TREND MICRO™

InterScan™ VirusWall™ 7

for Small and Medium Businesses

Integrated virus and spam protection for your Internet gateway

for Windows™

Administrator's Guide

Messaging Security

Web Security

Document Part No. IVEM74091/90513
Release Date: July, 2009
Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698 and 6,119,165

The Administrator's Guide for Trend Micro InterScan VirusWall is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

To contact Trend Micro Support, please see *Obtaining Technical Support* on page 15-31 of this document.

At Trend Micro, we are always seeking to improve our 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 Trend Micro InterScan VirusWall

Chapter 2: Planning to Install InterScan VirusWall

Chapter 3: Installing InterScan VirusWall

Chapter 4: Configuring SMTP Services

Chapter 5: Configuring HTTP Services

Chapter 6: Configuring FTP Services

Chapter 7: Configuring POP3 Services

Chapter 8: Outbreak Prevention Services

Chapter 9: Quarantines

Chapter 10: Update

Chapter 11: Local Reports

Chapter 12: Logs

Chapter 13: Administration

Chapter 14: Using Real-Time Scan Monitor

Chapter 15: Troubleshooting and Support

Appendix A: System Checklists

Appendix B: Default Values

Appendix C: Migration from InterScan VirusWall 3.55

Appendix D: Migration from InterScan VirusWall 5.0

Appendix E: Migration from InterScan VirusWall 6.0, 6.01, or 6.02

Appendix F: TMCM Replication Limitations

Preface

Preface

Welcome to the *Trend Micro™ InterScan VirusWall Administrator's Guide* for release 7.0. This guide provides detailed information about the InterScan VirusWall (ISVW) for Windows configuration options. Topics include installation and deployment options, how to keep security updates current, how to protect Web and email traffic from malicious viruses/spyware/spam and phishing traffic, how to configure and use policies to support your security objectives, configuring scanning, configuring URL blocking and filtering, and generating reports on security events.

This preface describes the following:

- *InterScan VirusWall Documentation*
- *Audience*
- *Document Conventions*

InterScan VirusWall Documentation

In addition to the *Trend Micro™ InterScan VirusWall Administrator's Guide*, the documentation set includes the following:

- **Quick Start Guide**—This guide helps you get "up and running" by introducing ISVW, assisting with installation planning, implementation, and configuration, and describing the main post-upgrade 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 ISVW Web 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 Quick Start 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`

- **TrendEdge**—A program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  `http://trendedge.trendmicro.com`

Audience

The ISVW documentation is written for IT managers and system administrators working in a medium or large enterprise environment. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP,SMTP, POP3 and FTP protocols
- Experience with Windows networking, email setup, and Microsoft Active Directory administration

The documentation does not assume the reader has any knowledge of antivirus or Web security technology.

Document Conventions

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

TABLE P-1. Document 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 Trend Micro InterScan VirusWall

InterScan™ VirusWall™ (ISVW) for Windows provides an all-in-one gateway antivirus, anti-spam, anti-spyware/grayware, and content scanning or filtering solution for your organization's network. For example, you do not have to install separate applications for virus protection, spam detection, or content filtering—all of these functions are available in a single, easy-to-use application. ISVW for Windows provides protection for SMTP, POP3, HTTP, and FTP traffic protocols, to ensure that employees do not accidentally bring in viruses or malware from their email accounts or when downloading files. In addition, ISVW for Windows provides heuristics based anti-spam and content scanning for SMTP and POP3 traffic.

ISVW offers simplified configuration for easy set up and requires minimal day-to-day maintenance, which is especially useful for users who have limited time or IT resources, yet still require full-time virus and spam prevention services.

Migration tools have been included to help existing ISVW users migrate from the earlier versions of the product.

Features and Benefits

ISVW provides the following features and benefits.

TABLE 1-1. ISVW Features and Benefits

FEATURES	DESCRIPTIONS
All-in-one defense	Antivirus, anti-spam, anti-spyware/grayware, anti-phishing, IntelliTrap™ (Bot threats), content filtering, Outbreak Prevention Services (OPS), URL blocking, URL filtering, and email reputation for SMTP *IntelliTrap is a real-time, rule-based, and pattern recognition scan engine technology that detects and removes known viruses in files compressed up to 20 layers deep using any of 16 popular compression types.*
Automatic threat protection	Outbreak Defense provides full protection when used with TMCM
Scalability	Small and Medium Business to Enterprise deployment, with the option to install all four services to one or several servers
Gateway protection	Protection from malware right at the Internet gateway
Flexible configuration	Specify files to scan, the action to take on infected files/messages, and the notification message recipients of infected files/messages will receive
Centralized management	A Web-based console, accessible from a local or remote system, that enforces enterprise-wide Internet security policies
Automated maintenance	Routine tasks, such as updating, reporting, and alerting, configured and automated to meet the unique needs of your company
Easy installation	Installation wizard guides you through installation and some configuration tasks The ISVW 7.0 Setup program has a pre-flight check function that verifies compatibility with respect to system requirements, disk space requirements, service packs or patches required, and ports that need to be available. With the pre-flight check function, ISVW is able to co-exist with other products in an evaluation environment.

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

FEATURES	DESCRIPTIONS
Local reports	Reports can summarize many types of traffic violations. The report can include what virus occurred and when and where they came from. For HTTP Web violations, reports can also include the users violating within specified time period along with the types and frequency of violations. Report options can be set for all four protocols.
Migration tool for ISVW 3.55 users	ISVW 3.55 users can easily migrate their configuration settings when they upgrade to ISVW 7.0
Migration tool for ISVW 5.0 users	ISVW 5.0 users can easily migrate their configuration settings when they upgrade to ISVW 7.0
Migration tool for ISVW 6.0, 6.01, and 6.02 users	ISVW 6.0, 6.01, and 6.02 users can easily migrate their configuration settings when they upgrade to ISVW 7.0

New Features

ISVW has new features to protect your network against the latest malware threats. The additional features in this release include protection against spam, spyware and other grayware, Bot threats, and phishing; URL filtering and blocking capabilities; and protection through Outbreak Prevention Services (OPS).

List of New Features for ISVW

New Feature	Descriptions
Anti-phishing using Web Reputation	ISVW provides anti-phishing through Web Reputation, URL Filtering, and PhishTrap. Web Reputation guards end-users against emerging Web threats. Web Reputation assigns reputation scores to URLs. For each accessed URL, ISVW queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.
Setting user/group-based policy for URL blocking and filtering	URL blocking and filtering rules can now be applied to specific computers, users, or groups. ISVW uses a plugin called Domain Controller Agent that interacts with the Active Directory server in the network to determine what users or groups are available to configure policies against. This feature includes identification settings, Microsoft Active Directory service support, policy item management, and user/group-based log and report.

List of New Features for ISVW (Continued)

New Feature	Descriptions
Local reports	Reports can summarize many types of traffic violations. The report can include what virus occurred and when and where it came from. The report can also include which users have caused violations within specified time periods, along with the types and frequency of violations. ISVW 7.0 is able to generate reports for SMTP, HTTP, POP3 and FTP protocols. You can schedule a report or generate a one-time report.
Windows user/groups support (using Domain Controller agents and servers to identify users)	The User Identification Settings allow you to identify individual users and groups in your organization making HTTP connections through ISVW. The Trend Micro Domain Controller Agent offers transparent user identification for users in a Windows-based directory service. The Domain Controller agent communicates with the Domain Controller server to gather up-to-date user logon information and provide it to the ISVW. This information can be used to create URL filtering and blocking policies applied to specific users and groups.
Pre-flight check function	The ISVW 7.0 Setup program has a pre-flight check function that verifies compatibility with respect to system requirements, disk space requirements, service packs or patches required, and ports that need to be available. With the pre-flight check function, ISVW is able to co-exist with other products in an evaluation environment.
Migration path from previous version	It is easy to migrate from previous ISVW version (3.55, 5.0, 6.0x) to ISVW 7.0.
TMCM 5.0 support	ISVW 7.0 supports TMCM 5.0.

How InterScan VirusWall Works

ISVW scans all SMTP, POP3, HTTP, and FTP traffic for viruses between the corporate network and the Internet. Whenever it detects a file type that it has been configured to scan (for example, *.zip*, *.exe, .doc*), ISVW copies the file to a temporary location and scans it for viruses. If the file is clean, ISVW deletes the copy and forwards the original to its destination. If a virus is found, a notification is issued and ISVW takes the action you configure:

- **Auto Clean** the infected file and send it to the original server for normal delivery
- **Quarantine** the infected file (without cleaning) and place it into a quarantine directory; the file is not delivered
- **Block** the infected file; it is not delivered

- **Delete** the infected file; it is not delivered
- **Pass** the infected file (without cleaning); the infected file is delivered with an optional notification message

Notifications

For SMTP and POP3 traffic, ISVW can send notifications automatically to the system administrator, the sender, and the intended recipient. If no viruses are found, ISVW can append a message stating that the email was scanned and virus-free. Notifications for HTTP and FTP traffic are "inline" notifications that only appear for the end-user.

How InterScan VirusWall Detects Viruses

Using a process called *pattern matching*, ISVW draws upon an extensive database of virus patterns to identify known virus signatures. Key areas of suspect files are examined for characteristic strings of virus code and compared against the tens of thousands of virus signatures that Trend Micro has on record.

For polymorphic, or mutation viruses, the ISVW scanning engine permits suspicious files to execute in a temporary environment. When the file is run, any encrypted virus code embedded within the file is decrypted. ISVW then scans the entire file, including the freshly decrypted code, and identifies any strings of mutation virus, taking whatever action you have specified—clean, delete, quarantine, or pass.

It is important to keep the virus pattern file up to date as there are new threats being discovered daily. Trend Micro makes it easy to update the virus pattern file by supporting automatic updates.

MacroTrap

Macro viruses are not confined to any one operating system—they are application-specific, so they can be spread between DOS, Windows, MACs, and even OS/2 systems. This is a fundamental change in the way viruses are spread.

With the ability to travel by email, and the increasing power of macro code, you can see that macro viruses are perhaps the biggest threat. To combat the advent of macro viruses, Trend Micro has developed MacroTrap™, an intelligent technology that greatly enhances your ability to protect your corporate network.

How MacroTrap works

The MacroTrap performs a rules-based examination of all macro code that is saved in association with a document. Macro virus code is typically contained as a part of the invisible template (.DOT, for example, in Microsoft Word) that travels with the document. Trend Micro's MacroTrap checks the template for signs of unknown macro viruses by seeking out instructions that perform virus-like activity— for example, copying parts of the template to other templates (replication), or executing harmful commands (destruction).

Compressed files

ISVW opens compressed files and examines the contents according to the criteria specified in the Scan Files option of each VirusWall. When ISVW encounters multiple layers of compression, it recursively extracts each, up to a limit of 20. For example, if an archive contains *.cab* files that have been compressed using common compression tools like pk-zip or winzip, ISVW will extract each layer until it finds no more compressed files (at which point, all files contained within the compressed file have been scanned), or the limit of 20 has been reached.

Performance

To maximize performance, ISVW makes some intelligent choices about the files it scans and the way it scans them. It scans only file types that are more prone to infection and to carrying a virus. In addition, it checks only key areas of these files for matching virus signatures. Files are checked against the Trend Micro proprietary database, which contains an extensive amount of known viruses. ISVW uses heuristic logic to analyze whether certain unknown code (unique to polymorphic viruses, for example) is virus-like in nature and warrants testing.

How InterScan VirusWall Detects Phishing Threats

ISVW detects phishing threats in the following ways:

- Pattern-based filter is applied to SMTP, HTTP, and POP3 mail.
- PhishTrap works in conjunction with ISVW to monitor outbound client URL requests and compare them to a known list of phish sites. Whenever a match occurs, PhishTrap blocks access to the site.
- URL filtering blocks URLs based on categories, using a phishing category.
- Web Reputation blocks URLs based on their reputation.

Only the pattern-based filter provides a notification message that is specific to phishing. The last two methods have general notification messages which do not specifically identify phishing as the reason for blocking a site.

Chapter 2

Planning to Install InterScan VirusWall

Installing InterScan VirusWall (ISVW) takes about 10 minutes and should be performed from the machine where the program(s) will reside. Allow another 10 to 15 minutes to configure ISVW to work with your existing servers.

If migrating from ISVW 3.55, 5.0, or 6.0x, ISVW provides a migration tool that allows you to export your configuration settings from these earlier versions and import them into version 7.0.

Installation Overview

The Trend Micro ISVW application for the gateway contains real-time scanning services that check for viruses in email (SMTP and POP3), Web (HTTP), and file (FTP) transfers to and from the LAN.

All services can be installed on the same machine. However, installing multiple services onto the same server is not typically recommended because scanning network traffic streams in real-time, along with the usual operations of the server, can be rather CPU and disk-intensive. It is more typical to run multiple iterations of Setup to install ISVW on several servers and then activate different services on different servers. For example,

run Setup once to install the SMTP and POP3 services on to the SMTP server, again to install the HTTP service onto an HTTP proxy server, and then again to install FTP VirusWall.

System Requirements

TABLE 2-1. Minimum and Recommended System Requirements

REQUIREMENT	MINIMUM	RECOMMENDED
CPU	1 CPU: Intel™ Pentium™ 4, 1.6GHz or higher	2 or 4 CPUs: Intel Pentium 4 with Hyper-Threading Technology™, 3.0GHz or higher
Memory	1GB RAM	2GB RAM or higher
Available hard disk space	1GB for the target program drive **Note**: The ISVW installation program checks the free disk space on the system and target drives. If your server lacks the 1GB minimum disk space, the installation process will not proceed.	20GB for the target program drive for quarantine files and log files
Operating system	• Windows 2000 Server/Advanced Server with Service Pack 4 • Windows Server 2003 Standard Edition/Enterprise Edition/Web Edition with Service Pack 2 (32 bit) • Windows Server 2003 Standard Edition/Enterprise Edition/Web Edition with Service Pack 2 (64 bit) • Windows Server 2003 R2 with service pack 2 (32 bit and 64 bit) • Windows Server 2003 R2 with Service Pack 2 • Windows 2008 Server Enterprise Edition/Standard Edition (64 bit)	• Windows Server 2003 Standard Edition/Enterprise Editions/Web Edition with service pack 1 • Windows Server/Advanced Server 2000 with service pack 4 • Windows 2003 with SP2 • Windows 2008 server enterprise edition/Standard Edition (32bit) **Note:** ISVW checks the platform and operating system before starting the installation process. If the platform and operating system are not supported, ISVW issues a message but still allows you to continue the installation.
Internet browser to access the Web management console	• Microsoft® Internet Explorer 6.0 • Firefox® 2.0	• Microsoft Internet Explorer 7.0 or 8.0 • Firefox 3.0

Domain Controller Agent Requirements

TABLE 2-2. Domain Controller Agent Requirements

REQUIREMENT	Description
Domain Controller Agent	• A designated computer to run Domain Controller Agent (preferably running on the same OS as the Domain Controller server) • Domain Controller Agent computer has to be part of the Windows domain • Firewall has to be on the Domain Controller Agent computer to allow inbound traffic on TCP port 65015

TABLE 2-2. Domain Controller Agent Requirements (Continued)

REQUIREMENT	Description
Domain Controller Server	• Windows 2000, 2003, or 2008 platform with Active Directory • Enable audit logon events on the Domain Controller server: 1. Choose Start > Control Panel > Administrative Tools. 2. Click Domain Controller Security Policy. 3. Expand Local Policies on the left pane, and then select Audit Policy. 4. Verify that Audit account logon events are enabled. See *User Identification* on page 15-29. • Enable log rotation/recycle for security logs on Domain Controller server: 1. Choose Start > Control Panel > Administrative Tools 2. Click **Event Viewer**. 3. Expand Event Viewer on the left pane, and then select **Security**. 4. Choose Action > Properties to open the Properties window 5. Make sure the log size is set appropriate and the **Overwrite events** option is selected. • If there is a firewall on the Domain Controller server, configure an exception to allow inbound traffic on TCP port 135 and TCP port 445 for RPC and remote event access.
ISVW	• Configure ISVW user identification settings to IP address and User Name (see *Selecting the User Identification Method* on page 13-15) • IP address of the Domain Controller Agent computer • User account with domain administrator's privileges

TABLE 2-2. Domain Controller Agent Requirements (Continued)

REQUIREMENT	Description
Windows Clients	• Remote Registry Service running on client computer • Log in using the domain account • If there is a firewall, configure exceptions to allow inbound RPC traffic on TCP port 445.

Planning Ahead

By default, ISVW uses port 25 to receive SMTP messages for processing, port 8080 for the HTTP proxy, port 21 for the FTP proxy server, and port 110 for POP3 incoming messages.

Depending on which services are installed and what proxy servers you have on the system, you may need to know the following information:

- The IP address of the current SMTP server
- The port number of the current SMTP server (usually 25)
- The IP address of the current POP3 server
- The port number of the current POP3 server (usually 110)
- The IP address of the current HTTP proxy server (if any)
- The port number of the current HTTP proxy server
- The port number ISVW will use if it is set up as the HTTP proxy server
- The IP address of the current FTP proxy server (if any)
- The port number of the current FTP proxy server
- The port number ISVW will use if it is set up as the FTP proxy server

Appendix A contains checklists to help you identify the appropriate server addresses and ports.

Deciding Where to Install

You can install ISVW on the same machine as the original server or on a different one. In deciding where to install, the most important issue is almost always whether there are sufficient resources on the target machine to adequately handle the additional load.

Before installing ISVW, you should evaluate the peak and mean traffic loads handled by the server and compare the results to the overall capacity of that machine. The closer the two measurements are, the more likely it is that you will want to install ISVW on a dedicated machine. Additional factors to consider include network bandwidth, current CPU load, CPU speed, total and available system memory, and the total amount of virtual memory space. Scanning one or more network protocols for viruses, in real-time, can be resource intensive—do not install ISVW onto a machine that does not have the capacity to handle the additional load.

Setup Choices

Same Machine—If you install ISVW on the same machine as the mail or a Web server, you will most likely need to change the port the original server uses and give the default to ISVW.

Defaults are typically: FTP: 21, SMTP: 25, HTTP: 80, POP3: 110.

Dedicated Machine—If ISVW is installed on a different machine than the server it will scan for, you do not need to change the port number of existing servers. You may, however, need to modify the clients to reflect the new IP address (or hostname) of the ISVW machine. If you would prefer not to change the clients:

- Consider swapping IP addresses (or hostnames) between the two machines so ISVW can use the original.
- Consider installing ISVW so that it is logically between the Internet, mail and HTTP proxy servers.

Installation Topologies

Trend Micro recommends installing ISVW directly behind a properly configured firewall or security device that offers network address translation (NAT) and other firewall-type equivalent protection.

You can strategically set up ISVW to address multiple topologies, ranging from a single integrated deployment where you install ISVW on a single server and then enable all services on that server, to a completely separate deployment where you run the ISVW installation on multiple servers and then enable only the desired service on each server.

Possible topology deployments include:

- Single, integrated deployment: install ISVW on one server and enable SMTP VirusWall, POP3 VirusWall, FTP VirusWall and HTTP VirusWall on that server
- Messaging/Web deployment:
  - For a messaging server, install ISVW on separate hardware and then enable SMTP and POP3 Virus Scanning during installation.
  - For Web security deployment, while installing ISVW enable the HTTP and FTP virus scanning options.
- Standalone deployment: install ISVW on four different servers and enable only one service on each server.

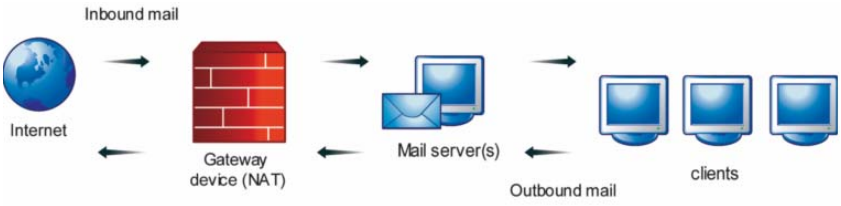
In the pages that follow, several possible installation topologies are presented, illustrating typical network setups before and after installing ISVW. Use the one that best fits your needs, or apply the principles to an installation strategy unique to your network.

SMTP

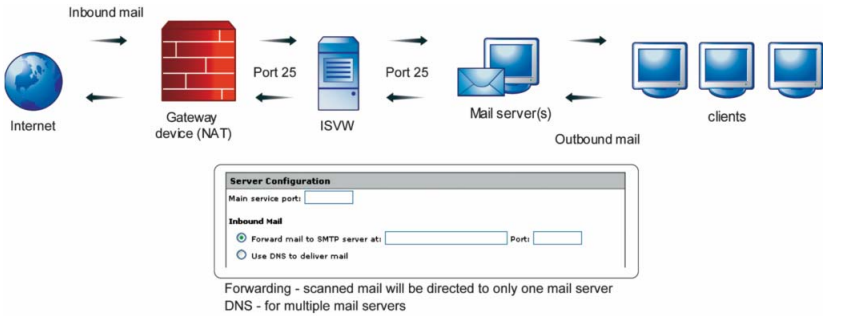
Remap the firewall's SMTP service, port 25, to the newly installed ISVW 7.0 server listening on port 25. Then use inbound mail forwarding (single server environment) or DNS (multi-server environment) to pass scanned mails to an internal mail server or servers. Ensure that the internal MX records are configured correctly when you choose to use DNS.

Using these suggestions will not require changing the IP address or addresses of internal mail server or servers. In addition, there are no changes to the client computers as they will still connect to their respective mail server.

Before installing ISVW 7.0



After installing ISVW 7.0 (ISVW 7.0 and mail server on different machines)



After installing ISVW 7.0 (ISVW 7.0 and mail server on the same machine)

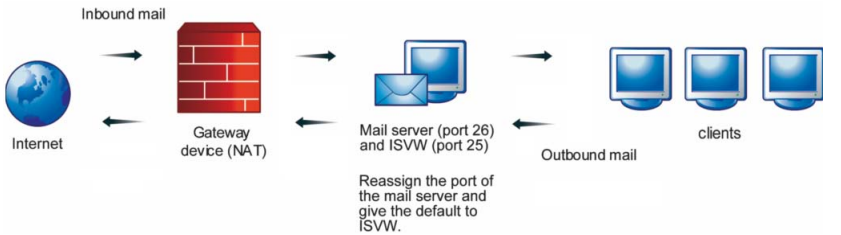


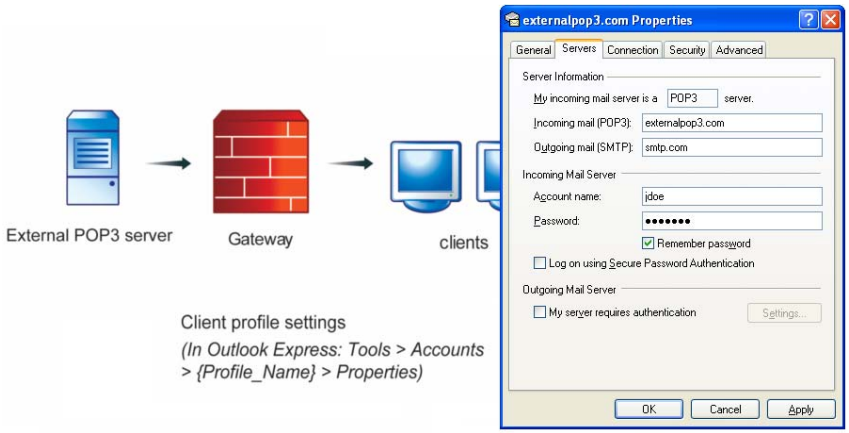
FIGURE 2-1. SMTP Installation Topologies

POP3

The typical POP3 topology requires modifying the client machine POP3 settings so that clients receive emails directly from ISVW 7.0. Change the clients' mailbox names from "Mailbox_name" to "Mailbox_name#POP3_server#Port_number".

For example, from "joedoe" to "joedoe#externalpop3.com#110".

Before installing ISVW



After installing ISVW 7.0

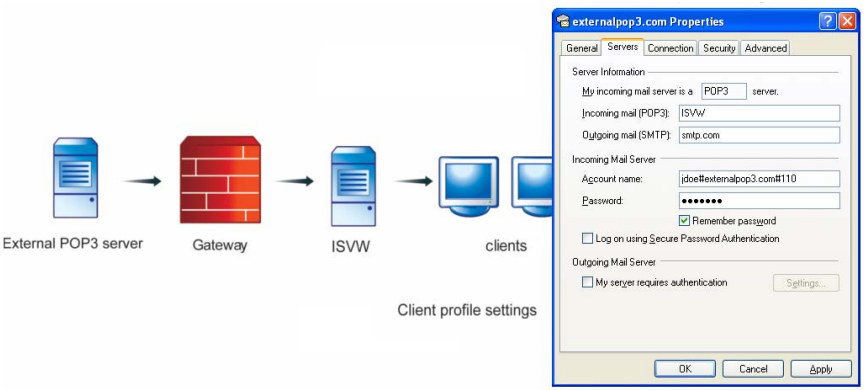


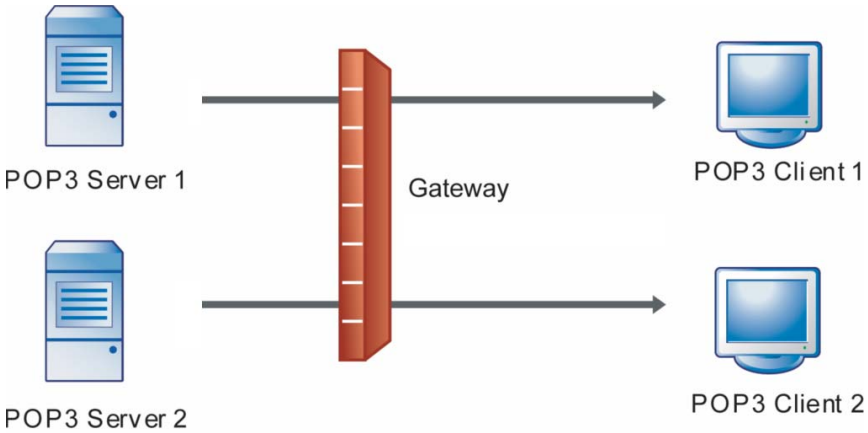
FIGURE 2-2. Typical POP3 Installation Topology

POP3 (Port Mapping)

If you set ISVW as a port-mapping server, the ports will be mapped to the listening port of ISVW and the specific POP3 servers. The required changes for this topology are as follows:

- In **Web management console > POP3 > Configuration**, inbound POP3 port should be the port that ISVW uses.
- In the POP3 settings on the client machines, incoming mail server name and port should be the ISVW server name and port number.

Before installing ISVW



After installing ISVW

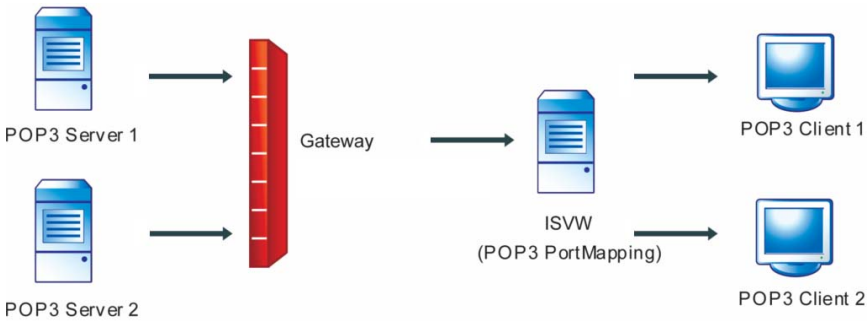


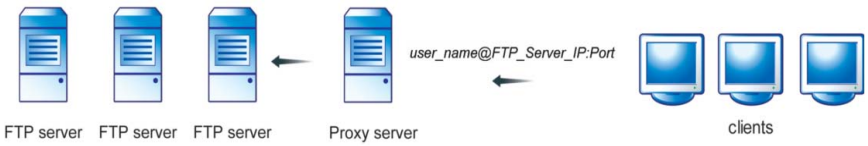
FIGURE 2-3. POP3 with ISVW Acting as a Port Mapping Server

FTP

In standalone mode, ISVW serves as the FTP proxy server. To connect to the specified FTP server through FTP VirusWall, users type the following:
`username@FTP_Server_IP:Port`

In dependent mode (ISVW works with an existing FTP proxy server), ISVW complements an existing FTP proxy server. If there is no proxy server, clients connecting to FTP VirusWall will be redirected to the real FTP server specified in the FTP Configuration screen in the ISVW Web management console. Every FTP session between the FTP server and the client machine will pass through FTP VirusWall, but this action is invisible to the end user.

Before installing ISVW 7.0 (with proxy server)



After installing ISVW 7.0 (with proxy server)

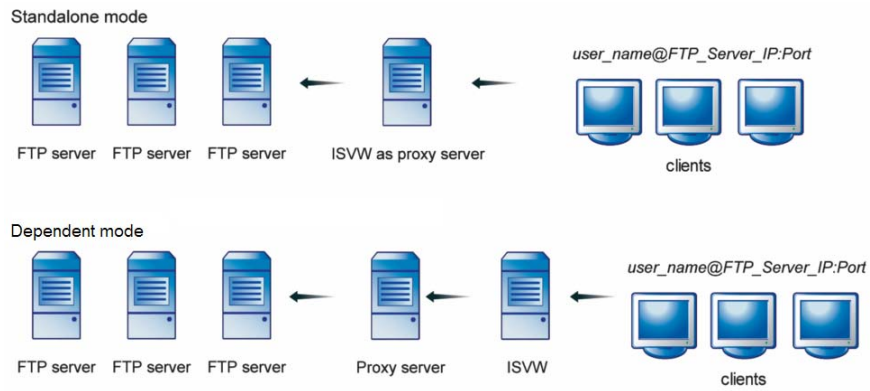
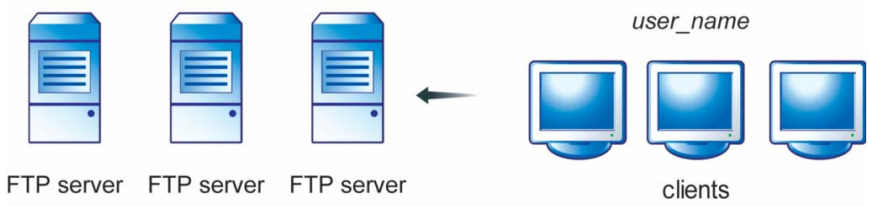


FIGURE 2-4. Installation Topology for FTP with Proxy Server

Before installing ISVW (without proxy server)



After installing ISVW 7.0 (without proxy server)

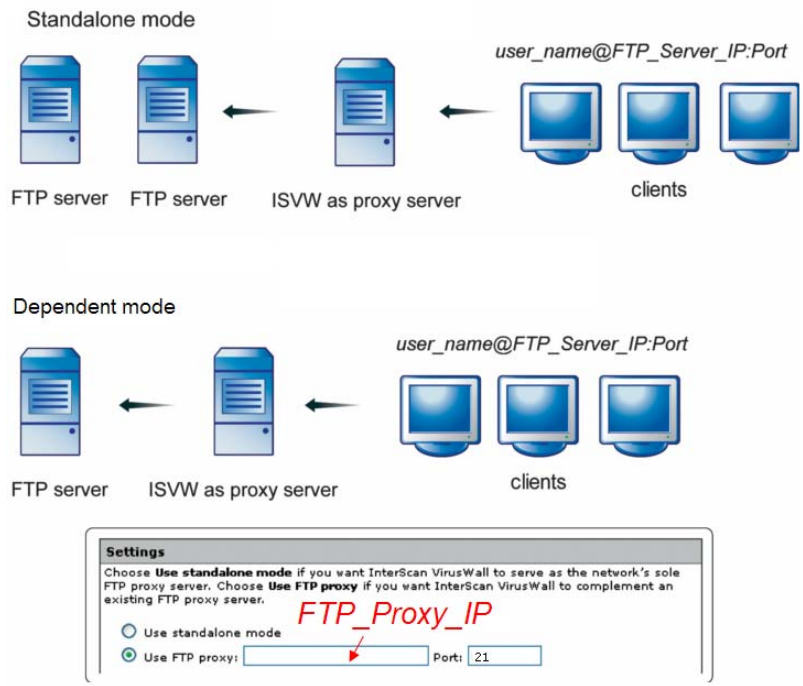


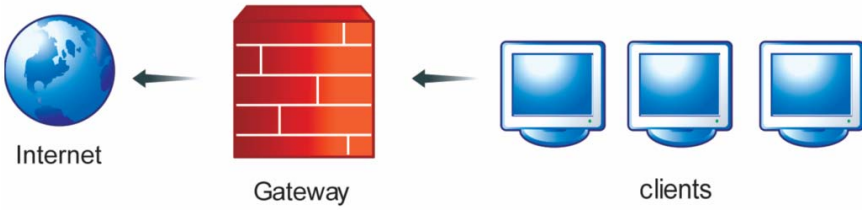
FIGURE 2-5. Installation Topology for FTP without a Proxy Server

HTTP

In standalone mode, ISVW is directly behind the gateway device, either serving as the HTTP proxy server or receiving HTTP traffic from an existing server.

In dependent mode, ISVW is deployed between the client machines and the HTTP proxy server.

Before installing ISVW (without proxy)



After installing ISVW (without proxy) Standalone Mode

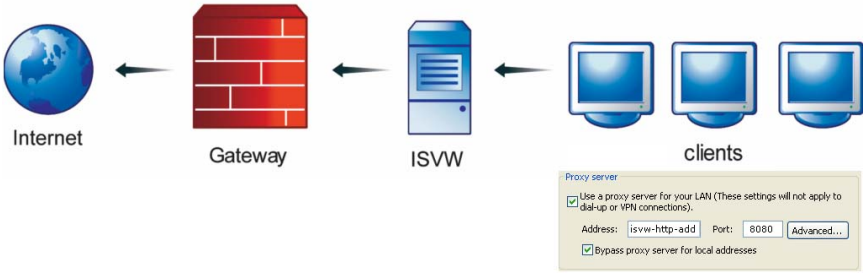
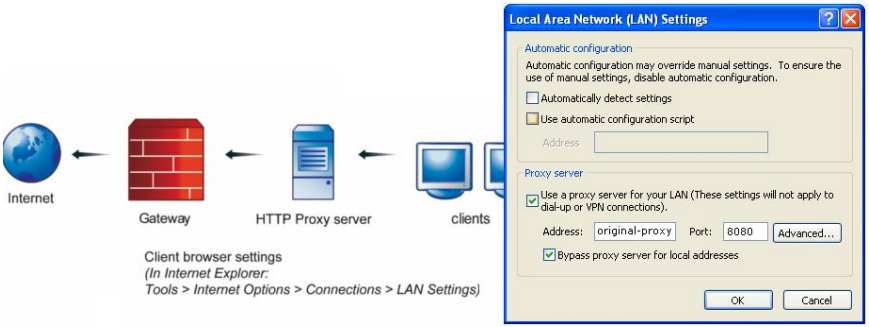


FIGURE 2-6. Installation Topology for HTTP without a Proxy Server (Standalone Mode)

After installing ISVW, browser clients should change their proxy settings to point at ISVW.

Before installing ISVW (with proxy)



After installing ISVW (with proxy)

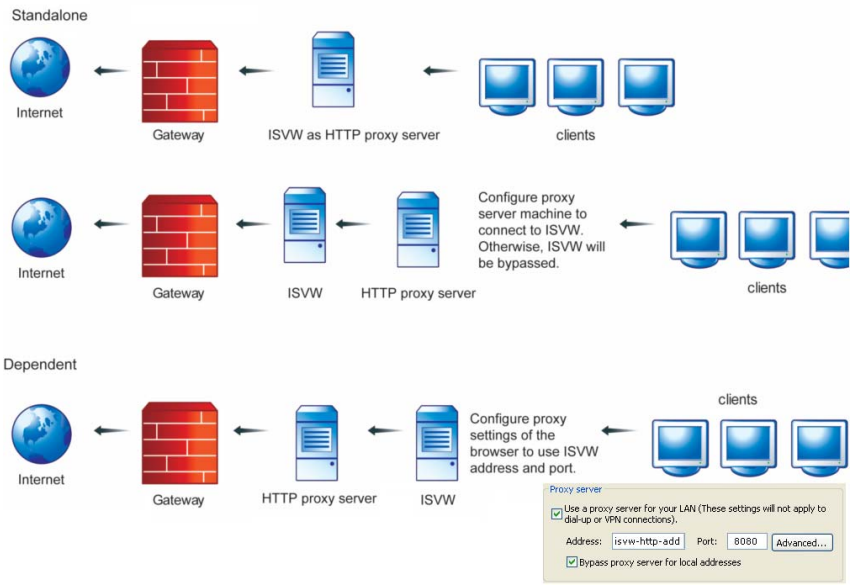
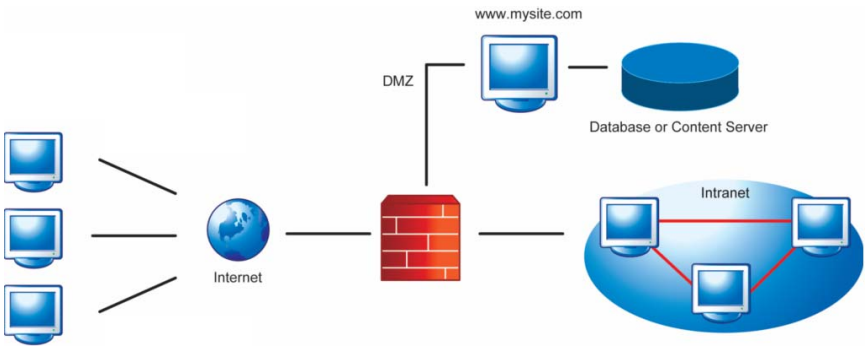


FIGURE 2-7. Installation Topology for HTTP with a Proxy Server (Dependent Mode)

HTTP Reverse Proxy

In reverse proxy deployment, a content server is made available to internal and external customers using a firewall to prevent direct, unmonitored access to the content server. In this topology, ISVW scans HTTP traffic from the content server to the clients within and outside the network.

Before installing ISVW



After installing ISVW

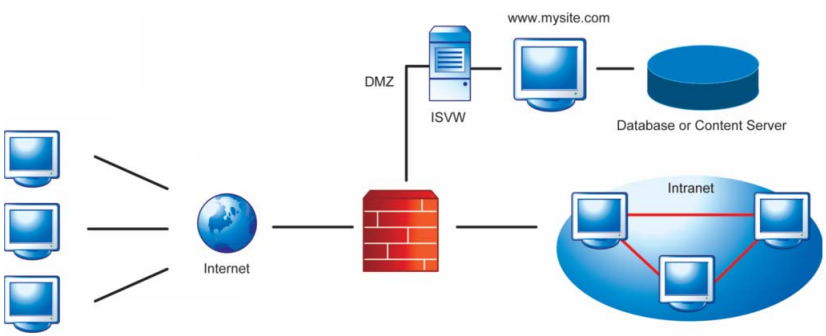


FIGURE 2-8. Installation Topology for HTTP with ISVW as a Reverse Proxy

Before Installing InterScan VirusWall

1. On the machine where you will install ISVW, remove any real-time scanning products such as anti-virus and anti-spyware products. If you do not want to remove the product, add the following items to the product's scanning exclusion list:
   - ISVW destination path
   - Quarantine path for the SMTP, POP3, HTTP, and FTP protocols
   - Windows™ Temp folder
2. Log on with administrator privileges on the machine.
3. Ensure the following default port numbers used by ISVW are not in use:
   - SMTP: 25
   - POP3: 110
   - HTTP: 8080
   - FTP: 21

   Note: For the Web management console, the default port numbers are 9240 for HTTP and 9241 for HTTPS. You can, however, specify different port numbers during installation.

4. If you are installing ISVW for the first time and installing SMTP, prepare a list of domains that SMTP VirusWall will recognize as valid domains.

   SMTP will only deliver inbound emails addressed to these domains.
5. If you are upgrading from ISVW 3.55 with eManager 3.52 to ISVW 7.0, enable the following before installation to enable content filter settings after the upgrade:
   - InterScan eManager Content Management service in ISVW 3.55
   - **Attachment Filter > Enable attachment filter** option in eManager 3.52

See *Appendix A* for a checklist of relevant system information useful for installing ISVW.

Chapter 3

Installing InterScan VirusWall

InterScan VirusWall (ISVW) can be installed and configured to support any number of physical network setups. ISVW offers simplified installation and configuration for easy setup. ISVW requires minimal day-to-day maintenance, which is especially useful for customers who have limited time or IT resources, yet still require full-time virus and spam prevention services.

The ISVW 7.0 Setup program has a pre-flight check function that verifies compatibility with respect to system requirements, disk space requirements, service packs or patches required, and ports that need to be available. With the pre-flight check function, ISVW is able to co-exist with other products in an evaluation environment.

This chapter provides step-by-step instructions for installing ISVW 7.0. It also provides instructions for migrating from ISVW 3.55, 5.0, 6.0, 6.01, or 6.02 to ISVW 7.0.

Installation Scenarios

The ISVW setup consists of launching the setup file and then following the InstallWizard instructions.

The following are the possible installation scenarios:

- *Installing InterScan VirusWall 7.0 as a Fresh Installation* starting on page 3-2

  Use this procedure if you are installing ISVW for the first time.

- *Installing InterScan VirusWall 7.0 on a Computer Where an Earlier Version of ISVW is Installed*

  Use this procedure if you are installing ISVW 7.0 on a computer that has ISVW 3.55, ISVW 5.0, or ISVW 6.0, 6.01, or 6.02 installed already, and you want to migrate the configuration settings to version 7.0.

- *Installing InterScan VirusWall 7.0 on a New Computer and Migrating the Configuration Settings of an Earlier Version of ISVW*

  Use this procedure if you are installing ISVW 7.0 on a new computer and want to migrate the configuration settings from a computer that has an earlier version of ISVW installed on it. You can use a migration tool or the command line to migrate version 5.0 or 6.0, 6.01, or 6.02 settings and import them during ISVW 7.0 installation.

- *Command Line Migration from Earlier Versions of ISVW*

  Use this procedure if you are installing ISVW 7.0 on a new computer and want to use the command line to migrate the configuration settings from a computer that has an earlier version of ISVW installed on it. You will use a migration tool to migrate the earlier version settings and import them during ISVW 7.0 installation.

Installing InterScan VirusWall 7.0 as a Fresh Installation

For the URL blocking and filtering Global Policy during a fresh installation, 12 categories are selected by default for the Internet Security group (see *Managing the Global URL Blocking and Filtering Policy* on page 5-20).

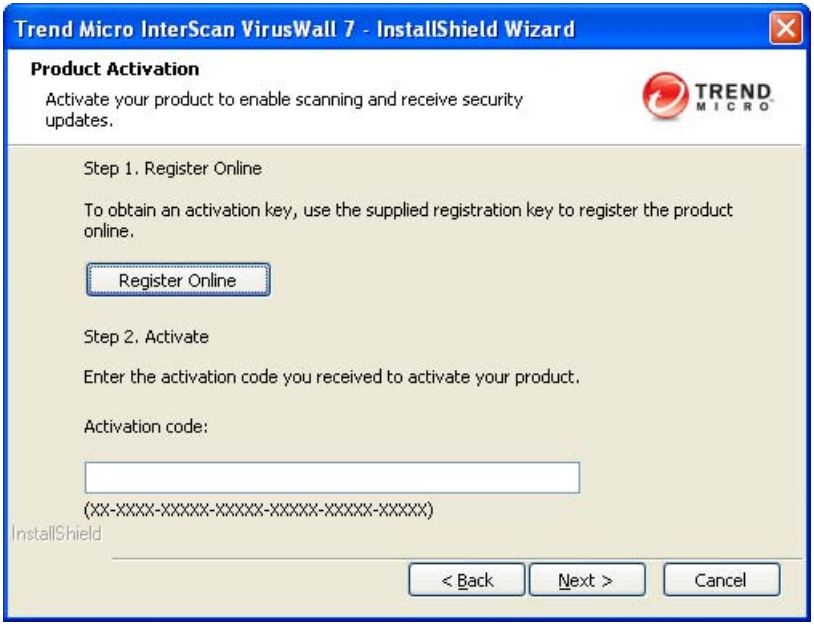
To perform a fresh ISVW installation:

1. Double click `setup.exe` to start the installation process.
2. When the Welcome window appears, click **Next**.
3. In the License Agreement window, read the entire license agreement and then select **I accept the terms of the license agreement** to proceed with the installation.

   You can scroll through the entire agreement online or print it. If you select **I do not accept the terms of the license agreement**, the installation process will terminate.
4. In the Setup Type window, select **Fresh Installation** and then click **Next**.
5. In the Product Activation window shown in *Figure 3-1*, do one of the following:

- If you have already registered and obtained a product activation code, then skip Step 1 on this screen and enter the product activation code in the **Activation Code** text box and click **Next**.
- If you have not registered and wish to do so now, click **Register Online**. The Trend Micro Online Registration screen appears in your browser. Register and obtain a product activation code, then enter the product activation code that you received in the **Activation Code** text box and click **Next**.
- Click **Next** without entering an activation code.

FIGURE 3-1. Product Activation Screen



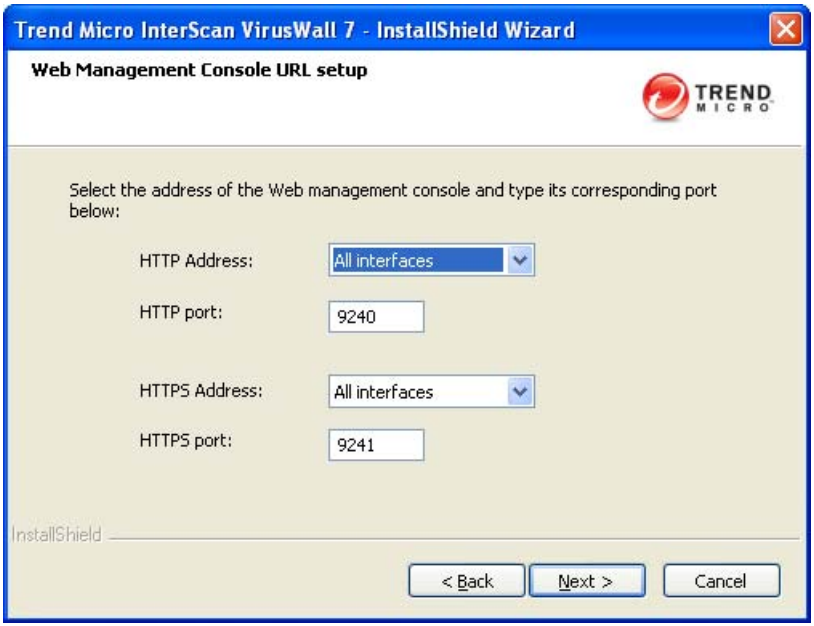
If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

The Choose Destination Folder window appears, indicating the directory path where ISVW 7.0 will be installed.

6. If you wish to change the installation path, click **Browse** and specify a different location.
7. When you have either accepted the default path or chosen a new destination, click **Next**.
8. In the Web Management Console URL Setup window, specify where the Web management console will bind.

   Default settings are shown in *Figure 3-2*.

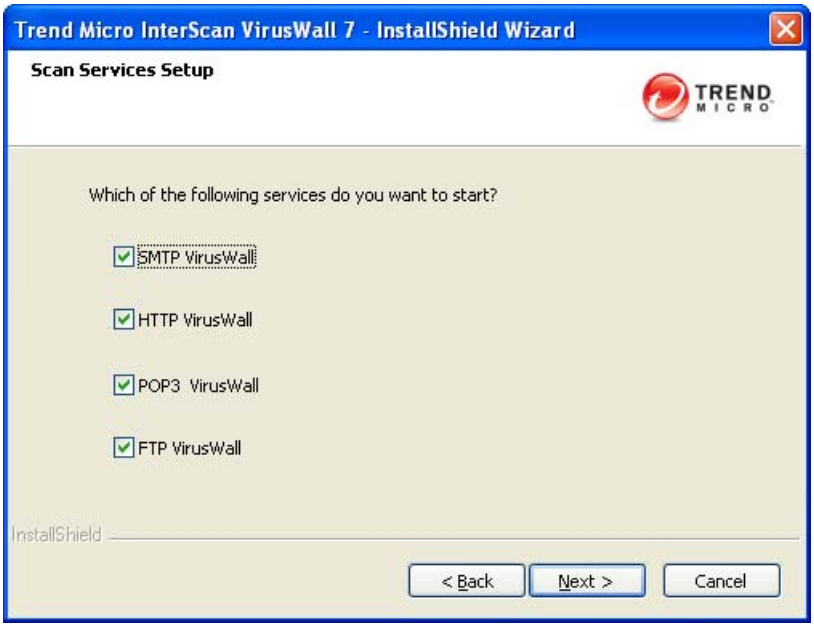
FIGURE 3-2. Web Management Console URL Setup Screen



9. Click **Next**.
10. In the Administrator Password Setup window, enter a 4- to 32-character password, confirm it, and then click **Next**.
11. In the Scan Services Setup window, select the ISVW services that you want to start after the installation completes.

By default, all services are selected (see *Figure 3-3*). When you have made your selections, click **Next**.

FIGURE 3-3. Scan Services Setup Screen



12. In the Allowed Relay Destinations Setup window, specify the domains that will accept inbound mail.

    ISVW 7.0 will only accept inbound mails addressed to these domains.

13. In the HTTP Web Reputation Feedback window, indicate whether you want to participate in the anonymous feedback of infected URLs and then click **Next**.
14. In the World Virus Tracking Setup window, indicate whether you want to participate in the World Virus Tracking program and then click **Next**.
15. In the Setup Confirmation window, view the current settings and then click **Next**.

    Click **Back** to go to previous screens to change any settings.

    The Setup Status screen appears showing the progress of the software installation.

16. In the Setup Complete screen, select whether you want to display the `readme.txt` file or start the Web management console and then click **Finish**.
    - If you chose to display the `readme.txt` file, it will be displayed in a new window.
    - If you chose to start the Web management console, a Web browser window will open automatically and display the logon page for ISVW 7.0.

Installing InterScan VirusWall 7.0 on a Computer Where an Earlier Version of ISVW is Installed

The setup program enables you to install ISVW 7.0 on a computer where an earlier versions of ISVW is already installed. The following are the supported versions of ISVW:

- ISVW 3.55
- ISVW 5.0
- ISVW 6.0, 6.01, or 6.02

During the installation of ISVW 7.0 on a computer having any one of the these earlier versions of ISVW installed, you are able to migrate the configuration settings to ISVW 7.0 (see *Installing InterScan VirusWall 7.0 on a New Computer and Migrating the Configuration Settings of an Earlier Version of ISVW* on page 3-10).

If you choose to migrate the settings, Trend Micro recommends that you back up the file before proceeding with the installation. The ISVW 7.0 installation program will remove the earlier version of ISVW completely, but will not remove eManager from an ISVW 3.55 installation.

Note: If the ISVW 7.0 Setup program detects ISVW 6.0, 6.01, or 6.02 and they are the same language version, the Setup program will prompt you to confirm the build upgrade. If the ISVW 7.0 Setup program detects ISVW 6.0, 6.01, or 6.02 are different language versions, the Setup program will prompt you to uninstall the different language version and then proceed with the installation.

To install ISVW 7.0 on a computer where an earlier version of ISVW is installed:

1. Double-click `setup.exe` to start the installation process.
2. When the Welcome screen appears, click **Next**.

3. When the License Agreement screen appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation.

   You can scroll through the entire agreement online or print it. If you select **I do not accept the terms of the license agreement**, the installation process will terminate.

4. To migrate settings from an earlier version of ISVW, select **Migrate configuration settings from previous version on current computer** check box.

   If you choose to migrate the settings, Trend Micro recommends that you back up the file before proceeding with the installation. The ISVW 7.0 installation program will remove the earlier version of ISVW completely, but will not remove eManager from an ISVW 3.55 installation.

   If you do not want to create a report that lists all the settings that were migrated, clear the **Create migration report** check box.

5. Click **Next**.

   The Product Activation screen appears.

6. In the Product Activation screen, do one of the following:

   - If you have already registered and obtained a product activation code, then skip Step 1 on this screen and enter the product activation code in the **Activation Code** field and click **Next**.
   - If you have not already registered and wish to do so now, click **Register Online**. The Trend Micro Online Registration screen appears in your browser. Register and obtain a product activation code, then enter the product activation code that you received in the **Activation Code** field and click **Next**.
   - Click **Next** without entering an activation code.

     If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

   The Choose Destination Location screen appears, indicating the directory path where ISVW 7.0 will be installed.

7. To change the installation location, click **Browse** and specify an alternative location.

8. When you have either accepted the default path or chosen a new destination, click **Next**.

   The Web Management Console Configuration screen appears.
9. In the Web Management Console Configuration screen, specify where the Web management console will bind.
10. Click **Next**.

    The Administrator Account screen appears.
11. Enter a 4- to 32-character password, confirm it, and then click **Next.**

    The Scan Services Setup screen appears.
12. Select the ISVW services that you want to start after the installation has finished.

    By default, all services are selected to start. After you make your selections, click **Next**.

    The Allowed Relay Destinations Setup screen appears.
13. To block relayed emails, specify in the **Domains** field the domains that will accept inbound emails.
14. Click **Next**.

    The HTTP Web Reputation Feedback screen appears.
15. To help improve the Web Reputation database, select the check box to send anonymous information on infected URLs.
16. Click **Next**.

    The World Virus Tracking Setup screen appears.
17. Select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.

    The Setup Confirmation screen appears. The setup program moves the quarantined data to the `C:\Relocated_ISVW6_Quarantine_Folder` directory. You can either relocated or delete this data. After installation, update the quarantine settings (see Chapter 9, *Quarantines*).
18. Review the current settings.
    - If the settings are correct, click **Next**.

- If you need to modify the settings, click **Back** until the appropriate previous screen appears and modify the setting. Click **Next** until the Setup Confirmation screen reappears, then click **Next** again to proceed**.**

When you click **Next** on the Setup Confirmation screen, a message appears indicating that the earlier version of ISVW will be uninstalled.

- Click **Yes** to uninstall the earlier version of ISVW.
- Click **No** to exit Setup.

Note: The warning message may vary depending on which version of ISVW you are migrating from.

When the uninstallation completes, the Setup Status screen appears. The Setup Status screen continues to show the progress of the ISVW 7.0 installation.

19. On the Setup Complete screen, select whether you want to display the `readme.txt` file, start the Web management console, or display the migration report and then click **Finish**.

- If you chose to display the `readme.txt` file, it will be displayed in a new window.
- If you chose to start the Web management console, a Web browser window will open automatically and display the logon page for ISVW 7.0.
- If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in *Figure 3-4*.

Note: The contents of the Migration report may vary depending on which version of ISVW from which you are migrating.

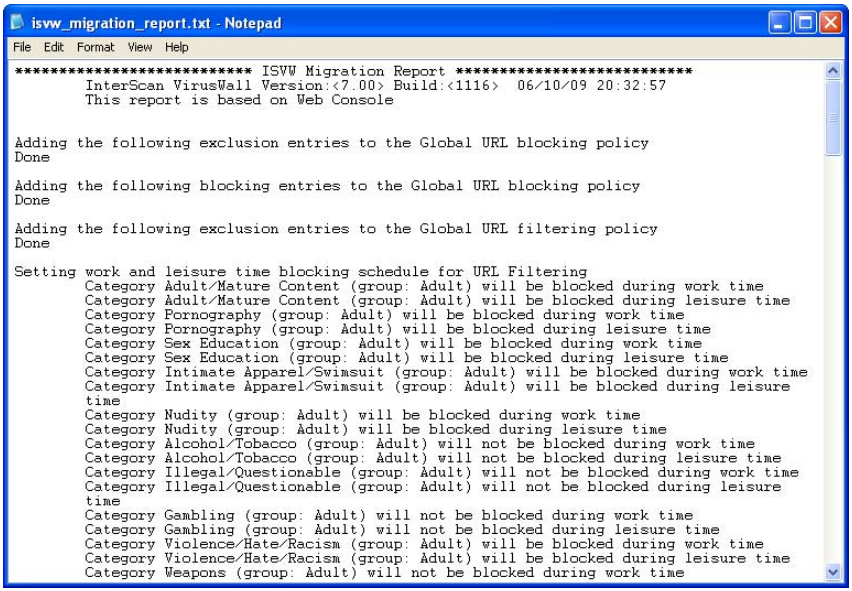


FIGURE 3-4. Sample ISVW 3.55 Migration Report

Note: If you decide to print the migration report after you have completed the installation process, navigate to its location at:

```
<ISVW_Installation_folder>\isvw_migration_report.txt
```

Installing InterScan VirusWall 7.0 on a New Computer and Migrating the Configuration Settings of an Earlier Version of ISVW

Once you install ISVW 7.0 on a new computer, the setup program enables you migrate the configuration settings from another computer that has an earlier version of ISVW installed on it. Migration is supported for the following versions of ISVW:

- ISVW 3.55
- ISVW 5.0

- ISVW 6.0, 6.01, or 6.02

ISVW 7.0 enables you to migrate quarantine files from ISVW 6.0, 6.01, and 6.02. This migration falls under one of two scenarios:

- If you did not change the default quarantine path, ISVW 7.0 will move the previous quarantine file to the root path of the default path. For example, if you installed ISVW at the location, `D:\ISVW` and the default setting of the quarantine file has not changed and all the quarantine files are at `D:\Relocated_ISVW6_Quarantine_Folder\xxx`, then ISVW 7.0 will move the quarantine file to `D:\Relocated_ISVW6_Quarantine_Folder\xxx`. Furthermore, the quarantine path used by ISVW 7.0 remains as it was for the original installation.
- If you changed the default quarantine path, ISVW 7.0 will not move the ISVW 6.x quarantine files to the new location. The new quarantine files that ISVW 7.0 generates will be stored in the same path with ISVW 6.x.

Note: When migrating settings from an earlier version of ISVW to ISVW 7.0, the installation program migrates the earlier version's selected URL categories for the URL filtering rules.

Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 3.55 Settings to that Computer

If you want to install ISVW 7.0 on a computer where it has not been installed before and you want to use the configuration settings from a computer where ISVW 3.55 is installed, you can export the settings to a file. That file will then be used during the installation process to import the saved settings to the computer where you are installing ISVW 7.0.

A migration tool that allows you to export the configuration settings to a file has been supplied as part of the ISVW 7.0 installation package. The migration tool allows you to export the ISVW 3.55 configuration settings and the eManager plug-in settings.

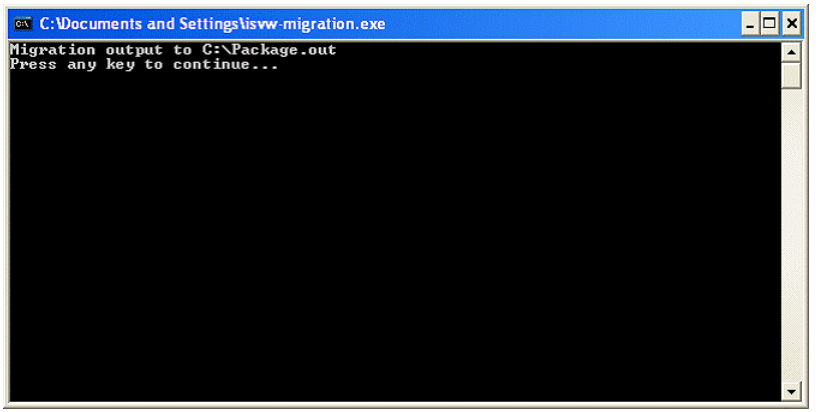
If ISVW 3.55 does not exist on the computer where you run the migration tool, ISVW issues a message and exits the installation setup.

To install ISVW 7.0 and migrate ISVW 3.55 configuration settings:

1. On the computer that contains the ISVW 3.55 installation, navigate to `<Installation package>\tools\isvw-migration.exe`.
2. Double click `isvw-migration.exe` to export the configuration settings.

   If ISVW 3.55 exists, the command window shown in *Figure 3-5* opens, listing the location of the configuration settings file that the migration tool has created. The default location and file name is `<system drive>:\Package.out`.

   FIGURE 3-5. Migration Tool Export Utility Screen Used in the ISVW 3.55 Migration



3. Press any key and the command window closes.
4. If you are unable to access this file through a network, copy `package.out` to a portable medium so you can access it on the computer where you will install ISVW 7.0.
5. On the computer where you wish to install ISVW 7.0, double-click `setup.exe` to start the installation process.
6. When the Welcome screen appears, click **Next**.
7. When the License Agreement screen appears, read the entire license agreement and then select **I accept the terms of the license agreement** to proceed with the installation.

You can scroll through the entire agreement online or print it. If you select **I do not accept the terms of the license agreement**, the installation process will terminate.

8. When the Setup Type window appears, select **Migrate configuration settings from previous version on remote computer** check box.

   If you do not want to create a report that lists all the settings that were migrated, clear the **Create migration report** check box.

9. Click **Next**.

   The Product Activation screen appears.

10. In the Product Activation screen, do one of the following:
    - If you have already registered and obtained a product activation code, then skip Step 1 on this screen and enter the product activation code in the **Activation Code** field and click **Next**.
    - If you have not already registered and wish to do so now, click **Register Online**. The Trend Micro Online Registration screen appears in your browser. Register and obtain a product activation code, then enter the product activation code that you received in the **Activation Code** field and click **Next**.
    - Click **Next** without entering an activation code.

      If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

    The Choose Destination Location screen appears, indicating the directory path where ISVW 7.0 will be installed.

11. To change the installation location, click **Browse** and specify an alternative location.

12. When you have either accepted the default path or chosen a new destination, click **Next**.

    The Web Management Console Configuration screen appears.

13. In the Web Management Console Configuration screen, specify where the Web management console will bind.

14. Click **Next**.

    The Administrator Account screen appears.

15. Enter a 4- to 32-character password, confirm it, and then click **Next.**

    The Scan Services Setup screen appears.

16. Select the ISVW services that you want to start after the installation has finished.

    By default, all services are selected to start. After you make your selections, click **Next**.

    The Allowed Relay Destinations Setup screen appears.

17. To block relayed emails, specify in the **Domains** field the domains that will accept inbound emails.

18. Click **Next**.

    The HTTP Web Reputation Feedback screen appears.

19. To help improve the Web Reputation database, select the check box to send anonymous information on infected URLs.

20. Click **Next**.

    The World Virus Tracking Setup screen appears.

21. Select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.

    The Setup Confirmation screen appears.

22. Review the current settings.

    - If the settings are correct, click **Next**.
    - If you need to modify the settings, click **Back** until the appropriate previous screen appears and modify the setting. Click **Next** until the Setup Confirmation screen reappears, then click **Next** again to proceed**.**

    The Setup Status screen appears. The Setup Status screen continues to show the progress of the ISVW 7.0 installation.

23. On the Setup Complete screen, select whether you want to display the `readme.txt` file, start the Web management console, or display the migration report and then click **Finish**.

    - If you chose to display the `readme.txt` file, it will be displayed in a new window.
    - If you chose to start the Web management console, a Web browser window will open automatically and display the logon page for ISVW 7.0.

- If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in *Figure 3-4*.

Note: If you decide to print the migration report after you have completed the installation process, navigate to its location at:

```
<ISVW_Installation_folder>\isvw_migration_report.txt
```

Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 5.0 Settings to that Computer

If you want to install ISVW 7.0 on a computer where it has not been installed before and you want to use the configuration settings from a computer where ISVW 5.0 is installed, you can export the settings to a file. That file will then be used during the installation process to import the saved settings to the computer where you are installing ISVW 7.0.

A migration tool that allows you export the configuration settings to a file has been supplied as part of the ISVW 7.0 installation package. The migration tool allows you to export the ISVW 5.0 configuration settings.

If ISVW 5.0 does not exist on the computer where you run the migration tool, ISVW issues a message and exits the installation setup.

To install ISVW 7.0 and migrate ISVW 5.0 configuration settings:

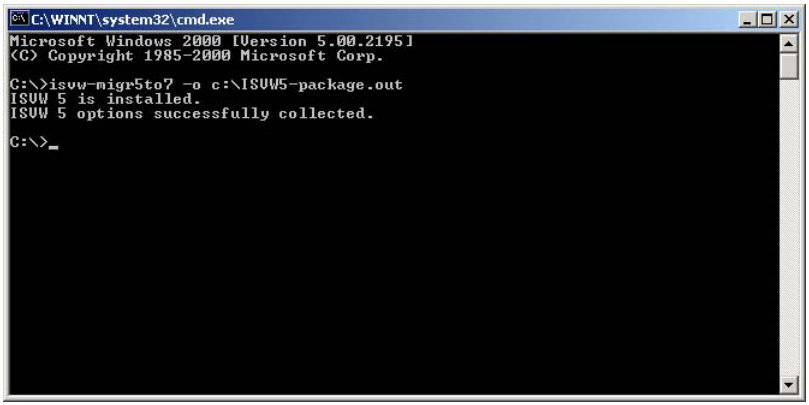
1. Find the tool named `isvw-migr5to7.exe` that is located in the ISVW 7.0 installation package directory `<Installation package>\tools` and copy it to the computer where ISVW 5.0 is installed.
2. From the command line, type the following:

   ```
   isvw-migr5to7 -o [Migration_Configuration_File_Name]
   Example: isvw-migr5to7 -o c:\ISVW5-package.out
   ```

   See *Figure 3-6*.

   Note: The ISVW 7.0 migration tool supports both absolute and relative path names.

FIGURE 3-6. Migration Tool Export Utility Screen Used in the ISVW 5.0 Migration



3. If you are unable to access this file through a network, copy the file `Migration_Configuration_File_Name` to a portable medium so you can access it on the computer where you will install ISVW 7.0.
4. On the computer where you wish to install ISVW 7.0, double click `setup.exe` to start the installation process.
5. When the Welcome screen appears, click **Next**.
6. When the License Agreement screen appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation.

   You can scroll through the entire agreement online or print it. If you select **I do not accept the terms of the license agreement**, the installation process will terminate.
7. When the Setup Type window appears, select **Migrate configuration settings from previous version on remote computer** check box.

   If you do not want to create a report that lists all the settings that were migrated, clear the **Create migration report** check box.
8. Click **Next**.

   The Product Activation screen appears.

9. In the Product Activation screen, do one of the following:
   - If you have already registered and obtained a product activation code, then skip Step 1 on this screen and enter the product activation code in the **Activation Code** field and click **Next**.
   - If you have not already registered and wish to do so now, click **Register Online**. The Trend Micro Online Registration screen appears in your browser. Register and obtain a product activation code, then enter the product activation code that you received in the **Activation Code** field and click **Next**.
   - Click **Next** without entering an activation code.

     If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

   The Choose Destination Location screen appears, indicating the directory path where ISVW 7.0 will be installed.
10. To change the installation location, click **Browse** and specify an alternative location.
11. When you have either accepted the default path or chosen a new destination, click **Next**.

    The Web Management Console Configuration screen appears.
12. In the Web Management Console Configuration screen, specify where the Web management console will bind.
13. Click **Next**.

    The Administrator Account screen appears.
14. Enter a 4- to 32-character password, confirm it, and then click **Next.**

    The Scan Services Setup screen appears.
15. Select the ISVW services that you want to start after the installation has finished.

    By default, all services are selected to start. After you make your selections, click **Next**.

    The Allowed Relay Destinations Setup screen appears.
16. To block relayed emails, specify in the **Domains** field the domains that will accept inbound emails.

17. Click **Next**.

    The HTTP Web Reputation Feedback screen appears.

18. To help improve the Web Reputation database, select the check box to send anonymous information on infected URLs.

19. Click **Next**.

    The World Virus Tracking Setup screen appears.

20. Select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.

    The Setup Confirmation screen appears.

21. Review the current settings.
    - If the settings are correct, click **Next**.
    - If you need to modify the settings, click **Back** until the appropriate previous screen appears and modify the setting. Click **Next** until the Setup Confirmation screen reappears, then click **Next** again to proceed**.**

    The Setup Status screen appears. The Setup Status screen continues to show the progress of the ISVW 7.0 installation.

22. On the Setup Complete screen, select whether you want to display the `readme.txt` file, start the Web management console, or display the migration report and then click **Finish**.
    - If you chose to display the `readme.txt` file, it will be displayed in a new window.
    - If you chose to start the Web management console, a Web browser window will open automatically and display the logon page for ISVW 7.0.
    - If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in *Figure 3-4*.

Note: If you decide to print the migration report after you have completed the installation process, navigate to its location at:

```
<ISVW_Installation_folder>\isvw_migration_report.txt
```

Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 6.0, 6.01, or 6.02 Settings to that Computer

If you want to install ISVW 7.0 on a computer where it has not been installed before and you want to use the configuration settings from a computer where ISVW 6.0, 6.01, or 6.02 is installed, you can export the settings to a file. That file will then be used during the installation process to import the saved settings to the computer where you are installing ISVW 7.0.

