TREND MICRO™

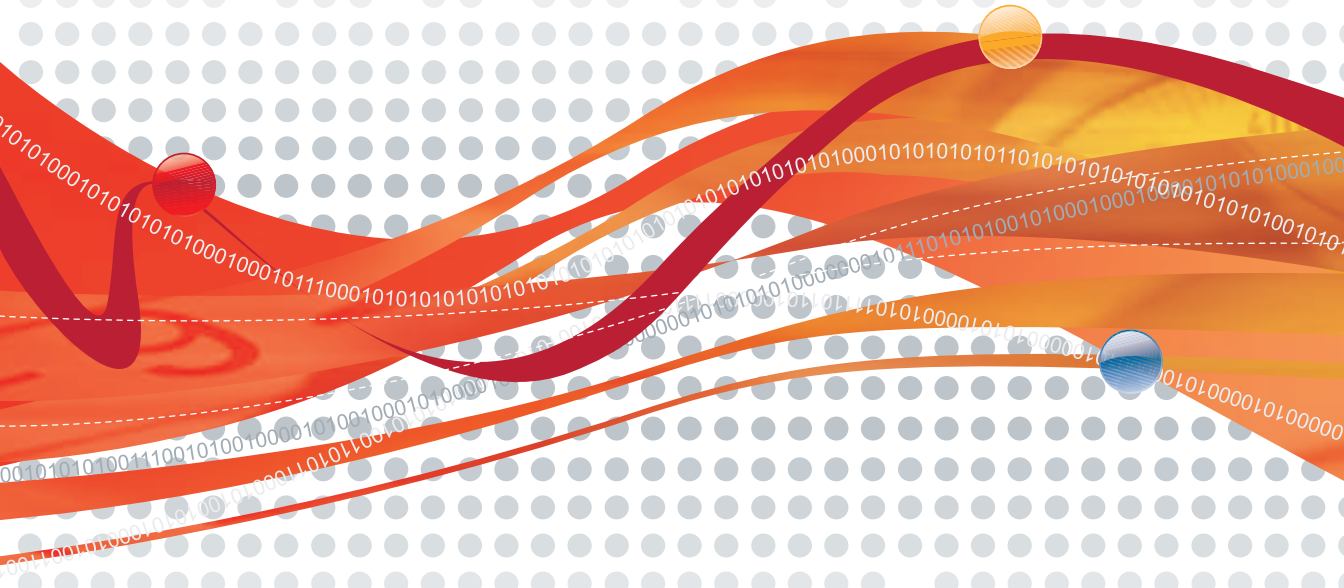
InterScan™ VirusWall™ 7

for Small and Medium Businesses

Integrated virus and spam protection for your Internet gateway

for Windows™

Quick Start Guide



Messaging Security

Web Security

Document Part Number: IVEM74092/90513

Release Date: July 2009

The Quick Start Guide for Trend Micro™ InterScan VirusWall™ introduces the main features of the software and installation instructions for your production environment. You should read it before 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 *Open* `config.xml` *and set the value of /Root/common/ActiveUpdate/notification/SuccessEnable to "1",* on page 5-6 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:

www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 1: Introducing InterScan VirusWall

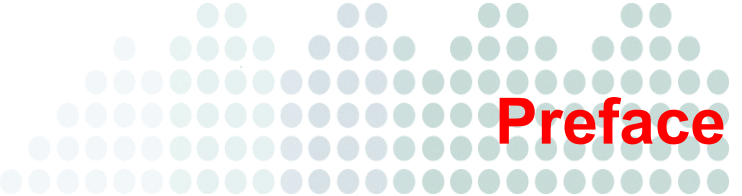
Chapter 2: Planning to Install InterScan VirusWall

Chapter 3: Installing InterScan VirusWall

Chapter 4: Using InterScan VirusWall

Chapter 5: Troubleshooting and Support

Index



Preface

The Quick Start Guide for InterScan™ VirusWall™ 7.0 for Windows provides the system administrator with the necessary information to set up, configure, and start managing an ISVW 7.0 installation.

About this Guide

The Quick Start Guide contains the following chapters:

- Chapter 1, *Introducing InterScan VirusWall* includes an overview of InterScan VirusWall (ISVW) and its features and benefits.
- Chapter 2, *Planning to Install InterScan VirusWall* includes installation planning, system requirements, and pre-installation tasks.
- Chapter 3, *Installing InterScan VirusWall* includes installation and migration procedures.
- Chapter 4, *Using InterScan VirusWall* includes a discussion of the Web management console and the menu options in the console, and basic tasks such as starting and stopping ISVW services and testing key ISVW features.
- Chapter 5, *Troubleshooting and Support* includes solutions to quick start tasks and how to obtain technical support.

InterScan VirusWall Documentation

In addition to the *Trend Micro™ InterScan VirusWall Quick Start Guide*, the documentation ISVW set includes the following:

- **Administrator's Guide**—The complete reference to managing ISVW, including product configuration and troubleshooting
- **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 and FTP protocols
- Database configuration

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 1-1. 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 InterScan VirusWall

InterScan VirusWall (ISVW) for Windows provides an all-in-one gateway antivirus, anti-spam, and content management solution for your organization's network. You do not have to install separate applications for virus protection, spam detection, or content filtering—all these functions are available in a single, easy-to-use application.

- ISVW's real-time scanning services—SMTP VirusWall, POP3 VirusWall, FTP VirusWall, and HTTP VirusWall— check for security threats in email and in the Web, and in file transfers to and from the local area network (LAN).
- ISVW 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 customers who have limited time or IT resources, yet still require real-time virus and spam prevention services.

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 full protection out of the box
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.

Chapter 2

Planning to Install InterScan VirusWall

InterScan VirusWall (ISVW) 7.0 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.

This chapter discusses installation planning, minimum and recommended system requirements, and pre-installation tasks that you need to perform.

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 with 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 with Service Pack 1 (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 the "Troubleshooting and Support" chapter in the Administrator's Guide. • 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.

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

REQUIREMENT	Description
ISVW	• Configure ISVW user identification settings to IP address and User Name (see the "Administration" chapter in Administrator's Guide) • IP address of the Domain Controller Agent computer • User account with domain administrator's privileges
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

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.

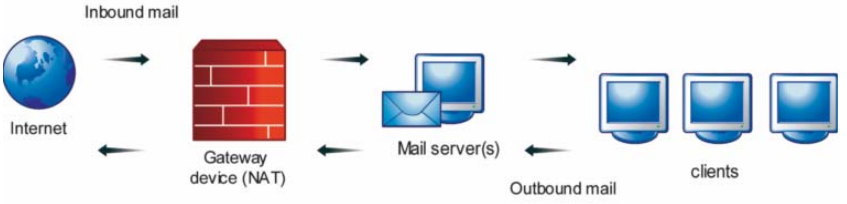
In the pages that follow, several possible installation topologies are presented, illustrating typical network setups before and after installing ISVW. Use the one that best fits your needs, or apply the principles to an installation strategy unique to your network.

SMTP

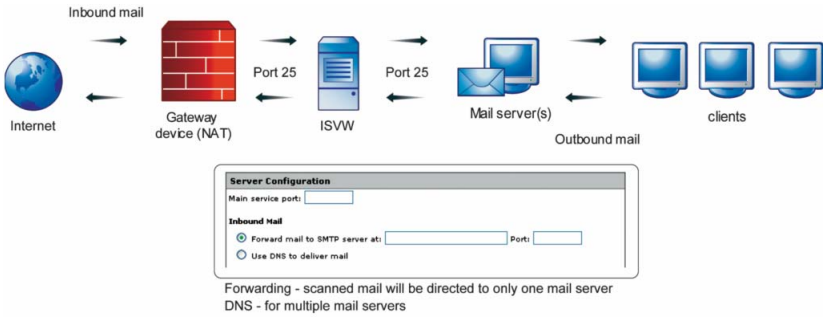
Remap the firewall's SMTP service, port 25, to the newly installed ISVW 7.0 server listening on port 25. Then use inbound mail forwarding (single server environment) or DNS (multi-server environment) to pass scanned mails to an internal mail server or servers. Ensure that the internal MX records are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

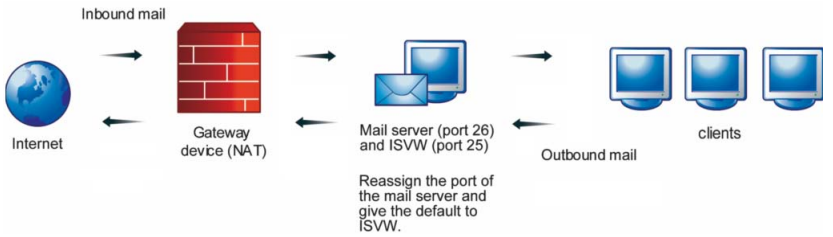


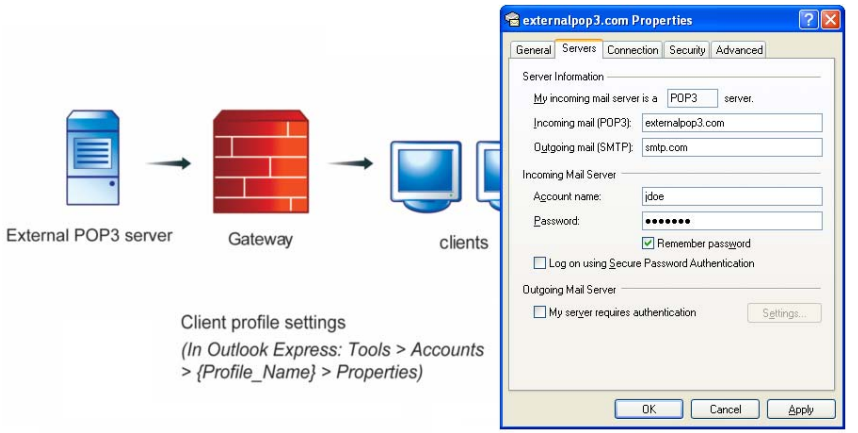
FIGURE 2-1. SMTP Installation Topologies

