TREND MICRO™

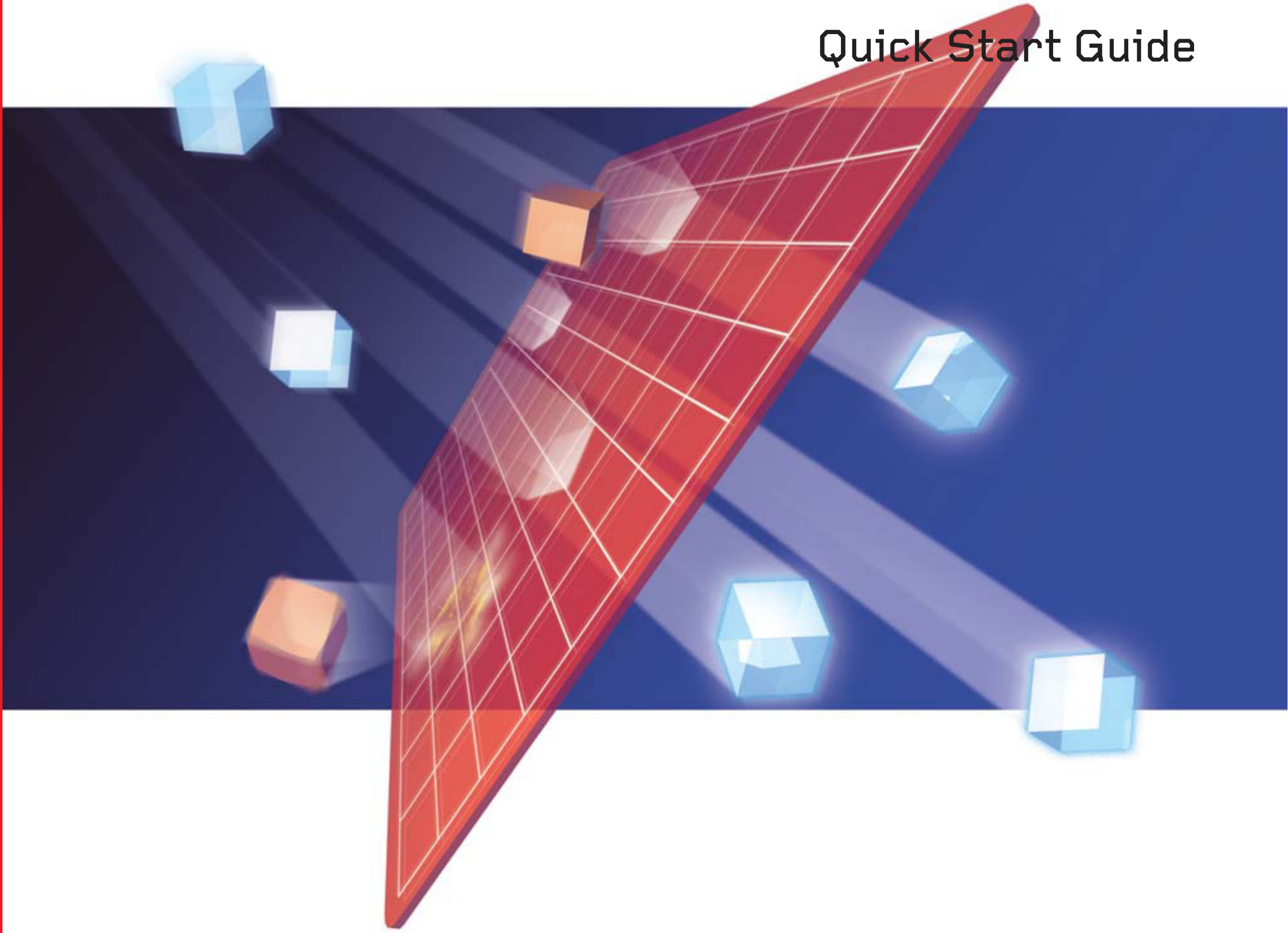
InterScan™ VirusWall™ 6

for Small and Medium Businesses

Integrated virus and spam protection for your Internet gateway

for Windows™

Quick Start Guide



TREND MICRO™

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document Part Number: IVEM62663/60223

Release Date: November 2006

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 Obtaining Technical Support on page 5-7 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

Preface

The Quick Start Guide for InterScan™ VirusWall™ (ISVW) 6 for Windows provides the system administrator with the necessary information to set up, configure, and start managing an InterScan VirusWall 6 installation.

About this Guide

The Quick Start Guide contains the following chapters:

- *Introducing InterScan VirusWall 6* on page 1-1 includes an overview of InterScan VirusWall 6 and its features and benefits.
- *Planning to Install InterScan VirusWall 6* on page 2-1 includes installation planning, system requirements, and pre-installation tasks.
- *Installation* on page 3-1 includes installation procedures and post-installation tasks.
- *Using InterScan VirusWall 6* on page 4-1 includes a discussion of the Web management console and the menu options in the console, and basic tasks such as starting and stopping InterScan VirusWall 6 services and testing key InterScan VirusWall 6 features.
- *Troubleshooting and Support* on page 5-1 includes solutions to quick start tasks and how to obtain technical support.

InterScan VirusWall 6 Documentation

In addition to this Quick Start Guide, you can access the following documents to obtain relevant information about InterScan VirusWall 6:

Document	Content	Where to access
Administrator's Guide	The complete reference to managing InterScan VirusWall 6, including product configuration and troubleshooting	In the product package From the Trend Micro download site: http://www.trendmicro.com/download/
Online Help	Information about product features, tasks, frequently asked questions, and troubleshooting commonly encountered problems Context-sensitive information for each page of the user interface and information concerning the purpose of each screen	From the InterScan VirusWall 6 Web Management console **Note**: Click **Contents and Index** in the Help drop-down menu to access the main help.
Readme	Late-breaking information that may not be included in other documentation, basic installation instructions, and a list of features	From the InterScan VirusWall 6 installation folder (you have the option to launch the readme file after installation) From the Trend Micro download site: http://www.trendmicro.com/download/

Contents

Chapter 1: Introducing InterScan VirusWall 6

Chapter 2: Planning to Install InterScan VirusWall 6

Chapter 3: Installation

Chapter 4: Using InterScan VirusWall 6

Chapter 5: Troubleshooting and Support

Chapter 1

Introducing InterScan VirusWall 6

InterScan VirusWall (ISVW) 6 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.

- InterScan VirusWall 6'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).
- InterScan VirusWall 6 provides heuristics-based anti-spam and content scanning for SMTP and POP3 traffic.
- InterScan VirusWall 6 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

TABLE 1-1. ISVW features and benefits

Features	Descriptions
All-in-one defense	Antivirus, anti-spam, anti-spyware, anti-phishing, IntelliTrap™ (Bot threats), content filtering, URL blocking, and URL filtering *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

What's New?

InterScan VirusWall 6 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, phishing, URL filtering and blocking capabilities, and protection through Outbreak Prevention Services (OPS).

TABLE 1-2. List of new features for ISVW 6

What's New?	Descriptions
Migration from ISVW 3.55 with the eManager™ 3.52 plug-in	Easy upgrade from version 3.55 to 6 while retaining most configuration settings
SMTP, POP3, FTP and HTTP scanning capabilities	SMTP and POP3 scanning support: antivirus, IntelliTrap, spyware/ grayware detection, anti-spam, anti-phishing, and content filtering, including notification messages to the administrator and users upon detection of phishing messages FTP scanning support: antivirus and spyware/grayware detection HTTP scanning support: antivirus, spyware/grayware detection, and blocking of phishing URLs
Anti-spam configuration	Allows an administrator to do the following: • Set the spam threshold to high, medium, or low • Specify approved and blocked senders • Define certain categories of mail as spam based on company policies
Outbreak Prevention Services (OPS)	OPS updates received directly from TrendLabs^{SM} and automatic deployment options available to the administrator
URL blocking and filtering	URL blocking and filtering for the HTTP protocol Allows the administrator to define and configure URL filtering policies Provides a notification to users if URL filtering blocks the URL they want to access
Transparent proxy	Support for the HTTP proxy transparency mode, with the ability to interoperate with an L4 switch
Reverse proxy support	Support for the HTTP reverse proxy mode in the HTTP VirusWall to protect the internal Web Server
HTTP large file handling	Ensures that the client server connection remains active when scanning large files

TABLE 1-2. List of new features for ISVW 6

What's New?	Descriptions
Quarantine "Resend" and "Scan and Resend"	ISVW 6 allows administrators to resend or scan and resend quarantined (SMTP) email messages.
POP3 Whole file scanning	Scans the entire email to identify special types of email viruses
SMTP Transaction Logging	Allows logging of SMTP protocol connection information including origin IP address, sender and recipient email address, time of connection, actions ISVW takes on email, and any associated error messages.