A migration tool that allows you export the configuration settings to a file has been supplied as part of the ISVW 7.0 installation package. The migration tool allows you to export the ISVW 6.0, 6.01, or 6.02 configuration settings.

If ISVW 6.0, 6.01, or 6.02 does not exist on the computer where you run the migration tool, ISVW issues a message and exits the installation setup.

To install ISVW 7.0 and migrate ISVW 6.0, 6.01, or 6.02 configuration settings:

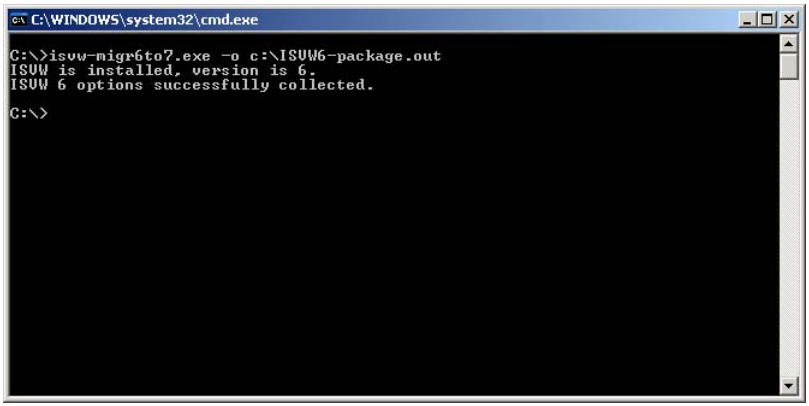
1. Find the tool named `isvw-migr6to7.exe` that is located in the ISVW 7.0 installation package directory `<Installation package>\tools` and copy it to the computer where ISVW 6.0x is installed.
2. From the command line type the following:

   ```
   isvw-migr6to7 -o [Migration_Configuration_File_Name]
   Example: isvw-migr6to7 -o c:\ISVW6-package.out
   ```

   See *Figure 3-7*.

Note: The ISVW 7.0 migration tool supports both absolute and relative path names.

FIGURE 3-7. Migration Tool Export Utility Screen Used in the ISVW 6.0x Migration



3. If you are unable to access this file through a network, copy the file `Migration_Configuration_File_Name` to a portable medium so you can access it on the computer where you will install ISVW 7.0.
4. On the computer where you wish to install ISVW 7.0, double-click `setup.exe` to start the installation process.
5. When the Welcome screen appears, click **Next**.
6. When the License Agreement screen appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation.

   You can scroll through the entire agreement online or print it. If you select **I do not accept the terms of the license agreement**, the installation process will terminate.
7. When the Setup Type window appears, select **Migrate configuration settings from previous version on remote computer** check box.

   If you do not want to create a report that lists all the settings that were migrated, clear the **Create migration report** check box.

8. Click **Next**.

   The Product Activation screen appears.

9. In the Product Activation screen, do one of the following:

   - If you have already registered and obtained a product activation code, then skip Step 1 on this screen and enter the product activation code in the **Activation Code** field and click **Next**.
   - If you have not already registered and wish to do so now, click **Register Online**. The Trend Micro Online Registration screen appears in your browser. Register and obtain a product activation code, then enter the product activation code that you received in the **Activation Code** field and click **Next**.
   - Click **Next** without entering an activation code.

     If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

   The Choose Destination Location screen appears, indicating the directory path where ISVW 7.0 will be installed.

10. To change the installation location, click **Browse** and specify an alternative location.

11. When you have either accepted the default path or chosen a new destination, click **Next**.

    The Web Management Console Configuration screen appears.

12. In the Web Management Console Configuration screen, specify where the Web management console will bind.

13. Click **Next**.

    The Administrator Account screen appears.

14. Enter a 4- to 32-character password, confirm it, and then click **Next.**

    The Scan Services Setup screen appears.

15. Select the ISVW services that you want to start after the installation has finished.

    By default, all services are selected to start. After you make your selections, click **Next**.

    The Allowed Relay Destinations Setup screen appears.

16. To block relayed emails, specify in the **Domains** field the domains that will accept inbound emails.
17. Click **Next**.

    The HTTP Web Reputation Feedback screen appears.
18. To help improve the Web Reputation database, select the check box to send anonymous information on infected URLs.
19. Click **Next**.

    The World Virus Tracking Setup screen appears.
20. Select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.

    The Setup Confirmation screen appears.
21. Review the current settings.
    - If the settings are correct, click **Next**.
    - If you need to modify the settings, click **Back** until the appropriate previous screen appears and modify the setting. Click **Next** until the Setup Confirmation screen reappears, then click **Next** again to proceed**.**

    The Setup Status screen appears. The Setup Status screen continues to show the progress of the ISVW 7.0 installation.
22. On the Setup Complete screen, select whether you want to display the `readme.txt` file, start the Web management console, or display the migration report and then click **Finish**.
    - If you chose to display the `readme.txt` file, it will be displayed in a new window.
    - If you chose to start the Web management console, a Web browser window will open automatically and display the logon page for ISVW 7.0.
    - If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in *Figure 3-4*.

Note: If you decide to print the migration report after you have completed the installation process, navigate to its location at:

```
<ISVW_Installation_folder>\isvw_migration_report.txt
```

Command Line Migration from Earlier Versions of ISVW

Once you install ISVW 7.0 on a new computer, you can use the command line to migrate the configuration settings from another computer that has an earlier version of ISVW installed on it. Migration is supported for the following versions of ISVW:

- ISVW 5.0
- ISVW 6.0, 6.01, or 6.02

Command Line Migration from ISVW 5.0 to ISVW 7.0

To migrate ISVW 5.0 configuration settings to a computer with ISVW 7.0 installed:

1. Find the tool named `isvw-migr5to7.exe` that is located in the ISVW 7.0 installation package directory `<Installation package>\tools` and copy it to the computer where ISVW 5.0 is installed.
2. From the command line type the following:

   ```
   isvw-migr5to7 -o [Migration_Configuration_File_Name]
   Example: isvw-migr5to7 -o c:\ISVW5-package.out
   ```

   See *Figure 3-6*.

Note: The ISVW 7.0 migration tool supports both absolute and relative path names.

3. If you are unable to access this file through a network, copy the file `Migration_Configuration_File_Name` to a portable medium so you can access it on the computer where you will install ISVW 7.0.
4. On the computer where ISVW 7.0 has been installed, open the command window.
5. Navigate to `<ISVW 7.0 Installation path>\Others`, and in the command window run the migration tool with the command:

```
isvw-migr5to7 -p [Migration_Configuration_File_Name] -i
[ISVW 7.0 Installation path]
Example: isvw-migr5to7 -p c:\ISVW5-package.out -i
"c:\Program Files\Trend Micro\InterScan VirusWall 7".
```

If the migration was successful, ISVW will display a migration successful message. The program will also create a migration report in the ISVW 7.0 installation directory.

6. Restart the ISVW service.

Command Line Migration from ISVW 6.0, 6.01, 6.02 to ISVW 7.0

To migrate ISVW 6.0x configuration settings to a computer with ISVW 7.0 installed:

1. Find the tool named `isvw-migr6to7.exe` that is located in the ISVW 7.0 installation package directory `<Installation package>\tools` and copy it to the computer where ISVW 6.0x is installed.
2. From the command line type the following:

   ```
   isvw-migr6to7 -o [Migration_Configuration_File_Name]
   Example: isvw-migr6to7 -o c:\ISVW6-package.out
   ```

   See *Figure 3-7*.

Note: The ISVW 7.0 migration tool supports both absolute and relative path names.

---

3. If you are unable to access this file through a network, copy the file `Migration_Configuration_File_Name` to a portable medium so you can access it on the computer where you will install ISVW 7.0.
4. On the computer where ISVW 7.0 has been installed, open the command window.
5. Navigate to `<ISVW 7.0 Installation path>\Others`, and in the command window run the migration tool with the command:

   ```
   isvw-migr6to7 -p [Migration_Configuration_File_Name] -i
   [ISVW 7.0 Installation path]
   Example: isvw-migr6to7 -p c:\ISVW5-package.out -i
   "c:\Program Files\Trend Micro\InterScan VirusWall 7".
   ```

If the migration was successful, ISVW will display a migration successful message. The program will also create a migration report in the ISVW 7.0 installation directory.

6. Restart the ISVW service.

After Installation

If you have registered and activated ISVW 7.0, you can do the following after you have completed installation:

- Adjust the default configuration of the product to meet the needs of your organization, or
- Begin virus scanning, spam detection, and content filtering immediately, using the default settings you chose during installation

Immediately after installing, you should also:

- Update the pattern files and scan engine
- Confirm that virus scanning is enabled
- Customize the notification messages
- Configure the alerts
- Set up an update schedule for the virus pattern file, scan engine, and anti-spam rules and engine

Depending on your installation, you may also need to perform the following tasks:

- Configure server to work with antivirus software installed on the same computer.

  If your ISVW server has an antivirus product installed, configure it to NOT scan the following folders:

  - ISVW 7.0 Program Folder after installation
  - Customized quarantine directory if you changed the default quarantine directory
  - Windows Temp folder

- Configure the proxy server to disable any cache mechanism or file size restrictions when accessing ISVW 7.0 pattern updates.If you use the proxy server to access the Internet for pattern updates, and the proxy server uses a cache mechanism to download large files, you will need to disable the cache mechanism or any file size restrictions when you want to download pattern updates. The ISVW 7.0 virus patterns and URL filtering database can be rather large files.

  This configuration applies when ISVW 7.0 goes through any mid-ware (FireWall or SOCKS/Proxy server) to connect to the URL and download pattern updates. To access pattern updates, go to the following URLs:

  `http://isvw602-av.activeupdate.trendmicro.com`

  `http://isvw602-as.activeupdate.trendmicro.com`

- Avoid listening port conflicts if ISVW 7.0 coexists with other services.

  ISVW 7.0 will use following default ports for listening ports:

  - SMTP: 25
  - HTTP: 8080
  - FTP: 21
  - POP3: 110

  Other services in the same servers may already be using these ports.

  On Windows SBS 2003 Standard/Enterprise editions, the following ports may be used by system itself:

  - 25: SMTP port, which may be used by Exchange server
  - 8080: HTTP proxy port, which may be used by ISA HTTP proxy
  - 110: POP3 port, which may be used by Exchange server
  - 21: FTP port, which may be used by IIS.

  IIS always ships with Windows server systems like 2000/2003/SBS.

  Exchange server is a base component of SBS.

  ISA server is a component of SBS enterprise edition.

  Trend Micro highly recommends that you use the ISVW 7.0 Web console to change the listening ports for related protocols if other components on the same servers are using the default ports.

- Anti-relay configurations if you use SMTP VirusWall after installation

ISVW 7.0 can act as a mail relay server. If the server accepts inbound mail for any domain, mail can be relayed, which can increase the amount of spam. To help secure the server against open-relay abuse, block relayed messages by accepting inbound mail addressed only to specific domains.

You can specify the correct setting from the Web console:

a. On the left side menu, select **SMTP > Configuration**.

b. Under Advanced Configuration, select **Block relayed messages by accepting inbound mail addressed only to the following domains:**

c. Type the domain names that can accept mail; separate each domain with a semicolon (;).

d. Click **Save**.

Opening the Web Console

After installation, ISVW automatically starts the basic services and the services you selected to start during installation. Although ISVW is configured to run on a robust set of default values, you should open the ISVW Web console and confirm the settings.

The following are the supported browsers:

- Internet Explorer 6.0 and above
- Firefox 2.0 and 3.0

1. Open a Web browser, then enter the ISVW URL followed by the number that you set during install (default value: `HTTP:9240`, `HTTPS:9241`).

```
http://IP address:port number
https://IP address:port number
```

The URL is determined by the IP address and port number that you bound to the Web management console during installation.

2. The ISVW console is password-protected.

Starting and Stopping InterScan VirusWall

ISVW has four services: SMTP VirusWall, POP3 VirusWall, FTP VirusWall and HTTP VirusWall. By default, all ISVW services that you selected during installation are automatically started following installation. Each VirusWall can also be individually controlled, however, by enabling or disabling real-time scanning for a given service. If you want to start a service that was not selected to start during installation or stop a service that was selected, enable or disable the service manually from the Summary page of the Web management console.

Restarting all services:

1. From the Control Panel, click the **Administrative Tools** icon to open the Administrative Tools screen.
2. Click the **Services** icon to open the Services window.
3. Navigate to "TrendMicro InterScan VirusWall" and click **Restart**.

   ISVW is typically set to **Automatic Startup**.

Testing InterScan VirusWall

After installation, test your ISVW installation to become familiar with the configuration and see how the program works.

The European Institute of Computer Antivirus Research (EICAR) and antivirus vendors have developed a test file that can be used to check your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose signature has been included in the Trend Micro virus pattern file. You can download the file from Trend Micro at:

`http://www.trendmicro.com/vinfo/testfiles/`

Once on your computer, you can use the test virus in email to test SMTP scanning, POP3 scanning, and to check FTP and HTTP file transfers.

Removing InterScan VirusWall

To remove the software from your computer:

1. Click **Start > Settings > Control Panel**.
2. On the Control Panel, click **Add/Remove Programs**.
3. On the Add/Remove Programs screen, select **Trend Micro InterScan VirusWall 7**.
4. Click **Change/Remove**.

   The Confirm Uninstall dialog box displays.
5. Click **Yes** to completely remove the application and all of its features, or **Cancel** to discontinue the uninstall process.

Chapter 4

Configuring SMTP Services

InterScan VirusWall (ISVW) allows you to monitor incoming and outgoing SMTP mail traffic. You can enable or disable scanning of SMTP traffic during the installation process or at any time thereafter through the Summary page of the ISVW Web console.

Available SMTP services include:

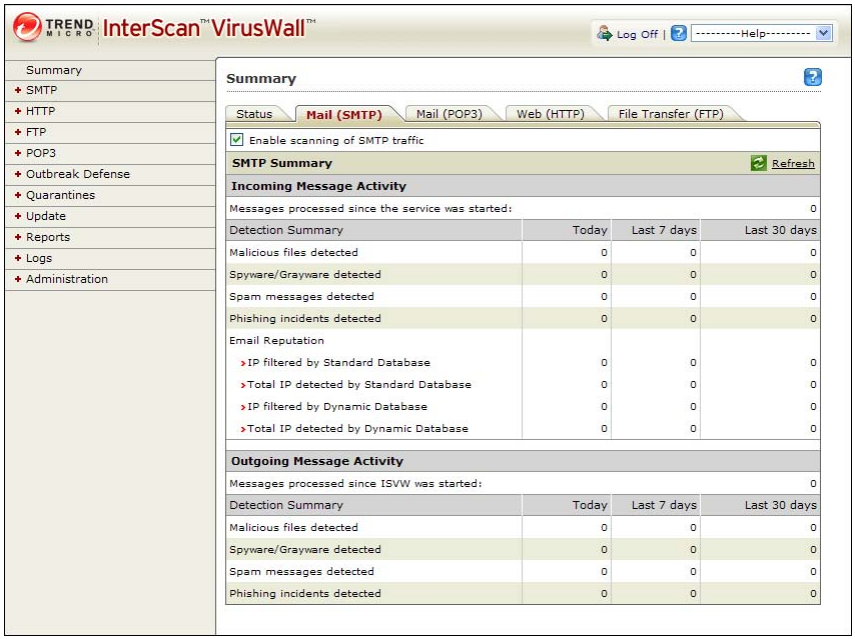
- Scanning for viruses and other types of malware
- IntelliTrap scanning of compressed executable files that could contain potentially malicious code
- Phishing site detection
- Spam detection
- Spyware and other grayware detection
- Content filtering
- Size filtering of messages and attachments
- Configuration of SMTP server port and delivery options for incoming and outgoing mail
- SMTP Transaction Logging

The Mail (SMTP) tab on the ISVW Summary screen provides statistics concerning the number of viruses, spyware, spam messages, and phishing messages that ISVW SMTP scanning detected in incoming and outgoing email communication.

Enabling or Disabling SMTP Services

To enable or disable SMTP service, select or clear the **Enable scanning of SMTP traffic** check box on the Mail (SMTP) tab of the Summary page (see *Figure 4-1*).

FIGURE 4-1. Summary screen (Mail (SMTP)) tab



Configuring SMTP Virus Scan Settings

ISVW offers the administrator flexibility in configuring how the SMTP service behaves. For example, you can specify the following:

- Attachment types to scan
- Individuals to notify when ISVW detects a virus
- Action that ISVW takes upon detection—clean, delete, quarantine, or pass

SMTP Virus Scanning Features

ISVW SMTP virus scanning includes the following features:

- Real-time scanning of incoming and outgoing SMTP email traffic
- Automatic, customizable virus notifications
- Option to clean, delete, move (quarantine), pass, or block infected files
- Size filtering of messages and attachments
- File name checking to protect against "email security flaws"
- Option to delete infected messages
- Ability to insert customized taglines in messages

Enabling SMTP Virus Scanning

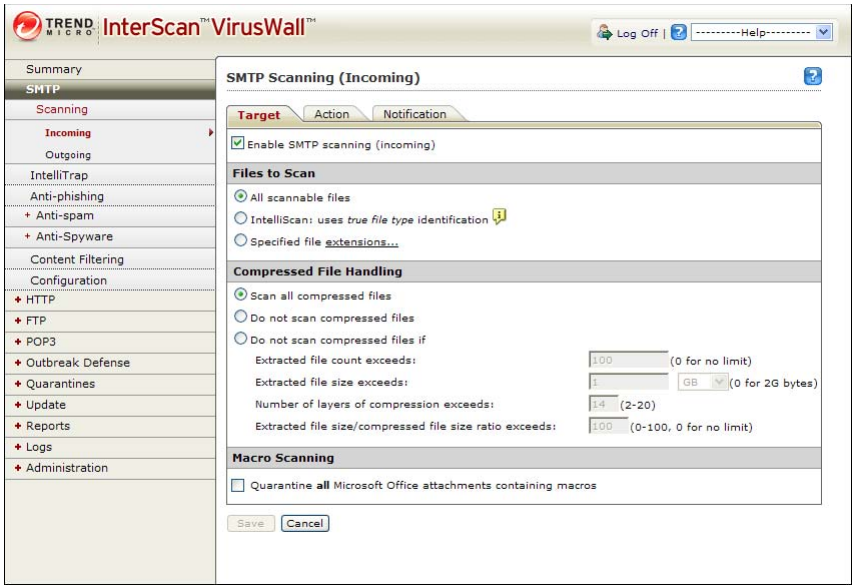
To enable SMTP virus scanning:

1. On the left side menu, select SMTP > Scanning > Incoming (or Outgoing).
2. Click the Target tab.
3. Select the **Enable SMTP scanning incoming (or outgoing)** check box.
4. Click **Save**.

Specifying the File Types to Scan

ISVW can check all or specified attachment types for viruses, including the individual files within compressed volumes. *Figure 4-2* shows the settings that you can specify when scanning file attachments.

FIGURE 4-2. SMTP Virus Scanning Target Tab



To select the file types to scan:

1. On the left side menu, select SMTP > Scanning > Incoming (or Outgoing) and click the Target tab.
2. Under "Files to Scan", select your preferred option:
   a. To scan all attachments, regardless of file type, select **All scannable files**. This is the most secure setting.
   b. To allow the product to intelligently identify the attachments to scan, select **IntelliScan: uses "true file type" identification**.

      This option passes some file types, which results in higher performance, but is less secure than when scanning all attachments.
   c. To scan only selected attachment types, select **Specified file extensions**. ISVW scans only those file types that are specified, explicitly, in the **Additional Extensions** text box.

By default, ISVW scans files with the following file name extensions:

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

Tip: Use the **Specified file extensions** option to modify the default scan list.

3. Click **Save**.

Note: Virus scanning settings apply to all types of SMTP scanning for malicious files, including virus/malware, IntelliTrap, and spyware scanning.

Configuring processing of compressed files

To specify how ISVW processes compressed files during SMTP scanning:

1. On the left side menu, select **SMTP > Scanning > Incoming (or Outgoing)** and click the **Target** tab.
2. Under **Compressed File Handling**, select your preferred option:
   a. To scan all compressed attachments, select **Scan all compressed files**. This is the most secure setting.
   b. To skip all compressed attachments, select **Do not scan compressed files**. ISVW will not scan any compressed attachments.
   c. To scan compressed attachments based on the number of files, the size after decompression, the number of compression layers, and the compressions ratio, select **Do not scan compressed files if**:. Then, specify the conditions when compressed attachments should not be scanned.
      - **Extracted file count exceeds**—the maximum number of files within the compressed attachment; (0 means no limit). ISVW scans the files in the compressed file until it reaches the restriction.

- **Extracted file size exceeds**—the maximum file size after decompression. ISVW scans only individual files within the limit.
- **Number of layers of compression exceeds**—the maximum number of compression layers. ISVW scans the files in the compressed file until it reaches the restriction.
- **Extracted file size**—ISVW scans only individual files within the limit.

3. Click **Save**.

Enabling Macro Scanning

ISVW can quarantine attachments that contain macros. It moves the attachments to the SMTP quarantine directory, which provides additional security against the threat of macro viruses. When this feature is in effect, the recipient still receives the original mail message; only the attachment is quarantined.

To quarantine attachments:

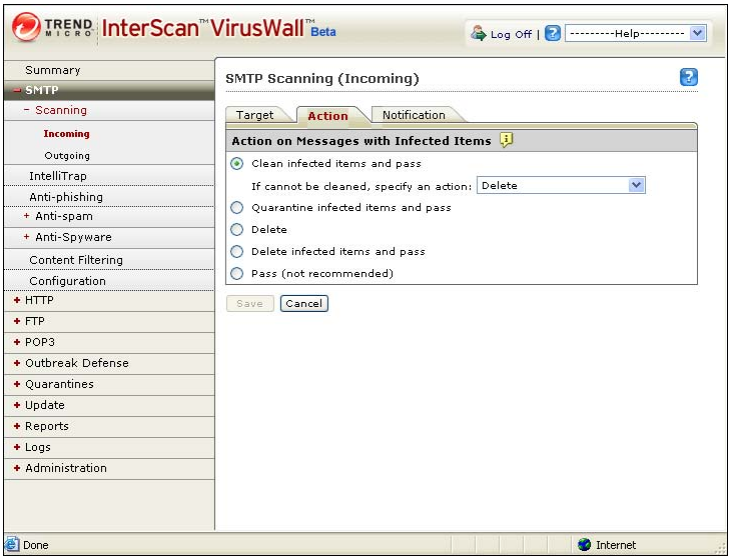
1. On the left side menu, select **SMTP > Scanning > Incoming (or Outgoing)** and click the **Target** tab.
2. Under **Macro Scanning**, select **Quarantine all Microsoft Office attachments containing macros**.
3. Click **Save**.

Note: The default quarantine folder for SMTP scanning is \quarantine\smtp.

Specifying the Action for Virus Detection

ISVW can take one of five actions when it detects a virus. Access possible actions on the SMTP Scanning **Action** tab shown in *Figure 4-3*.

FIGURE 4-3. SMTP Scanning Action Tab



To specify the action to take when ISVW detects infected attachments:

1. On the left side menu, select **SMTP > Scanning > Incoming** (or **Outgoing**) and then click the **Action** tab.
2. Under "Action on Messages with Infected Items", select your preferred option:
   - To clean infected attachments and deliver the message, select **Clean infected items and pass**. Then, select the action to take when infected attachments cannot be cleaned:
     - **Quarantine**—removes and quarantines attachments.
     - **Delete**—removes attachments without quarantining them.
     - **Pass (not recommended)**—delivers attachments with the message.
   - To quarantine attachments without cleaning them and deliver the message, select **Quarantine infected items and pass**.
   - To delete the message, select **Delete**.
   - To permanently delete attachments and deliver the message, select **Delete infected items and pass**.

- To deliver the message with infected attachments, select **Pass (not recommended)**.

3. Click **Save**.

Note: The default quarantine folder for SMTP scanning is `\quarantine\smtp`.

Configuring Virus Scan Notification Settings

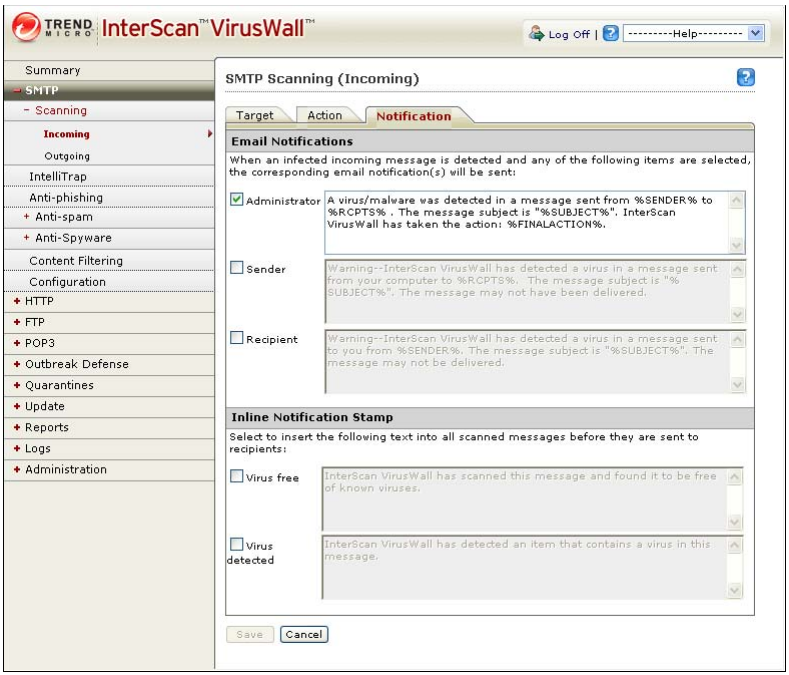
When ISVW finds a virus, it can notify the administrator, the message recipient, or the sender. You can configure the settings, include inline notifications on all scanned messages, and specify separate notification settings for incoming and outgoing messages.

Specifying notification settings for virus detection

To specify notification settings when ISVW detects a virus in an incoming or outgoing message attachment:

1. On the left side menu, select **SMTP > Scanning > Incoming** (or **Outgoing**) and click the **Notification** tab, shown in *Figure 4-4*.

   FIGURE 4-4. SMTP Scanning Notification Tab



2. Under **Email Notifications**, select the recipients of the notification sent when a virus is found.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address

Token	Description
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Specifying inline notification settings

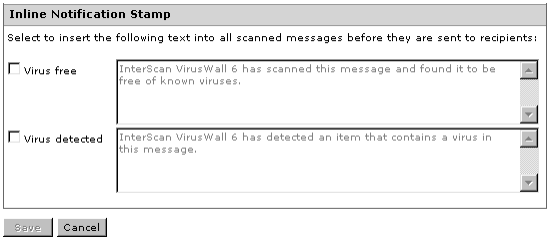
ISVW can insert text, known as an inline notification, into the message body of an incoming or outgoing message. When you select the message types **Virus free** and **Virus detected**, the inline notification will appear in all messages that ISVW scans.

To specify inline notification settings for incoming or outgoing messages:

1. On the left side menu, select **SMTP > Scanning > Incoming** (or **Outgoing**) and click the **Notification** tab.
2. Under "Inline Notification Stamp" (see *Figure 4-5*), select the message types (**Virus free** and **Virus detected**) that should contain the inline notice.
3. Type the inline notice that ISVW will insert in the message body.
4. Click **Save**.

Note: The notice will be attached on the original message as the file `InterScan_SafeStamp.txt`.

FIGURE 4-5. Inline Notification Stamp



SMTP Whole File Scan

SMTP Whole File Scan is a supplement to the regular ISVW mail scan. Whole File Scan can detect special kinds of email viruses that cannot be detected by regular scanning methods. Whole file scanning can be configured from the intscan.ini file which is located in your product folder.

Note: Whole File Scan cannot be configured from the ISVW Web console. Configure Whole File Scan using the intscan.ini file that is located in the ISVW Windows product folder.

How Whole File Scanning Works

When ISVW receives an email (incoming or outgoing), the email is first tested with the virus filter. If the virus filter does not detect a virus, the email is then tested with the whole file filter. If the email triggers the whole file filter, meaning the email contains a virus, ISVW will take an action on the message and, if enabled, send a notification to the administrator, sender, and recipient.

Configuring Whole File Scan for SMTP

Configuring Whole File Scan is a four (4) step process. You must first enable Whole File Scan. Next you must set (enable) an action for ISVW to take if it detects a virus. Next you should set up a notification to notify the administrator and recipient that ISVW detected a virus.

Note: Whole File Scan is disabled by default.

Enabling or Disabling Whole File Scan

To enable/disable whole file scan:

1. Open the ISVW Windows product folder and locate the file `intscan.ini`.
2. Open the intscan.ini file in any text editor program
3. Scroll down the screen until you locate the following values:

   InboundWholeMailVirusScan

   OutboundWholeMailVirusScan
4. Set the value to "yes" to enable Whole File Scan and "no" to disable Whole File Scan.
5. Save and close the file.
6. Restart the ISVW server for changes to take affect.

Setting the Action

There are two (2) actions that ISVW can take when the whole file filter detects a virus, Delete and Quarantine. The default action is Delete. Set the action to quarantine to quarantine the email.

To set the action ISVW should take when the whole file filter detects a virus:

1. Open the ISVW Windows product folder and locate the file `intscan.ini`.
2. Open the intscan.ini file in any text editor program.
3. Scroll down the screen until you locate the following value:

   WholeMailScanAction

Note: There are two possible actions that ISVW can take when the whole file filter detects a virus. The default action for Whole File Scan is Delete.

4. Set the action that ISVW should take when the whole file filter detects a virus.
   - Delete
   - Quarantine

5. Save and close the file.
6. Restart the ISVW server for changes to take affect.

Sending Notifications

ISVW can send a notification message to the administrator, sender, or recipient if the whole file filter detects a virus. From the Web console, you can enable or disable notifications for any or all of the aforementioned people. ISVW has a default notification message. You can modify the notification message from the Web console. See *Configuring Virus Scan Notification Settings* on page 4-8 for instructions on configuring notifications.

Configuring IntelliTrap Settings

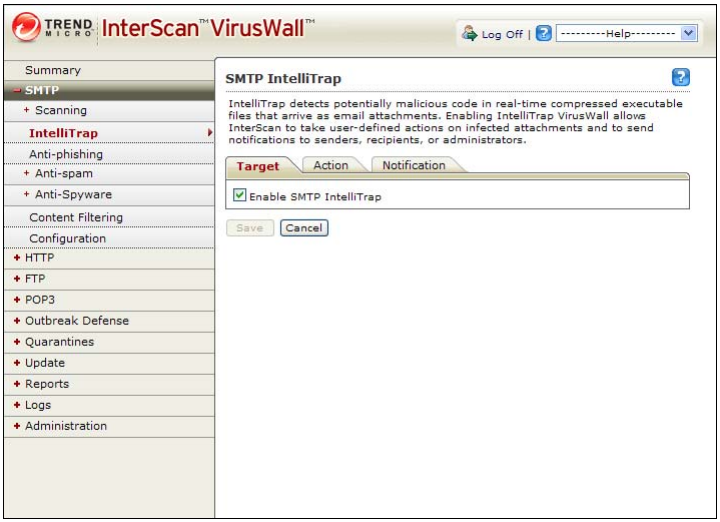
IntelliTrap detects potentially malicious code in real-time compressed executable files that arrive as email attachments. Enabling IntelliTrap allows ISVW to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Enabling or Disabling SMTP IntelliTrap Scanning

To enable or disable SMTP IntelliTrap scanning:

1. On the left side menu, select **SMTP > IntelliTrap** and click the **Target** tab, shown in *Figure 4-6*.

   FIGURE 4-6. SMTP IntelliTrap Target Tab



2. Select or clear the **Enable SMTP IntelliTrap** check box to enable or disable IntelliTrap scanning.
3. Click **Save**.

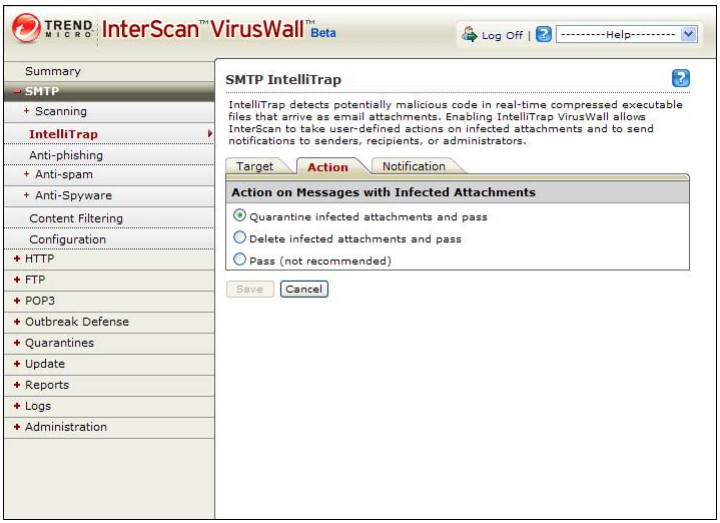
Specifying the Action to Take when IntelliTrap Detects Potentially Malicious Code

You can select one of three actions for ISVW when IntelliTrap detects potentially malicious code.

To specify the action to take when IntelliTrap detects potentially malicious code:

1. On the left side menu, select **SMTP > IntelliTrap** and click the **Action** tab, shown in *Figure 4-7*.

FIGURE 4-7. IntelliTrap Action Tab



2. Under **Action on Messages With Infected Attachments**, select your preferred option:
   - Select **Quarantine infected attachments and pass** to quarantine attachments and deliver the message. Users will receive the message without the attachment(s); the attachment(s) will be stored in the quarantine folder.
   - Select **Delete infected attachments and pass** to permanently delete attachments and deliver the message. Users will receive the message without the attachment.
   - Select **Pass (not recommended)** to deliver the message with infected attachments. Users will receive the message with the attachment(s) and an inline warning.
3. Click **Save**.

Note: The default quarantine folder for SMTP scanning is `\quarantine\smtp`.

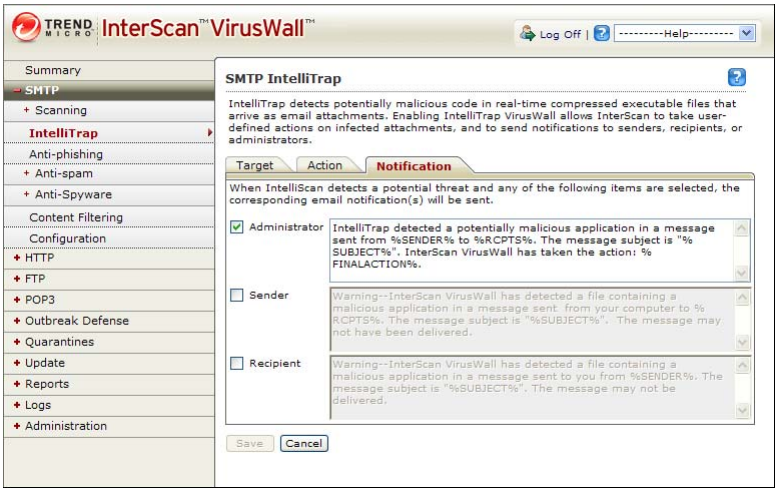
Configuring IntelliTrap Notification Settings

ISVW can automatically notify selected recipients whenever IntelliTrap detects potentially malicious code in compressed executable files.

To specify notification settings when IntelliTrap detects a security threat in a message attachment:

1. On the left side menu, select **SMTP > IntelliTrap** and click the **Notification** tab, shown in *Figure 4-8*.

FIGURE 4-8. SMTP IntelliTrap Notification Tab



2. Select the recipients of the notification sent when IntelliTrap detects a security risk.

3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save.**

Configuring SMTP Anti-phishing Settings

Phish, or *phishing*, is a rapidly growing form of fraud that mimics a legitimate Web site and seeks to fool Web users into divulging private information. Phishing attacks involve email messages that falsely claim to be from an established, legitimate organization. The messages typically encourage recipients to click on a link that will redirect their browsers to a fraudulent Web site, where they are asked to update personal information. Victims usually give up passwords, social security numbers, and credit card numbers.

In a typical scenario, unsuspecting users receive an urgent sounding (and authentic looking) email telling them that there is a problem with their account that they must immediately fix, or the account will be closed. The email will include a URL to a Web

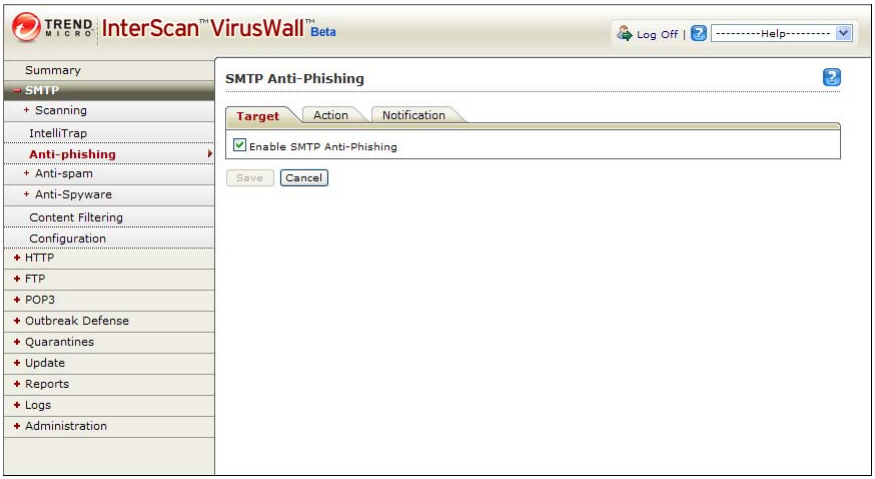
site that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate Web site but then change the back end—where the collected data is actually sent.

Enabling SMTP Anti-phishing

To enable the SMTP anti-phishing feature:

1. On the left side menu, select **SMTP > Anti-phishing** and click the **Target** tab, shown in *Figure 4-9*.
2. Select the **Enable SMTP Anti-phishing** check box.
3. Click **Save**.

FIGURE 4-9. SMTP Anti-phishing Target Tab

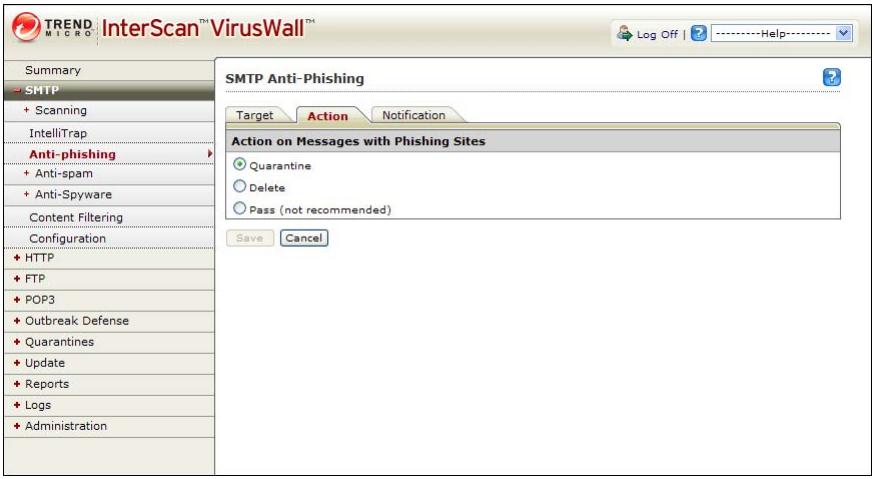


Specifying the Action to Take upon Detection of a Phishing Message

To specify the action on phishing messages:

1. On the left side menu, select **SMTP > Anti-phishing** and click the **Action** tab, shown in *Figure 4-10*.
2. Select the action for phishing messages:
   - Select **Quarantine** to move the message to the quarantine folder.
   - Select **Delete** to delete the message without delivering it.
   - Select **Pass (not recommended)** to deliver the phishing message normally.
3. Click **Save**.

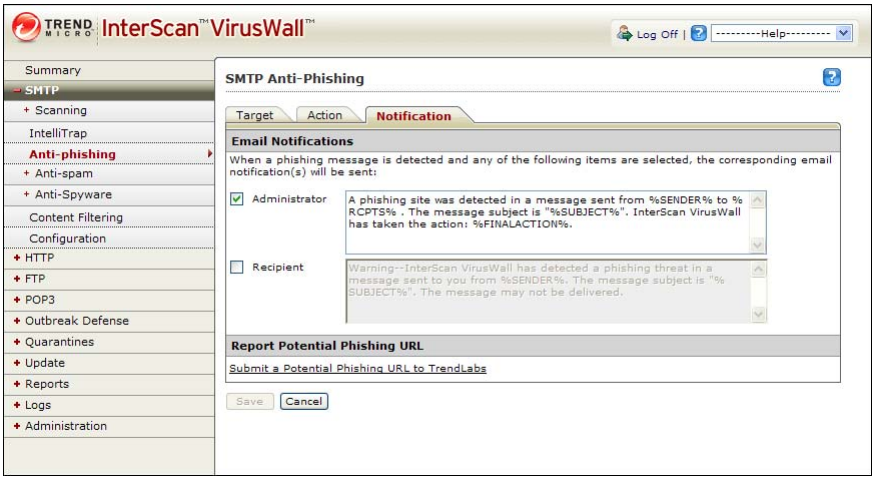
FIGURE 4-10. SMTP Anti-phishing Action Tab



Specifying Notification Settings when a Phishing Site Is Detected

When ISVW detects a phishing message, it can send an email notification to the administrator, the recipient(s), or both. You can report suspected or known phishing sites to TrendLabs. *Figure 4-11* shows the SMTP Anti-phishing Notification tab that allows you to specify whether to send email notifications when ISVW detects a phishing site.

FIGURE 4-11. SMTP Anti-phishing Notification Tab



To specify notification settings when a phishing URL is detected:

1. On the left side menu, select **SMTP > Anti-phishing** and click the **Notification** tab.
2. Select the recipients of the notification sent when ISVW detects a phishing URL.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol

Token	Description
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Reporting a Potential Phishing URL

To report suspected or known phishing sites to TrendLabs, click **Submit a Potential Phishing URL to TrendLabs** and provide the URL in an email that you will send to `antifraud@support.trendmicro.com`.

TrendLabs monitors sites that obtain information for fraudulent purposes and distributes known phishing site information as part of the automatic updates that Trend Micro makes available to ISVW customers.

Note: To view a list of phishing emails, go to http://www.trendmicro.com/en/security/phishing/overview.htm.

Configuring SMTP Anti-spam

ISVW uses the following Content Scanning and Email Reputation features to filter spam in SMTP email communication:

- **RBL+ Service**—provides information that can be used to protect against spam email, phishing attacks and other unwelcome messages before they reach the network. If enabled, the service provides subscribers with electronic access to a comprehensive database of Internet Protocol ("IP") addresses consisting of known sources of spam mail and other proven and suspicious sources of electronic communications, such as open proxies, open relays and dynamically assigned IP addresses.

- **Trend Micro Network Anti-Spam Service**—provides highly dynamic, real-time detection and blocking of currently active spam sources that may not yet have a history of sending spam. The setting is ideal for detecting botnet and zombie attacks.
- **Approved and Blocked Senders lists**—these lists filter on the sender's email address rather than on content. ISVW always delivers approved sender messages and always classifies blocked sender messages as spam.

Note: The Exchange administrator maintains a separate Approved and Blocked Senders list for the Exchange server. If an end user creates an approved sender, but that sender is on the administrator's Blocked Senders list, then messages from that sender will be blocked.

- **Spam filter**—administrators set a spam detection level to filter out spam. The higher the detection level, the more messages that ISVW classifies as spam. Administrators can set a global detection level for all messages or set one detection level for each spam category.

  The detection level determines how tolerant ISVW will be toward suspect email messages.

  - A high detection level quarantines the most email as spam, but it might also falsely identify and quarantine legitimate email messages as spam, creating "false positive" spam mail.
  - A low detection level does not rigorously screen email messages, and does not create many false positive spam messages.

Enabling SMTP Anti-spam (Email Reputation)

The SMTP Anti-spam Target tab allows you to enable Email Reputation and specify the level of service desired.

To enable SMTP anti-spam Email Reputation:

1. On the left side menu, select **SMTP > Anti-spam > Email Reputation**.
2. Click the **Target** tab.
3. Select the **Enable SMTP Anti-spam (Email Reputation)** check box.
4. Click **Save**.

Setting the Service Level

To set the service level for Email Reputation:

1. On the left side menu, select **SMTP > Anti-spam > Email Reputation**.
2. Click the **Target** tab.
3. Select the **Enable SMTP Anti-spam (Email Reputation)** check box.
4. Select a service level:
   - **Standard (recommended) -** ISVW queries only the RBL database. With the Standard setting there is less of a chance that ISVW will wrongly identify a legitimate email as spam (false positive). Select this setting if you are concerned about false positives detections.
   - **Advanced -** ISVW queries the RBL database, if nothing found then it queries the QIL database. With the Advanced setting there is a greater chance that ISVW will identify some legitimate email as spam. (false positive)
5. Click **Save**.

Maintaining the Approved IP Address(es) List

To maintain the Approved IP Address(es) list:

1. On the left side menu, select **SMTP > Anti-spam > Email Reputation**.
2. Click the **Target** tab.
3. Select the **Enable SMTP Anti-spam (Email Reputation)** check box.
4. Add Approved IP address(es):
   a. Type one or more IP Addresses for ISVW to exclude in the **Approved IP** field.
   b. Click **Add**.
5. Click **Save**.

Setting the Action for Email Reputation

To set SMTP Anti-spam (Email Reputation) Action:

1. From the left side menu select **SMTP > Anti-spam > Email Reputation** and then click the **Action** tab.
2. Choose one of the following actions that ISVW should take when it detects a message originating from an IP address that is a known spam source:

   Action for RBL+ (Applies to both Low and High settings)

   - Connection denied with error message to user. User will receive SMTP error code: (range 400 - 599; default=550)
   - Connection denied with no error message to user
   - Pass (not recommended)

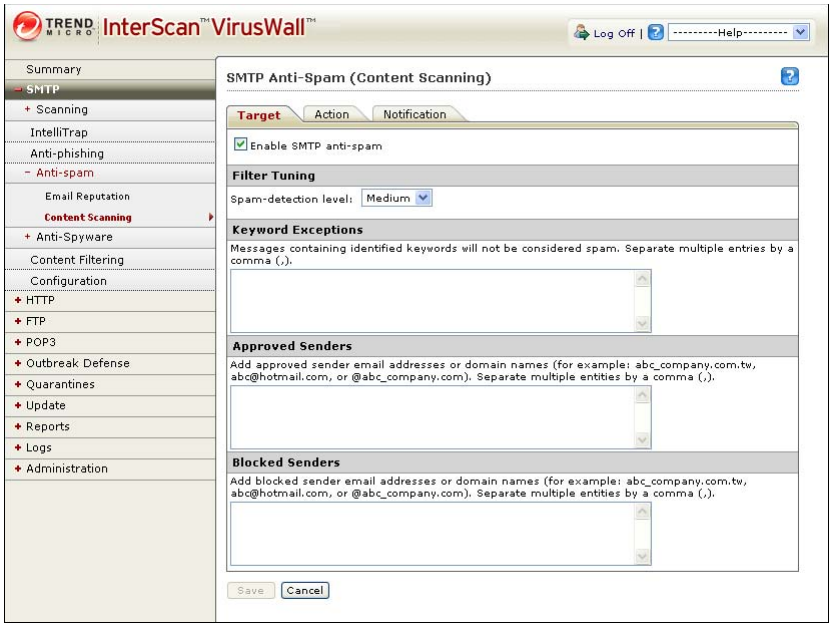
   Action for QIL+ (Applies to High setting)

   - Connection denied with error message to user. User will receive SMTP error code: (range 400 - 599; default=450)
   - Connection denied with no error message to user
   - Pass (not recommended)
3. Click **Save**.

Enabling SMTP Anti-spam (Content Scanning)

The SMTP Anti-spam Target tab, shown in *Figure 4-12*, allows you to enable spam filtering.

FIGURE 4-12. SMTP Anti-spam Target Tab



To enable SMTP anti-spam Content Scanning:

1. On the left side menu, select **SMTP > Anti-spam > Content Scanning**.
2. Click the **Target** tab.
3. Select the **Enable SMTP Anti-spam (Content Scanning)** check box.
4. Click **Save**.

Setting the Spam Detection Level (Filter Tuning)

To specify the spam detection level:

1. On the left side menu, select **SMTP > Anti-spam > Content Scanning**.
2. Click the **Target** tab.
3. In the **Filter Tuning** section, select the desired span detection level.

Spam Detection Levels

ISVW uses the following detection levels:

Detection Level	Filtering Criteria
Low	ISVW filters only the most obvious and common spam messages, but there is a very low chance that it will filter false positives. This is most lenient level of spam detection.
Medium	ISVW monitors at a high level of spam detection with a moderate chance of filtering false positives. This is the default setting.
High	ISVW monitors all email messages for suspicious files or text, but there is greater chance of false positives. This is the most rigorous level of spam detection.

Determining Spam Detection Levels

The ISVW anti-spam engine uses heuristics and algorithms to calculate the spam detection level. The engine scans the message or file and assigns the scanned item a spam score. Based on this spam score and the spam detection and confidence levels that you specify, ISVW determines whether the item is spam.

The following are the predefined threshold settings:

	Low Confidence	Medium Confidence	High Confidence
Low detection level	6	7	10
Medium detection level	4.5	6	10
High detection level	4	5	7

Note: The scores in the spam threshold settings table may vary depending on the anti-spam pattern in use.

- If you specify a low detection level and the spam score is 6.5, then ISVW will perform the action specified for the low confidence level.
- If the spam score is 8, ISVW will perform the action specified for the medium confidence level.

- If the spam score is 11, ISVW will perform the action specified for the high confidence level.

To see a spam score, see the spam log. A sample entry might be:

```
2009/02/04 20:10:32, SMTP, , Stamp, Success, "LastName\,
FirstName"

 <FirstName.LastName@Level3.com>,"SPAM@TrendMicro.com"

 <SPAM@TrendMicro.com>, FW:How are you doing?

 <D7626E4452B0F745B4C7C15BC97EA052D66887@idclexc0005.corp.globa
l.

 level3.com>, 3.51.0.1033, 13974000, Spam, ,14.594000
```

Tuning the Spam Filter

If you are getting too many false positives, set the spam detection level to a lower setting. Conversely, if users report that they are getting too much spam, adjust the detection level to a higher setting.

To submit samples of false positives to Trend Micro, go to `http://subwiz.trendmicro.com/SubWiz/spam_mail-Form.asp`

Specifying Keyword Exceptions

Keyword exceptions will exclude messages that contain certain text from spam filtering. Separate keywords in the exception lists with a comma. Type keywords that should *not* be considered spam in the Keyword Exceptions text box shown in *Figure 4-13*.

Note: No characters except a single comma (,) is allowed between two keywords, this excludes a space and a hard return.

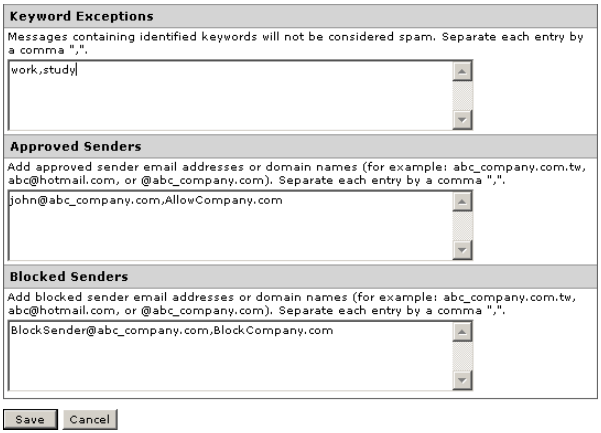


FIGURE 4-13. SMTP Anti-spam Keyword Exceptions and Blocked and Approved Senders Lists

Maintaining Approved and Blocked Senders Lists

The Approved Senders list contains trusted email addresses. ISVW does not filter messages arriving from these addresses for spam, except when you enable **Detect Phishing incidents**.

The Blocked Senders list contains email addresses that cannot be trusted. ISVW automatically considers messages arriving from these addresses as spam and deletes such messages. ISVW does not notify anyone that it deleted the messages.

When an email address is in both the Approved Senders and Blocked Senders lists, messages arriving from this address are considered spam and are deleted.

When adding email addresses to the lists, separate them with a comma. Type all email addresses in the appropriate list, shown in *Figure 4-13*.

ISVW supports wildcard (*) matching for the Approved and Blocked Senders lists. Sample patterns are shown in *Table 4-1*.

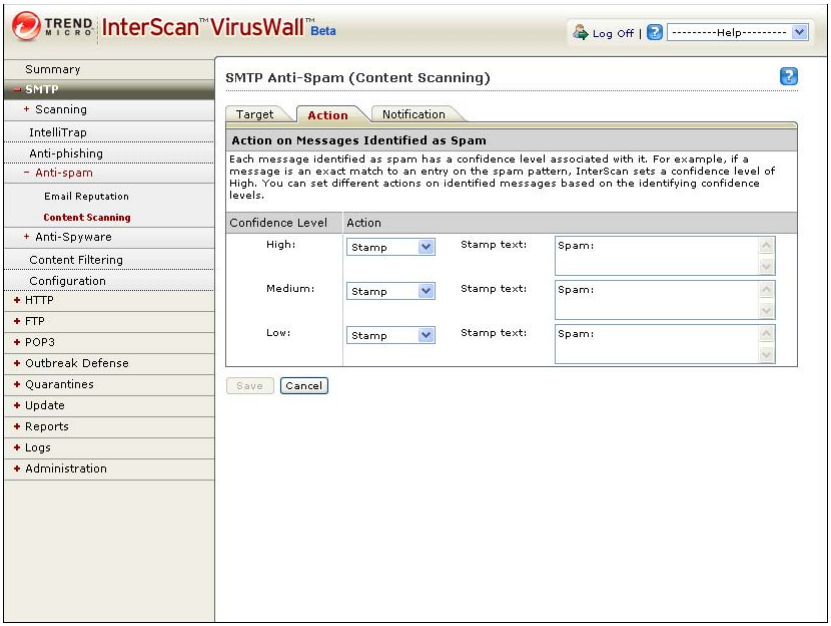
TABLE 4-1. Using Wildcards (*) in the Senders Lists

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
john@trend.com	john@trend.com john@trend.com.	Any address different from the pattern.
@trend.com *@trend.com	john@trend.com mary@trend.com.	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com.	john@trend.com.tw mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com.	john@trend.com john@trend.com.tw mary@ms1.trend.comon
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw.	john@trend.com john@ms1.trend.com. john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw.	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com.
..*.trend.com *****.trend.com	The same as "*.trend.com"	The same as "*.trend.com"
trend.com trend.com trend.*.com @*.trend.com	They are all INVALID.	They are all INVALID.

Specifying Actions on Messages Identified as Spam

ISVW can take one of several actions when it identifies a message as spam. The detection level(s) that you set on the Target tab determine the action. *Figure 4-14* shows the SMTP Anti-spam Content Scanning Action tab.

FIGURE 4-14. SMTP Anti-spam (Content Scanning) Action Tab



To specify the action on spam messages:

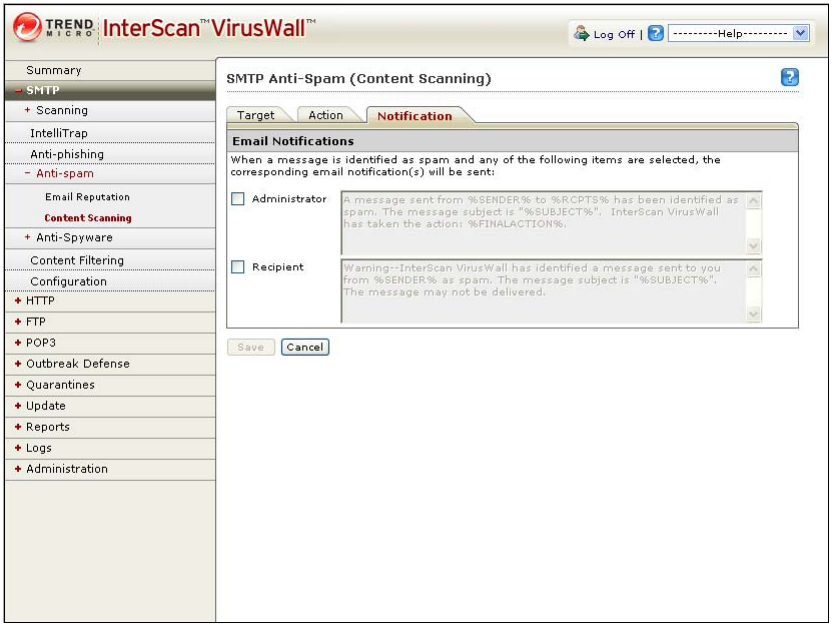
1. On the left side menu, select **SMTP > Anti-spam > Content Scanning** and click the **Action** tab.
2. Specify the action to take based on the detection confidence level:
   - **High**—ISVW is very confident that the mail message is spam.
   - **Medium**—ISVW is fairly confident that the mail message is spam.
   - **Low**—ISVW is fairly confident that the mail message is not spam.

   For each confidence level, you can select one of four actions:
   - **Delete**—The whole message is deleted.
   - **Quarantine**—The message is quarantined.
   - **Stamp**—A notification content stamp will be inserted into the subject line of the message.
   - **Pass**—ISVW does nothing to the message and it is processed normally.

Specifying Notification Settings for Detected Spam

ISVW can notify the administrator or the recipient when it detects spam email messages. You can specify recipients for the email notification and create messages to send to the administrator and mail recipients. *Figure 4-15* shows the SMTP Anti-spam (Content Scanning) Notification Settings tab.

FIGURE 4-15. SMTP Anti-spam (Content Scanning) Notification Settings Tab



To specify notification settings when ISVW detects spam:

1. On the left side menu, select **SMTP > Anti-spam > Content Scanning** and click the **Notification** tab.
2. Under **Email Notifications**, select the recipients who will be notified when ISVW detects spam.

3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Configuring SMTP Anti-spyware Settings

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular updates in a pattern file.

Some common types of grayware include:

TYPE OF GRAYWARE	TYPICAL FUNCTION
Spyware	gathers data, such as account user names and passwords, and transmits them to third parties
Adware	displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser

TYPE OF GRAYWARE	TYPICAL FUNCTION
Dialers	changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	helps hackers enter computers
Remote Access Tools	help hackers remotely access and control computers
Password Cracking Applications	helps hackers decipher account user names and passwords
Others	other types not covered above

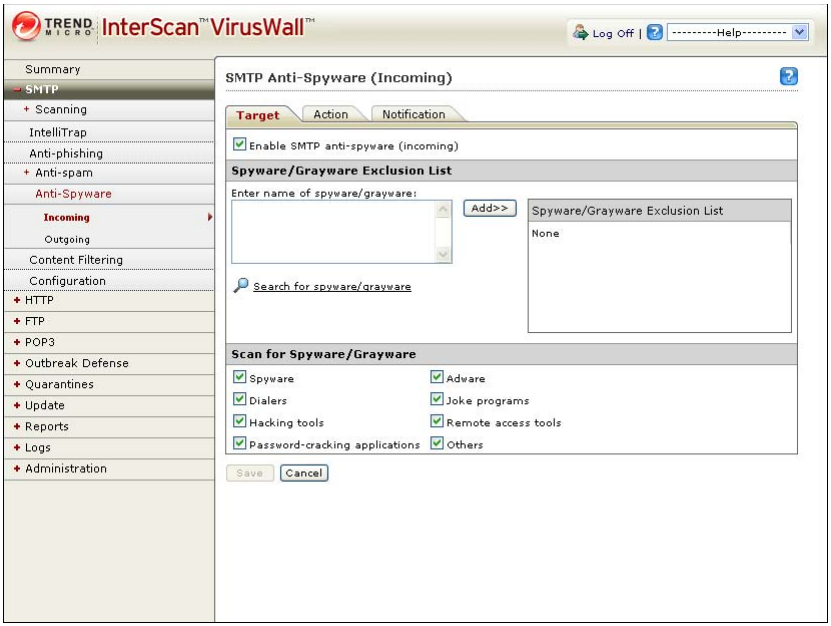
Enabling SMTP Spyware Scanning Incoming or Outgoing

To enable SMTP spyware scanning:

1. On the left side menu, select **SMTP > Anti-spyware > Incoming (or Outgoing)** and click the **Target** tab.
2. Select the **Enable SMTP Anti-spyware (incoming) or (outgoing)** check box.
3. Click **Save**.

Figure 4-16 shows the SMTP Anti-spyware Target tab, which allows you to enable SMTP spyware scanning types and exclusions.

FIGURE 4-16. SMTP Anti-spyware (Incoming) Target Tab



Setting the Spyware Scanning Exclusion List

To list specific file names or file name extensions to exclude from spyware/grayware scanning:

1. On the left side menu, select **SMTP> Anti-spyware** > **Incoming (or Outgoing)** and click the **Target** tab.
2. In **Enter name of spyware/grayware**, type the spyware name you want to exclude from spyware/grayware scanning.

   If you are not sure of the spyware name, click the **Search for spyware/grayware** link.
3. Click **Add**.
4. Click **Save**.

Note: To delete entries on the exclusion list, click the trash bin icon. Click **Save** to finalize changes.

Specifying Spyware and Grayware Types to Scan

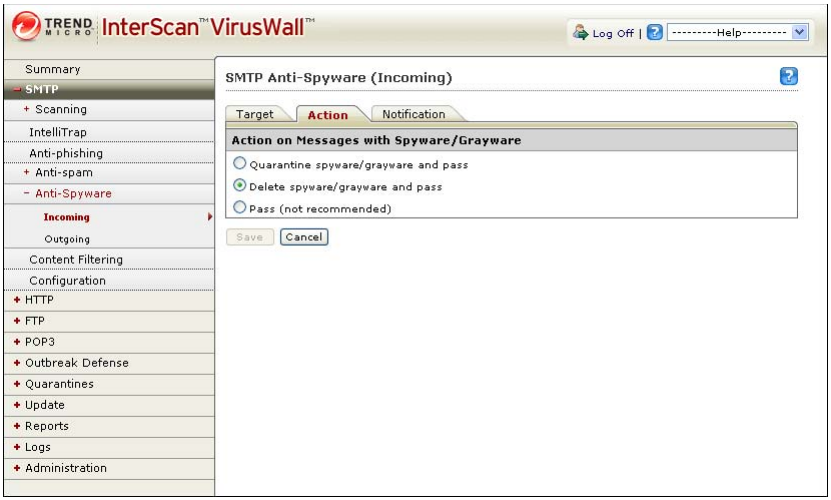
To specify the types of spyware and grayware for which you want ISVW SMTP services to scan:

1. On the left side menu, select **SMTP > Anti-spyware > Incoming (or Outgoing)** and click the **Target** tab.
2. Under **Scan for Spyware/Grayware**, select the types of spyware and grayware for which SMTP services will scan.
3. Click **Save**.

Specifying the Action to Take upon Spyware Detection

ISVW can take one of three actions when it detects spyware or other grayware (see *Figure 4-17*).

FIGURE 4-17. SMTP Anti-spyware (Incoming) Action Tab



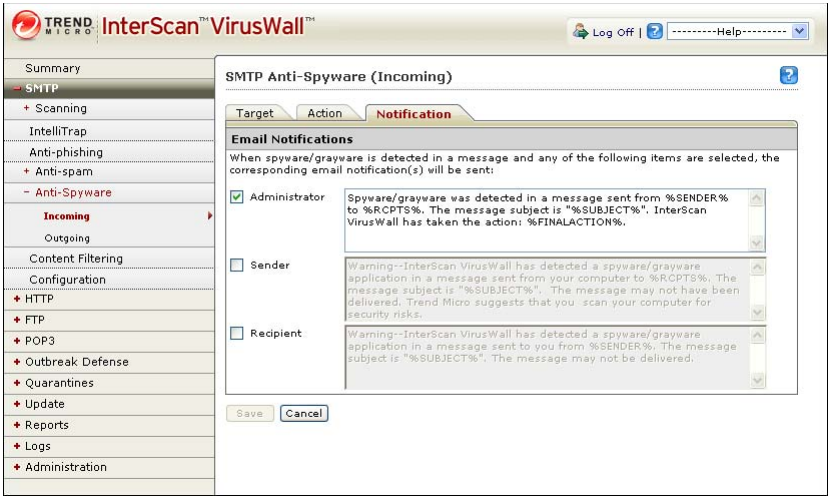
To specify the action to take when ISVW detects spyware/grayware:

1. On the left side menu, select **SMTP > Anti-spyware > Incoming** (or **Outgoing**) and click the **Action** tab.
2. Under **Action for Detected Spyware/Grayware Messages**, select your preferred option:
   - To quarantine attachments and deliver the message, select **Quarantine spyware/grayware and pass**. Users will receive the message without the attachment; the attachment will be stored in the quarantine folder.
   - To permanently delete detected attachments and deliver the message, select **Delete spyware/grayware and pass**. Users will receive the message without the attachment.
   - To deliver the message with the detected attachments, select **Pass (not recommended)**.
3. Click **Save**.

Specifying Notification Settings for Detected Spyware/Grayware

When ISVW detects spyware or other grayware in an incoming or outgoing message, you can specify whether to send notifications to the sender, recipient(s), and administrator (see *Figure 4-18*).

FIGURE 4-18. SMTP Anti-spyware (Incoming) Notification Tab



To specify notification settings when spyware or grayware is detected:

1. On the left side menu, select **SMTP > Anti-spyware > Incoming (or Outgoing)** and click the **Notification** tab.
2. Select the recipients of the notification sent when spyware or grayware is detected.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject

Token	Description
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

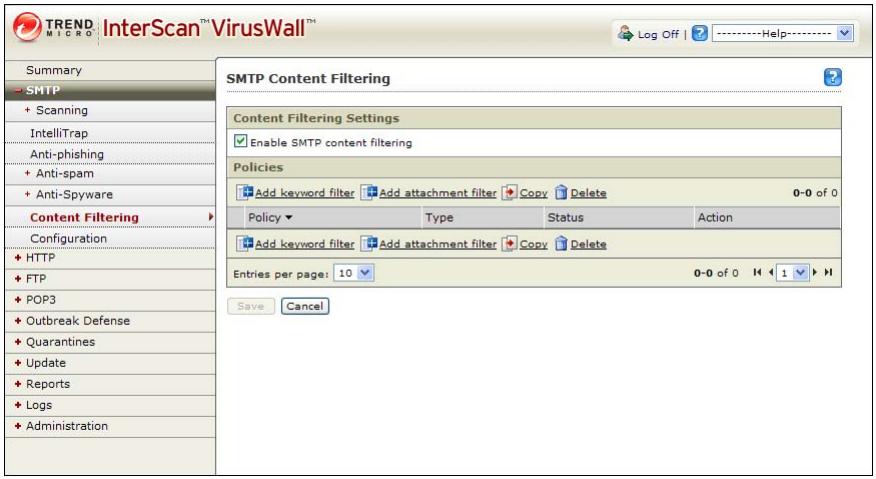
SMTP Content Filtering

ISVW provides email content filtering for SMTP. This feature provides real-time monitoring and control of information that enters or leaves the network through SMTP.

Enabling SMTP Content Filtering

When you enable SMTP content filtering, ISVW scans all information that enters or leaves the network through SMTP for possible matches with the policies that you have defined to filter the content of SMTP traffic. *Figure 4-19* shows the content filtering settings. All policies that have been defined to filter content will be listed under **Policies**.

FIGURE 4-19. SMTP Content Filtering Settings



To enable SMTP content filtering:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Content Filtering Settings**, select the **Enable SMTP content filtering** check box.
3. Click **Save**.

Disabling SMTP Content Filtering

If you disable SMTP content filtering, ISVW will not monitor the content of SMTP traffic. Any other SMTP scanning features that are enabled will continue to function as specified.

To disable SMTP content filtering:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Content Filtering Settings**, clear the **Enable SMTP content filtering** check box.
3. Click **Save**.

Creating Policies

ISVW uses policies that can use either a keyword filter or an attachment filter.

To create a policy:

To create a policy, click either **Add keyword filter** or **Add attachment filter**.

Creating an SMTP Content Filtering Policy Based on Keywords

Keyword filters allow the ISVW administrator to evaluate and control the delivery of email messages based on the message content itself. These filters can monitor both inbound and outbound messages to check for sensitive or offensive content. The keyword filter also provides a synonym-checking feature, which allows you to extend the reach of your policies. The keyword filter supports scanning of content in double-byte characters, such as messages in Chinese or Japanese.