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

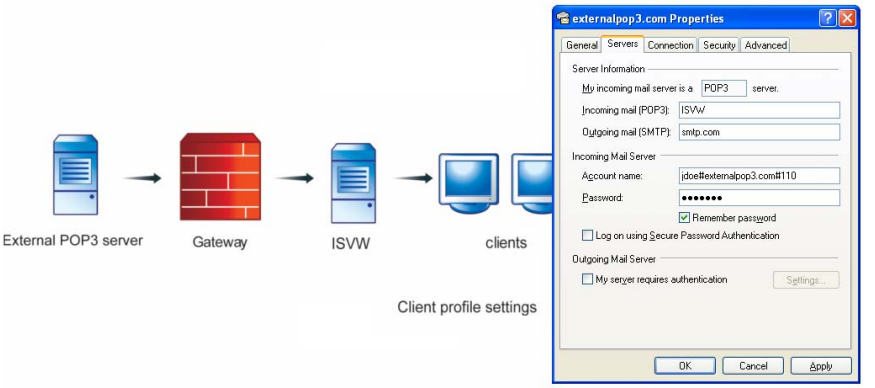


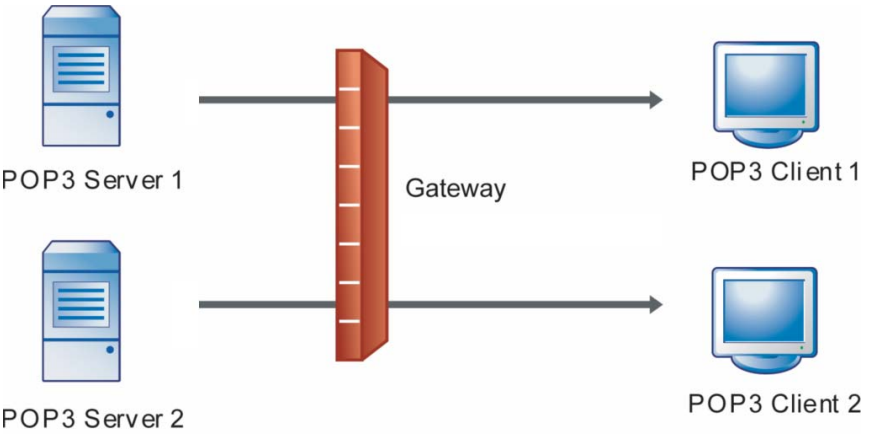
FIGURE 2-2. Typical POP3 Installation Topology

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

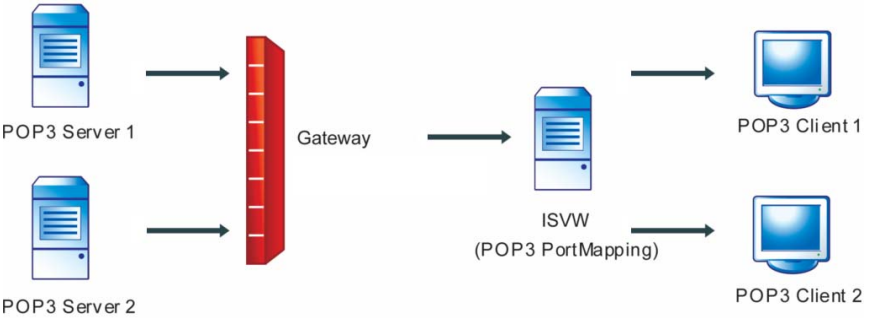


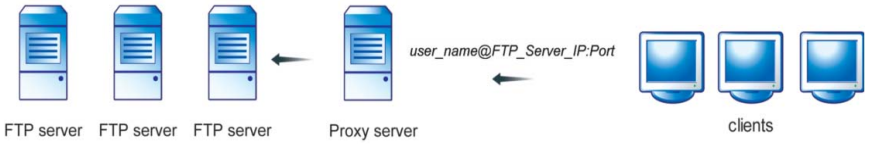
FIGURE 2-3. POP3 with ISVW Acting as a Port Mapping Server

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)

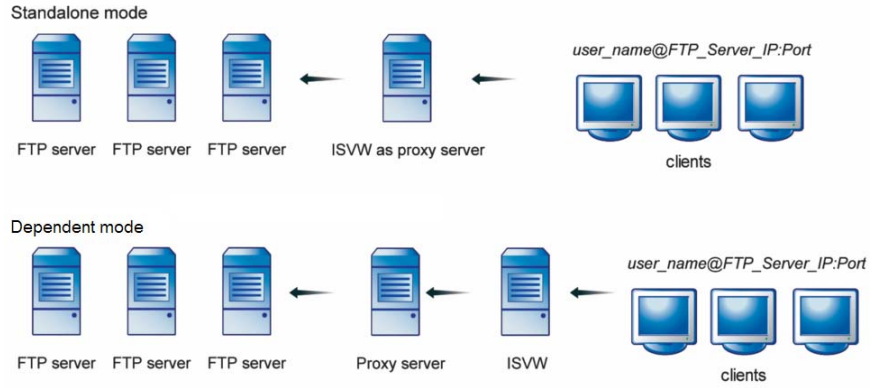
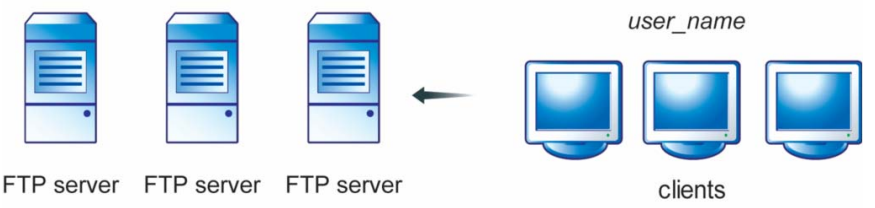


FIGURE 2-4. Installation Topology for FTP with Proxy Server

Before installing ISVW (without proxy server)



After installing ISVW 7.0 (without proxy server)

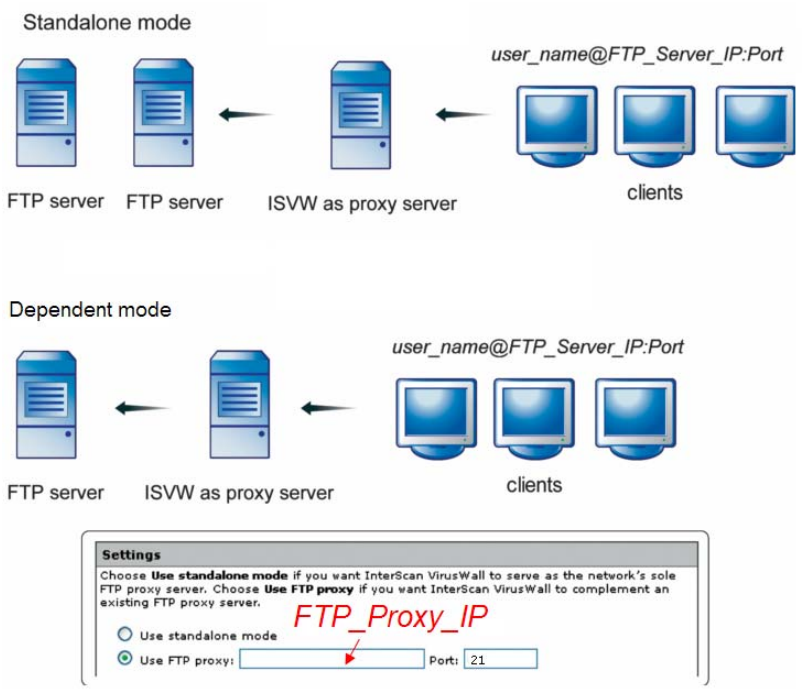


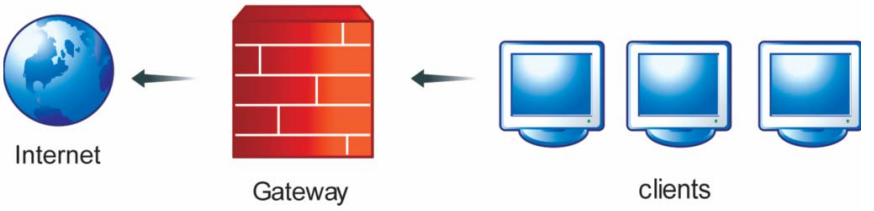
FIGURE 2-5. Installation Topology for FTP without a Proxy Server

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

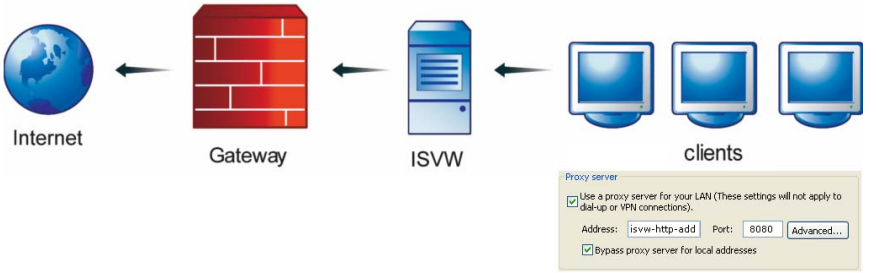
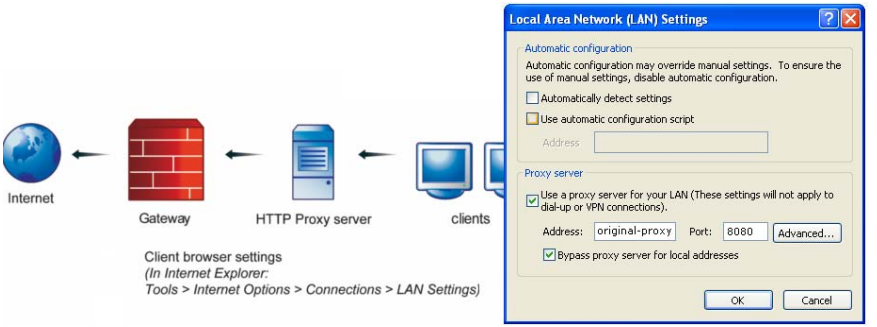


FIGURE 2-6. Installation Topology for HTTP without a Proxy Server (Standalone Mode)

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

Before installing ISVW (with proxy)



After installing ISVW (with proxy)