Chapter 2

Planning to Install InterScan VirusWall 6

InterScan VirusWall 6 can be installed and configured to support any number of physical network setups.InterScan VirusWall 6 offers simplified installation and configuration for easy setup. InterScan VirusWall 6 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

Trend Micro InterScan VirusWall 6 antivirus package 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 computer. 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 InterScan VirusWall 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 with Intel™ Pentium™ 4, 1.6 GHz or higher	2 or 4 CPUs with Intel Pentium 4 with Hyper-Threading Technology™, 3.0 GHz or higher
Memory	• 512 MB RAM, without enabling HTTP VirusWall URL filtering • 1 GB RAM, with HTTP VirusWall URL filtering enabled • 1 GB free RAM for Windows Small Business Server	1 GB RAM or higher
Available hard disk space	2 GB 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 minimum disk space, the installation process will not proceed.	20 GB for the target program drive for quarantine files and log files
Operating system	• Windows Server 2003 series, Service Pack 1 • Windows Server 2000 series, Service Pack 4 • Windows XP Professional, Service Pack 2 • Windows Small Business Server 2003, Service Pack 1 • Windows Server 2003 x64 editions	• Windows Server 2003 series, Service Pack 1 • Windows Server 2000 series, Service Pack 4 • Windows Small Business Server 2003, Service Pack 1 **Note:** InterScan VirusWall 6 for Windows checks the platform and operating system before starting the installation process. If the platform and operating system are not supported, InterScan VirusWall 6 for Windows issues a message and exits the installation setup.
Internet browser to access the Web management console	• Microsoft® Internet Explorer® 5.5 or above • FireFox® 1.5 • Netscape® 8.0 • Mozilla® 1.7	Microsoft Internet Explorer 6.0 or above
Monitor	800 x 600 resolution or higher	1024 x 768 resolution or higher
Network interface	10/100M Full Duplex NIC	10/100M Full Duplex NIC

After installation, each process will use the following amounts of memory:

Process	**Memory Used (approximate)**	**When Started**
isvw-main	5 MB	If service is started
isvw-svr	4 MB	If service is started
isvw-scan	110–120 MB	If service is started
isvw-webui	6 MB	If service is started
isvw-smtp	85–90 MB	If SMTP VirusWall is enabled
isvw-pop3	90–95 MB	If POP3 VirusWall is enabled
isvw-http	• 60–65 MB with URL filter disabled • 320–330 MB with URL filter enabled	If HTTP VirusWall is enabled
isvw-ftp	24–30 MB	If FTP VirusWall is enabled

Planning Ahead

By default, InterScan VirusWall 6 uses port 25 to receive SMTP messages for processing, port 8080 for the HTTP listening port, 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
- The IP address of the current POP3 server
- The port number of the current POP3 server
- The IP address of the current HTTP proxy server
- The port number of the current HTTP proxy server
- The port number InterScan will use if it is set up as the HTTP proxy server
- The IP address of the current FTP proxy server
- The port number of the current FTP proxy server
- The port number InterScan will use if it is set up as the FTP proxy server

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

Deciding Where to Install

You can install InterScan VirusWall 6 on 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 server to adequately handle the additional load.

Before installing InterScan VirusWall 6, evaluate the peak and mean traffic loads that the server handles and compare the results to the overall capacity of that computer. The closer the two measurements are, the more likely it is that you will want to install InterScan VirusWall on a dedicated server. Additional factors to consider include network bandwidth, current CPU load, CPU speed, total and available system memory, and the total amount of available swap space. Scanning one or more network protocols for viruses, in real-time, can be resource intensive—do not install InterScan VirusWall 6 onto a computer that does not have the capacity to handle the additional load.

If you are planning to install InterScan VirusWall 6 on a dedicated computer, consider the impact of your choice on overall network bandwidth—installing InterScan VirusWall 6 onto a dedicated computer, although less resource intensive, will consume more network bandwidth than installing InterScan VirusWall 6 on the same computer as the server it is scanning.

Setup Choices: Effects on InterScan VirusWall Configuration

Same Machine. If you install InterScan VirusWall 6 on the original server, you will most likely need to change the port the original server uses and give the default to InterScan VirusWall.

Defaults are typically: FTP: 21, SMTP: 25, HTTP: 8080, POP3: 110.

Dedicated Machine. If InterScan VirusWall is installed on a different computer than the server it will scan, you do not need to change the port of the original server. You may, however, need to modify the clients to reflect the new IP address (or hostname) of the InterScan VirusWall server. If you would prefer not to change the clients:

- Consider swapping IP addresses (or hostnames) between the two servers so InterScan VirusWall can use the original IP address.
- Consider installing InterScan VirusWall so that it is logically between the Internet and server or proxy server.

Installation Topologies

Trend Micro recommends installing InterScan VirusWall 6 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 InterScan VirusWall 6 to address multiple topologies, ranging from a single integrated deployment where you install InterScan VirusWall 6 on a single server and then enable all services on that server, to a completely separate deployment where you run the InterScan VirusWall 6 installation on multiple servers and then enable only the desired service on each server.

Possible topology deployments include:

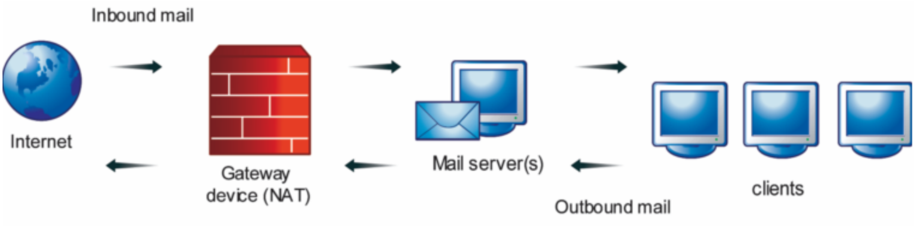
- Single, integrated deployment: install InterScan VirusWall 6 on one server and enable SMTP VirusWall, POP3 VirusWall, FTP VirusWall and HTTP VirusWall on that server
- Messaging/Web deployment:
    - Install InterScan VirusWall 6 on one server and then enable SMTP VirusWall and POP3 VirusWall on that server
    - Install InterScan VirusWall 6 on one server and enable FTP VirusWall and HTTP VirusWall on that server
- Standalone deployment: install InterScan VirusWall 6 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 InterScan VirusWall 6. Use the one that best fits your needs, or apply the principles to an installation strategy unique to your network.

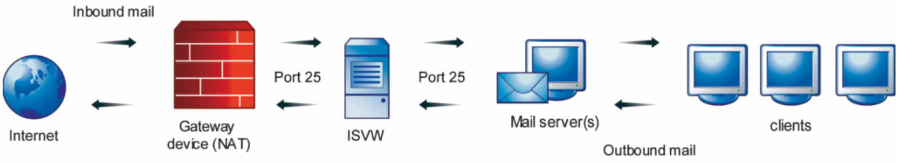
SMTP

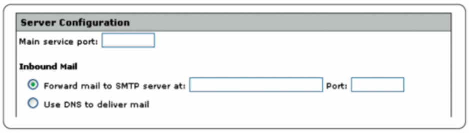
Remap the firewall’s SMTP service, port 25, to the newly installed InterScan VirusWall 6 server listening on port 25. Then use inbound mail forwarding (single server environment) or DNS (multi-server environment) to pass scanned mails to an internal mail server or servers. Ensure that the DNS is working correctly if you choose to use DNS, and use nslookup to resolve internal MX records. These suggestions do not require you to change the IP address(es) of the internal mail server(s). In addition, the client computers require no changes as they will still connect to their respective mail server.

Before installing InterScan VirusWall 6



After installing InterScan VirusWall 6 (InterScan VirusWall 6 and mail server on different machines)




Server Configuration

Main service port:

Inbound Mail

● Forward mail to SMTP server at: Port:

○ Use DNS to deliver mail

Forwarding - scanned mail will be directed to only one mail server
DNS - for multiple mail servers

After installing InterScan VirusWall 6 (InterScan VirusWall 6 and mail server on the same machine)

