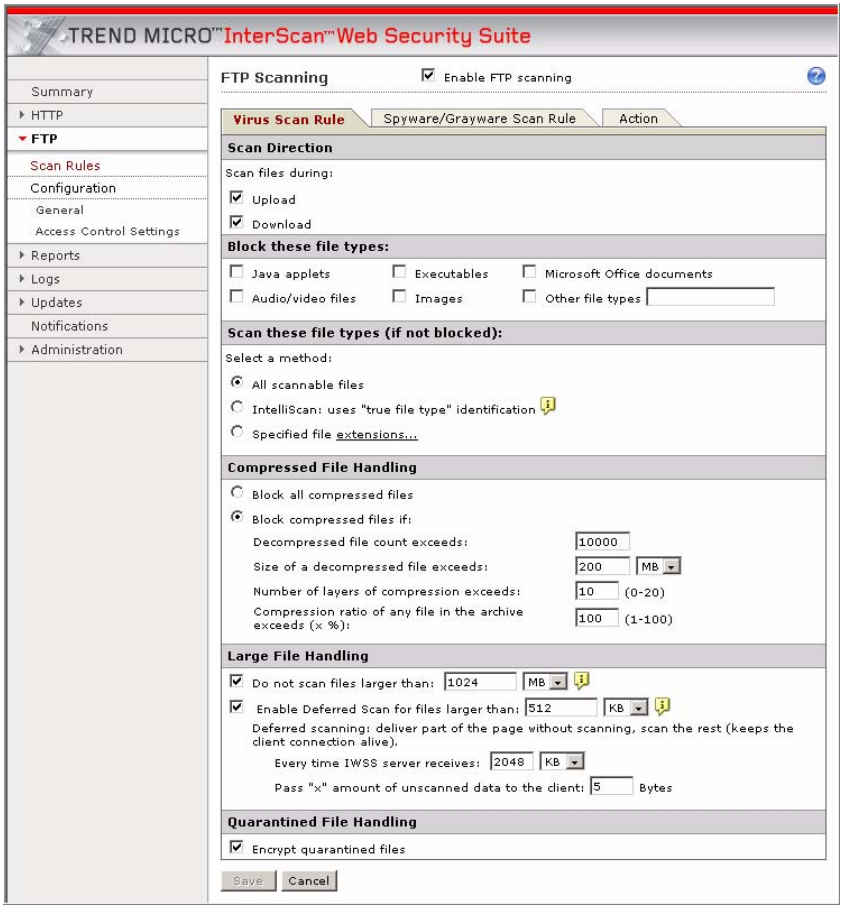


FIGURE 8-2 Configuring the FTP scanning settings

4. Under the **Block these file types** section, select the file types to be blocked. In the **Other file types** field, type other file types to block (use a space to delimit multiple entries). See Appendix, *Mapping File Types to MIME Content-types* starting on page 215 for a list of other file types that can be blocked.
5. Select the files to scan:

- To scan all file types regardless of extension, select **All scannable files**. IWSS opens compressed files and scans all files within. Scanning all files is the most secure configuration.
- To use true file type identification, select **IntelliScan**. IntelliScan uses a combination of true attachment type scanning and exact extension name scanning. True attachment type scanning recognizes the file type even if the file extension has been changed. IntelliScan automatically determines which scanning method to use.
- To scan file types based on their extensions, select **Specified file extensions**. This contains the list of file types known to harbor viruses. IWSS scans only those file types that are explicitly specified in the **Default Extensions** list and in the **Additional Extensions** text box. The default list of extensions is periodically updated from the virus pattern file.

  Use this option, for example, to decrease the aggregate number of files IWSS checks, thus decreasing overall scan times.

Note: There is no limit to the number or types of files you can specify. Do not precede an extension with the (*) character. Delimit multiple entries with a semicolon.

---

6. Under **Compressed file handling**, select from the following two options:
   - **Block all compressed files**
   - **Block compressed files if**

   If you enable the second option, type a value for the following parameters:
   - Decompressed file count exceeds (default is 10000)
   - Size of a decompressed file exceeds (default is 200MB)
   - Number of layers of compression exceeds (0-20, default is 10)
   - Compression ratio of any file in the archive exceeds (1-100%, default is 100)
7. Under **Large File Handling**, select **Do not scan files larger than** and enter the file size.
8. To avoid browser timeout issues when downloading large files, select **Enable Deferred Scan** and type the file size above which deferred scanning will occur. Also type the number of bytes to be sent to the client per data received.

WARNING! *The partial delivery of a file may result in a virus leak; thus, this would be a performance versus absolute security choice for you. Use this option only if you are currently experiencing an issue with timeouts.*

9. To encrypt files sent to the quarantine directory to prevent them from being inadvertently opened or executed, select **Encrypt quarantined files**.
10. Click **Save** and switch to the **Spyware/Grayware Scan Rule** tab.
11. Select the types of additional risks to scan for, and click **Save**.
12. Switch to the **Action** tab, and select the actions for IWSS to take in response to scanning.
13. Click **Save**.

Setting Scan Actions on Viruses

You can specify the action for FTP scanning to take upon finding an infected file (the recommended action setting is **Clean**):

- Choose **Quarantine** to move an infected file to the quarantine directory without cleaning. The requesting client will not receive the file.
- Choose **Delete** to delete an infected file at the server. The requesting client will not receive the file.
- Choose **Clean** to automatically clean and process an infected file. The requesting client will receive the cleaned file if it is cleanable.

You can specify the action for FTP scanning to take upon finding an uncleanable file, which includes worms and Trojans (the recommended action setting is **Quarantine**):

- Choose **Pass** to send an uncleanable file to the client without cleaning (Trend Micro does not recommend this choice, because it may allow infected files into your network).
- Choose **Quarantine** to move, without cleaning, an uncleanable file to the quarantine directory. The requesting client will not receive the file.
- Choose **Delete** to delete an uncleanable file at the server. The requesting client will not receive the file.

You can specify the action for FTP scanning to take in handling a password-protected compressed file (the recommended action setting is **Pass**):

- Choose **Pass** to send a password-protected file to the client without cleaning.
- Choose **Quarantine** to move, without cleaning, a password-protected file to the quarantine directory. The requesting client will not receive the file.
- Choose **Delete** to delete a password-protected file at the server. The requesting client will not receive the file.

In the event a file containing macros (not necessarily macro viruses) is detected during FTP transfers, the following actions are available (the recommended action setting is **Pass**).

- Choose **Quarantine** to move the files containing macro(s) to the quarantine directory.
- Choose **Clean** to remove macros before delivering the file.
- Choose **Pass** to disable special handling of files containing macro(s).

FTP Access Control Settings

IWSS includes several access control settings for additional security and performance tuning:

- FTP access can be enabled based on the client's IP address.
- Trusted servers over which you have close control of their content and are frequently accessed can be added to a white list and transfers will not be scanned for a performance benefit.
- The IWSS FTP server can be locked down by denying access to ports that you configure.

By Client IP

By default, all clients on the network are allowed to access FTP sites through the IWSS server (provided FTP traffic is enabled, see *Enabling FTP Traffic and FTP Scanning* starting on page 154).

To limit FTP access based on client IP address:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.

2. Switch to the **Client IP** tab.

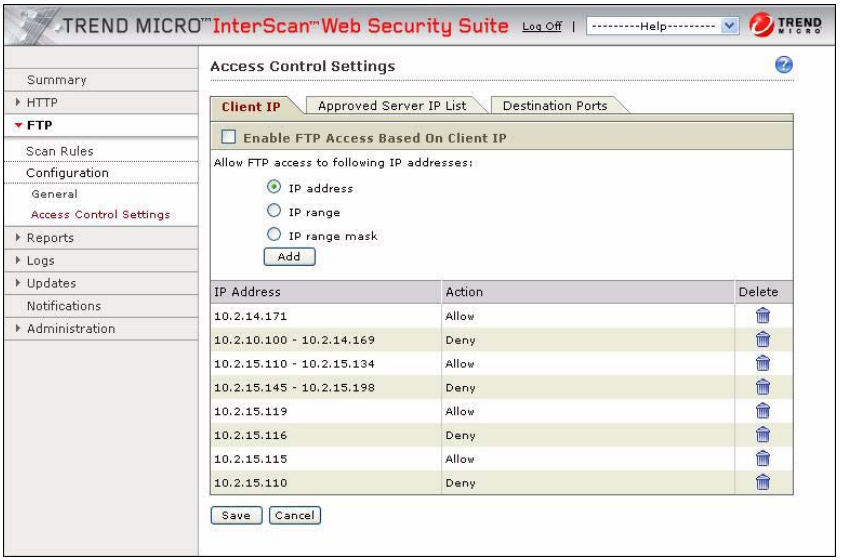


FIGURE 8-3 Access control settings restrict traffic through the InterScan Web Security Suite server

3. Select **Enable FTP Access Based on Client IP**.
4. Enter the IP addresses of clients allowed FTP access through InterScan Web Security Suite. The following are acceptable entries:
   - **IP address**: a single IP address, for example, 123.123.123.12.
   - **IP range**: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15.
   - **IP range mask**: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 will identify all machines in the 192.168.1.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32).
5. Click **Add** and continue entering other clients that are allowed access FTP sites.
6. Click **Save**.

Via Server IP White List

To reduce possible performance issues when accessing trusted FTP sites over which you directly control the content, you can exempt some FTP sites from scanning by adding their IP addresses to a white list.

Note: Skipping scanning via the IP white list only applies to file downloads. Uploaded files will still be scanned.

To add trusted servers to the white list:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.
2. Switch to the **Server IP White List** tab.

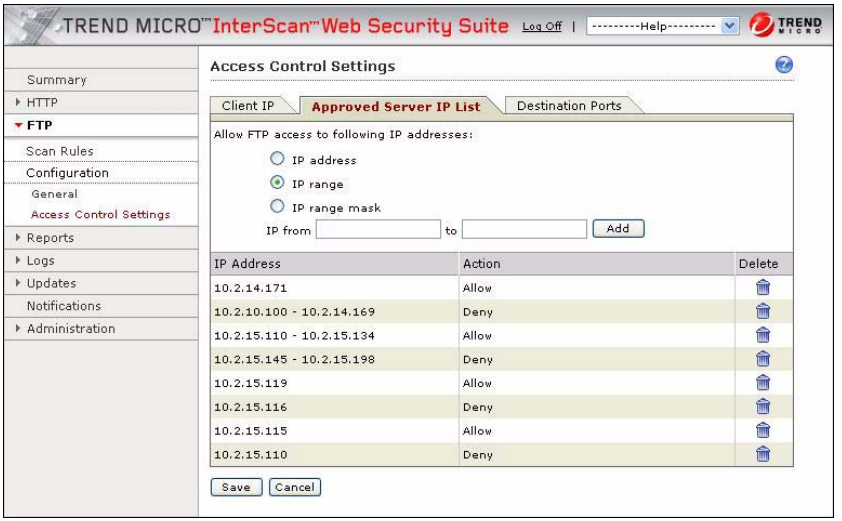


FIGURE 8-4 Access Control Settings Approved Server IP List tab

3. Enter the IP addresses of FTP sites to exempt from InterScan Web Security Suite FTP virus scanning. See *Identifying Clients and Servers* starting on page 43 for information and examples about how to identify the servers.
4. Click **Add** and continue entering other FTP sites to exempt.
5. Click **Save**.

Via Destination Ports

By default, clients can access any port on the InterScan Web Security Suite FTP server. To increase security, you can selectively allow or deny access to the ports.

To configure IWSS FTP ports to which clients can connect:

1. Click **FTP > Configuration > Access Control Settings** from the main menu.
2. Switch to the **Destination Ports** tab.

FIGURE 8-5 Access Control Settings Destination Port tab

3. Choose the action to apply to a port, either **Deny** or **Allow**.
4. Enter the **Port** or **Port Range** to which the action will apply and click **Add**.
5. Continue to add other ports to allow or deny.
6. Click **Save**.

Note: The destination port list at the bottom of the **Destination Port** tab reflects the processing order (or reverse priority order). Destination port access control is only applied during a FTP command connection, and FTP data connections are not affected. A typical configuration is 1. "Deny ALL" and 2. "Allow 21" which results in only allowing access to port 21.

Chapter 9

Reports, Logs and Notifications

This chapter describes how administrators can get timely information about their gateway security via InterScan Web Security Suite reports, logs and notifications.

Topics in this chapter include the following:

- Introducing blocking event, traffic, spyware/grayware and cleanup reports
- Configuring report settings and setting the report's scope
- Generating real-time and scheduled reports
- Customizing reports, and several examples of sample InterScan Web Security Suite report content
- Configuring the various InterScan Web Security Suite logs
- Querying and viewing logs
- Configuring log settings
- Exporting log data to CSV files and querying logs using Microsoft Excel
- Introducing notifications, including configuring email notification settings
- Using tokens in notifications to dynamically provide event information
- Using SNMP notifications

Introduction to Reports

IWSS can generate reports about virus and malicious code detections, files blocked, URLs accessed and DCS cleanups. You can use this timely information about InterScan Web Security Suite program events to help optimize program settings and fine tune your organization's security policies.

You can configure and customize reports. For example, InterScan Web Security Suite allows you to generate reports for all or specific user(s), all or specific group(s), either on-demand (in real time) or on a scheduled basis. To allow you to share the latest program information with those who need it, IWSS can send notifications via email when a scheduled report is ready for viewing.

Types of Reports

IWSS uses data from reporting logs to generate reports. You can configure InterScan Web Security Suite to write reporting log data to both the database and text logs, only to the database, or only to the text log. If you choose the text-only option, then neither reports nor logs can be viewed from within IWSS. In this case, you can only review the logs by directly opening the generated text files.

Configure reporting log options in the IWSS management console under **Logs > Settings** (see *Log Settings* starting on page 187 for more information). Text logs provide backward compatibility with previous versions of IWSS and allow further analysis of log data through custom scripts or other third-party applications. You can also use them to validate the completeness and accuracy of the data logged to the database.

There is a performance penalty for enabling the access log (**Log HTTP/FTP access events** is disabled by default). If you do not enable the access log, many reports on user activities will not be available. Moreover, if IWSS is configured as an upstream proxy, valuable data on user activities may not be available. If you want InterScan Web Security Suite to summarize all Web-related activities, enable the access log under **Logs > Settings > Reporting Logs > Options**.