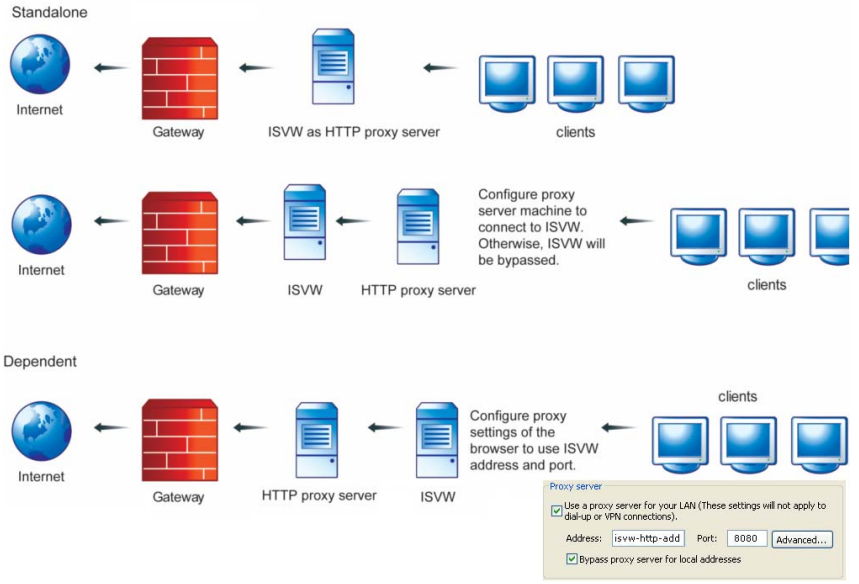
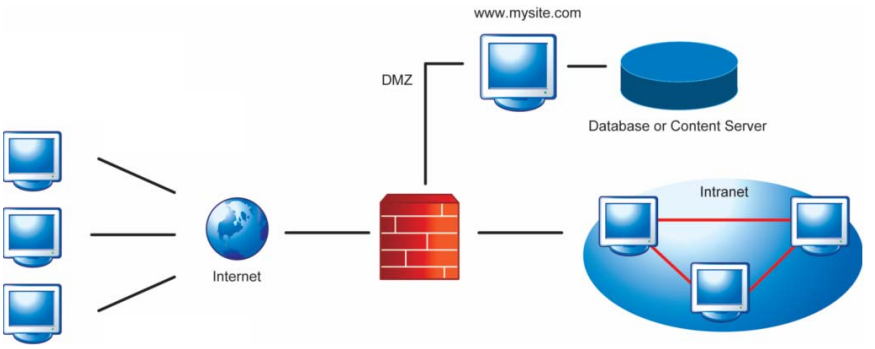


FIGURE 2-7. Installation Topology for HTTP with a Proxy Server (Dependent Mode)

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

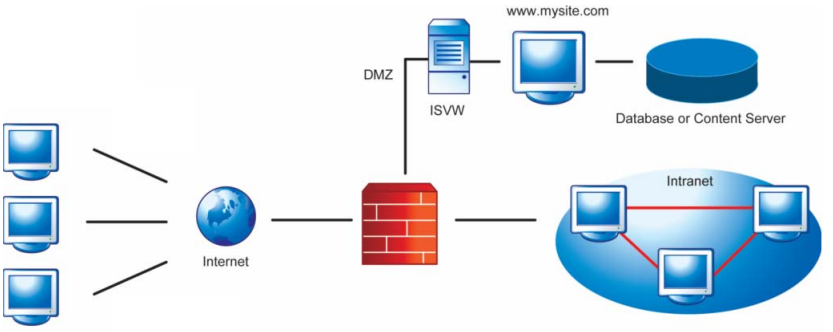


FIGURE 2-8. Installation Topology for HTTP with ISVW as a Reverse Proxy

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

Chapter 3

Installing InterScan VirusWall

InterScan VirusWall (ISVW) installation 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.

This chapter provides instructions for installing ISVW 7.0 for Windows. It also provides instructions for migration. Migration is supported for the following earlier versions of ISVW:

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

If this chapter does not provide all the information you need, refer to the Administrator's Guide.

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 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 early version settings and import them during ISVW 7.0 installation.

Installing InterScan VirusWall 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).

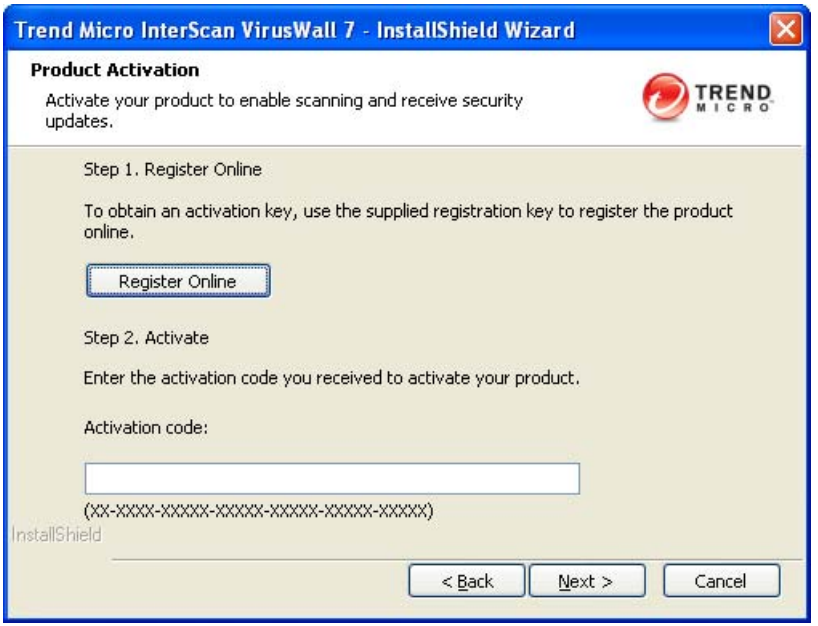
To perform a fresh ISVW installation:

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



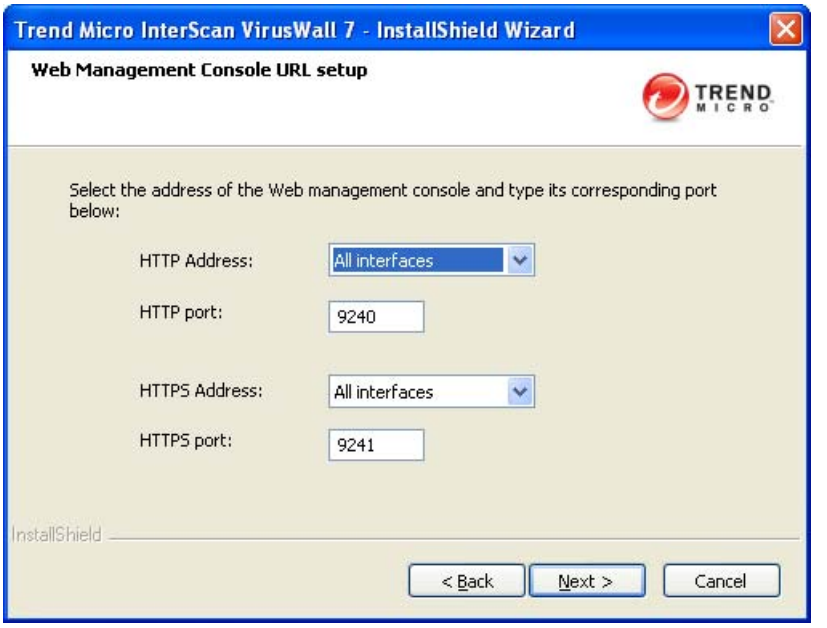
If you clicked **Next** without entering an activation code, a message appears warning you of the missing information and informing you that a 30-day trial version of ISVW 7.0 will be installed. Click **OK** to proceed with the installation.

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*.

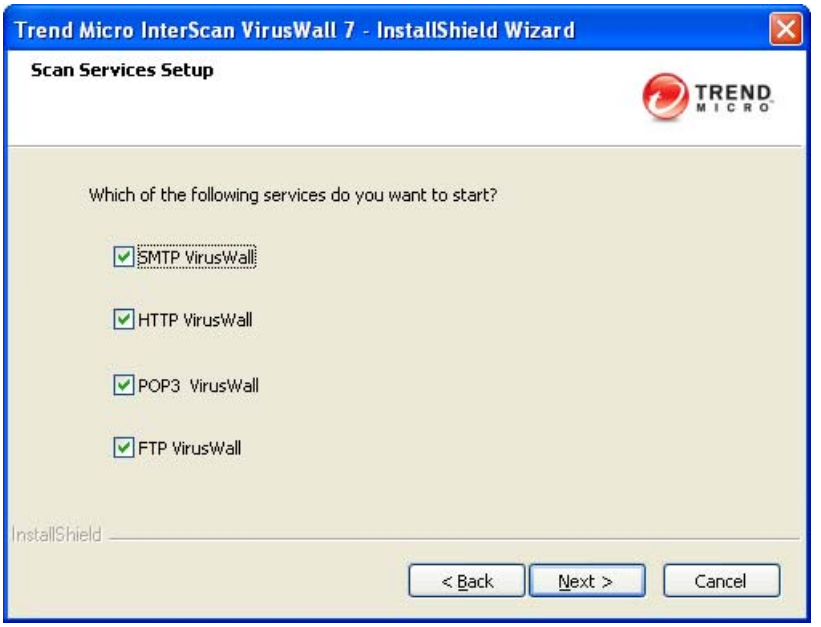
FIGURE 3-2. Web Management Console URL Setup Screen



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 as an Upgrade

ISVW supports two types of upgrades:

- Installing on a computer where an earlier version of ISVW is installed
- Installing on a new computer and migrating the configuration settings of an earlier version of ISVW

For further detail about these upgrade scenarios, see the Administrator's Guide.

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

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.

For further detail about this upgrade scenario, see the Administrator's Guide.

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.
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.
5. Click **Next**.
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.
7. To change the installation location, go in the Choose Destination Location screen, click **Browse** and then specify an alternative location.
8. When you have either accepted the default path or chosen a new destination, click **Next**.
9. In the Web Management Console Configuration screen, specify where the Web management console will bind.
10. Click **Next**.

11. In the Administrator Account screen, enter a 4- to 32-character password, confirm it, and then click **Next.**
12. In the Scan Services Setup screen, select the ISVW services that you want to start after the installation has finished and then click **Next**.
13. To block relayed emails, go in the Allowed Relay Destinations Setup screen and specify in the **Domains** field the domains that will accept inbound emails.
14. Click **Next**.
15. To help improve the Web Reputation database, go in the HTTP Web Reputation Feedback screen and select the check box to send anonymous information on infected URLs.
16. Click **Next**.
17. In the World Virus Tracking Setup screen, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.
18. Review the current settings in the Setup Confirmation screen and then click **Next**.