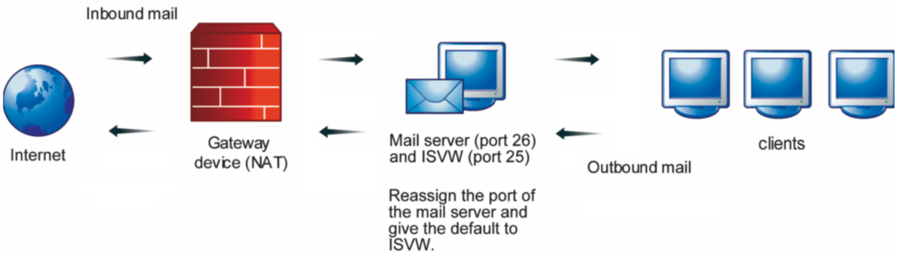
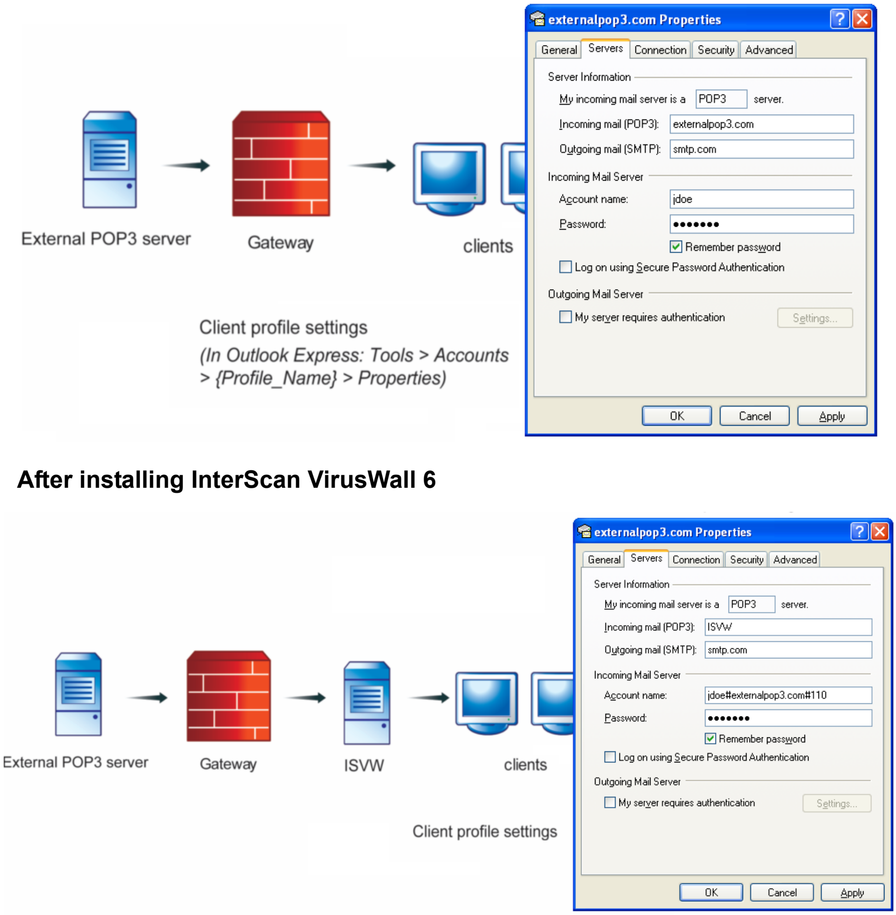

Inbound mail
Internet
Gateway device (NAT)
Mail server (port 26) and ISVW (port 25)
Reassign the port of the mail server and give the default to ISVW.
clients
Outbound mail

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 InterScan VirusWall 6. 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 InterScan VirusWall 6

Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): externalpop3.com

Outgoing mail (SMTP): smtp.com

Incoming Mail Server

Account name: jdoe

Password: •••••••

☑ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication

After installing InterScan VirusWall 6

Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): ISVW

Outgoing mail (SMTP): smtp.com

Incoming Mail Server

Account name: jdoe#externalpop3.com#110

Password: •••••••

☑ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication

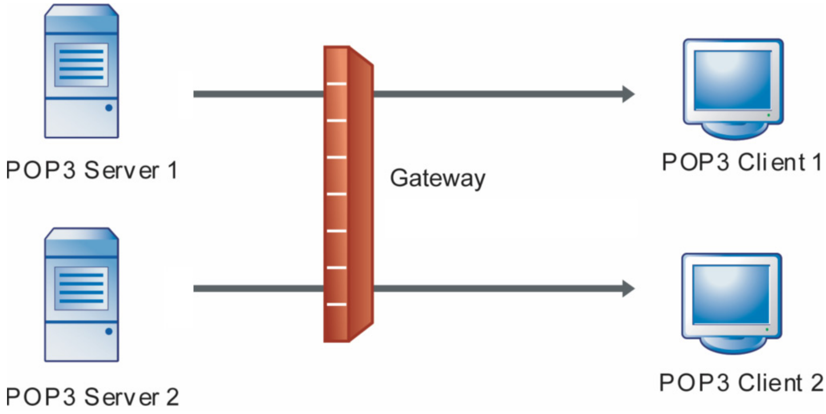
FIGURE 2-2. Typical POP3 Installation Topology

POP3 (Port Mapping)

If InterScan VirusWall 6 acts as a port mapping server, the ports will be mapped to the listening port of InterScan VirusWall 6 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 InterScan VirusWall 6 uses.
- In the POP3 settings on the client machines, incoming mail server name and port should be the InterScan VirusWall 6 server name and port number.

Before installing InterScan VirusWall 6



After installing InterScan VirusWall 6

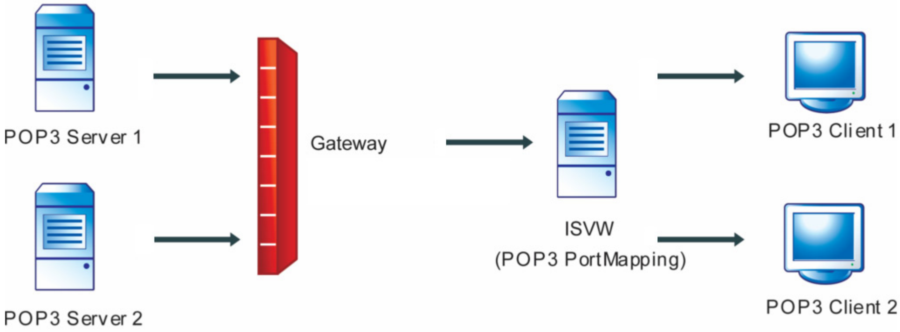
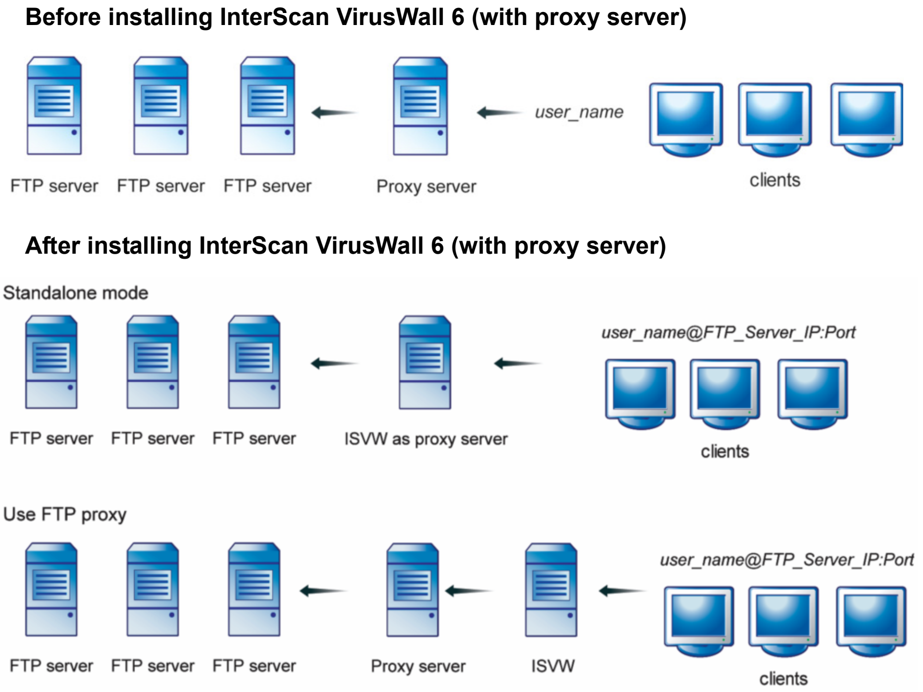


FIGURE 2-3. POP3 with InterScan VirusWall 6 Acting as a Port Mapping Server

FTP

In standalone mode, InterScan VirusWall 6 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”.