Note: When the access log is enabled, the InterScan Web Security Suite service is restarted. During the restart, a router may take up to 30 seconds to recognize

InterScan Web Security Suite again, during which the router will not redirect packets.

InterScan Web Security Suite can generate the following categories of reports:

- Blocking event reports: reports about virus detections, policy violations, and blocked URLs
- Traffic reports: reports about Web browsing activity, the most popular Web sites and downloads, and other details about Web browsing activity
- Spyware/Grayware reports: Reports about spyware detections
- Cleanup reports: Reports about DCS cleanup attempts requested by InterScan Web Security Suite
- Individual user reports

The following is a list of all available reports.

Blocking-event Reports

- Riskiest URLs by viruses detected
- Users with most requests for malicious URLs
- Most violations by user
- Most violations by group
- Most blocked URL categories
- Most blocked Applets and ActiveX objects
- Most blocked URLs
- Most blocked URLs by day of the week
- Most blocked URLs by hour

Individual user reports

- Overview report
- Most popular sites visited by user
- Most blocked URLs categories by user Most infected users
- Most blocked URLs by user
- URL activity by user

Traffic Reports

- Most active users
- Most popular URLs
- Most popular downloads
- Most popular search engines
- Daily traffic report
- Top categories (weighted)
- Activity level by day of the week
- Activity level by hour

Note: Traffic reports may take a long time to generate, that is, up to a few hours for large sites with extensive access logs.

Note: To access the top categories (weighted) report, an additional license is required.

Spyware/Grayware Reports

- Most spyware/grayware detections by category
- Top spyware/grayware detections
- Most detections per user

Cleanup Reports

- Cleanup events by category
- Top cleanup events by name
- Most infected IP addresses

Report Settings

When generating a real-time report or setting up scheduled reports, you need to specify the information in this section.

Report Scope (Users and Groups)

Select the user(s) and or group(s) for which you want to generate a report. Options include:

- **All users**: all clients accessing the Internet through IWSS
- **Specific users**: clients with specific IP addresses, host name, or LDAP directory entry
- **All groups**: all groups in the LDAP directory; if using the IP address or host name identification method, then "All groups" is equivalent to "All users"
- **Specific groups**: either specified LDAP groups or a range of IP addresses

When generating reports for specific users or groups, the user selection method is determined by the method configured under **HTTP > Configuration > User Identification**. For more information about user identification, see *Configuring the User Identification Method* starting on page 54.

Report Type (Consolidated or Individual)

In Scheduled Reports, IWSS can generate consolidated reports, which contain all possible reports. In either Scheduled Reports or Real-time Reports, IWSS can generate individual reports that you specify. For a list of available reports, see *Types of Reports* starting on page 166.

Options

IWSS can present program information in either bar, stacked bar or line charts. Different chart shading for URLs or downloads blocked by IWSS versus successful requests can also be used.

Additional Report Settings

For real-time reports, specify the time period the report will cover.

When setting up a scheduled report, there are some additional settings:

- Send a notification email message when the scheduled report runs.
- Run the reports at a specific time and day.
- "Enable" the report to run at the scheduled time.

Generating Reports

Real-time Reports

IWSS allows you to generate reports in real time for either all or a subset of the clients accessing the Internet.

To configure real-time reports:

1. Click **Reports > Real-Time Reports** in the main menu.
2. Under **Time period**, select a time period for the report (either **All Dates**, **Today**, **Last 7 days**, **Last 30 days**).
3. Click **Range** to generate a report in a given time range, and then select the **From** and **To** dates.
4. Under **Report by**, select the users for which the report will be generated—either **All users**, **Specific user(s)**, **All groups**, or **Specific group(s)**. For more information about running reports for specific users or groups, see *To select specific group(s):* and *To select specific user(s):* starting on page 174.

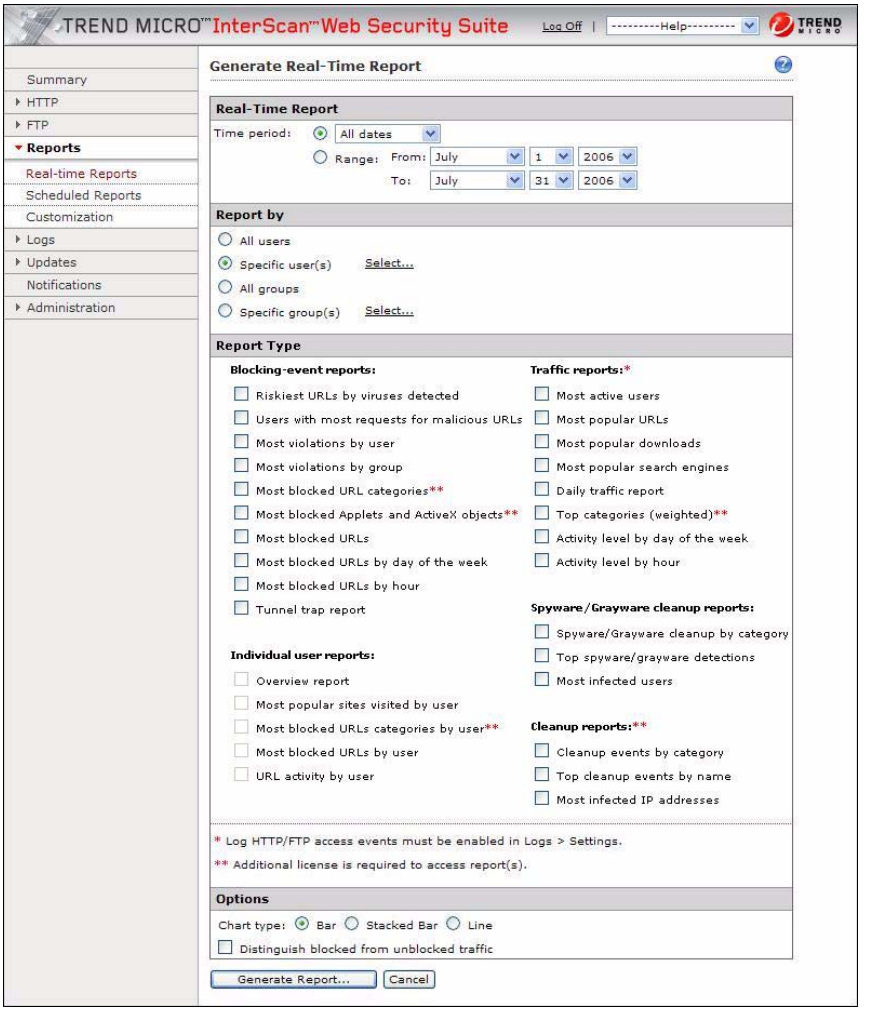


FIGURE 9-1 Generating a real-time report

5. Under **Report Type**, select the desired report parameter(s).

Note: IWSS groups multiple report parameters into a single report, with each report parameter having its own section.

6. Under **Options**, select the chart type from the menu. To denote blocked traffic from unblocked traffic using different shading, select **Distinguish blocked from unblocked traffic**.
7. Click **Generate Report**. Click **Reset** to reset the form to the default values.

The following table provides information about the parameters that can comprise a report:

Report by	Included Report Parameters
All users	Includes all listed report parameters except for "Individual user reports"
Specific users	Includes only the "Individual user reports" parameters
All groups or Specific groups	The following reports are enabled: • Most violations by group· • Most blocked URL categories • Most blocked URL categories by user • Most blocked Applets and ActiveX objects • Most blocked URLs • Most blocked URLs by day of the week • Most blocked URLs by hour

TABLE 9-1. Report parameter availability depends on the report type

To select specific group(s):

1. Click **Reports > Real-time Reports** in the main menu.
2. Under **Report by**, select **Specific group(s)**, and then click **Select**.

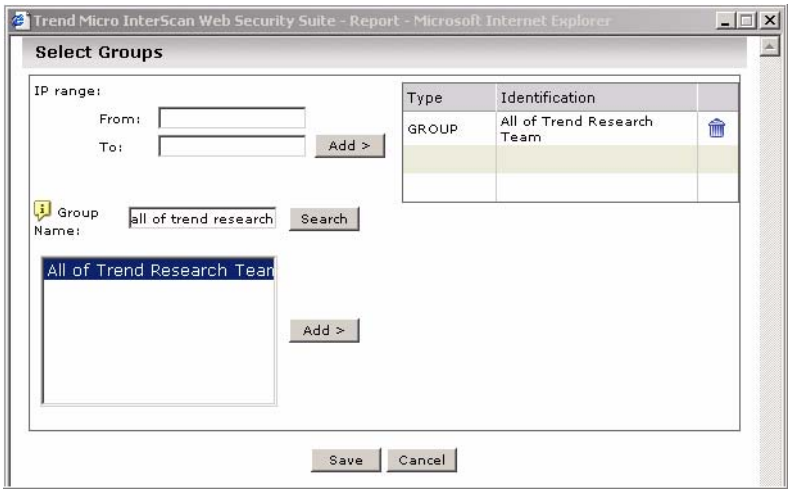


FIGURE 9-2 Configuring a report's scope using the user/group (LDAP) identification method

---

Note: When you click **Select** on **Specific group(s)** (**Reports > Real-time Reports > Report by**), the **Select Groups** pop-up screen displays according to the configured user identification method (**HTTP > Configuration > User Identification**).

---

3. Type the IP address range (or search for a group name in your LDAP directory if using the "User/group name via proxy authorization" identification method).
4. Click **Add**.
5. After adding all the groups, click **Save**.

To select specific user(s):

1. Click **Reports > Real-time Reports** in the main menu.
2. Under **Report by**, select **Specific user(s)**, and then click **Select**.

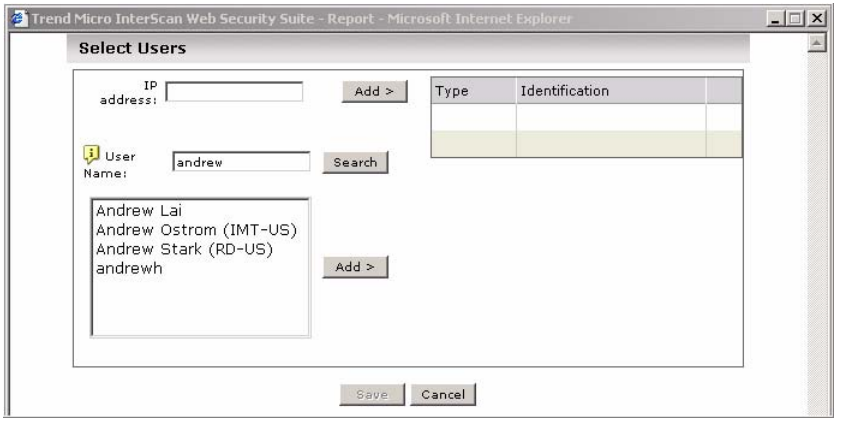


FIGURE 9-3 Configuring a report's scope using the user/group (LDAP) identification method

---

Note: When you click **Select** on **Specific user(s)** (**Reports > Real-time Reports > Report by**), the **Select Users** pop-up screen displays according to the setting made in the user identification method (**HTTP > Configuration > User Identification**).

---

3. Type the **IP address**, **Host name** or search for a user name in your LDAP directory if using the "User/group name via proxy authorization" identification method.
4. Click **Add**.
5. After adding the users to include in the report, click **Save**.

Scheduled Reports

You can configure InterScan Web Security Suite to generate scheduled reports on a daily, weekly, or monthly basis. To manage the large volume of reports generated, IWSS allows you to generate only the reports that you specify and delete unnecessary scheduled reports from the archive directory.

To configure scheduled reports:

1. Click **Reports > Scheduled Reports** from the main menu.
2. Click the tab that corresponds to the frequency of scheduled report to run—either **Daily**, **Weekly** or **Monthly**.
3. Select **Enable <*Frequency*> Report**.
4. Click the **Report Settings** link.

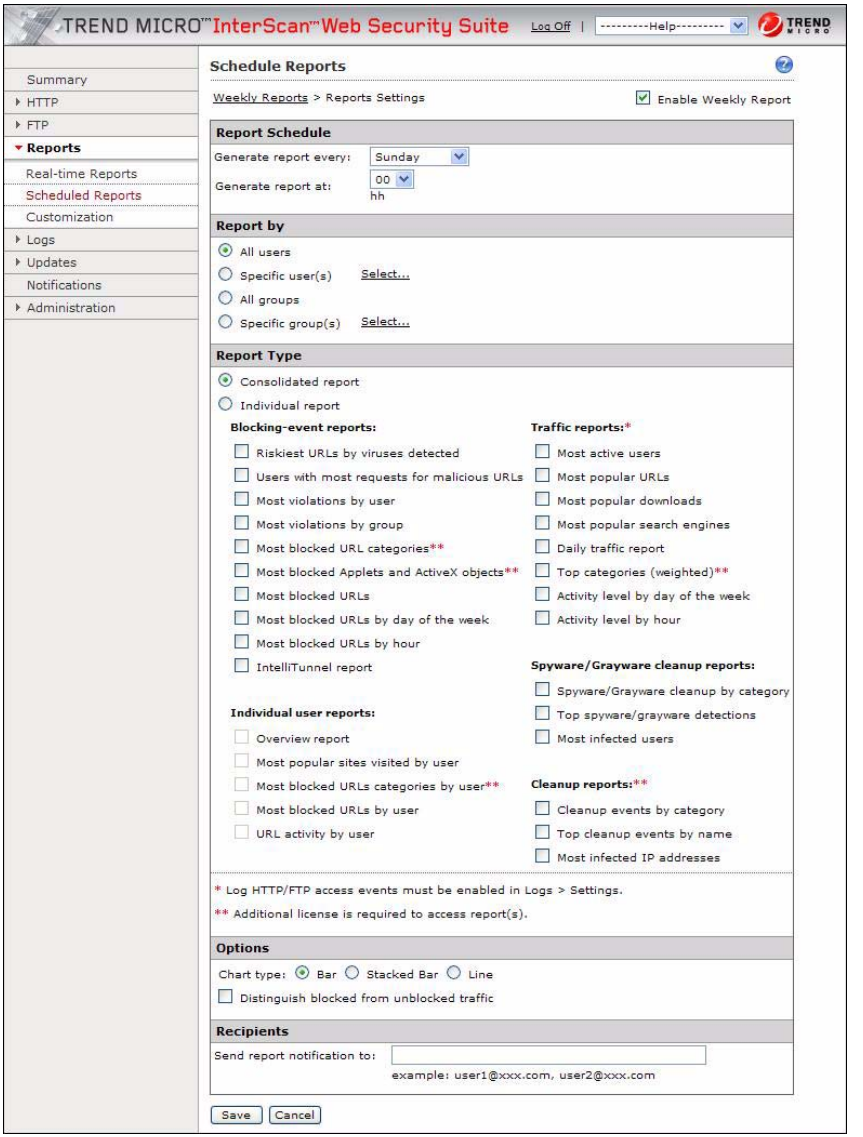


FIGURE 9-4 Scheduled Report Settings page (weekly report shown)

5. Set the time and/date to generate the scheduled report.
6. Under **Report by**, select the scope of the report:
   - **All users**
   - **Specific user(s)**
   - **All groups**
   - **Specific group(s)**\

Note: For more information about configuring specific users or groups, see *To select specific group(s):* starting on page 173 and *To select specific user(s):* starting on page 174.