    When you click **Next** on the Setup Confirmation screen, a message appears indicating that the earlier version of ISVW will be uninstalled.
19. In 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 create a migration report at the beginning of installation, click **Export**. The report will display in a new window.

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 earlier 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:\ISVW\quarantine\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 6.0x quarantine files to the new location. The new quarantine files that ISVW 7.0 generates will be stored in the same path with ISVW 6.0x.

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

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 (and any eManager plug-in 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.

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 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`.
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.
8. When the Setup Type window appears, select **Migrate configuration settings from previous version on remote computer** check box.
9. Click **Next**.
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.
11. To change the installation location, go in the Choose Destination Location screen, click **Browse** and then specify an alternative location.
12. When you have either accepted the default path or chosen a new destination, click **Next**.
13. In the Web Management Console Configuration screen, specify where the Web management console will bind.
14. Click **Next**.

15. In the Administrator Account screen, enter a 4- to 32-character password, confirm it, and then click **Next.**
16. In the Scan Services Setup screen, select the ISVW services that you want to start after the installation has finished.
17. Click **Next**.
18. To block relayed emails, go in the Allowed Relay Destinations Setup screen and specify in the **Domains** field the domains that will accept inbound emails.
19. Click **Next**.
20. To help improve the Web Reputation database, go in the HTTP Web Reputation Feedback screen and select the check box to send anonymous information on infected URLs.
21. Click **Next**.
22. In the World Virus Tracking Setup screen, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.
23. Review the current settings in the Setup Confirmation screen and then click **Next**.

    When you click **Next** on the Setup Confirmation screen, a message appears indicating that the earlier version of ISVW will be uninstalled.
24. 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 create a migration report at the beginning of installation, click **Export**. The report will display in a new window.

Installing InterScan VirusWall 7.0 on a New Computer and Migrating ISVW 5.0 or ISVW 6.0x Settings

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 or ISVW 6.0, 6.01, or 6.02 is installed, you can export the settings to a file. This file will then be used during the installation process to import the saved settings to the computer where you are installing ISVW 7.0.

To install ISVW 7.0 and migrate ISVW 5.0 or ISVW 6.0x configuration settings:

1. Find and copy the migration tool.
   - For an ISVW 5.0 migration, 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.
   - For an ISVW 6.0x migration, 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:
   - For an ISVW 5.0 migration:
     ```
     isvw-migr5to7 -o [Migration_Configuration_File_Name]
     Example: isvw-migr5to7 -o c:\ISVW5-package.out
     ```
   - For an ISVW 6.0x migration:
     ```
     isvw-migr6to7 -o [Migration_Configuration_File_Name]
     Example: isvw-migr6to7 -o c:\ISVW6-package.out
     ```

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

10. To change the installation location, go to the Choose Destination Location screen, click **Browse** and then specify an alternative location.
11. When you have either accepted the default path or chosen a new destination, click **Next**.
12. In the Web Management Console Configuration screen, specify where the Web management console will bind.
13. Click **Next**.
14. In the Administrator Account screen, enter a 4- to 32-character password, confirm it, and then click **Next.**
15. In the Scan Services Setup screen, select the ISVW services that you want to start after the installation has finished.
16. Click **Next**.
17. To block relayed emails, go in the Allowed Relay Destinations Setup screen and specify in the **Domains** field the domains that will accept inbound emails.
18. Click **Next**.
19. To help improve the Web Reputation database, go in the HTTP Web Reputation Feedback screen and select the check box to send anonymous information on infected URLs.
20. Click **Next**.
21. In the World Virus Tracking Setup screen, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, and then click **Next**.
22. Review the current settings in the Setup Confirmation screen and then click **Next**.

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 create a migration report at the beginning of installation, click **Export**. The report will display in a new window.

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 earlier versions of ISVW:

- ISVW 5.0
- ISVW 6.0, 6.01, or 6.02

To migrate ISVW 5.0 or ISVW 6.0x configuration settings to a computer with ISVW 7.0 installed:

1. Find and copy the migration tool.
   - For an ISVW 5.0 migration, 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.
   - For an ISVW 6.0x migration, 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:
   - For an ISVW 5.0 migration:
     ```
     isvw-migr5to7 -o [Migration_Configuration_File_Name]
     Example: isvw-migr5to7 -o c:\ISVW5-package.out
     ```
   - For an ISVW 6.0x migration:
     ```
     isvw-migr6to7 -o [Migration_Configuration_File_Name]
     Example: isvw-migr6to7 -o c:\ISVW6-package.out
     ```

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.

   See *Starting and Stopping InterScan VirusWall* on page 4-24.

Verifying a Successful Installation

Use Windows™ Task Manager to verify that ISVW has been installed successfully and is working properly. If you have installed ISVW correctly and it is functioning properly, you will see the following eight (8) ISVW services running in Windows Task Manager.

TABLE 3-1. ISVW default services

Service	Service Description
isvw-svr.exe	Responsible for all protocol notifications
isvw-smtp.exe	Responsible for scanning SMTP streams including virus scanning, spam, and content filter
isvw-scan.exe	Responsible for scanning POP3 streams including virus scanning, spam, and content filter
isvw-pop3.exe	Responsible for handling POP3 protocol commands
isvw-main.exe	Responsible for main ISVW processes. It acts as a watch dog, ensuring that ISVW processes keep running. It also performs the ActiveUpdating task.
isvw-http.exe	Responsible for scanning HTTP streams including virus scanning, URL filtering, URL blocking, and Anti-phishing
isvw-ftp.exe	Responsible for scanning HTTP streams including virus scanning.
isvw-agent.exe	Agent responsible for registering to TMCM server

Note: Disabling any of the protocols from the summary screen of the Web console will cause the corresponding service to stop running. In this situation, the service will not be viewable in Windows Task Manager.

Post-Installation Tasks

After installing ISVW, you can immediately perform a number of tasks to ensure that everything is set up and working properly.

Note: Refer to the online help for instructions on how to accomplish the tasks.

1. If not completed during installation, register and activate InterScan VirusWall 6, or begin your 30-day evaluation period.
2. Enable and then begin virus scanning, spam detection, and content filtering.

3. Update the pattern files and scan engine and set up an update schedule for the virus pattern file, scan engine, and anti-spam rules and engine.
4. Set the notification settings, including the notification server, port, administrator email address, and preferred character set.
5. Adjust the default configuration of the product to meet the needs of your organization. Depending on the services installed and the proxy servers on the system, the following information may be needed when you configure InterScan VirusWall 6 after installation:
   - IP address and port number of the current SMTP server
   - IP address and port number of the current POP3 server
   - IP address and port number of the current HTTP proxy server
   - Port number that InterScan VirusWall 6 will use if it is set up as the HTTP proxy server
   - IP address and port number of the current FTP proxy server
   - Port number that InterScan VirusWall 6 will use if it is set up as the FTP proxy server
6. **Tasks**:
   a. Configure outbreak alerts.
   b. If you need a proxy to connect to the Internet, configure the proxy information for Registration/Activation, ActiveUpdate and World Tracking Center services.
   c. If the SMTP protocol is enabled:
      - Configure inbound and outbound SMTP traffic.
      - Configure policies and notifications for SMTP scanning, IntelliTrap, anti-phishing, anti-spam, anti-spyware, and content filtering.
   d. If the HTTP protocol is enabled:
      - Configure your HTTP working mode.
      - Configure policies and notifications for HTTP scanning, anti-phishing, anti-spyware, URL blocking and URL filtering settings.
   e. If the FTP protocol is enabled:
      - Configure your FTP working mode.

- Configure policies and notifications for FTP scanning and anti-spyware.

f. If the POP3 protocol is enabled:

- Configure POP3 IP addresses and connections.
- Configure policies and notifications for POP3 scanning, IntelliTrap, anti-phishing, anti-spam, anti-spyware, and content filtering.

g. Obtain the EICAR test file to determine if your installation is working properly.

- If the SMTP protocol is enabled, test SMTP inbound and outbound scanning.
- If the SMTP protocol is enabled, test SMTP inbound and outbound content filtering.
- If the POP3 protocol is enabled, test POP3 inbound scanning and content filtering settings.
- If the HTTP protocol is enabled, test HTTP download and upload scanning.
- If the HTTP protocol is enabled, test HTTP URL blocking and URL filtering.
- If the FTP protocol is enabled, test FTP download and upload scanning.

7. Install additional instances of InterScan VirusWall 6 to the network if desired.

Chapter 4

Using InterScan VirusWall

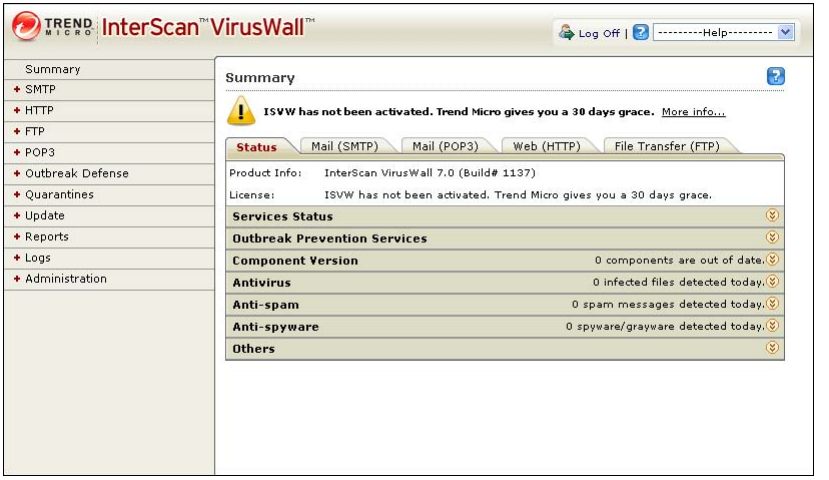
In this chapter, you will familiarize yourself with InterScan VirusWall (ISVW) using the Web management console, and learn about tasks such as starting and stopping the various ISVW services, and testing key ISVW features.

Note: The online help discusses all the ISVW tasks that you can perform. It also provides a list of best practices to help you manage ISVW optimally.