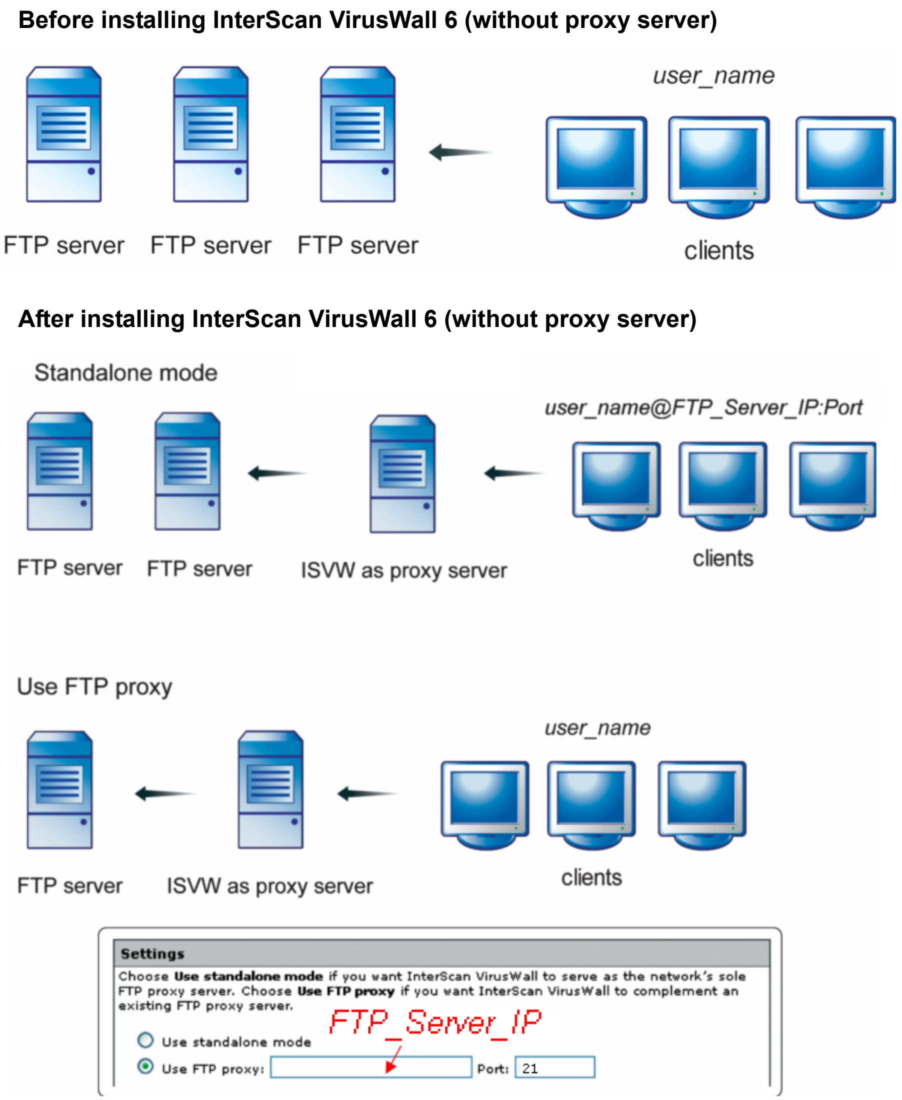
In dependent mode (Use FTP proxy), InterScan VirusWall 6 complements an existing FTP proxy server. If there is no proxy server, clients connecting to FTP VirusWall will be redirected to the real FTP server specified in the FTP Configuration screen in the InterScan VirusWall 6 Web management console. 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 InterScan VirusWall 6 (with proxy server)

After installing InterScan VirusWall 6 (with proxy server)

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



Before installing InterScan VirusWall 6 (without proxy server)

After installing InterScan VirusWall 6 (without proxy server)

Settings

Choose **Use standalone mode** if you want InterScan VirusWall to serve as the network's sole FTP proxy server. Choose **Use FTP proxy** if you want InterScan VirusWall to complement an existing FTP proxy server.

○ Use standalone mode

● Use FTP proxy: Port: 21

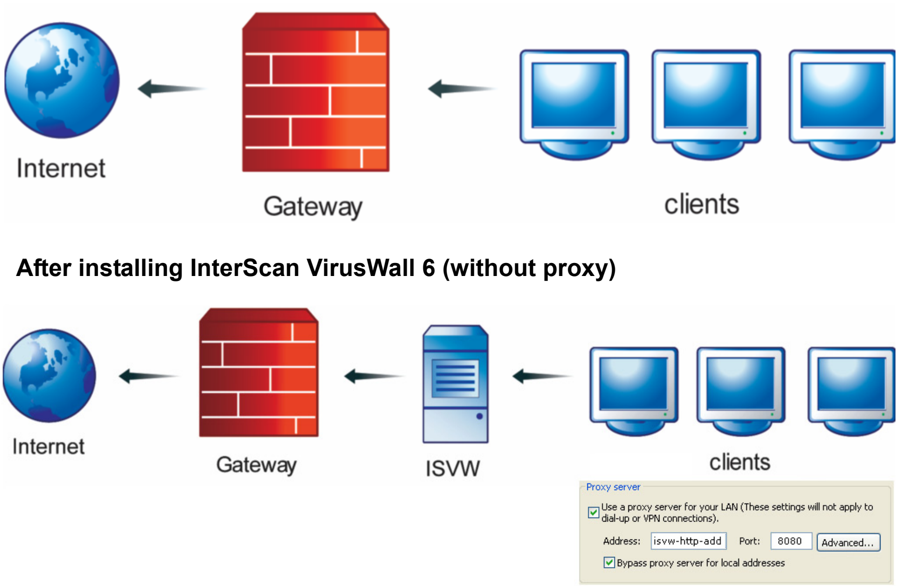
FIGURE 2-5. Installation Topology for FTP without a Proxy Server

HTTP

In standalone mode, InterScan VirusWall 6 is directly behind the gateway device, either serving as the HTTP proxy server or receiving HTTP traffic from an existing server.

In dependent mode, InterScan VirusWall 6 is deployed between the client machines and the HTTP proxy server.

Before installing InterScan VirusWall 6 (without proxy)



After installing InterScan VirusWall 6 (without proxy)

Proxy server

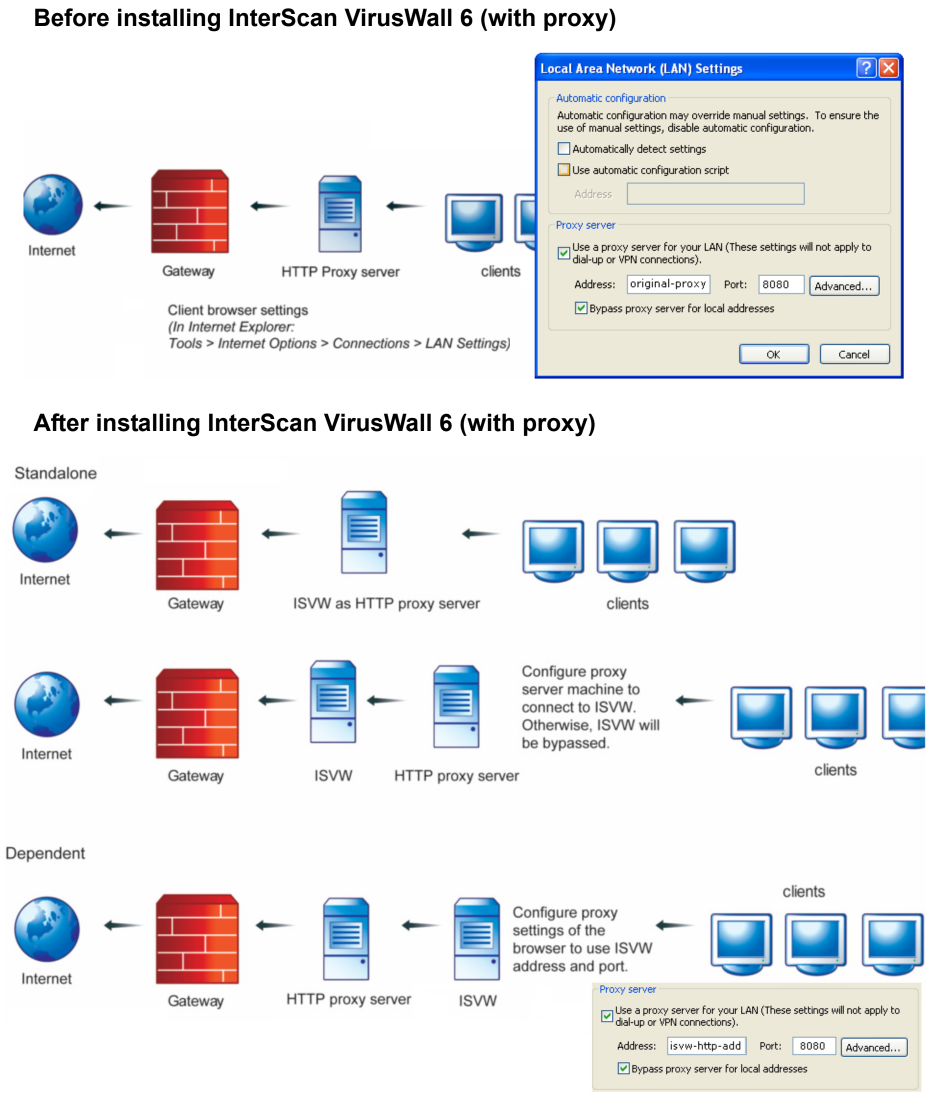
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: isvw-http-add Port: 8080 Advanced...

☑ Bypass proxy server for local addresses

FIGURE 2-6. Installation Topology for HTTP without a Proxy Server

After installing InterScan VirusWall 6, the clients need to set their browsers’ proxy server to InterScan VirusWall 6



Before installing InterScan VirusWall 6 (with proxy)

Client browser settings
(In Internet Explorer:
Tools > Internet Options > Connections > LAN Settings)

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: original-proxy Port: 8080

☑ Bypass proxy server for local addresses

After installing InterScan VirusWall 6 (with proxy)

Configure proxy server machine to connect to ISVW. Otherwise, ISVW will be bypassed.

Configure proxy settings of the browser to use ISVW address and port.