---

7. Under **Report Type**, select the type of report to be generated:
   - **Consolidated report**.
   - **Individual report**. If you opt for the individual reports, select the type(s) of reports to include.
8. Under **Options**, select the chart type from the menu—either **Bar**, **Stacked bar** or **Line**. To denote blocked traffic from unblocked traffic using different shading, select **Distinguish blocked from unblocked traffic**.
9. Under **Recipients**, in the **Send report notification to** field, type the email address(es) where IWSS should send a notification when a newly generated report is ready for viewing. Separate multiple email addresses with a comma.
10. Click **Save**.

To delete scheduled reports:

1. Click **Reports > Scheduled Reports** in the main menu.
2. Click the tab that corresponds to the reports to delete—either **Daily**, **Weekly**, or **Monthly**.

3. Select the reports to remove and click **Delete**.

FIGURE 9-5 Delete old scheduled reports from the server

Customizing Reports

IWSS allows you to customize the number of records shown in different reports. For example, you can configure the number of users to be listed on the "Most active users" Web traffic report. The default number of records for all reports is ten.

You can configure IWSS to archive scheduled reports. The default path for archiving reports is `/etc/iscan/report` but can be modified. The default configuration is to archive 60 daily reports, 20 weekly reports and 4 monthly reports before deleting them from the server, but you can configure the number of scheduled reports to save.

To customize the report data maintenance settings:

1. Click **Reports > Customization** in the main menu.
2. Under **Customize the Number of Records**, type the number of records to include in each of the reports.

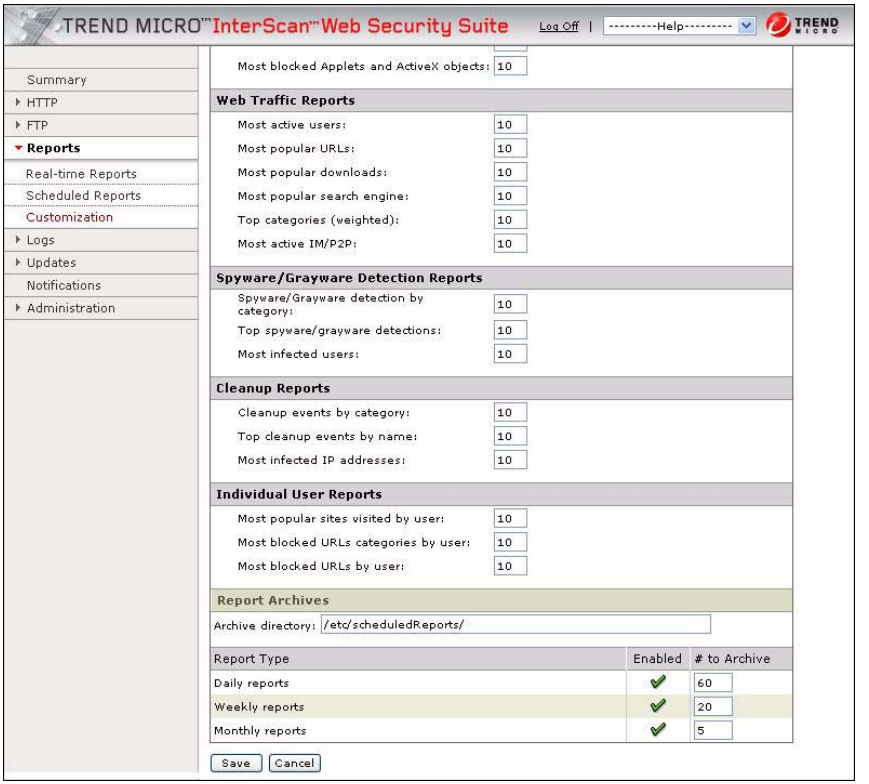


FIGURE 9-6 Customizing the reports

3. Under **Report Archives**, type the following information in the fields provided:
   a. **Archive Directory** to save the reports (the default is `/etc/iscan/report`)
   b. Number of scheduled reports to save:
      - **Daily reports** (default is 60)
      - **Weekly reports** (default is 20)
      - **Monthly reports** (default is 4)
4. Click **Save**.

Note: When changing the **Archive Directory**, the folder must exist on the IWSS server before it is entered into the **Report Customization** page. In order to view reports already generated, copy them over to the new folder.

Introduction to Logs

There are two types of logs available with IWSS: Reporting Logs and System Logs. There are several examples of each type of log: System logs include the HTTP scan, FTP scan, Mail delivery daemon, Administration, and Update logs and Reporting logs include the Virus, URL blocking, Performance, and URL access logs.

System logs contain unstructured messages about state changes or errors in the software, and are only visible by viewing the log file—they cannot be seen from the Web console. Reporting logs provide program event information, and the IWSS management console can be used to query and view them. The database stores all log data. It may optionally also be stored in text log files for compatibility with previous IWSS versions and to permit additional data analysis using customer scripts, and provides redundancy to verify the database is properly updated. Trend Micro recommends using the database as the only storage location for log data.

Querying and Viewing Logs

The IWSS management console provides tools to query log files.

Virus Log

The virus log contains information about viruses that IWSS has detected.

To view the virus log:

1. Click **Logs > Virus Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to view the virus log in a given time range, then select the start and end dates.

3. Under **Viruses**, select the virus(es) for which you want to view log entries. Click **Add** (or **Add All** for all viruses listed). To remove virus(es) from the right list box, click **Remove** (or **Remove All** for all viruses listed).

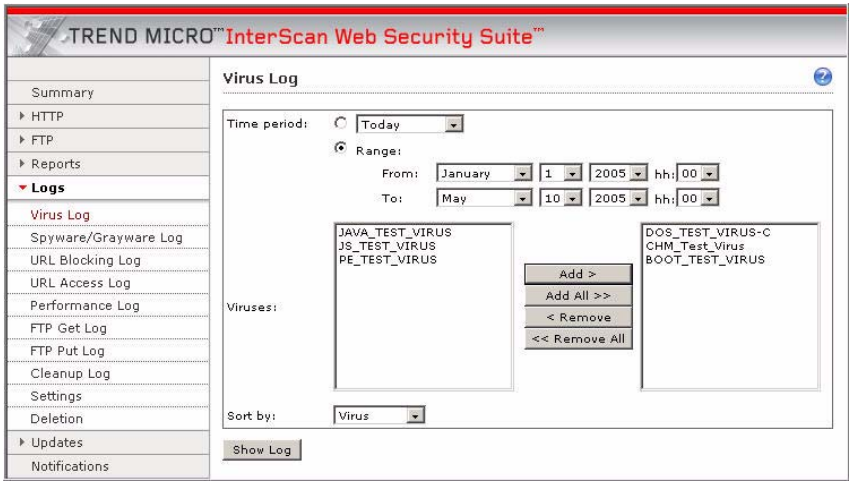


FIGURE 9-7 Filtering virus log queries by the virus name

4. Under the **Sort by** section, select a sort option to sort the display log (Virus, Date, Action, Scan Type, File Name, User ID).
5. Click **Show Log**. The **Virus Log** screen displays.
6. Click **Refresh** to update the screen.

Spyware/Grayware Log

The spyware/grayware log contains information about spyware/grayware detected by IWSS, including the name of the spyware/grayware, date, action, category, scan type, file name affected and user ID of the client involved.

To view the spyware/grayware log:

1. Click **Logs > Spyware/Grayware Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.

3. Under **Grayware**, select the spyware/grayware for which you want to view log entries. Click **Add** (or **Add All** for all grayware listed). To remove grayware from the right list box, click **Remove** (or **Remove All** for all viruses listed).
4. Under the **Sort by** section, select a sort option (Grayware, Date, Action, Category, Scan Type, File Name, User ID).
5. Click **Show Log**. The **Spyware/Grayware Log** viewing screen displays.
6. Click **Refresh** to update the display.

URL Blocking Log

The URL blocking log contains information about URLs that have been blocked, including the date and time blocking occurred, category, blocking rule applied, user ID, Outbreak Prevention Policy (OPP) ID if applicable, and scan type.

To view the URL blocking log:

1. Click **Logs > URL Blocking Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **URLs blocked**, you can add the URL(s) listed in the left list box to the right list box. Highlight the URL(s) to add, and then click **Add** (or **Add All** for all URLs listed). To remove the list of URLs from the right list box, click **Remove** (or **Remove All** for all URLs listed).
4. Under **Sort by**, select the appropriate option to sort the display log.
   - **URL**—the blocked URL
   - **Date**—the date and time when the URL was blocked
   - **Category**—the rule defined by the user in the URL filtering, Access Quota, file blocking, and URL blocking policy
   - **Rule**—how the URL was blocked:
     - IWSS-defined rule (block the URL containing a virus): displays the URL that has been blocked
     - URL blocking rule: displays the URL in the block list
     - URL filtering rule: displays the policy name
     - OPP defined rule: displays the OPP rule
     - File type defined rule: displays blocked file type

  - PhishTrap defined rule: displays a PhishTrap violation rule
  - Access Quota defined rule: displays access quota violation rule
- **User ID**—the IP address, host name, or LDAP user/group name associated with the client that requested the URL
- **OPP ID**—the ID number of the Outbreak Prevention Policy (OPP)
- **Scan Type**—either access quota, file type, URL memory block list, content filter, or PhishTrap

5. Click **Show Log**. The **URL Blocking Log** viewing screen displays.
6. Click **Refresh** to update the screen.

Note: You can also find an entry in the **URL Blocking Log** when an FTP proxy blocks a file by type.

URL Access Log

The URL access log contains URL access information. IWSS writes to the URL access log only when **Log HTTP/FTP access events** is enabled (**Log HTTP/FTP access events** is disabled by default) under **Logs > Settings > Reporting Logs**. Each access monitoring record contains the following information:

- Date and time the access occurred
- User who visited the site
- IWSS server that processed the access
- IP address of the client system that requested the access

Note: Network address translation may render this data meaningless, or at least make it appear that all access occurs from a single client. Also, when the access log is enabled, the IWSS service is restarted. During the restart, a router may take up to 30 seconds to recognize IWSS again, during which the router will not redirect packets.

- Domain accessed
- Path portion of the URL (the HTTP service can get the full URL path)
- IP address of the server from which the data was retrieved

To view the URL access log:

1. Open the IWSS management console and click **Logs > URL Access Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort option.
4. Click **Show Log**. The **URL Access Log** viewing screen displays.
5. Click **Refresh** to update the URL access log.

Performance Log

The performance log contains information about server performance. Each performance metric record contains:

- Date and time the metric was recorded
- IWSS server that recorded the metric
- Metric name (one of: `HTTP Requests Processed`, `HTTP Responses Processed`, `Number of HTTP threads`, `HTTP CPU Utilization`)
- Metric value

To view the performance log:

1. Open the IWSS management console and click **Logs > Performance Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort order.
4. Click **Show Log**. The **Performance Log** viewing screen displays.
5. Click **Refresh** to update the screen.

FTP Get Log

The FTP Get log contains all FTP Get transaction information, including user ID, date, FTP transfer source, and file name.

To view the FTP Get log:

1. Click **Logs > FTP Get Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort order.
4. Click **Show Log**. The **FTP Get Log** screen displays.
5. Click **Refresh** to update the screen.

FTP Put Log

The FTP Put log contains all FTP Put transaction information, which includes user ID, date, sender identification, and file name.

To view the FTP Put log:

1. Click **Logs > FTP Put Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort option.
4. Click **Show Log**. The **FTP Put Log** viewing screen displays.
5. Click **Refresh** to update the screen.

Cleanup Log

The cleanup log contains information about cleanups taken by DCS after IWSS has detected a risk.

To view the virus log:

1. Click **Logs > Cleanup Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Malware cleaned**, select the malware name(s). Highlight the names to add, and then click **Add** (or **Add All** for all viruses listed). To remove malware name(s) from the right list box, click **Remove** (or **Remove All** for all viruses listed).

4. Under some circumstances, DCS is unable to connect to a client machine when IWSS sends the cleanup request. Since no malware is cleaned during these attempts, querying the cleanup log by malware name will not display any information. To view logs about cleanup attempts when DCS could not successfully connect to the client machine, select **Show connection failure attempts**.
5. Under the **Sort by** section, select a sort option (Malware, Date, IP address, Action, malware Type and Subtype).
6. Click **Show Log**. The **Cleanup Log** viewing screen displays.
7. Click **Refresh** to update the screen.

Deleting Logs

If you no longer need to refer to text log files, you can delete them from the directory.

Note: The following procedure deletes text log files; logs in the database cannot be deleted manually. Configure a scheduled deletion for database logs on the **Logs > Settings** screen.

To delete one or more logs:

1. Click **Logs > Deletion** in the main menu.
2. On each of the four tabs (**Virus Log**, **URL Blocking Log**, **URL Access Log** and **Performance Log**), select the log to delete.