Keyword lists

The keyword list for a given keyword filter contains the words and phrases matched by the filter to message content. When multiple keywords appear on the same line of a policy, a match occurs only when the message being evaluated contains all of the keywords on that line. Consider the following keywords examples:

Example 1:

resume, position

resume, job

resume, experience

resume, enclosed

In Example 1, the word “resume” appears with an additional word four times instead of using it just once as a single entry. Using just resume would probably produce unreliable results because resume can mean either curriculum vitae or to start again. To minimize the chance of such false matches, it is a good idea to qualify the primary word with additional words typically associated with it; in this example, words that are likely to appear in a job-seeking letter include enclosed, position, job, and experience. Including several keyword groups will increase the reach of the filter.

As configured in the example, messages that contain any of the keyword pairs are considered a match.

Alternatively, the filter could trigger the configured action only when all five words appear in a single outbound message. To do this, include all the keywords on a single line.

Example 2:

Resume, position, job, experience, enclosed

Obviously, the likelihood of detecting every outbound resume on the basis of this filter is much less than for a policy that contains several rule sets based upon the word resume, as shown in Example 1.

Example 3 shows a policy wherein the occurrence of any one of the four words in Example 2 triggers a match.

Example 3:

job

resume

enclosed

position

experience

Generally speaking, keywords linked by the AND operator should not include more than four or five words or the policy risks being overly restrictive. On the other hand, if only one keyword is included on any given line (OR operator), the policy risks being too permissive—too many email messages will be found to match. Of course, as shown above, a lot depends upon what you are filtering.

The criteria you specify are evaluated exactly as entered, including any spaces and punctuation. Phrases delimited by commas are treated as a single unit. Only when each word, space, and so on in the phrase appears in the message, in the order entered, will a match occur.

Operators on keyword lists

Consider the following cases for keywords and the logical operators that apply to them based on the position of the keywords, as shown in:

TABLE 4-2. Keyword list showing logical operators and sample matching results

Case	*Result*
In the following examples, items within brackets [...] are for example purposes only and should not be included when creating the keyword list.	
Case 1. Keywords appear on a single line Example: Apple Juice, [AND] Pear, [AND] Orange Provides the same capabilities as the Logical Operator "AND"	Only messages containing all items, Apple Juice, Pear, and Orange (in any order, anywhere in the message text) are considered a match.
Case 2. Keywords each appear on their own individual lines Example: Apple Juice [OR] Pear [OR] Orange Provides the same capabilities as the Logical Operator "OR"	All messages containing the phrase *Apple Juice* are considered a match, all messages that contain the word Pear are considered a match, and all messages that contain the word Orange are considered a match.
Case 3. Keywords appear on a single line and synonym checking is enabled for the word Orange Example: Apple Juice, [AND] Pear, [AND] Orange (*The words orangish, red, and yellow in the synonyms list are synonymous with the word orange.) Provides the same capabilities as the Logical Operators "AND" and "OR"	With synonym checking on, messages that contain the phrase *Apple Juice,* the word *Pear,* and any of the words *Orange, orangish, red,* or *yellow* are considered a match.

Other keyword notes

Note that Apple Juice is a phrase because the words Apple and Juice are not delimited

with a comma; even if the words Apple and Juice both appear somewhere in the message, no match occurs unless they occur together as Apple Juice.

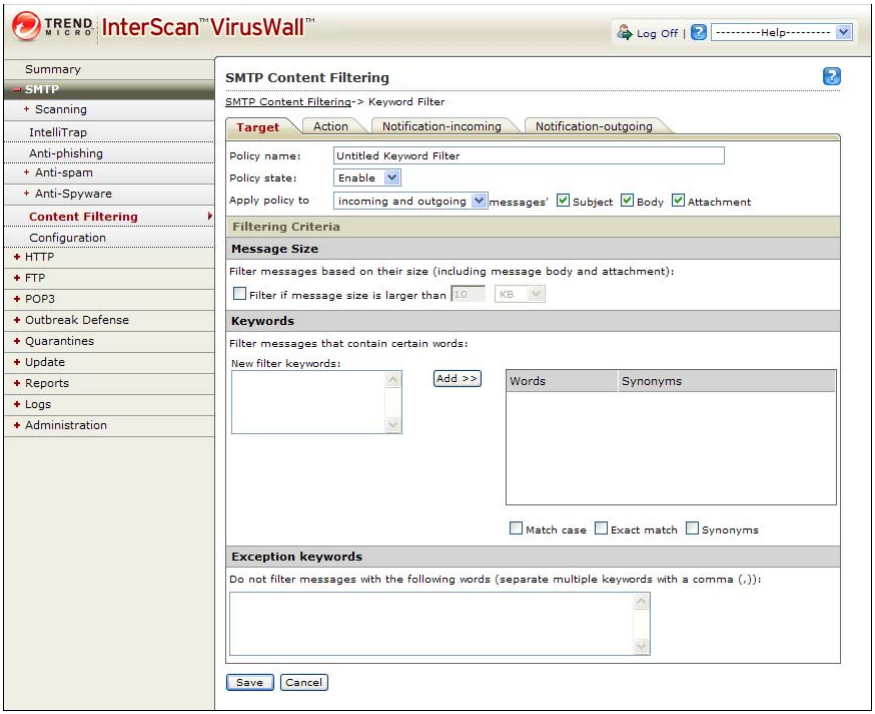
The capitalization and exact-match properties of synonyms are consistent with those defined for the keyword itself. In other words, if the word red appears in the synonyms list, it will trigger a match with the word Red if Exact Match is not checked; likewise, the word red will trigger a match with the word Red in the message text if Match Case comparison is not checked.

If a user adds multiple keywords in a single line separated by commas, the policy will be triggered only when all the keywords at that line appear in the same part of the mail. For example, if a user adds the keywords apple, pear, if apple appears in the subject of the message and pear appears in the body, the policy will not be triggered.

Adding a Policy Based on a Keyword Filter

To create a policy that uses keywords as the criteria to filter SMTP content, use the SMTP Content Filtering Keyword Filter Target tab shown in *Figure 4-20* to specify the policy rules.

FIGURE 4-20. SMTP Content Filtering Keyword Filter Target Tab



To add a policy based on a keyword filter:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, click the **Target** tab.
4. In the **Policy name** text box, type a policy name.
5. For **Policy status**, select **Enable** to apply the policy or **Disable** if you do not want to apply it.
6. In **Apply policy to**, select the type of messages (incoming, outgoing, or incoming and outgoing) and the sections of the messages (Subject, Body, or Attachment) to which this policy applies.

7. If you want the policy to block messages with attachments larger than a specified size, select **Filter if message size is larger than** and specify the size limit.
8. Under **Keywords**, type the keywords for which you want ISVW to scan messages and click **Add**. To specify synonyms for each keyword, click the link under the **Synonyms** column (default is [none]).

   If desired, enable any of the options **Match case**, **Exact match**, and **Synonyms**.

Note: For more information in creating a keyword list for your policy, see *Creating an SMTP Content Filtering Policy Based on Keywords* on page 4-41.

---

9. To reduce the chances of ISVW blocking messages that it should pass, type keywords that will identify these messages in **Exception keywords**.

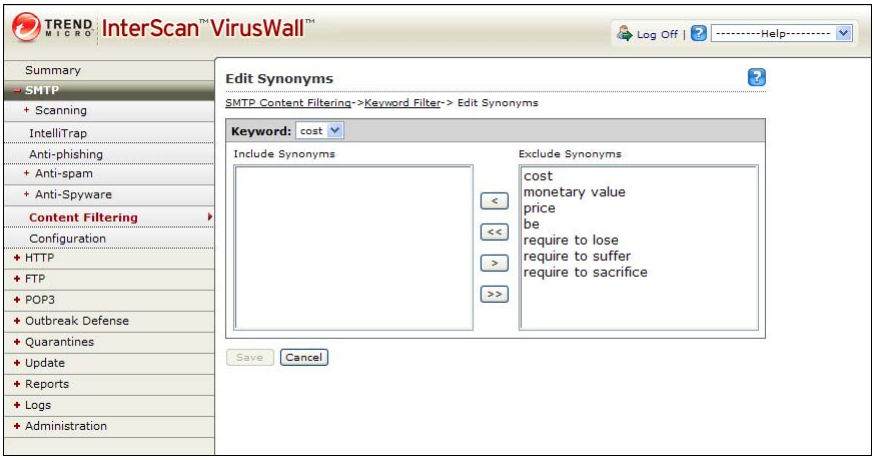
   The policy will not block messages that contain these keywords even when a keyword filter matches.
10. Click **Save**.

Modifying a Keyword's Synonym List

ISVW has a predefined list of synonyms for certain keywords. To view this predefined list and add the words as synonyms for your keyword, use the Edit Synonyms screen shown in *Figure 4-21*.

You cannot modify or add to the predefined list of synonyms.

FIGURE 4-21. Edit Synonyms Screen



To modify a keyword's synonyms list:

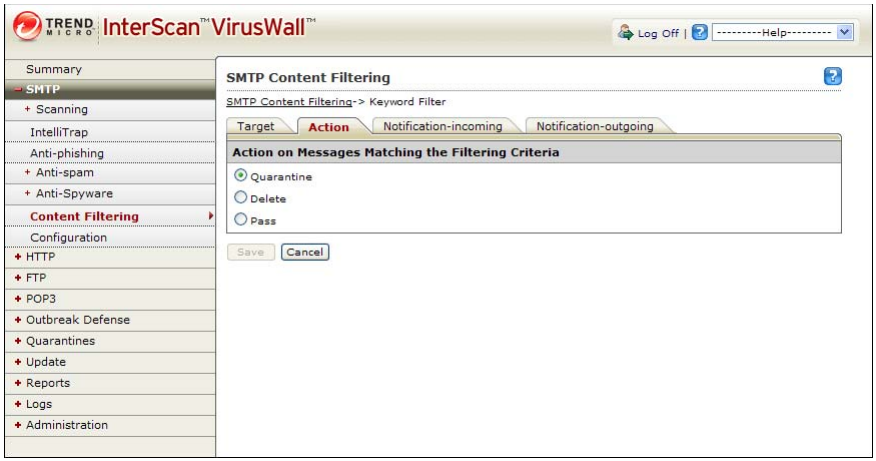
1. From the SMTP Content Filtering (Target tab) screen, go to the "Keywords" area and under the "Synonyms" column, click the hyperlink of the synonym you want to modify.
2. When the prompt appears, click **OK** to proceed to the Edit Synonyms screen.

   If you have entered multiple keywords that you separated with commas, all the keywords will appear in a drop-down list.
3. Select the one keyword for which you want synonyms to be displayed.
4. Select the synonyms you want to use for the keyword from the list of synonyms in the "Exclude Synonyms" column and click **<** to move the synonyms into the "Include Synonyms" column.
5. Click **Save**.

Setting the Action on Messages that Match the Keyword Filtering Policy

When an SMTP message meets the filtering criteria that you have specified, ISVW can take one of three actions on the message, as shown in *Figure 4-22*.

FIGURE 4-22. SMTP Content Filtering Keyword Filter Action Tab



To set the action on messages that match the content filtering policy:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, click the **Action** tab.
4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To delete the message, select **Delete**; messages will not be delivered.
   - To deliver the message, select **Pass**. Users will receive the message.
5. Click **Save**.

Specifying notification settings when a message meets the filtering criteria

You can notify the administrator and the recipients that prohibited content has been detected in an incoming (*Figure 4-23*) or outgoing (*Figure 4-24*) mail message attachment.

FIGURE 4-23. SMTP Content Filtering Keyword Filter Notification–incoming Tab

FIGURE 4-24. SMTP Content Filtering Keyword Filter Notification–outgoing Tab

To specify notification settings when a message triggers a policy:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, select the **Notification-incoming** or **Notification-outgoing** tab as appropriate.
4. Select the recipients of the notification.
5. Create the message to send to each recipient. You can use the following tokens or tags on the message:

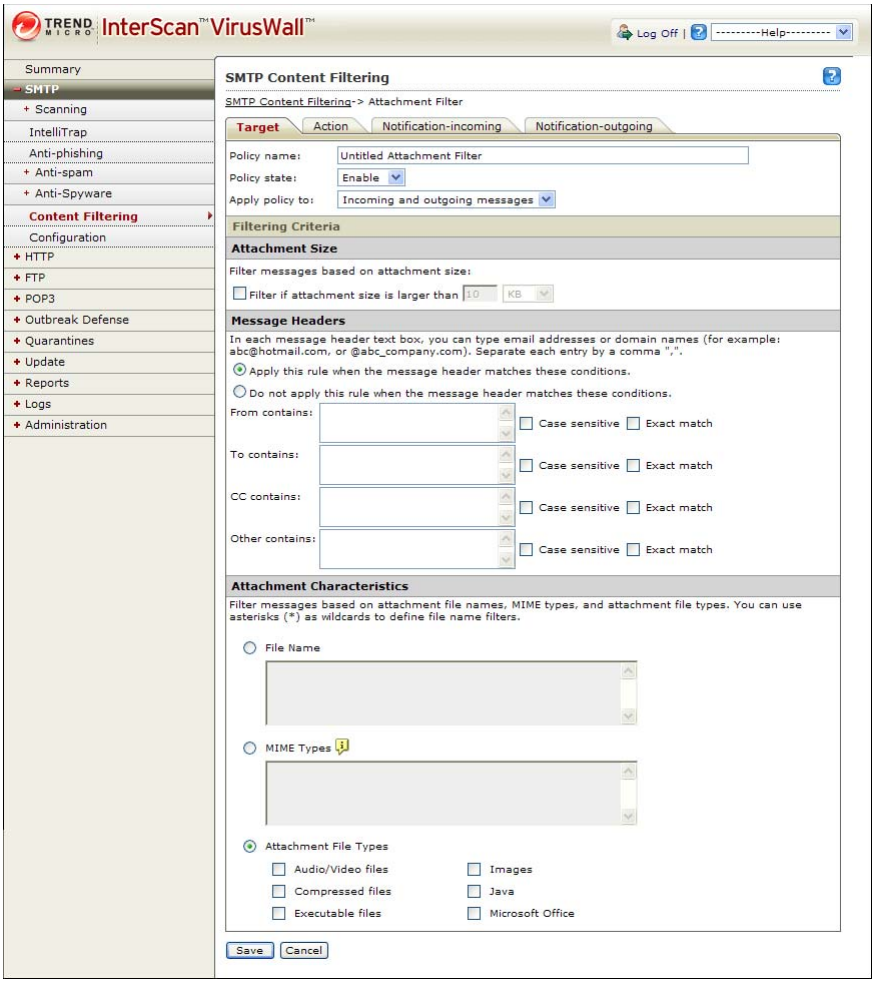
Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

6. Click **Save**.

Creating an SMTP Attachment Filter Policy for Content Filtering

To create a policy that uses attachments or message headers as the criteria to filter SMTP content, use the SMTP Content Filtering Attachment Filter Target tab shown in *Figure 4-25* to specify the policy rules.

FIGURE 4-25. SMTP Content Filtering Attachment Filter Target Tab



To add a policy based on an attachment filter:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.

3. When the Attachment Filter screen opens, click the **Target** tab.
4. In the **Policy name** text box, type a policy name.
5. For **Policy state**, select **Enable** to apply the policy or **Disable** if you do not want to apply it.
6. In **Apply policy to**, select the type of messages (incoming, outgoing, or incoming and outgoing) to which this policy applies.
7. If you want the policy to block attachments of messages larger than a specified size, select **Filter if attachment size is larger than**, and specify the size limit.
8. Under **Message Headers**, you can specify whether you want to apply this rule when strings in the message header match certain conditions, including the From, To, CC, and Reply-to fields. Select whether you want to block or pass messages based on the header strings.

   To specify multiple entries in the message header text boxes, separate each entry with a comma; for example, `user1@isvw.com,user2@isvw.com`.

   - Select **Apply this rule when the message header matches these conditions** to apply the settings under Attachment Characteristics to message headers that match the header strings you specified.
   - Select **Do not apply this rule when the message header matches these conditions** to apply the settings under Attachment Characteristics to message headers that do not match the header strings you specified.
9. Specify the header rules.
10. Under **Attachment Characteristics**, select the filtering criteria for message attachments.
    - **File Name**—specify a file name or a string using a wildcard (*). ISVW will filter all attachments with file names that match the names or the strings.
    - **MIME Types**—specify the MIME types to filter.
    - **Attachment File Types**—specify file type categories that you want to block. ISVW will block all attachments that are in the specified file type categories.

Note: To specify multiple entries in the File Name and MIME Types text boxes, separate each entry with a comma; for example, ***.jpg,*.txt** or **text/plain,image/jpeg**.

---

11. Click **Save**.

Setting the Action for an SMTP Content Filtering Attachment Policy

When an SMTP message meets the filtering criteria you have specified, ISVW can take one of three actions on the message, as shown in *Figure 4-26*.

FIGURE 4-26. SMTP Content Filtering Attachment Filter Action Tab

To set the action on messages that match the policy for attachments:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, click the **Action** tab.
4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To deliver the message, select **Pass**. Users will receive the message.
   - To remove the attachment, select **Delete attachment and pass**. Users will receive the message without the attachment.
5. To insert a notification into the body of the message, select **Insert the following notification in the message:**. You can modify the text of the message that you insert and use the following tokens:

- %FILENAME%: the name of the removed attachment
- %RULENAME%: the name of the policy

6. Click **Save**.

Specifying Notification Settings when a Message Attachment Meets the Filtering Criteria

You can send a notification to the administrator and the recipients that ISVW detected prohibited content in an incoming (*Figure 4-27*) or outgoing (*Figure 4-28*) mail message attachment.

FIGURE 4-27. SMTP Content Filtering Attachment Filter Notification–incoming Tab

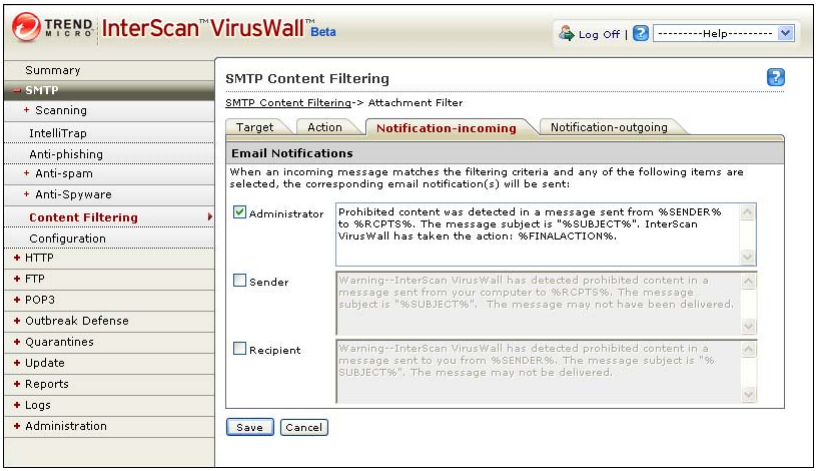
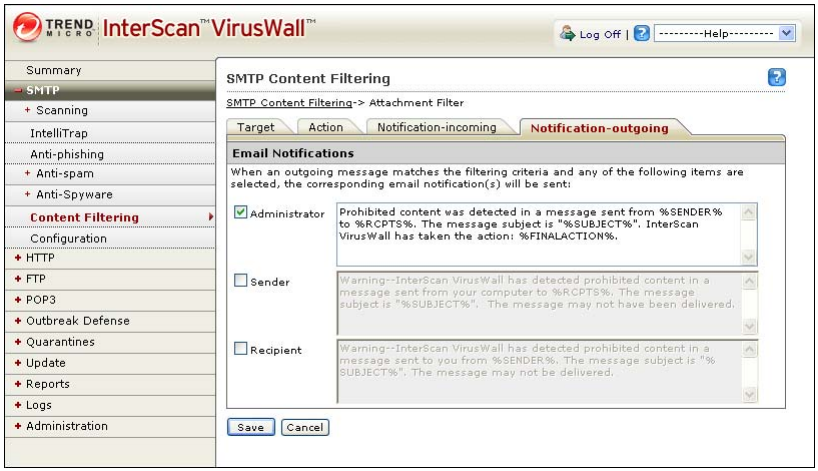


FIGURE 4-28. SMTP Content Filtering Attachment Filter Notification–outgoing Tab



To specify notification settings when a message triggers a policy:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, select the **Notification-incoming** or **Notification-outgoing** tab as appropriate.
4. Select the recipients of the notification.
5. Create the message to send to each recipient. You can use the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol

Token	Description
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

6. Click **Save**.

Copying or Deleting an SMTP Content Filtering Policy

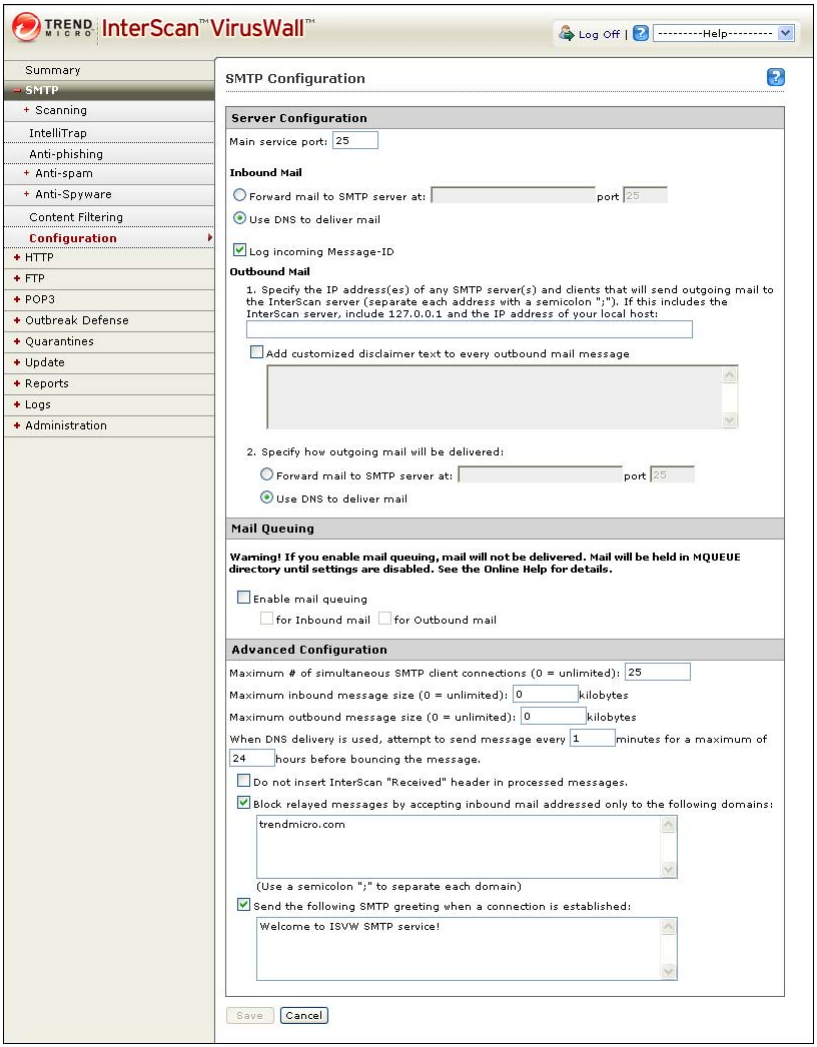
To copy an existing SMTP content filtering policy and modify it or delete a policy that you longer want:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under Policies, select a policy and click **Copy** or **Delete**.
3. Click **OK** on the pop-up message box to finalize changes.

SMTP Configuration

When you enable scanning of SMTP traffic, you need to configure how inbound and outbound traffic will be processed. *Figure 4-29* shows the configuration settings that you may need to specify.

FIGURE 4-29. SMTP Configuration Settings



Configuring SMTP Service Settings

To configure SMTP service settings:

1. On the left menu, select **SMTP > Configuration**.
2. Under **Server Configuration**, in the Main service port field, type the SMTP port number that ISVW will use to receive messages for processing. Typically, this port is 25. ISVW receives mail at this port, scans it for viruses, and then forwards the message.

Configuring Inbound Messages

To configure inbound messages:

1. Under **Inbound mail**, select how ISVW forwards inbound mail.
   - Select **Forward mail to SMTP server at** to specify the SMTP server and the specific port that the server uses.
   - Select **Uses DNS to deliver mail** to allow ISVW to use the DNS server to forward the incoming mail to the network mail server.

Note: The IP address and port you specify here will depend on whether you have installed ISVW on the same machine as the SMTP server.

---

2. Select **Log incoming Message-ID** to track processed messages.

Note: ISVW logs the incoming Message-ID in the debug log. To enable the debug log:

1. Modify config.xml, which is located in the install folder. Set the value of \root\Common\Logging\DebugEnable to 1.

2. Restart the service.

If InterScan VirusWall and the SMTP server are on the same machine

SMTP VirusWall receives inbound SMTP traffic on port 25, scans it for viruses, and then routes it to the original SMTP server at a port other than 25, where it is received and processed as usual.

1. Modify the original SMTP server's configuration so that it no longer receives SMTP traffic on port 25. Change it to a free port such as 6000 or above.
2. On the Server Configuration screen, type localhost or 127.0.0.1 in **Forward mail to SMTP server at**.
3. In the Port field, specify the original SMTP server's new port number.

If InterScan VirusWall and the SMTP server are on different machines

If ISVW and the SMTP server are on different machines, the ISVW server must receive inbound messages first. There are a number of possible ways to accomplish this, including editing the MX record so that ISVW replaces the original SMTP server or swapping the two servers' IP addresses.

Choose a method and set the inbound message destination before configuring ISVW to forward scanned messages to the original SMTP server for delivery.

Configuring Outbound Messages

1. In the **Specify the IP address(es)** field, type the IP address of each SMTP server that will send outbound email to ISVW for processing.

   Separate multiple IP addresses with a semicolon. ISVW supports the following formats:

   - 192.168.5.*
   - 192.168.5.1-158
   - 192.168.5.242

   You can combine one or more of the formats and separate them with semicolons; for example: 192.168.3.*;192.168.5.2;192.168.5.148-245

   If ISVW and the SMTP server sending outbound mail are on the same machine, type both the actual IP address and 127.0.0.1.

Based on these IP addresses, ISVW differentiates between inbound messages, which are scanned for viruses and passed to the inbound SMTP server, and outbound messages, which are scanned and then routed to the outbound SMTP server. Typically, the original SMTP server IP address is among those entered in this field.

Select **Add customized disclaimer text to every outbound mail message** and then type a customized disclaimer message in the text field provided.

2. In **Specify how the outgoing mail will be delivered**, select an option depending on the following conditions:
   - If ISVW will handle the delivery of scanned, outbound mail, choose **Use DNS t**o deliver mail. This is the typical method of handling outbound mail after scanning, regardless of whether SMTP VirusWall is installed on the same machine as the SMTP server or a different one.
   - If another mail gateway or mail hub will handle delivery of scanned messages on behalf of ISVW, select **Forward mail to the SMTP server at** and type its IP address and port.

Using Mail Queuing

This option allows ISVW to accept messages and hold them in a queue for later scanning. This feature can be used during emergencies. For example, if a virus outbreak occurs, messages can be held until a solution to the outbreak is in place.

To use mail queuing:

1. On the left side menu, select **SMTP > Configuration**.
2. Under **Queue Mail**, select **Enable mail queuing** to start mail queuing and select whether you want to queue mail for inbound mail, outbound mail, or both.

Note: To scan and forward mail, you must disable mail queuing.

Advanced Configuration Options

Other configuration options include the following:

- *Maximum # of simultaneous SMTP client connections: __*

- *Maximum inbound and outbound message size: __*
- *When DNS delivery is used, attempt to send message every __ minutes for a maximum of __ hours before bouncing the message.*
- *Do not insert InterScan "Received" header in processed messages.*
- *Block relayed messages by accepting inbound mail only from the following domains: __*
- *Send the following SMTP greeting when a connection is established: __*

Maximum # of simultaneous SMTP client connections: __

ISVW can limit the total number of concurrent SMTP connections.

The default value is 25. A zero (0) in this field means the number of connections will be unlimited. If you are experiencing performance issues, you may want to allow fewer simultaneous SMTP client connections.

Maximum inbound and outbound message size: __

ISVW can reject inbound or outbound messages that are larger than a certain size. The rejection occurs during the SMTP transaction between the remote SMTP server and ISVW. The remote SMTP server generates the non-delivery report.

When DNS delivery is used, attempt to send message every __ minutes for a maximum of __ hours before bouncing the message.

You can specify the interval between attempts that ISVW makes to send messages when it uses DNS. You can also specify the period in which ISVW will attempt to send a message before returning the message as a "bounced" message.

ISVW records the delivery attempts and their results in the ISVW log file.

Do not insert InterScan "Received" header in processed messages.

After processing a message, ISVW inserts header information before forwarding it to the SMTP server, thus "signing" the message. This header information includes the date and time when ISVW received the mail message and its origination.

- When this option is enabled, you can completely mask ISVW processing.

- When the option is disabled, ISVW will write some additional header information during processing.

An example of the ISVW message header is as follows:

[Received: from 100.10.113.10 by us-washington.us-states

(InterScan VirusWall); Mon, 15 Jun 2009 11:49:34 -0800]

Block relayed messages by accepting inbound mail only from the following domains: __

To help secure the server against open-relay abuse, block relayed messages by accepting inbound mail addressed only to the domains you specify. Select this option and specify the domains for which you want to allow your SMTP server to relay messages. For example, if your company name is Widgets and your domain is widgets.com, type widgets.com in the text field.

Remember the following tips:

- Delimit multiple addresses with a semicolon (for example, `*.isvw.com; isvwtest.com`).
- Entries are not case sensitive.
- Use wildcards (*) to specify multiple subdomains.

Send the following SMTP greeting when a connection is established: __

By default, when you connect to ISVW using the SMTP service, it will reply back with the following greeting:

```
->telnet [machine name] 25
<-220 ISVW-EN2K3ET-A5 ISVW ESMTP ready at [date and time]
```

You can disable this option or customize it when you enable it.

Enabling SMTP Transaction Logging

Currently ISVW supports transaction logging for SMTP. Transaction logging for SMTP is enabled by default.

To enable or disable SMTP transaction logging:

1. Open the `Config.xml` file.
2. Search for the key named "WriteConnectionMsg" located under "SMTP".
3. Set "WriteConnectionMsg" value to "1" (enabled) or "0" (disabled).
4. Restart the service.

Chapter 5

Configuring HTTP Services

InterScan VirusWall (ISVW) allows you to monitor HTTP traffic to maintain security at your network gateway. You can enable or disable scanning of HTTP traffic during the installation process or at any time thereafter through the Summary page of the ISVW Web console.

Available HTTP services include:

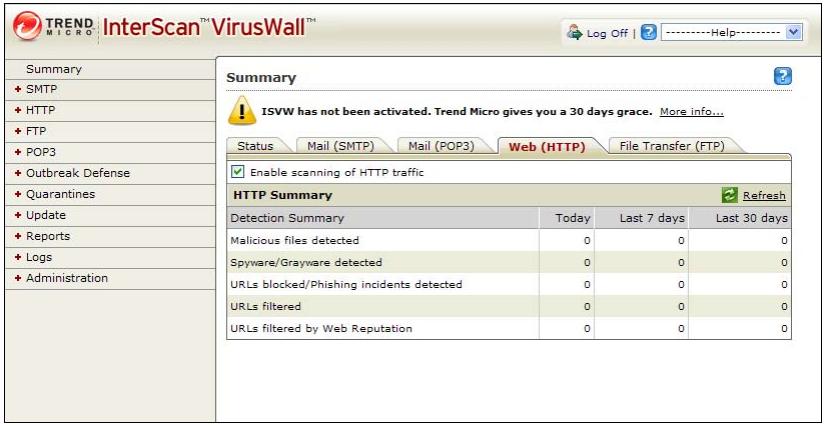
- Scanning for viruses and security risks in uploads and downloads
- Phishing site detection
- Spyware and other grayware detection
- URL blocking
- URL filtering
- Web Reputation
- Configuration of HTTP server mode and listening port

The Web (HTTP) tab on the ISVW Summary screen provides statistics concerning the number of infected files, spyware, grayware, and phishing incidents that ISVW HTTP scanning has detected in uploaded and downloaded files. The Summary screen also lists the number of URLs that have been blocked and filtered.

Enabling or Disabling HTTP Services

To enable or disable scanning services for HTTP protocol file downloads and uploads, select or clear the **Enable HTTP Traffic** check box on the Web (HTTP) tab on the Summary screen shown in *Figure 5-1*.

FIGURE 5-1. Web (HTTP) Summary Screen



HTTP scanning statistics for virus/malware detection, spyware/grayware detection, URL blocking/anti-phishing, and URL content filtering appear in the HTTP Summary table.

Configuring HTTP Virus Scan Settings

ISVW 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 different scanning methods at the HTTP gateway and set how ISVW scans compressed and large files to prevent performance issues and browser time-outs.

As an administrator, you can configure HTTP Scanning for viruses and other malware when you select **HTTP > Scanning**.

Enabling HTTP Virus Scanning

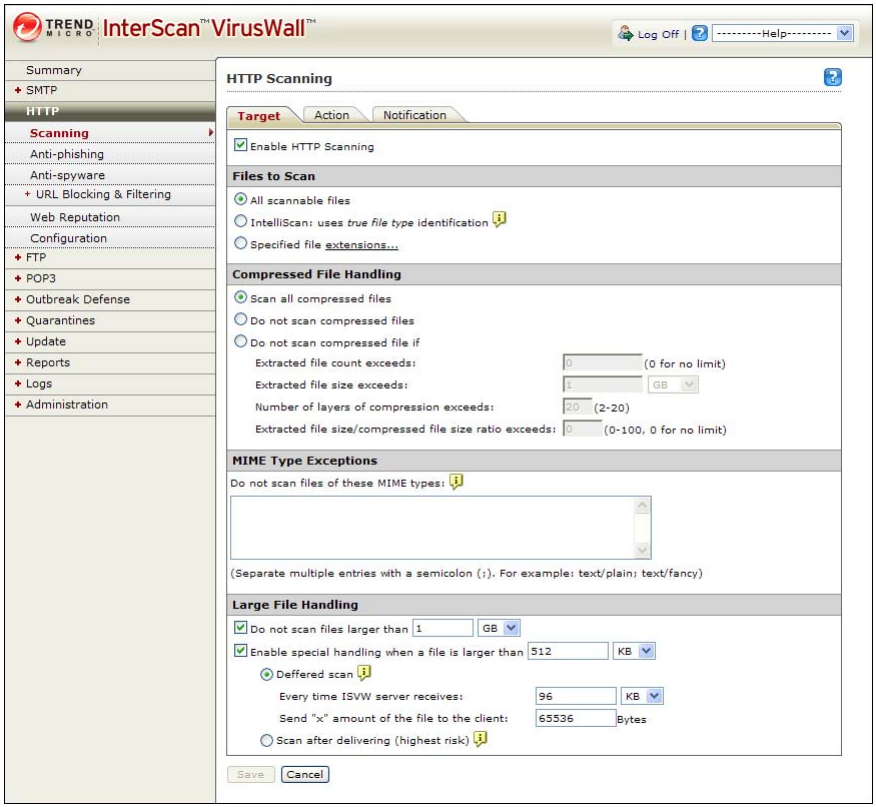
To enable HTTP virus scanning:

1. On the left side menu, select **HTTP > Scanning**.
2. Click the **Target** tab.
3. Select the **Enable HTTP Scanning** check box.
4. Click **Save**.

Specifying File Types to Scan

ISVW can check all file types or specified file types for viruses, including the individual files within compressed volumes. *Figure 5-2* shows the settings that you can specify when scanning files.

FIGURE 5-2. HTTP Virus Scanning Target Tab



To select the file types to scan:

1. On the left side menu, select **HTTP > Scanning** and click the **Target** tab.
2. Under "Files to Scan", select your preferred option:
   a. To scan all files, regardless of file type, select **All scannable files**. This is the most secure setting.
   b. To allow the product to intelligently identify the files to scan, select **IntelliScan: uses "true file type" identification**.

This option will pass some file types, which will result in higher performance, but will be less secure than when scanning all files.

c. To scan only files with specific extensions, select **Specified file extensions**. ISVW scans only files that have same extensions as those that are specified in the **Additional Extensions** text box.

By default, ISVW scans files with the following file name extensions:

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

Tip: Use the Specified file extensions option to modify the default scan list.

3. Click **Save**.

Note: The scan type and compressed file handling options apply to all types of file scans, including virus and spyware.

Compressed File Handling

To specify how ISVW processes compressed files during HTTP scanning:

On the left menu, select **HTTP > Scanning** and click the **Target** tab.

- To scan all compressed files, select **Scan all compressed files**. This is the most secure configuration.
- To skip scanning of all compressed files, select **Do not scan compressed files**. ISVW will not scan any compressed files.
- To scan compressed files within user-specified limits, select **Do not scan compressed files if:**, and specify the conditions when compressed files should not be scanned.

- **Extracted file count exceeds**—the maximum number of files within the compressed file; (0 means no limit). ISVW does not scan any files in the compressed file.
- **Extracted file size exceeds**—the maximum file size after decompression. ISVW scans only individual files within the limit.
- **Number of layers of compression exceeds**—the maximum number of compression layers. For instance, if a ZIP file contains a RAR file, and that file contains another compressed file, there would be three layers. ISVW does not scan any files in the compressed file.
- **Extracted file size/compressed file size ratio exceeds**—the maximum size ratio before and after compression. ISVW scans only individual files within the limit.

Note: The scan type and compressed file handling options apply to all types of file scans, including virus and spyware/grayware.

MIME Type Exceptions

To improve data throughput rates, you can configure ISVW to skip scanning files with MIME types that present a low risk of harboring viruses. For example, if you type audio/aiff, afc files will not be scanned.

However, since MIME types can be easily forged, ISVW verifies that a file really is the indicated MIME type through true file type checking. Small files that would otherwise not be scanned due to their MIME type are always scanned.

Table 5-1 shows the file types that you can enter in the HTTP virus scanning policy **MIME Type Exceptions** field to prevent scanning of the corresponding MIME content types.

TABLE 5-1. Mapping File Types to MIME Types

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
afc	audio/aiff	av	video/avs-video	bin	application/x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/binhex
ani	application/octetstream	base64	application/base64	binhex	application/binhex4
arc	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex
arj	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex40
asf	video/x-ms-asf	bin	application/octetstream	binhex	application/x-binhex40
bin	application/xmacbinary	bmp	image/bmp	bmp	image/x-windowsbmp
bw	image/x-sgi-bw	bzip2	application/x-bzi2	cgm	image/cgm
cmx	application/x-cmx	cmx	image/x-cmx	com	application/octetstream
core	application/octetstream	cpio	application/x-cpio	dcr	application/x-director
doc	application/wordperfect	dwg	application/acad	dwg	application/x-acad
dwg	drawing/x-dwg	dwg	image/vnd.dwg	dwg	image/x-dwg

TABLE 5-1. Mapping File Types to MIME Types (Continued)

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
eps	application/ postscript	eps	image/x-eps	exec	application/ octetstream
exec	application/ x-msdownload	exe	application/ octetstream	fh9	image/x-freeha nd
fli	video/x-fli	fm	application/ vnd.framem aker	gif	image/gif
gzip	application/x-gzip	gzip	encoding/x-g	hpexe	application/ octetstream
iff	audio/x-aiff	java	text/x-javas ource	java	application/ java-class
java	application/ x-javaapplet	java	application/ x-javavm	java	text/x-javasour ce
java	application/ java-class	java	application/ x-javaapplet	java	application/ x-javavm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	applica-tion/x-lha
lisp	application/x-lisp	maud	audio/x-ma	ud	midi audio/midi
mif	application/x-mif	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpe g-3	mp3	video/mpeg
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/ x-cainetwin32-x86
msdoc	application/ msword	msexl	applica-tion/excel	msexl	application/ x-msexcel

TABLE 5-1. Mapping File Types to MIME Types (Continued)

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
msexl	application/ x-excel	msexl	application/ vnd.ms-exc el	msmdb	application/ x-msaccess
msppt	application/ mspowerpoint	msppt	application/ powerpoint	msppt	application/ vnd.mspower-point
msproj	application/ vnd.msproject	msproj	application/ x-msproject	msproj	application/ x-project
mswri	application/ mswrite	pcx	image/x-pcx	pdb	application/ x-pilot-pdb
pdf	application/pdf	pdf	applica-tion/x-pdf	pfb	applica-tion/x-font
pict	image/pict	pict	image/x-pict	picture	image
png	image/png	ppm	image/ x-porta-blepixmap	ps	application/ postscript
psd	application/ octetstream	qtm	video/quick-time	ra	audio/ vnd.mrealau-dio
ra	audio/ xpnrealaudio	ra	audio/xre-alaudio	rar	application/rar
ras	image/ x-cmuraster	ras	image/cmu-raster	risc	application/ octetstream
rmf	application/ vnd.m-realme-dia, g_audiovideo	rtf	applica-tion/rtf	rtf	application/x-rtf
rtf	text/rich text	scm	application/ vnd.lotuss-creencam	scm	application/ x-lotusscreen-cam

TABLE 5-1. Mapping File Types to MIME Types (Continued)

File Type	MIME Content Type	File Type	MIME Content Type	File Type	MIME Content Type
scm	application/ x-screencam	scm	video/x-scm	sf	audio/x-sf
swf	application/ x-shock-wave-flash	tar	applica-tion/x-tar	tga	image/tga
tiff	image/tiff	tnef	applica-tion/ms-tnef	tnef	application/ vnd.mstnef
txt	text/plain	uuen-code	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

Large File Handling

With large files, the nature of virus scanning causes the download time to double (that is, the time to transfer the entire file to ISVW, scan the file, and then transfer the entire file to the client). In some environments, the extra download time may not be acceptable. Other factors such as network speed and server capability must be considered. If the file is not big enough to trigger large-file handling settings, the file will be scanned as a normal file.

When downloading a large file, the time to download the file and scan it for viruses may be long enough to cause the browser to time out. The size of file that you should consider "large" varies, depending on the hardware where ISVW is installed, the mix of file types in the particular environment, and other factors. Trend Micro recommends that files larger than 512 KB (default value) be considered large and files larger than 2097151 KB (about 2 GB) not be scanned; however, these values might vary depending on your network speed, server capability, and security requirements.

The following settings apply to large file handling:

- **Do not scan files larger than**—sets the maximum file size for scanning. ISVW will not scan files larger than the size specified. The default is 1 GB.
- **Enable special handling when a file is larger than**—defines the minimum size at which a file will be treated as a large file and receive special handling. There are two types of special handling:
  - **Deferred scan:** loads part of the page while scanning; stops the connection if a virus is found
    - **Every time ISVW server receives** controls how often data is passed to the requesting client as a file downloads to the ISVW server. This data prevents the requesting browser from timing out.
    - **Send x amount of file to the client** controls the amount of data released to the requesting client. For example, assume the following configurations:
    - Every time ISVW server receives = 512KB
    - Send x amount of file to the client = 1024Bytes

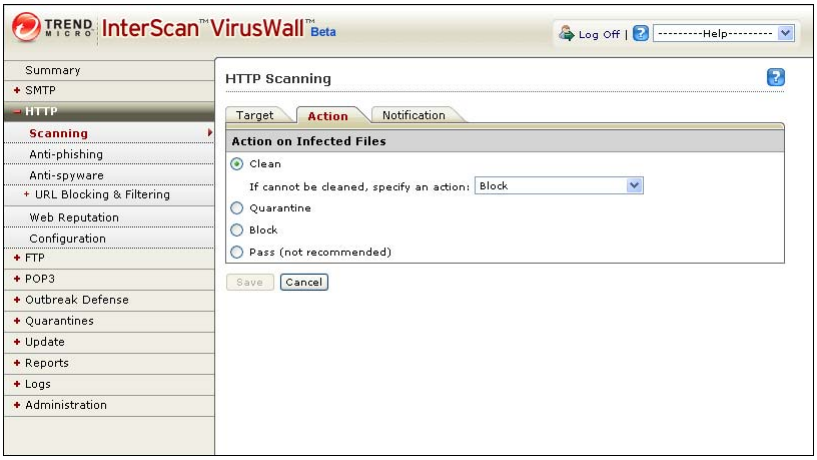
      When downloading a large file, 1024 bytes of data are released to the requesting client for every 512KB that is downloaded to the ISVW server.
  - **Scan after delivering**: loads the page first, and then scans afterward (highest risk of infection). If you don't enable special handling for large files, ISVW will first scan the file and then load the page.

4. Click **Save**.

Specifying the Action to Take upon Virus Detection

When ISVW detects an infected file, it can perform one of six actions, as shown in *Figure 5-3*.

FIGURE 5-3. HTTP Scanning Action Tab



- **Clean + Quarantine**—ISVW will attempt to clean the infected file. If it cannot clean the file, ISVW will move it to the quarantine directory and notify the user.
- **Clean + Block**—ISVW will attempt to clean the infected file. If it cannot clean the file, ISVW will delete the file and notify the user.
- **Clean + Pass (not recommended)**—ISVW will attempt to clean the infected file. If it cannot clean the file, ISVW will allow the infected file to pass.
- **Quarantine**—ISVW will quarantine this file and notify the user.
- **Block**—ISVW will delete the infected file.
- **Pass (not recommended)**—ISVW will allow the infected file to pass.

To specify the action to take upon detection of infected files:

1. On the left side menu, select **HTTP > Scanning** and click the **Action** tab.
2. Under **Action on Infected Files**, select your preferred option:
   - Select **Clean** to always clean the infected file and deliver it to the recipient. Then, select the action to take when infected files cannot be cleaned:
     - **Quarantine**—removes and quarantines infected files
     - **Block**—removes infected files without quarantining them
     - **Pass (not recommended)**—delivers the infected file.

- Select **Quarantine** to move, without cleaning, the infected file to the quarantine directory. The recipient will not receive the infected file.
- Select **Block** to delete the infected file. The recipient will not receive the infected file.
- Select **Pass (not recommended)** to deliver the infected file to the recipient.

3. Click **Save**.

Note: The default quarantine folder for HTTP scanning is \quarantine\http.

Specifying the Virus Scan Notification Message

When ISVW quarantines or blocks a file, it will display a notification message in the user's Web browser. You can modify the message text for the User Notification.

To configure the notification message:

1. On the left side menu, select **HTTP > Scanning** and click the **Notification** tab.
2. Type the message you want ISVW to send.
3. Click **Save**.

Configuring HTTP Anti-Phishing Settings

Phish, or *phishing*, is a rapidly growing form of fraud that mimics a legitimate Web site and seeks to fool Web users into divulging private information. Phishing attacks involve email messages that falsely claim to be from an established, legitimate organization. The messages typically encourage recipients to click on a link that will redirect their browsers to a fraudulent Web site, where they are asked to update personal information. Victims usually give up passwords, social security numbers, and credit card numbers.

In a typical scenario, unsuspecting users receive an urgent sounding (and authentic looking) email telling them that there is a problem with their account that they must immediately fix, or the account will be closed. The email will include a URL to a Web site that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate Web site but then change the back end—where the collected data is actually sent.

Enabling HTTP Anti-Phishing

To enable the HTTP anti-phishing feature:

1. On the left side menu, select **HTTP > Anti-phishing** and click the **Target** tab, shown in *Figure 5-4*.

   FIGURE 5-4. HTTP Anti-phishing Target Tab

2. Select the **Enable HTTP anti-phishing** check box.
3. Choose the types of phish categories that ISVW should protect against.

Note: The Spyware option is different from the spyware scanning option in **HTTP > Anti-spyware > Action**.

---

4. Click **Save**.

Specifying the Action to Take When Phishing are Detected

You can specify whether to block or allow access for detected phishing sites.

To specify the action on phishing sites:

1. On the left side menu, select **HTTP > Anti-phishing** and click the **Action** tab.
2. Select the action for phishing sites:
   - Select **Block** to block access to the site.
   - Select **Allow (not recommended)** to allow users access to the site.
3. Click **Save**.

Specifying the Notification Message when a Phishing Site Is Detected

When ISVW detects a phishing site, it will display a notification message in the user's Web browser. You can modify the message text for the User Notification. You can also report suspected or known phishing sites to TrendLabs.

Specifying the User Notification

To configure the notification message:

1. On the left side menu, select **HTTP > Anti-phishing** and click the **Notification** tab.
2. Type the message you want ISVW to send.
3. Click **Save**.

Reporting a Potential Phishing URL

You can report suspected or known phishing sites to TrendLabs. Click **Submit a Potential Phishing URL to TrendLabs** and provide the URL in an email that you will send to antifraud@support.trendmicro.com.

TrendLabs monitors sites that obtain information for fraudulent purposes and distributes known phishing site information as part of the automatic updates that Trend Micro makes available to ISVW customers.

Configuring HTTP Anti-Spyware Settings

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular updates in a pattern file.

Some common types of grayware include:

Type of grayware	Typical Function
Spyware	gathers data, such as account user names and passwords, and transmits them to third parties
Adware	displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser
Dialers	changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	helps hackers enter computers
Remote Access Tools	help hackers remotely access and control computers
Password Cracking Applications	helps hackers decipher account user names and passwords
Others	other types not covered above

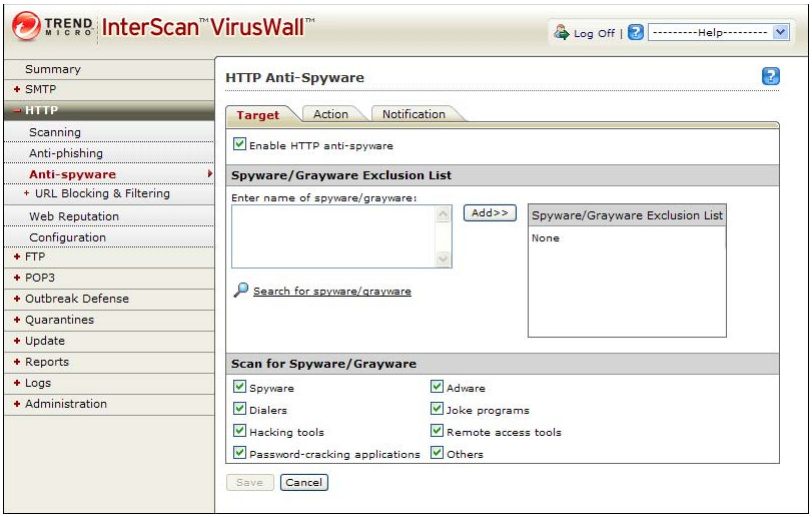
Enabling HTTP Spyware Scanning

To enable HTTP spyware scanning:

1. On the left side menu, select **HTTP > Anti-spyware** and click the **Target** tab.
2. Select the **Enable HTTP Anti-spyware** check box.
3. Click **Save**.

Figure 5-5 shows the HTTP Anti-spyware Target tab, which allows you to enable HTTP spyware scanning and specify spyware scanning exclusions.

FIGURE 5-5. HTTP Anti-spyware Target Tab



Setting the Spyware Scanning Exclusion List

To list specific file names or file name extensions to exclude from spyware/grayware scanning:

1. On the left side menu, select **HTTP> Anti-spyware** and click the **Target** tab.
2. In **Enter name of spyware/grayware**, type the spyware name you want to exclude from spyware/grayware scanning.

   If you are not sure of the spyware name, click the **Search for spyware/grayware** link.
3. Click **Add**.
4. Click **Save**.

Note: To delete entries on the exclusion list, click the trash bin icon. Click **Save** to finalize changes.

Specifying Spyware and Grayware Types to Scan

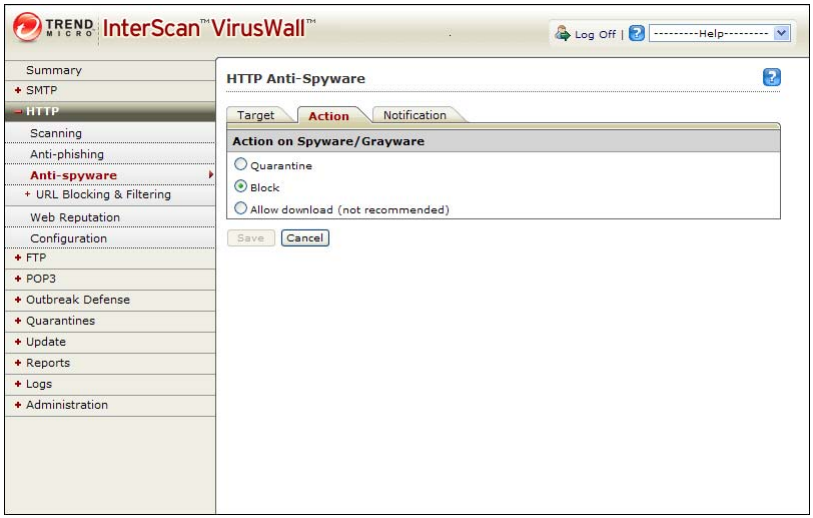
To specify the types of spyware and grayware for which you want ISVW HTTP services to scan:

1. On the left side menu, select **HTTP > Anti-spyware** and click the **Target** tab.
2. Under **Scan for spyware/grayware**, select the types of spyware and grayware for which HTTP services will scan.
3. Click **Save**.

Specifying the Action to Take upon Spyware Detection

You can select one of three actions for ISVW to take when it detects spyware or other grayware.

FIGURE 5-6. HTTP Anti-spyware Action Tab



To specify the action to take when ISVW detects spyware or grayware:

1. On the left side menu, select **HTTP > Anti-spyware** and click the **Action** tab.
2. Under **Action on Spyware/Grayware**, select one of the following options:

- Select **Quarantine** to move the spyware/grayware file to the quarantine directory. The user will not receive the file.
- Select **Block** to prevent the file transfer of spyware/grayware programs. The user will not receive the file.
- Select **Allow download (not recommended)** to send the spyware/grayware to the intended recipient.

3. Click **Save**.

Specifying the User Notification Message When Spyware/Grayware Is Detected

When ISVW quarantines or blocks a file, it will display a notification message in the user's Web browser. You can modify the message text for the User Notification.

To specify the notification message when ISVW detects spyware or grayware:

1. On the left side menu, select **HTTP > Anti-spyware** and click the **Notification** tab.
2. Type the message you want ISVW to send.
3. Click **Save**.

HTTP URL Blocking and Filtering

ISVW can block access to Web sites with undesirable content through a user-configured block list. It can also apply exceptions to this list.

ISVW has a policy framework that allows the association of URL Filtering and Blocking policies to specific groups or individual users based on the user or group identity (see *Selecting the User Identification Method* on page 13-15). This feature includes the following:

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

ISVW supports up to 20 URL Filtering and Blocking policies for users and groups. The Domain Controller Agent software can be deployed on a Domain Controller Server or Windows machine that is on the Intranet. The agent communicates with ISVW over port 65015, a secure TCP port, and works with Microsoft Active Directory.

Note: In a situation where there are multiple policies for a user or group, if the traffic matches the policy with the higher priority, then the action taken is based on this policy while ISVW ignores the other policies.

Managing the Global URL Blocking and Filtering Policy

ISVW is pre-configured with a default URL blocking and filtering policy—the Global Policy. This policy applies to all clients on the network. It uses listening port 8080.

The Global Policy has the following 12 default categories selected for the Internet Security group:

- Proxy Avoidance
- Spyware
- Phishing
- Adware
- Malware Accomplice
- Disease Vector
- Cookies
- Dialers
- Hacking
- Joke Program
- Password Cracking
- Remote Access Program

To make Global Policy changes, see *Modifying an Existing URL Blocking and Filtering Policy* on page 5-28.

Changing the URL Blocking and Filtering Policy Priority

To change policy priority:

1. Choose **HTTP > URL Blocking & Filtering > Policies**.
2. From the "Priority" column click the down arrow to move the policy down in priority and click the up arrow to move a policy up in priority.

   The higher a policy is located in the list, the greater its priority.

Creating a New URL Blocking and Filtering Policy

Creating a new URL blocking and filtering policy is a four-part process:

- Specify Policy Information
- Specify Target Clients
- Specify URL Blocking Rules
- Specify URL Filtering Rules

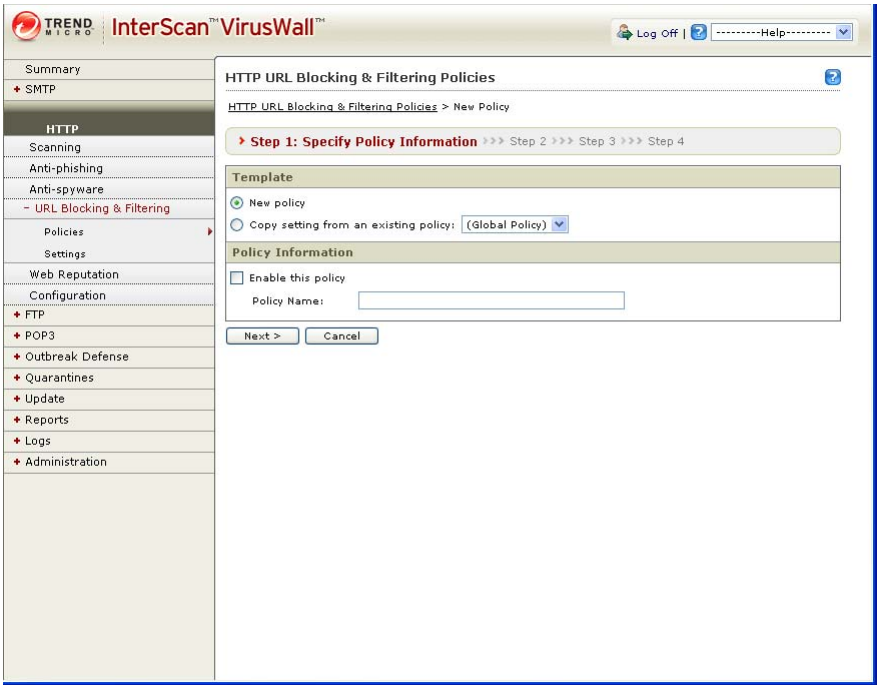
To create a new URL blocking and filtering policy:

Step 1. Specify the policy information.

1. Choose **HTTP > URL Blocking & Filtering > Policies**.
2. In the HTTP URL Blocking & Filtering Policies screen, click **New Policy**.

   The HTTP URL Blocking & Filtering Policies screen shows the first step of the procedure (see *Figure 5-7*).

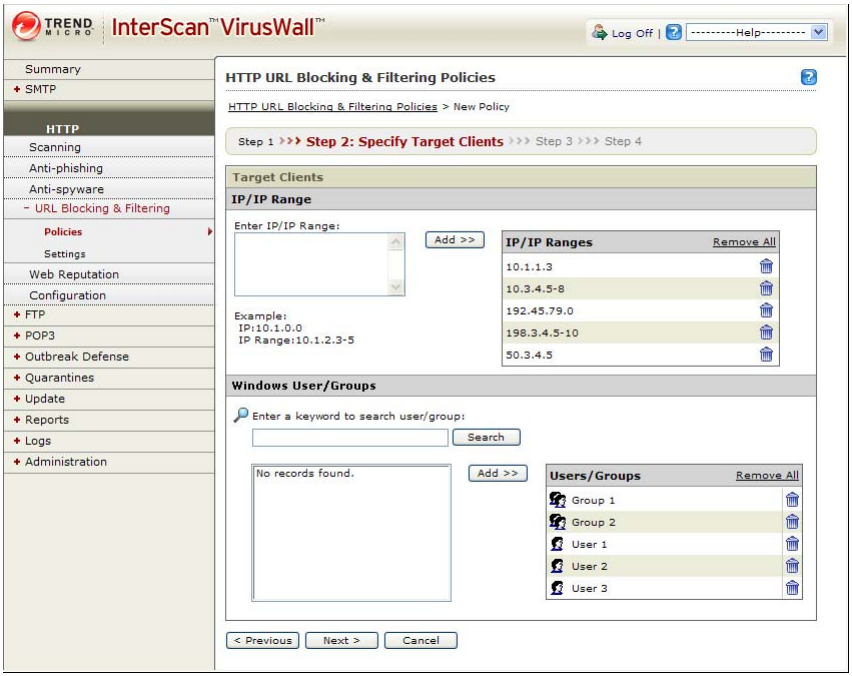
FIGURE 5-7. HTTP URL Blocking & Filtering Policies screen displaying Step 1: Specify Policy Information



3. In the Template area, determine if you want to create a new policy based on an existing policy or not.
4. In the Policy Information area, specify a name for the new policy and then determine if you want to enable the policy when you are done creating it.
5. Click **Next**.

   The HTTP URL Blocking & Filtering Policies screen shows the second step of the procedure (see *Figure 5-8*).

FIGURE 5-8. HTTP URL Blocking and Filtering Policies screen displaying Step 2: Specify Target Clients



Step 2. Specify the target client(s) of the URL blocking and filtering policy.

6. Specify the target client(s) of the URL blocking and filtering policy.

See *Selecting the User Identification Method* on page 13-15 to identify individual users and groups for URL filtering and blocking policies.

Note: You can search for a user or group using the **Enter a keyword to search user/group** field. ISVW automatically adds a hidden asterisk (*) at the end of the text you type to broaden the search. If no match is found, "no records found" appears in the **Users/Groups** text box.

To specify a target client by IP address:

- Type the IP address or IP address range in the **Enter IP/IP Range** field in the "IP/IP Range" area.
- Click **Add** and the IP address or IP address range appears in the "IP/IP Ranges" table.

To remove an IP address or IP address range, click the trash can icon located in the same row as the desired IP address or IP address range.

To specify a target client by user or group name:

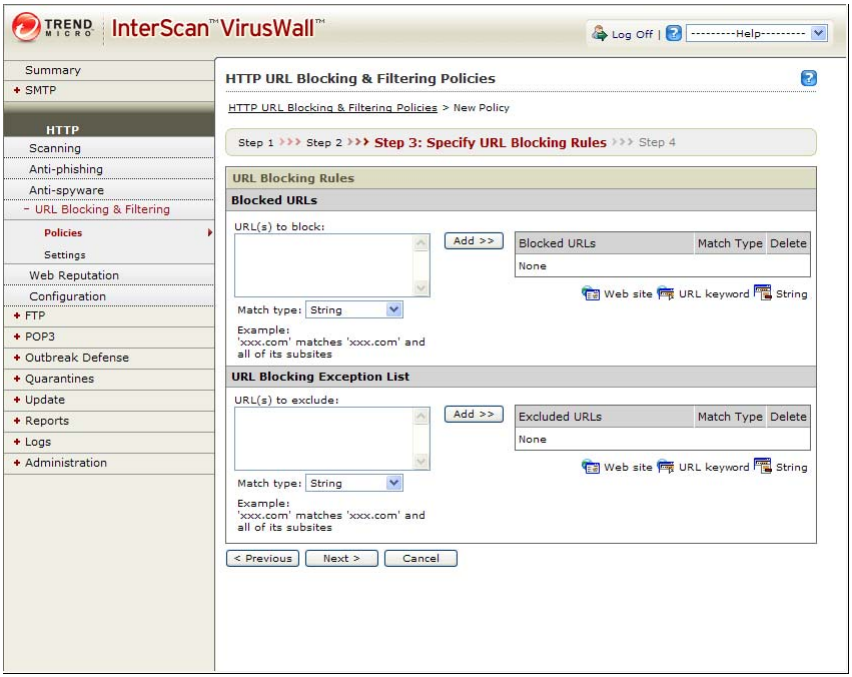
- Type the desired name in the search field in the "Windows User/Groups" area and then click **Search** to locate the target client. The located target client appears in the list.
- Click **Add** and the target client appears in the "Users/Groups" table.

To remove a user or group name, click the trash can icon located in the same row as the desired user or group name.

7. Click **Next** after specifying the target client information.

The HTTP URL Blocking & Filtering Policies screen shows the third step of the procedure (see *Figure 5-9*).

FIGURE 5-9. HTTP URL Blocking & Filtering Policies screen displaying Step 3: Specify URL Blocking Rules



Step 3. Specify a URL to block.

8. To specify a URL to block, select the match type from the **Match type** drop-down list in the "Blocked URLs" area and then enter the correct information in the **URL(s) to block** scroll box.

   Match types include the following:

   - **Web site** - The URL of a Web site you want blocked.
   - **URL keyword** - A word used in the URL of multiple Web sites that you want blocked.

- **String** - The exact-match URL string.

9. Click **Add**.

   The URL appears in the "Blocked URLs" table. Below the table is a legend that describes the URL type.

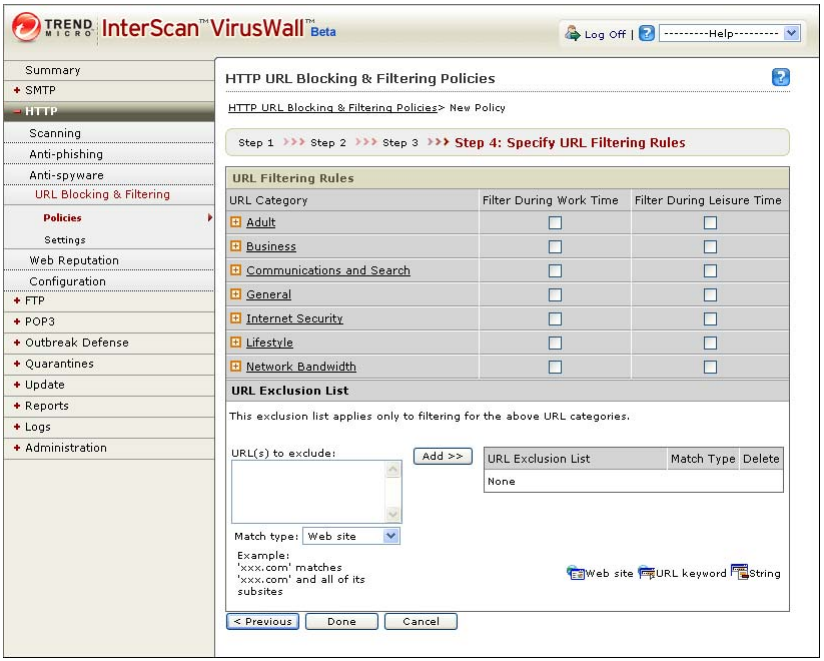
10. To specify a URL exception, complete the necessary information in the "URL Blocking Exception List" area.

    This procedure is similar to specifying a URL to block. (See Step 8 and Step 9 for complete details.)

11. Click **Next**.

The HTTP URL Blocking & Filtering Policies screen shows the fourth step of the procedure (see *Figure 5-10*).

FIGURE 5-10. HTTP URL Blocking & Filtering Policies screen displaying Step 4: Specify URL Filtering Rules



Step 4. Select the URL categories to which you want to restrict access.

12. From the "URL Filtering Rules" area, 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. The group does not need to be expanded for you to select all categories in a group.
    - Select the check box of the category that you want to blocked during leisure time. The group does not need to be expanded for you to select all categories in a group. Unspecified times are considered "leisure" times.

See *Scheduling URL Filtering* on page 5-30 to specify restricted days and hours.

13. To specify a URL category exception, complete the necessary information in the "URL Exclusion List" area.

    This procedure is similar to specifying a URL to block. (See Step 8 on page 5-25 and Step 9 on page 5-26 for complete details.)

14. Click **Done**.

    ISVW returns you to the User Group Policies view of the HTTP URL Blocking & Filtering Policies screen. Here the new policy is listed. Once a policy is created, you are still able to make changes to it (see *Modifying an Existing URL Blocking and Filtering Policy* on page 5-28).

To enable URL filtering and URL blocking at the global level, set the scanning schedule, and specify the notification message, see *Settings for URL Blocking and Filtering* on page 5-29.

Modifying an Existing URL Blocking and Filtering Policy

The procedure in this section can be used to modify the global policy and a policy that you created.

To modify a URL blocking and filtering policy:

1. Choose **HTTP > URL Blocking & Filtering > Policies**.

   The HTTP URL Blocking & Filtering Policies screen appears.

2. From the User Group Policies table, click the desired policy.

   The HTTP URL Blocking & Filtering Policies screen appears with the Target Clients tab active.

3. To change the name of the policy, type in the Policy Name field the desired name.

   You can make this name change while in any tab of the HTTP URL Blocking & Filtering Policies screen

4. To disable the policy, uncheck the **Enable this policy** check box.

   You can make this change while in any tab of the HTTP URL Blocking & Filtering Policies screen

Note: In order to use the URL blocking and filtering policies that you create, you need to enable URL blocking and filtering at the global level in the HTTP URL Blocking & Filtering Settings screen (see *Enabling URL Blocking and Filtering* on page 5-29)

5. To add or delete target clients, make the appropriate changes in the Target Clients tab of the HTTP URL Blocking & Filtering Policies screen and then click **Save** after making your changes.

   See Step 2 for complete details.