InterScan VirusWall Web Management Console

The main menu of the Web Management console consists of ten menu items. Except for Summary, each of the console's menu items has several submenu items. See *Navigating the Console* on page 4-3 for an overview of the different menu items and the various tasks you can perform on each screen that opens when you click a submenu item.

FIGURE 4-1. ISVW Web management console showing the Summary screen



Accessing the 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 console and confirm the settings.

Use any of the following browsers to access the console:

- Microsoft Internet Explorer 6.0, 7.0, and 8.0
- Firefox 2.0 and 3.0

To access the console:

1. Open a Web browser, then type the ISVW URL followed by the port number that you set during the installation. The default port numbers are 9240 (HTTP) and 9241 (HTTPS).
   - http://IP address:port number
   - https://IP address:port number

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

2. Type the password you specified during installation and then click **Log On**.

   The Summary screen of the Web management console appears.

Navigating the Console

This section describes the menu items on the Web Management console and highlights the tasks you can perform from the different screens. For information on performing these tasks, see the *InterScan VirusWall Administrator's Guide*.

Summary

The Summary menu item provides a quick overview of the status of ISVW and its four services. When you log on to the console, the Summary screen opens by default. To open the Summary screen, click **Summary**; the Status tab is pre-selected.

FIGURE 4-2. Summary screen

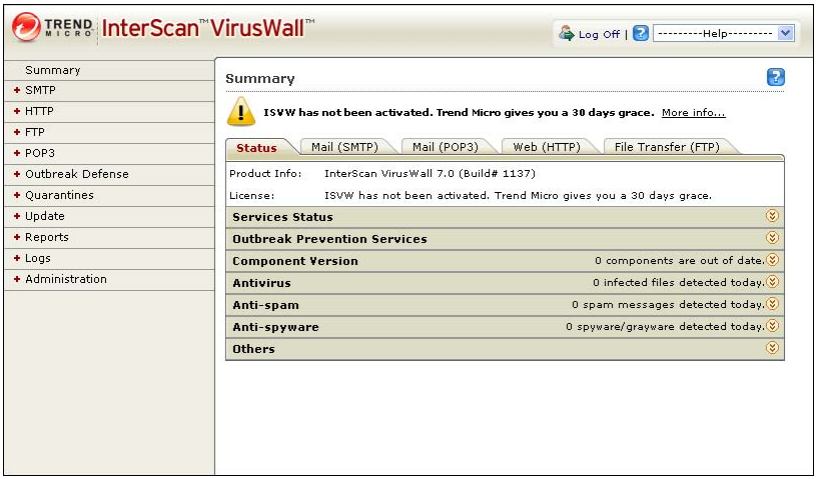


TABLE 4-1. Summary screen tabs

Tab	Available Information	Tasks
Status	The current status of each of the four protocols. Your product and license information Outbreak Prevention Services status Current versions of pattern files and engines The following statistics: • Files scanned for viruses, spam, spyware/grayware • URLs and content filtered • Files infected with viruses (includes files detected by IntelliTrap) • Spam messages • Spyware/Grayware files • Phishing incidents	Update to the latest versions of ISVW components Roll back the previous versions of pattern files

TABLE 4-1. Summary screen tabs (Continued)

Tab	Available Information	Tasks
Mail (SMTP)	Number of viruses, spyware, spam messages, and phishing messages SMTP scanning detected in incoming and outgoing email communication	Enable or disable SMTP traffic
Mail (POP3)	Number of viruses, spyware, spam messages, and phishing messages POP3 scanning detected in incoming email communication	Enable or disable POP3 traffic
Web (HTTP)	The following HTTP scanning statistics: • Virus/malware detection • Spyware/Grayware detection • URL blocking/anti-phishing • URL filtering	Enable or disable HTTP traffic
File Transfer (FTP)	FTP scanning statistics for virus/malware and spyware/grayware detection	Enable or disable FTP traffic

SMTP

The SMTP menu item allows you to configure SMTP security settings and rules.

FIGURE 4-3. SMTP Scanning screen with the Target tab selected

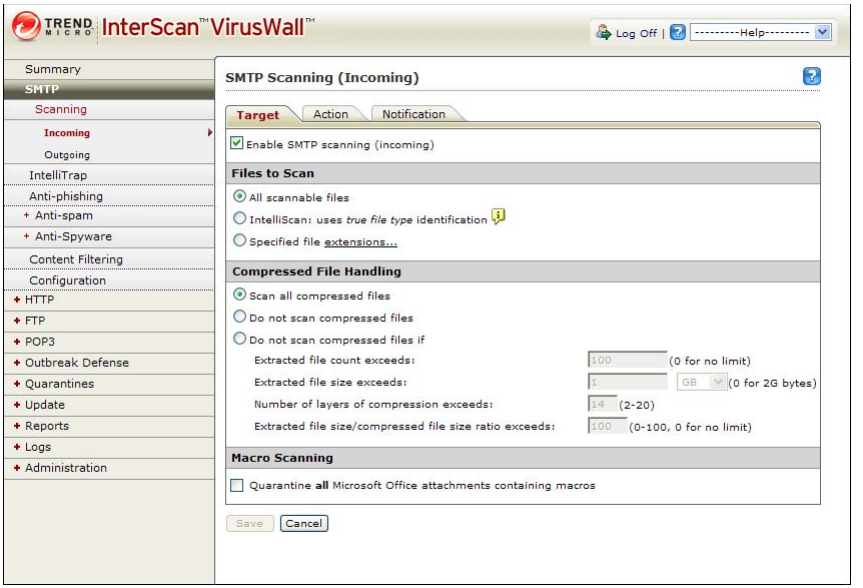


TABLE 4-2. Submenu items under SMTP

Submenu	Description	Tasks
Scanning >Incoming >Outgoing	Provides real-time incoming and outgoing scanning of SMTP traffic	Enable or disable SMTP scanning for incoming and outgoing SMTP email messages Target the attachment types to scan Determine the action to take for infected files (clean, delete, move, or block) For both incoming and outgoing mail, customize the notification sent to specific individuals (administrator, sender, or recipient) or the inline stamp on an email when a virus is detected

TABLE 4-2. Submenu items under SMTP (Continued)

Submenu	Description	Tasks
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable SMTP IntelliTrap Determine the action to take against Bots detected by IntelliTrap (Quarantine, Delete, or Pass) Customize the notification message an administrator, sender, or recipient receives when a heuristic scan detects a security risk in a compressed file
Anti-phishing	Detects phishing attempts in SMTP mail	Enable or disable SMTP anti-phishing Define the action to take for all messages containing links to known phishing sites (quarantine, delete, or deliver message) Customize the notification message the administrator or recipient receives when a phishing message is detected Report a potential phishing URL to TrendLabs
Anti-spam >Content Scanning) >Email Reputation Services)	Detects spam messages sent through your SMTP email server	Enable or disable SMTP anti-spam content scanning and email reputation services Tune the spam detection rate to Low, Medium, or High, or by category (Commercial, Health, Religion, and so on) Define keyword exceptions (messages containing identified keywords will not be considered spam) or Approved or Blocked Senders by email address or domain names Specify the action to take for spam messages based on their confidence level Customize the notification message an administrator or recipient receives when spam is detected

TABLE 4-2. Submenu items under SMTP (Continued)

Submenu	Description	Tasks
Anti-spyware >Incoming >Outgoing	Detects spyware in incoming and outgoing SMTP email messages and allows you to perform specific actions upon it	Enable or disable SMTP anti-spyware scanning for incoming and outgoing SMTP email messages Specify filenames or filename extensions that will be excluded from spyware search Search for spyware/grayware Target the kind of spyware/grayware you wish to scan Determine the action to take against spyware (Quarantine, Delete, or Pass) Automatically notify selected recipients whenever spyware is detected during SMTP scanning
Content Filtering	Provides real-time monitoring and control of information that enters or leaves the network via the SMTP server	Enable or disable SMTP Content Filtering Specify keyword and attachment filters to evaluate and control the delivery of email messages on the basis of the message content itself
Configuration	Allows you to configure the way the ISVW server—as a proxy server—routes incoming and outgoing mail through your SMTP server, while defining certain limits and constraints	Specify the main service port Specify how ISVW forwards inbound mail and delivers outbound mail Track processed messages Queue inbound or outbound mails Configure the number of simultaneous client connections, size of inbound/outbound messages, frequency of message sending attempts, and other advance settings

HTTP

The HTTP menu item provides you with features to help maintain HTTP gateway security.