3. Click **Delete**, and then confirm by clicking **OK** on the next screen.

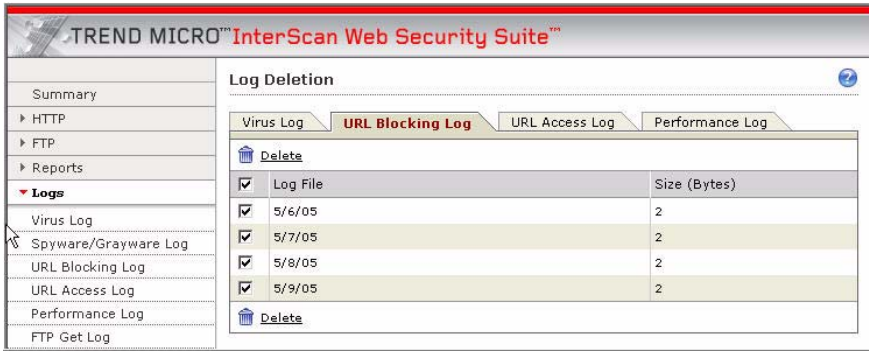


FIGURE 9-8 Delete older URL blocking logs from the server

Log Settings

From the **Log Settings** screen, you can configure:

- Directories for reporting and system logs (for the text log files only)
- Number of days to keep the system logs
- Whether to gather performance data or log HTTP/FTP access events, and the logging interval for each
- Database log update interval, and the number of days to keep logs in the database
- Whether to write logs to database and log files, to the database only, or to the log file only

---

Note: Text log files cannot be automatically deleted—they can be manually deleted on the **Logs > Deletion** screen. Database logs cannot be manually deleted—a deletion schedule can be configured on the **Logs > Settings** screen.

Log File Folder Locations

You can configure the folders for the reporting logs and the system logs. The default location is `/etc/iscan/log`. A folder must exist on the IWSS server and you must have the correct permission before the folder can be configured as the log file

location. IWSS checks after a folder path is entered, and an error message will display if the folder entered is not accessible.

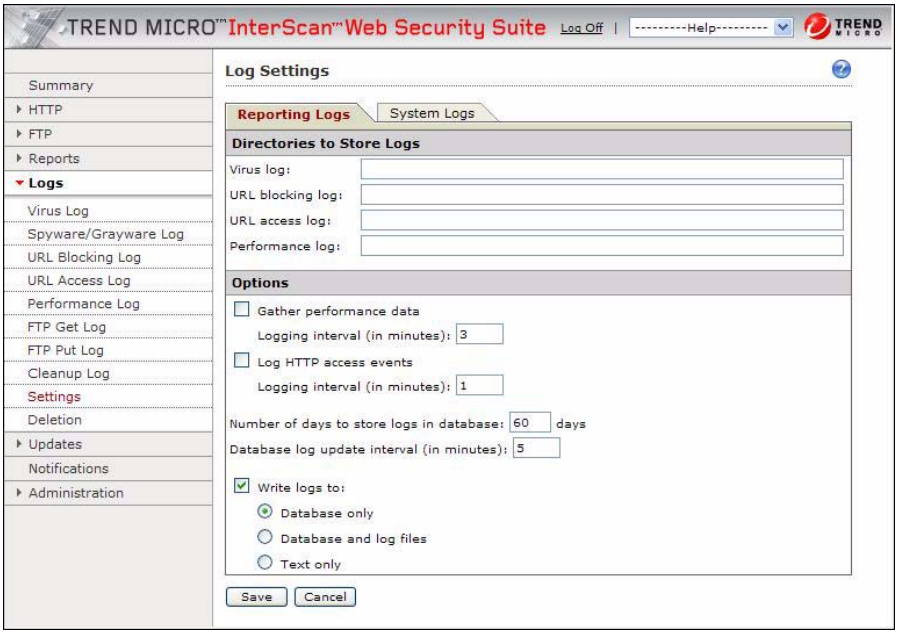


FIGURE 9-9 Configure reporting log settings

To configure reporting log directories:

1. Click **Logs > Settings > Reporting Logs** from the main menu.
2. In the corresponding text boxes, type the folder locations for the log files.
3. Click **Save**.

To configure the system log directories:

1. Click **Logs > Settings > System Logs**.
2. In the corresponding text boxes, type the folder locations for the log files.
3. Click **Save**.

Other Log Options

There are some additional settings that control how IWSS logs events. These can be configured on the **Log Settings** screen.

System Logs

On the **System Logs** tab, configure the number of days to retain system logs before automatically deleting them (default = 5 days).

Reporting Logs

On the **Reporting Logs** tab, you can configure IWSS to gather performance data and log HTTP/FTP access events. If you enable these, configure the logging interval.

The default time period that logs will be kept in the database is 30 days; customize this to reflect your specific environment's needs. In addition, set the time interval that the database will be updated with new logs (default = 30 seconds).

Log File Naming Conventions

By default, log files are written to the `/etc/iscan/log` directory. IWSS has a standard convention for naming log files. For instance, the convention for virus logs is:

```
virus.log.2007.01.09
```

which can be read as virus log for January 9, 2007

The naming conventions for each type of log are described in the table below:

TABLE 9-2. Log files naming conventions

Virus Log	`virus.log.yyyy.mm.dd`
URL Blocking	url_blocking.log.yyyy.mm.dd
Performance Log	perf.log.yyyy.mm.dd
URL Access Log	access.log.yyyy.mm.dd

TABLE 9-2. Log files naming conventions

FTP Log	ftp.log.yyyymmdd.0001
HTTP Log	http.log.yyyymmdd.0001
Mail Delivery Log	mail.log.yyyymmdd.0001
Update Log	update.log.yyyymmdd.0001
Scheduled Update Log	admin.log.yyyymmdd.0001
Temporary Control Manager Log	CM.yyyymmdd.0001
Java Applet Scanning Log	jscan.log.yyyymmdd.0001
Database Log	log_to_db.log.yyyymmdd.0001
World Virus Tracking Center Log	logtowvts.log.yyyymmdd.0001

Note: Deleting a log will not necessarily remove the corresponding data from displaying in the IWSS management console. To prevent InterScan Web Security Suite from displaying data, you must remove the corresponding data from the appropriate database table.

TABLE 9-3. Major database tables for IWSS logging/reporting

Table Name	Example Columns
tb_url_usage	username, url, path
tb_report_by	period, category, entity_type, entity_name

TABLE 9-3. Major database tables for IWSS logging/reporting

Table Name	Example Columns
tb_violation	username, url, file_name, action, blocked_by, category
tb_performance_value	server, date_field, metric_value, metric_id

Exporting Log and Report Data as CSV Files

When viewing your log query or a real-time report, IWSS supports exporting log data to a CSV file in order to view and analyze the data in other applications. Click **Export to CSV** and then download the file from the IWSS server.

Note: The character format that IWSS uses to save CSV files is configurable using the csvcharformat parameter under the [Common] section of the intscan.ini file. The default is UTF-8 format. Some versions of Microsoft Excel cannot display double-byte characters in UTF-8 text files. If your logs contain double-byte characters, Trend Micro recommends opening and saving the files as Unicode using Notepad before attempting to open the CSV file using Excel.

Introduction to Real-time Statistics

IWSS includes dynamic displays where you can view the “real-time” statistics of the IWSS server.

Virus and Spyware Trend Display

This is a static display that shows the rate at which viruses and spyware are coming up against your system. (You can specify threshold alerts so that you are notified of a critical level of virus and/or spyware "hits.") The rate is based on a seven-day period and "hits" are recorded daily. Therefore, a new display is started every seven days. The display does not include the names of users involved.

Note: Since each day's virus and spyware data is represented by a single point on the display, IWSS cannot start graphing data until there are two points, or two days worth of data available.

The information in the Virus and Spyware display is for the entire IWSS installation (single server and up to a server farm).

Hard Drive Display

This is a static display that shows the status of the disk(s) used by IWSS for its system files, quarantine space, temporary space, and logs. The Hard Drive display can monitor up to 12 disks.

If the database resides on the same drive as any of these directories, then the database disk usage is also included in the display. The scale along the Y-axis ranges from 10 to 100 percent.

You can specify threshold alert values and the frequency of alerts so that you are notified when any of the hard disk statuses reach a critical level. IWSS can send these alert either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 9-195 and *SNMP Trap Notifications* on page 9-208.

Bandwidth Usage Display

This is a dynamic display that shows the bandwidth usage of both inbound and outbound traffic for HTTP and FTP. IWSS sees traffic in terms of requests and responses. Therefore, the display interprets all requests as outbound traffic and all responses as inbound traffic. From this display, you can view any potential bandwidth problems.

The display shows ten data points, which gives the graph a history of five to ten minutes of activity. This activity is only monitored for the local IWSS server. With the ideal refresh rate being between 30 and 60 seconds, the display has a default refresh rate of 30 seconds.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of usage, respectively. IWSS retrieves this information from the

database. If the database does not contain enough data, then the display shows the data that is available.

Note: Since each day's bandwidth usage data is represented by a single point on the display, IWSS cannot start graphing data until there are two points, or two days worth of data available.

You can specify threshold alert values and the frequency of alerts so that you are notified when a bandwidth usage reaches a critical level. IWSS can send alerts either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 9-195 and *SNMP Trap Notifications* on page 9-208.

Note: The bandwidth setting should be very high—above "out of normal range" values to avoid frequent alerts.

CPU Usage Display

This is a dynamic display that shows CPU utilization on the local system. In the case of multiple CPUs, the display shows the average IWSS usage across all CPUs. It does this by displaying a single line for all CPU utilization. IWSS determines the CPU utilization based on CPU cycles used, CPU cycles used by IWSS, and total CPU cycles used by the backend, CPU-monitoring API.

By default, IWSS samples the CPU usage each second for two minutes, giving you 120 data points. In the init file, you can change the default refresh rate.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of CPU usage, respectively. IWSS retrieves this information from the database. If the database does not contain enough data, then the display shows the data that is available.

Note: Since each day's CPU usage data is represented by a single point on the display, IWSS cannot start graphing data until there are two points, or two days worth of data available.

You can specify the threshold alert value and the frequency of the alert so that you are notified when a CPU usage reaches a critical level. IWSS can send alerts either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 9-195 and *SNMP Trap Notifications* on page 9-208.

Physical Memory Usage Display

This is a dynamic display that shows the amount of physical memory used by the local IWSS computer.

By default, IWSS samples the physical memory usage each second for two minutes, giving you 120 data points. In the init file, you can change the default refresh rate.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of physical memory usage, respectively. IWSS retrieves this information from the database. If the database does not contain all the data, then the display shows the data that is available.

Note: Since each day's physical memory data is represented by a single point on the display, IWSS cannot start graphing data until there are two points, or two days worth of data available.

You can specify the threshold alert value and the frequency of the alert so that you are notified when physical memory usage reaches a critical level. IWSS can send alerts either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 9-195 and *SNMP Trap Notifications* on page 9-208.

Introduction to Notifications

Notifications can be issued in response to scanning, blocking, alerting, and program update events. There are two types of notifications—administrator notifications and user notifications:

- Administrator notifications provide information about HTTP scanning, HTTP file blocking, FTP scanning, threshold alerts, restricted tunnel traffic, and Applets/ActiveX security events, as well as pattern file and scan engine updates. IWSS sends administrator notifications via email to addresses that you configure in the **Email Settings** screen.

- User notifications provide information about HTTP scanning, HTTP file blocking, FTP scanning, and Applets/ActiveX scanning events. IWSS presents user notifications in the client's browser or FTP client, in lieu of the prohibited Web page or file that the client is trying to view or download.

The messages presented in both the administrator and user notifications are configurable and can include "tokens", or variables, to customize notification messages with information about the event. In addition, user notification messages support HTML tags to customize the appearance of the message and provide links to other resources, such as security policy documents hosted on your intranet.

Email Notification Settings

IWSS sends administrator notifications to email addresses that you specify. The administrator enters email settings when installing IWSS and running the setup program, but email settings can also be modified post-installation in the management console's **Email Settings** screen.

To configure email settings for administrator notifications:

1. Click **Notifications** in the main menu.
2. In the **Notifications** screen, click **Send notification to**.
3. Type the email address to send notifications, the sender's email address, the SMTP server, the SMTP server port and the time interval between checking the mail queue.

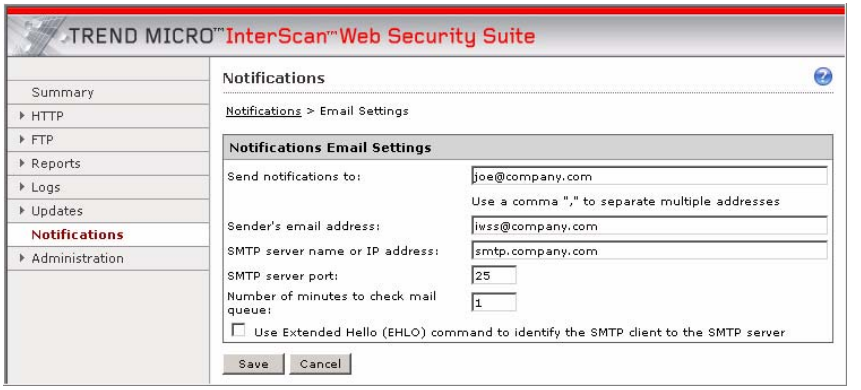


FIGURE 9-10 Configuring administrator notification settings

4. If your mail server requires ESMTP, enable **Use Extended Hello (EHLO)** for IWSS to initial SMTP sessions using the EHLO command.
5. Click **Save**.

Notification Tokens/Parameters

To make notifications more meaningful, InterScan Web Security Suite can use tokens (or variables) as informational placeholders in a notification. When an event occurs, InterScan Web Security Suite dynamically substitutes the specific information in place of the variable, providing detailed information about that specific event.

For example, you could create a generic notification as follows:

```
A virus was detected in HTTP traffic.
```

This notification lets you know there is a problem, but does not provide any details.

Instead, you could configure the notification using variables as follows:

```
On %d, InterScan Web Security Suite detected a security risk %v in
the file %F. %t attempted to download the file from %f.
```

The notification might read as follows:

```
On 1/23/2007 8:36AM, InterScan Web Security Suite detected a
security risk TROJ_VIPERIK.A in the file game.exe. 123.123.123.12
attempted to download the file from http://www.example.com.
```

With this information, administrators can contact the client and provide more security information. The notification in this example uses five variables: %d, %v, %F, %t and %f.

The following table contains a list of variables that can be used in notification messages and pages.