6. To add or delete URL blocking rules:
   - Click the URL Blocking Rules tab and then make the appropriate changes in the HTTP URL Blocking & Filtering Policies screen (URL Blocking Rules tab).
   - Click **Save** after making your changes.

   See the Step 3 for complete details.

7. To add or delete URL filtering rules:
   - Click the URL Filtering Rules tab and then make the appropriate changes in the of the HTTP URL Blocking & Filtering Policies screen (URL Filtering Rules tab).
   - Click **Save** after making your changes.

   See Step 4 for complete details.

Settings for URL Blocking and Filtering

Enabling URL Blocking and Filtering

In order to use the URL blocking and filtering policies that you create, you need to enable URL blocking and filtering at the global level in the HTTP URL Blocking & Filtering Settings screen. ISVW allows you to enable URL blocking or URL filtering or both.

To enable URL blocking and URL filtering:

1. Choose **HTTP > URL Blocking & Filtering > Settings**.
2. In the "Scan Status" section of the HTTP URL Blocking & Filtering Settings screen, select the desired check box(es).
3. Click **Save**.

Scheduling URL Filtering

To schedule URL filtering:

1. Choose **HTTP > URL Blocking & Filtering > Settings**.

   The HTTP URL Blocking & Filtering Settings screen opens.
2. In the "URL Filtering Work Hours" area, select the work days and work times.
3. Click **Save**.

Specifying the Message for Blocked URLs

To specify a message for blocked URLs:

1. Choose **HTTP > URL Blocking & Filtering > Settings**.

   The HTTP URL Blocking & Filtering Settings screen opens.
2. In the "User Notification" area, type in free-flow text box the message you want to display when a blocked URL is encountered.
3. Click **Save**.

Reclassifying a URL

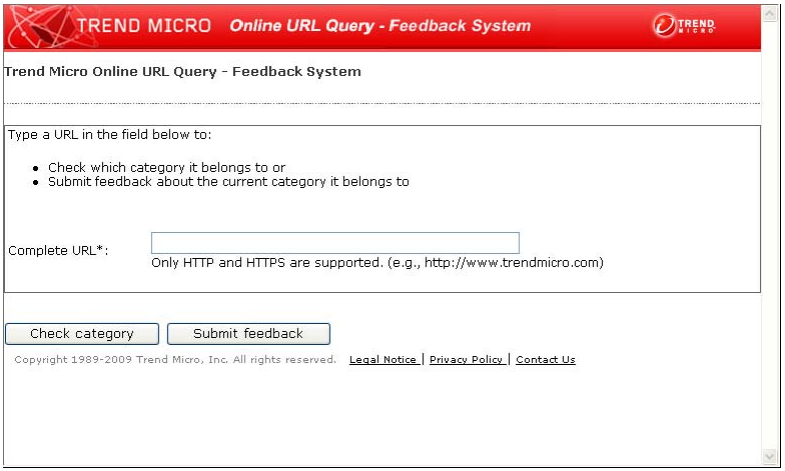
To reclassify a URL:

1. Choose **HTTP > URL Blocking & Filtering > Settings**.

   The HTTP URL Blocking & Filtering Settings screen opens.
2. In the "URL Reclassification" area, click **Submit URL to TrendLabs for Reclassification**.

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

FIGURE 5-11. The Trend Micro Online URL Query - Feedback System screen



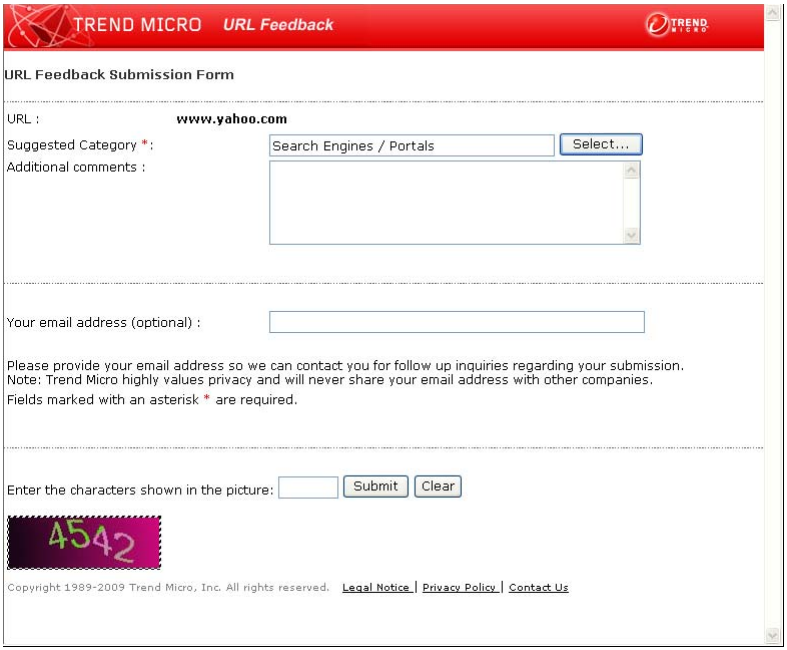
3. Enter the URL in question in the **Complete URL** field.

   You can check the current category of the URL in question by clicking **Check category**.

4. Click **Submit feedback**.

   The URL Feedback Submission Form screen opens.

FIGURE 5-12. The URL Feedback Submission Form screen



5. Click **Select** to choose a different URL category.
6. Type any comments in the **Additional comments** free-flow text field.
7. Type in the **Enter the characters shown in the picture** field the characters displayed in the picture.
8. Click **Submit**.

   The URL Feedback window opens. This screen provides you with links to other Trend Micro Web sites in case you need further assistance.
9. Click **Return Home**.
10. Close the Trend Micro Online URL Query - Feedback System screen to return to the HTTP URL Blocking & Filtering Settings screen.

Deleting a URL Blocking and Filtering Policy

To delete a URL blocking and URL filtering policy:

1. Choose **HTTP > URL Blocking & Filtering > Policies**.

   The HTTP URL Blocking & Filtering Policies screen opens.
2. From the User Group Policies table, select the check box of the desired policy and then click **Delete**.
3. Click **Save**.

   Click **Cancel** to un-do the deletion.

Web Reputation

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

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

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

Using Trend Micro Web Reputation technology (part of the Smart Protection Network), you perform Web site scanning at varying levels of protection (low, medium, and high) and add Web sites to the Exceptions List (HTTP > Web Reputation > Target tab > URL Exception List section) so that Web sites can be viewed without scanning or blocking (`yourcompany.com`, for example).

Note: Pre-approving Web sites must be done carefully. Not scanning or blocking a Web site could pose a security risk.

Anti-phishing Using Web Reputation

ISVW provides HTTP anti-phishing through the following:

- **PhishTrap** — This is the primary anti-phishing technology used in ISVW. From the HTTP > Anti-phishing screen, you specify how PhishTrap operates. PhishTrap works in conjunction with ISVW to monitor outbound client URL requests and compare them to a known list of phish sites. Whenever a match occurs, PhishTrap blocks access to the site. When a site is blocked by PhishTrap, the user receives a notification message.
- **Anti-phishing category of URL Filtering** — This is the secondary anti-phishing technology used by ISVW. ISVW can block access to Web sites with undesirable content through a user-configured block list. Since there is only one notification message that is used for all URL blocking and URL filtering (for all categories), the notification message for detecting anti-phishing using URL filtering cannot be specific to anti-phishing (unless URL blocking was disabled and only the anti-phishing category of URL filtering was enabled).
- **Web Reputation** — This is the last means used by ISVW to perform anti-phishing. For each accessed URL, ISVW queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level. Sites blocked by Web Reputation do not necessarily fall into the anti-phishing category. Phishing sites (and other sites) blocked by Web Reputation will provide a "low reputation" message.

Web Reputation Database

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

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

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

Likewise, you can click HTTP > Web Reputation > Notification > **Submit URL to TrendLabs for Reclassification**.

Web Reputation Settings

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

Web Reputation settings involve specifying the following:

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

Security Sensitivity Level

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

To set the security sensitivity level:

1. Go to the HTTP > Web Reputation > Target tab.
2. Click **Enable HTTP real-time Web Reputation checking**.

   This check box is selected by default.
3. Specify the URL blocking sensitivity level (High, Medium, or Low).
4. Click **Save**.

Web Reputation Exceptions

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

WARNING! **Lack of scanning could cause security holes if a Web site on the Approved list has been hacked and had malicious code injected.**

To specify Web Reputation exceptions:

1. Go to the HTTP > Web Reputation > Target tab > URL Exclusion List section.
2. In the **URL(s) to exclude** box, type the URL text.
3. In the **Match type** drop-down list, select the option that describes the URL text.
4. Click **Add** to add the URL to the URL Exclusion List.
5. Click **Save**.

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

HTTP Configuration

Before you can start monitoring HTTP traffic, you must specify the configuration settings for your HTTP server. ISVW can protect your users and network resources from HTTP-borne risks in one of these modes:

- As a forward proxy in standalone mode
- As a secondary proxy in dependent mode
- As a reverse proxy in reverse mode
- As a transparent proxy when an L4 switch is installed

In all configurations, ISVW resides between the clients and a Web server.

Standalone Mode

The standalone mode configuration protects 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 standalone proxy topology shown in *Figure 5-13*, ISVW and the clients that it protects are typically installed within the same LAN.

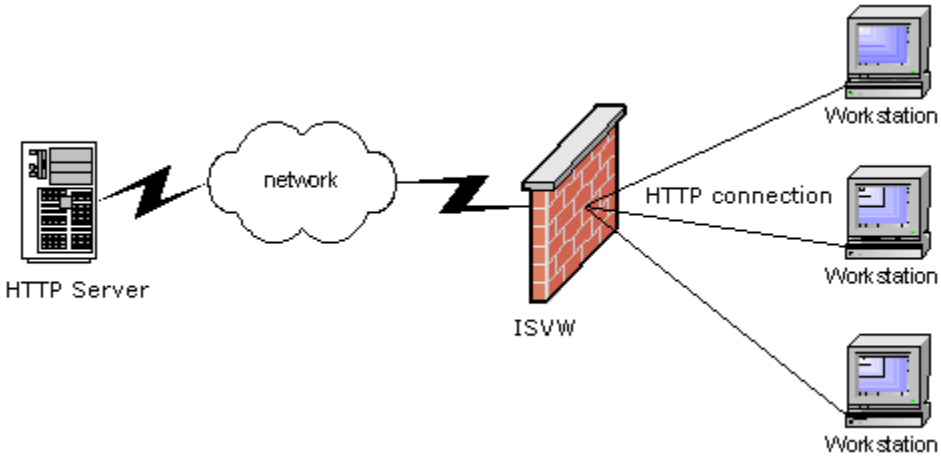


FIGURE 5-13. Standalone Mode Topology

Dependent Mode

Dependent mode is similar to standalone mode, except that ISVW depends on an upstream proxy to access the HTTP server, as shown in *Figure 5-14*.

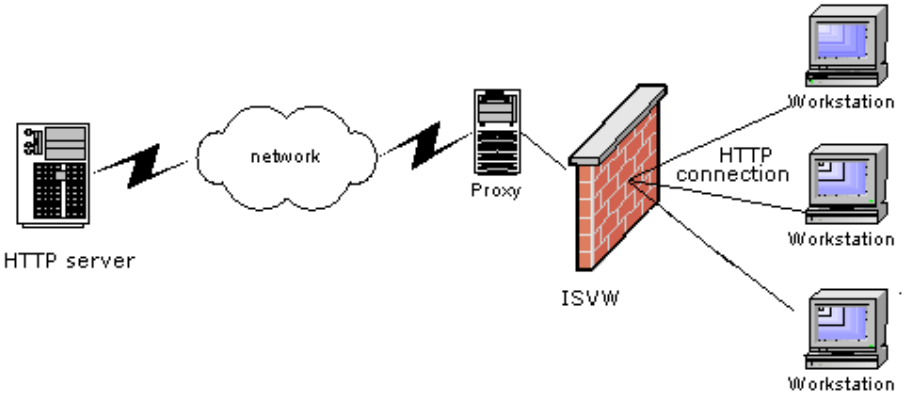


FIGURE 5-14. Dependent Mode Topology

Reverse Mode

The reverse mode configuration places ISVW between a Web server and the clients of that server. This is a less common configuration, and is typically used to protect Web servers from having malicious content uploaded to them. In the reverse mode proxy topology, ISVW is typically installed close to the Web server that it protects and is separated from the clients by the Internet.

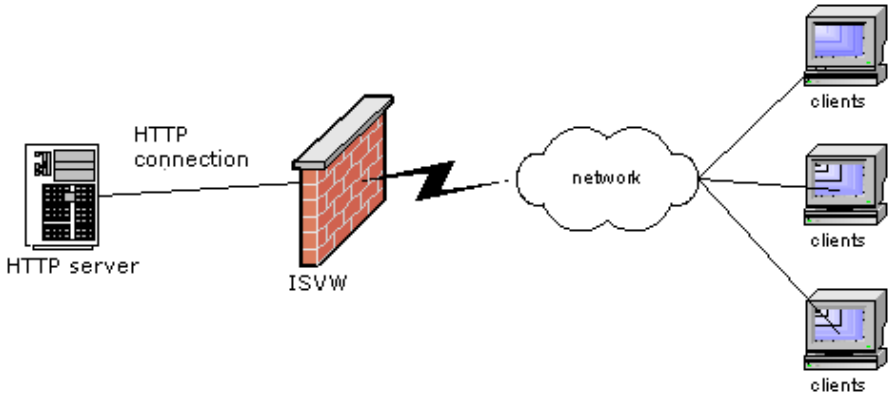


FIGURE 5-15. Reverse Mode Topology

Transparent Mode

ISVW supports HTTP proxy transparency mode when an L4 switch is used. ISVW is transparent to the user. In this mode, ISVW settings are the same as when in reverse mode or even standalone mode depending on the network topology.

Note: Web Cache Control Protocol (WCCP) is not supported.

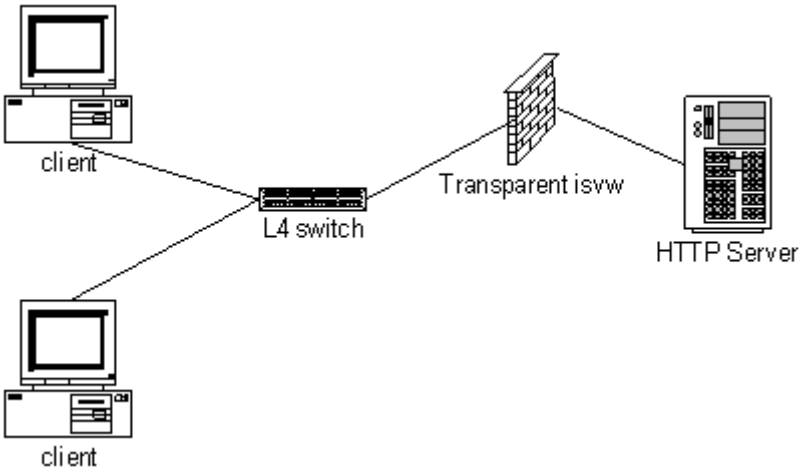


FIGURE 5-16. Transparent Mode Topology

Configuring the HTTP Proxy Settings

Before ISVW can monitor HTTP traffic, you need to specify the configuration settings for the HTTP server.

To configure the HTTP proxy settings for ISVW:

1. On the left menu, select **HTTP > Configuration**.
2. Select the mode.
   - Use **standalone mode** if you want ISVW to serve as the network's sole HTTP proxy server.
   - If using **dependent mode**, type the upstream proxy name and port number.

     Dependent mode protects clients from receiving malicious HTTP-borne risks from a server. The typical use case is to protect Web users on your network from receiving malicious Internet downloads. In the dependent mode, ISVW and the clients that it protects are typically installed within the same LAN, and ISVW is dependent upon an upstream proxy to access the HTTP server.
   - If using **reverse mode**, type the HTTP server address that you want to protect.

Reverse mode places ISVW between a Web server and the clients of that server. This is a less common configuration, and is typically used to protect Web servers from having malicious content uploaded to them. In the reverse mode proxy topology, ISVW is typically installed close to the Web server that it protects and is separated from the clients by the Internet.

3. Type the HTTP Listening Port (default 8080).

   If FTP over HTTP Anonymous users is enabled, the setting address is used as password "**logon email address**".

4. If you want to record all HTTP requests in a log file, select **Log HTTP requests**.

   By default, this function is disabled.

Binding to a Specific Network Interface

After default installation, HTTP will listen on all network interfaces.

To restrict listening to a specific network interface:

1. Modify Config.xml as follows:

   <Key Name="Http">
   <Key Name="Main">
   <Key Name="http">
   <Value Name="listening_interface" string="IP" type="string" int="0" />

   where IP = the IPv4 address of the network interface to which you want to bind.

2. Restart ISVW services.

Setting the Proxy at the Client Browser (Internet Explorer)

To set the proxy for an Internet Explorer browser when using ISVW to scan HTTP traffic:

1. Open the Internet Explorer browser.
2. From the browser tool bar, select **Tools > Internet Options**.

3. Click the **Connections** tab, then click **LAN Settings** as shown in *Figure 5-17*.

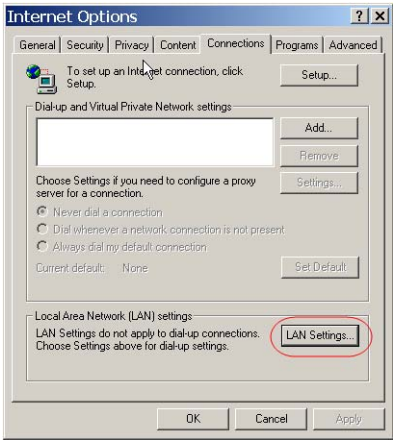


FIGURE 5-17. Internet Options > Connections > LAN Settings

4. In the **Local Area Network (LAN) Settings** dialog box, select the radio button before "**Use a proxy server for your …**" Type the ISVW server IP or name in the address field and type the ISVW service port number in the Port field (the default value is 8080).

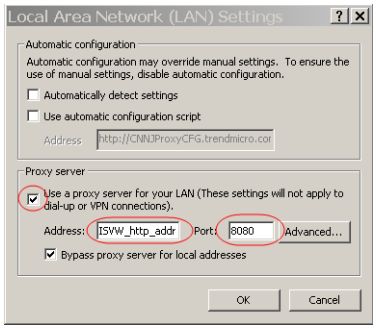


FIGURE 5-18. Local Area Network (LAN) Settings

5. Click **OK** to save your settings.

Enabling HTTP Transaction Logging

Currently ISVW supports transaction logging for HTTP. Transaction logging for HTTP is enabled by default.

To enable or disable HTTP transaction logging:

1. Open the file Config.xml
2. Search for the key named "WriteConnectionMsg" located under "HTTP".
3. Set "WriteConnectionMsg" value to "1" (enabled) or "0" (disabled).
4. Restart the service.

Chapter 6

Configuring FTP Services

InterScan VirusWall (ISVW) allows you to monitor FTP traffic to maintain security at your network gateway. You can enable or disable scanning of FTP traffic during the installation process or at any time thereafter through the Summary page of the ISVW Web console.

Available FTP services include:

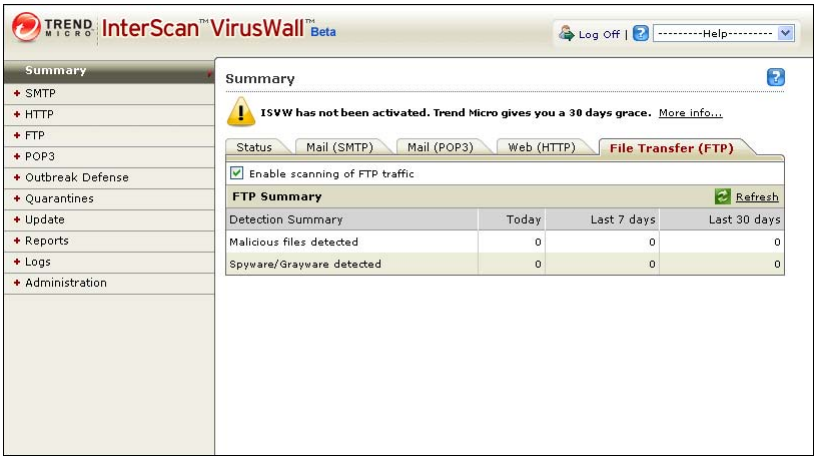
- Scanning for viruses and security risks in uploads and downloads
- Spyware and other grayware detection
- Configuration of FTP server mode and listening port

The File Transfer (FTP) tab on the ISVW Summary screen provides statistics concerning the number of viruses and spyware files that ISVW FTP scanning has detected in incoming and outgoing file traffic.

Enabling or Disabling FTP Services

To enable or disable scanning services for FTP protocol file downloads and uploads, select or clear the Enable FTP Traffic check box on the File Transfer (FTP) tab on the Summary page shown in *Figure 6-1*.

FIGURE 6-1. File Transfer (FTP) Summary Screen



The File Transfer (FTP) tab also shows scanning statistics for infected files detected and spyware/grayware detection.

Note: When the "Enable FTP traffic" is disabled, the client will not be able to connect through ISVW to an FTP server. When the "Enable FTP Scanning" is disabled the client will still be able to connect, through ISVW, to the FTP server and will be able to download items from the FTP server. However, the items will not be scanned for viruses.

Configuring FTP Virus Scan Settings

ISVW scans the FTP traffic flow to detect viruses and other security risks in uploads and downloads. FTP scanning is highly configurable. For example, you can set the types of files to block and how ISVW scans compressed and large files to prevent performance issues and browser time-outs.

As an administrator, you can configure FTP Scanning for viruses and other malware when you select **FTP > Scanning**.

Enabling FTP Virus Scanning

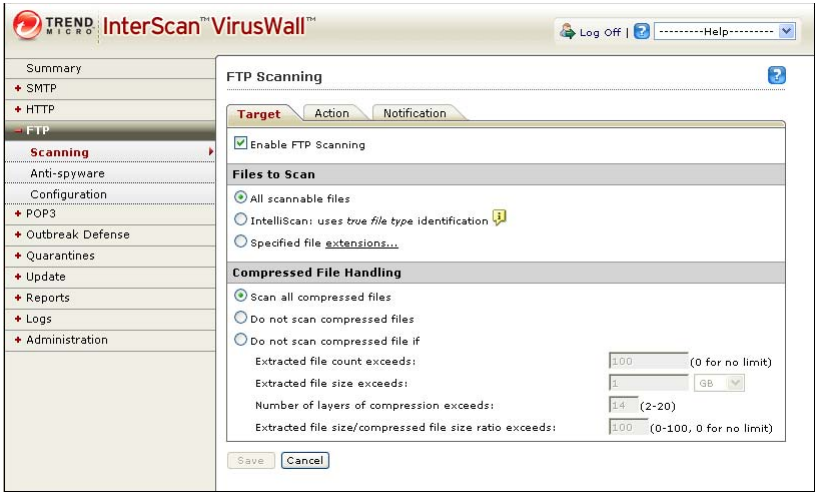
To enable FTP virus scanning:

1. On the left side menu, select **FTP > Scanning**.
2. Click the **Target** tab.
3. Select the **Enable FTP Scanning** check box.
4. Click **Save**.

Specifying File Types to Scan

ISVW can check all or specified file types for viruses, including the individual files within compressed volumes. *Figure 6-2* shows the settings that you can specify when scanning files.

FIGURE 6-2. FTP Virus Scanning Target Tab



To select the file types to scan:

1. On the left side menu, select **FTP > Scanning** and click the **Target** tab.
2. Under Files to Scan, select your preferred option:

a. To scan all files, regardless of file type, select All scannable files. This is the most secure setting.

b. To allow the product to intelligently identify the files to scan, select IntelliScan: uses "true file type" identification.

   This option will pass some file types, which will result in higher performance, but will be less secure than when scanning all files.

c. To scan only files with specific extensions, select Specified file extensions. ISVW scans only the files that have the same extensions as those that are specified in the Additional Extensions text box.

   By default, ISVW scans files with the following file name extensions:

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

   Tip: Use the Specified file extensions option to modify the default scan list.

3. Click Save.

Note: The scan type and compressed file handling options apply to all types of file scans, including virus and spyware.

Compressed File Handling

To specify how ISVW processes compressed files during FTP scanning:

On the left menu, select **FTP > Scanning** and click the Target tab.

- To scan all compressed files, select Scan all compressed files. This is the most secure configuration.
- To skip scanning of all compressed files, select Do not scan compressed files. ISVW will not scan any compressed files.

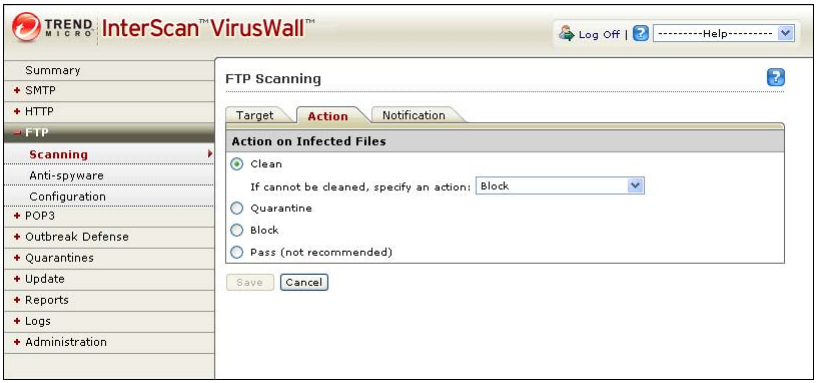
- To scan compressed files within user-specified limits, select Do not scan compressed files if:, and specify the conditions when compressed files should not be scanned.
  - Extracted file count exceeds—the maximum number of files within the compressed file (0 means no limit). ISVW scans the files in the compressed file until it reaches the restriction.
  - Extracted file size exceeds—the maximum file size after decompression. ISVW scans only individual files within the limit.
  - Number of layers of compression exceeds—the maximum number of compression layers. For instance, if a ZIP file contains a RAR file, and that file contains another compressed file, there would be three layers. ISVW scans the files in the compressed file until it reaches the restriction.
  - Extracted file size/compressed file size ratio exceeds—the maximum size ratio before and after compression. ISVW scans only individual files within the limit.

Note: The scan type and compressed file handling options apply to all types of file scans, including virus and spyware/grayware.

Specifying the Action to Take upon Virus Detection

When ISVW detects an infected file, it can perform one of six actions, as shown in *Figure 6-3*:

FIGURE 6-3. FTP Scanning Action Tab



To specify the action to take upon detection of infected files:

1. On the left side menu, select FTP > Scanning and click the Action tab.
2. Under Action on Infected Files, select your preferred option:
   - Select Clean to always clean the infected file and deliver it to the recipient. Then, select the action to take when infected files cannot be cleaned:
     - Quarantine—removes and quarantines infected files
     - Block—removes infected files without quarantining them
     - Pass (not recommended)—delivers the infected file.
   - Select Quarantine to move, without cleaning, the infected file to the quarantine directory. The recipient will not receive the infected file.
   - Select Block to delete the infected file. The recipient will not receive the infected file.
   - Select Pass (not recommended) to deliver the infected file to the recipient.
3. Click Save.

Note: The default quarantine folder for FTP scanning is \quarantine\ftp.

Specifying the Virus Scan Notification Message

When ISVW finds a security risk, it notifies the user through the FTP client. You can modify the message text for the user notification, and you can notify the administrator by email.

To configure the notification message:

1. On the left side menu, select FTP > Scanning and click the Notification tab.
2. For the user notification, type the message text you want ISVW to send.
3. Select Administrator to enable sending notifications to the administrator. You can modify the message content as desired. The following tokens are supported in administrator notification for FTP scanning:

TABLE 6-1.

TOKEN	DESCRIPTION
%DATETIME%	scan date and time
%PROTOCOL%	protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Configuring FTP Anti-Spyware Settings

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular updates in a pattern file.

Some common types of grayware include:

TABLE 6-2. Common Types of Grayware Tracked by ISVW

TYPE OF GRAYWARE	TYPICAL FUNCTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser
Dialers	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Helps hackers enter computers
Remote Access Tools	Helps hackers remotely access and control computers
Password Cracking Applications	Helps hackers decipher account user names and passwords
Others	Other types not covered above

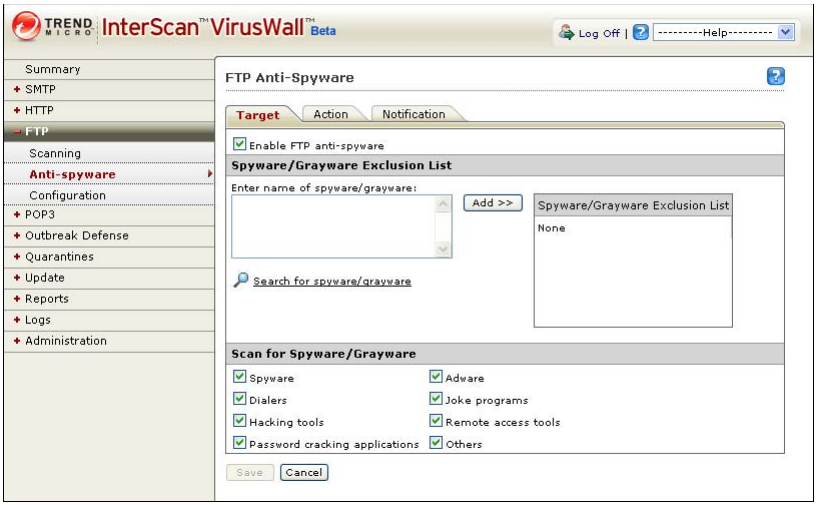
Enabling FTP Spyware Scanning

To enable FTP spyware scanning:

1. On the left side menu, select **FTP > Anti-spyware** and click the **Target** tab.
2. Select the **Enable FTP Anti-spyware** check box.
3. Click **Save**.

   Figure 6-5 shows the FTP Anti-spyware **Target** tab, which allows you to enable FTP spyware scanning and specify spyware scanning exclusions.

FIGURE 6-4. FTP Anti-spyware Target Tab



Setting the Spyware Scanning Exclusion List

To list specific file names or file name extensions to exclude from spyware/grayware scanning:

1. On the left side menu, select **FTP> Anti-spyware** and then click the **Target** tab.
2. In **Enter name of spyware/grayware**, type the spyware name you want to exclude from spyware/grayware scanning.

   If you are not sure of the spyware name, click the **Search for spyware/grayware** link.
3. Click **Add**.
4. Click **Save**.

Note: To delete entries on the exclusion list, click the trash bin icon. Click **Save** to finalize changes.

Specifying Spyware and Grayware Types to Scan

To specify the types of spyware and grayware for which you want ISVW FTP services to scan:

1. On the left side menu, select **FTP > Anti-spyware** and click the **Target** tab.
2. Under "Scan for Spyware/Grayware", select the types of spyware and grayware for which FTP services will scan.
3. Click **Save**.

Specifying the Action to Take upon Spyware Detection

You can select one of three actions for ISVW to take when it detects spyware or other grayware.

To specify the action to take when ISVW detects spyware/grayware:

1. On the left side menu, select **FTP > Anti-spyware** and click the Action tab.
2. Under "Action on Spyware/Grayware", select one of the following options:
   - Select **Quarantine** to move the spyware/grayware file to the quarantine directory. The user will not receive the file.
   - Select **Block** to prevent the file transfer of spyware/grayware programs. The user will not receive the file.
   - Select **Allow** download (not recommended) to send the spyware/grayware to the intended recipient.
3. Click **Save**.

Specifying the User Notification Message When InterScan VirusWall Detects Spyware/Grayware

When ISVW quarantines or blocks a file, it will notify the user. You can modify the message text for the User Notification.

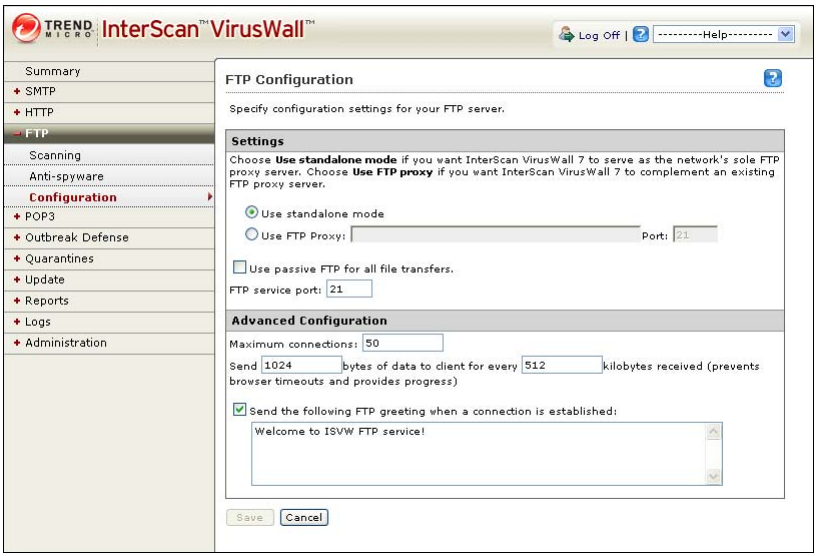
To specify the notification message when spyware or grayware is detected:

1. On the left side menu, select **FTP > Anti-spyware** and click the Notification tab.
2. Type the message you want ISVW to send.
3. Click **Save**.

FTP Configuration

Before ISVW can monitor FTP traffic, you need to specify the configuration settings for the FTP server. *Figure 6-5* shows the configuration settings that you can specify.

FIGURE 6-5. FTP Configuration Settings



- Select **Standalone mode** if there is no existing FTP proxy server on the network and you want FTP VirusWall to serve as the system's FTP proxy server.
- Select **Use FTP proxy** if there is an existing FTP proxy server on the system that you want to continue to use. After installing ISVW, all subsequent FTP sessions will pass through it; this action will be invisible to the end user.

Standalone Mode

When configured for standalone mode, clients always open a FTP session with FTP VirusWall (using its IP address). When prompted for a user name and password, clients will need to enter the expected user name, modified with the computer name.

Use FTP Proxy Mode

Select Use FTP proxy if there is an existing FTP proxy server on the system that you want to continue to use. After installing ISVW, all subsequent FTP sessions will pass through it; this action will be invisible to the end user.

To use FTP to transfer files to or from a site:

1. Use the FTP command to connect to ISVW:

   ```
   - > ftp [MachineName]
   ```

   The session responds with:

   ```
   < - 220 InterScan VirusWall (Stand-alone Mode), Security
   risk scan on. Welcome to ISVW FTP service!
   User (ISVW-test:(none)):
   ```

   If the FTP service port is not 21, you can use the open command:

   ```
   - > ftp
   ftp> open [MachineName] [FTPServicePort]
   ```

   The session responds with:

   ```
   < - Connected to [MachineName]
   220 InterScan VirusWall (Stand-alone Mode), Security risk
   scan on. Welcome to ISVW FTP service!
   ```

2. When you get the login prompt, type your user name and password. The user name should be in the format: `originalname@ftpsite:ftpport`

   For example, if your FTP loginname is john, and the FTP site is antivirus.com, and the port is 21, then type `john@antivirus.com:21` when you get the user prompt and type the original password when you get the password prompt:

   The session responds with:

   ```
   User (ISVW-test:(none)):john@antivirus.com:21
   Password: opensesame
   ```

   Note: If the FTP site you want to access is using port 21, you can omit the FTP port, so you can also login with user `john@antivirus.com` in this example.

3. When you have successfully logged in, use the get or put command to download/upload files. Virus detection information will be displayed when you upload or download files in a command window.

```
ftp> get eicar.com
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for eicar.com (68
bytes).
451-Message from InterScan VirusWall
451-InterScan has found virus in eicar.com
451-
451-Eicar_test_file virus was found
451-
451-Trend Micro InterScan VirusWall has determined that the
file you are attempt
ing to transfer is infected. It has taken action on the file.
451-
451 The file has been rejected
ftp>
```

4. When the file download/upload finishes, use the quit command to exit.

Note: FTP VirusWall supports Proxy OPEN and anonymous users.

Configuring FTP Proxy Server Settings

To configure FTP proxy server settings:

1. On the left side menu, select **FTP > Configuration**.
2. Select the mode.

   If using an existing proxy server, also:

   - Type the IP address (name or number) of the existing FTP proxy server.
   - Type the Port, usually 21.
3. Select Use passive FTP for all file transfers (or PASV mode) when
   - the client is behind a NAT or
   - there is a firewall on the network that performs packet filtering, and the firewall is configured to deny inbound connections from the Internet to the LAN (usually for ports above 1024).

Active FTP (PORT mode): In active mode FTP, the client connects from a random unprivileged port (N > 1023) to the FTP server's command port, port 21. The client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect to the client's specified data port from its local data port, which is port 20.

Passive FTP (PASV mode): In passive mode FTP, the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect to its data port, the client will issue the PASV command. The server then opens a random unprivileged port (P > 1023) and sends the PORT P command to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data.

4. Enter the FTP service port, usually 21.

   This is the listening port for FTP traffic.

5. In the **Maximum Connections** field, enter the maximum number of simultaneous FTP connections that you want to allow ISVW to accept.

   Whenever this limit is reached, users trying to access the site are queued. This can improve throughput in certain circumstances, depending on the number of processors in the system. Choose a number that represents an equitable balance between the physical resources available on your system and the number and frequency of connections you anticipate.

6. Enter trickle amount and trickle period into **Send X bytes of data to client for every Y kilobytes received** field. This helps prevent lost connections while ISVW is scanning the file being transferred. Very small amounts can be used.

7. To enable sending greeting message to FTP clients, select **Send the following FTP greeting when a connection is established:**. You can customize the content of the greeting message in the text box.

8. Click **Save**.

Enabling FTP Transaction Logging

Currently ISVW supports transaction logging for FTP. Transaction logging for FTP is enabled by default.

To enable or disable FTP transaction logging:

1. Open the file `Config.xml`.
2. Search for the key named "WriteConnectionMsg" located under "FTP".
3. Set "WriteConnectionMsg" value to "1" (enabled) or "0" (disabled).
4. Restart the service.

Chapter 7

Configuring POP3 Services

InterScan VirusWall (ISVW) allows you to monitor incoming POP3 mail traffic. You can enable or disable scanning of POP3 traffic during the installation process or at any time thereafter through the Summary page of the ISVW Web console.

Available POP3 services include:

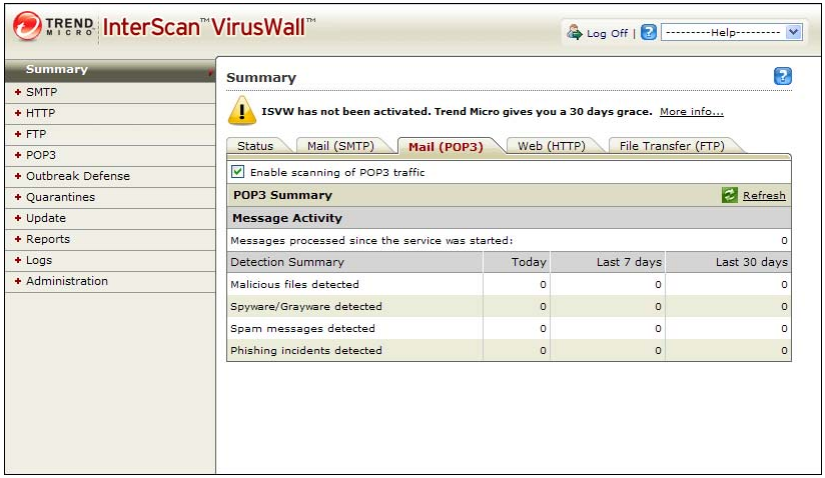
- Scanning for viruses and other types of malware
- IntelliTrap scanning of compressed executable files that could contain potentially malicious code
- Phishing site detection
- Spam detection that allows the Administrator to configure categories and content levels
- Spyware and other grayware detection
- Content filtering
- Size filtering of messages and attachments
- Configuration of POP3 server port and delivery options for incoming mail
- POP3 Whole File Scan

The Mail (POP3) tab on the ISVW Summary screen provides statistics concerning the number of viruses, spyware, spam messages, and phishing messages that ISVW POP3 scanning has detected in incoming email communication.

Enabling or Disabling POP3 Services

To enable or disable scanning services for POP3 mail message traffic, select or clear the **Enable POP3 Traffic** check box on the Mail (POP3) tab on the Summary page shown in *Figure 7-1*.

FIGURE 7-1. Mail (POP3) Summary Screen



Configuring POP3 Virus Scan Settings

ISVW offers the administrator flexibility in configuring how the POP3 service behaves. For example, you can specify

- the attachment types to scan
- the individuals to notify when a virus is detected
- the action that ISVW takes upon detection—clean, delete, move, or block

POP3 Virus Scanning Features

ISVW POP3 virus scanning includes the following features:

- Automatic, customizable virus notifications

- Option to clean, delete, move (quarantine), pass, or block infected files
- Ability to insert customized taglines in messages

Enabling POP3 Virus Scanning

To enable POP3 virus scanning:

1. On the left side menu, select **POP3 > Scanning**.
2. Click the **Target** tab.
3. Select the **Enable POP3 Scanning** check box.
4. Click **Save**.

Specifying the File Types to Scan

ISVW can check all or specified attachment types for viruses, including the individual files within compressed volumes.

To select the file types to scan:

1. On the left side menu, select **POP3 > Scanning** and click the **Target** tab.
2. Under "Files to Scan", select your preferred option:
   a. To scan all attachments, regardless of file type, select **All scannable files**. This is the most secure setting.
   b. To allow the product to intelligently identify the attachments to scan, select **IntelliScan: uses “true file type” identification**.

      This option will pass some file types, which will result in higher performance, but will be less secure than when scanning all attachments.
   c. To scan only selected attachment types, select **Specified file extensions**. ISVW scans only those file types that are specified, explicitly, in the **Additional Extensions** text box.

      By default, ISVW scans files with the following file name extensions:

      "";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;

SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;
XLT;XML;Z;ZIP;{*;

Tip: Use the Specified file extensions option to modify the default scan list.

3. Click **Save**.

Note: Virus scanning settings apply to all types of POP3 scanning for malicious files, including virus/malware, IntelliTrap, and spyware scanning.

Configuring the Processing of Compressed Files

To specify how ISVW processes compressed files during POP3 scanning:

1. On the left side menu, select **POP3 > Scanning** and click the **Target** tab.
2. Under **Compressed File Handling**, select your preferred option:
   a. To scan all compressed attachments, select **Scan all compressed files**. This is the most secure setting.
   b. To skip all compressed attachments, select **Do not scan compressed files**. ISVW will not scan any compressed attachments.
   c. To scan compressed attachments based on the number of files, the size after decompression, the number of compression layers, and the compressions ratio, select **Do not scan compressed files if**:. Then, specify the conditions when compressed attachments should not be scanned.
      - **Extracted file count exceeds**—the maximum number of files within the compressed attachment; (0 means no limit). ISVW does not scan any files in the compressed file.
      - **Extracted file size exceeds**—the maximum file size after decompression. ISVW scans only individual files within the limit; (0 means no limit).
      - **Number of layers of compression exceeds**—the maximum number of compression layers. ISVW does not scan any files in the compressed file.
      - **Extracted file size/compressed file size ratio exceeds**—the maximum size ratio before and after compression. ISVW scans only individual files within the limit.

3. Click **Save**.

Specifying the Action to Take upon Virus Detection

ISVW can take one of five actions when it detects a virus.

To specify the action to take upon detection of infected attachments:

1. On the left side menu, select **POP3 > Scanning** and click the **Action** tab.
2. Under **Action on Messages with Infected Items**, select your preferred option:
   - To clean infected attachments and deliver the message, select **Clean infected items and pass**. Then, select the action to take when ISVW cannot clean an infected attachment:
     - **Quarantine**—removes and quarantines attachments.
     - **Delete**—removes attachments without quarantining them.
     - **Pass (not recommended)**—delivers attachments with the message.
   - To quarantine attachments without cleaning them and deliver the message, select **Quarantine infected items and pass**.
   - To delete the message, select **Delete**.
   - To permanently delete attachments and deliver the message, select **Delete infected items and pass**.
   - To deliver the message with infected attachments, select **Pass (not recommended)**.
3. Click **Save**.

Note: The default quarantine folder for POP3 scanning is \quarantine\POP3.

Configuring Virus Scan Notification Settings

When ISVW finds a virus, it can notify the administrator, the message recipient, or the sender. You can configure the settings, include inline notifications on all scanned messages, and specify notification settings.

Specifying Notification Settings when InterScan VirusWall Detects a Virus

To specify notification settings when ISVW detects a virus in an incoming message attachment:

1. On the left side menu, select **POP3 > Scanning** and click the **Notification** tab.
2. Under **Email Notifications**, select the recipients of the notification sent when a virus is found.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Specifying Inline Notification Settings

ISVW can insert text, known as an inline notification, into the message body of an incoming message. When you select the message types **Virus free** and **Virus detected**, the inline notification will appear in all messages that are scanned.

To specify inline notification settings for incoming messages:

1. On the left side menu, select **POP3 > Scanning** and click the **Notification** tab.
2. Under Inline Notification Stamp (see *Figure 7-2*), select the message types (**Virus free** and **Virus detected**) that should contain the inline notice.

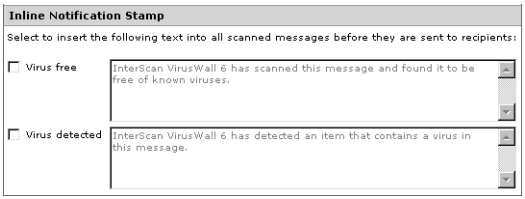


FIGURE 7-2. Inline Notification Stamp

3. Type the inline notice that ISVW will insert in the message body. Use any of the following tokens:

Token	Description
%VIRUSNAME%	name of the virus found
%FILENAME%	name of the infected file
%CONTAINERNAME%	name of the archive or other files that contain compressed files
%ACTION%	action taken on the infected attachment

4. Click **Save**.

POP3 Whole File Scan

POP3 Whole File Scan is a supplement to the regular ISVW mail scan. Whole File Scan can detect special kinds of email viruses that cannot be detected by regular scanning methods. Whole file scanning can be configured from the Config.xml file which is located in your ISVW Windows product folder.

How Whole File Scanning Works

When ISVW receives an email, the email is first tested with the virus filter. If the virus filter does not detect a virus, the email is then tested with the whole file filter. If the email triggers the whole file filter, meaning the email contains a virus, ISVW will take an action on the message and, if enabled, send a notification to the administrator and/or recipient. If the action taken is set to deliver, ISVW can be configured to warn the user that email they are receiving contains a virus.

Configuring Whole File Scan for POP3

Configuring Whole File Scan is a four (4) step process. You must first enable Whole File Scan. Next you must set (enable) an action for ISVW to take if it detects a virus. Next you should set up a notification to notify the administrator and recipient that ISVW detected a virus. Finally, set up the disclaimer statement that will be inserted into the email if the action for detected viruses is deliver.

Note: Whole File Scan is disabled by default.

Enabling or Disabling whole file scan

To enable/disable whole file scan:

1. Open the ISVW Windows product folder and locate the file `Config.xml`.
2. Open the `Config.xml` file in any text editor program.
3. Scroll down the screen until you locate the following value:

   <Value Name="EnableWholeFileScan" string="" type="int"
   int="0" />

TABLE 7-1. Path to the "EnableWholeFileScan" value

```
<Key Name="POP3">
 <Key Name="Policies">
  <Key Name="Rule1">
   <Key Name="MailVirusScan">
   <Value Name="EnableWholeFileScan" string="" type="int" int="0" />
```

4. Set the "Int" value to "1" to enable Whole File Scan and "0" to disable Whole File Scan.
5. Save and close the file.
6. Restart the ISVW server for changes to take affect.

Setting the Action

There are three (3) actions that ISVW can take when the whole file filter detects a virus: Deliver, Delete, and Quarantine. The default action is Quarantine. If you change the action to Deliver, ISVW will deliver the mail to the original recipient. You can elect to insert a disclaimer into the body of the email to warn the recipient that the email that they are receiving contains a virus. Set the action to delete in order to delete the email.

To set the action ISVW should take when the whole file filter detects a virus:

1. Open the ISVW Windows product folder and locate the file "Config.xml".
2. Open the Config.xml file in any text editor program.
3. Scroll down the screen until you locate the following keys:

   <Key Name="Deliver">

   <Key Name="Delete">

   <Key Name="Quarantine">

TABLE 7-2. Path to Deliver, Delete, and Quarantine keys

```
<Key Name="POP3">
 <Key Name="Policies">
   <Key Name="Rule1">
     <Key Name="MailVirusScan">
      <Key Name="Outcomes">
       <Key Name="OutcomeWholeFileScanVirus">
        <Key Name="Actions">
         <Key Name="Deliver">
          <Value Name="Enable" string="" type="int" int="0" />
         <Key Name="Delete">
          <Value Name="Enable" string="" type="int" int="0" />
         <Key Name="Quarantine">
          <Value Name="Enable" string="" type="int" int="1" />
```

Note: There are three possible actions that ISVW can take when the whole file filter detects a virus. Make sure that only one of the three actions is enabled in the Config.xml file. The default action for Whole File Scan is Quarantine.

4. Set the action that ISVW should take when the whole file filter detects a virus.

TABLE 7-3. Whole File Scan actions

	Action Settings		
Action types	**To Deliver**	**To Delete**	**To Quarantine**
Deliver	1	0	0
Delete	0	1	0
Quarantine	0	0	1

5. Save and close the file.
6. Restart the ISVW server for changes to take affect.

Sending Notifications

ISVW can send a notification message to the administrator and/or recipient if the whole file filter detects a virus. From the Config.xml file you can enable or disable notifications for either of the aforementioned people. ISVW has a default notification message. You can modify the notification message from the Config.xml file.

To enable ISVW to send a notification when the whole file filter detects a virus:

1. Open the ISVW Windows product folder and locate the file "Config.xml".
2. Open the Config.xml file in any text editor program.
3. Scroll down the screen until you locate the following keys:

   <Key Name="NotificationAdmin">

   <Key Name="NotificationRecipient">

   TABLE 7-4. Path to NotificationAdmin and NotificationRecipient keys

```
<Key Name="POP3">
 <Key Name="Policies">
  <Key Name="Incoming"> or <Key Name="Outgoing">
   <Key Name="Rule1">
    <Key Name="MailVirusScan">
     <Key Name="Outcomes">
      <Key Name="OutcomeWholeFileScanVirus">
       <Key Name="Actions">
        <Key Name="NotificationAdmin">
         <Value Name="Enable" string="" type="int" int="0" />
        <Key Name="NotificationRecipient">
         <Value Name="Enable" string="" type="int" int="1" />
```

4. Set the "Enable" value to "1" to enable notifications. To disable notifications for a specific person, set "Enable" to "0".
5. [Optional] Find the tag

   <Value Name="Body"string="..."

   and modify the message to send to each recipient or accept the defaults.
6. Save and close the file.
7. Restart the ISVW server for changes to take affect.

Modifying the Disclaimer Statement

If the action for a message that contains a virus is Deliver, you can have ISVW add a diclaimer notice to the original email. To have ISVW add a disclaimer to the email first enable the inline notification stamp in the ISVW Web console. Then set the Whole File Scan action to Deliver.

To modify the content of the disclaimer statement:

1. Open the ISVW Windows product folder and locate the file "Config.xml".
2. Open the Config.xml file in any text editor program.
3. Scroll down the screen until you locate the following value tag:

   <Value Name="VirusAlert4WholeFileScan" string="..."

   TABLE 7-5. Path to "VirusAlert4WholeFileScan" tag

```
<Key Name="POP3">
 <Key Name="Policies">
   <Key Name="Rule1">
     <Key Name="MailVirusScan">
     <Value Name="VirusAlert4WholeFileScan" string="..."
```

4. Modify or replace the text within the parenthesis for the string value.

Note: The token "%VIRUSNAME%" can be used in the disclaimer statement to identify the name of the virus.

5. Save and close the file.
6. Restart the ISVW server for changes to take affect.

Configuring IntelliTrap Settings

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

Enabling or Disabling POP3 IntelliTrap Scanning

To enable or disable POP3 IntelliTrap scanning:

1. On the left side menu, select **POP3 > IntelliTrap** and click the **Target** tab.
2. Select or clear the **Enable POP3 IntelliTrap** check box to enable or disable IntelliTrap scanning.
3. Click **Save**.

Specifying the Action to Take When IntelliTrap Detects Potentially Malicious Code

ISVW can take one of three actions when IntelliTrap detects potentially malicious code.

To specify the action to take when IntelliTrap detects potentially malicious code:

1. On the left side menu, select **POP3 > IntelliTrap** and click the **Action** tab.
2. Under "Action on Messages With Infected Attachments", select your preferred option:
   - Select **Quarantine infected attachments and pass** to quarantine attachments and deliver the message. Users will receive the message without the attachment(s); the attachment(s) will be stored in the quarantine folder.
   - Select **Delete infected attachments and pass** to permanently delete attachments and deliver the message. Users will receive the message without the attachment.
   - Select **Pass (not recommended)** to deliver the message with infected attachments. Users will receive the message with the attachment(s) and an inline warning.
3. Click **Save**.

Note: The default quarantine folder for POP3 scanning is \quarantine\POP3.

Configuring IntelliTrap Notification Settings

ISVW can automatically notify selected recipients whenever IntelliTrap detects potentially malicious code in compressed executable files.

To specify notification settings when IntelliTrap detects a security threat in a message attachment:

1. On the left side menu, select **POP3 > IntelliTrap** and click the **Notification** tab.
2. Select the recipients of the notification sent when IntelliTrap detects a security risk.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Configuring POP3 Anti-Phishing Settings

Phish, or *phishing*, is a rapidly growing form of fraud that mimics a legitimate Web site and seeks to fool Web users into divulging private information. Phishing attacks involve email messages that falsely claim to be from an established, legitimate organization. The messages typically encourage recipients to click on a link that will redirect their browsers to a fraudulent Web site, where they are asked to update personal information. Victims usually give up passwords, social security numbers, and credit card numbers.

In a typical scenario, unsuspecting users receive an urgent sounding (and authentic looking) email telling them that there is a problem with their account that they must immediately fix, or the account will be closed. The email will include a URL to a Web site that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate Web site but then change the back end—where the collected data is actually sent.

Enabling POP3 Anti-Phishing

To enable the POP3 anti-phishing feature:

1. On the left side menu, select **POP3 > Anti-phishing** and click the **Target** tab.
2. Select the **Enable POP3 Anti-phishing** check box.
3. Click **Save**.

Specifying the Action when InterScan VirusWall Detects Phishing Messages

To specify the action on phishing messages:

1. On the left side menu, select **POP3 > Anti-phishing** and click the **Action** tab.
2. Select the action for phishing messages:
   - Select **Quarantine** to move the message to the quarantine folder.
   - Select **Delete** to delete the message without delivering it.
   - Select **Pass (not recommended)** to deliver the phishing message normally.
3. Click **Save**.

Specifying Notification Settings When InterScan VirusWall Detects a Phishing Site

When ISVW detects a phishing message, it can send an email notification to the administrator, the recipient(s), or both. You can also report suspected or known phishing sites to TrendLabs. The POP3 Anti-phishing Notification tab allows you to specify whether to send email notifications when ISVW detects a phishing site.

To specify notification settings when a phishing URL is detected:

1. On the left side menu, select **POP3 > Anti-phishing** and click the **Notification** tab.
2. Select the recipients of the notification sent when a phishing URL is detected.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Reporting a Potential Phishing URL

To report suspected or known phishing sites to TrendLabs, click **Submit a Potential Phishing URL to TrendLabs** and provide the URL in an email that you will send to `antifraud@support.trendmicro.com`.

TrendLabs monitors sites that obtain information for fraudulent purposes and distributes known phishing site information as part of the automatic updates that Trend Micro makes available to ISVW customers.

Note: To view a list of phishing emails, go to http://www.trendmicro.com/en/security/phishing/overview.htm.

Configuring POP3 Anti-Spam Settings

ISVW uses the following basic features to filter spam in POP3 email communication:

- **Approved and Blocked Senders lists**—these lists filter on the sender's email address rather than on content. ISVW always delivers approved sender messages and always classifies blocked sender messages as spam.

  Note: The Exchange administrator maintains a separate Approved and Blocked Senders list for the Exchange server. If an end user creates an approved sender, but that sender is on the administrator's Blocked Senders list, then messages from that sender will be blocked.

- **Spam filter**—administrators set a spam detection level to filter out spam. The higher the detection level, the more messages that are classified as spam. Administrators can set a global detection level for all messages or set one detection level for each spam category.

  The detection level determines how tolerant ISVW will be toward suspect email messages.

  - A high detection level quarantines the most email as spam, but it might also falsely identify and quarantine legitimate email messages as spam, creating "false positive" spam mail.
  - A low detection level does not rigorously screen email messages, but does not create many false positive spam messages.

Enabling POP3 Anti-Spam

The POP3 Anti-spam Target tab, shown in *Figure 7-3*, allows you to enable spam filtering, and specify detection levels for various predefined categories of spam.

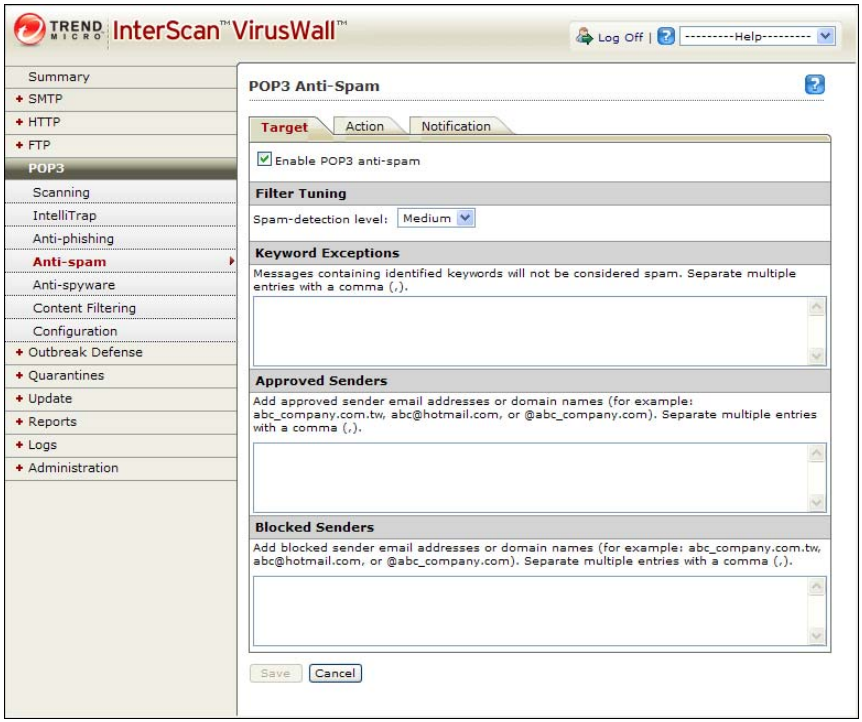


FIGURE 7-3. POP3 Anti-spam Target Tab

To enable POP3 anti-spam filtering:

1. On the left side menu, select **POP3 > Anti-spam**.
2. Click the **Target** tab.
3. Select the **Enable POP3 Anti-spam** check box.
4. Click **Save**.

Setting the Spam Detection Level (Filter Tuning)

To specify the spam detection level:

1. On the left side menu, select **POP3 > Anti-spam**.
2. Click the **Target** tab.
3. In the **Filter Tuning** section, select the desired span detecting level.

Spam Detection Levels

ISVW uses the following detection levels:

Detection Level	Filtering Criteria
Low	ISVW filters only the most obvious and common spam messages, but there is a very low chance that it will filter false positives. This is most lenient level of spam detection.
Medium	ISVW monitors at a high level of spam detection with a moderate chance of filtering false positives. This is the default setting.
High	ISVW monitors all email messages for suspicious files or text, but there is greater chance of false positives. This is the most rigorous level of spam detection.

Determining Spam Detection Levels

The ISVW anti-spam engine uses heuristics and algorithms to calculate the spam detection level. The engine scans the message or file and assigns the scanned item a spam score. Based on this spam score and the spam detection and confidence levels that you specify, ISVW determines whether the item is spam.

The following are the predefined threshold settings:

	Low Confidence	Medium Confidence	High Confidence
Low detection level	6	7	10
Medium detection level	4.5	6	10
High detection level	4	5	7

Note: The scores in the spam threshold settings table may vary depending on the anti-spam pattern in use.

- If you specify a low detection level and the spam score is 6.5, then ISVW will perform the action specified for the low confidence level.
- If the spam score is 8, ISVW will perform the action specified for the medium confidence level.
- If the spam score is 11, ISVW will perform the action specified for the high confidence level.

To see a spam score, see the spam log. A sample entry might be:

```
2006/02/04 20:10:32, SMTP, , Stamp, Success, "LastName\,
FirstName"

 <FirstName.LastName@Level3.com>,"SPAM@TrendMicro.com"

 <SPAM@TrendMicro.com>, FW:How are you doing?

 <D7626E4452B0F745B4C7C15BC97EA052D66887@idclexc0005.corp.globa
l.

 level3.com>, 3.51.0.1033, 13974000, Spam, ,14.594000
```

Tuning the Spam Filter

If you are getting too many false positives, set the spam detection level to a lower setting. Conversely, if users report that they are getting too much spam, adjust the detection level to a higher setting.

To submit samples of false positives to Trend Micro, go to `http://subwiz.trendmicro.com/SubWiz/spam_mail-Form.asp`

Specifying Keyword Exceptions

You can use keyword exceptions to exclude messages that contain certain text from spam filtering. Separate keywords in the exception lists with a comma. Type keywords that should **not** be considered spam in the Keyword Exceptions text box shown in *Figure 7-4*.

Note: No characters except a single comma (,) is allowed between two keywords, this excludes a space and a hard return.

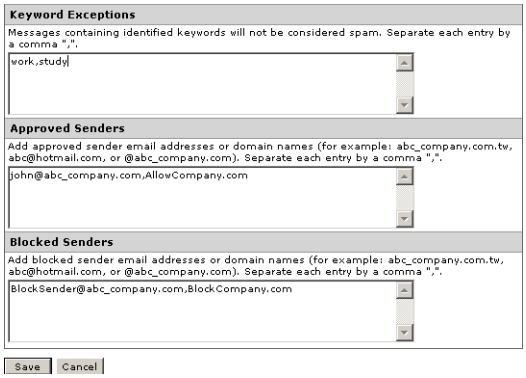


FIGURE 7-4. POP3 Anti-spam Keyword Exceptions and Blocked and Approved Senders Lists

Maintaining Approved and Blocked Senders Lists

The Approved Senders list contains trusted email addresses.ISVW does not filter messages arriving from these addresses for spam, except when **Detect Phishing incidents** is enabled.

The Blocked Senders list contains email addresses that cannot be trusted. Ja automatically considers messages arriving from these addresses as spam and deletes such messages. ISVW does not notify anyone that it deleted the messages.

When an email address is both in the Approved Senders and Blocked Senders lists, messages arriving from this address are considered spam and are deleted.

When adding email addresses to the lists, separate them with a comma. Type all email addresses in the appropriate list, shown in *Figure 7-4*.

ISVW supports wildcard (*) matching for the Approved and Blocked Senders lists. Sample patterns are shown in *Table 7-6*.

TABLE 7-6. Using Wildcards (*) in the Senders Lists

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
john@trend.com	john@trend.com john@trend.com.	Any address different from the pattern.
@trend.com *@trend.com	john@trend.com mary@trend.com.	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com.	john@trend.com.tw mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com.	john@trend.com john@trend.com.tw mary@ms1.trend.comon
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw.	john@trend.com john@ms1.trend.com. john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw.	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com.
..*.trend.com *****.trend.com	The same as "*.trend.com"	The same as "*.trend.com"
trend.com trend.com trend.*.com @*.trend.com	They are all INVALID.	They are all INVALID.

Specifying Actions on Messages Identified as Spam

ISVW can take one of several actions when it identifies a message as spam. This action is based on the detection level(s) that you set on the Target tab. *Figure 7-5* shows the POP3 Anti-spam Action tab.

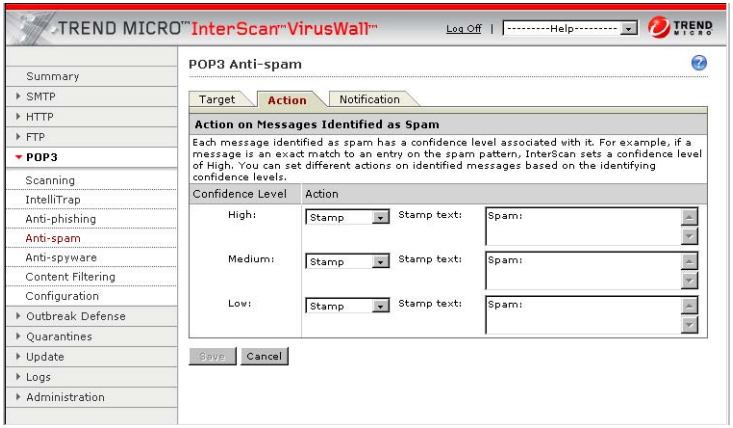


FIGURE 7-5. POP3 Anti-spam Action Tab

To specify the action on spam messages:

1. On the left side menu, select **POP3 > Anti-spam** and click the **Action** tab.
2. Specify the action to take based on the detection confidence level:
   - **High**—ISVW is very confident that the mail message is spam.
   - **Medium**—ISVW is fairly confident that the mail message is spam.
   - **Low**—ISVW is fairly confident that the mail message is not spam.

   For each confidence level, you can select one of four actions:
   - **Delete**—The whole message is deleted.
   - **Quarantine**—The message is quarantined.
   - **Stamp**—A notification content stamp will be inserted into the subject line of the message.
   - **Pass**—ISVW does nothing to the message and it is processed normally.

Specifying Notification Settings When InterScan VirusWall Detects Spam

ISVW can notify the administrator or the recipient when it detects spam email messages. You can specify recipients for the email notification and create messages to send to the administrator and mail recipients. *Figure 7-6* shows the POP3 Anti-spam Notification Settings tab.

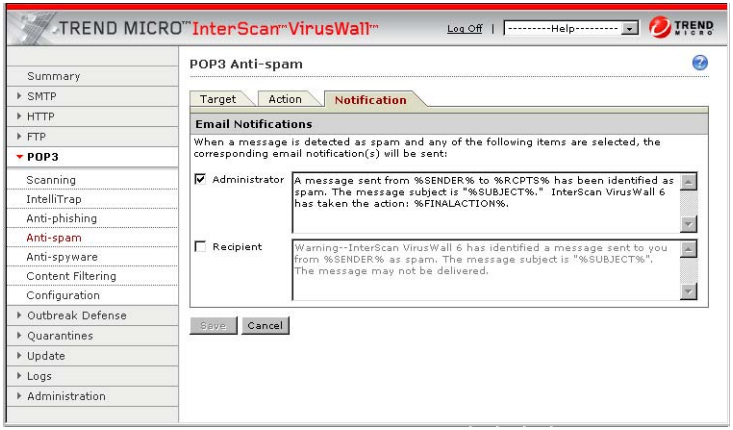


FIGURE 7-6. POP3 Anti-spam Notification Settings Tab

To specify notification settings when ISVW detects spam:

1. On the left side menu, select **POP3 > Anti-spam** and click the **Notification** tab.
2. Under **Email Notifications**, select the recipients who will be notified when ISVW detects spam.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers

Token	Description
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

Configuring POP3 Anti-Spyware Settings

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular updates in a pattern file.

Some common types of grayware include:

Type of Grayware	Typical Function
Spyware	gathers data, such as account user names and passwords, and transmits them to third parties
Adware	displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser
Dialers	changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	helps hackers enter computers
Remote Access Tools	help hackers remotely access and control computers

Type of Grayware	Typical Function
Password Cracking Applications	helps hackers decipher account user names and passwords
Others	other types not covered above

Enabling POP3 Spyware Scanning

To enable POP3 spyware scanning:

1. On the left side menu, select **POP3 > Anti-spyware** and click the **Target** tab.
2. Select the **Enable POP3 Anti-spyware** check box.
3. Click **Save**.

Figure 7-7 shows the POP3 Anti-spyware Target tab, which allows you to enable POP3 spyware scanning and specify spyware scanning exclusions.