FIGURE 4-4. HTTP Scanning screen with the Target tab selected

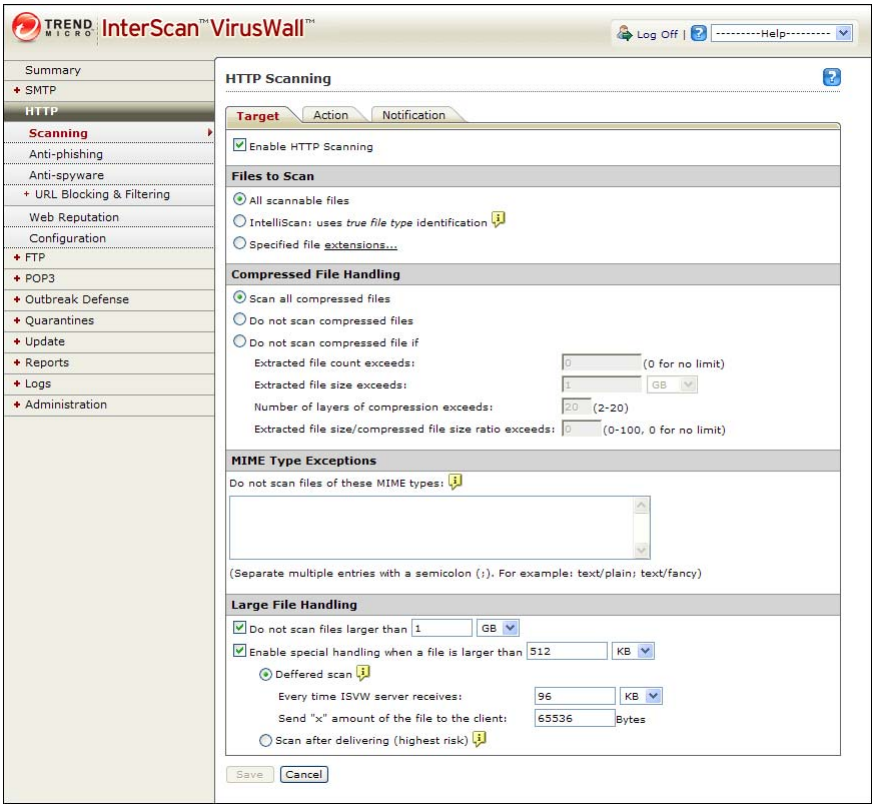


TABLE 4-3. Submenu items under HTTP

Submenu	Description	Tasks
Scanning	Lets you determine how ISVW scans HTTP traffic for viruses and other security risks in uploads and downloads	Enable or disable HTTP scanning Target the types of files to scan List MIME Type Exceptions Specify how ISVW handles large files to prevent performance issues and browser timeouts Determine actions for infected files (Clean, Quarantine, Block, or Pass) Customize the message in the user's browser when ISVW detects an infected file
Anti-phishing	Lets you determine how ISVW handles phishing attempts initiated while browsing the Internet	Enable or disable HTTP anti-phishing Set categories to block URLs (for example, phishing, spyware, virus accomplice, and disease vector sites) Define actions for all known phishing sites (block or allow) Customize the message in the user's browser when a known phishing site is detected Submit a potential phishing URL to TrendLabs
Anti-spyware	Scans HTTP traffic to detect many types of malware uploads and downloads	Enable or disable HTTP anti-spyware Create exclusion lists for spyware/grayware Search for spyware/grayware Target the kind of spyware/grayware to scan Set the action to take when spyware/grayware is detected (block, quarantine, or allow) Customize the message in the user's browser when spyware/grayware is detected

TABLE 4-3. Submenu items under HTTP (Continued)

Submenu	Description	Tasks
URL Blocking & Filtering	Blocks access to Web sites with undesirable content through a user-configured list Allows access to certain URLs by adding them to an exception list	Enable or disable HTTP URL blocking Define matching URL lists (defined through a Web site, URL keyword, IP address, or string), one for URLs that will be blocked, and another for URLs excluded from blocking Import lists of blocked or exempted sites Customize the message in the user's browser when a blocked URL is accessed
	Lets you set the rules by which URL categories are filtered	Enable or disable HTTP URL filtering Set the time when the rules apply (during work time, during leisure time)
	Defines how URL filtering is applied across the URL categories in the ISVW database	Move a URL subcategory to another category (for example, Adult/Mature Content from “Company Prohibited Sites” to “Not Work Related”) Create or import URL Filtering Exception lists matched by Web site, URL keyword, or string, even though the URL is classified in a prohibited content category Designate the day and time the settings apply Submit a URL to TrendLabs for reclassification
Web Reputation	Queries a URL request and returns URL category information Web Reputation also assigns reputation scores to URLs.	URL Filtering uses the category information in its filtering process. ISVW uses a URL reputation score to take certain action, depending on whether this score is below or above the user-specified sensitivity level.
Configuration	Allows you to specify configuration settings for your HTTP server	Determine if you want ISVW to operate in standalone, dependent, or reverse proxy mode Specify the HTTP listening port Specify anonymous FTP over a specified HTTP logon email Allow logging of HTTP requests

FTP

The FTP menu item provides you with features to help secure file transfers to and from your FTP server.

FIGURE 4-5. FTP Scanning screen with the Target tab selected

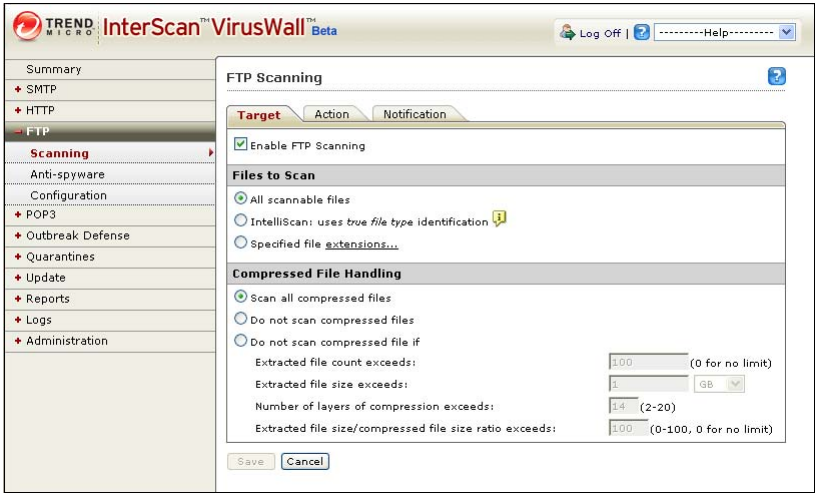


TABLE 4-4. Submenu items under FTP

Submenu	Description	Tasks
Scanning	Checks all or specified types of files for viruses and other malware, including individual files within a compressed volume	Enable or disable FTP scanning Determine the files you want to scan Designate if and how attached compressed files are scanned Specify the action to take on infected files (Clean, Quarantine, Block, or Pass) Customize the notification message an administrator or user receives when an infected file is detected

TABLE 4-4. Submenu items under FTP (Continued)

Submenu	Description	Tasks
Anti-spyware	Allows you to block spyware/grayware during FTP file transfers	Enable or disable FTP anti-spyware Create an Exclusion list for spyware/grayware Search for spyware/grayware Scan for spyware/grayware according to specific categories Determine the action to take when spyware/grayware is detected (Block, Quarantine, Allow) Customize the message in the user's browser when spyware/grayware is detected
Configuration	Lets you determine how your FTP server is set up	Choose between standalone or FTP proxy mode • Choose standalone mode if there is no FTP proxy server on the network and you want FTP VirusWall to serve as the system's FTP proxy server. • Choose FTP proxy if there is an existing FTP proxy server that you want to continue using. Enable PASV mode and specify the FTP service port Determine the maximum connections allowed Designate the number of bytes to send versus those received (to prevent browser timeouts) Customize the greeting to send when connection is established

POP3

With minor differences, the POP3 menu item is nearly identical to the SMTP menu item. The exceptions are the Scanning and Configuration submenu items.

FIGURE 4-6. POP3 Scanning screen with the Target tab selected

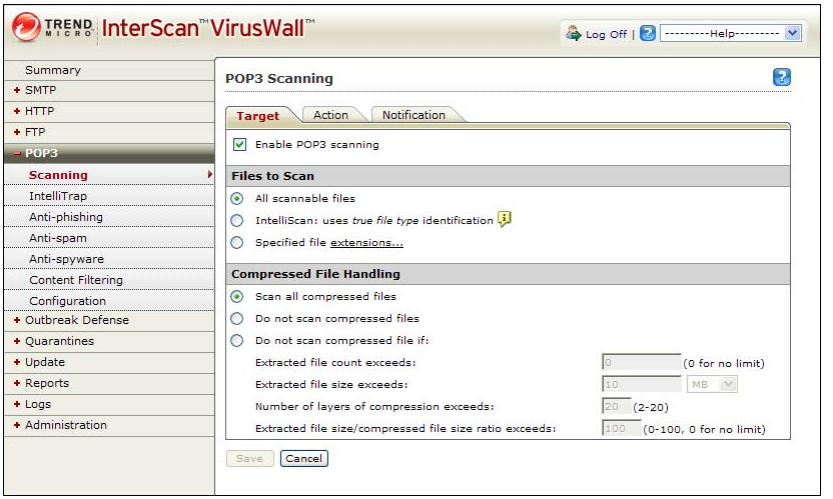


TABLE 4-5. Submenu items under POP3

Submenu	Description	Tasks
Scanning	Provides real-time scanning of POP3 traffic	Enable or disable POP3 scanning Determine the attachments to scan Designate if and how attached compressed files are scanned Determine the action to take for infected files (clean, delete, move, or block) Customize the notification sent to specific individuals (administrator or recipient) or the inline stamp on an email when a virus is detected

TABLE 4-5. Submenu items under POP3 (Continued)

Submenu	Description	Tasks
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable POP3 IntelliTrap Take action on Bots detected by IntelliTrap (Quarantine, Delete, or Pass) Determine the action to take against Bots detected by IntelliTrap (Quarantine, Delete, or Pass) Customize the notification message an administrator or recipient receives when a heuristic scan detects a security risk in a compressed file
Anti-phishing	Detects phishing attempts in POP3 mail	Enable or disable POP3 anti-phishing Define the action to take for all messages containing links to known phishing sites (quarantine, delete, or deliver message) Customize the notification message the administrator or recipient receives when a phishing message is detected Report a potential phishing URL to TrendLabs
Anti-spam	Detects spam messages sent through your POP3 email server	Enable or disable POP3 anti-spam Tune the spam detection rate to Low, Medium, or High, or by category (Commercial, Health, Religion, and so on) Define keyword exceptions (messages containing identified keywords will not be considered spam) or Approved or Blocked Senders by email address or domain names Customize the notification message an administrator or recipient receives when spam is detected

TABLE 4-5. Submenu items under POP3 (Continued)

Submenu	Description	Tasks
Anti-spyware	Detects incoming spyware and allows you to perform specific actions upon it	Enable or disable POP3 Anti-spyware Specify filenames or filename extensions that will be excluded from spyware search Search for spyware/grayware Target the kind of spyware/grayware you wish to scan Determine the action to take against spyware (Quarantine, Delete, or Pass) Automatically notify selected recipients whenever spyware is detected during POP3 scanning
Content Filtering	Provides real-time monitoring and control of information that enters or leaves the network via the POP3 server	Enable or disable POP3 Content Filtering Specify keyword and attachment filters to evaluate and control the delivery of email messages on the basis of the message content itself
Configuration	Allows you to configure the way the ISVW's POP3 proxy server handles POP3 traffic	Specify the POP3 IP address the ISVW POP3 proxy server binds to Specify the number of simultaneous local connections allowed, the port POP3 clients will use to connect to ISVW (the default port is 110), and the settings for secure password authentication

Outbreak Defense

Trend Micro provides Outbreak Prevention Services (OPS) to help you contain a threat while TrendLabs is developing a solution.