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: isvw-http-add Port: 8080

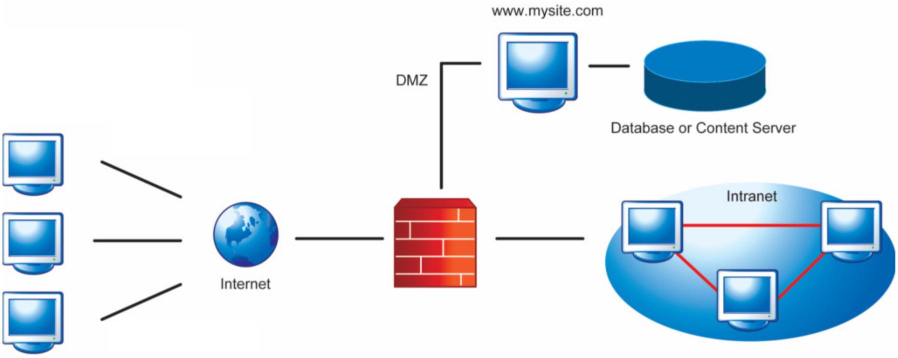
☑ Bypass proxy server for local addresses

FIGURE 2-7. Installation Topology for HTTP with a Proxy Server

HTTP Reverse Proxy

In reverse proxy, a content server is made available to outside clients and intranet users but a firewall prevents direct, unmonitored access to the server. In this topology, InterScan VirusWall 6 scans HTTP traffic from the content server to the clients within and outside the network.

Before installing InterScan VirusWall 6



After installing InterScan VirusWall 6

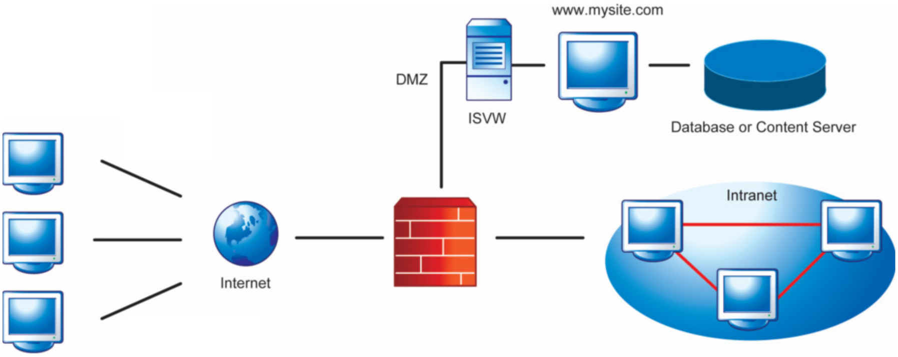


FIGURE 2-8. Installation Topology for HTTP with a Reverse Proxy

Before Installing InterScan VirusWall 6

1. On the machine where you will install InterScan VirusWall 6, uninstall any version of InterScan VirusWall that is not version 3.55.
2. Remove any real-time scanning product. If you do not want to remove the product, add the following items to the product's scanning exclusion list:
   - InterScan VirusWall destination path
   - Quarantine path for the SMTP, POP3, HTTP, and FTP protocols
   - Windows™ Temp folder
3. Log on with administrator privileges on the machine.
4. Ensure the following default port numbers used by InterScan VirusWall 6 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.

5. If you are installing InterScan VirusWall 6 for the first time, prepare a list of domains that SMTP VirusWall will recognize as valid domains. SMTP will only deliver inbound emails addressed to these domains.
6. If you are upgrading from ISVW 3.55 with eManager 3.52 to InterScan VirusWall 6, 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

Installation

InterScan VirusWall 6 installation takes about 10 minutes and should be performed from the machine where the program(s) will reside. Allow another 10-15 minutes to configure InterScan VirusWall 6 to work with your existing servers.

InterScan VirusWall 6 provides a migration tool to help existing InterScan VirusWall for Windows customers migrate from version 3.55 to version 6.

This chapter provides instructions for installing InterScan VirusWall 6 for Windows. It also provides instructions for migrating from ISVW 3.55 to InterScan VirusWall 6 for Windows.

Installing InterScan VirusWall 6

The InterScan VirusWall 6 setup consists of launching the setup file and following the instructions on the InstallShield Wizard screens.

There are four types of installation scenarios:

- *Installing InterScan VirusWall 6 as a Fresh Installation* starting on page 3-2

  Use this procedure if you are installing InterScan VirusWall 6 for Windows for the first time.

- *Installing InterScan VirusWall 6 on a Machine Where ISVW 3.55 Is Installed* starting on page 3-11

  Use this procedure to install InterScan VirusWall 6 or Windows on a computer that has ISVW 3.55 installed on it, and migrating version 3.55 settings to 6.

- *Installing InterScan VirusWall 6 on a New Computer and Migrating ISVW 3.55 Settings to that Computer* starting on page 3-21

  Use this procedure if you are installing InterScan VirusWall 6 for Windows on a new computer, and migrating settings from another machine that has ISVW 3.55 installed on it. You will use a migration tool to migrate version 3.55 settings and import them during installation.

- *Upgrading from ISVW Windows Version 6.0* starting on page 3-33

  Use this procedure if you are upgrading from InterScan VirusWall 6 for Windows. The installer imports all of your previous ISVW 6.0 settings.

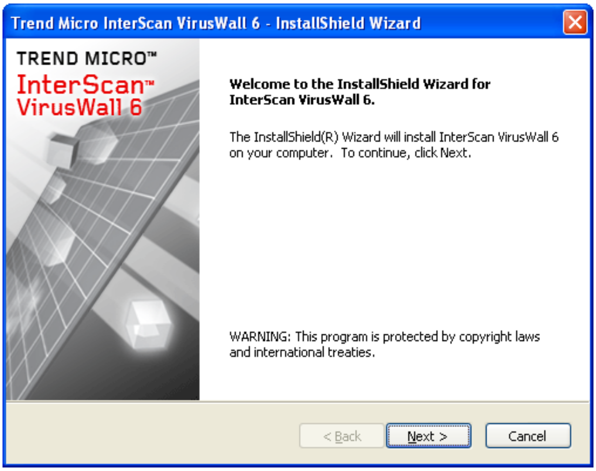
Installing InterScan VirusWall 6 as a Fresh Installation

To perform a fresh installation of InterScan VirusWall, perform the following steps:

1. Double-click setup.exe to start the installation process.

Note: If the InterScan VirusWall 6.01 Setup detects InterScan VirusWall 6.0 and they are the same language version, the Setup program will prompt you to confirm the build upgrade. If InterScan VirusWall 6.01 and 6.0 are different language versions, the Setup program will ask to uninstall version 6.0 before proceeding. If the Setup program detects that you have a different langauge version of InterScan VirusWall 6.01 installed, it will prompt you to uninstall the different language version and then proceed with the installation. Currently only the English version of InterScan VirusWall 6.01 is available.

2. When the Welcome screen shown in Figure 3-1 appears, click **Next**.



Welcome to the InstallShield Wizard for InterScan VirusWall 6.

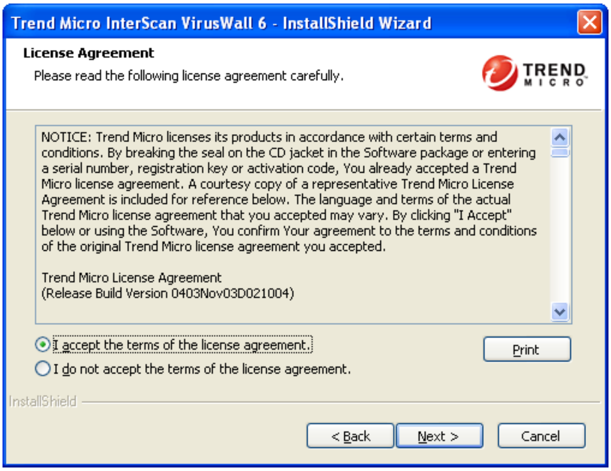
The InstallShield(R) Wizard will install InterScan VirusWall 6 on your computer. To continue, click Next.

WARNING: This program is protected by copyright laws and international treaties.

FIGURE 3-1. InterScan VirusWall Welcome screen

3. When the License Agreement screen shown in Figure 3-2 appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation. You can scroll through the entire agreement online or print it.

If you select **I do not accept the terms of the license agreement**, the installation process will terminate.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or entering a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

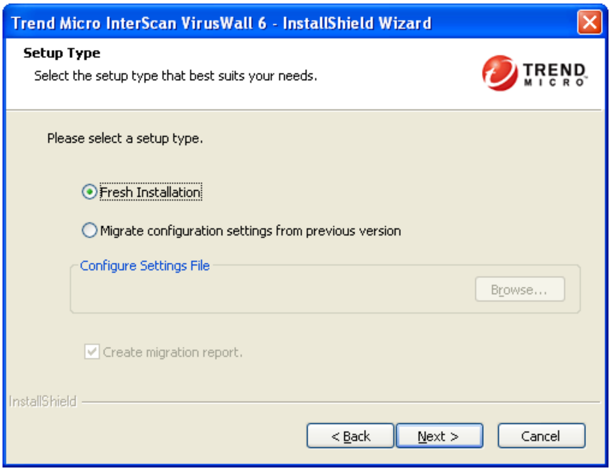
Trend Micro License Agreement
(Release Build Version 0403Nov03D021004)

● I accept the terms of the license agreement.

○ I do not accept the terms of the license agreement.