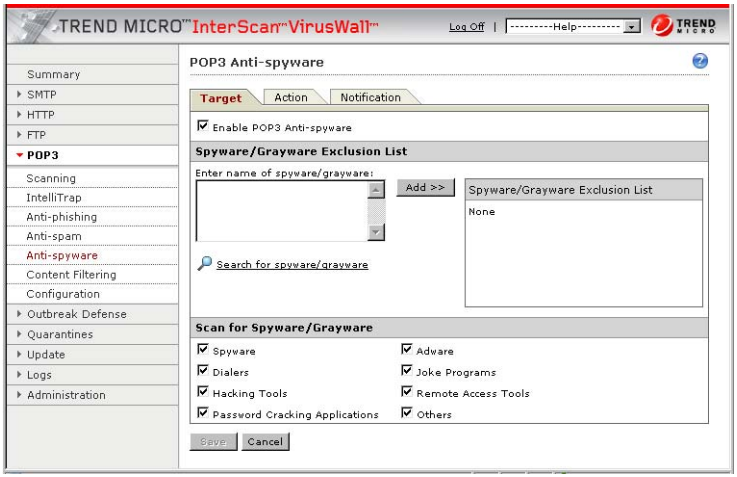


FIGURE 7-7. POP3 Anti-spyware Target Tab

Setting the Spyware Scanning Exclusion List

To list specific file names or file name extensions to exclude from spyware/grayware scanning:

1. On the left side menu, select **POP3> Anti-spyware** and click the **Target** tab.
2. In **Enter name of spyware/grayware**, type the spyware name you want to exclude from spyware/grayware scanning.

   If you are not sure of the spyware name, click the **Search for spyware/grayware** link.
3. Click **Add**.
4. Click **Save**.

Note: To delete entries on the exclusion list, click the trash bin icon. Click **Save** to finalize changes.

Specifying Spyware and Grayware Types to Scan

To specify the types of spyware and grayware for which you want ISVW POP3 services to scan:

1. On the left side menu, select **POP3 > Anti-spyware** and click the **Target** tab.
2. Under **Scan for spyware/grayware**, select the types of spyware and grayware for which POP3 services will scan.
3. Click **Save**.

Specifying the Action to Take upon Spyware Detection

You can select one of three actions for ISVW to take when it detects spyware or other grayware (see *Figure 7-8*).

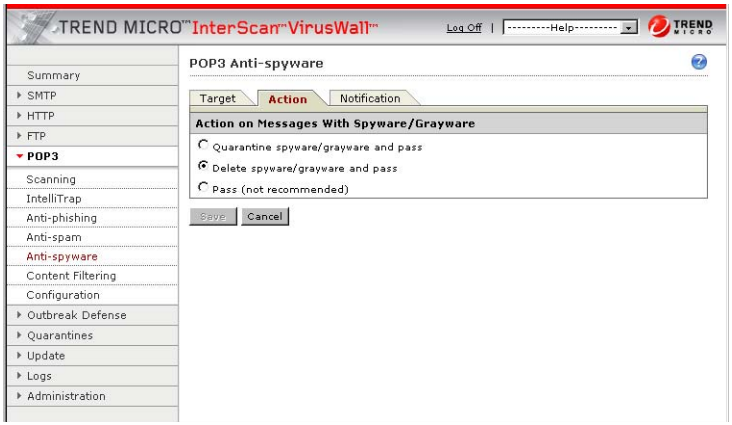


FIGURE 7-8. POP3 Anti-spyware Action Tab

To specify the action to take when spyware/grayware is detected:

1. On the left side menu, select **POP3 > Anti-spyware** and click the **Action** tab.
2. Under **Action for Detected Spyware/Grayware Messages**, select your preferred option:
   - To quarantine attachments and deliver the message, select **Quarantine spyware/grayware and pass**. Users will receive the message without the attachment; the attachment will be stored in the quarantine folder.
   - To permanently delete detected attachments and deliver the message, select **Delete spyware/grayware and pass**. Users will receive the message without the attachment.
   - To deliver the message with the detected attachments, select **Pass (not recommended)**.
3. Click **Save**.

Specifying Notification Settings When InterScan VirusWall Detects Spyware/Grayware

When ISVW detects spyware or other grayware in an incoming or outgoing message, you can specify whether to send notifications to the sender, recipient(s), and administrato.

To specify notification settings when ISVW detects spyware or grayware:

1. On the left side menu, select **POP3 > Anti-spyware** and click the **Notification** tab.
2. Select the recipients of the notification sent when spyware or grayware is detected.
3. Create the message to send to each recipient. Use any of the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

4. Click **Save**.

POP3 Content Filtering

ISVW provides email content filtering for POP3. This feature provides real-time monitoring and control of information that enters or leaves the network through POP3.

Enabling POP3 Content Filtering

When you enable POP3 content filtering, all information that enters or leaves the network through POP3 is scanned for possible matches with the policies that you have defined to filter the content of POP3 traffic. All policies that have been defined to filter content will be listed under "Policies".

To enable POP3 content filtering:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Content Filtering Settings**, select the **Enable POP3 Content Filtering** check box.
3. Click **Save**.

Disabling POP3 Content Filtering

If you disable POP3 content filtering, ISVW will not monitor the content of POP3 traffic. Any other POP3 scanning features that are enabled will continue to function as specified.

To disable POP3 content filtering:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Content Filtering Settings**, clear the **Enable POP3 Content Filtering** check box.
3. Click **Save**.

Creating Policies

ISVW uses policies that can use either a keyword filter or an attachment filter.

To create a policy:

To create a policy, click either **Add keyword filter** or **Add attachment filter**.

Creating a POP3 content filtering policy based on keywords

Keyword filters allow the ISVW administrator to evaluate and control the delivery of email messages based on the message content itself. Use these filters to monitor both inbound and outbound messages to check for sensitive or offensive content. The

keyword filter also provides a synonym-checking feature, which allows you to extend the reach of your policies. The keyword filter supports scanning of content in double-byte characters, such as messages in Chinese or Japanese.

Keyword lists

The keyword list for a given keyword filter contains the words and phrases matched by the filter to message content. When multiple keywords are included on the same line of a policy, a match occurs only when the message being evaluated contains all of the keywords on that line. For example, you can use the following keywords to a list.

Example 1:

resume, position

resume, job

resume, experience

resume, enclosed

In this example, the word "resume" appears with an additional word four times instead of using it just once as a single entry. Using just resume would probably produce unreliable results because resume can mean either curriculum vitae or to start again. To minimize the chance of such false matches, it is a good idea to qualify the primary word with additional words typically associated with it; in this example, words that are likely to appear in a job-seeking letter include enclosed, position, job, and experience. Including several keyword groups will increase the reach of the filter.

As configured in the example, messages that contain any of the keyword pairs are considered a match.

Alternatively, the filter could trigger the configured action only when all five words appear in a single outbound message. To do this, include all the keywords on a single line.

Example 2:

Resume, position, job, experience, enclosed

Obviously, the likelihood of detecting every outbound resume on the basis of this filter is much less than for a policy that contains several rule sets based upon the word resume, as shown in Example 1.

Example 3 shows a policy wherein the occurrence of any one of the four words in Example 2 triggers a match.

Example 3:

job

resume

enclosed

position

experience

Generally speaking, keywords linked by the AND operator should not include more than four or five words or the policy risks being overly restrictive. On the other hand, if only one keyword appears on any given line (OR operator), the policy risks being too permissive—too many email messages will match. Of course, as shown above, a lot depends upon what you are filtering.

The criteria you specify are evaluated exactly as entered, including any spaces and punctuation. Phrases delimited by commas are treated as a single unit. Only when each word, space, and so on in the phrase appears in the message, in the order entered, will a match occur.

Operators on keyword lists

Consider the following cases for keywords and the logical operators that apply to them based on the position of the keywords:

TABLE 7-7. Keyword list showing logical operators and sample matching results

Case	*Result*
In the following examples, items within brackets [...] are for example purposes only and should not be included when creating the keyword list.	
Case 1. Keywords appear on a single line Example: Apple Juice, [AND] Pear, [AND] Orange Provides the same capabilities as the Logical Operator "AND"	Only messages containing all items, Apple Juice, Pear, and Orange (in any order, anywhere in the message text) are considered a match.
Case 2. Keywords each appear on their own individual lines Example: Apple Juice [OR] Pear [OR] Orange Provides the same capabilities as the Logical Operator "OR"	All messages containing the phrase *Apple Juice* are considered a match, all messages that contain the word Pear are considered a match, and all messages that contain the word Orange are considered a match.
Case 3. Keywords appear on a single line and synonym checking is enabled for the word Orange Example: Apple Juice, [AND] Pear, [AND] Orange (*The words orangish, red, and yellow in the synonyms list are synonymous with the word orange.) Provides the same capabilities as the Logical Operators "AND" and "OR"	With synonym checking on, messages that contain the phrase *Apple Juice,* the word *Pear,* and any of the words *Orange, orangish, red,* or *yellow* are considered a match.

Other keyword notes

Note that Apple Juice is a phrase because the words Apple and Juice are not delimited

with a comma; even if the words Apple and Juice both appear somewhere in the message, no match will be triggered unless they occur together as Apple Juice.

The capitalization and exact-match properties of synonyms are consistent with those defined for the keyword itself. In other words, if the word red appears in the synonyms list, it will trigger a match with the word Red if Exact Match is not checked; likewise, the word red will trigger a match with the word Red in the message text if Match Case comparison is not checked.

If a user adds multiple keywords in a single line separated by commas, the policy will be triggered only when all the keywords at that line appear in the same part of the mail. For example, if a user adds the keywords apple, pear, if apple appears in the subject of the message and pear appears in the body, the policy will not be triggered.

Adding a policy based on a keyword filter

To create a policy that uses keywords as the criteria to filter POP3 content, use the POP3 Content Filtering Keyword Filter Target tab to specify the policy rules.

To add a policy based on a keyword filter:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, click the **Target** tab.
4. In the **Policy name** text box, type a policy name.
5. For **Policy status**, select **Enable** to apply the policy or **Disable** if you do not want to apply it.
6. In **Apply policy to**, select the sections of the messages (Subject, Body, or Attachment) to which this policy applies.
7. If you want the policy to block messages with attachments larger than a specified size, select **Filter if message size is larger than**, and specify the size limit.
8. Under **Keywords**, type the keywords for which you want ISVW to scan messages and click **Add**. To specify synonyms for each keyword, click the link under the **Synonyms** column (default is [none]).

   If desired, enable any of the options **Match case**, **Exact match**, and **Synonyms**.

Note: For more information in creating a keyword list for your policy, see *Creating a POP3 content filtering policy based on keywords* on page 7-30.

9. To reduce the chances of ISVW blocking messages that should be allowed to pass, type keywords that will identify these messages in **Exception keywords**. Messages that contain these keywords will not be blocked by the policy even when a match is made with a keyword filter.
10. Click **Save**.

Modifying a keyword's synonym list

ISVW has a predefined list of synonyms for certain keywords. To view this predefined list and add the words as synonyms for your keyword, use the Edit Synonyms screen.

You cannot modify or add to the predefined list of synonyms.

To modify a keyword's synonyms list:

1. On the **Keyword Filter Target** tab, select the value in the **Synonyms** column for the keyword whose synonyms you want to modify.
2. When the message box appears, click **OK** to proceed to the Edit Synonyms screen.
3. If you have entered multiple keywords that you separated with commas, all the keywords will appear in a drop-down box. Select the one keyword for which you want synonyms to be displayed.
4. Select the synonyms you want to use for the keyword from the list of synonyms in the **Exclude Synonyms** column and click **<** to move the synonyms into the **Include Synonyms** column.
5. Click **Save**.

Setting the action on messages that match the keyword filtering policy

When a POP3 message meets the filtering criteria that you have specified, ISVW can take one of three actions on the message.

To set the action on messages that match the content filtering policy:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, click the **Action** tab.

4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To delete the message, select **Delete**; messages will not be delivered.
   - To deliver the message, select **Pass**. Users will receive the message.
5. Click **Save**.

Specifying notification settings when a message meets the filtering criteria

You can send a notification to the administrator and the recipients that ISVW has detected prohibited content in an incoming mail message attachment.

To specify notification settings when a message triggers a policy:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, select the **Notification** tab.
4. Select the recipients of the notification.
5. Create the message to send to each recipient. You can use the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken

Token	Description
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

6. Click **Save**.

Creating a POP3 content filtering policy based on an attachment filter

To create a policy that uses attachments or message headers as the criteria to filter POP3 content, use the POP3 Content Filtering Attachment Filter Target tab to specify the policy rules.

To add a policy based on an attachment filter:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, click the **Target** tab.
4. In the **Policy name** text box, type a policy name.
5. For **Policy state**, select **Enable** to apply the policy or **Disable** if you do not want to apply it.
6. If you want the policy to block attachments of messages larger than a specified size, select **Filter if attachment size is larger than**, and specify the size limit.
7. Under **Message Headers**, you can specify whether you want to apply this rule when strings in the message header match certain conditions, including the From, To, CC, and Reply-to fields. Select whether you want to block or pass messages based on the header strings.

   You can specify multiple entries in the message header text boxes and separate each entry with a comma. For example, `user1@isvw.com,user2@isvw.com`.

   - Select **Apply this rule when the message header matches these conditions** to apply the settings under Attachment Characteristics to message headers that match the header strings you specified.
   - Select **Do not apply this rule when the message header matches these conditions** to apply the settings under Attachment Characteristics to message headers that do not match the header strings you specified.

8. Specify the header rules.
9. Under **Attachment Characteristics**, select the filtering criteria for message attachments.
   - **File Name**—specify a file name or a string using a wildcard (*). ISVW will filter all attachments with file names that match the names or the strings.
   - **MIME Types**—specify the MIME types to filter.
   - **Attachment File Types**—specify file type categories that you want to block. ISVW will block all attachments that are in the specified file type categories.

Note: To specify multiple entries in the File Name and MIME Types text boxes, separate each entry with a comma; for example, ***.jpg,*.txt** or **text/plain,image/jpeg**.

---

10. Click **Save**.

Setting the action for a POP3 content filtering policy

When a POP3 message meets the filtering criteria that you have specified, ISVW can take one of three actions on the message.

To set the action on messages that match the policy for attachments:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, click the **Action** tab.
4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To deliver the message, select **Pass**. Users will receive the message.
   - To remove the attachment, select **Delete attachment and pass**. Users will receive the message without the attachment.
5. To insert a notification into the body of the message, select **Insert the following notification in the message:**. You can modify the text of the message that you insert and use the following tokens:
   - %FILENAME%: the name of the removed attachment

- %RULENAME%: the name of the policy

6. Click **Save**.

Specifying notification settings when a message attachment meets the filtering criteria

You can notify the administrator and the recipients that ISVW detected prohibited content in an incoming mail message attachment.

To specify notification settings when a message triggers a policy:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, select the **Notification** tab.
4. Select the recipients of the notification.
5. Create the message to send to each recipient. You can use the following tokens or tags on the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the ISVW machine

6. Click **Save**.

Copying or Deleting a POP3 Content Filtering Policy

To copy an existing POP3 content filtering policy and modify it or delete a policy that is no longer desired:

1. On the left side menu, select **POP3 > Content Filtering**.
2. Under Policies, select a policy and click **Copy** or **Delete**.
3. Click **OK** on the pop-up message box to finalize changes.

POP3 Configuration

Before you can configure the ISVW POP3 service, you must enable it. To access the POP3 Configuration screen, select **POP3 > Configuration** on the left side menu.

On the POP3 Configuration screen, you can configure the following:

- Specify the POP3 IP address from a drop-down list or select **All interfaces** to bind to the IP addresses associated with the server.
- Set the maximum number of simultaneous end user mail client connections.
- Specify the POP3 mail server connection.
- Map the ports of the specific POP3 servers to the listening port of ISVW.

Specifying the POP3 IP Address

Specify the IP address from the IP drop-down list where you would like the ISVW POP3 service to bind and listen.

- **All interfaces** sets the POP3 service to listen on all IP addresses that are assigned to the machine where ISVW is installed.
- **127.0.0.1** configures the service to listen on the local host, leaving it inaccessible to other machines.
- You can also select a specific IP address so that other machines can access the POP3 service through this IP address.

Setting the Maximum Number of Simultaneous Connections

To specify the maximum number of simultaneous client connections allowed, type an integer value between 1 and 100 in the text box.

Specifying POP3 Connections

The ISVW POP3 service supports two types of POP3 connections. Normally, you would select **Connect to any POP3 server requested by end-user mail clients** and then assign a port for the POP3 service.

POP3 Port Mapping

If ISVW acts as a port mapping server, map the ports of the specific POP3 servers to the listening port of ISVW.

If your server supports secure password authentication and you want to use Secure Password Authentication, you must use port mapping mode.

To map the ports of specific POP3 servers to the listening port of ISVW:

1. Select the **Enable port mapping mode and specify remote inbound pop3 server IP and its service port** check box and add tuples.
2. For each of the tuples, specify:
   - **Inbound POP3 port**—the port on which the ISVW POP3 service listens
   - **IP address**—the address of the specific POP3 server
   - **POP3 server port**—the port that the server uses for POP3
3. Click **Add** to add each tuple to the list on the right. To delete a specific tuple, click the trash bin icon.
4. Click **Save** to finalize changes.

Note: Do not allow other programs to use the IP addresses and the ports that you specify because the ISVW POP3 service will fail to bind to and listen on those ports if the ports are being used.

Configuring Outlook Express

To configure Outlook Express as the end user mail client:

1. In Outlook Express, click **Tools > Accounts**. The Internet Accounts screen appears.
2. Click **Add > Mail**. The Internet Connection Wizard launches.
3. Type the user's user name, such as John Smith, on the Your Name screen in the Internet Connection Wizard. Click **Next**.
4. Type the user's email address, such as John_Smith@anycompany.com, on the Internet E-mail Address screen. Click **Next**. The E-mail Server Names screen appears.
5. Select POP3 in the **My incoming mail server is a...**.
6. Type the address (192.168.5.139 as an example) for the ISVW server in Incoming mail (POP3, IMAP, or HTTP).
7. Type the address for the ISVW server in Outgoing mail (SMTP) server. Click **Next**.
8. If the POP3 server does not require secure password authentication:
   a. On the Internet Mail Logon screen, type the account name the user will use to retrieve his or her POP3 mail in Account name. The format must be name, followed by the pound sign (#), then the name of the POP3 server, then another # followed by the port number, if it is not 110. For example:

      someusername#pop3.earthlink.net

      someusername#pop3.earthlink.net#111

   b. Type a password for the user's POP3 mail account. Check **Remember password** if appropriate.

   If the POP3 server requires secure password authentication:

   a. On the Internet Mail Logon screen, type the account name the user will use to retrieve his or her POP3 mail in Account name.

   b. Select **Log on using Secure Password Authentication (SPA)**.

   c. Click **Next**.
9. Click **Finish** on the Congratulations screen. When you view the Internet Accounts screen again, the POP3 connection appears.

Note: SPA requires that you set up a corresponding (inbound port, server, port) tuple on the ISVW POP3 Configuration screen. You may need to change the default POP3 port setting in your mail client into “inbound port” in the specific tuple, as shown in *Figure 7-9*.

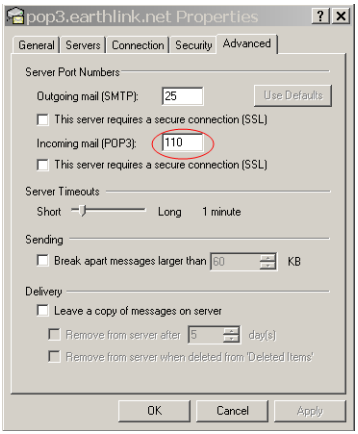


FIGURE 7-9. Advanced Properties Tab

Enabling POP3 Transaction Logging

Currently ISVW supports transaction logging for POP3. Transaction logging for POP3 is enabled by default.

To enable or disable POP3 transaction logging:

1. Open the file Config.xml
2. Search for the key named "WriteConnectionMsg" located under "POP3".
3. Set "WriteConnectionMsg" value to "1" (enabled) or "0" (disabled).
4. Restart the service.

Chapter 8

Outbreak Prevention Services

Outbreak Prevention Services (OPS) allows you to receive updates directly from TrendLabs to help stop virus and worm outbreaks as interim protection from threats while a solution is being developed. OPS has automatic deployment options available to the administrator, including when to activate an outbreak policy and how long to keep the policy in effect.

An OPS policy is activated depending on the issue date and expiration period set within the policy. If OPS is activated, and the OPS policy that Trend Micro has issued has an expiration date that occurs after the current system time, then that policy is activated. Trend Micro specifies the duration of the policy but you can manually override it if desired.

To receive OPS policies for POP3, SMTP, HTTP, and FTP services, you must have these services enabled to enable corresponding OPS policies.

Enabling Outbreak Prevention Services

To enable OPS and view detailed status information:

1. On the left side menu, select **Outbreak Defense > Current Status**.
2. Select the **Enable Outbreak Prevention Services (OPS)** check box.
3. Click **Save**.

To see whether Outbreak Prevention Services (OPS) is enabled and active:

1. On the left side menu, select **Summary** and then click the **Status** tab.
2. If necessary, click the icon on the right to expand the Outbreak Prevention Services information so that you can check the status of the services.

Figure 8-1 shows a sample Summary Status tab with information about Outbreak Prevention Services.

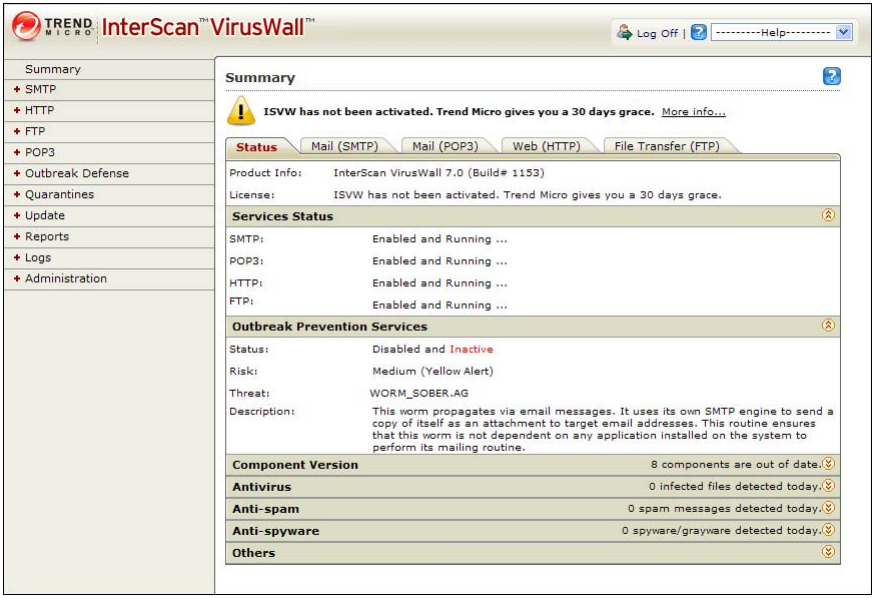


FIGURE 8-1. Summary Status Tab

Available Current Status

Since Trend Micro issues and manages the OPS policies, you can view but not modify the rest of the information on this screen.

- The **Threat Status** section provides status of the current threat.
- The **Attachment Filter** section lists the types of files in email messages (through POP3/SMTP services) that are blocked.

  - File names being blocked solely matches file extensions (the "*" wildcard can be used in the name only, not the extension).
  - File types being blocked detects the true file type from actual file content and blocks by type. The numbers that appear here are internal file type representations for ISVW.
- The **Content Filter** section shows which email message contents (through POP3/SMTP services) OPS is blocking. This is a regular-expression filter for mail attachment name. The wildcard characters "*" and "?" can be used in the expression.
- The **URL Blocking** section lists the URLs (through HTTP service) that OPS is blocking.
- The **File Blocking** section shows the type of files (through HTTP and FTP services) that OPS is blocking.

Configuring Settings for Outbreak Prevention Services (OPS)

Trend Micro specifies the expiration time of OPS policies, but you can manually change the time.

To configure the settings for OPS:

1. On the left side menu, select **Outbreak Defense > Settings**.
2. Under **OPS Expiration Disable Outbreak Prevention Services**, specify when you want the alert for the Outbreak Prevention Policy (OPP) to expire. The expiration date is based on when the OPP is issued.
3. To schedule policy download settings, select the **Enable scheduled policy update** check box and select a download frequency (expressed in minutes) for OPS policies.
4. Click **Save**.

Note: If InterScan VirusWall (ISVW) downloads and activates a new OPS policy, this setting will be overwritten. To manually manage the effective duration of the OPS policies, modify the expiration period for each individual OPS policy.

Chapter 9

Quarantines

If you specify that InterScan VirusWall (ISVW) quarantine files and email messages when it detects a security risk, it will move all infected files to a quarantine directory. ISVW uses separate quarantine directories for each protocol.

The Quarantine feature of ISVW allows you to do the following:

- Query the SMTP/POP3 quarantine directories to obtain information about the files that are in the directories
- Specify the directory paths for the quarantine folders for SMTP, HTTP, FTP, and POP3
- Specify whether you want to have files in the directories deleted automatically or manually delete files whenever desired

Quarantine Query

ISVW has a query feature that allows you to generate reports about the types of files that it has quarantined and the reasons the files were quarantined for the SMTP and POP3 protocols. For example, you can specify criteria that would generate a report of all spam messages that a specific email address received during a two-week period.

Note: You can only query the files that are currently in the SMTP and POP3 quarantine folders. If you have purged the folders, you will be unable to obtain information about the deleted files.

Generating a Query

To see details regarding SMTP/POP3 quarantined email messages and attachments, specify criteria for the query and view the results. *Figure 9-1* shows the Quarantine Query page that allows you to specify criteria for a query.

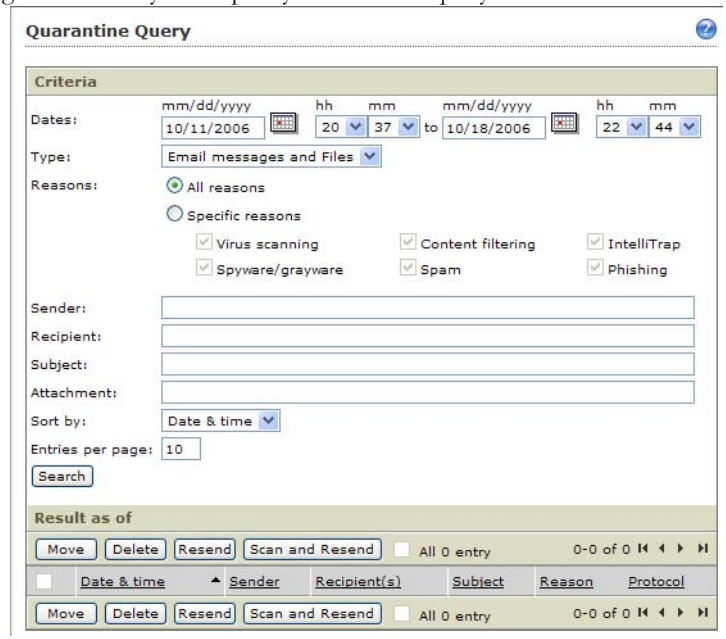


FIGURE 9-1. Quarantine Query Page

To generate a query:

1. From the left side menu, select **Quarantines > Query**.
2. Specify the criteria for the query.

- **Dates:** Enter the date and time range that you want to view.
- **Type:** Choose whether to query quarantined email messages, files, or both types.
- **Reasons:** Select quarantine reasons, either **All reasons** or **Specific reasons**. For **Specific reasons**, select the appropriate check boxes for Virus/Malware, Spyware/Grayware, Content filtering, Spam, IntelliTrap, and Phishing.
- **Sender:** Type a keyword included in the Sender field of email messages.
- **Recipient:** Type a keyword included in the Recipient field of email messages.
- **Subject:** Type a keyword included in the Subject field of email messages.
- **Attachment:** Type a keyword included in the file name of the attachment (file).
- **Sort by**: Choose a sort criteria for the query results, either **Date and time**, **Sender**, **Recipient**, **Subject**, or **Reason**.
- **Entries per page:** Type a number between 1 and 100 to specify how many items to show on one page.

3. Click **Search** to view the results.

Manipulating the Query Results

To re-sort the results, click the column header in the query result table.

To move or delete items, select one or more of the corresponding check boxes and click **Move** or **Delete**.

When you click **Move**, the Move Quarantine Items page opens. Specify the destination directory where you want to move the items and then click **Move**.

To resend or scan and resend quarantined SMTP email messages, select one or more of the corresponding check boxes and then click **Resend** or **Scan and Resend**.

When you click **Resend**, ISVW attempts to send the quarantined SMTP email messages to the initial recipient(s). When you click **Scan and Resend**, ISVW will first scan the selected quarantined SMTP email messages. If no threats are found, the items will be sent to the initial recipient(s).

Note: The Resend and Scan and Resend actions may take several hours to complete. The duration is dependent on a number of factors including but not limited to the number of items selected, network speed, and processing power of the ISVW server.

Quarantine Directory Settings

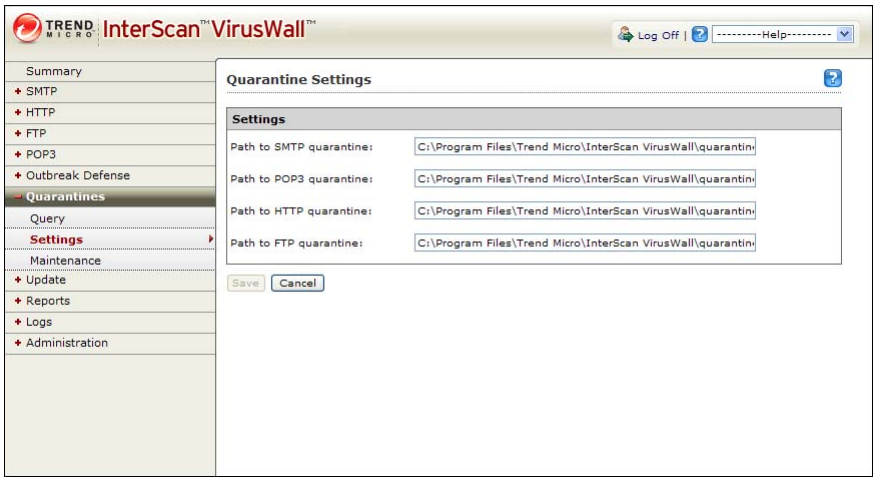
By default, ISVW creates separate quarantine directories for each protocol as follows:

- \quarantine\smtp
- \quarantine\http
- \quarantine\ftp
- \quarantine\pop3

To specify different quarantine folders use the Quarantine Settings feature. Absolute paths are required, and you must specify a different path for each protocol.

Figure 9-2 shows the Quarantine Settings page that allows you to modify the default directory paths for quarantined files.

FIGURE 9-2. Quarantine Settings Page



To modify the quarantine directory for SMTP, POP3, HTTP, or FTP scanning:

1. On the left side menu, select **Quarantines > Settings**.
2. Type the absolute path for each of the protocols whose quarantine directory you want to change.

   Each protocol must have a different folder for its quarantined items.
3. Click **Save**.

Quarantine Maintenance

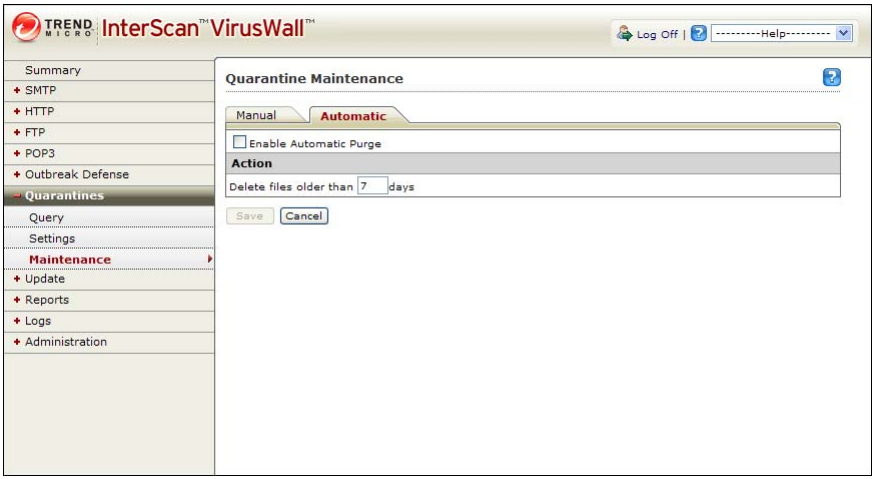
Quarantine directories need periodic purging to avoid a large volume of undesired files accumulating. ISVW allows you to schedule periodic maintenance of the quarantine directories, which means that you can have quarantined files deleted daily, weekly, monthly, or at any interval (in days) that you specify, up to once every 360 days.

You can also manually delete quarantined files. ISVW will delete all files that have been in the folder longer than the time that you specify.

Automatic Maintenance

To schedule automatic maintenance for purging the files in the quarantine folders, use the automatic quarantine maintenance feature shown in *Figure 9-3*.

FIGURE 9-3. Quarantine Maintenance Automatic Tab



To schedule automatic deletion of quarantined files:

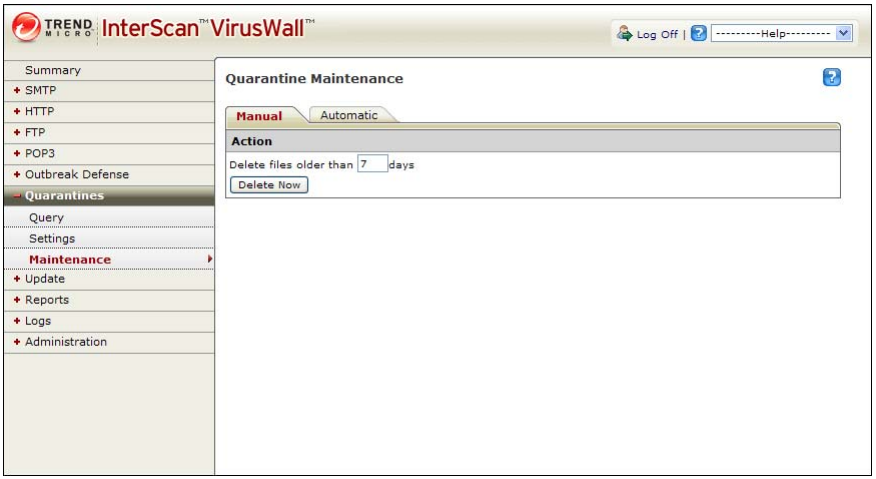
1. On the left side menu, select **Quarantines > Maintenance**.
2. Click the **Automatic** tab.
3. Select the **Enable automatic purge** check box.
4. Enter an expiration age in days between 0 and 360 into the text box.

   ISVW removes all files that have been quarantined longer than this period, including email messages, attachments, and files received through SMTP, POP3, HTTP, or FTP.
5. Click **Save**.

Manual Maintenance

To manually purge the files in the quarantine folders, use the manual quarantine maintenance feature shown in *Figure 9-4*.

FIGURE 9-4. Quarantine Maintenance Manual Tab



To manually delete quarantined files:

1. On the left side menu, select **Quarantines > Maintenance**.
2. Click the **Manual** tab.
3. Enter an expiration age in days between 0 and 360 into the text box.

   ISVW removes all files that have been quarantined longer than this period, including email messages, attachments, and files received through SMTP, POP3, HTTP, or FTP.
4. Click **Delete Now**.

Chapter 10

Update

New malicious programs and offensive Web sites are developed and launched every day, so it is imperative that you keep your software updated with the latest pattern files, scan engine, and URL filtering database.

Trend Micro provides an automatic update service that ensures that your computers contain the latest protection against security threats. ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to download pattern files, the scan engine, and the URL filtering database.

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.

InterScan VirusWall (ISVW) can poll the ActiveUpdate server directly for updated components. These updated components are deployed to ISVW on a schedule that you define, such as:

- Minute(s)
- Hour(s)
- Day(s)
- Week(s)

Components Available for Update

The following components of ISVW can be scheduled for regular automatic updates or you can update the components manually. You can also roll back certain components to their previous version.

COMPONENT	DESCRIPTION
Virus pattern	File that contains the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, ISVW 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.
Scan engine	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.
IntelliTrap pattern	File that contains the binary "signatures" or patterns of known viruses in files compressed up to 20 layers deep using any of 16 popular compression types. The IntelliTrap pattern file is updated whenever new threat information is available.
Spyware detection pattern	File that contains the binary "signatures" or patterns of known spyware/grayware security risks. When used in conjunction with the scan engine, ISVW is able to detect known risks as they pass through the Internet gateway. The spyware detection pattern file is updated whenever new threat information is available.
PhishTrap pattern	File that contains the binary "signatures" or patterns of known phishing site security risks. When used in conjunction with the scan engine, ISVW is able to detect known risks as they pass through the Internet gateway. The PhishTrap pattern file is updated whenever new threat information is available.
Anti-spam rules and engine	The module that analyzes the content of a message or attachment and compares it against predefined categories of spam, default detection levels, and lists of approved and blocked senders.

How Trend Micro Products Detect Security Threats

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 ISVW management console displays the following format:

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

- **Roll number** represents the number of rounds when the pattern version exceeded 999 and could be up to five digits.
- **Pattern version** is the same as the pattern extension of lpt$vpn.### and contains three digits.
- **Build number** 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 **Update > Scheduled** page. Updates are available to all Trend Micro customers with valid maintenance contracts.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire 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.

Updating Components Manually

You can manually update pattern files, engines, and databases at any time, either using the Summary page or the Manual Update page. You can also roll back to the previous version of a virus pattern file, spyware detection pattern file, or IntelliTrap pattern file, if necessary. If you decide to roll back to a previous version, you cannot update to the version that you had installed before you rolled back; you must wait for a new version to be available for the rolled back component before you can update.

Using the Summary Page to View and Update Components

The Summary page displays the pattern version status and update availability for each component, similar to the **Component Version** section shown in *Figure 10-1*.

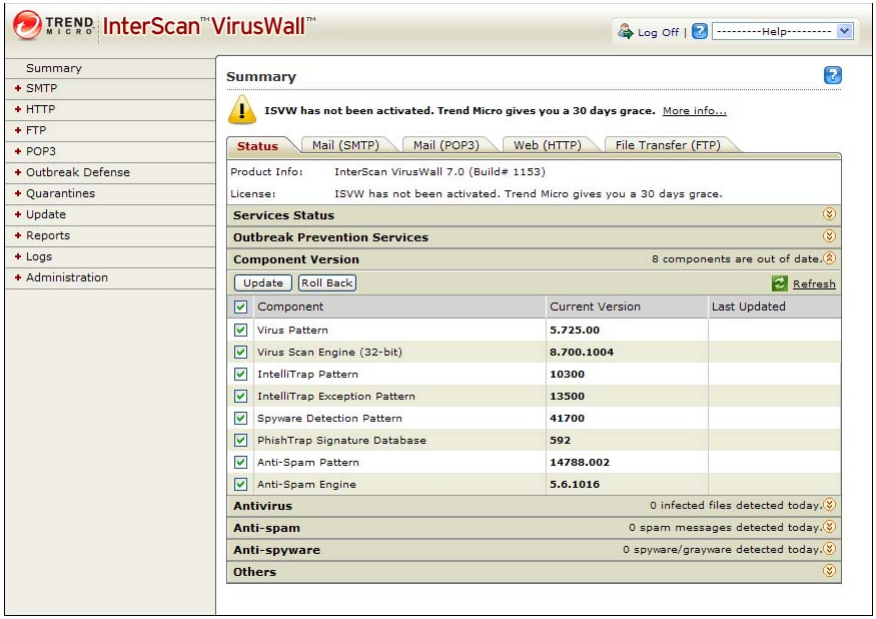


FIGURE 10-1. Summary Page—Component Versions

You can update to the latest pattern files or roll back to a previous version. If you roll back to a previous pattern file, you cannot update that particular pattern file until a version newer than the current one becomes available.

Note: Only three patterns support rollback. They are the virus pattern, spyware detection pattern, and intellitrap pattern

---

To update or roll back a component:

1. Ensure that you are on the **Status** tab of the **Summary** screen.
2. Select the check box next to the component you want to update or roll back.

   To select all the components, select the check box next to "Component" column name or select any of the following:

   - Virus pattern[1]
   - IntelliTrap pattern[1]
   - IntelliTrap exception pattern[1]
   - Spyware detection pattern[1]
   - Virus scan engine (32-bit)
   - PhishTrap signature database
   - Anti-spam pattern
3. Click **Update** or **Rollback** to refresh the selected files.
4. Click **Refresh** to view the new versions and modification dates of the components.

Note: Only those components marked with a [1] can be rolled back.

Updating Components through Manual Update

The manual update feature checks for the latest available components and then displays the version number for the components that you have currently installed and the version number for all available updates.

To update components manually:

1. On the left side menu, select **Update > Manual**.

   When the Manual Update screen opens, the message "Please wait while ISVW checks the availability of new components..." displays while ISVW searches for the latest updates.
2. When the Select Components to Update screen appears, select the pattern files and engines for which you would like to obtain updates.
3. Click **Update**.

Note: You can also roll back to a previous version of a pattern files but if you do, you will be unable to update the current versions of pattern files until a version newer than the one that you have rolled back is available. only three patterns support rollback. They are the virus pattern, spyware detection pattern, and intellitrap pattern.

Scheduling Updates

Trend Micro recommends that you update components daily, preferably during times of low traffic volume. The Scheduled Update screen allows you to specify automatic updating of pattern files, scan engines, and database components.

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

1. On the left side menu, select **Update > Scheduled**.
2. Select the **Enable Scheduled Updates** check box.
3. Select the check box next to each of the components you want to update.
4. Select the update interval. The information on the right side will change, depending on whether you select **Minute(s)**, **Hour(s)**, **Day(s)**, or **Week(s)** on the left side.
5. Click **Save**.

ISVW will then check the ActiveUpdate server at the interval you specified and will automatically download any new component updates that are available for the components that you selected for automatic update.

Updating InterScan VirusWall

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

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

When the Update Center screen displays, select the **InterScan VirusWall for SMB** link on this screen. Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Chapter 11

Local Reports

Reports in InterScan VirusWall (ISVW) summarize all types of traffic violations. For HTTP Web violations, reports can also include the users violating within a specified time period. Reports can include the following information:

- What virus occurred
- From when and where the viruses came
- Violating users for a given time period (up to six months) along with the types and frequency of violations

This chapter describes the following topics:

- *Managing Report Profiles*
- *Managing Generated Reports*
- *Performing Report Maintenance*

Managing Report Profiles

This section describes how to create a new report profile, specify the frequency at which reports should be generated, how to modify an existing report profile, and finally how to delete a report profile.

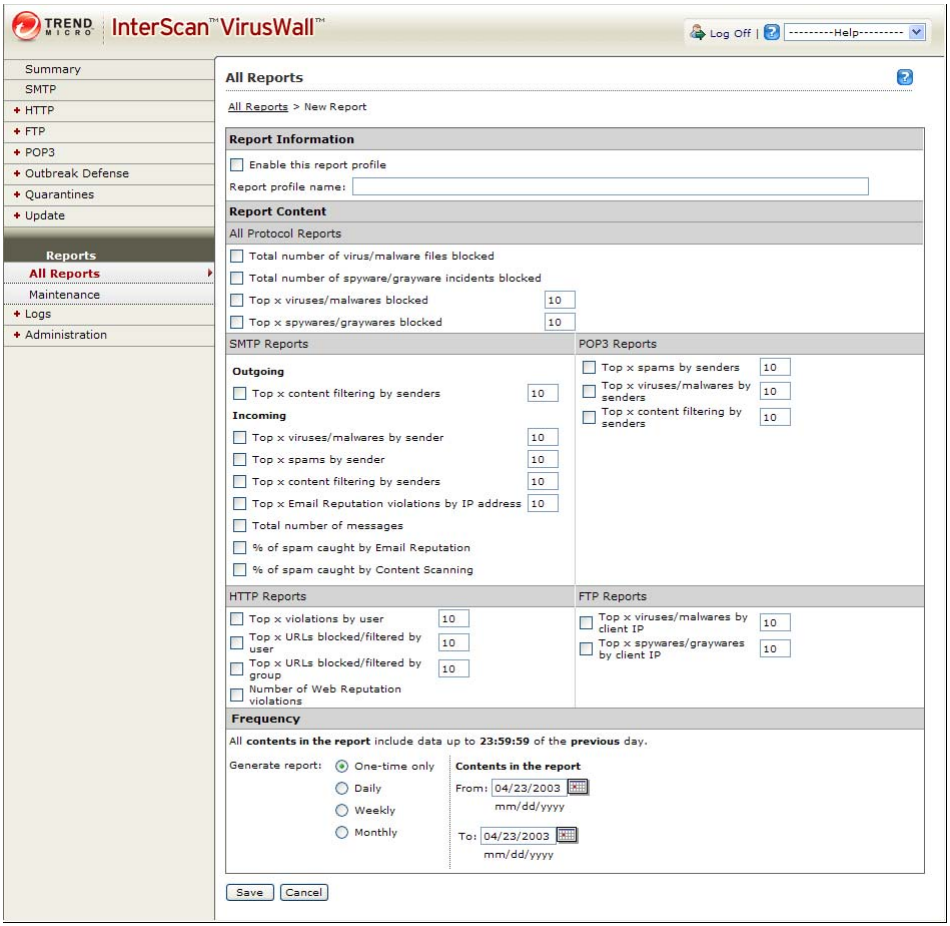
Creating a New Report Profile

To create a new report profile:

1. Go to **Reports > All Reports**.
2. Click **New Report**.

   The All Reports screen appears (see *Figure 11-1*).

FIGURE 11-1. The All Reports screen



3. In the "Report Information" section, specify the report profile name and whether you want to enable the report profile.

   If you select the **Enable this report profile check box**, then ISVW generates a new report based on the specified report profile.

4. In the "Report Content" section, select the report options you want as part of the report profile.

   Ten (10) is the default value for all options with a variable.

5. Specify when the report should be generated.

   See *Specifying Report Frequency* on page 11-4 for complete details.

6. Click **Save**.

   The new report profile appears in the "Reports" table of the All Reports screen.

Specifying Report Frequency

This section describes how to specify the report frequency for a new report and how to change this for an existing report.

To specify the report frequency:

1. Go to the "Frequency" section of the All Reports screen.
   - For a new report profile, go to **Reports > All Reports** and click **New Report**.
   - For an existing report profile, go to **Reports > All Reports** and click on a report profile in the "Reports" table.
2. From the "Generate report" area, specify the frequency at which reports should be generated.
   - One-time only—this option requires you to specify the duration period, the start and end dates for which the report will be generated
   - Daily—this option requires you to specify the daily starting hour for when the report will be generated. (This values provided in the **start at** drop-down list are based on 24-hour time.)
   - Weekly—this option requires you to specify the day and time for when the report will be generated. (This values provided in the **start at** drop-down list are based on 24-hour time.)
   - Monthly—this option requires you to specify the day of the month and time for when the report will be generated. (This values provided in the **start at** drop-down list are based on 24-hour time.)

Modifying an Existing Report Profile

To modify an existing report profile:

1. Go to **Reports > All Reports**.
2. Click on the desired report profile link in the "Reports" table.

   The All Reports screen appears (see *Figure 11-1*).
3. In the "Report Information" section, make any changes to the report profile name and whether you want to enable the report profile or not.

   If you select the **Enable this report profile check box**, then ISVW will generate a new report based on the specified report profile.
4. In the "Report Content" section, make any necessary changes in this section by selecting or un-selecting report options.
5. To change the report generation time, see *Specifying Report Frequency* on page 11-4.
6. Click **Save**.

   The updated report profile appears in the "Reports" table of the All Reports screen.

Deleting a Report Profile

To delete a report profile:

1. Go to **Reports > All Reports**.
2. In the Reports table (check box column), check the check box of the desired report profile and then click **Delete**.

   ISVW removes the desired report profile from the Reports table.

Managing Generated Reports

This section describes how to view and delete generated reports.

Viewing Generated Reports

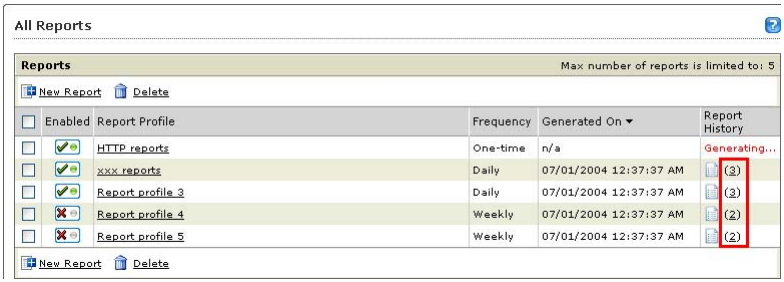
To view a generated report:

1. Go to **Reports > All Reports**.

   The All Reports screen appears.

2. In the Reports table (Report History column), click the number next to the report icon for the desired report (see *Figure 11-2*).

   FIGURE 11-2. Report icon as listed in the Reports table



   The Report History screen opens showing all the reports for the report profile. Reports can be generated either in HTML or XML.

3. In the Report History table (View Report column), click the desired report link.

   The report opens.

4. Scroll to the bottom of the report and then click **Close** to exit the report.

Deleting a Generated Report

To delete a generated report:

1. Go to **Reports > All Reports**.

   The All Reports screen appears.

2. In the Reports table (Report History column), click the number next to the report icon for the desired report (see *Figure 11-2*).

   The All Reports screen displays the Report History table, which shows all the reports for the report profile.

3. In the Report History table (check box column), check the check box of the desired report and then click **Delete**.
4. Click **Back** to exit Report History.

Performing Report Maintenance

Report maintenance is specifying the maximum amount of reports kept in ISVW. This specified value controls the number of reports available to you in the All Reports screen (see *Managing Generated Reports* on page 11-5).

To specify the maximum amount of reports kept in ISVW:

1. Go to **Reports > Maintenance**.

   The All Reports screen appears.
2. In the "Maximum Reports to Keep" column, specify a value between 1 and 30 and then click **Save**.

Chapter 12

Logs

InterScan VirusWall (ISVW) tracks all scanning and detection activity that it performs and writes this information to various logs. The log query feature allows you to create reports that show detection activity for the different protocols for the various types of scanning tasks that ISVW performs. You can also view the event log.

Since logs accumulate and occupy disk space, ISVW allows you to schedule automatic purging of logs, and to purge logs manually.

You can access all log files under {Installation Folder}\Log. The log types are as follows:

TABLE 12-1. Log File Descriptions

Log Type	Description
DebugLog	Provides debug information for all protocols, by default, it is not open.
Eventlog	Event information is written to this log
Systemlog	System level information is written into this log
Viruslog	Logs all viruses found
Antispylog	Logs all spyware/grayware found
Antispamlog	Logs the spam mails and phishing mails found in SMTP and POP3 traffic

TABLE 12-1. Log File Descriptions

Log Type	Description
Emanagerlog	Logs the mails that trigger keyword filter/attachment filter in SMTP and POP3 traffic
UrlAccesslog	Logs the requests in HTTP traffic
urlblocklog	Logs the pages or files that are blocked by HTTP URL blocking, URL filtering, and phishing
connectlog	Logs SMTP, POP3, HTTP, and FTP transactions
nrslog	Logs the emails that are blocked by Email Reputation

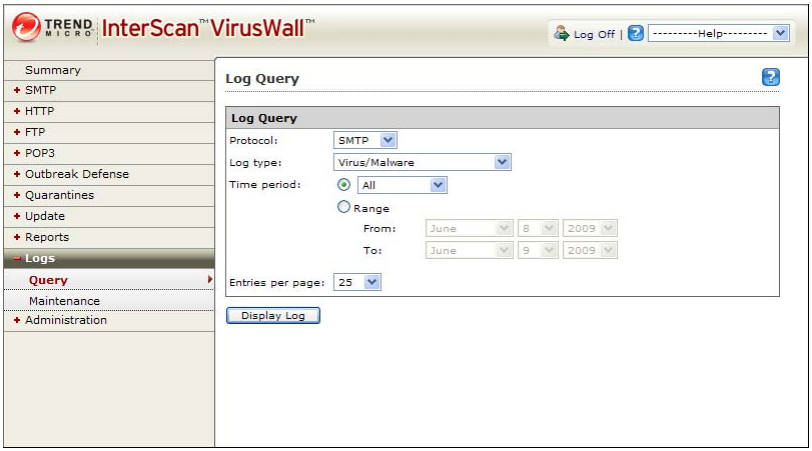
Use UltraEdit or Notepad to open the log files manually. You can also use the Web console to query logs.

Note: You can view log statistics, except for debug, system, event, and connection logs, from the Summary screen of the Web management console.

Log Query

The log query feature allows you to view logs for different scanning activities and to export the results to an Excel spreadsheet or other similar type of program.
Figure 12-1.shows the options available to generate a log query.

FIGURE 12-1. Log Query Screen



To query logs and generate a report:

1. On the left side menu, select **Logs > Query**.
2. Select the protocol whose ISVW logs you want to query.
3. Select the **Log type**.

   Different protocols have different log types.

Protocol	Available Log Types
SMTP/POP3	Virus/Malware Spyware/Grayware Attachment filter Keyword filter Anti-spam Anti-phishing Email Reputation (Only for SMTP)
HTTP	Virus/Malware Spyware/Grayware URL Blocking URL Filtering URL Accessing Web Reputation
FTP	Virus/Malware Spyware/Grayware

Protocol	Available Log Types
Others	Event Log

4. Select a predefined duration or specify a range of dates for which you want to see log entries.
5. Specify how many log entries to display on a page.
6. Click **Display Log** to display query results.

To export the query results to a file in text, XML or CSV format, click **Export**, and choose a file type to export from the Export Log File screen.

To manipulate the query results:

To change the number of result entries that are displayed per page, select from the **Entries per page** drop-down list.

To switch to other pages of results, click arrow buttons or select from the Page index list.

To export queried logs to a text/XML/CSV file, click **Export**.

Note: To speed up log query when there are a number of log entries to display, the Page drop-down list will not display all page indexes; that is, it will display 200 indexes around the current page, and subsequent indexes will be skipped at regular intervals.

Query Result Table Fields

When you query the different logs, the results are displayed as follows:

TABLE 12-2. Log Query Results Table Fields

Type of Log	Query Result Table Fields and Description
SMTP/POP3 Virus Log	**Date**: date and time when the item was logged. **Virus/Malware Name**: name of the virus/malware that ISVW detected. **Type**: type of virus/malware detected. **Sender:** email address of the sender. **Recipient**: list of email addresses of all recipients. **Subject**: subject of the mail. **Content Action**: action taken for the attachment when virus/malware was detected.
SMTP/POP3 Spyware/Grayware Log	**Date**: date and time when the item was logged. **Spyware/Grayware Name**: name of the spyware/grayware that ISVW detected. **Type**: type of spyware/grayware detected. **Sender**: email address of the sender. **Recipient**: list of email addresses of all recipients. **Subject**: subject of the mail. **Content Action**: action taken for the attachment where spyware/grayware was detected.
SMTP/POP3 Attachment Filter Log	**Date**: date and time when the item was logged. **Sender**: email address of the sender. **Recipient**: list of email addresses of all recipients. **Subject**: subject of the mail. **Action**: action taken when the attachment filter was matched.
SMTP/POP3 Content (Keyword) Filter Log	**Date**: date and time when the item was logged. **Sender**: email address of the sender. **Recipient**: list of email addresses of all recipients. **Subject**: subject of the mail. **Action**: action taken when the keyword filter was matched.
SMTP/POP3 Spam Detection Log	**Date**: date and time when the item was logged. **Sender**: email address of the sender. **Recipient**: list of email addresses of all recipients. **Subject**: subject of the mail. **Message Action**: action taken for the email message that was considered to be spam.

TABLE 12-2. Log Query Results Table Fields (Continued)

Type of Log	Query Result Table Fields and Description
SMTP/POP3 Phish Detection Log	**Date:** date and time when the item was logged. **Sender:** email address of the sender. **Recipient:** list of email addresses of all recipients. **Subject:** subject of the mail. **Message Action:** action taken for the email message that was considered to be a phishing type of message.
SMTP Email Reputation Log	**Date:** date and time when the item was logged. **IP address:** the IP address of client. **Action:** action taken for this connection. **Result:** action result for connection, pass or reject.
HTTP/FTP Virus Log	**Date:** date and time when the item was logged. **Virus/Malware Name:** name of the virus/malware that ISVW detected. **Type:** type of virus/malware detected. **File Name:** name of the file that contained the virus/ malware. **Client IP/User ID:** IP address or user name of the client who tried to transfer the file. **Action:** action taken for the file when the virus/ malware was detected.
HTTP/FTP Spyware/Grayware Log	**Date**: date and time when the item was logged. **Spyware/Grayware Name**: name of the spyware/ grayware that ISVW detected. **Type**: the type of spyware/grayware detected. **File Name**: the file that contained the spyware/grayware. **Client IP/User ID**: IP address or user name of the client who tried to transfer the file. **Action**: action taken for the file when the spyware/ grayware was detected.
URL Blocking Log	**Date**: date and time when the item was logged. **Client IP**: IP address of the client that tried to connect to this URL. **URL**: web page link that has been blocked. **Blocking Rule**: reason this URL was blocked.
URL Filtering Log	**Date**: date and time when the item was logged. **Client IP**: IP address of the client that tried to connect to this URL. **URL**: web page link that has been filtered. **Blocking Rule**: the reason that allowed this URL to be filtered.

TABLE 12-2. Log Query Results Table Fields (Continued)

Type of Log	Query Result Table Fields and Description
Web Reputation Log	**Date**: date and time when the item was logged. **Client IP**: IP address of the client that tried to connect to this URL. **URL**: web page link that has been filtered. **Damage Potential**: the potential damage that the blocked URL could have caused.
URL Accesses Log	**Date**: date and time when the item was logged. **Client IP**: IP address of the client that tried to connect to this URL. **Domain Name**: domain name of the web page that has been accessed. **Path**: path of the web page that has been accessed.
Event Log	**Date**: date and time when the item was logged. **Event**: ISVW activity at the time.

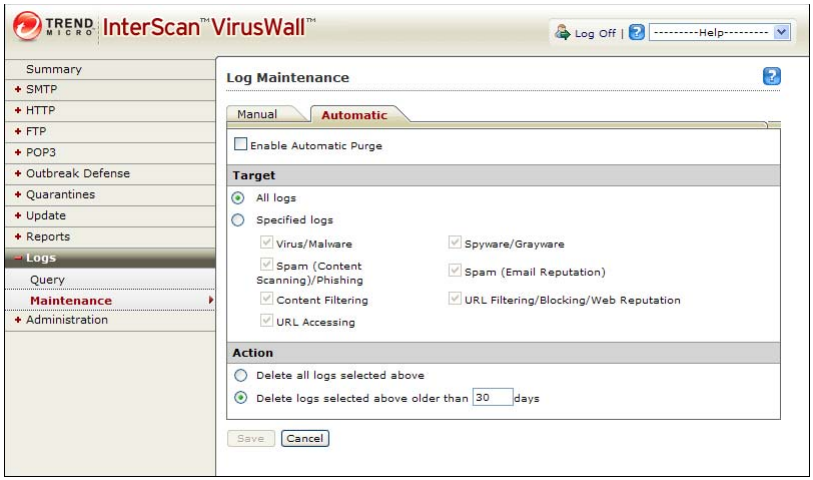
Log Maintenance

ISVW allows you to manage the number of logs that are stored on the system. You can schedule automatic purging of log files or delete them manually.

Automatic Deletion of Logs

To schedule automatic deletion of log files, access the Automatic Log Maintenance tab shown in *Figure 12-2*.

FIGURE 12-2. Automatic Log Maintenance Tab



To schedule automatic deletion of logs:

1. On the left side menu, select **Logs > Maintenance**.
2. Click the **Automatic** tab.
3. Select the **Enable automatic purge** check box.
4. Under **Target**, specify whether you want to delete **All logs** or **Specified logs**.

   If you select **Specified logs**, select the appropriate check boxes for the logs that you want to delete:

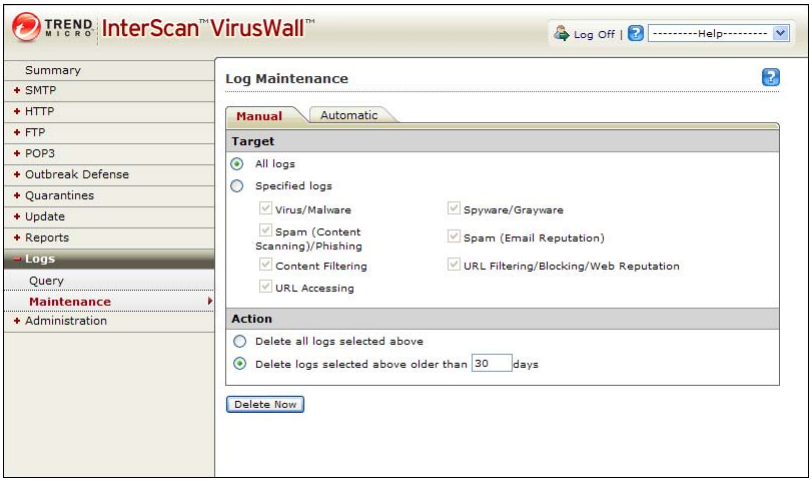
   - Virus/Malware
   - Spam (Content Scanning)/Phishing
   - Content Filtering
   - URL Accessing
   - Spyware/Grayware
   - Spam (Email Reputation)
   - URL Filtering/Blocking/Web Reputation
5. Specify whether all logs of the selected type(s) should be deleted, or only those older than a specified date.

6. Click **Save**.

Manual Deletion of Logs

To manually delete log files, access the Manual Log Maintenance tab shown in *Figure 12-3*.

FIGURE 12-3. Manual Log Maintenance Tab



To delete logs manually:

1. On the left side menu, select **Logs > Maintenance**.
2. Click the **Manual** tab.
3. Under **Target**, specify whether you want to delete **All logs** or **Specified logs**.

   If you select **Specified logs**, select the appropriate check boxes for the logs that you want to delete:

   - Virus/Malware
   - Spam (Content Scanning)/Phishing
   - Content Filtering
   - URL Accessing
   - Spyware/Grayware

- Spam (Email Reputation)
- URL Filtering/Blocking/Web Reputation

4. Specify whether all logs of the selected type(s) should be deleted, or only those older than a specified date.
5. Click **Delete Now**.

Debug and System Logs

In addition to the logs you can generate from the Web management console, you can also obtain debug logs for all the protocols and system logs. ISVW creates new logs at the beginning of a day or when the original log exceeds a specified size.

System logs include:

- ISVW Daemon Start/Stop
- Protocol Daemon Start/Stop
- Fatal errors with a brief description (*fatal* means the program fails to start because of the error)
- System errors and exceptions

You can access the debug and system logs, along with all the ISVW logs, from {Installation_ Folder}\Log. The debug log file names are debuglog.{yyyymmdd.nnnn}, where "yyyymmdd" is the date, and "nnnn" is the sequence number. To open these files, use a text editor like Notepad.

Note: By default, debug logging is not enabled.

To manually enable debug logging:

1. Open the `Config.xml` file on in the installation path; for example, {local_drive}\Program Files\Trend Micro\ISVW.
2. Search for the following: <Value Name="DebugEnable" string=""type="int" int="0" />
3. Change the text to: <Value Name="DebugEnable" string="" type="int" int="1" />

4. Save and close the file, and then restart one of the SMTP/POP3/HTTP/FTP processes or the whole ISVW service.

Chapter 13

Administration

Registering and Activating InterScan VirusWall

When you purchase InterScan VirusWall (ISVW), you will receive a product license certificate. The certificate contains a code, either a Registration Key or an Activation Code. The codes are needed to complete the following tasks:

- Product registration, which is required to receive product updates, including updates to the virus pattern file, scan engine, anti-spam rules, and anti-spam engine
- Product activation, which is required to enable ISVW to begin scanning, filtering, and blocking

If you have a Registration Key, register ISVW before proceeding. If you have an Activation Code, skip to *Activating InterScan VirusWall* on page 13-5.

Registering InterScan VirusWall

Your Registration Key or Activation Code can be found on your license certificate, which you should have received from Trend Micro shortly after your purchase of ISVW. If you do not have a license certificate, contact Trend Micro for assistance.

Figure 13-1 shows a sample license certificate with the Registration Key enclosed in red

FIGURE 13-1. Sample Trend Micro Software License Certificate


TREND MICRO SOFTWARE LICENSE CERTIFICATE

Issued to confirm the purchase by: YOUR COMPANY

Customer No:	38505
Product Name:	INTERSCAN VIRUSWALL 7
No. of License	415
Reseller Name:	BIZCO, INC.
SKU:	SEXEMME32
TM Program Number:	3144
TM Reference Number:	01008866
S/N (R/K):	AJ-43B2-P388-WJ5T-Z9Q1
Maintenance Start Date:	
Maintenance End Date:	

Customer Service and Sales Support – email sales@trendmicro.com

TREND MICRO

www.trendmicro.com

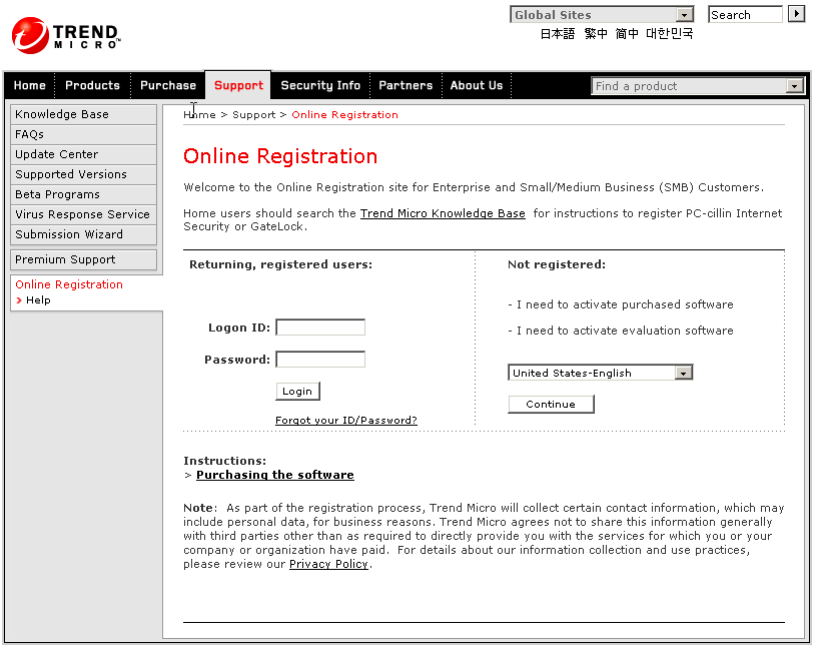
If you did not register ISVW before or during installation, register now. If you do not complete the registration process at this time, you will still be able to use ISVW under the 30-day trial period.

Registering online

1. To register online, visit the following URL:
   `https://olr.trendmicro.com/registration`

The Trend Micro Online Registration screen appears (see *Figure 13-2*).

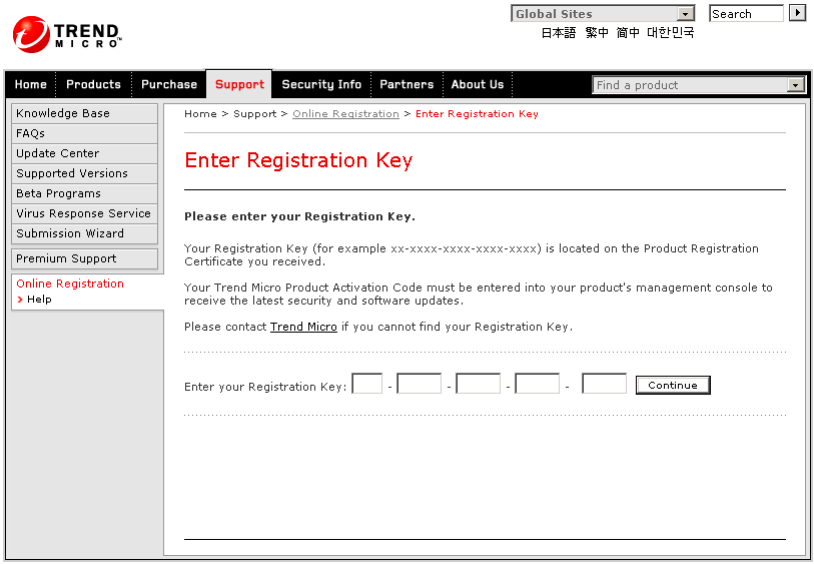
FIGURE 13-2. Trend Micro Online Registration Screen



2. Begin in the New customer registration section of the Online Registration screen. Select your preferred language from the language pull-down, and click **Register your product**.
3. When the Enter Registration Key screen shown in *Figure 13-3* appears, type the registration key from your license certificate and click **Continue**. Follow the

prompts on the subsequent registration screens to complete the registration process.

FIGURE 13-3. Trend Micro Enter Registration Key Screen



Your Logon ID and Password

Some of the information you provide during registration is used to create a logon ID and password, so that the next time you visit the Online Registration screen (for example, to update your Maintenance Agreement), you can log on as an existing customer rather than as a new customer.