FIGURE 4-7. Outbreak Defense Current Status screen

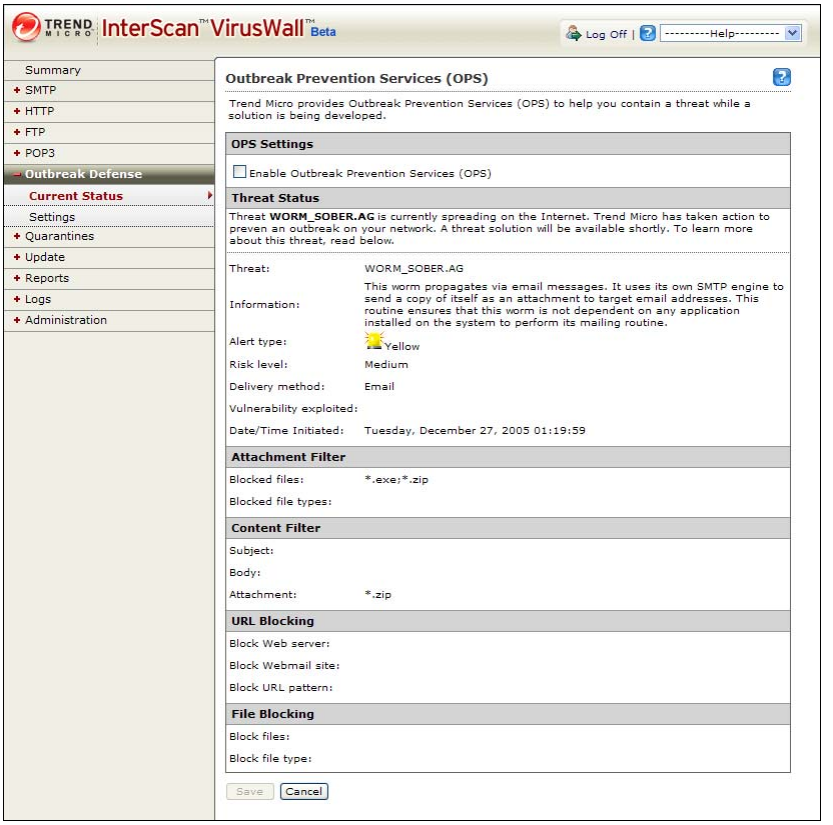


TABLE 4-6. Submenu items under Outbreak Defense

Submenu	Description	Tasks
Current Status	Informs you of the active OPS policies being enforced	Enable or disable OPS View the OPS status

TABLE 4-6. Submenu items under Outbreak Defense (Continued)

Submenu	Description	Tasks
Settings	Lets you view and modify OPS settings	Manually change the default expiration time of OPS policies

Quarantines

The Quarantines menu item allows you to manage files quarantined by ISVW.

FIGURE 4-8. Quarantine Query screen

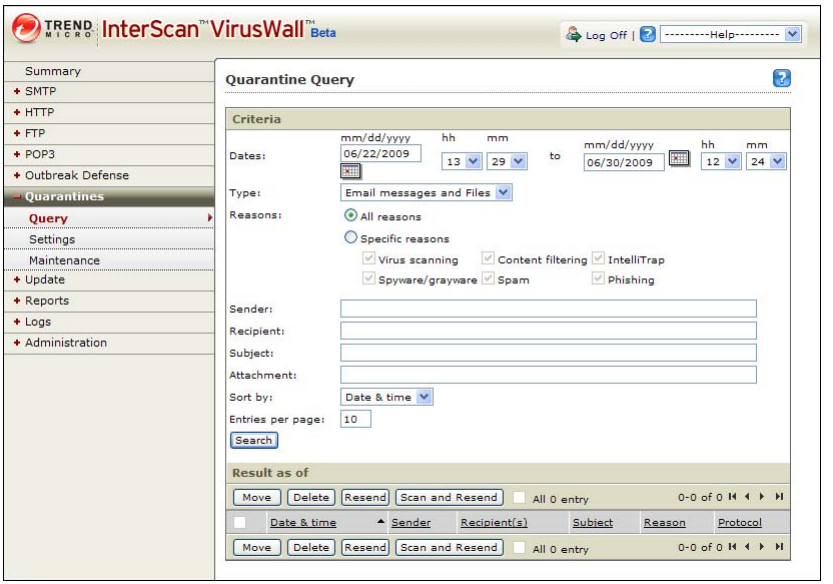


TABLE 4-7. Submenu items under Quarantines

Submenu	Description	Tasks
Query	Provides details regarding SMTP/POP3 quarantined email messages and attachments	Specify the query criteria by dates, type, reasons, sender, recipient, subject, and attachment Order the sort result by any of the above criteria, while limiting the number of entries per page
Settings	Allows you to modify the quarantine directories	Modify the quarantine directories for SMTP, HTTP, POP3, and FTP quarantined items
Maintenance	Allows you to determine how long to store infected files in the Quarantine directory before ISVW deletes them	Delete quarantined files Schedule automatic deletion times

Update

Because new malicious programs and offensive Web sites are developed and launched every day, ISVW provides both on-demand and automated methods to keep your software updated with the latest pattern files, scan engine, and URL filtering database without interrupting your network services or requiring you to reboot your computers. It polls the ISVW ActiveUpdate server directly, then downloads the updates either manually or on a schedule.

FIGURE 4-9. Manual Update screen

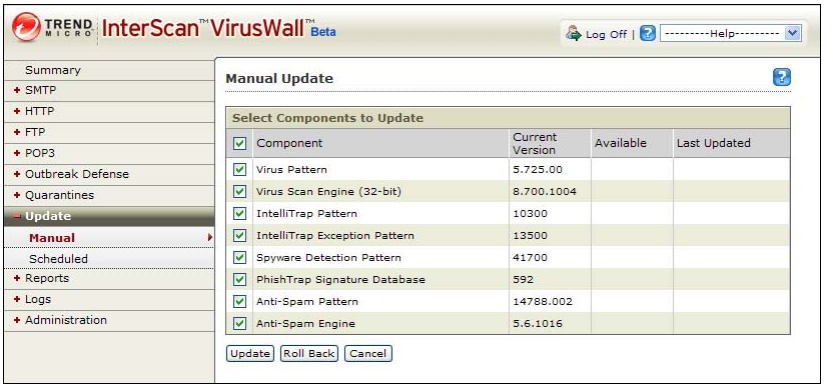


TABLE 4-8. Submenus under Update

Submenu	Description	Tasks
Manual	Allows you to update your components on-demand	Select the components to update Roll back selected components to the previous update
Scheduled	Allows you to schedule a regular interval for updating ISVW components	Enable or disable the scheduled update function Select the components to update Set an update schedule

Logs

The Logs menu item allows you to query incidents of security threats that ISVW has detected.

FIGURE 4-10. Log Query screen

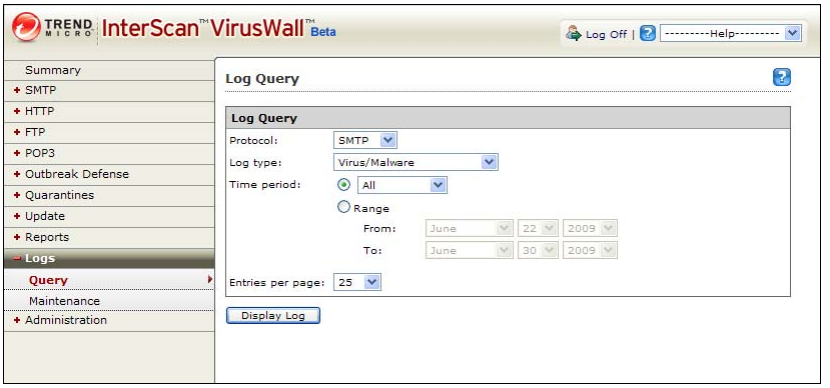


TABLE 4-9. Submenu items under Logs

Submenu	Description	Tasks
Query	Lets you query the automatic logging feature in ISVW	Query by protocol, log type, and time period Designate the number of entries per page that will be displayed Browse the log using a paging tool and re-specify how many items (10, 25, 50, 100) will be listed on a page Export the log query result as a text, Excel or XML file
Maintenance	Lets you delete old logs according to specific criteria	Specify the target logs you want to delete Delete logs older than *n* days Enable or disable automatic purging of target logs

Local Reports

Reports in 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

FIGURE 4-11. All Reports Screen

TABLE 4-10. Submenu items under Reports

Submenu	Description	Tasks
All Reports	Enables you to create a new report profile	Specify the report profile name and whether you want to enable the report profile. Select the report options you want as part of the report profile. Specify when the report should be generated. Specify the report frequency. Modify an existing report profile. Delete a report profile.
Maintenance	Enables you to specifying the maximum amount of reports kept in ISVW.	Specify the maximum amount of reports kept in ISVW.

Administration

The Administration menu item allows you to manage the notification settings, password, license, and proxy settings of your ISVW installation. It also allows you to take part in Trend Micro's World Virus Tracking Program.

FIGURE 4-12. Notification Settings screen

TABLE 4-11. Submenu items under Administration

Submenu	Description	Tasks
Control Manager Settings	Allows administrators to use the Control Manager server and Web console to manage ISVW	Register ISVW to or unregister ISVW from the Trend Micro Control Manager server Specify settings for registering ISVW to a Trend Micro Control Manager server
Notification Settings	Determines the settings that will be used when sending email notifications from ISVW	Specify the following settings: • SMTP server • Port • Administrator email address • Preferred character set for receiving notifications • Sender's email address for notifications

TABLE 4-11. Submenu items under Administration (Continued)

Submenu	Description	Tasks
Password	Allows you to change the password you use to log on to ISVW	Specify the old password, the new password, and a new password confirmation to change your current password
Product License	Displays information about your maintenance agreement and product license for ISVW	View license upgrade instructions View license online Enter a new Activation Code Update the information on the screen
Proxy Settings	If using a proxy server to connect to the Internet, lets you specify the settings used to update the pattern file, engine, and license	Enable or disable the proxy server Determine the proxy settings Test your connection
User Identification	Can identify users through IP addresses or by user/group names using proxy authorization	Allows you to identify the user roles, apply group HTTP access rules, and create URL filtering and blocking policies that are user- or group-specific
World Virus Tracking	Trend Micro's program for consolidating virus scanning results from customers worldwide, compiling real-time statistics, and displaying them on the Virus Map	Choose whether to participate in the World Virus Tracking Program or not View the typical sample data sent to TrendLabs View virus trends for each continent and selected countries

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. This section provides instructions for testing the antivirus and content filtering features.