Variable	Variable Meaning	How the Variable is Used
%Y	date and time	The date and time of the triggering event

Variable	Variable Meaning	How the Variable is Used
%F	file name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm
%V	malware name (virus, Trojan, etc.)	The name of the risk detected
%	the character '%' itself	To insert the percentage character into a notification message or page
%f	from	The server where the infected or blocked file, or filtered URL, originated. This variable is not available for use in notifications (email or SNMP).
%A	action taken	The action taken by IWSS
%m	method	The processing method that triggered the event. This variable is not available for use in notifications (email or SNMP).
%M	moved to location	The quarantine folder location where a file was moved
%h	host name	The IWSS host name where the event was triggered

TABLE 9-4. Description of variables

Configuring Notifications

To configure a notification, select the types of events that will issue the notification and edit the email and browser notification messages.

Using HTML Tags in User Notifications

You can use HTML to format user notification messages. While the HTML files can include reference links to external images or styles, InterScan Web Security Suite only supports uploading HTML files. Any additional files will have to be separately uploaded to a Web server, and Trend Micro recommends using absolute links to help avoid broken links.

HTTP Scanning

When IWSS detects malicious code in a file requested by a client, it will issue an administrator notification via email and a user notification in the requesting client's browser.

To configure HTTP scanning notifications:

1. Click **Notifications** and then click **HTTP Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other Internet threats**).

3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the message as described in *Notification Tokens/Parameters* starting on page 196.

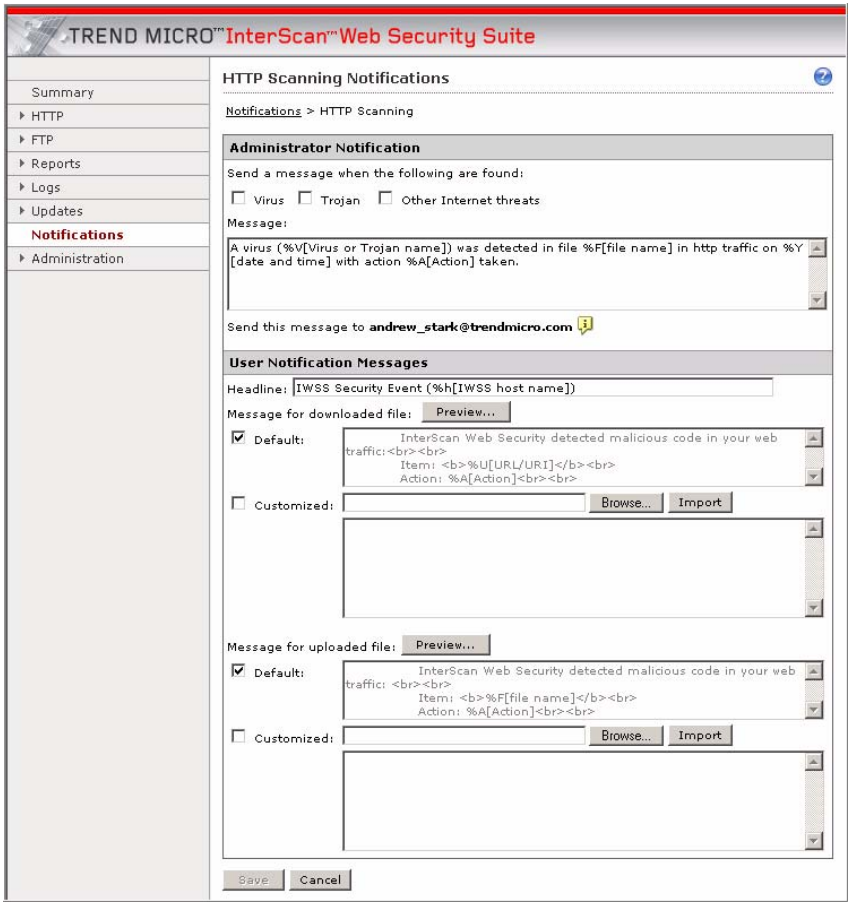


FIGURE 9-11 Configure HTTP scanning notifications

4. Type the **Headline** to display in the browser. The default is *IWSS Security Event (Server Name)*. The header line is common for virus infection messages, file type blocking, and URL blocking messages.

5. For **Message for downloaded file** and **Message for uploaded file**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import the customized message's content from an HTML file.
   c. Verify the notifications display correctly by clicking **Preview**.
6. Click **Save**.

HTTP Blocked File Type

When IWSS blocks a file, it sends an administrator notification via email, and a user notification message is displayed in the requesting client's browser.

To configure HTTP file blocking notifications:

1. Click **Notifications** and then click **HTTP Blocked File Type**.
2. Under **Administrator Notification**, select **Send a message when the blocked file type is accessed**.

3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the text as described in *Notification Tokens/Parameters* starting on page 196.

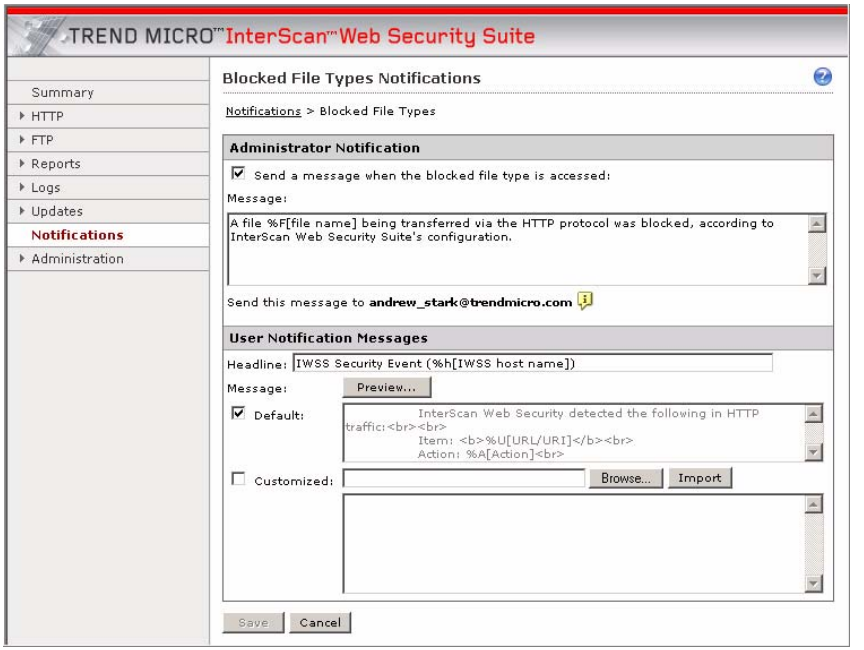


FIGURE 9-12 Configure HTTP blocked file notifications

4. For **Headline**, type the header line to display in the browser. The default headline is *IWSS Security Event (%h)*. The headline is common for virus infection messages, file type blocking, and URL blocking messages.
5. For the **Message**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import content from an HTML file.
6. Verify the notifications by clicking **Preview**.
7. Click **Save**.

URL Blocking

When IWSS detects an attempt to access a URL in the PhishTrap pattern file or a prohibited URL from the local IWSS list, IWSS displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for blocked URLs:

1. Click **Notifications** in the main menu, then click **URL Blocking**.
2. Under **User Notification Message for Restricted or Blocked URLs**:
   a. Click **Default** to display the default warning message.
   b. Click **Customized** to display your own warning message—type the message in the text box, or **Import** it from a HTML file on your local machine.
3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

FTP Scanning

When IWSS detects malicious code in a user's FTP transfer, it can automatically send a customized administrator notification to the designated email addresses and/or display a notification in the requesting FTP client program.

To configure the FTP scanning notification settings:

1. Click **Notifications**. in the main menu, then click **FTP Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other malicious code**).

3. If you do not want to use the default notification messages, highlight the default text and type your own. If applicable, insert variables in the text as described in *Notification Tokens/Parameters* starting on page 196.

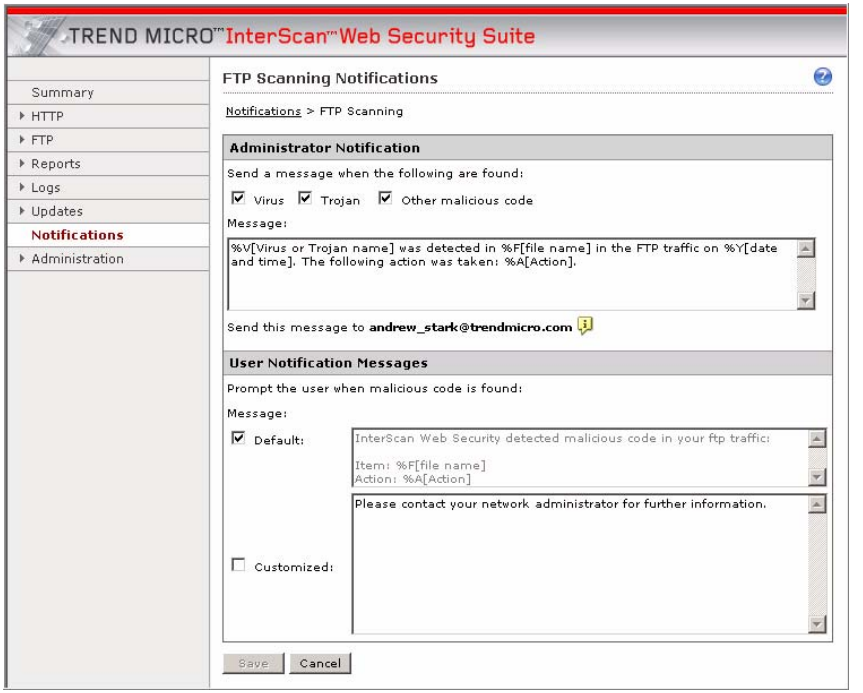


FIGURE 9-13 Configure FTP scanning notifications

4. For the user notification **Message**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and type the customized content.
5. Click **Save**.

IntelliTunnel Security

When IWSS detects restricted tunnel traffic across port 80, the application blocks this traffic and sends an email to the address specified IntelliTunnel Notification page. See Chapter 10, *IntelliTunnel Security*.

To configure the IntelliTunnel security notification settings:

1. Click **Notifications** in the main menu and then click **IntelliTunnel**.
2. Under **Administrator Notification**, select **Send a message when restricted tunnel traffic is detected**.

FIGURE 9-14 Configure IntelliTunnel security notifications

3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in *Notification Tokens/Parameters* starting on page 196
4. Click **Save**.

Applets and ActiveX Security

When IWSS detects an attempt to download a Java Applet or ActiveX object that violates a security policy, the application sends an administrator notification via email and a user notification message in the requesting client's browser.

To configure the Applets and ActiveX security notification settings:

1. Click **Notifications** in the main menu, then click **Applets and ActiveX Instrumentation**.

2. Under **Administrator Notification**, select **Send a message when a malicious Applet or ActiveX attempt is detected**.
3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in *Notification Tokens/Parameters* starting on page 196.

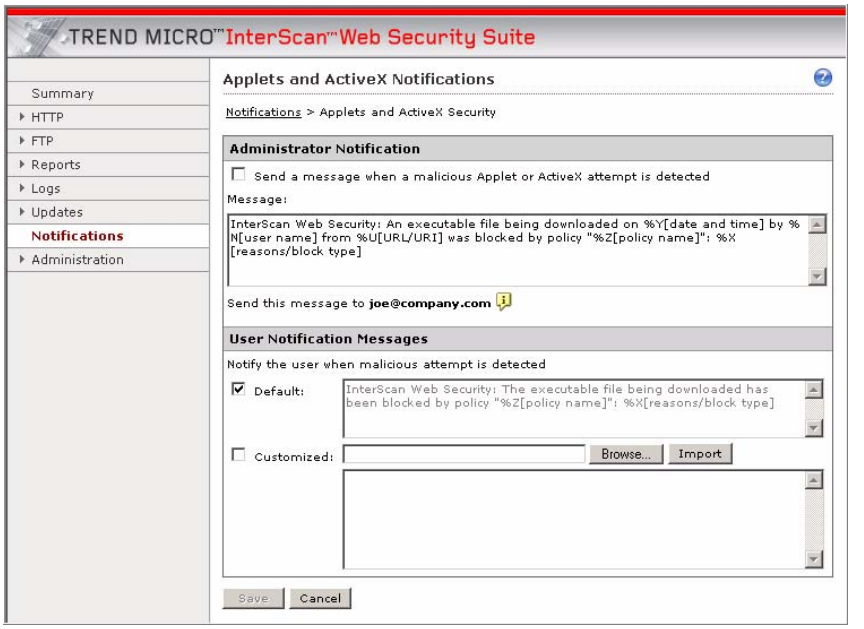


FIGURE 9-15 Configure Java applet and ActiveX security notifications

4. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or **Import** the customized message's content.
5. Click **Save**.

Pattern File Updates

IWSS can issue administrator notifications in response to attempts to update the virus, PhishTrap or spyware pattern files, or the URL filtering database.

To enable pattern and URL filtering database update notifications:

1. Click **Notifications** from the main menu, then click **Pattern File Updates**.

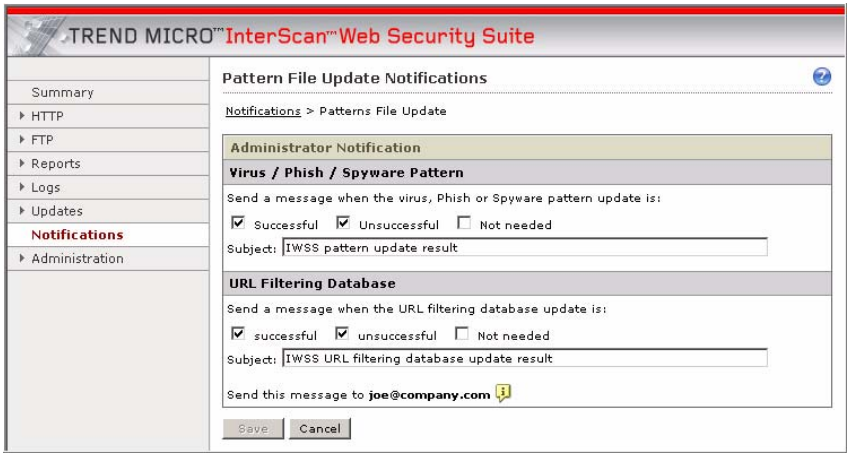


FIGURE 9-16 Pattern file and URL filtering database update notifications

2. For the pattern and URL filtering database update attempts:
   a. Select the update events that will trigger a notification. You can configure notifications for **Successful**, **Unsuccessful** or **Not needed** update attempts.
   b. Type a **Subject** for the notification message
3. Click **Save**.