After Registration

Shortly after you complete the registration process (typically within 20 minutes), you will receive an email message from Trend Micro that contains your Activation Code.

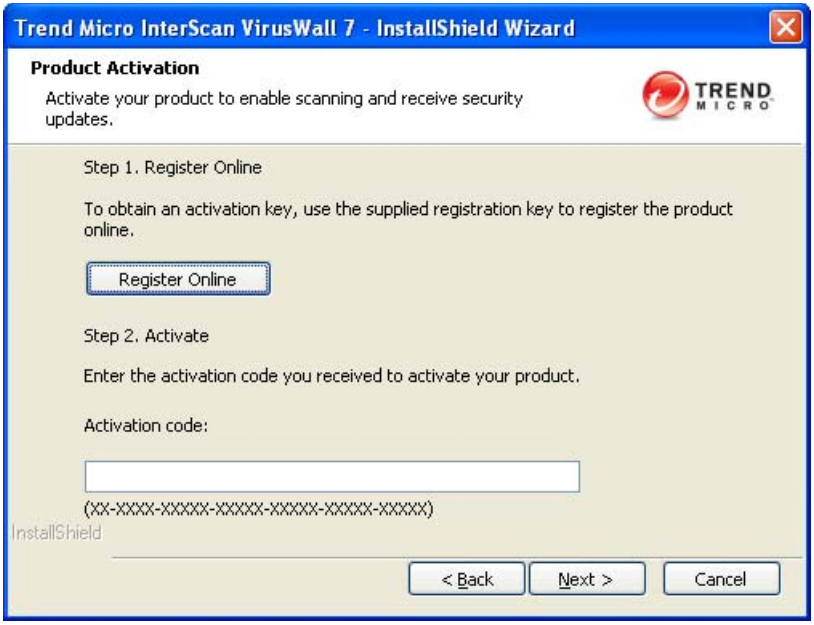
Activating InterScan VirusWall

Once you have your Activation Code, which you either received in an email message from Trend Micro following product registration, or taken directly from your license certificate, you are ready to activate ISVW.

To activate during installation:

Enter the Activation Code in the Activate step on the Product Activation screen.

FIGURE 13-4. Product Activation Screen During Installation



Note: Trend Micro will give you a 30-day grace period if you install ISVW without activating it. You can use all features and update patterns during this period. However, once the grace period has expired, you will not be able to use the features.

If you installed ISVW without activating it, the Web console will issue a message that ISVW has not been activated.

If you do not activate ISVW for 30 days after installing it, ISVW will allow you to modify the configuration settings but none of the product feature will work and no pattern updates will occur.

To activate after installation:

1. Select **Administration > Product License** to display the Product License screen.
2. Click **Enter a new code**.

   The Enter a New Code screen appears.
3. Enter the Activation Code in the **Activation Code** field.
4. Click **Activate**.

   After activation, the message at the top of the Administration Product License screen changes to let you know that activation was successful.

   As soon as ISVW is activated, it begins scanning the default security settings. To enable content filtering, URL, and file blocking, configure these features according to your organization's communications policies and the license you purchased.

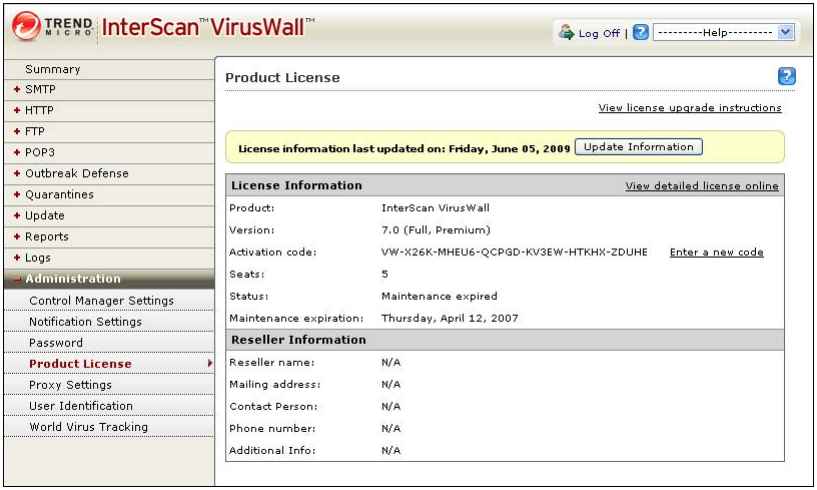
ISVW supports automatic online update if the Activation Code that activated ISVW is a full version AC and its expiration date has been changed.

To perform online updates manually:

1. Check the network status, Proxy settings (if necessary).
2. Select **Administration > Product License** to display the Product License screen (see *Figure 13-5*).

3. Click **Update Information**.

FIGURE 13-5. The Product License screen



To view renewal instructions, click **View license upgrade instructions**.

To view detailed information about the current license, click **View detailed license online**.

For More Information About Activation and Registration

To view product registration frequently asked questions (FAQ), see the Trend Micro Knowledge Base at the following site:

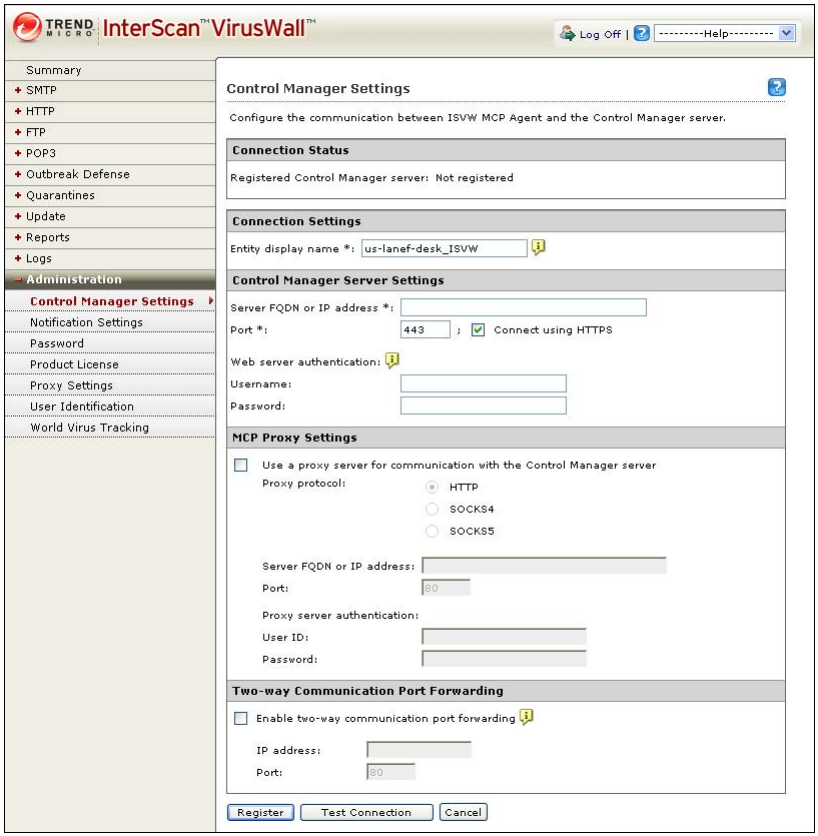
`http://esupport.trendmicro.com`

Using the Administration Features

Control Manager Settings

The Control Manager Settings screen is used to set up the connection settings between ISVW and the Control Manager server and to register ISVW to Control Manager. After the settings have been applied and ISVW has been registered to the Control Manager server, ISVW can be administered from the Control Manager Web console.

FIGURE 13-6. Control Manager Settings



Note: Refer to the Trend Micro Control Manager documentation for instructions on how to manage ISVW.

To configure Control Manager Settings:

1. Select **Administration > Control Manager Settings** to display the Control Manager Settings screen.
2. Type a name that will represent ISVW and that will appear in the Control Manager server product tree.
3. Type the server FQDN or IP address and port information for the Control Manager server.
4. Type the username and password that will be used to access the IIS server that hosts the Control Manager server.
5. Configure MCP Proxy Settings

   If a proxy server is required for communication between ISVW and the Control Manager server, select the Use a proxy server for communication with the Control Manager server to enable and then select a proxy protocol. Enter the FQDN or IP address and port number of the proxy server. If the proxy server requires authentication, enter the username and password used to communicate through the proxy server.
6. Configure Two-way Communication Port Forwarding.

   If you have NAT or a firewall between ISVW and the Control Manager server, and you want to be able to send command notifications from the Control Manager server to ISVW, you need to configure the NAT or Firewall to forward the connection to ISVW. To set up two-way communication port forwarding, select Enable two-way communication port forwarding and enter the IP address and port number of the NAT or firewall.
7. Click **Register**.

Note: Refer to the Trend Micro Control Manager documentation for instructions on how to manage ISVW.

InterScan VirusWall Supported Features for TMCM

Table 13-1 lists some of the ISVW administration tasks that can be performed from the Trend Micro Control Manager Web console.

TABLE 13-1. ISVW supported features for TMCM

TMCM FEATURE SUPPORTED BY ISVW	TASKS SUPPORTED
Status Monitor	TMCM can monitor the status (components and system information) of ISVW servers that are registered to the Control Manager server.
AC renew/deploy	TMCM can renew/deploy the product AC for ISVW servers that registered to the Control Manager server.
Patterns/ Engines deploy	TMCM can deploy new patterns and engines to ISVW servers that are registered to the Control Manager server.
Single-sign on	Using the TMCM Web console, administrators can configure ISVW servers that are registered to the Control Manager server.
Group Configuration	Using the TMCM Web console, administrators can replicate settings from one registered ISVW server to another registered ISVW server.
Log upload	The registered ISVW server can upload event logs and security logs to the TMCM server allowing for centralized monitoring.
OPP	TMCM server can deploy OPP rules to ISVW servers that are registered to the Control Manager server.

Notification Settings

The SMTP/POP3/FTP/HTTP modules use notification settings to send email notifications when they detect a security risk or when a message or a file triggers content filter settings.

FIGURE 13-7. Notification Settings

By default, ISVW detects the Fully Qualified Domain Name (FQDN) of the machine where it is installed, and uses this FQDN when sending notifications. For example, if the machine belongs to the sample.com domain, the ISVW notification email address will become `isvw@sample.com`. If the machine does not belong to any domain, ISVW will use `isvw@localdomain` as the address.

WARNING! **Using the FQDN to send notification messages may expose the FQDN to users outside the network. To address this issue, replace the notification email address with a different email address.**

To configure notification settings:

1. Set the SMTP server name or IP address and port you use to send notifications. If you type a domain name, either
   a. Use the nslookup command to verify that the domain name can be resolved correctly:
      - nslookup
      - notification.domainname

   —or—

   b. Add the domain name and IP mapping to your hosts file at `%windir%\system32\drivers\etc\hosts`. For example:
      - notificationIP notification.domainname

   To ensure that ISVW can send all notifications through this SMTP server correctly, add the IP address of the ISVW server in your SMTP server trusted IP list. Set the Administration email address that will receive notifications for administrators. If you have more than one notification address, separate them with semicolons (;); for example:

   `admin1@isvwtest.com;admin2@isvwtest.com`
2. Set the Sender email address that ISVW will use to send notifications.
3. Choose the preferred character set to use:
   - English (us-ascii)
   - Unicode (utf-8)
   - ISO (ISO-8859-1)
   - ISO (ISO-8859-2)
   - ISO (ISO-8859-3)
   - Simplified Chinese(gb2312)
   - Traditional Chinese (big5)
   - Chinese (iso-2022-cn)
   - Korean (iso-2022-kr)
   - Japanese (iso-2022-jp)
   - Japanese (Shift_JIS)

Note: UTF-8 can be used with most languages.

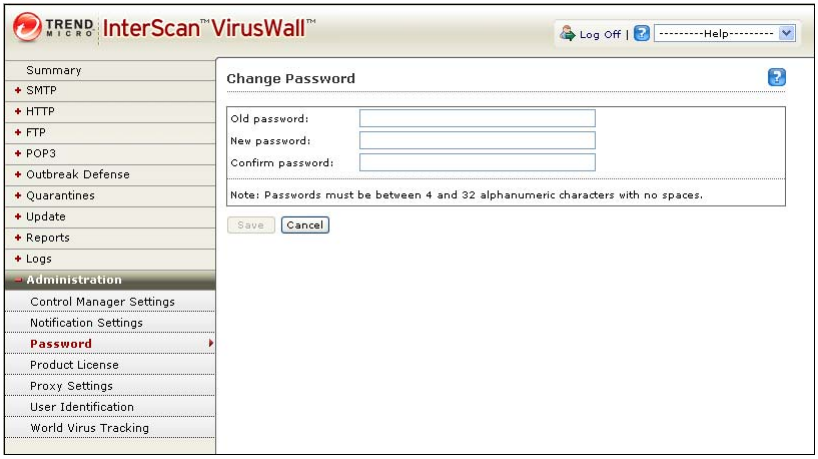
To replace the sender email address:

1. Go to Administration > Notification Settings page on Web console.
2. Modify the Sender email address field.
3. Click **Save**.

Password

The Administration > Password screen allows you to set the password that manages the Web console.

FIGURE 13-8. Change Password Page



The password must be between 4 and 32 alphanumeric characters with no spaces. When the password has been successfully changed, a notification message appears.

Proxy Settings

If you use a proxy server to connect to the Internet, specify the proxy settings. ISVW needs the proxy information to:

- Update pattern/engine files
- Update license information
- Send virus logs to the WTC server
- Download OPS rules from the OPS server

FIGURE 13-9. Proxy Settings

To configure your proxy settings:

1. Go to **Administration > Proxy Settings**.
2. Choose your proxy server type.
3. Specify the proxy server name or IP address, and port.
4. If your proxy server needs authentication, input a valid user ID and password.
5. Click **Test Connection**.

   If the settings are correct, you will receive a verification notice.
6. Click **Save**.

World Tracking Center

The World Tracking Center (WTC) allows Trend Micro to monitor threat outbreaks and provide improved protection. If you select `Yes`, ISVW will send virus logs to a WTC server at scheduled intervals. No other information will be sent.

For more information, visit the WTC Web site: `http://wtc.trendmicro.com`

Configuring User ID Settings

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

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

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

The User Identification page includes the following information:

- *Selecting the User Identification Method*
- *About the Domain Controller Agent*
- *About the Domain Controller Agent*
- *Adding Domain Controller Server Credentials*

Selecting the User Identification Method

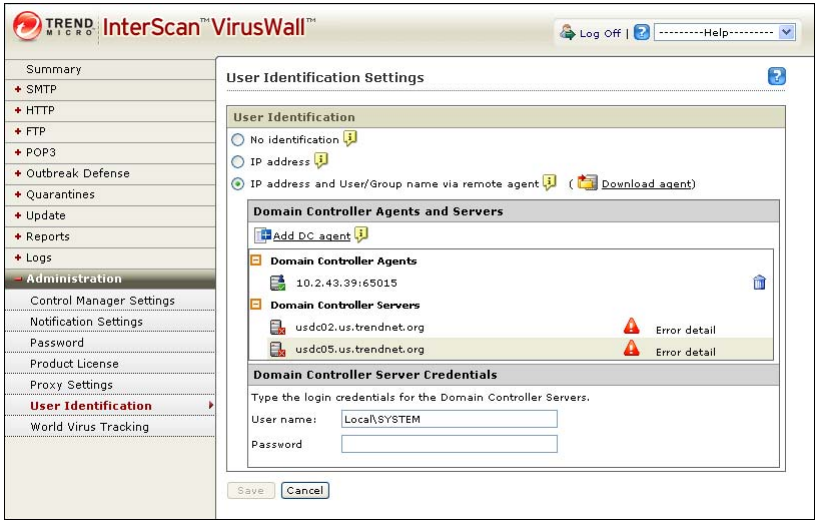
You can identify users through IP addresses or by user/group names using proxy authorization, as shown in *Figure 13-10*.

Identifying users enables you to do the following:

- Set up user and group policies for URL Filtering and Blocking
- Display user information in the violation logs

- Have domain name and account information appear in the HTTP debugging log

FIGURE 13-10. The User Identification Settings Screen



To configure the user identification settings:

1. Choose **Administration > User Identification**.
2. Select one of the following radio buttons:
   - **No identification** — No user or group identification is used for the connection and the global user policy applies.
   - **IP address** — Users will be identified by an IP address.
   - **IP address/User/group name via remote agent** — Using this setting allows you to identify both individual users and groups, by name (first) or IP address (second). Requires configuring the Domain Controller agent and server.

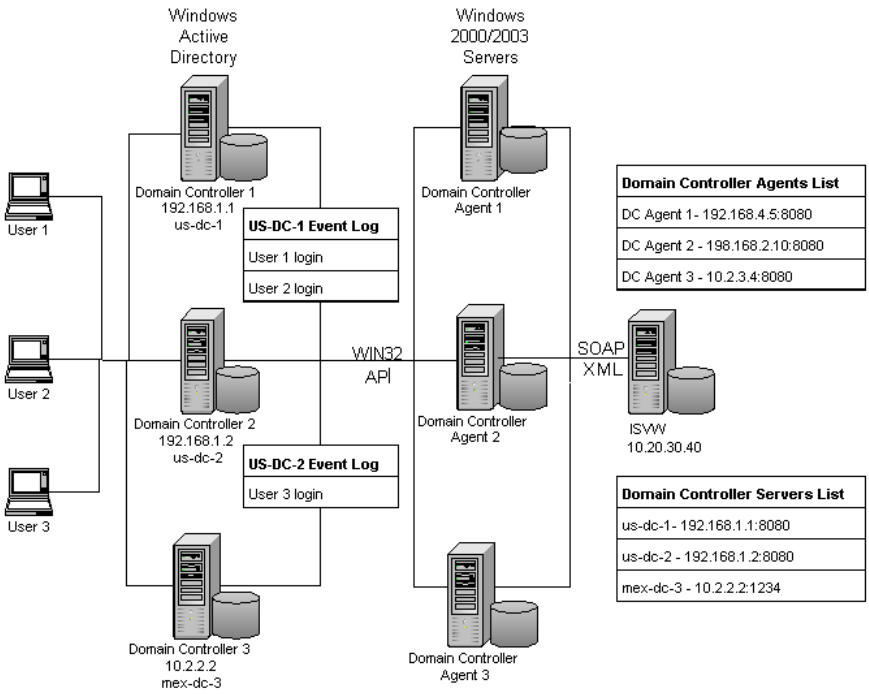
About the Domain Controller Agent

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

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

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

FIGURE 13-11. Network Configuration for Domain Controller Agent Installation



Installing the Domain Controller Agent

The Domain Controller Agent should be installed on any Windows 2000, 2003, or 2008 server that is part of the Active Directory domain, separate from both the Domain Controller server and ISVW computer. Windows 2000 servers and greater support the ISVW auto-discovery feature for all Windows Active Directory Domain Controller

servers, running on Windows 2000 or greater servers.

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

To install the Domain Controller Agent:

1. Before installation, verify that logging is enabled for logon events.

   If it is not, the Domain Controller Agent cannot access user information from the Domain Controller logs.

   a. To enable Windows server events in the Domain Controller event log, choose **Start > Administrative Tools > Domain Controller Security Policy** on each Domain Controller machine.

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

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

2. Log in with administrator privileges to the server (Windows 2000 or Windows 2003) on which the Domain Controller Agent will be installed.
3. Access the ISVW UI at: `isvw: http://<ip>:9240` and log in.
4. Choose **Administration > User Identification**.
5. Click the **Download Agent** link and follow the on-screen instructions.

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

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

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

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

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

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

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

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

---

e. Click **Install**.

A progress bar displays.

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

6. Repeat Step 1 through Step 5 for additional installations of Domain Controller Agents.

   A maximum of eight Domain Controller Agents can point to one ISVW.

7. Add the Domain Controller Agent and Domain Controller to ISVW according to the procedure listed in *Adding a Domain Controller Agent to InterScan VirusWall* on page 13-20

8. Add the Domain Controller log on credentials according to the procedure listed in *Adding Domain Controller Server Credentials* on page 13-22.

Adding a Domain Controller Agent to InterScan VirusWall

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

Adding Domain Controller Agents allows the ISVW to access user logon information from the Domain Controller Agent. Domain Controller Servers are populated into ISVW using the built-in auto-discovery feature of the Domain Controller Agent.

Domain Controller Agents are added manually and are not auto-detected like Domain Controller Servers. You cannot manually add a Domain Controller Server.

Note: The auto-detect feature is available for Domain Controller Agents installed on Windows 2000 Pro, Windows 2000, Windows 2003, Windows XP, and Windows 2008 servers. All Windows Active Directory Domain Controller Servers are auto-detected.

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

To add a Domain Controller agent:

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

   The User Identification Settings screen appears (see *Figure 13-10*).
2. Select the **IP address and User/Group name via remote agent** option and then click the **Download agent** link.
3. Click the **Add DC agent** link in the "Domain Controller Agents and Servers" section.

   The User Identification Settings screen displays the "Domain Controller Agent" section.
4. For a Domain Controller Agent, type the following information:
   - **Host name or IP address** — The host name or IP address of the machine where the Domain Controller Agent is installed. (See *Figure 13-10*.)

   The port number is for the computer on which the Domain Controller Agent is installed. The default port number 65015 is specified in the `IdAgent.ini` file (`[Setting]/AgentPort` parameter.
5. Click **Save**.

   The Domain Controller Agent name appears in the list shown in *Figure 13-10*.
6. Click **Save**.

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

Deleting a Domain Controller Agent from InterScan VirusWall

To remove a Domain Controller agent from the list:

1. Choose **Administration > User Identification**.
2. Find the desired agent in the list.
3. Click the trash can icon next to the name.

   Click **Cancel** to undo the deletion.
4. Click **Save** to make the deletion permanent.

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

Detecting A Domain Controller Server to InterScan VirusWall

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

A Domain Controller server provides information to the Domain Controller agent, which accesses the Domain Controller logon events to retrieve user information.

Note: You cannot add a Domain Control server manually in ISVW. A Domain Control server is added automatically by an auto-detect mechanism in ISVW. You cannot delete a Domain Controller server.

- The **User/group name (via Domain Controller Agent)** radio button must be selected as the method of user identification to add a Domain Controller server.
- The auto-detect feature is available for Domain Controller agents installed on Windows 2000 Pro, Windows 2000, Windows 2003, Windows XP, and Windows 2008 servers. All Windows Active Directory Domain Controller servers are auto-detected.
- If more than one Domain Controller server is added, all the logs for credentials must be identical in order to use the Domain Controller Server Credentials section (see *Adding Domain Controller Server Credentials* on page 13-22).

Adding Domain Controller Server Credentials

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

Domain Controller Agent installation requires administrator privileges. If the Domain Controller Agent is installed on a Windows machine where the local system account does not have the permission to access the domain controller, ISVW will not be able to

query domain users and groups. The ISVW user can enter the domain controller credential in the user name and password fields of the Domain Controller Server Credentials section of the User Identification Settings screen to enable access.

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

To specify the requirements on client machine's firewall:

1. Run the Remote Registry Service on the client computer.
2. Log in using the domain account.
3. If there is a firewall, configure exceptions to allow inbound RPC traffic on TCP port 445.

   To open port 445 on Windows XP Pro SP2:

   a. Click **Start**, open control panel, and then choose **Windows Firewall**.

   b. Click the **Exceptions** tab.

   c. Check **File and printers sharing** and then click **OK**.

   For any other firewall, please see the product manual for how to open a port.

To add Domain Controller server credentials:

1. Choose **Administration > User Identification**.
2. Go to the Domain Controller Server Credentials section at the bottom of the screen. (See *Figure 13-10*.)
3. Type the user name in the domain name\username format.
4. Type the password.
5. Click **Save**.

Chapter 14

Using Real-Time Scan Monitor

The InterScan VirusWall (ISVW) Real-time Scan Monitor provides real-time monitoring of SMTP scanning functions, and access to the SMTP and FTP performance data through the Windows Performance Monitor.

Note: To monitor remotely, use Windows 2003 Server Remote Desktop or a remote control software such as Remote Administrator.

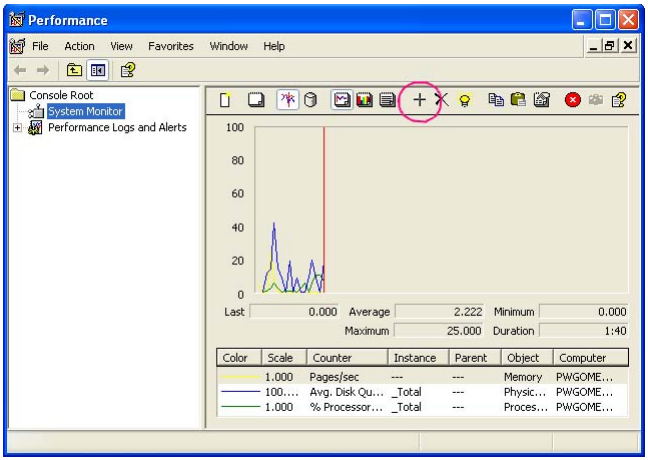
To run the Real-time Scan Monitor:

1. On the Windows Start menu, select **Programs > InterScan VirusWall 7 > InterScan VirusWall 7 Realtime Scan Monitor**.

   When you send email through SMTP, real-time statistics and activity information will be shown in the monitor panel.

2. To open the Windows Performance Monitor, click **Performance Monitor**.

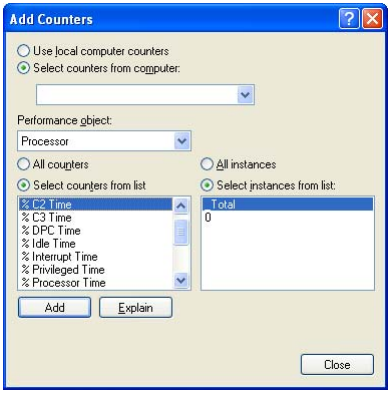
FIGURE 14-1. Windows Performance Monitor



To add counters to the Windows Performance Monitor:

1. Click "+" in the Windows Performance Monitor screen (see circled item in *Figure 14-2*). The **Add Counters** screen displays.

   FIGURE 14-2. Add Counters Screen



2. Select the **Select counters from computer** option and then select the computer where ISVW is installed.

3. Choose either **ISVW – FTP** or **ISVW – SMTP** from the **Performance object** drop-down list.
4. Choose **All counters,** or choose **Select counters from list:** and then select the counters to add.
5. Click **Add**.
6. Click **Close** to return to the Windows Performance Monitor.
7. View performance data in graph view, histogram view, or report view.

Chapter 15

Troubleshooting and Support

This chapter provides useful information to solve problems you may encounter while installing, configuring or using InterScan VirusWall (ISVW). If your problem is not included in the list of issues provided in this chapter, refer to the online help. If you need further assistance, see *Obtaining Technical Support* on page 15-31.

Troubleshooting

TABLE 15-1. Troubleshooting Issues

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Unsuccessful installation	• System requirements are not satisfied. See *System Requirements* on page 2-3. • If the operating system version or service pack is not satisfied, installation will continue with a warning message. • There is insufficient space on the target disk. You need at least 1 GB of hard disk space to install ISVW. Free up some disk space or install ISVW on a server with sufficient disk space. • You do not have sufficient privileges to install ISVW. Log on with administrator privileges to install. • If you have satisfied the above requirements and installation still fails, contact Trend Micro Support.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS

Failure to migrate configuration settings during installation	• Failure to migrate from file occurs when you are installing ISVW on a new computer and migrating ISVW 3.55 settings to that computer using a corrupt configuration settings file.
	• To resolve this issue:
	  • On the machine where ISVW 3.55 is installed, generate a new configuration settings file. For the procedure, see steps 1 to 4 of *Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 3.55 Settings to that Computer* on page 3-11.
	  • Install ISVW again on the new computer. For the procedure, continue with steps 5 to 18 of the same topic.
	• Failure to get the configuration settings of ISVW 3.55 occurs when you are installing ISVW 7.0 on a machine where ISVW 3.55 was installed improperly.
	• To resolve this issue:
	  • Generate a configuration settings file on the machine. For the procedure, see steps 1 to 3 of *Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 3.55 Settings to that Computer* on page 3-11.
	  • Install ISVW 7.0 again on the machine. To re-install ISVW 7.0, see *Installing InterScan VirusWall 7.0 on a Computer Where an Earlier Version of ISVW is Installed* on page 3-6.
	
	Note: If migration from ISVW 5.0 to 7.0 fails, please refer the migration section of the Administrator's Guide for Migration from ISVW 5.0.
	
	If you have satisfied the above requirements and migration still fails, contact Trend Micro Support.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
100% CPU utilization right after installation	This normally happens because ISVW 7.0 needs to initialize components such as the scan engine, anti-spam engine, configuration file, log file, and loading pattern before it can run normally. Initialization will take no more than a few minutes on the recommended environment. After that, CPU usage will normalize.
Issues after upgrading from ISVW 3.55 with eManager 3.52 to ISVW 7.0	• The eManager 3.52 plug-in may still be installed after upgrading because other machines with ISVW 3.55 are still using the plug-in. It is possible for several ISVW 3.55 installations to share the same eManager 3.52 plug-in. • All content filter settings were migrated but they may be disabled upon upgrade because: • In version 3.55, the service InterScan eManager Content Management is disabled during migration. • In eManager 3.52, the Attachment Filter > Enable attachment filter option is disabled during migration. • ISVW 7.0 does not support the migration of email management rules. You need to define these rules again. • Migration of anti-spam rules is not supported. ISVW 7.0 uses eManager 6 to support the content filtering feature, and the anti-spam feature is provided by Trend Micro Anti-spam Engine 3.52. • The Configuration window of ISVW 3.55 is still open after the upgrade. Stop the process manually from Windows Task Manager, and then remove all files under the path where ISVW 3.55 was installed. • Some folders under the installation folder of eManager 3.52 still exist after the upgrade. Manually delete these folders.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Cannot stop or start a service	• If you cannot stop a service after following the procedure in *Starting and Stopping InterScan VirusWall* on page 3-28: • Go to Control Panel > Administrative Tools > Services, right-click the service and then click Stop. • If this does not work, Go to Control Panel > Administrative Tools > Services, right-click the service and then click Properties. In the General tab, go to Startup type: and choose Manual. Restart the system. • After restart, the status becomes “Stopped”. • If you cannot start a service after following the procedure in *Starting and Stopping InterScan VirusWall* on page 3-28, call Trend Micro Technical Support.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Cannot update license	• Activate your product before you update your license. • Do not use an evaluation-version of ISVW 7.0 to update your license. • If you encounter a system or program exception error in the backend online update license server, wait for a few minutes and try again. If you still experience problems, contact Trend Micro Technical Support. • If you cannot update your license because an incorrect server URL stored in `Config.xml\Common\ProductRegistration\OnLineUpdate\ Server\Source`, check your configuration and try again. • If the Activation Code used is not found in the online update license server, type a valid activation code and try again. • If you cannot update your license online, check the network status. If you are using a proxy server, check whether the server can connect to the Product Registration server. If you still experience problems, contact Trend Micro Technical Support.
Problems with activation	• The Activation Code used is invalid. Do not use your full-version or evaluation-version Activation Code to activate the product again. • The evaluation-version or full-version Activation Code you used has expired. • Do not use an evaluation-version Activation Code if you installed a full version, and vice versa. • If activation still fails, contact Trend Micro Support.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Web management console issues	• If the Web management console does not display normally after typing some Chinese/Japanese characters in a text box, check the encoding of the browser. For Internet Explorer, go to View > Encoding and select UTF-8 so that the Web UI can display DBCS characters (such as Chinese/Japanese) correctly. • If the Web management console does not open, check the machine where ISVW 7.0 is installed. Ensure that there is enough space for query cache files before opening the console. • If you forget your Web management console password, contact Trend Micro Technical Support and ask for assistance in resetting your password. Please note that only registered ISVW 7.0 installations are eligible for technical support. If your ISVW 7.0 is not registered, you cannot recover your password.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Issues with ISVW 7.0 components	• Although Trend Micro recommends that you schedule ISVW 7.0 to perform automatic updates of the scan engine and pattern file, you can also update them manually. • On the left menu, select **Update > Manual**. • Wait while ISVW 7.0 checks the availability of new components. • When the list of available engines and pattern file updates appears, select the check box beside the components you want to update. • Click **Update**. • Component rollback does not take effect on some processes. • Go to the Summary screen on the Web management console and check whether any of the processes (SMTP/POP3/HTTP/FTP) is disabled. You can also open Windows Task Manager (or Process Explorer) and check whether the process is running. If the process is not running while performing rollback, component rollback will not take effect on that process.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
When the primary SMTP server requires authentication and ISVW 7.0 does not provide the authentication, the mails are queued.	Generally, when the destination requires authentication, ISVW 7.0 will not queue the mail but will return it to the sender with messages such as “530 server needs authentication” or, if the mail is forwarded to an Exchange Server that needs authentication, a message of “454 server needs authentication” is returned. ISVW 7.0 will assume that an error has occurred and will retry until the maximum retry limit is reached. Since ISVW 7.0 does not support authentication, deploy your email server (for example, Exchange Server) ahead of ISVW 7.0 if you want to use the authentication function of your email server. For information about deploying the SMTP VirusWall, see *Installation Topologies* starting on page 2-7.

Notifications to sender or recipient are not working.	• Ensure that the notification settings are correct. See Notification Settings starting on page 6-12.
	• If the configurations are all correct but you still do not receive a notification, check the settings of your notification server. By default, ISVW 7.0 will detect the FQDN of a local machine and use it as the domain name of the notification mail address. If a local computer does not belong to a domain, ISVW 7.0 will use `isvw@localdomain` as the address.
	There are two solutions to this problem:
	  • Specify a valid address for the notification server. For more information, see To replace the sender email address: starting on page 6-14.
	  • Add the IP address for ISVW 7.0 to the trusted IP list of your notification server.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Some quarantined files do not appear in the quarantine query result.	Quarantined files from HTTP or FTP traffic do not display in the query result table because ISVW 7.0 does not support HTTP/FTP quarantine query. If the quarantined files are from SMTP or POP3 traffic but are not included in the query result, check the query date/time period setting. The quarantine query will remember the time of your first query from the console. If you make a second query without logging off, the time period is still the time of your first query, so the new quarantined items are not included. Change the query time and ensure that it includes the whole time period before querying again.
Files of 0 KB remain in the FTP download folder.	This is a limitation of the FTP trickling feature. FTP trickling can prevent connection time-out, but once the file is created in the client, ISVW 7.0 cannot request the client to remove the file, even though the action on the file is quarantine or delete.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Some of the processes are not running even though they are enabled.	Check the system and event logs to see whether a fatal error occurred during process initialization. In most cases, port conflicts prevent processes from running. An entry such as “SMTP: Unable to bind a specific port” will appear in the log. Change the port number in the Web management console, and then restart the process from the Summary screen. If you cannot get enough information from the system log and event log, enable the debug log from `config.xml` and restart the process. To enable the debug log: 1. Open the `config.xml` file on the ISVW 7 installation folder. 2. Search for the following: <Value Name="DebugEnable" string="" type="int" int="0" /> 3. Change the text to: <Value Name="DebugEnable" string="" type="int" int="1" /> 4. Save and close the file, then restart one of the SMTP/POP3/HTTP/FTP processes or the whole ISVW 7.0 service. You can now reproduce the problem and obtain information from the debug log under the Log folder.
The SMTP server unexpectedly terminates the connection when sending email or connecting to the SMTP port.	Open the system log or real-time scan monitor to check whether there is an error. For example, if “A server error occurred; the program is unable to accept a connection” was logged in the system log, or you see errors like “Inbound (or outbound) server error, InterScan does not accept connections” in real-time scan monitor, open the Web management console and check that the settings for the inbound server, outbound server, and notification server are correct.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Outlook Express 6.0 recognizes InterScan_SafeStamp.txt as an unsafe attachment.	Outlook treats a file as unsafe according to the unsafe file list and settings of "confirm open after download" for the specified file. To make the `.txt` file a safe attachment, open **Settings > Control Panel > Folder Options**, click the **File Types** tab, and select TXT. Afterward, click **Advanced**, and on the new window, clear **Confirm open after download**.
How to set the domain control for incoming and outgoing mail	In ISVW 7.0, two settings control incoming and outgoing messages: 1. In the Web management console, select **SMTP > Configuration**. Go to item 1 under Outbound Mail and specify the IP address in the text box. ISVW 7.0 will relay all messages from the IP address specified here. IP address formats supported are: - 192.168.5.* - 192.168.5.1-158 - 192.168.5.242 If you specify multiple IP addresses, separate them with semicolons; for example: 192.168.3.*;192.168.5.2;192.168.5.148-245 2. To configure ISVW 7.0 to accept incoming email messages addressed only to specified internal domains, select **SMTP > Configuration**. Go to the Advanced Configuration section, select **Block relayed messages by accepting...**, and then type the domains in the text box. Separate multiple domains with semicolons. Domain names can start with a wildcard; for example: *.isvw.com;isvwbeta.com

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
Some folders still exist after uninstalling ISVW 7.0.	If the folder was open during uninstallation, it will not be removed. Remove the folder manually. The "Log" and "Quarantine" folders are kept after uninstallation.
User receives the NDR message from ISVW stating that the Helo command was rejected	The user may receive a Non Delivery Report (NDR) from ISVW if the remote mail transfer agent (MTA) requires a fully qualified domain name (FQDN) when it receives the HELO command. To resolve this issue, modify the value for DomainHostName key in intscan.ini file to the FQDN name of ISVW machine, and then restart ISVW
Where can I find the logs for failures or errors, such as when some processes crash?	Use the Windows system log and the ISVW 7.0 system log. Two joint initializing lines without a terminating line between them in the ISVW 7.0 system logs indicate that a crash has occurred. The debug log contains more detailed information if you have enabled it.

TABLE 15-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
TMCM - I receive an error when I try to access ISVW from the TMCM Web console	ISVW and TMCM use a public key, to ensure security, when communicating with each other. If the IIS settings for TMCM do not allow the public key to be downloaded you may receive an error when trying to access an ISVW device from the TMCM Web console. Do the following to ensure that TMCM can download the public key: • Open the IIS console. • Right click on **Default Web Site** and select **Properties** from the contextual menu. • Click the HTTP Headers tab. • Depending on the version of IIS you are running, you might see a button File Type or MIME Types in the bottom right corner of the window, click the button. The File Types window appears. • In the File Types window, click the **New Type** button. The File Type dialogue box appears. • Type **.pem** In the Associated extension field • Type **pem** in the Content type (MIME) field. • Click **OK**, then **OK** again, and finally click **OK** once more. • If this does not work. Manually copy `SSO_PKI_Publickey.pem` which is located in CM server side (The directory is `<CMServer_direcotry>/WebUI/Download/SSO_PKI_Publickey.pem`) to `<ISVW_directory>/CMAgent`, and then try again.

Domain Controller Agent Debugging

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

Enabling Domain Controller Agent Debugging

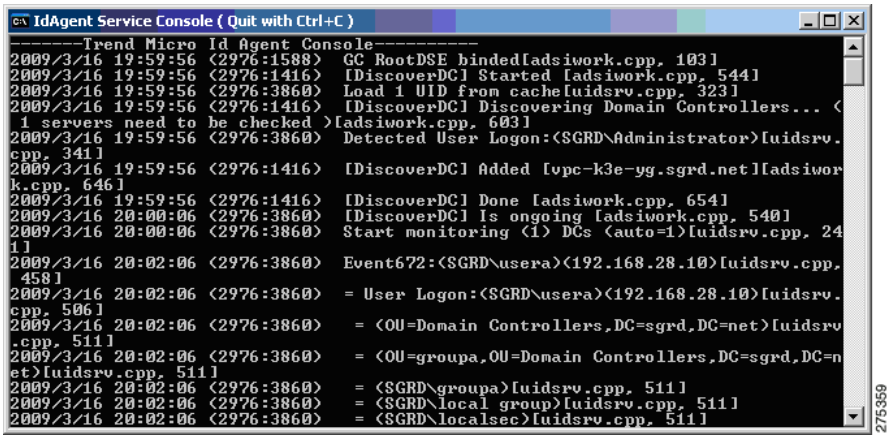
To enable Domain Controller Agent debugging:

1. Log on to the server that runs the agent program.
2. Open the Registry Editor, or remotely connect to the registry on that server.
3. Assign a non-zero value to the following registry value:
   a. Choose **Start > Run**.
   b. Type `regedit`.
   c. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IdAgent\`
   d. Double click on **DebugLevel**.
   e. Change the value data from 0 to 1.
4. Run **services.msc**, choose **TMIdAgent**, and click **Restart** ( ) to stop and restart the Domain Controller Agent service.
5. Locate the debugging log file (`IdAgentDebug.log`) in the Domain Controller Agent installation folder.

Console Mode

In addition to enabling the Domain Controller agent debugging log, you can run the agent in console mode. When the agent program is running in console mode, it shows the logged-on users and displays debugging messages on the console screen. Console mode can be useful for diagnosing agent connectivity issues. You can see the request and response log immediately. *Figure 15-1* shows the console mode interface.

FIGURE 15-1. Domain Controller Agent Running in Console Mode



To start the console mode:

1. Stop the running Domain Controller Agent service.
2. In the Trend Micro Domain Controller Agent installation directory, double click the **DebugMode** shortcut.

   The default directory is `C:\Program Files\Trend Micro\IdAgent\`.
3. Press **Ctrl + C** to exit the running console.

Domain Controller Agent, Active Directory, and User Identification Troubleshooting

This section includes the following topics:

Domain Controller Agent Installation or Service Failure

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

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

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

Domain Controller Agent Connectivity

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

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

To configure a Domain Controller server, see *Domain Controller Server Connectivity* on page 15-23.

Table 15-2 lists the possible errors, potential causes, and possible solutions for Domain Controller Agent issues.

TABLE 15-2. Domain Controller Agent Issues

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Invalid host or IP address	Incorrect agent address is specified.	• Check the agent hostname or IP address and port number. • Verify that the DNS is working for the ISVW when the hostname is used.
Version not supported	ISVW requires a newer version of the agent.	Download the agent from the ISVW Web console and re-install it on the target server. See *Installing the Domain Controller Agent* on page 13-18 for details.
Any other error	Unexpected error	• Enable Domain Controller Agent debugging. See *Enabling Domain Controller Agent Debugging* on page 15-15. • Send the log file to Trend Micro support.

TABLE 15-2. Domain Controller Agent Issues (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Connection Failed	• Firewall blocked the connection • Service is down	• If there is a firewall on the Domain Controller agent computer, make sure to add the inbound TCP port 65015 to the exception list. • Make sure the server is running. • Check the agent hostname or IP address and port number. • Verify that the DNS is working for the ISVW when the hostname is used.

TABLE 15-2. Domain Controller Agent Issues (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Connection Refused	• The agent denied the request based on the access rule settings • Firewall blocked RPC on the Domain Controller server	Agents will not response to any client if the client's identifier or IP address is not in the access list. When the agent first starts, the agent access list is empty. The first registered client occupies the agent and determines who else is allowed to access this agent. One way to register another ISVW is to configure a failover device. However, you can always manually configure the access list on the agent side. To manually configure the access list, perform these steps: 1. Log on to the Domain Controller Agent server machine using an administrator account. 2. Browse to the agent installation folder, C:\Program Files\Trend Micro\IdAgent\ 3. Locate and open the agent configuration INI file named IdAgent.ini. 4. In the [ClientList] section, add a new line with a value pair (a key + a value) in the following format:

TABLE 15-2. Domain Controller Agent Issues (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS

		`<Your-Temp-ID>=<host:port>|0`
		where
		• `<Your-Temp-Id>` = any unique key name, such as xxxx. This must be different from any existing string.
		• `<host:port>|0` = the Domain Controller Agent server IP address and port number followed by pipe zero (|0).
		
		Example:
		`[ClientList]`
		`??????=192.168.1.1:65014|0`
		
		The temporary client ID must be unique, or else it will replace an existing one. The default port is 65014.
		5. Restart the agent service.
		• Check the firewall on Domain Controller server, make sure to add inbound TCP port 445 to the exception list.

I/O Failed	Network error	Check the network connection.

TABLE 15-2. Domain Controller Agent Issues (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Default DC/GC Not Found	• The computer that the agent is installed on is not in the Active Directory domain • The agent is installed on a pre-Vista system, but the Active Directory server is on Windows Server 2008	• Join the computer to the Active Directory domain • Install the Domain Controller Agent on a Windows Server 2008
No DC Connected	The Domain Controller agent is still searching for the Domain Controller servers from the Active Directory.	Wait for a few minutes and then try again.
Logon failed	The username and password provided in the User Identification Settings page is not correct.	• Find the username that the agent is currently using as shown by choosing Administration > User Identification Settings in the Domain Controller server credentials section. • Type the correct username and password.

Domain Controller Server Connectivity

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

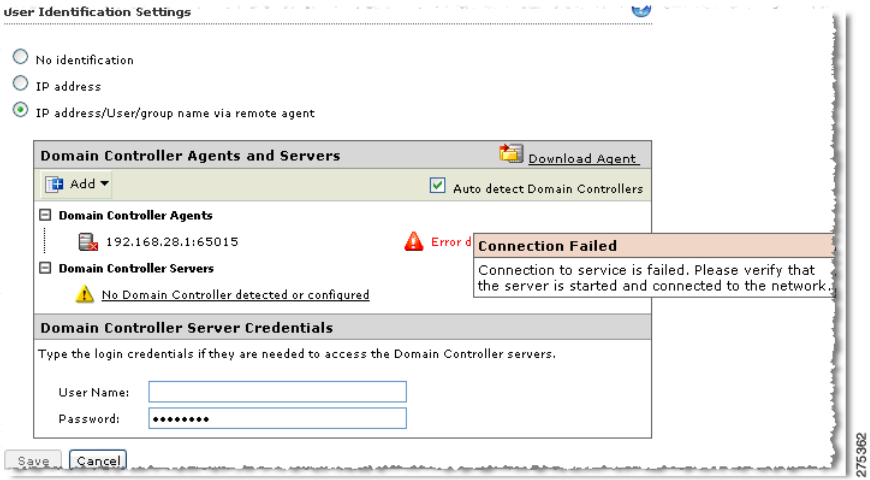
To configure the Domain Controller server:

1. Open the ISVW Web console.
2. Choose **Administration > User Identification**.
3. From the User Identification Settings page perform the following tasks:
   - Add the agent (see *Adding a Domain Controller Agent to InterScan VirusWall* on page 13-20).
   - Save the settings.
   - View the agent status.
4. Specify the Domain Controller server credentials (see *Adding Domain Controller Server Credentials* on page 13-22).
5. Wait for about 30 seconds and then refresh the screen.

   Both the Domain Controller agent and server should be green, which means the agent is ready for user0-identification requests.

If there is a connectivity error, a detailed message displays in the mouse-over tool tip, as shown in *Figure 15-2*.

FIGURE 15-2. Connectivity Error Message



Auto-detect Domain Controller Servers

A Domain Control Server cannot be added manually in ISVW. A Domain Control server is added automatically by an auto-detect mechanism in ISVW. This functionality allows the agent to detect and evaluate the Domain Controller servers at the same site. Auto-detection eliminates errors.

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

For autodetection issues, check the Domain Controller Agent privileges.

Connectivity

If configured correctly, the Domain Controller server listed on the User Identification Settings page should show the Domain Controller server as operational. If there is an error, the details display as do the Domain Controller agent errors shown in *Figure 15-2*.

Table 15-3 lists the possible errors and potential causes.

FIGURE 15-3. Diagnosing and Solving Domain Controller Server Connectivity

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Any other error	Unexpected error	• Enable Domain Controller Agent debugging. See *Enabling Domain Controller Agent Debugging* on page 15-15. • Send the log file to Trend Micro support.
Connection Failed	• Firewall blocked the connection • Service is down	• If there is a firewall on the Domain Controller server, make sure to add inbound TCP port 135 and 445 to the exception list • Make sure the server is running

FIGURE 15-3. Diagnosing and Solving Domain Controller Server Connectivity (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Connection Refused	• The agent does not have the correct access privileges to view the Domain Controller server event log. • Firewall blocked the RPC on Domain Controller server.	• Find the username that the agent is currently using as shown by choosing Administration > User Identification Settings in the Domain Controller Server Credentials section. • Verify the agent is running with the correct access privileges. • Change the logged-on user if needed. • Use the Event Viewer to determine if access privileges are the problem. • To determine if the problem is access privileges, log on to the Domain Controller agent server using the Domain Controller agent credentials, open the Event Viewer (`eventvwr.msc`) and try to connect to the Domain Controller server to see if it can be accessed.

FIGURE 15-3. Diagnosing and Solving Domain Controller Server Connectivity (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
		• Check the firewall on Domain Controller server and make sure to add inbound TCP port 445 to the exception list.
I/O Failed	Network error.	Check the network condition.
Logon Event Not Detected	The logon audit is disabled on the Domain Controller server.	To enable the audit account logon events to detect something other than a connectivity or privilege problem: 1. Choose Start > Control Panel > Administrative Tools. 2. Click Domain Controller Security Policy. 3. Expand Local Policies on the left pane, and then select Audit Policy. 4. Verify that Audit account logon events are enabled.
Logon Event Setting Incorrect	The event log size and overwrite setting are incorrect.	Set the appropriate event log size and enable event log overwriting.

FIGURE 15-3. Diagnosing and Solving Domain Controller Server Connectivity (Continued)

ERROR	POTENTIAL CAUSE	POSSIBLE SOLUTION OR DIAGNOSTIC STEPS
Client Validation Failed	• Domain Controller agent does not have enough privileges to access client machine(s). • Firewall on client blocked RPC.	• Provide the current credential for Domain Controller agent. • Check the client firewall setting and make sure to add inbound TCP port 445 to the exception list.
Status Pending	It takes some time for the Domain Controller agent to apply the new settings, such as a credential change or the re-discovery of Domain Controller servers.	Refresh the page.

Windows Active Directory Searching for Users/Groups

The Active Directory searching for users/groups functionality requires correctly configured user identification settings.

To troubleshoot the searching function:

1. Verify that the **IP address/User/group name via remote agent** option is selected on the Administration > User Identification Settings page. See *Figure 15-2*.
2. Verify that the Domain Controller agent(s) and the Domain Controller server(s) are correctly configured and that they display no error messages on the Administration > User Identification Settings page. If an error appears, match the error message with the correct solution in the previous sections. See *Table 15-2* and *Figure 15-3* for a list of solutions.
3. If the Domain Controller agent(s) and Domain Controller server(s) work, but you still do not obtain search results, enable the Domain Controller agent debugging log to see if the search request has been correctly handled. See *Enabling Domain*

Controller Agent Debugging on page 15-15. The Active Directory® Service Interfaces Editor (ADSI Edit) can also be used to verify that the search contains valid results.

4. Check the client timeout value. The default timeout value is 10 seconds. To change this value, edit the `AcceptTimeoutSecs=10 parameter` in the `IdLib.ini` file located at `<installation directory>\http\conf` on ISVW. The `RecvTimeoutSecs` parameter defines how long the ISVW waits for the search result.

It is necessary to enable debugging on ISVW and, if necessary, to send the debugging log to Trend Micro support. See *Enabling Domain Controller Agent Debugging* on page 15-15.

User Identification

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

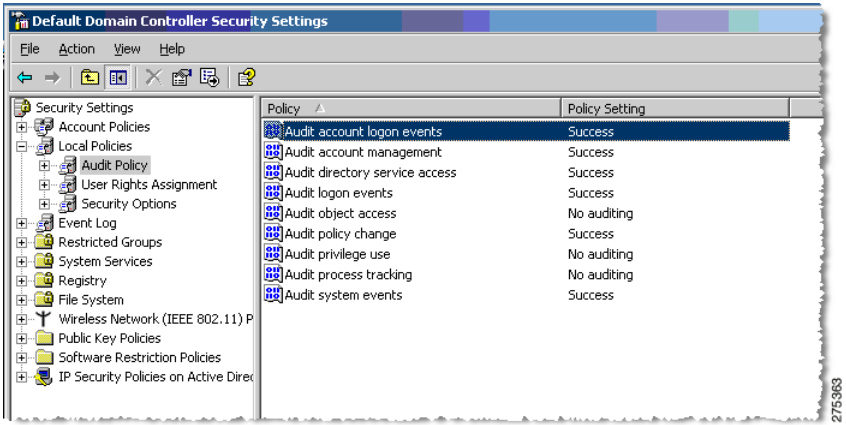
To diagnose user identification problems:

1. Choose **Administration > User Identification Settings**.
2. Verify that both the Domain Controller agent(s) and Domain Controller server(s) are configured correctly.

   If an error exist, please refer to *Table 15-2* and *Figure 15-3* for troubleshooting solutions.
3. Enable the audit account logon events to detect something other than a connectivity or privilege problem.
   a. Choose **Start > Control Panel > Administrative Tools**.
   b. Click **Domain Controller Security Policy**.
   c. Expand **Local Policies** on the left pane, and then select **Audit Policy**.

d. Verify that Audit account logon events are enabled. See *Figure 15-4*.

FIGURE 15-4. Enabled Audit Logon Account



Collecting Data for Trend Micro Support

Make sure that you always collect the Domain Controller agent debugging log and the ISVW HTTP daemon debugging log before calling Trend Micro technical support. For more information, see *Domain Controller Agent Debugging* on page 15-15.

Obtaining Technical Support

There are several ways to obtain technical support.

- The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

  `http://esupport.trendmicro.com/support/supportcentral/supportcentral.do`

- TrendEdge is a program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  `http://trendedge.trendmicro.com`

- If you are not able to find an answer in the documentation, Knowledge Base, or through TrendEdge, you can email your question to Trend Micro technical support.

  `support@support.trendmicro.com`

- For a list of the worldwide support offices, go to:

  `http://kb.trendmicro.com/solutions/includes2/ContactTechSupport.asp`

  In the United States, you can reach Trend Micro representatives by phone or fax:
  Toll free: +1 (800) 228-5651 (sales)

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

  Fax: +1 (408) 257-2003

To speed up the resolution of your product issue, provide the following information when you send an email or call Trend Micro:

- Program version and number (Click About on the main console's footer menu to learn about the program version and build number.)
- Serial number
- Exact text of the error message, if any
- Steps to reproduce the issue

Appendix A

System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

Server Address Checklist

You must provide the following server address information during installation and during the configuration of the Trend Micro Security Server to work with your network. Record them here for easy reference.

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Trend Micro InterScan VirusWall (ISVW) server information		
IP address	10.1.104.255	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Proxy server for component download		

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
IP address	10.1.174.225	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
Notification server information		
IP address	10.1.123.225	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	

Ports Checklist

InterScan VirusWall (ISVW) uses the following ports:

TABLE A-2. Port Checklist

PORT	SAMPLE	YOUR VALUE
SMTP	25	
POP3	110	
HTTP	8080	
FTP	21	
Web console	9240	
Web console (SSL)	9241	

Supported Commands

SMTP

The ISVW SMTP module does not support ESMTP commands (except size) and SMTP SSL.

TABLE A-3. SMTP Supported Commands

Command Name	Explanation
HELO	helo: be polite
MAIL	mail: designate sender
RCPT	rcpt: designate recipient
DATA	data: send message text
RSET	rset: reset state
HELP	help: give usage info
NOOP	noop: do nothing
QUIT	quit: close connection and die
SAML	saml: send AND mail
SOML	soml: send OR mail
EHLO	extended SMTP hello command

FTP

ISVW supports most FTP commands supported in popular FTP servers and clients. A known unsupported command is STOU. When Store unique is on, the FTP "put" command is not implemented.

Compatibility known issues:

- Problems logging on to an FTP site using a Linux system with Kerberos Authentication
- FTP user notification will cause FTP disconnection from the ISVW server
- FTP Virus/Spyware notification fails to display in Client NetAnts

POP3

POP3 supported commands include CAPA, AUTH, and all commands specified in RFC 1939. POP3 SSL is not supported.

TABLE A-4. POP3 Supported Commands

Command Name	Explanation	RFC
CAPA	List support features	RFC 2449
APOP	Logon with MD5	RFC 1939
AUTH	For Exchange servers	RFC 1734/3206
USER	Send user name	RFC 1939
PASS	Send password	RFC 1939
QUIT	Quit sessions	RFC 1939
STAT	List status of mailbox	RFC 1939
LIST	List info of mails	RFC 1939
UIDL	List UID of mails	RFC 1939
TOP	Get header of mails	RFC 1939
RETR	Get mails	RFC 1939
DELE	Mark mails as deleted	RFC 1939
RSET	Unmark deleted mails	RFC 1939
NOOP	Do nothing	RFC 1939

Appendix B

Default Values

The InterScan VirusWall (ISVW) Web management console provides different options to help you configure your ISVW installation to your specifications.

This appendix provides a reference when there is an absolute need to modify the ISVW configuration files (`intscan.ini and config.xml`). Please note that certain default values should never be changed directly because they are derived from, or dependent upon, corresponding values. Changing these values independently of their related contexts can result in invalid configurations and unexpected results.

Note: It is always good practice to back up the configuration files before you edit them.

This appendix contains a list of the ISVW configuration options. Each parameter is accompanied by an explanation, its default value, a list of any other possible values, and an explanation of the other possible values.

SMTP Virus/Spyware/IntelliTrap and Configuration

Parameter	Default Value	Possible Values	Explanation
intscan.ini [common] NotificationFromAddress	isvw@FQDN	Any email address	Appears in the From field of ISVW notifications for SMTP and FTP protocols
intscan.ini [Scan-Configuration] MailScan	Yes	Yes/No	Yes: scanning is on No: scanning is off if this item is off, virus/spyware/IntelliTrap scanning will all be disabled
Intscan.ini [EMail-Scan] MaxScanningThreadsProc	25		Limits the number of messages being scanned per processor
Intscan.ini [EMail-Scan] MaxSMTPClient-ThreadsProc	50		Limits the number of threads created to deliver mail after scanning
Intscan.ini [EMail-Scan] BackgroundMqueueInThreadsProc	2		Fixed number of background threads per processor created to deliver inbound mail in the mqueue after scanning. When mqueue is backed up, this value can be increased.
Intscan.ini [EMail-Scan] BackgroundMqueueOutThreadsProc	2		Fixed number of background threads per processor created to deliver outbound mail in the mqueue after scanning. When mqueue is backed up, this value can be increased.
Intscan.ini [EMail-Scan] BackgroundBMqueueThreadsProc	1		Fixed number of threads to deliver ISVW generated messages in the bmqueue.
Intscan.ini [EMail-Scan] MaxClientConnections	25		Maximum number of simultaneous connections accepted by ISVW.