Antivirus Testing Using the EICAR Test Virus

The European Institute for Computer Antivirus Research (EICAR) has developed a test "virus" you can use to test your ISVW installation and configuration. The test virus is an inert text file whose binary pattern is included in the virus pattern file of most antivirus vendors. It is *not* a virus and does not contain any program code. It will cause no harm and will not replicate.

Once on your machine, you can use the test virus to simulate a virus infection. You can then observe ISVW's virus clean/deletion features. ISVW will take action on the EICAR test file, a zipped EICAR test file, and an EICAR test file zipped twice. The incident will be logged in the SMTP Virus Log.

In the following section, you will test the antivirus capability of the SMTP VirusWall. Once familiar with SMTP VirusWall testing, you can proceed and test the other protocols.

To obtain the test virus, do any of the following:

- Download the file from the following URLs:
  - http://www.trendmicro.com/vinfo/testfiles/
  - www.eicar.org/anti_virus_test_file.htm

Note: You can also download a zipped EICAR test file (eicar_com.zip), and an EICAR test file zipped twice (eicarcom2.zip) from the EICAR Web site.

- Create your own EICAR test virus by typing the following into a text file, and then naming the file "eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FI
LE!$H+H*
```

To test ISVW using the EICAR test virus:

1. Send an email message with the eicar.com, eicar_com.zip, and eicarcom2.zip files enclosed. Use the email client you designated to send email.
2. Receive the email. Use the email client (or its equivalent) you designated to receive email.

   When you open an attachment, you will get a message indicating that it is not cleanable and was therefore deleted.
3. Check the SMTP Virus Log.
   a. Open the Web management console and click **Logs > Query**. The Log Query screen appears.
   b. Select from the following popup menu settings:
      - Protocol: SMTP
      - Log type: Virus/Malware
      - Time period: All
   c. Click **Display Log**. The SMTP Virus Log screen appears.
   d. Review the details for the test virus log entries.

Content Filtering

Test the SMTP content filtering feature by sending an email message whose subject and content have a certain keyword that will be blocked. The email will be quarantined and the incident will be logged in the SMTP Keyword Filter Log and the Quarantines Query.

Note: After testing SMTP content filtering, you can test the POP3 content filtering feature using the same method described in this section.

To test the content filtering feature:

1. In the Web management console, click **SMTP > Content Filtering**. On the **Target** tab, go to the Keywords section, type "sex", and click **Add**. The keyword "sex" will be added to the list on the right.
2. Send an email message with the word "sex" in the **Subject** and **Message** fields. Use the email client you designated to send email, or its equivalent.

   For example:

   To: jane@trendsmb.com

   Subject: Sex in "Last Tango in Paris"

   Message field:
   Hello Jane,
   "Last Tango in Paris" is a sexually explicit film.

   Best regards,
   John

3. Receive the email message. Use the email client you designated to receive email, or its equivalent.

   The email will not appear because it has been filtered.
4. Check the SMTP Keyword Filter Log.
   a. Open the Web management console and click **Logs > Query**. The Log Query screen appears.
   b. Select from the following popup menu settings:
      - Protocol: SMTP
      - Log type: Keyword Filter
      - Time period: All
   c. Click **Display Log**. The SMTP Keyword Filter Log screen appears.
   d. Review the details for the content filtering log entries, specifically entries in the Subject column with the term "sex".

5. Query the ISVW quarantine.
   a. In the Web management console, click **Quarantines** > **Query**. The Quarantine Query screen appears.
   b. Under Criteria, narrow down your query by typing the date you sent the test email, the email address of the sender in step 1, the email address of the recipient in step 2, and "sex" as the subject.
   c. Click **Query**. The query will execute and display the results.

      The Quarantine Query Results panel shows the date and time the email was quarantined, the sender and recipient email addresses, the subject of the email, and the reason it was quarantined.

Using Real-time Scan Monitor

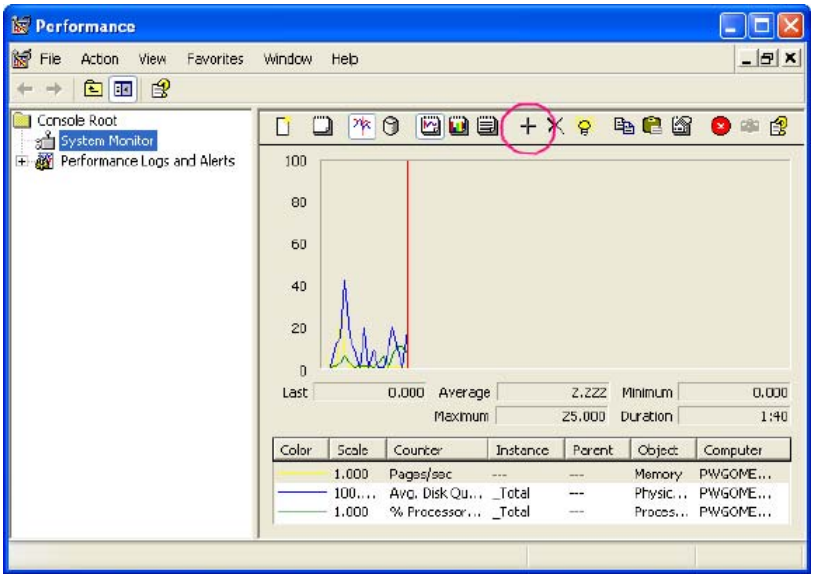
The ISVW Real-time Scan Monitor provides real-time monitoring of SMTP scanning functions, and access to the SMTP and FTP performance data through the Windows Performance Monitor.

To run the Real-time Scan Monitor:

1. On the Windows Start menu, select **Programs > InterScan VirusWall 7 > InterScan VirusWall 7 Real-time Scan Monitor**.

   When you send email through SMTP, real-time statistics and activity information are shown in the monitor panel.
2. Click **Performance Monitor** to open the Windows Performance Monitor.

FIGURE 4-13. The Windows Performance Monitor

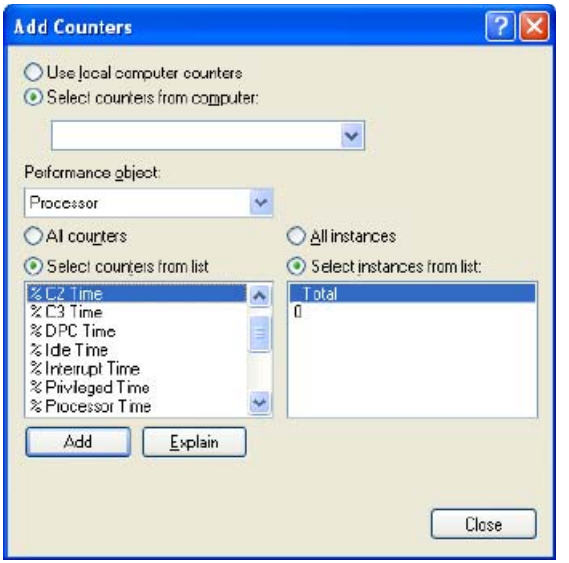


To add counters to the Windows Performance Monitor:

1. Click "+" in the Windows Performance Monitor screen (see encircled item in *Figure 4-13*).

   The Add Counters screen displays.

FIGURE 4-14. The 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 5

Troubleshooting and Support

This chapter provides useful information to solve problems you may encounter while installing, configuring, or starting to use InterScan VirusWall (ISVW).

If this chapter does not provide a solution to your problem, refer to the Administrator's Guide.

Troubleshooting

TABLE 5-1. 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 5-1. 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* on page 3-9.
	  • 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* on page 3-9.
	  • 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 5-1. 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.
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.

TABLE 5-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
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.
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.
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.

TABLE 5-1. Troubleshooting Issues (Continued)

ISSUE	EXPLANATIONS, POSSIBLE CAUSES AND SOLUTIONS
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.

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 about these logs, see the Administrator's Guide.

Frequently Asked Questions

Question:

How do I enable the ActiveUpdate notification?

Answer:

1. Stop the ISVW service.
2. Open `config.xml` and set the value of `/Root/common/ActiveUpdate/notification/SuccessEnable` to "1",

   and set the value of

   `/Root/common/ActiveUpdate/notification/FailEnable` to "1".
3. Restart the ISVW service.

Question:

When migrating from ISVW 5.0 to ISVW 7.0 and during the uninstallation part of the migration process, I am directed to stop the ISVW 5.0 service. How do I stop the ISVW 5.0 service?

Answer:

1. Open the Microsoft Management Console (MMC) by accessing the Start menu and clicking Run.
2. In the **Open** field, type the following: `services.msc`
3. In the Services window, select the InterScan VirusWall System Monitor.
4. Highlight the service and then right click anywhere in the highlighted area. From the contextual menu, select **Stop**. The service stops.

Question:

After migrating from ISVW 5.0 to ISVW 7.0, the System Monitor service for ISVW 5.0 still appears (disabled) in the Services window. How do I remove the System Monitor service?

Answer:

The System Monitor service will automatically be removed after you restart the computer that hosts ISVW.

Question:

After migrating from ISVW 5.0 to ISVW 7.0, the actions associated with my SMTP incoming email are applied to outgoing email. How come my SMTP inbound/outbound traffic settings are not migrated from ISVW 5.0 to ISVW 7.0?

Answer:

ISVW 5.0 uses a different concept for inbound and outbound traffic than ISVW 7.0. As a result, the SMTP settings for incoming and outgoing are not transferred during migration. After migration is complete, the settings will have to be configured manually in the SMTP configuration section of the ISVW Web console.

Question:

How come I receive an error message while trying to install or uninstall ISVW?

Answer:

It is likely that you have real-time virus scanning software installed, and enabled, on the computer that you are trying to install ISVW on. If you have real-time virus scanning software installed on the computer that you are trying to install ISVW on, or remove ISVW from, you will receive an error message. Before installing or removing ISVW, you should temporarily disable the real-time virus scanning.

Question:

How do I resolve the `MFC80.dll` error that appears in the system event log after I have installed ISVW 7.0?

Answer:

You need to install the "Microsoft Visual C++ 2005 Redistributable Package (x86)". You can download this package from the following location:

`http://go.microsoft.com/fwlink/?linkid=65127&clcid=0x409`

After you have downloaded the package, run vcredist_x86.exe on the target computer. This installs Visual C++ libraries as shared assemblies.

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

- 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 via 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

Index

S

T

U

W