FIGURE 3-2. License Agreement screen

4. When the Setup Type window in Figure 3-3 appears, select **Fresh Installation** and click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Please select a setup type.

● Fresh Installation

○ Migrate configuration settings from previous version

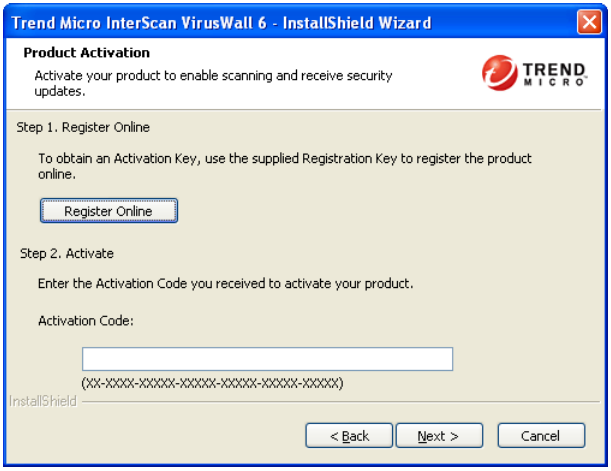
Configure Settings File

☑ Create migration report.

FIGURE 3-3. Setup Type screen

5. When the Product Activation screen shown in Figure 3-4 appears, do one of the following:

   - If you have already registered and obtained a product activation code, then skip registration 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 you received in the Activation Code text box and click **Next**.
   - Click **Next** without entering an activation code.


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Product Activation

Activate your product to enable scanning and receive security updates.

Step 1. Register Online

To obtain an Activation Key, use the supplied Registration Key to register the product online.

Step 2. Activate

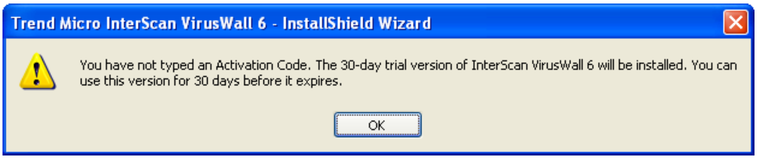
Enter the Activation Code you received to activate your product.

Activation Code:

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

FIGURE 3-4. Product Activation screen

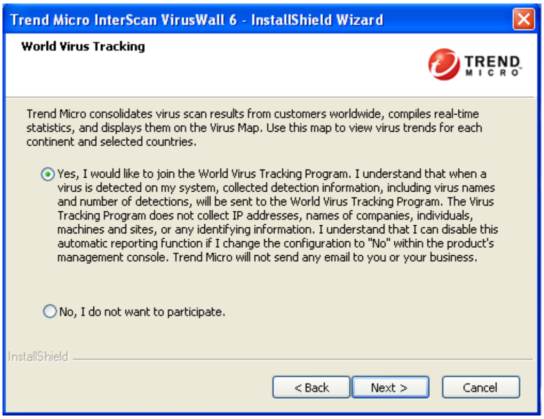
If you clicked **Next** without entering an activation code, the 30-day trial version of InterScan VirusWall 6 will be installed. Click **OK** to proceed with the installation.


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

You have not typed an Activation Code. The 30-day trial version of InterScan VirusWall 6 will be installed. You can use this version for 30 days before it expires.

FIGURE 3-5. Product Activation message

6. When the World Virus Tracking screen shown in Figure 3-6 appears, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, then click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

World Virus Tracking

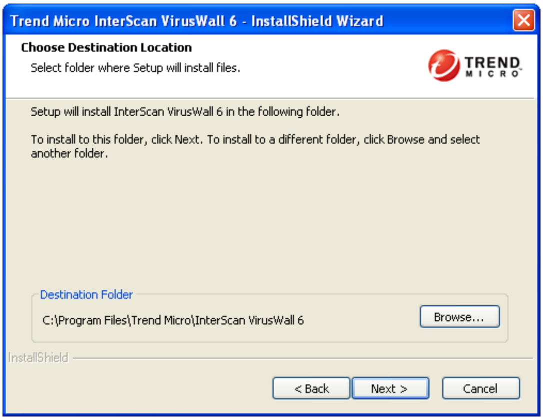
Trend Micro consolidates virus scan results from customers worldwide, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries.

● Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, collected detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program. The Virus Tracking Program does not collect IP addresses, names of companies, individuals, machines and sites, or any identifying information. I understand that I can disable this automatic reporting function if I change the configuration to "No" within the product's management console. Trend Micro will not send any email to you or your business.

○ No, I do not want to participate.

FIGURE 3-6. World Virus Tracking screen

7. The Choose Destination Location screen shown in Figure 3-7 appears, indicating the directory path where InterScan VirusWall 6 will be installed. If you wish to change the directory path, click **Browse** and specify a different location. When you have either accepted the default path or chosen a new destination, click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install InterScan VirusWall 6 in the following folder.

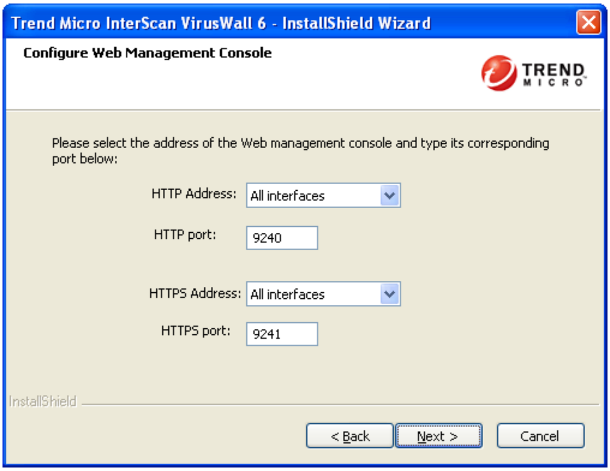
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Trend Micro\InterScan VirusWall 6

FIGURE 3-7. Choose Destination Location screen

8. When the Configure Web Management Console screen appears, specify where the Web management console will bind. Default settings are shown in Figure 3-8. Click **Next**.


Trend Micro InterScan VirusWall 6 - InstallShield Wizard
Configure Web Management Console
TREND MICRO
InstallShield
< Back
Next >
Cancel

Please select the address of the Web management console and type its corresponding port below:

HTTP Address: All interfaces

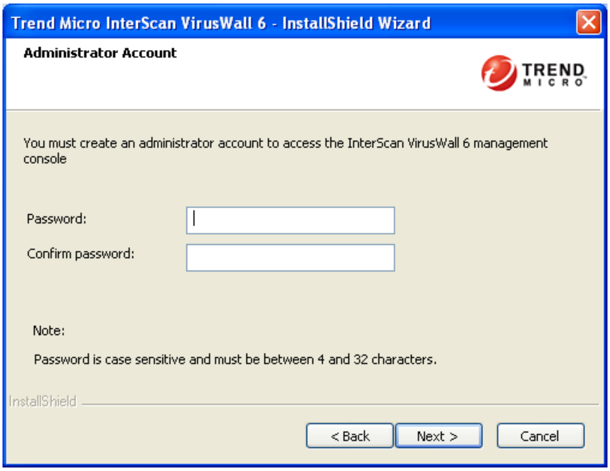
HTTP port: 9240

HTTPS Address: All interfaces

HTTPS port: 9241

FIGURE 3-8. Configure Web Management Console screen

9. When the Administrator Account screen shown in Figure 3-9 appears, enter a 4- to 32-character password, confirm it, and click **Next**.



You must create an administrator account to access the InterScan VirusWall 6 management console

Password:

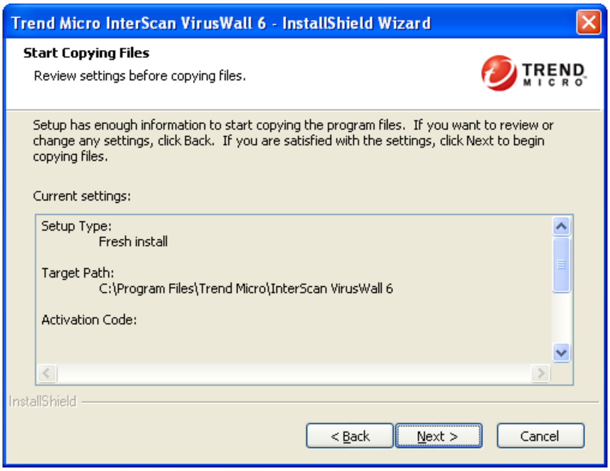
Confirm password:

Note:

Password is case sensitive and must be between 4 and 32 characters.