Scan Engine Updates

Though less frequent than pattern file updates, Trend Micro periodically releases new versions of the scan engine to reflect advances in virus and malicious code detection methods. IWSS can issue administrator notifications in response to scan engine updates.

To enable scan engine update notifications:

1. Click **Notifications** from the main menu, and then click **Scan Engine Updates**.

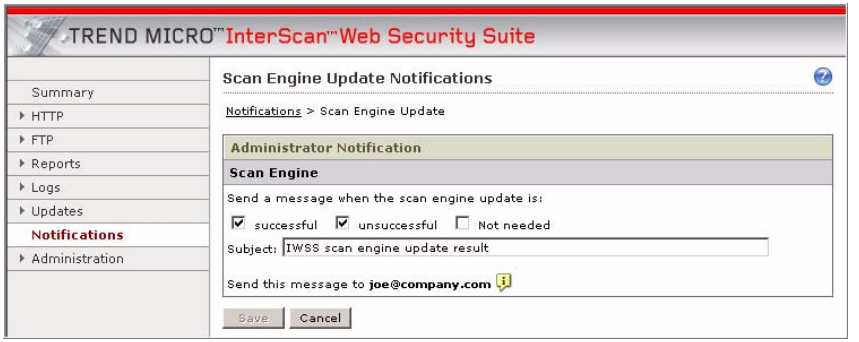


FIGURE 9-17 Scan engine notification configuration

2. Select the scan engine update events that will trigger a notification. You can configure notifications for **Successful**, **Unsuccessful** or **Not needed** update attempts.
3. Type the **Subject** of the notification email message.
4. Click **Save**.

Threshold Alerts

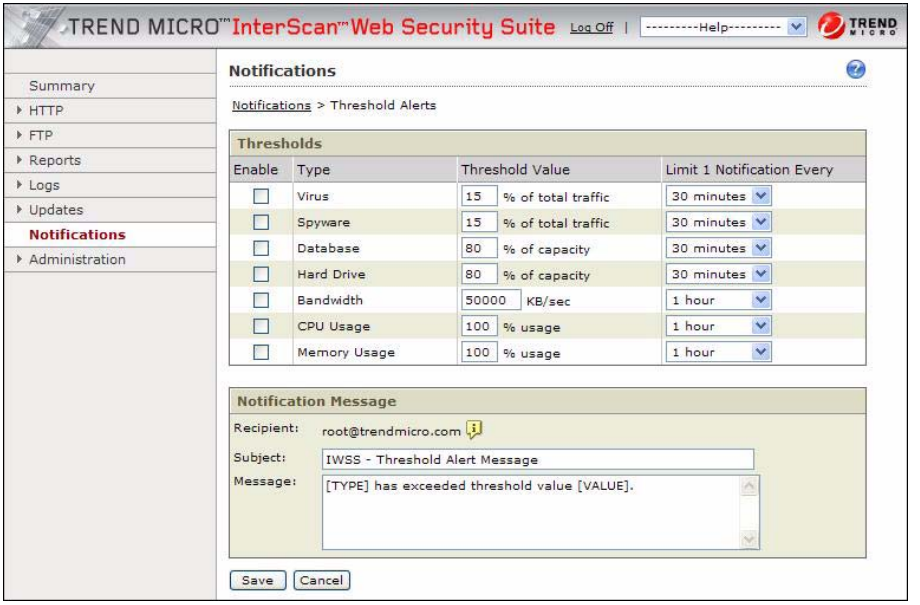
You can specify threshold alert values and the frequency of alerts so that you are notified when any the following reach a critical level:

- Virus
- Spyware
- Database
- Hard drive
- Bandwidth

IWSS can send these alert either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 9-195 and *SNMP Trap Notifications* on page 9-208.

To enable threshold alert notifications:

1. Click **Notifications** in the main menu and then click **Threshold Alerts**.
2. Under **Thresholds**, specify the desired thresholds and either accept the defaults or specify new values in the **Threshold Value** and **Limit 1 Notification Every** columns.



3. If you do not want to use the default notification messages under **Notification Message**, highlight the default text and type your own version. If applicable, insert variables in the text as described in *Notification Tokens/Parameters* starting on page 196
4. Click **Save**.

SNMP Trap Notifications

IWSS supports sending SNMP traps in response to security, update, or program events.

Note: In order to send SNMP traps, you first need to configure the SNMP settings and then enable this feature. To do this, choose **Administration > IWSS Configuration > SNMP Settings**.

To enable sending SNMP traps:

1. Click **Notifications** on the main menu and then click **SNMP Notification Settings**.

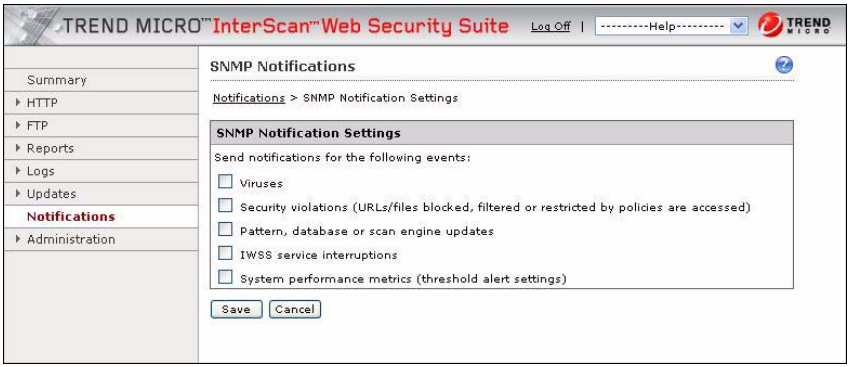


FIGURE 9-18 Configure SNMP notifications

2. Select the types of events that will trigger an SNMP trap. The different classes of events are:
   - **Virus or Internet threats**—events related to virus or malicious code detections
   - **Security violations**—activities that are prohibited by IWSS policies, not related to viruses or malicious code
   - **Pattern, database or scan engine updates**—events related to IWSS updates
   - **IWSS service interruptions**—issues with any of the essential IWSS services
3. Click **Save**.

Chapter 10

IntelliTunnel Security

IWSS uses IntelliTunnel technology to block undesirable instant messaging (IM) and authentication connection protocols tunneled through port 80. It uses a dynamically, updatable pattern file to distinguish normal browser traffic from other protocols communicating over port 80. Currently, the pattern file can identify three popular types of IM traffic when this traffic is tunneled through port 80.

Note: Since IntelliTunnel can block undesirable traffic through port 80 only, other ports go unfiltered.

This chapter describes the protocols used for IM and authentication connections. It also describes how to edit and create an IntelliTunnel policy.

Protocols Used in Instant Messenging and Authentication Connections

IWSS can filter HTTP traffic for IM protocols and authentication connections protocols and based on a specified policy, block certain content from entering the LAN. You can create multiple policies to have IWSS apply different filter criteria to different user groups within your organization.

Note: IM/authentication connections policy enforcement is only possible when the IM/authentication connections clients are made to use HTTP tunneling. This requires that the site is set up to allow only external network access via HTTP. This means, internal clients are prevented from connecting directly to external servers of any form, on any port. This is part of the firewall configuration, not IWSS.

About Instant Messenger Protocol

IWSS can block most services using popular instant messenger protocols, such as AOL, MSN, and YM.

About Authentication Connection Protocols

IWSS can block authentication connection communications that use the following technology:

- **Google Talk** - A full-fledged IM client based on the open Jabber protocol which also includes Voice over Internet Protocol (VoIP). VoIP is a category of hardware and software that enables you to use the Internet as the transmission medium for telephone calls. This technology sends voice data in packets using IP rather than by traditional circuit transmissions of the Public Switched Telephone Network (PSTN).
- **Jabber IM** (jabber.org) - An open XML protocol for message and presence exchange in real time between two points on the Internet. Jabber's asynchronous instant messaging platform is similar to IM systems such as AIM, ICQ and MSN but is open source, extensible through XML, decentralized (allowing anyone to

run a Jabber server), and any Jabber server can be isolated from the public Jabber network in order to increase security.

Note: IntelliTunnel does not block Google Talk or Jabber IM in ICAP mode.

Editing an IntelliTunnel Policy

When editing a policy, you can edit the account information or policy information, or both.

To edit IntelliTunnel policy information:

1. Select **HTTP > IntelliTunnel** from the main menu.
2. Click the desired policy name.
3. From the **IntelliTunnel : Edit Policy** page (Rule tab), select or de-select the desired option(s).
4. Click **Save**.

To edit IntelliTunnel account information:

5. Click the **Account** tab.

   You can also access the **Account** tab by clicking on the desired account name in the IntelliTunnel Policies page.
6. Specify a policy name.
7. Specify an IP range and/or an IP address and then click **Add**.

   IWSS applies the IM and authentication connections rules to any IP range and IP address that you specify. If you are using LDAP, then you may see more descriptive information in the Add table, such as the user name.
8. Click **Save**.

Creating a New IntelliTunnel Policy

Creating a new IntelliTunnel policy is basically a two-step process: specify an account and specify IM/authentication connections security rules.

To create a new IntelliTunnel policy:

1. Select **HTTP > IntelliTunnel** from the main menu.
2. In the IntelliTunnel Policies page, click the **Add** link.
3. From the "1. Select Accounts" view of the IntelliTunnel: Add Policy page, specify a policy name.
4. Specify an IP range and/or an IP address and then click **Add**.

   IWSS applies the IM and authentication connections rules to any IP range and IP address that you specify. If you are using LDAP, then you may see more descriptive information in the Add table, such as the user name.
5. Click **Next**.
6. From the "2. Specify IntelliTunnel Security Rules" view of the IntelliTunnel: **Add Policy** page, select the desired option(s).

   See the IWSS 3.0 online help for a complete description of the IM and authentication connections protocols.
7. Click **Finish**.

Appendix A

Mapping File Types to MIME Content-types

The following table describes file types that you can enter in the HTTP and FTP virus scanning policy **Other file types** fields to block corresponding MIME content-types. For example, if you type `afc`, both the `audio/aiff` and `audio/x-aiff` MIME content-types will be blocked.

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
afc	audio/aiff	avs	video/ avs-video	bin	application/ x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/ binhex
ani	application/ octet-stream	base64	application/ base64	binhex	application/ binhex4
arc	application/ octet-stream	bin	application/ mac-binary	binhex	application/ mac-binhex

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
arj	application/ octet-stream	bin	application/ macbinary	binhex	application/ mac-binhex40
asf	video/ x-ms-asf	bin	application/ octet-stream	binhex	application/ x-binhex40
bin	application/ x-macbinary	bmp	image/bmp	bmp	image/ x-windows-bmp
bw	image/ x-sgi-bw	bzip2	application/ x-bzi2	cgm	image/cgm
cmx	application/ x-cmx	cmx	image/ x-cmx	com	application/ octet-stream
core	application/ octet-stream	cpio	application/ x-cpio	dcr	application/ x-director
doc	application/ wordper-fect	dwg	application/ acad	dwg	application/ x-acad
dwg	drawing/ x-dwg	dwg	image/ vnd.dwg	dwg	image/ x-dwg
eps	application/ postscript	eps	image/ x-eps	exec	application/ octet-strea m
exec	application/ x-msdown-load	exe	application/ octet-stream	fh9	image/ x-freehand

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
fli	video/x-fli	fm	application/vnd.frame-maker	gif	image/gif
gzip	applica-tion/x-gzip	gzip	encoding/x-gzip	hpexe	application/octet-stream
iff	audio/x-aiff	java	text/x-java-source	java	application/java-class
java	applica-tion/x-java-applet	java	applica-tion/x-java-vm	java	text/x-java-source
java	application/java-class	java	applica-tion/x-java-applet	java	applica-tion/x-java-vm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-lha
lisp	application/x-lisp	maud	audio/x-maud	midi	audio/midi
mif	application/x-mif	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpeg-3	mp3	video/mpeg
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/x-cainet-win32-x86
msdoc	application/msword	msexl	application/excel	msexl	application/x-msexcel

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
msexl	application/x-excel	msexl	application/vnd.ms-excel	msmdb	application/x-msaccess
msppt	application/mspowerpoint	msppt	application/powerpoint	msppt	application/vnd.ms-powerpoint
msproj	application/vnd.ms-project	msproj	application/x-msproject	msproj	application/x-project
mswri	application/mswrite	pcx	image/x-pcx	pdb	application/x-pilot-pdb
pdf	application/pdf	pdf	application/x-pdf	pfb	application/x-font
pict	image/pict	pict	image/x-pict	picture	image/
png	image/png	ppm	image/x-portable-pixmap	ps	application/postscript
psd	application/octet-stream	qtm	video/quicktime	ra	audio/vnd.rn-realaudio
ra	audio/x-pn-realaudio	ra	audio/x-realaudio	rar	application/rar
ras	image/x-cmu-raster	ras	image/cmu-raster	risc	application/octet-stream

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
rmf	application/ vnd.rn-real media, g_audiovid eo	rtf	application/ rtf	rtf	application/ x-rtf
rtf	text/ richtext	scm	application/ vnd.lotus-screencam	scm	application/ x-lotuss-creencam
scm	application/ x-screen-cam	scm	video/ x-scm	sf	audio/ x-sf
swf	application/ x-shock-wave-flash	tar	application/ x-tar	tga	image/ tga
tiff	image/ tiff	tnef	application/ ms-tnef	tnef	application/ vnd.mstnef
txt	text/plain	uuencode	text/ x-uuen-code	zip	application/ zip
voc	audio/voc	voc	audio/ x-voc	wav	audio/wav
wbc	application/ x-webshots	wmf	application/ x-msmeta-file	wmf	image/ x-wmf

Appendix B

Configuration Files

There are three types of configuration files (main, protocol module, scanning module). All the configuration files are in the `{IWSS root}` directory; the default location for `{IWSS root}` is `/etc/iscan/`. The main configuration file is in `intscan.ini`.