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] DisableReceivedHeader	No		
Intscan.ini [EMail-Scan] InterScanSMTPServicePort	25		
Intscan.ini [EMail-Scan] InboundUseDNS	Yes	Yes/No	
Intscan.ini [EMail-Scan] OutboundUseDNS	Yes	Yes/No	
Intscan.ini [EMail-Scan] EOrg		IP address	The SMTP server IP address for inbound email
Intscan.ini [EMail-Scan] EOrgPort	25		The SMTP server port for inbound mail
Intscan.ini [EMail-Scan] NotificationSMTPAddr	default	Default or IP address	Notification server IP address
Intscan.ini [EMail-Scan] NotificationSMTPPort	25	Any number between 1 to 65535	Notification server port
Intscan.ini [EMail-Scan] InterScanSMTPServiceIP		IP address	
Intscan.ini [EMail-Scan] OutboundMailScan	Yes	Yes/No	Enable or disable outbound MailScan processing
Intscan.ini [EMail-Scan] OutboundMailVirusScan	Yes	Yes/No	Enable or disable outbound MailScan virus scanning
Intscan.ini [EMail-Scan] OutboundMailClientIP		IP address	
Intscan.ini [EMail-Scan] OutboundMailSMTPAddr			The SMTP server IP address for outbound mail
Intscan.ini [EMail-Scan] OutboundMailSMTPPort	25	Number between 1 and 65535	The SMTP server port for outbound mail

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] DeliveryMaxHours	24		
Intscan.ini [EMail-Scan] DeliveryRetryMinutes	1		
Intscan.ini [EMail-Scan] ScanExtensions			Incoming extensions that will be scanned if user sets Level to scanExt
Intscan.ini [EMail-Scan] OutgoingScanExtensions			Outgoing extensions that will be scanned if user sets Level to scanExt
Intscan.ini [EMail-Scan] Level	ScanAll	ScanAll/ScanExt/IntelliScan	
Intscan.ini [EMail-Scan] OutgoingLevel	ScanAll	ScanAll/ScanExt/IntelliScan	
Intscan.ini [EMail-Scan] EMail	Yes	Yes/No	Send notification to the administrator or not when virus is detected in inbound message
Intscan.ini [EMail-Scan] Addr		Email address	Email address used to receive notifications to the administrator when virus/spyware/IntelliTrap is found
Intscan.ini [EMail-Scan] Message1	A virus/malware was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". ISVW has taken the action: %FINALACTION%.		Message content sent to the administrator when virus is detected in inbound message

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] EWarning	No	Yes/No	Send notification to recipient or not when virus is detected in inbound message
Intscan.ini [EMail-Scan] EMessage	Warning - ISVW has detected a virus in a message sent to you from %SENDER%. The message subject is “%SUBJECT%” . The message may not be delivered.		Message content sent to recipient when virus is detected in inbound message
Intscan.ini [EMail-Scan] EWarningSender	No	Yes/No	Send notification to sender or not when virus is detected in inbound message
Intscan.ini [EMail-Scan] EMessageSender	Warning - ISVW has detected a virus in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT% ". The message may not have been delivered.		Message content sent to sender when virus is detected in inbound message
Intscan.ini [EMail-Scan] Stamp	No	Yes/No	Add virus free message to incoming message or not
Intscan.ini [EMail-Scan] StampMessage	ISVW has scanned this message and found it to be free of known viruses.		The content that will be added to incoming message without virus
Intscan.ini [EMail-Scan] VirusMessage	No	Yes/No	Add virus found message to incoming message or not

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] VirusMessageText	ISVW has detected an item that contains a virus in this message.		The content that will be added to incoming message when virus is detected
Intscan.ini [EMail-Scan] StampOutGoing	No	Yes/No	Add virus free message to outgoing message or not
Intscan.ini [EMail-Scan] StampMessageOutGoing	ISVW has scanned this message and found it to be free of known viruses.	string	The content that will be added to outgoing message without virus
Intscan.ini [EMail-Scan] VirusMessageOutGoing	No	Yes/No	Add virus found message to outgoing message or not
Intscan.ini [EMail-Scan] VirusMessageTextOutGoing	ISVW has detected an item that contains a virus in this message.	string	The content that will be added to outgoing message when virus is detected
Intscan.ini [EMail-Scan] EnableOutgoingNotiToAdmin	Yes	Yes/No	Send notification to the administrator or not when virus is detected in outgoing message
Intscan.ini [EMail-Scan] MsgOutgoingNotiToAdmin	A virus/malware was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". ISVW has taken the action: %FINALACTION%.	string	Message content sent to the administrator when virus is detected in outgoing message
Intscan.ini [EMail-Scan] EnableOutgoingNotiToRecipient	No	Yes/No	Send notification to recipient or not when virus is detected in outgoing message

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] MsgOutgoingNotiToRecipient	Warning - InterScan VirusWall has detected a virus in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	string	Message content sent to recipient when virus is detected in outgoing message
Intscan.ini [EMail-Scan] EnableOutgoingNotiToSender	No	Yes/No	Send notification to sender or not when virus is detected in outgoing message
Intscan.ini [EMail-Scan] MsgOutgoingNotiToSender	Warning - InterScan VirusWall has detected a virus in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	string	Message content sent to sender when virus is detected in outgoing message
Intscan.ini [EMail-Scan] Action	autoclean	Pass/move/delete/autoclean/blockmsg	Action taken on incoming message with virus detected
Intscan.ini [EMail-Scan] OutgoingAction	autoclean	Pass/move/delete/autoclean/blockmsg	Action taken on outgoing message with virus detected
Intscan.ini [EMail-Scan] UnCleanedFileRecipientAction	Delete	Pass/move/delete	Action on incoming files that cannot be cleaned
Intscan.ini [EMail-Scan] OutgoingUnCleanedFileRecipientAction	Delete	Pass/move/delete	Action on outgoing files that cannot be cleaned
Intscan.ini [EMail-Scan] InESMTPSIZE	0		Maximum incoming message size (0 means no limit)

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] OutESMTPSIZE	0		Maximum outgoing message size (0 means no limit)
Intscan.ini [EMail-Scan] RestrictInDomain	Yes	Yes/No	Accept incoming message only from specified domains
Intscan.ini [EMail-Scan] RestrictInDomainList	User specify		The list of accepted domains
Intscan.ini [EMail-Scan] QuarantineOfficeMacros	No	Yes/No	Quarantine incoming Microsoft Office document with macros or not
Intscan.ini [EMail-Scan] OutgoingQuarantineOfficeMacros	No	Yes/No	Quarantine outgoing Microsoft Office document with macros or not
Intscan.ini [EMail-Scan] Greeting	Welcome to ISVW SMTP service!		Greeting message shown when user connects to the SMTP port
Intscan.ini [EMail-Scan] EnableGreeting	Yes	Yes/No	Send customized greeting message
Intscan.ini [EMail-Scan] DecompressionLayerLimit	14	1~20	The maximum scan layer for incoming compressed files when the setting is to only scan files that meet certain criteria
Intscan.ini [EMail-Scan] OutgoingDecompressionLayerLimit	14	1~20	The maximum scan layer for outgoing compressed files when the setting is to only scan files that meet certain criteria
Intscan.ini [EMail-Scan] ExtractFileSizeLimit	1073741824		The maximum file size for incoming compressed files when the setting is to only scan files that meet certain criteria
Intscan.ini [EMail-Scan] OutgoingExtractFileSizeLimit	1073741824		The maximum file size for outgoing compressed files when the setting is to only scan files that meet certain criteria

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] BlockMethod	BlockNone	BlockNone/ BlockAll/ BlockIf	BlockNone: Scan all incoming compressed files BlockAll: Not scan all incoming compressed file BlockIf: Do not scan incoming compressed file if certain conditions are met
Intscan.ini [EMail-Scan] OutgoingBlockMethod	BlockNone	BlockNone/ BlockAll/ BlockIf	BlockNone: Scan all outgoing compressed files BlockAll: Not scan all outgoing compressed file BlockIf: Do not scan outgoing compressed file if certain conditions are met
Intscan.ini [EMail-Scan] MaxDecompressCount	100	0~0x7fffffff	The maximum scan count for incoming compressed files when the setting is to only scan files that meet certain criteria
Intscan.ini [EMail-Scan] OutgoingMaxDecompressCount	100	0~0x7fffffff	The maximum scan count for outgoing compressed files when the setting is to only scan files that meet certain criteria
Intscan.ini [EMail-Scan] MaxDecompressRatio	100	0~100	If set to only scan incoming files that meet certain criteria, SMTP will scan files whose ration is under the value specified here
Intscan.ini [EMail-Scan] OutgoingMaxDecompressRatio	100	0~100	If set to only scan outgoing files that meet certain criteria, SMTP will scan files whose ration is under the value specified here

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] NotifyCharSet			The preferred character set used for SMTP notifications
Intscan.ini [EMail-Scan] AntiVirus	Yes	Yes/No	Enable incoming virus scanning or not
Intscan.ini [EMail-Scan] OutgoingAntiVirus	Yes	Yes/No	Enable outgoing virus scanning or not
Intscan.ini [EMail-Scan] LoggingMsgID	Yes	Yes/No	Log incoming message ID or not
Intscan.ini [EMail-Scan] EnableSpywareNotiToAdmin	Yes	Yes/No	Send notification to the administrator or not when incoming spyware is detected
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToAdmin	Yes	Yes/No	Send notification to the administrator or not when outgoing spyware is detected
Intscan.ini [EMail-Scan] MsgSpywareNotiToAdmin	Spyware/grayware was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	string	Content sent to the administrator when incoming spyware is detected

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToAdmin	Spyware/grayware was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	string	Content sent to the administrator when outgoing spyware is detected
Intscan.ini [EMail-Scan] EnableSpywareNotiToRecipient	No	Yes/No	Send notification to recipient or not when incoming spyware is detected
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToRecipient	No	Yes/No	Send notification to recipient or not when outgoing spyware is detected
Intscan.ini [EMail-Scan] MsgSpywareNotiToRecipient	Warning - InterScan VirusWall has detected a spyware/grayware application in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	string	Content sent to recipient when incoming spyware is detected

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToRecipient	Warning - InterScan VirusWall has detected a spyware/grayware application in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	string	Content sent to recipient when outgoing spyware is detected
Intscan.ini [EMail-Scan] EnableSpywareNotiToSender	No	Yes/No	Send notification to sender or not when incoming spyware is detected
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToSender	No	Yes/No	Send notification to sender or not when outgoing spyware is detected
Intscan.ini [EMail-Scan] MsgSpywareNotiToSender	Warning - InterScan VirusWall has detected a spyware/grayware application in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered. Trend Micro suggests that you scan your computer for security risks.	string	Content sent to sender when incoming spyware is detected

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToSender	Warning - InterScan VirusWall has detected a spyware/grayware application in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered. Trend Micro suggests that you scan your computer for security risks.	string	Content sent to sender when outgoing spyware is detected
Intscan.ini [EMail-Scan] EnableBotTrapNotiToAdmin	Yes	Yes/No	Send notification to the administrator or not when a Bot threat is detected
Intscan.ini [EMail-Scan] MsgBotTrapNotiToAdmin	IntelliTrap detected a potentially malicious application in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	string	Content sent to the administrator when a Bot threat is detected
Intscan.ini [EMail-Scan] EnableBotTrapNotiToRecipient	No	Yes/No	Send notification to recipient or not when a Bot threat is detected

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [EMail-Scan] MsgBotTrapNotiToRecipient	Warning - InterScan VirusWall has detected a file containing a malicious application in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	string	Content sent to recipient when a Bot threat is detected
Intscan.ini [EMail-Scan] EnableBotTrapNotiToSender	No	Yes/No	Send notification to sender or not when a Bot threat is detected
Intscan.ini [EMail-Scan] MsgBotTrapNotiToSender	Warning--InterScan VirusWall has detected a file containing a malicious application in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	string	Content sent to sender when a Bot threat is detected
Intscan.ini [Email-Scan] WholeMailScanAction	Delete	Delete,Quarantine	Set smtp whole file scan action as delete
Intscan.ini [Email-Scan] OutboundWholeMailVirusScan	no	yes/no	Enable/Disable the smtp-outgoing whole file scan feature
Intscan.ini [Email-Scan] EnableOutgoingNotiToAdmin	yes	yes/no	Send or not send notification to administrator when detect virus in smtp-outgoing

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [Email-Scan] MsgOutgoingNotiToAdmin	A virus/malware was detected in a message sent from %SENDER% to %RCPTS% . The message subject is "%SUBJECT% ". InterScan VirusWall has taken the action: %FINALACTION%.	String	The body of notification sent to administrator
Intscan.ini [Email-Scan] EnableOutgoingNotiToRecipient	no	yes/no	Send or not send notification to recipient when detect virus in smtp-outgoing
Intscan.ini [Email-Scan] MsgOutgoingNotiToRecipient	Warning--InterScan VirusWall has detected a virus in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be delivered.	String	The body of notification sent to recipient
Intscan.ini [Email-Scan] EnableOutgoingNotiToSender	no	yes/no	Send or not send notification to sender when detect virus in smtp-outgoing

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [Email-Scan] MsgOutgoingNotiToSender	Warning--InterScan VirusWall has detected a virus in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	String	The body of notification sent to sender
Intscan.ini [Email-Scan] InboundWholeMailVirusScan	no	yes/no	Enable/Disable the smtp-incoming whole file scan feature
Intscan.ini [Email-Scan] Email	yes	yes/no	Send or not send notification to administrator when detect virus in smtp-incoming
Intscan.ini [Email-Scan] Message1	A virus/malware was detected in a message sent from %SENDER% to %RCPTS% . The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	String	The body of notification sent to administrator
Intscan.ini [Email-Scan] Ewarning	no	yes/no	Send or not send notification to recipient when detect virus in smtp-incoming

Parameter	Default Value	Possible Values	Explanation
Intscan.ini [Email-Scan] Emessage	Warning--InterScan VirusWall has detected a virus in a message sent to you from %SENDER%. The message subject is %SUBJECT%. The message may not be delivered.	String	The body of notification sent to recipient
Intscan.ini [Email-Scan] EWarningSender	no	yes/no	Send or not send notification to sender when detect virus in smtp-incoming
Intscan.ini [Email-Scan] EMessageSender	Warning--InterScan VirusWall has detected a virus in a message sent from your computer to %RCPTS%. The message subject is "%SUBJECT%". The message may not have been delivered.	String	The body of notification sent to sender
Config.xml SMTP\AntiSpyware\Enable	1	1,0	Enable SMTP spyware scanning or not
Config.xml SMTP\AntiSpyware\SpywareTypes	255	0~255	The spyware types that will be scanned
Config.xml SMTP\AntiSpyware\Action	delete	Pass/Quarantine/Delete	Action taken on attachment when spyware is detected
Config.xml SMTP\AntiSpyware\SpywareExceptions		string	The spyware exception file name list for SMTP
Config.xml SMTP\AntiBotTrap\Enable	1	1,0	Enable SMTP IntelliTrap scanning or not
Config.xml SMTP\ AntiBotTrap \Action	Quarantine	Pass/Quarantine/Delete	Action on attachment when a Bot threat is detected

Parameter	Default Value	Possible Values	Explanation
Config.xml SMTP\AntiSpyware\ OutgoingEnable	1	1,0	Enable SMTP spyware outgoing scanning or not
Config.xml SMTP\AntiSpyware\ OutgoingSpywareTypes	255	0~255	The spyware types that will be scanned
Config.xml SMTP\AntiSpyware\ OutgoingAction	Delete	Pass/Quarantine/Delete	Action taken on attachment when spyware is detected
Config.xml SMTP\AntiSpyware\ OutgoingSpywareExceptions		string	The spyware exception file name list for SMTP outgoing

SMTP Content Filtering

Parameter	Default Value	Possible Values	Explanation
config.xml Smtp/Emanager/Enable	1	1,0	Enable SMTP content filtering

SMTP Anti-spam

Parameter	Default Value	Possible Values	Explanation
Smtp\TMASE\AntiSpam\ Enable	1	0,1	Enable/Disable the SMTP anti-spam feature
Smtp\TMASE\AntiSpam\ WhiteList	None	String	SMTP anti-spam approved sender list
Smtp\TMASE\AntiSpam\ BlackList	None	String	SMTP anti-spam blocked sender list
Smtp\TMASE\AntiSpam\ WhiteKeyword	None	String	SMTP anti-spam exception list
Smtp\TMASE\AntiSpam\ MostConfidentAction	Stamp	StampDeleteDeliverQuarantine	SMTP anti-spam action for message with high confidence level

Parameter	Default Value	Possible Values	Explanation
Smtp\TMASE\AntiSpam\ ConfidentAction	Stamp	StampDeleteDeliver Quarantine	SMTP anti-spam action for message with medium confidence level
Smtp\TMASE\AntiSpam\ LeastConfidentAction	Stamp	StampDeleteDeliver Quarantine	SMTP anti-spam action for message with low confidence level
Smtp\TMASE\AntiSpam\ Notifications\Administrator \Enable	1	0,1	Enable/Disable SMTP notification sent to the administrator
Smtp\TMASE\AntiSpam\ Notifications\Administrator \FromUser	isvw@FQDN	String	Sender's address on the SMTP anti-spam notification email sent to the administrator
Smtp\TMASE\AntiSpam\ Notifications\Administrator \Body	A message sent from %SENDER% to %RCPTS% has been identified as spam. The message subject is "%SUBJECT %". InterScan VirusWall has taken the action: %FINALACTI ON%.	String	Body of the SMTP anti-spam notification email sent to the administrator
Smtp\TMASE\AntiSpam\ Notifications\Administrator \Charset	UTF-8	String	Character set of the SMTP anti-spam notification email sent to the administrator
Smtp\TMASE\AntiSpam\ Notifications\Administrator \Subject	Spam email was identified.	String	Subject of the SMTP anti-spam notification email to the administrator
intscan.ini [EMail-Scan] NRSEnable	yes	yes/no	Enable or disable Email Reputation
intscan.ini [EMail-Scan] ServiceLevel	low	low/high	The Email Reputation service level
intscan.ini [EMail-Scan] ApprovedIpAddresses		IP addresses	The Approved IP addresses list
intscan.ini [EMail-Scan] RBLSpamAction	1	0/1/2	The action for RBL+. 0 means pass, 1 means disconnect with error code, 2 means disconnect without error code

Parameter	Default Value	Possible Values	Explanation
intscan.ini [EMail-Scan] RBLErrorCode	550	400~599	Return error code
intscan.ini [EMail-Scan] QILSpamAction	1	0/1/2	The action for QIL+. 0 means pass, 1 means disconnect with error code, 2 means disconnect without error code
intscan.ini [EMail-Scan] QILErrorCode	450	400~599	Return error code

SMTP Anti-phishing

Parameter	Default Value	Possible Values	Explanation
Smtp\TMASE\AntiPhish\Enable	1	0,1	Enable/Disable anti-phishing for SMTP
Smtp\TMASE\AntiPhish\AntiPhishAction	Quarantine	QuarantineDeliverDelete	SMTP anti-phishing action
Smtp\TMASE\AntiPhish\Notifications\Administrator\Enable	1	0,1	Enable/Disable SMTP notification to the administrator
Smtp\TMASE\AntiPhish\Notifications\Administrator\FromUser	isvw@FQDN	String	Sender's address on the SMTP anti-phishing email notification sent to the administrator
Smtp\TMASE\AntiPhish\Notifications\Administrator\Body	A phishing site was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%" . InterScan VirusWall has taken the action: %FINALACTION%.	String	Body of the SMTP anti-phishing notification email sent to the administrator

Parameter	Default Value	Possible Values	Explanation
Smtp\TMASE\AntiPhish\Notifications\Administrator\Charset	UTF-8	String	Character set of the SMTP anti-phishing notification email sent to the administrator
Smtp\TMASE\AntiPhish\Notifications\Administrator\Subject	A possible phishing security risk was identified in the message.	String	Subject of the SMTP anti-phishing email sent to the administrator

POP3 Virus/Spyware/IntelliTrap Scanning

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\MailVirus Scan\Enable	1	0,1	Enable VirusScan or not. If disabled, all of MacroScan/MailTrap/ Anti-spyware/Virus filters will be disabled.
Pop3\Policies\Rule1\MailVirus Scan\AddAlert	1	0,1	Insert VirusAlert or MacroStripAlert into user's message or not
Pop3\Policies\Rule1\MailVirus Scan\AddInfo	1	0,1	Insert disclaimer message into the user's email or not
Pop3\Policies\Rule1\MailVirus Scan\Additional	1	0,1	Insert additional message into the user's message or not
Pop3\Policies\Rule1\MailVirus Scan\AdditionalMsg	"Please contact the administrator for further information."	String	Showed when 'Additional' is enabled and there are other messages inserted as the last sentence of the warning message. This is inserted once for the whole email.

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\MailVirus Scan\CleanLayerExceedMsg	"Warning: Your file, %CONTAINER NAME%, is infected with too many viruses. ISVW-SE stopped attempting to clean them, and it still may contains some viruses"	String	Related to MultipleCleanLayer. When the number of cleaning is beyond MultipleCleanLayer, the infected files might not be cleaned entirely. This message will be inserted into the user's message.
Pop3\Policies\Rule1\MailVirus Scan\CompressScan	1	0,1	Enable or disable scanning of compressed file/attachment
Pop3\Policies\Rule1\MailVirus Scan\EnableMailTrap	1	0,1	Perform MailTrap scan or not
Pop3\Policies\Rule1\MailVirus Scan\EnableSpywareScan	1	0,1	Perform spyware scan or not
Pop3\Policies\Rule1\MailVirus Scan\EnableTrendExt	1	0,1	If enabled and file/attachment extension matches the scan engine's recommended extensions, then the file/attachment will be scanned.
Pop3\Policies\Rule1\MailVirus Scan\EnableUserExcludeExt	1	0,1	If enabled and file/attachment extension matches UserExcludeExtensions, then the file/attachment will not be scanned. See also CheckExtension.
Pop3\Policies\Rule1\MailVirus Scan\EnableUserExt	1	0,1	If enabled and file/attachment extension matches UserExtensions, then the file/attachment will be scanned. See also CheckExtension.
Pop3\Policies\Rule1\MailVirus Scan\EnableVirusScan	1	0,1	Perform virus scanning or not
Pop3\Policies\Rule1\MailVirus Scan\EnableWholeFileScan	0	0,1	Enable/Disable the Pop3 whole file scan feature

Parameter	Default Value	Possible Values	Explanation
Pop3\Polices\Rule1 \MailVirusScan \VirusAlert4WholeFileScan	InterScan VirusWall has detected an item that contains a virus in this message.	String	Disclaimer inserted into mail body
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Deliver\Enable	0	0,1	Set POP3 whole file scan action as deliver or not
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Delete\Enable	0	0,1	Set POP3 whole file scan action as delete or not
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Delete\CreateReplac eMail	1	0,1	Send or not send a replace mail to recipint when detect a virus by whole file scan
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Delete\Subject	The message has been deleted.	String	Subject of the replacement email
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Delete\Body	A virus has been detected and your message has been deleted.	String	Content of replacement email
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Quarantine \CreateReplaceMail	1	0,1	Send or not send a replace mail to recipint when detect a virus by whole file scan
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Quarantine\Subject	The message has been quarantined.	String	Subject of replacement email
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\Quarantine\Body	A virus has been detected and your message has been quarantined.	String	Content of replacement email

Parameter	Default Value	Possible Values	Explanation
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationAdmin\Enable	1	0,1	Send or do not send notification to administrator when detect virus by whole file scan
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationAdmin\Body	Virus/malware was detected in a message sent from %SENDER% to %RCPTS% . The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	String	Content of notification
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationAdmin\Subject	A virus was detected.	String	Subject of notification
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationRecipient \Enable	0	0,1	Send or do not send notification to administrator when detect virus by whole file scan
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationRecipient\ Body	Warning: InterScan VirusWall has detected a virus in a message sent to you from %SENDER%. The message subject is "%SUBJECT%". The message may not be delivered.	String	Content of notification
Pop3\Polices\Rule1 \MailVirusScan\Outcomes \OutcomeWholeFileScanVirus \Actions\NotificationRecipient \Subject	A virus was detected.	String	Subject of notification

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\MailVirus Scan\IntelliScan	1	0,1	If enabled, ISVW will try to scan file/attachment by true type, but not by extension.
Pop3\Policies\Rule1\MailVirus Scan\MaxDecompressCount	0	0~2148473647	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\MailVirus Scan\MaxDecompressDepth	20	1~20	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\MailVirus Scan\MaxDecompressSize	2147483647	1~2147483647	ISVW will scan compressed files that do not exceed the value specified here
Pop3\Policies\Rule1\MailVirus Scan\MaxEntityCount	50	10~2148473647	ISVW will scan compress mails with entities under the value specified here
Pop3\Policies\Rule1\MailVirus Scan\MaxScanSize	0	0~2148473647	The maximum size of file/attachment VirusScan will process
Pop3\Policies\Rule1\MailVirus Scan\MaxVirusCount	20	0~50	Number of viruses to display
Pop3\Policies\Rule1\MailVirus Scan\MultipleClean	1	0,1	Whether to circularly check and clean if file/attachment is infected with a virus
Pop3\Policies\Rule1\MailVirus Scan\MultipleCleanLayer	5	0~2148473647	When user sets the option MultipleClean, virus filter will loop clean the infected file until no more viruses can be cleaned. This option can limit the loop count.
Pop3\Policies\Rule1\MailVirus Scan\NoVirusAlert	0	0,1	Whether to insert NoVirusMsg into the user's message or not when attachment contains no virus
Pop3\Policies\Rule1\MailVirus Scan\NoVirusMsg	"The file attachment, (%CONTAINER NAME%), has been scanned using antivirus software. No viruses were detected."	string	Displays if NoVirusAlert is enabled and attachment has no virus. This is inserted for each email attachment.
Pop3\Policies\Rule1\MailVirus Scan\ReplaceWarning	1	0,1	Whether to replace the deleted attachment with this warning message or not

Parameter	Default Value	Possible Values	Explanation
Pop3\Policies\Rule1\MailVirus Scan\ReplaceWarningMsg	"A file attached to this message, (%CONTAINER NAME%), was removed because it was infected with the %VIRUSNAME % computer virus."	String	If attachment has been deleted, and ReplaceWarning is set to 1(nonzero=enable), the attachment will be inserted into the user's message to replace the removed attachment
Pop3\Policies\Rule1\MailVirus Scan\SafeStamp	1	0,1	Whether to insert SafeStampMsg into the user's message or not
Pop3\Policies\Rule1\MailVirus Scan\SafeStampMsg	"InterScan VirusWall has scanned this message and found it to be free of known viruses."	string	Displays when SafeStamp is enabled and message is regarded as safe by virus filter. This is inserted once on the entire email.
Pop3\Policies\Rule1\MailVirus Scan\ScanAll	1	0,1	If enabled, every file/attachment will be passed to the scan engine for scanning. See also CheckExtension.
Pop3\Policies\Rule1\MailVirus Scan\UserExcludeExtensions	None	string	Extension list, with extension names delimited by semicolon. For example, "exe;zip;r??", support wildcard "*" and "?". Do not insert any redundant space. See EnableUserExcludeExt.
Pop3\Policies\Rule1\MailVirus Scan\UserExtensions	None	String	Extension list, with extension names delimited by semicolon. For example, "exe;zip;r??", support wildcard "*" and "?". Do not insert any redundant space. See EnableUserExt.
Pop3\Policies\Rule1\MailVirus Scan\VirusAlert	"InterScan VirusWall has scanned this message and found it to be free of known viruses."	String	Contained in scan result. This is inserted into users' message, and inserted for each email attachment

POP3 Content Filtering

Parameter	Default Value	Possible Values	Explanation
config.xml Pop3/Policies/Rule1/Mail ContentScanEnable	1	1,0	POP3 content filtering enabled

POP3 Anti-spam

Parameter	Default Value	Possible Values	Explanation
Scan\TMASE\AntiSpam\Enable	1	0,1	Enable/Disable POP3 anti-spam
Scan\TMASE\AntiSpam\WhiteList	None	String	POP3 anti-spam approved sender list
Scan\TMASE\AntiSpam\BlackList	None	String	POP3 anti-spam blocked sender list
Scan\TMASE\AntiSpam\WhiteKeyword	None	String	POP3 anti-spam exception list
Scan\TMASE\AntiSpam\MostConfident Action	Stamp	Stamp Delete Deliver Quarantine	POP3 anti-spam action for message with high confidence level
Scan\TMASE\AntiSpam\ConfidentAction	Stamp	Stamp Delete Deliver Quarantine	POP3 anti-spam action for message with medium confidence level
Scan\TMASE\AntiSpam\LeastConfident Action	Stamp	Stamp Delete Deliver Quarantine	POP3 anti-spam action for message with low confidence level
Scan\TMASE\AntiSpam\Notifications\ Administrator\Enable	1	0,1	Enable/Disable POP3 notification sent to the administrator
Scan\TMASE\AntiSpam\Notifications\ Administrator\FromUser	isvw@FQDN	String	Sender’s address on the POP3 anti-spam notification email sent to the administrator

Parameter	Default Value	Possible Values	Explanation
Scan\TMASE\AntiSpam\Notifications\Administrator\Body	A message sent from %SENDER% to %RCPTS% has been identified as spam. The message subject is "%SUBJECT %". InterScan VirusWall has taken the action: %FINALACTION%.	String	Body of the POP3 anti-spam notification email sent to the administrator
Scan\TMASE\AntiSpam\Notifications\Administrator\Charset	UTF-8	String	Character set of POP3 anti-spam notification email sent to the administrator
Scan\TMASE\AntiSpam\Notifications\Administrator\Subject	Spam email was identified	String	Subject of POP3 anti-spam notification email sent to the administrator

POP3 Anti-phishing

Parameter	Default Value	Possible Values	Explanation
Scan\TMASE\AntiPhish\Enable	1	0,1	Enable/Disable anti-phishing for POP3
Scan\TMASE\AntiPhish\AntiPhishAction	Quarantine	Quarantine Deliver Delete	POP3 anti-phishing action
Scan\TMASE\AntiPhish\Notifications\Administrator\Enable	1	0,1	Enable/Disable POP3 notification sent to the administrator
Scan\TMASE\AntiPhish\Notifications\Administrator\FromUser	isvw@FQDN	String	Sender address on the POP3 anti-phishing notification email sent to the administrator

Parameter	Default Value	Possible Values	Explanation
Scan\TMASE\AntiPhish\Notifications\Administrator\Body	A phishing site was detected in a message sent from %SENDER% to %RCPTS%. The message subject is "%SUBJECT%". InterScan VirusWall has taken the action: %FINALACTION%.	String	Body of the POP3 anti-phishing notification email sent to the administrator
Scan\TMASE\AntiPhish\Notifications\Administrator\Charset	UTF-8	String	Character set of the POP3 anti-phishing notification email sent to the administrator
Scan\TMASE\AntiPhish\Notifications\Administrator\Subject	A possible phishing security risk was identified in the message.	String	Subject of the POP3 anti-phishing notification email sent to the administrator

POP3 Configuration

Parameter	Default Value	Possible Values	Explanation
config.xml root/Pop3/IPAddressToBind	INADDR_ANY		Listening IP addresses
config.xml root/Pop3/MaxSimultaneousClientConnections	100	1~100	Concurrent clients
config.xml root/Pop3/AllowLoginParameter	1	0/1	Enable/Disable proxy mode
config.xml root/Pop3/InboundPort	110		Proxy mode listening port
config.xml root/Pop3/AllowServerPortMapping	0	0/1	Enable/Disable port mapping

Parameter	Default Value	Possible Values	Explanation
config.xml root/Pop3/ServerPortMapping Count	0		Number of ports mapped

HTTP

Parameter	Default Value	Possible Values	Explanation
Config.xml HTTP\Main\http\virus_scan_ enabled	Yes	Yes/No	Enable or disable virus scanning
Config.xml HTTP\Main\http\skiptype		A list of MIME types	This provides better performance but less security since the content-type header may not truly represent the type of the content.
Config.xml HTTP\Main\http\action	clean	Pass/ Delete/ Move/ Clean	Pass: pass to user Delete: block the transfer Move: move the data into a temporary file on proxy host Clean: clean the file then continue the transfer, if it is cleanable. If uncleanable, 'ucaction' must be set. 'ucaction' can be pass, move or delete. The default value is delete.
Config.xml HTTP\Main\http\unaction	delete	Pass/ Move/ Delete	'ucaction' can be pass, move or delete. The default value is delete.
Config.xml HTTP\Main\http\movedir	C:\Program Files\Trend Micro\InterScan VirusWall\ quarantine\http	Path	The directory to move the virus to (quarantine)
Config.xml HTTP\Main\http\spyware_scan_ enabled	Yes	Yes/No	Enable or disable spyware scan

Parameter	Default Value	Possible Values	Explanation
Config.xml HTTP\Main\http\spyaction	delete	Action can be move, pass or delete	How to handle spyware
Config.xml HTTP\Main\http\virus_notification	Trend Micro InterScan VirusWall has determined that the file you are attempting to transfer is infected. It has taken action on the file.	String	Notification displayed when virus is found
Config.xml HTTP\Main\http\spyware_ notification	Trend Micro InterScan VirusWall has determined that the file you are attempting to transfer contains spyware/gray ware. It has taken action on the file.	String	Notification displayed when spyware is found
Config.xml HTTP\Main\http\reject_notification	The file that you are attempting to transfer has been blocked. Organization policy prohibits transfer of this type of file.	string	Notification displayed when request is blocked (can be caused by URL blocking, URL filtering, or OPP blocking)

Parameter	Default Value	Possible Values	Explanation
Config.xml HTTP\Main\http\phish_notification	The URL you are attempting to access may redirect you to a site to collect your confidential and personal data. Access to this URL has been blocked for security reasons. If you have any questions, contact your administrator.	string	Notification displayed when URL access is blocked by PhishTrap
Config.xml HTTP\Main\http\url_blocking_ enabled	Yes	Yes/No	Enable or disable all URL blocking functions
Config.xml HTTP\Main\scan\ special_handling	Yes	Yes/No	Yes: handle large files with either a progress page or with "scan-behind". No: large files will be treated the same as all other contents. Enable/Disable "deferred" or "scan-behind" scan when a file is larger than the file size limitation
Config.xml HTTP\Main\scan\scan_huge_file	Yes	Yes/No	Enable/Disable scanning of large files. If this is set to 'Yes' then no files larger than max_scan_size will be scanned.
Config.xml HTTP\Main\scan\ max_scan_size	1048576	Sensible large file size	Specify the file size limitation of scanned files, in KB.
Config.xml HTTP\Main\scan\ deferred_scanning	Late	Yes/No/Late	Setting for deferred scanning
Config.xml Http\Main\scan\trickle_rate	512K	File size that is less than 2M-1	File size that the ISVW server receives
Config.xml Http\Main\scan\trickle_max_size	1024Bytes	file size that is less than 2M-1	File size that ISVW server sends to the client

Parameter	Default Value	Possible Values	Explanation
Config.xml HTTP\Main\scan\ max_synchronous_scan_size	524288	File size for deferred scan setting	File size for deferred scanning
Config.xml HTTP\Main\internet-access-monitoring\ enable	No	Yes/No	Turn On/Off Access Log
Config.xml HTTP\Protocol\HttpProxy\http\ self_proxy	Yes	Yes/No	Self_proxy indicates whether ISVW will act as a direct HTTP proxy (i.e. Browser --> ISVW --> Web server) or as a dependent proxy (Browser --> ISVW --> Upstream HTTP proxy --> Web server). Set this to "Yes" to operate as a direct proxy, or "No" to act as a dependent proxy. If set to "No" you must specify the upstream proxy's name and port number in original_server and original_server_port, respectively.
Config.xml HTTP\Protocol\HttpProxy\http\ original_server		IP address or host name	original_server indicates the name of the upstream HTTP proxy server that ISVW will pass traffic through if it is installed in dependent mode
Config.xml HTTP\Protocol\HttpProxy\http\ original_server_port	8080	Port number	original_server_port contains the port number that the upstream HTTP proxy server is listening to for HTTP traffic
Config.xml HTTP\Protocol\HttpProxy\http\ anonymous_ftp_mail_address		Anonymous FTP mail address	anonymous_ftp_mail_addre ss indicates the email address ISVW should supply when connecting anonymously to an FTP server for FTP-over-HTTP requests
Config.xml HTTP\Protocol\HttpProxy\http\ reverse_proxy	No	Yes/No	Checked when self_proxy=no, if this is set to "Yes", reverse proxy mode is activated, original server/port will be used as an ordinary HTTP server, not an upstream-proxy.

Parameter	Default Value	Possible Values	Explanation
Config.xml HTTP\plugin\ScanVsapi\http\level	scanall	scanall/ scanintelli/ scanext	scanall: scan all traffic scanintelli: the scan engine decides which files to scan based on TrueFileType scanext: scan only files with certain extensions
Config.xml HTTP\plugin\ScanVsapi\http\ extensions		Extension list	The default list of extensions to scan if level is set to "scanext". Items should be separated with a semicolon (;). Do not add a dot (.) to each extension.
Config.xml HTTP\plugin\ScanVsapi\http\ spyware_exceptions		A string list separated by ";"	The list of exception file names for spyware scanning. To use a file name extension, add a '*'. For example, "filename.exe;*.ext1"
Config.xml HTTP\Plugin\URLFilter\plug-in\ enabled	No	Yes/No	Enable or disable the scan module

FTP

Parameter	Default Value	Possible Values	Explanation
intscan.ini [FTP-Scan] MaxThreads	50	>= 0	FTP > Configuration > Maximum connections
intscan.ini [FTP-Scan] InterScanFTPServicePort	21	1 ~ 65535	FTP service port of ISVW. Cannot be modified from the console.
intscan.ini [FTP-Scan] UseFTPProxy	No	Yes/No	FTP > Configuration > Use FTP proxy
intscan.ini [FTP-Scan] FOrgPort	21	1 ~ 65535	FTP > Configuration > Use FTP proxy: the port of the existing FTP proxy
intscan.ini [FTP-Scan] ForcePassiveFTP	No	Yes/No	FTP > Configuration > Use passive FTP for all file transfers

Parameter	Default Value	Possible Values	Explanation
intscan.ini [FTP-Scan] Level	ScanAll (All scannable files)	ScanAll / IntelliScan / ScanExt	FTP > Scanning > Target > Files to Scan
intscan.ini [FTP-Scan] SMTPServerPort	25	1 ~ 65535	Administration > Notification Settings: the port of the SMTP server
intscan.ini [FTP-Scan] EMail	Yes	Yes/No	FTP > Scanning > Notification > Administrator
intscan.ini [FTP-Scan] Action	Cleandelete (Clean files. If cannot be cleaned, then Block.)	Cleanmove / Cleandelete / Cleanpass / Move / Delete / Pass	FTP > Scanning > Action
intscan.ini [FTP-Scan] TrickleAmount	1024	>= 0	FTP > Configuration: Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received
intscan.ini [FTP-Scan] TricklePeriod	512	>= 0	FTP > Configuration: Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received
intscan.ini [FTP-Scan] DecompressionLayerLimit	14	2 ~ 20	FTP > Scanning > Target > Number of layers of compression exceeds
intscan.ini [FTP-Scan] ExtractFileSizeLimit	1073741824 (1 GB)	0 ~ 2147483647	FTP > Scanning > Target > Extracted file size exceeds
intscan.ini [FTP-Scan] AntiVirus	Yes	Yes/No	FTP > Scanning > Target > Enable FTP Scanning
intscan.ini [FTP-Scan] BlockMethod	BlockNone (Scan all compressed files)	BlockNone / BlockAll / BlockIf	FTP > Scanning > Target > Compressed File Handling
intscan.ini [FTP-Scan] MaxDecompressCount	100	>= 0	FTP > Scanning > Target > Extracted file count exceeds
intscan.ini [FTP-Scan] MaxDecompressRatio	100	0 ~ 100	FTP > Scanning > Target > Extracted file size/compressed file size ratio exceeds

Parameter	Default Value	Possible Values	Explanation
intscan.ini [FTP-Scan] EnableGreeting	Yes	Yes/No	FTP > Configuration > Send a greeting message when connection is established
config.xml [FTP] Enable	1	1 / 0	Summary > FTP > Enable FTP Traffic
config.xml [FTP\AntiSpyware] Enable	1	1 / 0	FTP > Anti-spyware > Enable FTP Anti-spyware
config.xml [FTP\AntiSpyware] SpywareTypes	255 (Scan for all types of spyware / grayware)	Select options from the console	FTP > Anti-spyware > Scan for Spyware/Grayware
config.xml [FTP\AntiSpyware] Action	Delete	Quarantine / Delete / Pass	FTP > Anti-spyware > Action
config.xml [Webui\FTP] MaxDecompressSizeUnit	1073741824 (1 GB)	Select options from the console	FTP > Scanning > Target > Extracted file size exceeds: unit options
config.xml [Webui\FTP\AntiVirus]Second Action	delete	move / delete / pass	FTP > Scanning > Action: If cannot be cleaned, specify an action

Logs

Parameter	Default Value	Possible Values	Explanation
config.xml [Common\Logging] LogDir	log		The relative path of log files. Cannot be modified from the console.
config.xml [Common\Logging] EnableMaintenance	1	1 / 0	Logs > Maintenance > Automatic > Enable Automatic Purge
config.xml [Common\Logging] WhatMaintenance	63 (All types of logs)	Select options from the console	Logs > Maintenance > Automatic > Target
config.xml [Common\Logging] ExpiredDays	30	0 ~ 360	Logs > Maintenance > Automatic > Action

Parameter	Default Value	Possible Values	Explanation
config.xml [Common\Logging] DebugEnable	0	1 / 0	Whether to enable debug log; disabled by default
config.xml [Webui\Log\Query] protocol	1(SMTP)	Select options from the console	Logs > Query > Protocol
config.xml [Webui\Log\Query] logtype	1(Virus/Malware)	Select options from the console	Logs > Query > Log type
config.xml [Webui\Log\Query] timeperiod	1 (All)	Select options from the console	Logs > Query > Time period
config.xml [Webui\Log\Query] ItemPerPage	25	10 / 25 / 50 / 100	Logs > Query > Entries per page
config.xml [Webui\Log\Maintenance \Auto] Enable	0	1 / 0	Logs > Maintenance > Automatic > Enable Automatic Purge
config.xml [Webui\Log\Maintenance \Auto] Action	1 (Delete all logs selected above)	Select options from the console	Logs > Maintenance > Automatic > Action
config.xml [Webui\Log\Maintenance \Auto] LogTypes	63(All types of logs)	Select options from the console	Logs > Maintenance > Automatic > Target
config.xml [Webui\Log\Maintenance \Auto] ExpiredDays	30	0 ~ 360	Logs > Maintenance > Automatic > Action
config.xml [Webui\Log\Maintenance \Manual] Action	1 (Delete all logs selected above)	Select options from the console	Logs > Maintenance > Manual > Action
config.xml [Webui\Log\Maintenance \Manual] LogTypes	63 (All types of logs)	Select options from the console	Logs > Maintenance > Manual > Target
config.xml [Webui\Log\Maintenance \Manual] ExpiredDays	30	0 ~ 360	Logs > Maintenance > Manual > Action

Parameter	Default Value	Possible Values	Explanation
config.xml [SMTP][HTTP][POP3][FTP] WriteConnectionMsg	1	0/1	Enable or disable transaction log for SMTP/HTTP/POP3/FTP
config.xml [SMTP][HTTP][POP3][FTP] ConnectionLogLevel	10	10/0	Set rough level (10) or diagnostic level (0) for SMTP/HTTP/POP3/FTP transaction logs

Quarantine

Parameter	Default Value	Possible Values	Explanation
config.xml [Webui\Quarantine\Maintenance] ManualDelete	7	0 ~ 360	Quarantines > Maintenance > Manual > Action

Outbreak Prevention Services (OPS)

Parameter	Default Value	Possible Values	Explanation
config.xml root/Scan/OPP/Enable	0	0/1	Disable/Enable OPP
config.xml root/Scan/OPP/IssueDuration	2880	1440 to 7200	OPS Expiration
config.xml root/Common/ActiveUpdate/ScheduleUpdate/OPSUpdate/EnableUpdate	1	0/1	Enable/Disable scheduled update
config.xml root/Common/ActiveUpdate/ScheduleUpdate/OPSUpdate/Minutes	10	1 to 120	Scheduled update Interval

Parameter	Default Value	Possible Values	Explanation
config.xml root/Common/ActiveUpdate/UpdateServers/Server.3/Source	http://oc.activeupdate.trendmicro.com/activeupdate/	The real TrendLabs OPS Update URL	OPS AU Server

ActiveUpdate

Parameter	Default Value	Possible Values	Explanation
Root\common\ActiveUpdate\UpdateServers\Server.1\Source	http://isvw602-av.activeupdate.trendmicro.com/activeupdate/	AU server URL	AU server for updating the virus/spyware detection pattern and engines
Root\common\ActiveUpdate\UpdateServers\Server.2\Source	http://isvw602-as.activeupdate.trendmicro.com/activeupdate/	AU server URL	AU server for updating the spam pattern and engine
Root\common\ActiveUpdate\UpdateServers\Server.3\Source	http://oc.activeupdate.trendmicro.com/activeupdate/	AU server URL	AU server for updating the OPP pattern
Root\common\ActiveUpdate\ScheduleUpdate\virusUpdate\EnableUpdate	1	1/0	Enable or disable scheduled update

Pattern Update Notification Default Values

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Common/ActiveUpdate/Notification/tmpdir	temp	Relative path of temporary folder	Temporary folder for ISVW usage

Parameter	Default Value	Possible Values	Explanation
Config.xml root/Common/ActiveUpdate/Notification/FromUser	isvw@client.tw.trendnet.org	Email address	The notification sender email addresses
Config.xml root/Common/ActiveUpdate/Notification/SuccessEnable	0	0/1	Disable/enable successfully update notification function
Config.xml root/Common/ActiveUpdate/Notification/SuccessSubject	ActiveUpdate success notification	String	Subject of successfully update notification email
Config.xml root/Common/ActiveUpdate/Notification/SuccessBody	ISVW updated following items successfully	String	Mail body of successfully update notification email
Config.xml root/Common/ActiveUpdate/Notification/FailEnable	0	0/1	Disable/enable unsuccessfully update notification function
Config.xml root/Common/ActiveUpdate/Notification/FailSubject	ActiveUpdate fail notification	String	Subject of unsuccessfully update notification email
Config.xml root/Common/ActiveUpdate/Notification/FailBody	ISVW updated following items failed	String	Mail body of unsuccessfully update notification email

Appendix C

Migration from InterScan VirusWall 3.55

Use this appendix as a reference when migrating settings from InterScan VirusWall (ISVW) 3.55 with eManager 3.52 to ISVW 7.0.

Topics in this appendix are as follows:

SMTP Migration

SMTP Migration Summary

ISVW 7.0 migrates most SMTP settings from ISVW 3.55, except for the following:

- "From:" address used in virus notifications
- "From:" address used in other notifications

SMTP settings migrate from ISVW 3.55 to ISVW 7.0 with conditions outlined in *Table C-1*.

TABLE C-1. SMTP Migration Conditions

Item	Description
Scan inbound messages	This item migrates. If this value is set to **no**, after migration, all inbound messages will be scanned for the following: Bot threats and spyware/grayware. Inbound messages will NOT be scanned for viruses if this value is set to **no**.
Enable outbound mail processing	This item migrates. If this value is set to **no**, after migration, outbound message processing does not function.
Enable outbound mail virus scanning	This item migrates. If this value is set to **no**, after migration, all outbound messages will not be scanned for the following: viruses, Bot threats and spyware/grayware.
Stop delivery of infected outbound messages	This item migrates, but does not display in UI. If this value is set to yes, after migration, all infected outbound messages will be blocked. To enable outbound mail processing, you must modify the configuration file manually and then restart the service.
Scan Extensions	ISVW 7.0 has a default scan list. After migration, the scan extension list is as follows: 7.0 default list + 3.55 scan extensions.
Notifications to administrators/ senders /recipients	After migration, these settings apply to both inbound message and outbound messages.

TABLE C-1. SMTP Migration Conditions (Continued)

Item	Description
Safe Stamp/Virus Message	After migration, these settings apply to both inbound message and outbound messages.
Decompression layer limit	After migration, this item will take effect only if you are scanning for compressed files.
Extract file size limit	After migration, this item will take effect only if you are scanning for compressed files.
Whole file scanning	This item migrates. Not configurable from Web UI.

SMTP Migration Table

Table C-2 provides detailed information about the SMTP migration from ISVW 3.55 to ISVW 7.0 .

TABLE C-2. Detailed SMTP Migration

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Whether to scan inbound message or not	[common] MailScan=yes	[common] MailScan=yes	SMTP configuration > enable virus scanning	NONE
Limits the number of messages being scanned per processor. Additional messages are sent a "452 Server too busy" response.	[EMail-Scan] MaxScanningThreadsProc=25	[EMail-Scan] MaxScanningThreadsProc=25	NONE	NONE
Limit the number of threads created to deliver mail after scanning.	[EMail-Scan] MaxSMTPClientThreadsProc=25	[EMail-Scan] MaxSMTPClientThreadsProc=25	NONE	NONE

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Fixed number of background threads per processor created to deliver inbound mail in the mqueue after scanning, When mqueue is backed up, this value can be increased.	[EMail-Scan] BackgroundMqueueInThreadsProc =2	[EMail-Scan] BackgroundMqueueInThreadsProc =2	NONE	NONE
Fixed number of background threads per processor created to deliver outbound mail in the mqueue after scanning, When mqueue is backed up, this value can be increased.	[EMail-Scan] BackgroundMqueueOutThreadsProc=2	[EMail-Scan] BackgroundMqueueOutThreadsProc=2	NONE	NONE
Fixed number of threads to deliver InterScan generated messages in the bmqueue.	[EMail-Scan] BackgroundBMqueueThreadsProc=1	[EMail-Scan] BackgroundBMqueueThreadsProc=1	NONE	NONE
Maximum number of simultaneous connections accepted by InterScan.	[EMail-Scan] MaxClientConnections=25	[EMail-Scan] MaxClientConnections=25	Advanced options > Maximum # of simultaneous SMTP client connections (0 = unlimited):	SMTP > configuration > Maximum # of simultaneous SMTP client connections (0 = unlimited):

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Disable insert received header in email or not	[EMail-Scan] DisableReceivedHeader=no	[EMail-Scan] DisableReceivedHeader=no	Advanced options > Disable insertion of InterScan "Received:" header when processing messages	SMTP > configuration > Disable insertion of InterScan "Received:" header when processing messages
InterScan Service port	[EMail-Scan] InterScanSMTPServicePort=25	[EMail-Scan] InterScanSMTPServicePort=25	Advanced options > service port	SMTP > configuration > Main service port
Use DNS to send inbound mail or not	[EMail-Scan] InboundUseDNS=yes	[EMail-Scan] InboundUseDNS=yes	SMTP configuration > Use DNS to deliver mail	SMTP > configuration > InboundMail >Use DNS to deliver mail
Use DNS to send outbound mail or not	[EMail-Scan] OutboundUseDNS=yes	[EMail-Scan] OutboundUseDNS=yes	SMTP configuration > Outbound Mail options > Use DNS to deliver mail	SMTP > configuration > OutboundMail >Use DNS to deliver mail
Forward inbound message to this SMTP server if not use DNS to send inbound message	[EMail-Scan] EOrg=	[EMail-Scan] EOrg=	SMTP configuration > Forward mail to SMTP server at	SMTP > configuration > InboundMail >Forward mail to SMTP server at
Forward inbound message to this SMTP port if not use DNS to send inbound message	[EMail-Scan] EOrgPort=25	[EMail-Scan] EOrgPort=25	SMTP configuration > Forward mail to SMTP server at	SMTP > configuration > InboundMail >Forward mail to SMTP server at
Notification server IP, default means use DNS to send notifications	[EMail-Scan] NotificationSMTPAddr=default	EMail-Scan] NotificationSMTPAddr=default	Advanced Configuration > SMTP server	Administration > notification settings > SMTP server

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Notification server port.	[EMail-Scan] NotificationSMTP Port=25	[EMail-Scan] NotificationSMTP Port=25	Advanced Configuration > at port:	Administration > notification settings > port
Enable outbound mail processing	[EMail-Scan] OutboundMailScan=yes	[EMail-Scan] OutboundMailScan=yes	SMTP configuration > Outbound Mail options > Enable outbound mail processing	NONE
Enable/disable outbound mail scanning	[EMail-Scan] OutboundMailVirusScan=yes	[EMail-Scan] OutboundMailVirusScan=yes	SMTP configuration > Outbound Mail options > Enable outbound mail virus scanning	NONE
Outbound Client IP	[EMail-Scan] OutboundMailClientIP=	[EMail-Scan] OutboundMailClientIP=	SMTP configuration > Outbound Mail options > Specify the IP address(es) of any SMTP server that will send outgoing mail to the InterScan server (separate with commas). If this includes the InterScan server, include 127.0.0.1 and the IP address of your local host:	SMTP > configuration> Specify the IP address(es) of any SMTP server that will send outgoing mail to the InterScan server (separate with commas). If this includes the InterScan server, include 127.0.0.1 and the IP address of your local host:

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Forward Outbound message to this SMTP server if not use DNS to send Outbound message	[EMail-Scan] OutboundMailSMTPAddr=	[EMail-Scan] OutboundMailSMTPAddr=	SMTP configuration > Outbound Mail options > Forward mail to SMTP server at:	SMTP > configuration > Outbound Mail > Forward mail to SMTP server at:
Forward Outbound message to this SMTP port if not use DNS to send Outbound message	[EMail-Scan] OutboundMailSMTPPort=25	[EMail-Scan] OutboundMailSMTPPort=25	SMTP configuration > Outbound Mail options > Forward mail to SMTP server at:	SMTP > configuration > Outbound Mail > Forward mail to SMTP server at:
If infectedOutboundmsg is hold, whom to notify?	[EMail-Scan] HoldInfectedOutboundMsgsNotify= ADMINISTRATOR SENDER RECEIVER	[EMail-Scan] HoldInfectedOutboundMsgsNotify= ADMINISTRATOR SENDER RECEIVER	SMTP configuration > Outbound Mail options > send notification message to (when infected outbound message is detected)	not available in UI
Hold infectedOutboundmsg or not	[EMail-Scan] HoldInfectedOutboundMsgs=no	[EMail-Scan] HoldInfectedOutboundMsgs=no	SMTP configuration > Outbound Mail options > stop delivery of infected outbound messages	not available in UI
If use DNS to send mail, the max delivery hours	[EMail-Scan] DeliveryMaxHours=24	[EMail-Scan] DeliveryMaxHours=24	Advanced options > When DNS delivery is used, attempt to send message every minutes for a maximum of hours before bouncing the message.	SMTP > configuration >When DNS delivery is used, attempt to send message every minutes for a maximum of hours before bouncing the message.

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
If use DNS to send mail, the retry minutes	[EMail-Scan] DeliveryRetryMinutes=15	[EMail-Scan] DeliveryRetryMinutes=15	Advanced options > When DNS delivery is used, attempt to send message every minutes for a maximum of hours before bouncing the message.	SMTP > configuration >When DNS delivery is used, attempt to send message every minutes for a maximum of hours before bouncing the message.
ScanLevel added value IntelliScan	[EMail-Scan] Level=ScanAll	[EMail-Scan] Incoming: Level=ScanAll Outgoing: OutgoingLevel=ScanAll	SMTP configuration > scan	SMTP > scanning >Incoming (or Outgoing) > target > Files to Scan
If level is set to scan extensions, which extension will scan (7.0 has a default scan list)	[EMail-Scan] ScanExtensions=exe,bin	[EMail-Scan] Incoming: ScanExtensions=exe,bin Outgoing: OutgoingScanExtensions=exe,bin	SMTP configuration > scan	SMTP > scanning ->Incoming (or Outgoing)> target > Files to Scan
Send notification to administrator or not	[EMail-Scan] EMail=no	[EMail-Scan] EMail=no EnableOutgoingNotiToAdmin=no	SMTP configuration > warning to users	SMTP > scanning ->Incoming (or Outgoing) > notification > administration
Admin notification address	[EMail-Scan] Addr=	[EMail-Scan] Addr=	SMTP configuration > warning to users	administration > notification settings > Email address

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Admin notification content	[EMail-Scan] Message1=Administrator, InterScan has detected virus(es) in users' e-mail attachment.	[EMail-Scan] Message1=Administrator, InterScan has detected virus(es) in users' e-mail attachment. MsgOutgoingNotiToAdmin=Administrator, InterScan has detected virus(es) in users' e-mail attachment.	SMTP configuration > warning to users	SMTP > scanning >Incoming (or Outgoing) > notification > administration
Send notification to recipient or not	[EMail-Scan] EWarning=yes	[EMail-Scan] EWarning=yes EnableOutgoingNotiToRecipient=yes	SMTP configuration > warning to recipient	SMTP > scanning >Incoming (or Outgoing) > notification > recipient
Notification content to recipient	[EMail-Scan] EMessage=Receiver, InterScan has detected virus(es) in the e-mail attachment.	[EMail-Scan] EMessage=Receiver, InterScan has detected virus(es) in the e-mail attachment. MsgOutgoingNotiToRecipient=Receiver, InterScan has detected virus(es) in the e-mail attachment.	SMTP configuration > warning to recipient	SMTP > scanning >Incoming (or Outgoing) > notification > recipient
Send notification to sender or not	[EMail-Scan] EWarningSender=yes	[EMail-Scan] EWarningSender=yes EnableOutgoingNotiToSender=yes	SMTP configuration > warning to sender	SMTP > scanning >Incoming (or Outgoing) > notification > sender

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Notification content to sender	[EMail-Scan] EMessageSender =Sender, InterScan has detected virus(es) in your e-mail attachment.	[EMail-Scan] EMessageSender =Sender, InterScan has detected virus(es) in your e-mail attachment. MsgOutgoingNoti ToSender=Sender , InterScan has detected virus(es) in your e-mail attachment.	SMTP configuration > warning to sender	SMTP > scanning >Incoming (or Outgoing) > notification > sender
Add Virus free message or not	[EMail-Scan] Stamp=no	[EMail-Scan] Stamp=no StampOutGoing= no	SMTP configuration > Safe stamp	SMTP > scanning >Incoming (or Outgoing) > notification > virus free
Virus-Free content to add	[EMail-Scan] StampMessage=	[EMail-Scan] StampMessage= StampMessageOu tGoing=	SMTP configuration > Safe stamp	SMTP > scanning >Incoming (or Outgoing) > notification > virus free
Add virus found message or not	[EMail-Scan] VirusMessage=no	[EMail-Scan] VirusMessage=no VirusMessageOut Going=no	SMTP configuration > Virus Message	SMTP > scanning >Incoming (or Outgoing) > notification > Virus detected
virus found content to add	[EMail-Scan] VirusMessageText =	[EMail-Scan] VirusMessageText = VirusMessageText OutGoing=	SMTP configuration > Virus Message	SMTP > scanning >Incoming (or Outgoing) > notification > Virus detected

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Action of virus	[EMail-Scan] Action=autoclean	[EMail-Scan] Incoming: Action=autoclean Outgoing: OutgoingAction=autoclean	SMTP configuration > Action on viruses	SMTP > scanning >Incoming (or Outgoing) > Action on Infected Files
Send cleaned file to whom	[EMail-Scan] CleanedFileDestination=RECIPIENT	[EMail-Scan] CleanedFileDestination=RECIPIENT	SMTP configuration > Auto clean > option	Not available in UI
Action on uncleaned file	[EMail-Scan] UnCleanedFileRecipientAction=Delete	[EMail-Scan] Incoming: UnCleanedFileRecipientAction=Delete Outgoing: OutgoingUnCleanedFileRecipientAction=Delete	SMTP configuration > Auto clean > option	SMTP > scanning >Incoming (or Outgoing) > If cannot be cleaned, specify an action
Max inbound email size	[EMail-Scan] InESMTPSIZE=0	[EMail-Scan] InESMTPSIZE=0	Advanced options > Maximum inbound message size (0 = unlimited): kilobytes	SMTP > Configuration > Maximum inbound message size (0 = unlimited): kilobytes
max outbound email size	[EMail-Scan] OutESMTPSIZE=0	[EMail-Scan] OutESMTPSIZE=0	Advanced options > Maximum outbound message size (0 = unlimited): kilobytes	SMTP > Configuration > Maximum outbound message size (0 = unlimited): kilobytes

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Check mime header or not	[EMail-Scan] MimeHeaderCheck=no	[EMail-Scan] MimeHeaderCheck=no	Advanced options > Treat MIME attachment whose name is larger than # characters as virus	Not available in UI
If check mime header, max mime header size	[EMail-Scan] MimeHeaderSize=200	[EMail-Scan] MimeHeaderSize=200	Advanced options > Treat MIME attachment whose name is larger than # characters as virus	not available in UI
Restrain inbound domain or not	[EMail-Scan] RestrictInDomain=no	[EMail-Scan] RestrictInDomain=no	Advanced Options > Accept inbound mail addressed only to the following domains (prevents relaying):	SMTP > configuration > Accept inbound mail addressed only to the following domains (prevents relaying):
Inbound domain list	[EMail-Scan] RestrictInDomainList=	[EMail-Scan] RestrictInDomainList=	Advanced Options > Accept inbound mail addressed only to the following domains (prevents relaying):	SMTP > configuration > Accept inbound mail addressed only to the following domains (prevents relaying):

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Quarantine Microsoft Office macros or not	[EMail-Scan] QuarantineOffice Macros=yes	[EMail-Scan] QuarantineOffice Macros=yes	Advanced Options > Quarantine Microsoft Office attachments containing macros	SMTP > Scanning >Incoming (or Outgoing) > Quarantine Microsoft Office attachments containing macros
Greeting message	[EMail-Scan] Greeting=	[EMail-Scan] Greeting=	NONE	SMTP > configuration > Send a greeting message when connection gets established.
MaxDecompress Layer	[EMail-Scan] DecompressionLayerLimit=14	[EMail-Scan] DecompressionLayerLimit=14	NONE	SMTP > scanning >Incoming (or Outgoing) > Target > Do not scan compressed file if Number of layers of compression exceeds:
MaxDecompress Size	[EMail-Scan] ExtractFileSizeLimit=	[EMail-Scan] ExtractFileSizeLimit=1073741824	NONE	SMTP > scanning >Incoming (or Outgoing) > Target > Do not scan compressed file if Extracted file size exceeds:

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Enable greetingmsg or not	[EMail-Scan] EnableGreeting=yes	[EMail-Scan] EnableGreeting=yes	NONE	SMTP > configuration > Send a greeting message when connection gets established.
Set smtp whole file scan action as delete	[Email-Scan] WholeMailScanAction	[Email-Scan] WholeMailScanAction	Cannot configure from Web console.	
Enable/Disable the smtp-incoming whole file scan feature	[Email-Scan] InboundWholeMailVirusScan	[Email-Scan] InboundWholeMailVirusScan	Cannot configure from Web console.	
Send or not send notification to administrator when detect virus in smtp-incoming	[Email-Scan] Email	[Email-Scan] Email	Cannot configure from Web console.	
The body of notification sent to administrator	[Email-Scan] Message1	[Email-Scan] Message1	Cannot configure from Web console.	
Send or not send notification to recipient when detect virus in smtp-incoming	[Email-Scan] Ewarning	[Email-Scan] Ewarning	Cannot configure from Web console.	
The body of notification sent to recipient	[Email-Scan] Emessage	[Email-Scan] Emessage	Cannot configure from Web console.	
Send or not send notification to sender when detect virus in smtp-incoming	[Email-Scan] EWarningSender	[Email-Scan] EWarningSender	Cannot configure from Web console.	

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
The body of notification sent to sender	[Email-Scan] EMessageSender	[Email-Scan] EMessageSender	Cannot configure from Web console.	
Enable/Disable the smtp-outgoing whole file scan feature	[Email-Scan] OutboundWholeMailVirusScan	[Email-Scan] OutboundWholeMailVirusScan	Cannot configure from Web console.	
Send or not send notification to administrator when detect virus in smtp-outgoing	[Email-Scan] EnableOutgoingNotiToAdmin	[Email-Scan] EnableOutgoingNotiToAdmin	Cannot configure from Web console.	
The body of notification sent to administrator	[Email-Scan] MsgOutgoingNotiToAdmin	[Email-Scan] MsgOutgoingNotiToAdmin	Cannot configure from Web console.	
Send or not send notification to recipient when detect virus in smtp-outgoing	[Email-Scan] EnableOutgoingNotiToRecipient	[Email-Scan] EnableOutgoingNotiToRecipient	Cannot configure from Web console.	
The body of notification sent to recipient	[Email-Scan] MsgOutgoingNotiToRecipient	[Email-Scan] MsgOutgoingNotiToRecipient	Cannot configure from Web console.	
Send or not send notification to sender when detect virus in smtp-outgoing	[Email-Scan] EnableOutgoingNotiToSender	[Email-Scan] EnableOutgoingNotiToSender	Cannot configure from Web console.	
The body of notification sent to sender	[Email-Scan] MsgOutgoingNotiToSender	[Email-Scan] MsgOutgoingNotiToSender	Cannot configure from Web console.	

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Enable mail queuing or not	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail\Enable	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\BlockingMail\Enable	SMTP configuration > Queue email	SMTP > configuration > Enable mail queuing
Enable mail queuing for inbound mail	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail\Inbound	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall 7.0\BlockingMail\Inbound	SMTP configuration > Queue email	SMTP > configuration > Enable mail queuing > for inbound mail
Enable mail queuing for outbound mail	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail\Outbound	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\BlockingMail\Outbound	SMTP configuration > Queue email	SMTP > configuration > Enable mail queuing > for outbound mail
Add outbound disclaimer to outbound message or not	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion\InsertMessageOn	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\CurrentVersion\InsertMessageOn	SMTP configuration > outbound mail options > Add customized text to every outbound message at	NONE
Content added to outbound message	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion\InsertMessage	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\CurrentVersion\InsertMessage	SMTP configuration > outbound mail options > Add customized text to every outbound message at	NONE

TABLE C-2. Detailed SMTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Add disclaimer at top	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion\InsertMessageAtTop	Registry: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\CurrentVersion\InsertMessageAtTop	SMTP configuration > outbound mail options > Add customized text to every outbound message at	NONE

FTP Migration

FTP Migration Summary

FTP virus scanning and configuration migrates from ISVW 3.55 to ISVW 7.0 with conditions outlined in *Table C-3*.:

TABLE C-3. FTP Migration Conditions

Item	Description
Enable Virus Scanning	This feature migrates to Enable FTP Scanning and Enable FTP anti-spyware in ISVW 7.0. If Virus Scanning is on in ISVW 3.55, both FTP scanning and FTP anti-spyware will be enabled after migration. If Virus Scanning is **off** in ISVW 3.55, both FTP scanning and FTP anti-spyware will not be enabled after migration.
FTP Proxy settings	This feature migrates to FTP Configuration Settings in ISVW 7.0.
FTP Configuration > Options	This feature migrates to FTP Advanced Configuration.
FTP Configuration > Scan	This feature migrates to FTP > Scanning > Target > Files to Scan. Also in ISVW 7.0, the IntelliScan option has been added in the UI.
FTP notification SMTP server settings	This feature does NOT migrate to ISVW 7.0 because the configuration entries have been changed.
Warning to user(s) and Virus Message	This feature migrates to FTP > Scanning > Notification > Administrator Notification and User Notification.
Action on Viruses	This feature migrates to FTP > Scanning > Action. The Move action has changed to Quarantine, and the Delete action has changed to Block.

FTP Migration Table

Table C-4 provides detailed information about the FTP migration from ISVW 3.55 to ISVW 7.0.

TABLE C-4. Detailed FTP Migration

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Enable FTP Scan	[Scan-Configuration] FTPScan=yes	[Scan-Configuration] FTPScan=yes	FTP Configuration > Enable Virus Scanning	FTP > Scanning > Enable FTP Scanning FTP > Anti-spyware > Enable FTP anti-spyware
Maximum connection	[FTP-Scan] MaxThreads=500	[FTP-Scan] MaxThreads=500	FTP Configuration > Maximum concurrent connections	FTP > Configuration > Maximum connections
InterScan FTP service port	[FTP-Scan] InterScanFTPServicePort=21	[FTP-Scan] InterScanFTPServicePort=21	NONE	FTP > Configuration > FTP service port
InterScan FTP service IP	[FTP-Scan] InterScanFTPServiceIP=	[FTP-Scan] InterScanFTPServiceIP=	NONE	NONE
Dependant mode	[FTP-Scan] UseFTPProxy=yes	[FTP-Scan] UseFTPProxy=yes	FTP Configuration > Use FTP proxy radio box	FTP > Configuration > Use FTP proxy radio box
Original FTP proxy server IP address	[FTP-Scan] FOrg=192.168.5.20	[FTP-Scan] FOrg=192.168.5.20	FTP Configuration > Use FTP proxy edit box	FTP > Configuration > Use FTP proxy edit box

TABLE C-4. Detailed FTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Original FTP proxy server port	[FTP-Scan] FOrgPort=2121	[FTP-Scan] FOrgPort=2121	FTP Configuration > Use FTP proxy > Port	FTP > Configuration > Use FTP proxy > Port
Use force passive mode	[FTP-Scan] ForcePassiveFTP=yes	[FTP-Scan] ForcePassiveFTP=yes	FTP Configuration > Use PASSIVE FTP for all file transfers	FTP > Configuration > Use passive FTP for all file transfers
Scan level: ScanAll, IntelliScan, ScanExt	[FTP-Scan] Level=IntelliScan	[FTP-Scan] Level=IntelliScan	FTP Configuration > Scan	FTP > Scanning > Target > Files to Scan
Specified extensions to scan when Level=ScanExt	[FTP-Scan] ScanExtensions=	[FTP-Scan] ScanExtensions=	FTP Configuration > Files with the following extensions	FTP > Scanning > Target > Specified file extensions > Additional Extensions
Display user notification on client	[FTP-Scan] VirusMessage=no	[FTP-Scan] VirusMessage=no	FTP Configuration > Virus message checkbox	NONE
Content of user notification	[FTP-Scan] VirusMessageText=	[FTP-Scan] VirusMessageText=	FTP Configuration > Virus message	FTP > Scanning > Notification > User Notification
SMTP server IP address for administrator notification	[FTP-Scan] SMTPServerAddr=	[FTP-Scan] SMTPServerAddr=	FTP Configuration > SMTP server	Administration > Notification Settings > SMTP Server

TABLE C-4. Detailed FTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
SMTP server port for administrator notification	[FTP-Scan] SMTPServerPort=25	[FTP-Scan] SMTPServerPort=25	FTP Configuration > SMTP port	Administration > Notification Settings > Port
Use administrator notification	[FTP-Scan] EMail=no	[FTP-Scan] EMail=no	FTP Configuration > Warning to user(s) checkbox	FTP > Scanning > Notification > Administrator checkbox
Administrator email address	[FTP-Scan] Addr=	[FTP-Scan] Addr=	FTP Configuration > Warning to user(s):	Administration > Notification Settings > Email address
Content of administrator notification	[FTP-Scan] Message1=InterScan has detected virus(es) in user's FTP traffic.	[FTP-Scan] Message1=InterScan has detected virus(es) in user's FTP traffic.	FTP Configuration > Warning to user(s):	FTP > Scanning > Notification > Administrator Notification
Action for detected virus	[FTP-Scan] Action=Delete	[FTP-Scan] Action=Delete	FTP Configuration > Action on Viruses	FTP > Scanning > Action
Trickle amount for trickle feature, unit: byte	[FTP-Scan] TrickleAmount=1024	[FTP-Scan] TrickleAmount=1024	FTP Configuration > Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received	FTP > Configuration > Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received

TABLE C-4. Detailed FTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Trickle period for trickle feature, unit: kilobyte	[FTP-Scan] TricklePeriod=512	[FTP-Scan] TricklePeriod=512	FTP Configuration > Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received	FTP > Configuration > Send (TrickleAmount) bytes of data to client for every (TricklePeriod) kilobytes received
Do not scan compressed file if decompression layer exceeds this limitation	[FTP-Scan] DecompressionLayerLimit=14	[FTP-Scan] DecompressionLayerLimit=14	NONE	FTP > Scanning > Target > Number of layers of compression exceeds
Do not scan compressed file if extract file size exceeds this limitation, unit: byte	[FTP-Scan] ExtractFileSizeLimit=1073741824	[FTP-Scan] ExtractFileSizeLimit=1073741824	NONE	FTP > Scanning > Target > Extracted file size exceeds

HTTP Migration

HTTP Migration Summary

HTTP settings in ISVW 3.55 migrate to ISVW 7.0 with conditions outlined in *Table C-5*.

TABLE C-5. HTTP Migration Conditions

Item	Description
Enable HTTP traffic scan	This setting migrates.

TABLE C-5. HTTP Migration Conditions (Continued)

Item	Description
Scanning service listening port	This setting migrates.
Dependent mode settings	If in dependent mode, this setting migrates the dependent's proxy IP address and port number.
Record HTTP requests setting	This setting migrates.
Compressed file settings	This setting migrates.
HTTP traffic scanning settings	This setting migrates.
Virus notification message content	This content migrates.
Infected files settings	This setting migrates.
MIME type settings	The MIME types exception list migrates.
HTTP connection timeout boundary setting	This setting migrates.
HTTP Trickle	This setting migrates

HTTP Migration Table

Table C-6 provides detailed information about the HTTP migration from ISVW 3.55 to ISVW 7.0.

TABLE C-6. Detailed HTTP Migration

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Enable HTTP module	[Scan-Configuration] HttpScan=yes	HTTP/Plugin/ScanVsapi/plug-in/enabled=yes/no	HTTP Scan Configuration > Enable Virus Scanning	HTTP Scanning > Enabled /Disabled
HTTP virus wall listening port	[HTTP-Scan] InterScanHTTPServicePort=8080	HTTP/Protocol/HttpProxy/main/port=number	InterScan Port	HTTP > Configuration > HTTP Listening Port

TABLE C-6. Detailed HTTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Dependent mode HTTP proxy IP address or host name	[HTTP-Scan] HOrg=host name or IP	HTTP/Protocol/HttpProxy/http/original_server=host name or ip	HTTP Proxy	HTTP > Configuration > Proxy
Dependent mode HTTP proxy IP address or host name	HTTP-Scan HOrgPort= port number	HTTP/Protocol/HttpProxy/http/original_server_port=number	Http Port	HTTP > Configuration > Proxy port
Log HTTP client requests	[HTTP-Scan] LogRequests=yes/no	HTTP/Main/internet-access-monitoring/enable=yes/no	Log HTTP client requests	HTTP > Configuration > Log HTTP requests
Define what files to scan	[HTTP-Scan] Level=scanall/scanext	HTTP/Plugin/ScanVsapi/http/level=scanall/scanext/scanintelli	Files to Scan	HTTP Scanning > Default Scanning Select a method
Scanning according file extension	[HTTP-Scan] ScanExtensions=string, Extension list	HTTP/Plugin/ScanVsapi/http/extensions=string, Extension list	Scan all files with the following extensions	HTTP Scanning > Specified file extensions
Notification message content	[HTTP-Scan] VirusMessageText=message	HTTP/Main/http/virus-notification=string	Notification: Virus Message Textbox	HTTP Scanning > Notification > User Notification
Uncleanable file, second action	[HTTP-Scan] Action=pass/move/delete/cleanpass/cleanmove/cleandelete	HTTP/Main/http/action, HTTP/Main/http/ucaction=clean/pass/move/delete	Action on Virus/HTTP Auto Clean Option > Action on Uncleanable File(s):	HTTP Scanning > Action

TABLE C-6. Detailed HTTP Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Define MIME type not to scan	[HTTP-Scan] MIMEBypassing=yes/no	HTTP/Main/http/skiptype=MIME type list, separated by semicolon	MIME Configuration > Do not scan the following MIME types checkbox	HTTP Scanning > MIME Type Exceptions
Define what MIME type should not be scanned	[HTTP-Scan] MIMEBypassingTypes=string, MIME type list, separated by comma		MIME Configuration > Do not scan the following MIME types listbox	
How to handle compressed file, layer limit	[HTTP-Scan] DecompressionLayerLimit=number	HTTP/Plugin/ScanVsapi/http/decompress_layer_limit=number		HTTP Scanning -> Number of layers of compression exceeds:
HTTP trickle settings	[HTTP-Scan] TrickleAmount=1024 TricklePeriod=512	HTTP/Main/Scan/trickle_max_size=1024 HTTP/Main/Scan/trickle_rate=512	HTTP Configuration > Options > Send 1024 bytes of data to client for every 512 kilobytes received	HTTP > Scanning > Target > Large File Handling > Deferred Scan

ActiveUpdate Migration

ActiveUpdate Migration Summary

ActiveUpdate settings in ISVW 3.55 migrate to ISVW 7.0 with conditions outlined in *Table C-7*.

TABLE C-7. ActiveUpdate Migration Conditions

Item	Description
Scheduled update settings	This setting migrates the time updates should occur.
Proxy settings	If you update through a proxy server, the proxy server information migrates.

Active Update Migration Table

Table C-8 provides detailed information about the ActiveUpdate migration from ISVW 3.55 to ISVW 7.0.

TABLE C-8. Detailed ActiveUpdate Migration

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
Method	[Active-Update] Method	Common\ ActiveUpdate\ ScheduleUpdate\ VirusUpdate\ EnableUpdate	Update	Update > Scheduled update
Frequency	[Active-Update] Frequency	Common\ ActiveUpdate\ ScheduleUpdate\ VirusUpdate\ Type	Update	Update > Scheduled Update
Hour, APM	[Active-Update] Hours	Common\ ActiveUpdate\ ScheduleUpdate\ VirusUpdate\ Hours	Update	Update > Scheduled Update

TABLE C-8. Detailed ActiveUpdate Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
DayOfMonth	[Active-Update] DayOfMonth	Common\ ActiveUpdate\ ScheduleUpdate\ VirusUpdate\ Days	Update	Update > Scheduled Update
DayOfWeek1	[Active-Update] DayOfWeek		Update	Update > Scheduled Update
UseProxyServer	[Active-Update] UseProxyServer	Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ UseProxy	Update	Update > Scheduled Update
UseSocks4Proxy	[Active-Update] UseSocks4Proxy	Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ IsSocksProxy	Update	Update > Scheduled Update
HTTPProxy	[Active-Update] HTTPProxy	Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ Proxy	Update	Update > Scheduled Update
HTTPPort	[Active-Update] HTTPPort	Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ ProxyPort	Update	Update > Scheduled Update

TABLE C-8. Detailed ActiveUpdate Migration (Continued)

Item	intscan.ini Location		UI Location	
	ISVW 3.55	ISVW 7.0	ISVW 3.55	ISVW 7.0
HTTPAuthorization	[Active-Update] HTTPAuthorization	Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ ProxyUsernam e Common\ ActiveUpdate\ UpdateItems\ UpdateServers\ Server.i\ ProxyPassword	Update	Update > Scheduled Update
UpdateEngine and UpdatePattern	[Active-Update] UpdateEngine= yes UpdatePattern= yes	Common\ ActiveUpdate\ ScheduleUpdat e\ VirusUpdate\ EnableItems	Update	Update > Scheduled Update

eManager Migration

eManager Migration Summary

Content and attachment filter features and settings migrate from eManager 3.52 to ISVW 7.0 with conditions outlined in *Table C-9*.