FIGURE 3-9. Administrator Account screen

10. When the Start Copying Files screen shown in Figure 3-10 appears, review the current settings.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

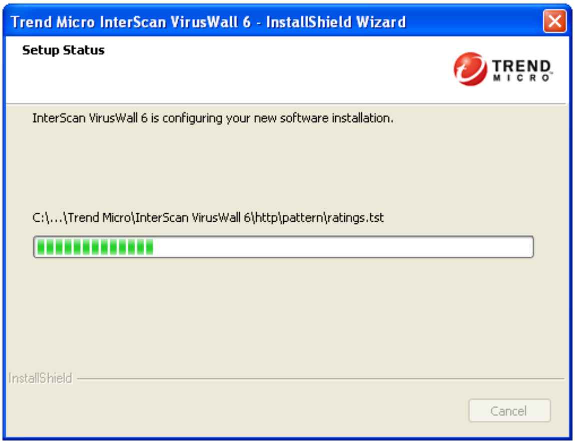
Current settings:

```
Setup Type:
          Fresh install

Target Path:
          C:\Program Files\Trend Micro\InterScan VirusWall 6

Activation Code:
```

FIGURE 3-10. Start Copying Files screen

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

The Setup Status screen shown in Figure 3-11 appears.


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

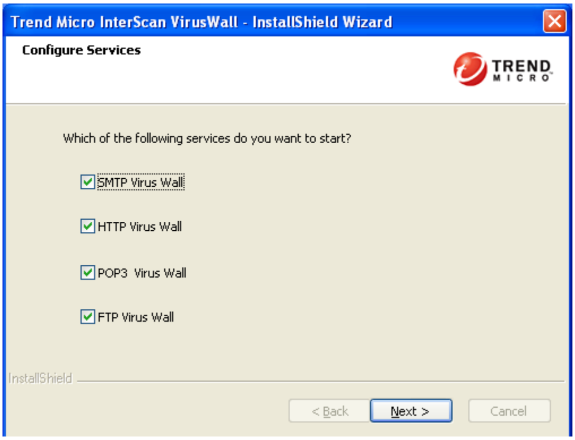
Setup Status

InterScan VirusWall 6 is configuring your new software installation.

C:\...\Trend Micro\InterScan VirusWall 6\http\pattern\ratings.tst

FIGURE 3-11. Setup Status screen

11. When Setup is complete, the Configure Services screen shown in Figure 3-12 appears. Select the InterScan VirusWall services you want to start after the installation has finished. By default, all services are selected to start. When you have made your selections, click **Next**.


Trend Micro InterScan VirusWall - InstallShield Wizard

Configure Services

Which of the following services do you want to start?

☑ SMTP Virus Wall

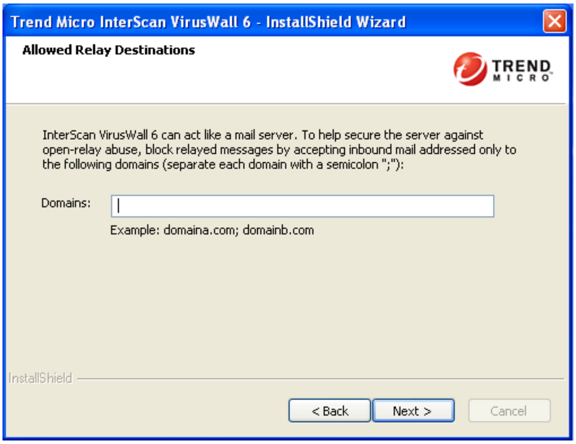
☑ HTTP Virus Wall

☑ POP3 Virus Wall

☑ FTP Virus Wall

FIGURE 3-12. Configure Services screen

12. Specify domains in the Allowed Relay Destinations screen. InterScan VirusWall 6 will only accept inbound mails addressed to these domains.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Allowed Relay Destinations

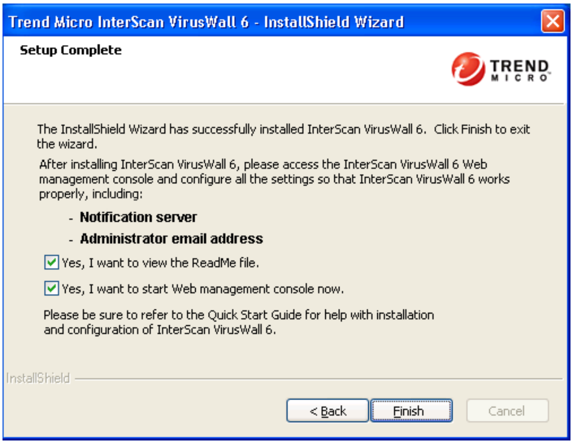
InterScan VirusWall 6 can act like a mail server. To help secure the server against open-relay abuse, block relayed messages by accepting inbound mail addressed only to the following domains (separate each domain with a semicolon ";"):

Domains:

Example: domaina.com; domainb.com

FIGURE 3-13. Allowed Relay Destinations screen

13. On the Setup Complete screen shown in Figure 3-14, select whether you want to display the readme.txt file or start the Web management console and click **Finish**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Setup Complete

The InstallShield Wizard has successfully installed InterScan VirusWall 6. Click Finish to exit the wizard.

After installing InterScan VirusWall 6, please access the InterScan VirusWall 6 Web management console and configure all the settings so that InterScan VirusWall 6 works properly, including:

- **Notification server**
- **Administrator email address**

☑ Yes, I want to view the ReadMe file.

☑ Yes, I want to start Web management console now.

Please be sure to refer to the Quick Start Guide for help with installation and configuration of InterScan VirusWall 6.

FIGURE 3-14. Setup Complete screen

- 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 InterScan VirusWall 6.

Installing InterScan VirusWall 6 on a Machine Where ISVW 3.55 Is Installed

If you will install InterScan VirusWall 6 for Windows on a computer where ISVW 3.55 for Windows is installed, you can choose to migrate the version 3.55 configuration settings to the new version during installation. If you have eManager 3.52 as a plug-in, you can also choose to migrate the configuration settings of eManager to InterScan VirusWall 6.

If you choose to migrate the settings, Trend Micro recommends that you back up the configuration file before proceeding with the installation. The InterScan VirusWall 6 for Windows installation program will remove ISVW 3.55 completely, but will not remove eManager.

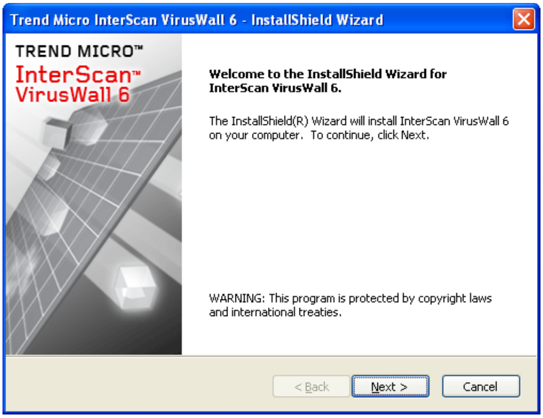
Installing on the same host and migrating the configuration settings:

To install InterScan VirusWall 6 and migrate the configuration settings from the existing ISVW 3.55 installation, perform the following steps:

1. Double-click setup.exe to start the installation process.

Note: If the InterScan VirusWall 6.01 Setup detects InterScan VirusWall 6.0 and they are the same language version, the Setup program will prompt you to confirm the build upgrade. If InterScan VirusWall 6.01 and 6.0 are different language versions, the Setup program will ask to uninstall version 6.0 before proceeding. If the Setup program detects that you have a different langauge version of InterScan VirusWall 6.01 installed, it will prompt you to uninstall the different language version and then proceed with the installation. Currently only the English version of InterScan VirusWall 6.01 is available.

2. When the Welcome screen shown in Figure 3-15 appears, click **Next**.



Welcome to the InstallShield Wizard for InterScan VirusWall 6.

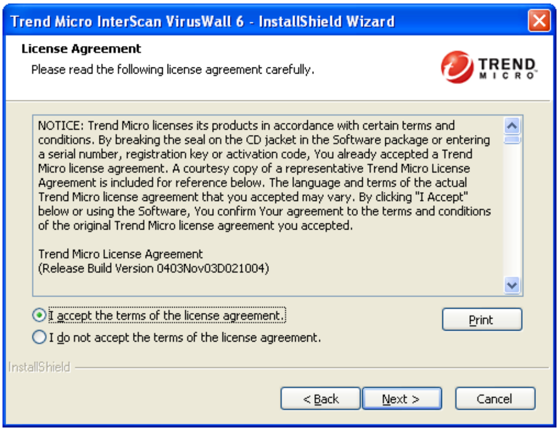
The InstallShield(R) Wizard will install InterScan VirusWall 6 on your computer. To continue, click Next.

WARNING: This program is protected by copyright laws and international treaties.

FIGURE 3-15. InterScan VirusWall Welcome screen

3. When the License Agreement screen shown in Figure 3-16 appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation. You can scroll through the entire agreement online or print it.

   If you select **I do not accept the terms of the license agreement**, the installation process will terminate.



License Agreement

Please read the following license agreement carefully.

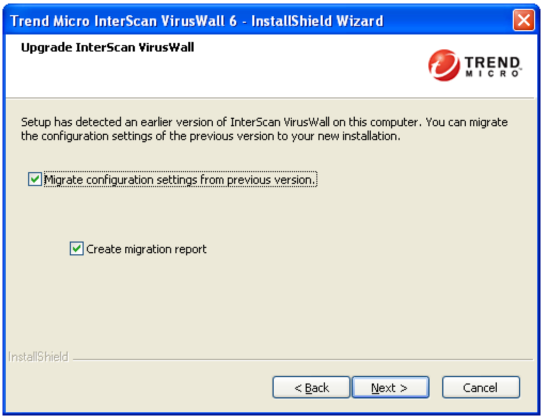
NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or entering a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement
(Release Build Version 0403Nov03D021004)

● I accept the terms of the license agreement.
○ I do not accept the terms of the license agreement.