- Settings specific to virus scanning are in:

`{IWSS root}\HTTP\IWSSPIScanVsapi.dsc`

- Settings that are specific to the ICAP protocol are in:

`{IWSS root}\HTTP\IWSSPIProtocolIcap.pni`

- Settings that are specific to the stand-alone proxy are in:

`{IWSS root}\HTTP\IWSSPIProtocolHttpProxy.pni`

- Settings for URL filtering scanning module are in:

`{IWSS root}\HTTP\IWSSPIUrlFilter.dsc`

- Settings specific to reporting are in:

`{IWSS root}\report.ini`

- Settings for the URL Categorization database are in:

`{IWSS root}\HTTP\urlfcIFX.ini`

- Settings for default URL categories and their mapping information are in:

```
{IWSS root}\HTTP\urlfcMapping.ini
```

- Settings for the list of IP address and IP ranges of all machines allowed to access the IWSS server are in:

```
{IWSS root}\HTTP\ClientACL.ini
```

- Settings for rules that define what ports IWSS will forward HTTP requests to are in:

```
{IWSS root}\HTTP\HttpPortPermission.ini
```

- Settings for rules that define what ports IWSS will allow HTTPS tunneling to are in:

```
{IWSS root}\HTTP\HttpsConnectACL.ini
```

- Settings for list of IP address and IP ranges of trusted servers are in:

```
{IWSS root}\HTTP\ServerIPWhiteList.ini
```

The IWSS management console varies depending on which modules are installed. If you have been using a previous version of IWSS, there are also many new features available in IWSS that require new `.ini` file entries.

Protocol Handlers

Functions responsible for interpreting and processing messages in some recognized transmission protocols are encapsulated in a dynamic library referred to as a protocol handler. IWSS provides a choice of either an ICAP protocol handler, which enables IWSS to act as an ICAP server, or an HTTP proxy handler, wherein IWSS acts like a direct HTTP proxy server. The application binary is independent of the protocol handler, allowing the same application to support different protocols with a configuration change.

Provide the complete path of the active configuration file of the protocol in the `main/protocol_config_path` entry in the `intscan.ini` file application.

Protocol handlers require their own specific configuration files, which contain entries that pertain only to that protocol. These protocol configuration files are denoted with a ".pni" filename extension.

Scanning Modules

Traffic scanning functionality is provided through dynamic libraries known as scanning modules. The first scanning module available to IWSS provides content scanning using the scan engine.

Each scanning module has a configuration file with a `.dsc` extension. The IWSS application locates the available scanning modules by searching for `.dsc` files in the directory that is provided in the `scan/plugin_dir` entry in the `intscan.ini` file.

Appendix C

OpenLDAP Reference

Though OpenLDAP supports Kerberos authentication, the packages to enable Kerberos authentication support are not installed by default. This appendix covers how to install and configure Kerberos support for OpenLDAP. In addition, this appendix explains how to set up your OpenLDAP directory so IWSS can query it when using the user/group authentication method.

This chapter includes the following topics:

- Software packages tested to enable Kerberos authentication when using IWSS with OpenLDAP
- Modifying OpenLDAP configuration files
- Sample user and group entries in LDIF format

OpenLDAP Server Side Configuration

Software Package Dependencies

The following software packages are compatible with IWSS 3.0:

- cyrus-sasl-2.1.19
- db-4.2.52.NC
- heimdal-0.6.2
- openldap-2.2.17
- openssl-0.9.7d

Configuration Files

Using OpenLDAP with IWSS requires modifying the following configuration files:

```
/etc/openldap/ldap.conf
```

```
/etc/openldap/slapd.conf
```

Sample ldap.conf

```
#
# System-wide ldap configuration files. See ldap.conf(5) for
# details
# This file should be world readable but not world writable.


# OpenLDAP supports the ldap.conf file. You could use this file to
# specify a number of defaults for OpenLDAP clients. Normally this
# file can be found under /etc/openldap based on /etc/init.d/ldap
# start script's setting

# Set host IP address or fully qualified domain name

HOST example.peter.com
#HOST 10.2.1.1

# Set the default BASE DN where LDAP search will start off

BASE dc=peter,dc=com

# Set the default URI
```

```
URI  ldap://example.peter.com

# SASL options
# specify the sasl mechanism to use. This is a user-only option.
# SASL_MECH <mechanism>
# specify the realm. This is a user-only option
# SASL_REALM <realm>
# specify the authentication identity.
# SASL_AUTHCID <authcid>
```

Sample slapd.conf

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file


# NOTE 1
# All the OpenLDAP config files and backend databases are accessed
# and created by “ldap”, so if you touch these config files by
# "root", “a Permission Denied” error will occur. Please modify
# ownership accordingly.

# NOTE 2
# krb5-kdc.schema fails to work with current OpenLDAP 2.2.x distro
# krb5ValidStart, krb5ValidEnd, krb5PasswordEnd need to have
# "EQUALITY generalizedTimeMatch" inserted before the ORDERING
# statement.
# www.openldap.org/lists/openldap-bugs/200309/msg00029.html

# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file

schemacheck on

# Included schemas

include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/krb5-kdc.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/java.schema
```

```
# Do not enable referrals since IWSS 2.5 has its own implementation
# referral ldap://root.openldap.org

# Directives say where to write out slapd's PID and arguments
# started with

pidfile /usr/local/var/run/slapd.pid
argsfile /usr/local/var/run/slapd.args

# Load dynamic backend modules:
# modulepath      /usr/local/libexec/openldap
# moduleload      back_bdb.la
# moduleload      back_ldap.la
# moduleload      back_ldbm.la
# moduleload      back_passwd.la
# moduleload      back_shell.la

# Sample security restrictions
#   Require integrity protection (prevent hijacking)
#   Require 112-bit (3DES or better) encryption for updates
#   Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#   Root DSE: allow anyone to read it
#   Subschema (sub)entry DSE: allow anyone to read it
#   Other DSEs:
#          Allow self write access
#          Allow authenticated users read access
#          Allow anonymous users to authenticate
#   Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#   by self write
#   by users read
#   by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
```

```
access to *
    by self write
    by users read
    by anonymous auth
    by * none

# We have found this gives a useful amount of information about
# directory

loglevel 256

#Specify the number of threads used in slapd, default = 16
#Increasing or decreasing the number of threads used can
#drastically affect performance, we found 20 threads to be optimal
#for our setup, but it can be different under other operating
#systems

threads 20

#Tell slapd to close connections that have been idle for 30 seconds
#or more

idletimeout 30

# Enable LDAPv2 support. This option is disabled by default.

allow bind_v2

# Disable anonymous bind

disallow bind_anon

# Comment this section to enable simple bind

#disallow bind_simple

# NOTE 3
# SASL Configuration
# Caution: make sure you use the canonical name of the machine
# in sasl-host. Otherwise, OpenLDAP wont be able to offer GSSAPI
# authentication

# Set the SASL realm and canonical name of the host
sasl_host         example.peter.com
sasl_realm        PETER.COM

# Allow proxy authentication if it's configured

sasl-authz-policy        both
```

```
# NOTE 4
# Mapping of SASL authentication identities to LDAP entries
# The sasl-regexp line are particularly critical. They are what
# rewrite incoming connections who have SASL formatted DNs to the
# DNs that are in the directory DB. It's important to remember that
# they are processed in order, so you want to write them from most
# specific to most general

# NOTE 5
# We set the cn=.* since we are going to adopt different security
# mechanisms. If Kerberos v5 is the only one used, change wildcard
# to cn=GSSAPI,cn=auth

#sasl-regexp uid=(.*),cn=GSSAPI,cn=auth
#uid=$1,ou=people,dc=peter,dc=com

sasl-regexp uid=(.*),cn=.*,cn=auth uid=$1,ou=people,dc=peter,dc=com

# ldbm database definitions

# NOTE 6
# Correctly configuring the backend Berkeley DB is very critical
# follow the guideline at
# http://www.openldap.org/faq/data/cache/1073.html

# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.

database   bdb

# These options specify a DN and passwd that can be used to
# authenticate as the super-user entry of the database. The DN and
# password specified here will always work, regardless of whether
# the entry named actually exists or has the password given.
# This solves the chicken-and-egg problem of how to authenticate and
# add entries before any entries yet exist

suffix     "dc=peter,dc=com"
rootdn     "cn=admin,dc=peter,dc=com"
rootpw     admin

# NOTE 7
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700
# recommended.

directory  /usr/local/var/openldap-data
```

```
#Tell the slapd to store the 10000 most accessed entries in memory
#Having a properly configured cache size can drastically affect
#performance

cachesize 10000

# Indices to maintain
# Some versions of OpenLDAP don't support the index of uniqueMember
# "pres" indexing allows you to see a filter that asks if the
# attribute is present in an entry
# "eq" indexing allows to ask if an attribute has an exact value
# "apporx" indexing allows to ask if an attribute value sounds like
# something
#  This option is tied to --enable-phonetic compile option in
# OpenLDAP
# "sub" indexing allows to do substring search on an attribute's
# values

index default                           eq,pres
index objectclass                       eq,pres
index cn,sn,givenname,mail              eq,pres,approx,sub
index uid                               eq,pres
index uidNumber,gidNumber,memberUid     eq,pres
```

Tools

- Create the server database and associate indices by importing an existing LDIF file

NAME

slapadd - Add entries to a SLAPD database

SYNOPSIS

```
/usr/sbin/slapadd  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

Slapadd is used to add entries specified in LDAP Directory Interchange Format (LDIF) to a slapd database.

- Dump the server database to an LDIF file. This can be useful when you want to make human-readable backup of current database.

NAME

slapcat - SLAPD database to LDIF utility

SYNOPSIS

```
/usr/sbin/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

slapcat is used to generate an LDAP Directory Interchange Format (LDIF) output based upon the contents of a slapd database.

- Rebuilds all indices based upon the current database contents

NAME

slapindex - SLAPD index to LDIF utility

SYNOPSIS

```
/usr/sbin/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf]
```

DESCRIPTION

Slapindex is used to regenerate slapd indices based upon the current contents of a database.

- Check the settings of slapd.conf

NAME

Slaptest – Check the suitability of the slapd conf file

SYNOPSIS

```
/usr/sbin/slaptest  [-v]  [-d  level] [-f slapd.conf]
```

DESCRIPTION

Slaptest is used to check the conformance of the slapd.conf configuration file. It opens the slapd.conf configuration file, and parses it according to the general and the backend-specific rules, checking its conformance.

- LDAP query utility

NAME

ldapsearch - LDAP search tool

SYNOPSIS

```
ldapsearch  [-D binddn] [-W]  [-w bindpasswd] [-H ldapuri] [-h
ldaphost] [-p ldap- port]  [-b searchbase] [-s base|one|sub] [-x]
[-Y mech] [-Z[Z]] filter [attrs...]
```

DESCRIPTION

ldapsearch opens a connection to an LDAP server, binds, and performs a search using specified parameters.

EXAMPLE

The command performs a query using simple plain text authentication for a matched entry with “uid=petery” and requests the mail attribute for a matched entry to be returned by the LDAP server.

```
ldapsearch -x -D "cn=admin,dc=peter,dc=com" -w admin -b
"dc=peter,dc=com" -s sub "uid=petery" mail
```

For further information, consult the manual page.

```
Verify SASL/OpenLDAP/Kerberos v5 Authentication

1. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -v -x \

-D "cn=admin,dc=peter,dc=com" -W -b "" -s base -LLL \

-H ldap://example.peter.com/ supportedSASLMechanisms

2. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -b
"dc=peter,dc=com" \

-H ldap://example.peter.com/

3. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapwhoami -H
ldap://example.peter.com
```

Customized Attribute Equivalence Table Configuration

If you configure IWSS to use the OpenLDAP or Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server) directories, there are several user group associations that can be configured.

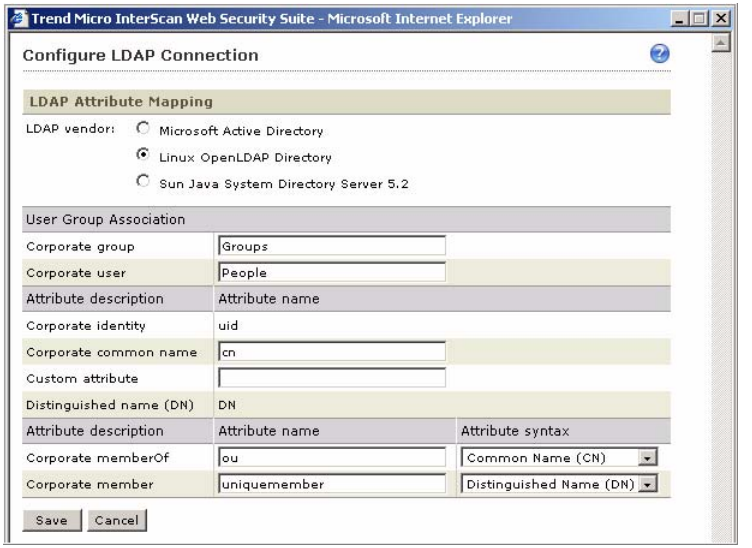


FIGURE C-1 OpenLDAP attribute mapping configuration screen

The "Corporate group" field tells IWSS the root container for all group entries while "Corporate user" indicates the root container for user entries. Since LDAP cannot distinguish whether an entry is group or user-specific, IWSS needs this "tag" to perform the query.

The "Corporate memberOf" field defines the group membership of an entry, a user or a group while the "Corporate member" field specifies the members in a group entry since a user is the finest entity and cannot contain any member. An attribute name is the first column in this equivalence table and it specifies the attribute that contains relevant information. Default attributes are "ou" and "uniquemember" in the standard OpenLDAP schema.

Attribute syntax is the second column in the equivalence table and it defines the attribute that IWSS needs to associate and look up to locate the group or member entry in the LDAP server. IWSS provides three options to configure this setting, namely {“Common Name (CN)”, “Distinguished Name (DN), “Customized Attribute”}.

Consider the following simple LDIF file as an example, keeping in mind the following:

- LDIF is a method for representing data in an LDAP directory in a human readable format.
- To simplify the example, some entries have been removed.
- To dump a LDIF file of an OpenLDAP server, execute slapcat, usually under the OpenLDAP installation path or `/usr/local/sbin`.