TABLE C-9. eManager Migration Conditions

Item	Description
Content Filter	
Content filter policies	All content filter policies in eManager 3.52 migrate to the keyword filter in ISVW 7.0.
"Archive" action	The action "Archive" in the content filter has been replaced with "Quarantine" in the ISVW 7.0 keyword filter.
"Enable scanning the content of attachment files"	The content filter global setting "Enable scanning the content of attachment files" migrates to the keyword filter in ISVW 7.0.
"Use exact matches only"	The content filter global setting "Use exact matches only" migrates to the keyword filters in ISVW 7.0.
"Case sensitive comparisons"	The content filter global setting "Case sensitive comparisons" migrates to the keyword filter in ISVW 7.0.
Attachment filter	
Attachment filter rules	All the attachment filter rules in eManager 3.52 migrate to the attachment filter in ISVW 7.0.
"RemoveAttachment"	The attachment filter global option "RemoveAttachment" in eManager 3.52 migrates to the attachment filter in ISVW 7.0.
"Make copies of original messages in quarantine directory"	This feature does NOT migrate.
Notification	
Content and attachment filter notification settings	All the content and attachment filter notification settings in eManager 3.52 migrate to the keyword and attachment filter in ISVW 7.0.
Notification name"	This setting does NOT migrate.
Notification	
"Admin list"	This setting does NOT migrate.
"From address"	This setting does NOT migrate.
"Show message text"	This setting does NOT migrate.

Key Config File Values

TABLE C-10. eManager Feature vs. ISVW Feature Comparison

Item	ISVW 3.55				ISVW 7		
Global setting	<install_path>\Content Management\contscan.ini				Config.xml		
	[Content Filter]				Keyword Filter (RuleType = 1), set in every filter property		
	CaseSensitive	no			CaseSensitive (in each filter)		0
		yes					1
	ExactMatch	no			Keyword (in each filter)		For Example, “.REG. “testKeyword””
		yes					For Example, “testKeyword”
	EnableAttachScan	no			FilterScope		Not | 0x60 (not “OR” operator “0x60” operand)
		yes					| 0x60 (“OR” operator “0x60” operand)
	[Specialized Filter]				Attachment Filter (RuleType = 2), set in every filter property		
	RemoveAttachment	no	Check every attachment policy rule enable property	yes	EnableRule	Result is decided by the two value “AND” operator result.	<Value Name="EnableRule" string="" type="int" int="0" />
				no			<Value Name="EnableRule" string="" type="int" int="0" />
		yes		yes			<Value Name="EnableRule" string="" type="int" int="1" />
				no			<Value Name="EnableRule" string="" type="int" int="0" />
	Quarantine	no			Action,		<Value Name="Action" string="Remove" type="string" int="0" />
		Yes					
Content filter	<install_path>\Content Management\Csconfig.dat				Config.xml		
Attachment filter	<install_path>\Content Management\spamrule\SFRule.txt				Config.xml		
Notification	<install_path>\Content Management\spamrule\notifyrule.txt				Config.xml		

TABLE C-11. Content Filter

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Policy header	RuleName	Copies the value	
	RuleType		1- Means keyword filter type
Action	Action	Delete	Delete
		Archive	Quarantine
		Quarantine	Quarantine
Inbound mail scan	InBound	Yes	1
		No	0
Outbound mail scan	OutBound	Yes	2
		No	0
Inbound notify	InBoundNotify	Copies the value	
Outbound notify	OutBoundNotify	Copies the value	
Syn enable	EnableSynonyms	Yes	1
		No	0
Policy enable	EnableRule	Yes	1
		No	0
(Hidden attribute from global setting)	CaseSensitive	Yes	1
		No	0
(Hidden attribute from global setting)	ExactMatch	Yes	1
		No	0
Import file	File name		Add the keyword in the file to the related keyword filter in ISVW 7.0.
Word head_	One Keyword Filter	<word head_0>…</word head_0>	<key Name=" KeywordFilter"> <key Name="word head_0"> … <key> </key>

TABLE C-11. Content Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW (Continued)7.0
Word_	One keyword of a content filter If 3.55 has more than one word, we should use .AND. to connect them	<word head_0> <word_0>test</word_0> <word_1>test1</word_1> </word head_0>	<key Name=" KeywordFilter"> <key Name="word head_0"> <Value Name="KeyWord" string="test,test1" type="string" int="0" /> <Value Name= "IncludeSyn" string="" type="string" int="0" /> <Value Name= "CaseSensitive" string="" type="int" int="0" /> <Value Name= "ExactMatch" string="" type="int" int="0" /> </key> <key>
Syn in_	One synonym for one keyword If 3.55 has more than one “syn in_”, we should use \t( ) to separate them	<word head_0> <word_0>test</word_0> <syn in_0_0>trial</syn in_0_0> <syn in_0_1>tryout</syn in_0_1> </word head_0>	<Key Name= "KeywordFilter"> <Key Name="word head_0"> <Value Name ="KeyWord" string="test" type="string" int="0" /> <Value Name= "IncludeSyn" string="trial tryout " type="string" int="0" /> <ValueName= "CaseSensitive" string="" type="int" int="0" /> <Value Name= "ExactMatch" string="" type="int" int="0" /> </key> </key>

TABLE C-11. Content Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW (Continued)7.0
Syn ex_	One excluded synonym for one keyword If 3.55 has more than one "syn ex_", we should use \t( ) to separate them	<word head_0> <word_0>test</word_0> <syn ex_0_0>trial</syn ex_0_0> <syn ex_0_1>tryout</syn ex_0_1> </word head_0>	Does not migrate
Exclusive word_	Keyword	<word head_0> <exclusive word_0>ex_1</exclusive word_0> <exclusive word_0>ex_2</exclusive word_0> </word head_0>	<Key Name="ExceptionFilter"> <Value Name="Trigger" string="" type="int" int="0" /> <Key Name="Exception">> <Value Name="KeyWord" string="ex_1" type="string" int="0" /> <Value Name="KeyWord" string="ex_2" type="string" int="0" /> </Key> </key>

TABLE C-12. Attachment Filter

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
ENABLE	EnableRule	Yes	1
		No	0
RULE NAME	RuleName	Copy the value	
	RuleType		2 – Means attachment type
Action	Action	Remove(Default value)	Remove
			Quarantine
			Delete
MAIL TYPE	InBound, OutBound	A	A(InBound=1,OutBound=0)
		B	B(InBound=0,OutBound=2)
		C	C(InBound=1,OutBound=2)

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
AttachmentFilter Condition Description		In the eManager 3.52 configuration file, there are four conditions to enable/disable the rule	In ISVW 7.0, there are four content filters inside the attachment filter, which decide if the attachment will be enabled or disabled
<ATTR><NAME>INCLUDE</NAME></ATTR>	INCLUDE, EXCLUDE	INCLUDE	Trigger: INCLUDE : 1
		EXCLUDE	EXCLUDE : 0

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Condition1 From address	Name Case sensitive Exact match	<FROM> <NAME>jing_gao@isvw.com</NAME> <I>yes</I> <S>yes</S> </FROM>	Compose one content filter inside the filter <keyname= ”AttachmentFilenameFilter”> <Value Name="FilterType" string=" "type="int" int="1" /> <ValueName= "AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="From"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <ValueName= "FilterScope" string="" type="int" int="4" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name= "CaseSensitive" string="" type="int" int="1" /> <Value Name= "ExactMatch" string="" type="int" int="1" /> </Key> …

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Condition2 To address	Name Case sensitive Exact match	<TO> <NAME>jing_gao@isvw.com</NAME> <I>yes</I> <S>yes</S> </TO>	Compose one content filter inside the filter <Key Name= "AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name= "AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="To"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name= "FilterScope" string="" type="int" int="8" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name= "CaseSensitive" string="" type="int" int="1" /> <Value Name= "ExactMatch" string="" type="int" int="1" /> </Key> …

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Condition3 ReplyTo address	Name Case sensitive Exact match	<RTO> <NAME>jing_gao@isvw.com</NAME> <I>yes</I> <S>yes</S> </RTO>	Compose one content filter inside the filter <Key Name= "AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name= "AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters">\ <Key Name="Others">\ <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name= "FilterScope" string="" type="int" int="128" /> <Key Name="word head_0">\ <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name= "CaseSensitive" string="" type="int" int="1" /> <Value Name= "ExactMatch" string="" type="int" int="1" /> </Key> ...

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Condition4 CC address	Name Case sensitive Exact match	<CC> <NAME>jing_gao@isvw.com</NAME> <I>yes</I> <S>yes</S> </CC>	Compose one content filter inside the filter <Key Name= "AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name= "AttachType" string="" type="int" int="1" /> <Value Name="AttachExp" string="*.txt" type="string" int="0" /> <Key Name="Filters"> <Key Name="CC"> <Value Name="FilterType" string="" type="int" int="0" /> <Value Name="Trigger" string="" type="int" int="1" /> <Value Name= "FilterScope" string="" type="int" int="16" /> <Key Name="word head_0"> <Value Name="KeyWord" string=" jing_gao@isvw.com " type="string" int="0" /> <Value Name= "CaseSensitive" string="" type="int" int="1" /> <Value Name= "ExactMatch" string="" type="int" int="1" /> </Key> …

TABLE C-12. Attachment Filter (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Attachment removal MIME option	One Attachment Filter	<MIME><NAME>text/plain</NAME></MIME>	<Key Name= "AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name= "AttachType" string="" type="int" int="2" /> <Value Name="AttachExp" string="text/plain" type="string" int="0" /> </Key>
Attachment removal True file types	One Attachment Filter	<ATTACH><NAME>exe</NAME></ATTACH>	<Key Name= "AttachmentFilenameFilter"> <Value Name="FilterType" string="" type="int" int="1" /> <Value Name="AttachType" string="" type="int" int="2" /> <Value Name="AttachExp" string="exe;txt" type="string" int="0" /> </Key>
IN NOTIFY	InBoundNotify	Copies the value	
OUT NOTIFY	OutBoundNotify	Copies the value	

TABLE C-13. Notifications

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Administrator-----<msg_op admin>…. </msg_op admin> Sender -----<msg_op sender>…. </msg_op sender> Recipient -----<msg_op receiver>…. </msg_op receiver>			

TABLE C-13. Notifications (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Enable/disable notification	Enable/disable notification	<send msg>yes</send msg>	<key name= ”administrator”> <value name=”enable” string=”” type=”int” int=”1”/> … </key>
		<send msg>no</send msg>	<key name= ”administrator”> <value name=”enable” string=”” type=”int” int=”0”/> … </key>
Headline	Body	<show head line>yes</show head line> <head line>Mybody</head line> (if show head line value is yes, migrate the value, else not)	<key name= ”administrator”> <value name=”Body” string=”Mybody” type=”string” int=”0”/> … </key>
Subject	Subject	<subject name>Mysubject</subject name>	<key name= ”administrator”> <value name=”Subject” string=”Mysubject” type=”string” int=”0”/> … </key>
Show source address	ShowFrom	<show source addr>yes</show source addr>	<key name= ”administrator”> <value name=”ShowFrom” string=”” type=”int” int=”1”/> … </key>
		<show source addr>no</show source addr>	<key name= ”administrator”> <value name=”ShowFrom” string=”” type=”int” int=”0”/> … </key>

TABLE C-13. Notifications (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
Show dest address	ShowTo	<show dest addr>yes</show dest addr>	<key name= ”administrator”> <value name=”ShowTo” string=”” type=”int” int=”1”/> … </key>
		<show dest addr>no</show dest addr>	<key name= ”administrator”> <value name=”ShowTo” string=”” type=”int” int=”0”/> … </key>
Show policy	ShowPolicy	<show policy>yes</show policy>	<key name= ”administrator”> <value name= ”ShowPolicy” string=”” type=”int” int=”1”/> … </key>
		<show policy>no</show policy>	<key name =”administrator”> <value name= ”ShowPolicy” string=”” type=”int” int=”0”/> … </key>
Show action	ShowAction	<show action>yes</show action>	<key name =”administrator”> <value name= ”ShowAction” string=”” type=”int” int=”1”/> … </key>
		<show action>no</show action>	<key name= ”administrator”> <value name= ”ShowAction” string=”” type=”int” int=”0”/> … </key>

TABLE C-13. Notifications (Continued)

eManager 3.52	ISVW 7.0	eManager 3.52 Value	ISVW 7.0 Value
	ToUserType	<msg_op admin></msg_op admin>	0
		<msg_op sender></msg_op sender>	1
		<msg_op receiver></msg_op receiver>	2
Notify type	NotifyType	<notify type>none</notify type>	0
		<notify type>header</notify type>	1
		<notify type>all</notify type>	2
		<notify type>all text</notify type>	3

Notes for eManager 3.52 Migration

1. The content filter action "Archive" in eManager 3.52 is replaced with “Quarantine” in the keyword filter for ISVW 7.0.
2. When the attachment filter global action “Quarantine” in eManager 3.52 is set, migration ignores the setting and takes the “Remove attachment” action in ISVW 7.0.
3. Migration rule: The global setings for the content and attachment filter in eManager 3.52 will all be applied to every rule in ISVW 7.0, not for all keyword filter or attachment filter global settings.
   - **CaseSensitive:** Content filter global option in eManager 3.52 applied to every keyword filter. See Table C-10 on page C-31 for more information.
   - **ExactMatch:** Content filter global option in eManager 3.52 applied to every keyword filter. See Table C-10 on page C-31 for more information.
   - **EnableAttachScan:** Content filter global option in eManager 3.52 applied to every keyword filter. See Table C-10 on page C-31 for more information.
   - **RemoveAttachment:** Attachment filter global option in eManager 3.52 applied to every attachment filter. See Table C-10 on page C-31 for more information.

- **Quarantine:** Attachment filter global option in eManager 3.52 that will not be applied into every attachment filter. See Table C-10 on page C-31 for more information.
- **Admin Lists:** In each notification setting, the admin list will not be migrated because ISVW 7.0 has only one admin setting.

Appendix D

Migration from InterScan VirusWall 5.0

Use this appendix as a reference when migrating settings from InterScan VirusWall (ISVW) 5.0 to ISVW 7.0.

The following are the topics in this appendix:

SMTP Migration

SMTP Migration Summary

ISVW 7.0 migrates most SMTP settings from ISVW 5.0. SMTP settings migrate from ISVW 5.0 to ISVW 7.0 with conditions outlined in *Table D-1*.

TABLE D-1. Items Migrated from ISVW 5.0 to ISVW 7.0

Item	Description
Scan inbound messages	This item migrates. If this value is set to 0, after migration, all inbound / outbound messages will not be scanned for viruses.
Scan outbound messages	This item migrates. If this value is set to 0, after migration, all inbound / outbound messages will not be scanned for viruses.
Scan Extensions	ISVW 7.0 has a default scan list. After migration, the scan extension list is as follows: 7.0 defaultlist+5.0 ScanExtensions.
SMTP Anti-spam	This item migrates. If this value is set to 0, after migration all email messages will not be scanned for the following: spam (content scanning)
SMTP content filter	This item migrates. If this value is set to 0, after migration, all rules with a value that is set to 0 will not be enabled.

SMTP Migration Table

Table D-2 provides detailed information about the SMTP migration from ISVW 5.0 to ISVW 7.0.

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	Registry	Registry		
Enables/disables mail queuing	"HLM\SOFTWARE\TrendMicro\ISNT5\SMTPSvr\BlockingMail\Enable"	"HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\BlockingMail\Enable"	Not supported	"SMTP Configuration ->Queue Mail-> Enable mail queuing"
Enables/disables mail queuing for inbound or outbound mail	"HLM\SOFTWARE\TrendMicro\ISNT5\SMTPSvr\BlockingMail\Inbound(Outbound)"	"HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\BlockingMail\Inbound(Outbound)"	Not supported	"SMTP Configuration ->Queue Mail-> for Inbound mail /for Outbound mail"
Configure outbound disclaimer content	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\outgoing\tasks\disclaimer\setting\fAnnotation\tok_wtrRichAnnotation"	"HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan VirusWall\CurrentVersion\InsertMessage	SMTP->Configuration->Disclaimer->SMTP Disclaimer Message	SMTP Configuration->Add customized disclaimer text
	Registry	intscan.ini		
Enables SMTP scanning	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\enable = 1/0"	[EMail-scan] Incoming: AntiVirus=yes/no Outgoing: OutgoingAntiVirus =yes/no	SMTP->Virus Scan->Incoming/Outgoing->Target->Enable/Disable	SMTP->Scanning->Incoming (or Outgoing)->Target->Enable SMTP Scanning

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure scan level	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\setting\ScanLevel = 0/1 IntelliScan = 0/1 ScanUserExt = 0/1"	[EMail-Scan] Incoming: Level=ScanAll/ScanExt/IntelliScan Outgoing: OutgoingLevel=ScanAll/ScanExt/IntelliScan	SMTP->Virus Scan->Incoming/Outgoing->Target->File Type	SMTP->Scanning->Incoming (or Outgoing)->Target->Files to Scan
Additional file extension to scan	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\setting\UserExtensions"	[EMail-Scan] Incoming: ScanExtensions=" Outgoing: OutgoingScanExtensions	SMTP->Virus Scan->Incoming/Outgoing->Target->File Type->added extensions	SMTP->Scanning->Incoming (or Outgoing)->Target->Files to Scan->additional file extensions
Scan action	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\setting\DoCleanFailed DoVirusFound"	[EMail-Scan] Incoming: Action=Pass/move/delete/autoclean/blockmsg Outgoing: OutgoingAction=Pass/move/delete/autoclean/blockmsg	SMTP->Virus Scan->Incoming/Outgoing->Action	SMTP->Scanning->Incoming (or Outgoing)->Action

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable notification for incoming and outgoing mail	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in(out)_virus\actions (If enable notification, a corresponding subfolder will be added under this branch.)"	"[EMail-Scan] incoming:Email/Ewarning/EWarningSender outgoing:EnableOutgoingNotiToAdmin/EnableOutgoingNotiToRecipient/EnableOutgoingNotiToSender"	SMTP->VirusScan->Incoming/Outgoing->Notification->enable Email notifications	SMTP->Scanning->Incoming (or Outgoing)->Notification->enable Email Notifications
Enable/disable inline notification for incoming and outgoing mail	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\setting\SafeStamp = 1/0 AddAlert = 1/0"	"[EMail-Scan] incoming:Stamp=yes/no VirusMessage=yes/no outgoing:StampOutGoing=yes/no VirusMessageOutgoing=yes/no"	SMTP->VirusScan->Incoming/Outgoing->Notification->enable Inline notifications	SMTP->Scanning->Incoming (or Outgoing)->Notification->enable Inline Notification Stamp
Configure email notification content	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in(out)_virus\actions\admin(recipient/sender)\setting\content"	"[EMail-Scan] incoming:Message1/Emessage/EMessageSender outgoing:MsgOutgoingNotiAdmin/MsgOutgoingNotiRecipient/MsgOutgoingNotiSender"	SMTP->VirusScan->Incoming/Outgoing->Notification->Email notifications content	SMTP->Scanning->Incoming (or Outgoing)->Notification->Email Notifications content
Configure email inline notification content	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\virus\setting\SafeStampMsg VirusAlert"	"[EMail-Scan] incoming:StampMessage/virusMessageText outgoing:StampMessageOutGoing/VirusMessageTextOutGoing"	SMTP->VirusScan->Incoming/Outgoing->Notification->Inline notifications content	SMTP->Scanning->Incoming (or Outgoing)->Notification->Inline Notification Stamp content

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure domain name of incoming mail	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming\condition#"	Not supported	SMTP->Configuration->Incoming Mail->SMTP Incoming Mail	Not supported
	Registry	config.xml		
Enable/disable keyword synonyms	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\advanced_subject(body)\setting\fLexAnalysis\f_vecExpression\f_exp_###\bEnableSynonym = 1/0	This item does not migrate	Cannot configure from UI	This item does not migrate
Enable/disable SMTP Anti-spam	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming\tasks\antispam\enable = 1/0"	"/root/Smtp/TMASE/AntiSpam/Enable=1/0"	SMTP->Anti-spam->Target->Enable/Disable	SMTP->Anti-spam->Content Scanning>Target->Enable SMTP Anti-spam
Configure anti-spam detection level	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming\tasks\antispam\setting\Threshold"	"/root/Smtp/TMASE/AntiSpam: MostConfidentAction=Delete/Quarantine/Stamp/Deliver LeastConfidentAction=Delete/Quarantine/Stamp/Deliver ConfidentAction=Delete/Quarantine/Stamp/Deliver"	SMTP->Anti-spam->Target->Threshold	SMTP->Anti-spam->Content Scanning>Target->Spam detection level

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure action on spam mail	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in_spam\actions"	"/root/Smtp/TMASE/AntiSpam/MostConfidentAction/Delete(Deliver/Quarantine/Stamp) /root/Smtp/TMASE/AntiSpam/LeastConfidentAction/Delete(Deliver/Quarantine/Stamp) /root/Smtp/TMASE/AntiSpam/ConfidentAction/Delete(Deliver/Quarantine/Stamp)"	SMTP->Anti-spam->Action	SMTP->Anti-spam->Content Scanning>Action
Configure the stamp text	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming\tasks\antispam\setting\SubjectTag"	"/root/Smtp/TMASE/AntiSpam/MostConfidentAction(LeastConfidentAction/ConfidentAction)/Stamp/StampText=Spam:"	SMTP->Anti-spam->Action->Stamp	SMTP->Anti-spam->Content Scanning>Action->Stamp text
Enable/disable content filter rule	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\content\enable = 1/0"	"/root/Smtp/Emanager/Filter-###/EnableRule=1/0 /root/Smtp/Emanager/Filter-###/Inbound(Outbound)"	SMTP->Content Filter->Incoming/Outgoing->Target->Enable/Disable	"SMTP->Content Filtering->Keyword Filter/Attachment Filter->Target->Policy status SMTP->Content Filtering->Keyword Filter/Attachment Filter->Target->Apply policy to incoming/outgoing messages"

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable message size filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\content\setting\fSizeThreshold\bEnableThreshold = 1/0"	"/root/Smtp/Emanager/Filter-###/FilterType=0/1"	SMTP->Content Filter->Incoming/Outgoing->Target->enable Message Size Filter Criteria	SMTP->Content Filtering->Keyword Filter->enable Message Size
Configure message size filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\content\setting\fSizeThreshold\ eCompare = 1/0 (smaller/larger) uiThreshold"	"/root/Smtp/Emanager/Filter-###/SizeThresholdUnit="	SMTP->Content Filter->Incoming/Outgoing->Target->Message Size Filter Criteria	SMTP->Content Filtering->Keyword Filter->Message Size
Configure subject filter keywords	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\advanced_subject\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	"/root/Smtp/Emanager/Filter-###/Filters/Filters/KeywordFilter= /root/Smtp/Emanager/Filter-###/Filters/Filters /KeywordFilter/KeyWord-0,KeyWord-1,..."	SMTP->Content Filter->Incoming/Outgoing->Target->Subject filter keywords	"SMTP->Content Filtering->Keyword Filter->Target->Apply policy to incoming/outgoing messages' Subject SMTP->Content Filtering->Keyword Filter->Target->Keywords list"

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure body filter keywords	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\advanced_body\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	"/root/Smtp/Emanager/Filter-###/Filters/Filters/KeywordFilter= /root/Smtp/Emanager/Filter-###/Filters/Filters /KeywordFilter/KeyWord-0,KeyWord-1,…"	SMTP->Content Filter->Incoming/Outgoing->Target->Body filter keywords	"SMTP->Content Filtering->Keyword Filte->Target->Apply policy to incoming/outgoing messages' Body SMTP->Content Filtering->Keyword Filter->Target->Keywords list"
Enable/disable match case	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\advanced_subject(body)\setting\fLexAnalysis\f_vecExpression\f_exp_###\bCaseSensitive = 1/0"	"/root/Smtp/Emanager/Filter-###/Filters/Filters /KeywordFilter/KeyWord-0,KeyWord-1,…/CaseSensitive=0/1"	SMTP->Content Filter->Incoming/Outgoing->Target->Match case	SMTP->Content Filtering->Keyword Filter->Target->Keywords->Match case
Configure attachment file name filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\attachment\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	"/root/Smtp/Emanager/Filter-###/Filters/AttachmentFilenameFilter/AttachExp="	SMTP->Content Filter->Incoming/Outgoing->Target->Attachment file name	SMTP->Content Filtering->Attachment Filter->Target->File Name

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure attachment file types filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\attachment\setting\fDataTypeConfig\vec_strSubformat\sz_###"	"/root/Smtp/Emanager/Filter-###/Filters/AttachmentFilenameFilter/AttachType="	SMTP->Content Filter->Incoming/Outgoing->Target->attachment file types	SMTP->Content Filtering->Attachment Filter->Target->Attachment File Types
Configure action on content filtered email	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in(out)_content\actions (A corresponding action subfolder will be added under this branch.)"	"Keyword Filter: /root/Smtp/Emanager/Filter-###/Action Attachment Filter: /root/Smtp/Emanager/Filter-###/Action"	SMTP->Content Filter->Incoming/Outgoing->Action	SMTP->Content Filtering->Keyword Filter/Attachment Filter->Action
Enable/disable insert notification in message that has been filtered by attachment filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\attachment\setting\uiReplaceWarning = 1/0"	"/root/Smtp/Emanager/Filter-###/Actions/Remove/EnableDisclaimer=0/1"	SMTP->Content Filter->Incoming/Outgoing->Action->enable Delete attachment and insert the following notification in the message	SMTP->Content Filtering->Attachment Filter->Action->enable Insert the following notification in the message
Configure the content of the inserted notification for messages that have been filtered by attachment filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\incoming(outgoing)\tasks\attachment\setting\strReplaceWarningMsg"	"/root/Smtp/Emanager/Filter-###/Actions/Remove/Disclaimer="	SMTP->Content Filter->Incoming/Outgoing->Action->Delete attachment and insert the following notification in the message	SMTP->Content Filtering->Attachment Filter->Action->Insert the following notification in the message

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable incoming/outgoing notification for content filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in(out)_content\actions (If enable notification, a corresponding subfolder will be added under this branch.)"	"Keyword Filter: /root/Smtp/Emanager/Filter-###/InBoundNotify(OutBoundNotify)/Administrator(Sender/Recipient)/Enable=0/1 Attachment Filter: /root/Smtp/Emanager/Filter-###/InBoundNotify(OutBoundNotify)/Administrator(Sender/Recipient)/Enable=0/1"	SMTP->Content Filter->Incoming/Outgoing->enable Notification	SMTP->Content Filtering->Keyword Filter/Attachment Filter->enable Notification-incoming/outgoing
Configure content of notification	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_smtp_in(out)_content\actions\admin(recipient/sender)\setting\content"	"Keyword Filter: /root/Smtp/Emanager/Filter-###/InBoundNotify(OutBoundNotify)/Administrator(Sender/Recipient)/Body=0/1 Attachment Filter: /root/Smtp/Emanager/Filter-###/InBoundNotify(OutBoundNotify)/Administrator(Sender/Recipient)/Body=0/1"	SMTP->Content Filter->Incoming/Outgoing->Notification	SMTP->Content Filtering->Keyword Filter/Attachment Filter->Notification-incoming/outgoing
	IsntSmtp.ini	config.xml		
Enable/disable SMTP traffic	[Email-Other] EnableIsntMTADll =yes/no	/root/Smtp/Enable =1/0	Summary->SMTP->SMTP Service status	Summary->SMTP->SMTP Traffic status
	IsntSmtp.ini	intscan.ini		

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable insert InterScan received header in processed messages	"[Delivery-Advanced] DisableReceivedHeader=no/yes"	"[EMail-Scan] DisableReceivedHeader=no/yes"	Not supported	SMTP Configuration ->Advanced Configuration->Do not insert InterScan "Received" header in processed messages
Configure SMTP service interface IP	[Receiver-Setting] ISNTSMTPServiceAddr=	Not supported	SMTP->Configuration->Server->IP	Not supported
Configure SMTP service listening port	[Receiver-Setting] ISNTSMTPServiceAddr=	"[Email-Scan] InterScanSMTPServicePort="	SMTP->Configuration->Server->Port	SMTP->Configuration->Main service port
Configure content of greeting message	[Receiver-Setting] GreetingMessage=	"[Email-Scan] Greeting="	SMTP->Configuration->Server->SMTP Greeting	SMTP->Configuration->Send the following SMTP greeting when a connection is established
Configure maximum recipients per message	[Message] LimitRecipientNumberPerMessageTo=	Not supported	SMTP->Configuration->Server->Reject messages with more than # recipients	Not supported
Configure maximum inbound/outbound message size	[Message] LimitInboundMessageSizeTo=	"[Email-Scan] InESMTPSIZE= OutESMTPSIZE="	SMTP->Configuration->Server->Reject messages larger than	SMTP->Configuration->Maximum inbound/outbound message size
	DomainTable.ini	intscan.ini		

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure inbound mail settings	All content of DomainTable.ini will migrate	"[Email-Scan] InboundUseDNS= EOrg= EOrgPort=25"	SMTP->Configuration->Server->Incoming Mail Delivery	SMTP->Configuration->Inbound Mail
Configure outbound mail settings	All content of DomainTable.ini will migrate	"[Email-Scan] OutboundUseDNS= OutboundMailClientIP= OutboundMailSMTPAddr= OutboundMailSMTPPort"	SMTP->Configuration->Server->Outgoing Mail Delivery	SMTP->Configuration->Outbound Mail
	conn_restrict.dat	intscan.ini		
Configure SMTP connection control	This item does not migrate	Not supported	SMTP->Configuration->Connection->SMTP Connection Control	Not supported
	localdomain.dat	intscan.ini		
Configure relay control trusted domains	All contents of file will migrate	"[Email-Scan] RestrictInDomain= RestrictInDomainList="	SMTP->Configuration->Relay Control->Trusted Domains	SMTP->Configuration->Block relayed messages by accepting inbound mail addressed only to the following domains
	rely_restrict.dat	intscan.ini		
Configure relay control trusted host IP	This item does not migrate	Not supported	SMTP->Configuration->Relay Control->Trusted Hosts IP	Not supported

TABLE D-2. ISVW 5.0 to ISVW 7.0 SMTP Migration Information (Continued)

Item	Configuration file		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	UserApprovedList.txt	intscan.ini		
Configure anti-spam approved sender list	All contents of file will migrate	/root/Smtp/TMASE/AntiSpam/WhiteList=	SMTP->Anti-spam->Target->Approved Senders	SMTP->Anti-spam->Target->Approved Senders
	UserBlockedList.txt	intscan.ini		
Configure anti-spam blocked sender list	All contents of file will migrate	/root/Smtp/TMASE/AntiSpam/BlackList=	SMTP->Anti-spam->Target->Blocked Senders	SMTP->Anti-spam->Target->Blocked Senders

FTP Migration

FTP Migration Summary

FTP virus scanning and configuration migrates from ISVW 5.0 to ISVW 7.0 with conditions outlined in *Table D-3*.:

TABLE D-3. ISVW 5.0 to ISVW 7.0 FTP Migration Conditions

Item	Description
Enable Virus Scanning	This feature migrates to Enable FTP Scanning in ISVW 7.0. If Virus Scanning is on in ISVW 5.0 FTP scanning will be enabled after migration. If Virus Scanning is **off** in ISVW 5.0 FTP scanning will not be enabled after migration.
FTP Proxy settings	This feature migrates to FTP Configuration Settings in ISVW 7.0.
FTP Configuration > Options	This feature migrates to FTP Advanced Configuration.
FTP Configuration > Scan	This feature migrates to FTP > Scanning > Target > Files to Scan. Also in ISVW 7.0, the IntelliScan option has been added in the UI.
Warning to user(s) and Virus Message	This feature migrates to FTP > Scanning > Notification > Administrator Notification and User Notification.
Action on Viruses	This feature migrates to FTP > Scanning > Action. The Move action has changed to Quarantine, and the Delete action has changed to Block.

FTP Migration Table

Table D-4 provides detailed information about the FTP migration from ISVW 5.0 to ISVW 7.0.

TABLE D-4. ISVW 5.0 to ISVW 7.0 FTP Migration Information

Item	Configuration file		UI location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	smbstatus.ini	config.xml		
Enable/disable FTP traffic	[Status] ftp=1/0	"/root/Ftp/Enable=1/0"	Summary->FTP->FTP Service status	Summary->FTP->FTP Traffic status
	intscan.ini	intscan.ini		
Enable/disable FTP scanning	[Scan-configuration] FTPScan=yes/no	"[FTP-Scan] AntiVirus=yes/no"	FTP->Virus Scan->Target->Enable/Disable	FTP->Scanning->Target->Enable FTP scanning
Configure FTP scan level	[ftp] level=scanall/scanintelli/scanext	"[FTP-Scan] Level=ScanAll/IntelliScan/ScanExt"	FTP->Virus Scan->Target->File Type	FTP->Scanning->Target->Files to Scan
Configure action on FTP virus scanning	"[ftp] action=pass/delete/move/cleanpass/cleanmove/cleandelete ucaction=pass/move/delete"	"[FTP-Scan] Action=Cleanmove/Cleandelete/Cleanpass/Move/Delete/Pass"	FTP->Virus Scan->Action	FTP->Scanning->Action
Configure FTP client notification	[ftp] VirusMessageText=	"[FTP-Scan] VirusMessageText="	FTP->Configuration->FTP Client Notification	FTP->Scanning->Notification->User Notification

TABLE D-4. ISVW 5.0 to ISVW 7.0 FTP Migration Information (Continued)

Item	Configuration file		UI location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable FTP notification for administrator	[ftp] Email=yes/no	"[FTP-Scan] Email=yes/no"	FTP->Configuration->enable FTP Admin Email Notification	FTP->Scanning->Notification->enable Administrator Notification
Enable/disable FTP file blocking	"[ftp] block_types= (When it's disabled, this value is null.)"	Not supported	FTP->File Blocking->File->Enable/Disable	Not supported
Configure FTP blocked file types	[ftp] block_types=	Not supported	FTP->File Blocking->File->Block file types	Not supported
Configure FTP service mode	[ftp] UseFTPProxy= yes/no	"[FTP-Scan] UseFTPProxy= yes/no"	FTP->Configuration->Stand-alone Mode / Use FTP Proxy	FTP->Configuration->Use stand-alone Mode / Use FTP Proxy
Configure FTP proxy server IP	[ftp] FOrg=	"[FTP-Scan] FOrg"	FTP->Configuration->Use FTP Proxy server	FTP->Configuration->Use FTP Proxy server
Configure FTP proxy server port	[ftp] FOrgPort=	"[FTP-Scan] FOrgPort"	FTP->Configuration->Use FTP Proxy server	FTP->Configuration->Use FTP Proxy server

TABLE D-4. ISVW 5.0 to ISVW 7.0 FTP Migration Information (Continued)

Item	Configuration file		UI location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable FTP passive mode	[ftp] ForcePassiveFTP=yes/no	"[FTP-Scan] ForcePassiveFTP=yes/no"	FTP->Configuration->Use passive FTP for all file transfers	FTP->Configuration->Use passive FTP for all file transfers
	ext_addition_ftp.lst	intscan.ini		
Configure FTP scan additional file extension	All content of file migrates	"[FTP-Scan] ScanExtensions="	FTP->Virus Scan->Target->File Type->added extensions	FTP->Scanning->Target->Files to Scan->additional file extensions

HTTP Migration

HTTP Migration Summary

HTTP settings in ISVW 5.0 migrate to ISVW 7.0 with conditions outlined in *Table D-5*.

TABLE D-5. ISVW 5.0 to ISVW 7.0 HTTP Migration Summary

Item	Description
Enable HTTP traffic scan	This setting migrates.
Scanning service listening port	This setting migrates.
Compressed file settings	This setting migrates.
HTTP traffic scanning settings	This setting migrates.
Virus notification message content	This content migrates.

TABLE D-5. ISVW 5.0 to ISVW 7.0 HTTP Migration Summary (Continued)

Item	Description
Infected files settings	This setting migrates.
Large file handling	This setting migrates.
URL blocking	This setting migrates.

HTTP Migration Table

Table D-6 provides detailed information about the HTTP migration from ISVW 5.0 to ISVW 7.0.

TABLE D-6. ISVW 5.0 to ISVW 7.0 HTTP Migration Information

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	smbstatus.ini	config.xml		
Enable/disable HTTP traffic	[Status] http=1/0	/root/Http/Enable=1/0	Summary->Web(HTTP)->HTTP Service status	Summary->Web(HTTP)->HTTP Traffic status
	IWSSPIScanVsapi.dsc	config.xml		
Enable/disable HTTP virus scanning	[plug-in] enabled=yes/no	/root/Http/Main/http/spyware_scan_enabled=yes/no	HTTP->Virus Scan->Target->Enable/Disable	HTTP->Scanning->Target->Enable HTTP scanning
Configure HTTP scan level	[http] level=scanall/scanintelli/scanext	"/root/Http/plugin/ScanVsapi/http/level=scanall/scanintelli/scanext"	HTTP->Virus Scan->Target->File Type	HTTP->Scanning->Target->Files to Scan

TABLE D-6. ISVW 5.0 to ISVW 7.0 HTTP Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure HTTP maximum number of files in compressed file to scan	[http] extract_limit_count=	"/root/Http/plugin/ScanVsapi/http/extract_limit_count="	HTTP->Configuration->Compressed File Scanning->Maximum number of files	HTTP->Scanning->Target->Compressed File Handling->Extracted file count exceeds
Configure HTTP maximum decompressed file size to scan	[http] extract_limit_size=	"/root/Http/plugin/ScanVsapi/http/extract_limit_size="	HTTP->Configuration->Compressed File Scanning->Maximum decompressed file size	HTTP->Scanning->Target->Compressed File Handling->Extracted file size exceeds
	ext_addition_http.lst	config.xml		
Configure HTTP scan additional file extensions	All items migrate	"/root/Http/plugin/ScanVsapi/http/extensions"	HTTP->Virus Scan->Target->File Type->added extensions	HTTP->Scanning->Target->Files to Scan->additional file extensions
	intscan.ini	config.xml		
Configure action on HTTP virus scan	"[http] action=pass/delete/move/clean ucaction=pass/move/delete"	"root/Http/Main/http/action=pass/delete/move/clean root/Http/Main/http/ucaction=pass/move/delete"	HTTP->Virus Scan->Action	HTTP->Scanning->Action
Configure HTTP user notification	[http] addtl_virus_message=	root/Http/Main/http/virus_notification	HTTP->Virus Scan->Notification	HTTP->Scanning->Notification->User Notification

TABLE D-6. ISVW 5.0 to ISVW 7.0 HTTP Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure HTTP file blocking browser notification	[http] addtl_type_message=	Not supported	HTTP->File Blocking->File->Notification->display in user's browser	Not supported
Enable/disable HTTP file blocking notification to administrator	[http] notify_type_admin=yes/no	Not supported	HTTP->File Blocking->File->Notification->enable email to admin	Not supported
Configure HTTP file blocking notification to administrator	[http] admin_type_msg=	Not supported	HTTP->File Blocking->File->Notification->email message to admin	Not supported
Enable/disable HTTP file blocking	"[Scan-configuration] block_types= (When it's disabled, this value is null.)"	Not supported	HTTP->File Blocking->File->Enable/Disable	Not supported
Configure HTTP blocked file types	[Scan-configuration] block_types=	Not supported	HTTP->File Blocking->File->Block file types	Not supported
Enable/disable URL blocking	[URL-blocking] enable=yes/no	/root/Http/Main/http/url_blocking_enable=yes/no	HTTP->URL Blocking->URL->Enable/Disable	HTTP->URL Blocking->Target->Enable HTTP URL Blocking
Configure URL blocking for user notification	[Request-scan] addtl_url_block_message=	/root/Http/Main/http/reject_notification	HTTP->URL Blocking->Notification	HTTP->URL Blocking->Notification->User Notification

TABLE D-6. ISVW 5.0 to ISVW 7.0 HTTP Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable HTTP large file handling	[scan] special_handling=yes/no	/root/Http/Main/scan/special_handling=yes/no	HTTP->Configuration->enable big sized file handling	HTTP->Scanning->Target->Enable special handling when a files is larger than
Configure HTTP minimum file size for large file handling	[scan] max_synchronous_scan_size=	/root/Http/Main/scan/max_synchronous_scan_size=	HTTP->Configuration->If download size is bigger than #	HTTP->Scanning->Target->Enable special handling when a files is larger than #
Configure HTTP large file handling settings	[scan] deferred_scanning=yes/no	/root/Http/Main/scan/defered_scanning=yes/late	HTTP->Configuration->option for big sized file handling	HTTP->Scanning->Target->option for Large File Handling
	URLB.ini	URLB.ini		
Configure HTTP URL blocking lists	All contents under [block] section migrate	[block] section in file	HTTP->URL Blocking->URL->Blocked URLs	HTTP->URL Blocking->Target->Block List
Configure HTTP URL blocking list	All contents under [block] section migrate	[block] section	HTTP->URL Blocking->URL->Blocked URLs containing following text strings	HTTP->URL Blocking->Target->Block List
Configure HTTP URL block list exceptions	All contents under [Allow] section migrate	[Allow] section	HTTP->URL Blocking->URL->Exceptions	HTTP->URL Blocking->Target->Block List Exceptions

TABLE D-6. ISVW 5.0 to ISVW 7.0 HTTP Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	IWSSPIProtocolHttpProxy.pni	config.xml		
Configure HTTP service listening port	[main] port=8080	/root/Http/Protocol/HttpProxy/http/original_server_port	HTTP->Configuration->HTTP Listening Port	HTTP->Configuration->HTTP Listening Port
Configure anonymous FTP over HTTP logon email	[http] anonymous_ftp_mail_address =	/root/Http/Protocol/HttpProxy/http/anonymous_ftp_mail_address	HTTP->Configuration->Anonymous FTP over HTTP logon email	HTTP->Configuration->Anonymous FTP over HTTP logon email

POP3 Migration

POP3 Migration Summary

ISVW 7.0 migrates most POP3 settings from ISVW 5.0. POP3 settings migrate from ISVW 5.0 to ISVW 7.0 with conditions outlined in *Table D-7*.

TABLE D-7. ISVW 5.0 to ISVW 7.0 POP3 Migration Summary

Item	Description
Scan email messages	This item migrates. If this value is set to 0, after migration, all email messages will not be scanned for viruses.
Scan Extensions	ISVW 7.0 has a default scan list. After migration, the scan extension list is as follows: 7.0 defaultlist+5.0 ScanExtensions.
POP3 Anti-spam	This item migrates. If this value is set to 0, after migration all email messages will not be scanned for the following: spam
POP3 content filter	This item migrates. If this value is set to 0, after migration, all rules with a value that is set to 0 will not be enabled.

POP3 Migration Table

Table D-8 provides detailed information about the POP3 migration from ISVW 5.0 to ISVW 7.0.

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	IsntSmtp.ini	config.xml		
Enable/disable POP3 traffic	[Email-Other] EnableIsntPop3Dll=yes/no	/root/Pop3/Enable=1/0	Summary->POP3->POP3 Service status	Summary->POP3->POP3 Traffic status
	Registry	config.xml		
Enable/disable POP3 scanning	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\enable = 1/0	/root/Pop3/Policies/Rules/MailVirusScan/Enable=0/1	POP3->VirusScan->Target->Enable/Disable	POP3->Scanning->Target->Enable POP3 Scanning
Configure POP3 scan level	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\setting\ ScanLevel = 0/1 IntelliScan = 0/1 ScanUserExt = 0/1"	/root/Pop3/Policies/Rules/MailVirusScan/ScanTypePolicy=1,2,3	POP3->VirusScan->Target->File Type	POP3->Scanning->Target->Files to Scan
Configure POP3 scan additional file extensions	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\setting\UserExtensions	/root/Pop3/Policies/Rules/MailVirusScan/UserExcludeExtensions,UserExtensions	POP3->VirusScan->Target->File Type->added extensions	POP3->Scanning->Target->Files to Scan->additional file extensions

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure POP3 virus scan action	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\setting\DoCleanFailed DoVirusFound"	/root/Pop3/Policies/Rules/Mail VirusScan/VirusAction=	POP3->Virus Scan->Action	POP3->Scanning->Action
Enable/disable email notification for administrator or recipient	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_virus\actions (If enable notification, a corresponding subfolder will be added under this branch.)"	/root/Pop3/Policies/Rules/Mail VirusScan/Outcomes/Action/NotificationAdmin(NotificationRecipient)/Enable	POP3->Virus Scan->Notification->>enable Email notifications	POP3->Scanning->Notification->enable Email Notifications
Enable/disable inline notification stamp	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\setting\SafeStamp = 1/0 AddAlert = 1/0"	/root/Pop3/Policies/Rules/Mail VirusScan/AddAlert(SafeStamp)	POP3->Virus Scan->Notification->>enable Inline notifications	POP3->Scanning->Notification->enable Inline Notification Stamp
Configure email notification content	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_virus\actions\admin(recipient)\setting\content	/root/Pop3/Policies/Rules/Mail VirusScan/Outcomes/Action/NotificationAdmin(NotificationRecipient)/Body=	POP4->Virus Scan->Notification->>Email notifications content	POP4->Scanning->Notification->Email Notifications content

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure inline notification stamp content	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\virus\setting\SafeStampMsg VirusAlert"	/root/Pop3/Policies/Rules/Mail VirusScan/Safe StampMsg=,VirusAlert=	POP3->Virus Scan->Notification->>Inline notifications content	POP3->Scanning->Notification->Inline Notification Stamp content
Enable/disable POP3 antispam	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\antispam\enable = 1/0	/root/Scan/TMASE/AntiSpam/Enable=0/1	POP3->Anti-spam->Target->Enable/Disable	POP3->Anti-spam->Target->Enable POP3 Anti-spam
Configure POP3 spam detection level	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\antispam\setting\Threshold	/root/Scan/TMASE/CategoryLevels=	POP3->Anti-spam->Target->Threshold	POP3->Anti-spam->Target->Spam detection level
Configure POP3 Anti-spam action	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_spam\actions	"/root/Scan/TMASE/MostConfidentAction=Stamp/Delete/Deliver/Quarantine /root/Scan/TMASE/ConfidentAction=Stamp/Delete/Deliver/Quarantine /root/Scan/TMASE/LeastConfidentAction=Stamp/Delete/Deliver/Quarantine"	POP3->Anti-spam->Action	POP3->Anti-spam->Action

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure POP3 spam stamp for mail subject	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\antispam\setting\SubjectTag	"/root/Scan/TMASE/MostConfidentAction/Stamp/StampText= /root/Scan/TMASE/ConfidentAction/Stamp/StampText= /root/Scan/TMASE/LeastConfidentAction/Stamp/StampText="	POP3->Anti-spam->Action->Spam Stamp	POP3->Anti-spam->Action->Spam Stamp
Enable/disable POP3 content filtering rule	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\content\enable = 1/0	"/root/Scan/Emanager/Filter-###/EnableRule=0/1 /root/Scan/Emanager/Filter-###/EnableRule=0/1"	POP3->Content Filter->Target->Enable/Disable	POP3->Content Filtering->Keyword Filter/Attachment Filter->Target->Policy status
Enable/disable POP3 message size filter	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\content\setting\fSizeThreshold\bEnableThreshold = 1/0	/root/Scan/Emanager/Filter-###/Filters/SizeFilter/FilterType	POP3->Content Filter->Target->enable Message Size Filter Criteria	POP3->Content Filtering->Keyword Filter->enable Message Size
Configure maximum message size for POP3 filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\content\setting\fSizeThreshold\ eCompare = 1/0 (smaller/larger) uiThreshold"	/root/Scan/Emanager/Filter-###/Filters/SizeFilter/SizeThreshold	POP3->Content Filter->Target->Message Size Filter Criteria	POP3->Content Filtering->Keyword Filter->Message Size

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure POP3 keywords list for subject keyword filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\advanced_subject\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	"/root/Scan/Emanager/Filter-###/Filters/Filters/KeywordFilter(ExceptionFilter)/FilterScope=1 /root/Scan/Emanager/Filter-###/Filters/Filters/KeywordFilter/KeyWord-0,KeyWord-1,…"	POP3->Content Filter->Target->Subject filter keywords	"POP3->Content Filtering->Keyword Filter->Target->Apply policy to messages' Subject POP3->Content Filtering->Keyword Filter->Target->Keywords list"
Configure POP3 keywords list for mail body keyword filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\advanced_body\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	"/root/Scan/Emanager/Filter-###/Filters/Filters/KeywordFilter(ExceptionFilter)/FilterScope=2 /root/Scan/Emanager/Filter-###/Filters/Filters/KeywordFilter/KeyWord-0,KeyWord-1,…"	POP3->Content Filter->Target->Body filter keywords	"POP3->Content Filtering->Keyword Filte->Target->Apply policy to incoming/outgoing messages' Body POP3->Content Filtering->Keyword Filter->Target->Keywords list"

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable match case for keyword list	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\advanced_subject(body)\setting\fLexAnalysis\f_vecExpression\f_exp_###\bCaseSensitive = 1/0	/root/Scan/Emanager/Filter-###/Filters/Filters/KeywordFilter/KeyWord-0,KeyWord-1,…/CaseSensitive=0/1	POP3->Content Filter->Target->Match case	POP3->Content Filtering->Keyword Filter->Target->Keywords->Match case
Configure attachment file name for POP3 attachment filtering	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\attachment\setting\fLexAnalysis\f_vecExpression\f_exp_###\op_wtrExpression (bEnable = 1)"	/root/Scan/Emanager/Filter-###/Filters/Filters/AttachmentFilenameFilter/AttachType	POP3->Content Filter->Target->Attachment file name	POP3->Content Filtering->Attachment Filter->Target->File Name
Configure attachment file type for POP3 attachment filtering	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\attachment\setting\fDataTypeConfig\vec_strSubformat\sz_###	/root/Scan/Emanager/Filter-###/Filters/Filters/AttachmentFilenameFilter/AttachExp	POP3->Content Filter->Target->attachment file types	POP3->Content Filtering->Attachment Filter->Target->Attachment File Types

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure action for POP3 content filter	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_content\actions (A corresponding action subfolder will be added under this branch.)"	/root/Scan/Emanager/Filter-###/Action=	POP3->Content Filter->Action	POP3->Content Filtering->Keyword Filter/Attachment Filter->Action
Enable/disable insert disclaimer in message if the attachment is deleted	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\attachment\setting\uiReplaceWarning = 1/0	/root/Scan/Emanager/Filter-###/Actions/Remove/EnableDisclaimer=0/1	POP3->Content Filter->Action->enable Delete attachment and insert the following notification in the message	POP3->Content Filtering->Attachment Filter->Action->enable Insert the following notification in the message
Configure the content of the dislaimer to be inserted into message	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Rule\Mail\rules\POP3\tasks\attachment\setting\strReplaceWarningMsg	/root/Scan/Emanager/Filter-###/Actions/Remove/Disclaimer=	POP3->Content Filter->Action->Delete attachment and insert the following notification in the message	POP3->Content Filtering->Attachment Filter->Action->Insert the following notification in the message

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable notification for POP3 content filtering	"HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_content\actions (If enable notification, a corresponding subfolder will be added under this branch.)"	"/root/Scan/Emanager/Filter-###/Notifications/Administrator(Recipient)/Enable=0/1 /root/Scan/Emanager/Filter-###/Notifications/Administrator(Recipient)/Enable=0/1"	POP3->Content Filter->enable Notification	POP3->Content Filtering->Keyword Filter/Attachment Filter->enable Notification
Configure notification content	HLM\SOFTWARE\TrendMicro\ISNT5\registry\policy\Classification\action_pop3_content\actions\admin(recipient)\setting\content	"/root/Scan/Emanager/Filter-###/Notifications/Administrator(Recipient)/Body= /root/Scan/Emanager/Filter-###/Notifications/Administrator(Recipient)/Body="	POP3->Content Filter->Notification content	POP3->Content Filtering->Keyword Filter/Attachment Filter->Notification content
	UserApprovedList.txt	config.xml		
Configure POP3 anti-spam approved senders list	All contents in the file migrate	/root/Scan/TMASE/WhiteList=	POP3->Anti-spam->Target->Approved Senders	POP3->Anti-spam->Target->Approved Senders
	UserBlockedList.txt	config.xml		
Configure POP3 anti-spam blocked senders list	All contents in the file migrate	/root/Scan/TMASE/BlackList=	POP3->Anti-spam->Target->Blocked Senders	POP3->Anti-spam->Target->Blocked Senders
	pop3.ini	config.xml		

TABLE D-8. ISVW 5.0 to ISVW 7.0 POP3 Migration Information (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure POP3 interface IP address	[Socket] ProxyServerId=	/root/Pop3/IPAddressToBind	POP3->Configuration->POP3 IP Address	POP3->Configuration->POP3 IP Address
Configure POP3 maximum allowed simultaneous client connections	[ThreadPool] ThreadCount=	/root/Pop3/MaxSimultanenousClientConnections=	POP3->Configuration->End User Mail Client Connections	POP3->Configuration->End User Mail Client Connections
Configure POP3 mail server connection settings	"[Socket_#] ProxyPort= ProxyService= POP3_GENERIC_SERVICE"	/root/Pop3/AllowLoginParameter	POP3->Configuration->POP3 Mail Server Connection	POP3->Configuration->POP3 Mail Server Connection
Configure POP3 port mapping settings	"[Socket_#] ProxyPort= ProxyService= POP3_DEDICATED_SERVICE DedicatedServerName= DedicatedServerPort="	/root/Pop3/AllowServerPortMapping,ServerPortMappingCount	POP3->Configuration->POP3 Mail Server Connection For Secure Password Authentication	POP3->Configuration->POP3 Port Mapping

ActiveUpdate Migration

ActiveUpdate Migration Summary

ActiveUpdate settings in ISVW 5.0 migrate to ISVW 7.0 with conditions outlined in *Table D-9*.

TABLE D-9. ISVW 5.0 to ISVW 7.0 ActiveUpdate Migration Summary

Item	Description
Scheduled update settings	This setting migrates the time updates should occur.
Pattern and engine update	This setting migrates the automatic update settings for updating the patterns and engines.

Active Update Migration Table

Table D-10 provides detailed information about the ActiveUpdate migration from ISVW 5.0 to ISVW 7.0.

TABLE D-10. ActiveUpdate Migration from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
	lsntSmtp.ini	config.xml		

TABLE D-10. ActiveUpdate Migration from ISVW 5.0 to ISVW 7.0 (Continued)

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Method	[Update] Method=Automatic/Manualy	/root/Common/ActiveUpdate/ScheduleUpdate/EnableUpdate	Update->Scheduled->Enable scheduled update	Update->Scheduled->Enable scheduled updates
Frequency	"[Update] Frequency=Hourly/Daily/Weekly Hour=#:# APM=AM/PM DayOfWeek1="	/root/Common/ActiveUpdate/ScheduleUpdate/Type,Days,Hours,Minutes	Update->Scheduled->Check for update	Update->Scheduled->Update Schedule
UpdateEngine and UpdatePattern	"[Update] UpdatePattern= yes/no (virus pattern) UpdateEngine= yes/no (virus scan engine) UpdatePIRANHA=yes/no (anti-spam rules and engine)"	/root/Common/ActiveUpdate/ScheduleUpdate/EnableItems=	Update->Scheduled->scheduled update component types	Update->Scheduled->Select Components

Administration, Quarantine, and Log Migration

Administration, Quarantine, and Log Migration Summary

These settings migrate from ISVW 5.0 to ISVW 7.0 with conditions outlined in *Table D-11*.

TABLE D-11. Administration, Quarantine, and Log Migration from ISVW 5.0 to ISVW 7.0

Item	Description
Administration	
Proxy settings	This item migrates.
Notification settings	This item migrates.
Logs	
Automatic maintenance	This item migrates.
Quarantine	
Quarantined files and email messages	All files and email messages under the ISVW 5.0 quarantine folder can be migrated to the ISVW 7.0 quarantine folder as long as migration takes place on the same computer.

Administration, Quarantine, and Log Migration Table

Table D-12 provides detailed information about the ActiveUpdate migration from ISVW 5.0 to ISVW 7.0.

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Administration				
	IsntSmtp.ini	config.xml		
Enable/disable proxy server settings	[Update] UseProxySetting=yes/no	"/root/Common/ActiveUpdate/UpdateServers/Server.1/UseProxy=0/1 /root/Common/ActiveUpdate/UpdateServers/Server.2/UseProxy=0/1 /root/Common/ActiveUpdate/UpdateServers/Server.3/UseProxy=0/1 /root/Common/ProductRegistration/OnlineUpdate/Server/UseProxy=0/1 /root/Services/WTC/UseProxy=0/1"	Update->Proxy->enable Use HTTP/Socks3 proxy	Administration->Proxy Settings->enable Use a proxy server

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure proxy protocol settings	[Update] UseSocks4Proxy=yes/no	"/root/Common/ActiveUpdate/UpdateServers/Server.1/IsSocksProxyProxy=0/1 /root/Common/ActiveUpdate/UpdateServers/Server.2/IsSocksProxyProxy=0/1 /root/Common/ActiveUpdate/UpdateServers/Server.3/IsSocksProxyProxy=0/1 /root/Common/ProductRegistration/OnlineUpdate/Server/IsSocksProxyProxy=0/1 /root/Services/WTC/IsSocksProxy=0/1"	Update->Proxy->Use HTTP/Socks4 proxy	Administration->Proxy Settings->Proxy protocol

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure proxy server name or IP address	[Update] HTTPProxy=	"/root/Common/ActiveUpdate/UpdateServers/Server.1/Proxy= /root/Common/ActiveUpdate/UpdateServers/Server.2/Proxy= /root/Common/ActiveUpdate/UpdateServers/Server.3/Proxy= /root/Common/ProductRegistration/OnlineUpdate/Server/Proxy= /root/Services/WTC/Proxy="	Update->Proxy->Address	Administration->Proxy Settings->Server name or IP address
Configure proxy server ports	[Update] HTTPPort=	"/root/Common/ActiveUpdate/UpdateServers/Server.1/ProxyPort= /root/Common/ActiveUpdate/UpdateServers/Server.2/ProxyPort= /root/Common/ActiveUpdate/UpdateServers/Server.3/ProxyPort= /root/Common/ProductRegistration/OnlineUpdate/Server/ProxyPort= /root/Services/WTC/ProxyPort="	Update->Proxy->Port	Administration->Proxy Settings->Port

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure the log storage directory	"[Log-File] LogDirectory= (The root of log directory should be the path upper than ""mail"" subfolder.) "	Not supported	Administration->Configuration->Directories->Log Storage Directory	Not supported
Configure SMTP server for sending email notifications	[General-Notification] NotificationSMTPAddr=	"/root/Smtp/Actions/Notification/MailServer /root/Scan/Actions/Notification/MailServer /root/Services/Notif/MailServer"	Administration->Configuration->Notification->SMTP server	Administration->Notification Settings->SMTP server
Configure SMTP server ports for notification	[General-Notification] NotificationSMTPAddr=	"/root/Smtp/Actions/Notification/Portr /root/Scan/Actions/Notification/Port /root/Services/Notif/Port"	Administration->Configuration->Notification->Port	Administration->Notification Settings->Port
Configure maximum notifications allowed per hour	[General-Notification] NotificationLimitationInHour=	Not supported	Administration->Configuration->Notification->Maximum notifications per hour	Not supported
Configure the maximum number of queued messages before sending alerts	"[SysMonitor] MonitorDeliveryQueue=1/0 NotifyMessageDeliveryQueue="	Not supported	Administration->Configuration->Alerts->Send alert when queue reaches # messages	Not supported

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Configure the maximum minutes to wait before sending notification when any service stops	"[SysMonitor] MonitorISNTService=1/0 MonitorISNTServiceThreshold = NotifyMessageISNTService="	Not supported	Administration->Configuration->Alerts->Send alert when any service stops for more than # minutes	Not supported
Configure the minimum free space for working directory before sending notification	"[SysMonitor] MonitorISNTMQueueFreeSpace=1/0 MonitorISNTMQueueFreeSpaceThreshold= NotifyMessageMQueueFreeSpace="	Not supported	Administration->Configuration->Alerts->Send alert when working directory has less than # MB free space	Not supported
Enable/disable sending notification after schedule update attempted	"[SysMonitor] MonitorScheduleUpdate=1/0"	Not supported	Administration->Configuration->Alerts->Send alert after scheduled update attempt	Not supported
	Registry	config.xml		
Configure the administrator's email address	HLM\SOFTWARE\TrendMicro\ISNT5\registry\config\Classification\0002\0001\Administrator	"/root/Smtp/Actions/Notification/Admin /root/Scan/Actions/Notification/Admin /root/Services/Notif/Admin"	Administration->Configuration->Notification->Admin email	Administration->Notification Settings->Email address
	intscan.ini	config.xml		

TABLE D-12. Administration, Quarantine, and Log Migration of ActiveUpdate from ISVW 5.0 to ISVW 7.0

Item	Configuration files		UI Location	
	ISVW 5.0	ISVW 7.0	ISVW 5.0	ISVW 7.0
Enable/disable write connection log for HTTP or FTP	"[http] [ftp] log_trans = yes/no"	"/root/http/WriteConnectionMsg = 1/0 and /root/ftp/WriteConnectionMsg = 1/0		
Log Maintenance				
	lsntSmtp.ini	config.xml		
Enable/disable automatic purge of logs	[Log-File] AutoDelete=yes/no	/root/Common/Logging/EnableMaintenance=0/1	Logs->Maintenance->enable Delete logs after	Logs->Maintenance->Automatic->Enable Automatic Purge
Configure the expiry date of logs	"[Log-File] KeepLastDayOfLog="	/root/Common/Logging/ExpiredDays=	Logs->Maintenance->Delete logs after	Logs->Maintenance->Automatic->Delete logs selected above older than # days
Quarantine				
Quarantined files under the quarantine folder	<isvw5_install_path>\quarantine	<isvw7_install_path>\quarantine		

Appendix E

Migration from InterScan VirusWall 6.0, 6.01, or 6.02

Use this appendix as a reference when migrating settings from InterScan VirusWall (ISVW) 6.0, 6.01, or 6.02 to ISVW 7.0.

Migrating from ISVW 6.0, 6.01, or 6.02 to ISVW 7.0 is quite similar to migrating from ISVW 6.0 to ISVW 7.0 (see Appendix D, *Migration from InterScan VirusWall 5.0*).

Table E-1 describes the settings not migrated from ISVW 6.0 to ISVW 7.0.

TABLE E-1. Keys Not Migrated From ISVW 6.0

KEY	SETTINGS
config.xml: Http\Main\scan\trickle_rate	ISVW 7.0 default value: 96. UI Location6.0x/7.0: HTTP > Scanning > Large File Handling | Deferred scan every time ISVW server receives
config.xml: Http\Main\scan\trickle_max_size	ISVW 7.0 default value: 65536. UI Location6.0x/7.0: HTTP > Scanning > Large File Handling | Deferred scan Send "x" amount of the file to the client
Config.xml: Http\Main\Http\reject_notification	ISVW 7.0 uses the key :Http\ Notification\ URLBlockFilter. Default value: Security policy for this network has blocked the requested URL. If you have any questions, contact your administrator. UI Location6.0x: HTTP > URL blocking > Notification. UI Location 7.0: HTTP > HTTP URL Blocking & Filtering > Settings | User Notification.
Quarantine	Quarantine files: If the ISVW 6.0x quarantine path is under the root path of ISVW 6.0, ISVW 7.0 will move the previous quarantine to the root driver path. For example, if the product is installed under D:\ISVW6, and the quarantine file is under D:\ISVW\quaratine, ISVW 7.0 will move the quarantine file to D:\Relocated_ISVW6_Quarantine_Folder\xxx. If the previous quarantine path is not under the root path of ISVW 6.0, ISVW 7.0 will keep the quarantine files under user's setting path. Quarantine setting: If the quarantine path was modified for ISVW 6.0x, ISVW 7.0 will keep the user setting. If the quarantine path was not modified in ISVW 6.0x, ISVW 7.0 quarantine file path is: <isvw7_install_path>\quarantine

Appendix F

TMCM Replication Limitations

Not all items are replicated when using the TMCM Web console to perform a configuration replication. This appendix lists items and settings that will not be replicated.

The following sections are part of the protocol-specific settings not replicaed:

- *SMTP Specific Settings Not Replicated*
- *HTTP Specific Settings Not Replicated*
- *FTP Specific Settings Not Replicated*
- *POP3 Specific Settings Not Replicated*

The following sections are part of the InterScan VirusWall (ISVW)-specific settings not replicated:

- *Outbreak Defense*
- *Quarantine*
- *Update*
- *Logs*
- *Administration*
- *Other ISVW User Interface Items and Settings Not Replicated*

Protocol Specific Settings Not Replicated

SMTP Specific Settings Not Replicated

All settings associated with SMTP Scanning, IntelliTrap, Anti-Phishing, Anti-Spam, Anti-Spyware, and Content Filtering are replicated when using the TMCM Web console. Only specific settings related to SMTP Configuration are not replicated when using the TMCM Web console.

TABLE F-1. SMTP Configuration screen settings not replicated

SMTP Configurations
Server Configuration
Main service port
Inbound Mail (Does not include the "Log incoming Message-ID")
Outbound Mail - items 1 & 2 (Does not include the "Add customized disclaimer...")
Queue Mail
All items in this section are replicated
Advanced Configuration
Block relayed messages by accepting inbound mail addressed only to the following domains (All other items in this section are replicated)

HTTP Specific Settings Not Replicated

All settings associated with HTTP Scanning, Anti-Phishing, Anti-Spyware, URL Blocking, URL Filtering Rules, and URL Filtering Settings are replicated when using the TMCM Web console. Only specific settings related to HTTP Configuration are not replicated when using the TMCM Web console.

TABLE F-2. HTTP Configuration screen settings not replicated

HTTP Configurations
Settings
ISVW's operating mode
HTTP listening port
Anonymous FTP over HTTP logon email
"Log HTTP requests" is replicated

FTP Specific Settings Not Replicated

All settings associated with FTP Scanning and Anti-Spyware are replicated when using the TMCM Web console. Only specific settings related to FTP Configuration are not replicated when using the TMCM Web console.

TABLE F-3. FTP Configuration screen settings not replicated

FTP Configurations
Settings
ISVW's operating mode information
Use passive FTP for all file transfers
FTP service port
Advanced Configurations
All items in the Advanced Configuration section are replicated

POP3 Specific Settings Not Replicated

All settings associated with POP3 Scanning, IntelliTrap, Anti-Phishing, Anti-Spam, Anti-Spyware, and Content Filtering are replicated when using the TMCM Web console. Only specific settings related to POP3 Configuration are not replicated when using the TMCM Web console.

TABLE F-4. POP3 Configuration screen settings not replicated

POP3 Configurations
POP3 IP Address
IP
End User Mail Client Connections
This field is replicated
POP3 Mail Server Connection
Connect to any POP3 server requested by end-user clients
POP3 clients connect to ISVW on port
POP3 Port Mapping
Enable port mapping mode and specify remote inbound POP3 server IP and its service port
Inbound POP3 port
IP address
POP3 server port

InterScan VirusWall Specific Settings Not Replicated

Outbreak Defense

TABLE F-5. Outbreak Defense settings not replicated

Outbreak Defense
Current Status - "Enable Outbreak Prevention Services (OPS)" is replicated
Settings - All settings in the "Settings" screen are replicated

Quarantine

TABLE F-6. Quarantine settings not replicated

Quarantines

Settings - None of the settings are replicated
Maintenance (Manual & Automatic) - All settings replicated

Update

TABLE F-7. Update settings not replicated

Update
Manual - N/A
Scheduled - All settings are replicated

Logs

TABLE F-8. Logs settings not replicated

Logs
Query - N/A
Maintenance (Manaul & Scheduled) - All settings are replicated

Administration

TABLE F-9. Administration settings not replicated

Administration
Control Manager Settings - None of the settings are replicated
Notification Settings - None of the settings are replicated
Password - None of the settings are replicated
Product License - None of the information is replicated
Proxy Settings - None of the settings are replicated
World Virus Tracking - None of the settings are replicated

Other ISVW User Interface Items and Settings Not Replicated

- Patterns and Engines
- Quarantined files
- Logs
- Control manager settings

- WTC settings
- Web console password
- Product registration profile

Index

A

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W