```
slapcat –l [output_file_name]
```

LDIF Format Sample Entries

The following are simplified example of a user and group entry in LDIF format:

1

```
dn: uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSS Developer Team
ou: People                      #Corporate User field
mail: petery@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: petery
cn: Peter Yen
```

2

FIGURE C-2 Sample user entry in LDIF format

```
dn: cn=All of IWSS Developer
Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=trendnet,dc=org
ou: Groups                      #Corporate Group field
ou: Engineering
description: All of IWSS Developer Team
objectClass: top
objectClass: groupOfUniqueNames
uniqueMember:uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
cn: All of IWSS Developer Team
```

FIGURE C-3 Sample group entry in LDIF format

Take note of the following:

- Associate the "Corporate Member" between a group and user entry using "Distinguished Name (DN)" as the attribute syntax.
- Associate the "Corporate MemberOf" in a group and user entry using "Common Name (CN)" as the attribute syntax.

Sample Configuration

Consider the following LDAP attribute mapping:

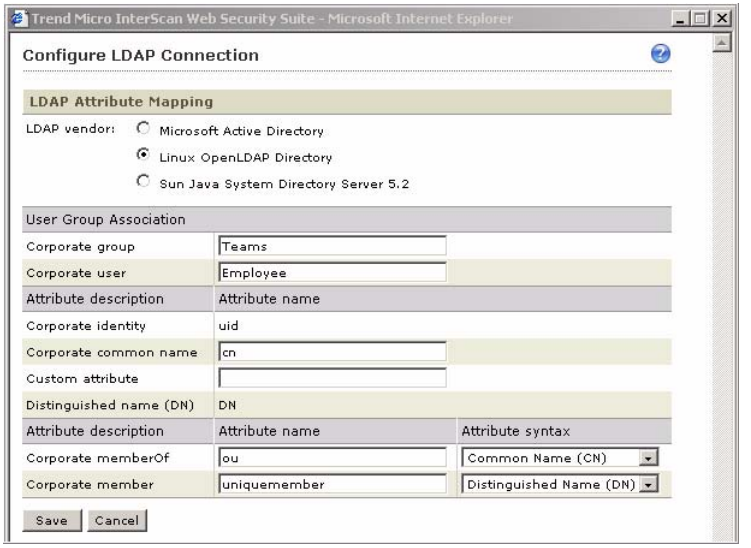


FIGURE C-4 OpenLDAP attribute mapping configuration screen

```
dn: uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSS Developer Team
ou: Employee                    #Corporate User field
mail: petery@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: petery
cn: Peter Yen
```

2

1

FIGURE C-5 Sample user entry in LDIF format

```
dn: cn=All of IWSS Developer
Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=trendnet,dc=org
ou: Teams                       #Corporate Group field
ou: Engineering
description: All of IWSS Developer Team
objectClass: top
objectClass: groupOfUniqueNames
teamMember: Peter Yen
cn: All of IWSS Developer Team
```

FIGURE C-6 Sample group entry in LDIF format

Take note the of the following:

1. Associate the "Corporate Member" between a group and user entry using "Distinguished Name (DN)" as the attribute syntax.
2. Associate the "Corporate MemberOf" in a group and user entry using "Common Name (CN)" as the attribute syntax.

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
100BaseT	An alternate term for “fast Ethernet,” an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT. *Also see* 10BaseT.
10BaseT	The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024. *Also see* 100BaseT.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.

Term	Explanation
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your Isoftware after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session.
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.
ActiveX malicious code	An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner. Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to "high."

Term	Explanation
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to “system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
anti-relay	Mechanisms to prevent hosts from “piggybacking” through another host’s network.
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.

Term	Explanation
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on pub-lic-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
bridge	A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address.
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from a file or message.

Term	Explanation
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.

Term	Explanation
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory on the C drive.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is: *C:\Programs\Trend Micro\ISVW\Quarantine*
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
(administrative) domain	A group of computers sharing a common database and security policy.

Term	Explanation
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
DOS virus	Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a Web site via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.
ELF	Executable and Linkable Format—An executable file format for Unix and Linux platforms.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

Term	Explanation
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
EXE file infector	An executable program with a .exe file extension. *Also see* DOS virus.
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.

Term	Explanation
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
filtering, dynamic	IP service that can be used within VPN tunnels. Filters are one way GateLock controls traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. *Also see* tunneling and Virtual Private Network (VPN).
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.

Term	Explanation
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.

Term	Explanation
hub	This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, crytography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install Unix versions of Trend Micro products.
integrity checking	*See* checksumming.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

Term	Explanation
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
"in the wild"	Describes known viruses that are actively circulating. *Also see* "in the zoo."
"in the zoo"	Describes known viruses that are currently controlled by antivirus products. *Also see* "in the wild."
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IP gateway	Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java applets	Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality. Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to "high."
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.

Term	Explanation
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of memory.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
LDAP (Lightweight Directory Access Protocol)	An internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name "Bob." An LDAP search would enable you to view the email addresses that meet this criteria.
license	Authorization by law to use a Trend Micro product.
license certificate	A document that proves you are an authorized user of a Trend Micro product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.

Term	Explanation
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
management console	The user interface for your Trend Micro product.

Term	Explanation
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
MB	Megabyte—1024 kilobytes of data.
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

Term	Explanation
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.

Term	Explanation
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
protected network	A network protected by Network VirusWall.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.

Term	Explanation
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
script	A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with "script" are "macro" or "batch file."
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
seat	A license for one person to use a Trend Micro product.

Term	Explanation
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
server farm	A server farm is a network where clients install their own computers to run Web servers, e-mail, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.
signature-based spam detection	A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file. *Also see* rule-based spam detection. *Also see* false positive.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.

Term	Explanation
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
spam	Unsolicited email messages meant to promote a product or service.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

Term	Explanation
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This may *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
trusted domain	A domain from which your Trend Micro product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, since the messages are from a known and trusted source.
trusted host	A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.

Term	Explanation
tunneling	A method of sending data that enables one network to send data via another network's connections. Tunnelling is used to get data between administrative domains which use a protocol that is not supported by the internet connecting those domains. With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.
tunnel interface	A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface. *Also see* Virtual Private Network (VPN).
tunnel zone	A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.

Term	Explanation
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions. By default, Trend Micro GateLock supports two virtual routers: Untrust-VR and Trust-VR.
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same Trend Micro GateLock remote appliance; each one can be managed by its own virtual system administrator.

Term	Explanation
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as /etc/iscan/iwss.

Term	Explanation
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
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.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).

Index

A

access control
  by client IP 44
  FTP 161
  identifying clients/servers 43
  settings 43
access log 166
  upstream proxy 166
access quotas 5–6, 119
  adding 120
  deactivating 123
  exceeding during a download 120
  Guest Policy 120
  introducing 120
  managing 120
actions
  infected file (FTP) 160
  Macro Scan (FTP) 161
  password-protected file (FTP) 161
  uncleanable file (FTP) 160
active FTP 153
ActiveUpdate 18, 138
  incremental updates 22
  without Control Manager 18
ActiveX objects
  security rules 106
  signature verification 95, 111
additional risks
  defined 89
anonymous FTP 41
anti-phishing 3
anti-spyware 3
Applets and ActiveX security 2, 5
  adding/modifying policies 98
  digital certificates 112
  enabling 98
  enabling/disabling 74
  how it works 94–95
  notifications 116, 204
  settings 108
  thread groups 105
architecture 14

C

cache servers 4
  Cisco 3
  flushing 29
  Network Appliance 3
cleanup log 185
comma-separated value (CSV) 7
compressed files 159
  handling 82
  security settings 81
concurrent connections 42
configuration files 221
Control Manager 3
controlled pattern releases (CPRs) 30
  incremental updates 31
  installing 30
CSV 7
cyrus-sasl-2.1.19 226

D

Damage Cleanup Services (DCS) 9, 86
database
  and log files 166
delete 177
dependent mode 37
destination ports (FTP) 164
digital certificates
  managing 112
disease vector 131
documentation set x

E

ESMTP 196

F

false alarm 29
file blocking

notification 200
file types 78
blocking 77
specifying (FTP) 155
flagged certificates 100
forced updates 29
forward proxy 34
FTP
anonymous 41
port restrictions 164
security risks 2
turning on/off the service 154
FTP Get log 184
FTP over HTTP 38, 88
FTP proxy 153
FTP Put log 185
FTP scanning 6, 10
compressed files 156, 159
configuring 156
enabling 154–155
file blocking 155
files to scan 155
large files 156
notifications 202
options 154
priority 156
proxy settings 152
quarantine 157
scan direction 155
server IP white list 163
settings 153, 157

G

Global Policy 51, 53
glossary 239
grayware
defined 89
Guest Policy 51, 53
about 53
guest port 51
enabling 53

H

heimdal-0.6.2 226
HTTP
enabling/disabling traffic 50
file types to block 77
file types to scan 78
port restrictions 46
security threats 2
service, turning on/off 34
HTTP scanning
compressed files 81
creating/modifying policies 76
deferred scanning 84–85
enabling/disabling 74
file blocking 77
files to scan 78
forward proxy 34
intranet sites 124
large files 82
notifications 198
performance 75
priority 81
progress page 84
quarantine 89
reverse proxy 34
rules 77
scan actions 91
scan after delivering 84, 86
scan before delivering 84
scan events 92
security settings 81
settings 33
skipping files 75
trusted URLs 124
HTTPS
port restrictions 48
scanning 41

I

ICAP 4
ICSA certification 24
incremental pattern file updates 22
instrumentation 96
IntelliScan 78
Internet Caching Acceleration Protocol. See ICAP
IWSS
benefits 2
components 14

features 5
how it detects viruses 2
main features 5
modules 14
services 14
IWSSPIUrlFilter.dsc 146

J

Java applets
instrumentation 11
instrumentation settings 100
instrumenting 96
real-time monitoring 97
security rules 99
signature status 99
signature validation 108
signature verification 95

K

Kerberos 225
Knowledge Base x
URL x

L

large file handling
deferred scanning 84
HTTP 43, 82
important notes 88
LDAP 3
AD Global Catalog 65
attribute names 61
authentication 58
communication flows 59
configuring 60
directory support 12
matching across referral servers 64
referral servers 63
supported directories 58
testing connection 64
ldapsearch 232
LDIF files 235
listening port 41
log files
FTP Get Log 184
FTP Put Log 185
naming conventions 189
URL blocking log 181
virus log 190
log settings 187
logs 6, 13
deleting 185–186
exporting as CSV files 191
file naming conventions 189
folders 187
introduction 180
querying/viewing 180
reporting 180
system 180
lpt$vpn.xyz 29

M

macro scanning 92
actions 92
MIME-type 10, 75, 80, 215
mixed threats 2
multiple installs 7

N

notifications 7, 13, 160
administrator vs. user 194
configuring 197
email settings 195
ESMTP support 196
introduction 194
SNMP 208
tokens 196
using HTML tags 197
using variables in 196

O

online help x
OpenLDAP 225
attribute equivalence 234
sample ldap.conf 226
sample slapd.com 227
software compatibility 226
openldap-2.2.17 226
openssl-0.9.7d 226
Outbreak Prevention Policy (OPP) 182
defined rule 182
ID 183

P

passive FTP 153
pattern files 20–21
  deleting 30
  manually deleting 30
  several on server 22
  spyware/grayware 22
  version numbering 21, 23
pattern matching 21
performance log 184
phishing 2, 131
  URLs 132
PhishTrap 9, 22
  benefits 131
  blocking 132
  categories 131
  criteria for inclusion 131
  defined rule 183
  introduction 2
  overview 132
  submitting URLs 132
policies
  configuring the scope 65
  default 53
  how they work 52
  practical examples 52
progress page 84–85
protocol handlers 222
proxy
  caching 37
  configuring 35
  examples 34
  listening port 41
  reverse 13, 39
  settings 18, 41
  stand-alone mode 35
  upstream proxy (dependent mode) 37

Q

quarantined files
  encrypting 157

R

readme x
RealAudio 80
receive greeting 160
register_user_agent_header.exe 58
reports 6, 13
  archiving 178
  availability 172
  blocking-event 167
  chart types 169
  configuring logs 188
  consolidated vs. individual 169
  customizing 178
  daily 175
  deleting scheduled 177
  introduction 166
  real-time 170
  scheduled 175
  setting the scope 169
  settings 168–169
  traffic 168
  types 166–167
REQMOD 45
RESPMOD 45
reverse proxy 34, 39
  configuring 40
  DNS changes 40
rollback 29

S

scan engine 20, 23
  events that trigger an update 24
  ICSA certification 24
  updates to 24
  updating 24
  URL to find current version 24
scanning
  modules 223
  select file types 79
scanning modules 223
scheduled tasks 15
server IP white list
  adding servers 45
  ICAP mode 45
ServerIPWhiteList.ini 45
signature status
  revocation status 110
  untrusted 109

slapadd 231
slapcat 232
slapd.conf 227
slapindex 232
slaptest 232
SNMP 7, 12, 208
SolutionBank-see Knowledge Base x
spyware/grayware 3, 9, 131
  reports 7
  scanning rules 89
spyware/grayware log 181
system
  log directories, configuration 188

T

time-to-live (TTL) 120
tokens in notifications 196
transparency 38
TrendLabs 4
true file type 78
trusted URLs 6, 12, 124
  importing 124
  managing 125
TTL 120

U

uniquemember 234
updates
  components 20, 26
  disabling scheduled updates 28
  forced 27
  incremental 22
  manual 27
  notifications 29, 206
  proxy settings 18
  recommendations 18
  rolling back 29
  scheduled 18, 27
  verifying success 29
URL access 6, 124
  log 183
URL blocking 6, 12, 127
  importing 129
  importing a list 130
  notifications 202
  PhishTrap 132
  rules 182
  via local list 129
  via pattern file 131
  wildcards 130
URL blocking log 182
URL filtering 5, 25
  creating a policy 139
  customizing 136
  database 20, 25, 137
  enabling 139
  exceptions 146
  importing exceptions 148
  managing categories 144
  managing policies 139
  overview 136
  policy, introduction 139
  re-classification 144
  remote classification server 138
  rule 182
  schedule 149
  settings 144
  time settings 149
  workflow 137
urlfcIfx.ini 138
URLFilteringExceptions.ini 146
URLs
  Knowledge Base x
  scan engine version 24
User ID 183
user identification method 6, 12, 51
  Client Registration Utility 57
  configuring 54
  host name 56, 67
  IP address 55, 66
  types of 54
  user/group name via proxy authorization 58, 69

V

variables
  using in notifications 196
virus
  "in the wild" 23
  "in the zoo" 23
  action 91

notifications 148
pattern file, published 22
virus accomplice 131
virus log 180
virus scanning 5
actions 160
configuration 34
deferred scanning 11
virus signatures
see virus pattern file

W

wildcards 130
work time 137
worker threads 42