FIGURE 3-16. License Agreement screen

4. When the Upgrade InterScan VirusWall screen in Figure 3-17 appears, select **Migrate configuration settings from previous version**. If you do not want to create a report that lists all the migrated settings, deselect **Create migration report**. Click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Upgrade InterScan VirusWall

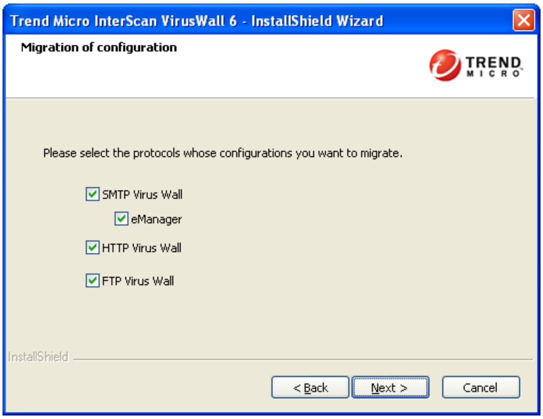
Setup has detected an earlier version of InterScan VirusWall on this computer. You can migrate the configuration settings of the previous version to your new installation.

☑ Migrate configuration settings from previous version.

☑ Create migration report

FIGURE 3-17. Upgrade InterScan VirusWall screen

5. When the Migration of configuration screen in Figure 3-18 appears, select the protocols whose configuration settings you want to migrate to InterScan VirusWall 6. Click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Migration of configuration

Please select the protocols whose configurations you want to migrate.

☑ SMTP Virus Wall

☑ eManager

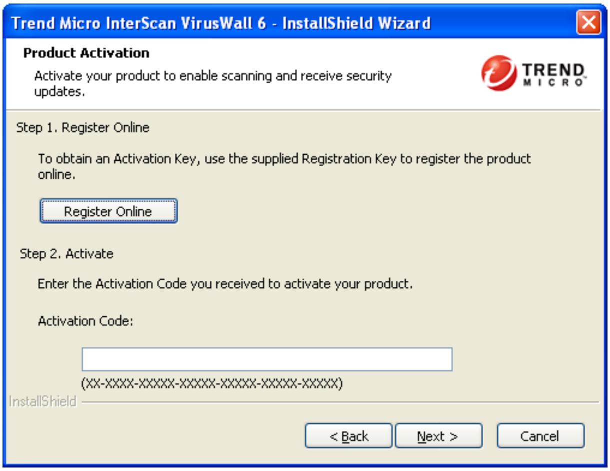
☑ HTTP Virus Wall

☑ FTP Virus Wall

FIGURE 3-18. Migration of configuration screen

Note: To migrate the configuration settings for eManager, you must select the SMTP protocol.

6. When the Product Activation screen shown in Figure 3-19 appears, 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 you received in the Activation Code text box and click **Next**.
   - Click **Next** without entering an activation code.



Product Activation

Activate your product to enable scanning and receive security updates.

Step 1. Register Online

To obtain an Activation Key, use the supplied Registration Key to register the product online.

Step 2. Activate

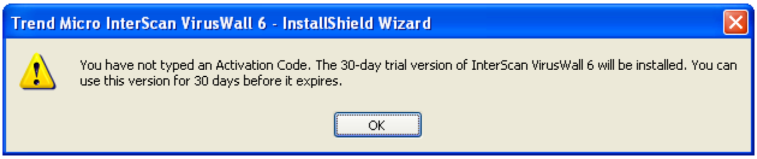
Enter the Activation Code you received to activate your product.

Activation Code:

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

FIGURE 3-19. Product Activation screen

If you clicked **Next** without entering an activation code, the 30-day trial version of InterScan VirusWall 6 will be installed. Click **OK** to proceed with the installation.

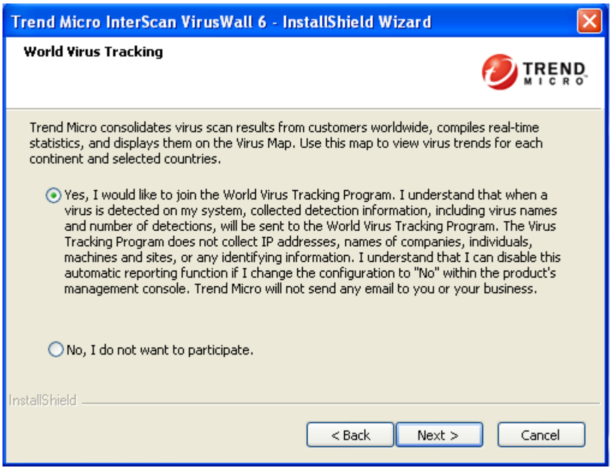


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

You have not typed an Activation Code. The 30-day trial version of InterScan VirusWall 6 will be installed. You can use this version for 30 days before it expires.

FIGURE 3-20. Product Activation message

7. When the World Virus Tracking screen shown in Figure 3-21 appears, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, then click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

World Virus Tracking

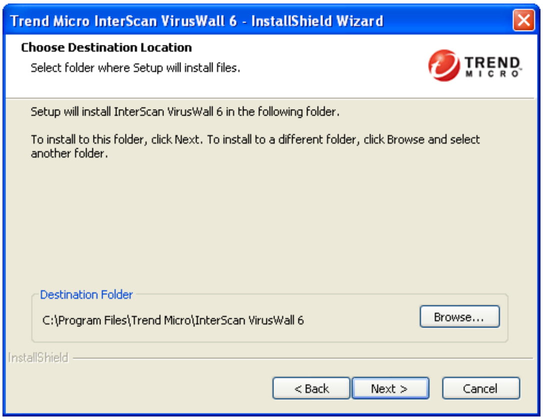
Trend Micro consolidates virus scan results from customers worldwide, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries.

● Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, collected detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program. The Virus Tracking Program does not collect IP addresses, names of companies, individuals, machines and sites, or any identifying information. I understand that I can disable this automatic reporting function if I change the configuration to "No" within the product's management console. Trend Micro will not send any email to you or your business.

○ No, I do not want to participate.

FIGURE 3-21. World Virus Tracking screen

8. The Choose Destination Location screen shown in Figure 3-22 appears, indicating the directory path where InterScan VirusWall 6 will be installed. To change the directory path, click **Browse** and specify a different location. When you have either accepted the default path or chosen a new destination, click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install InterScan VirusWall 6 in the following folder.

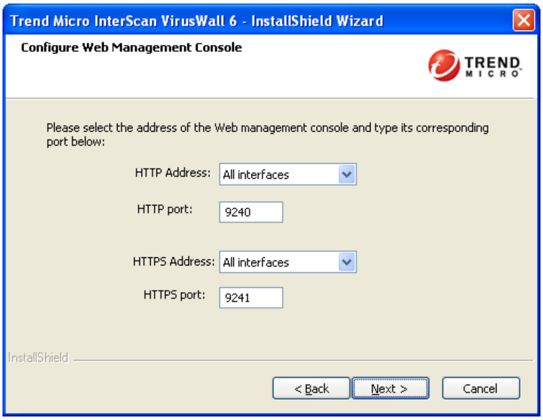
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Trend Micro\InterScan VirusWall 6

FIGURE 3-22. Choose Destination Location screen

9. When the Configure Web Management Console screen appears, specify where the Web management console will bind. Default settings are shown in Figure 3-23. Click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Configure Web Management Console

Please select the address of the Web management console and type its corresponding port below:

HTTP Address: All interfaces

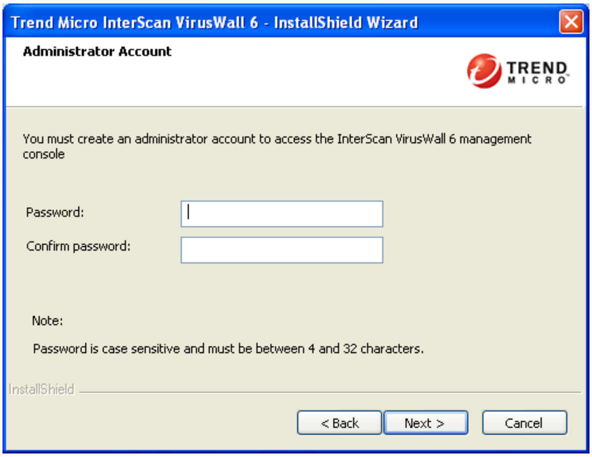
HTTP port: 9240

HTTPS Address: All interfaces

HTTPS port: 9241

FIGURE 3-23. Configure Web Management Console screen

10. When the Administrator Account screen shown in Figure 3-24 appears, enter a 4- to 32-character password, confirm it, and click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Administrator Account

You must create an administrator account to access the InterScan VirusWall 6 management console

Password:

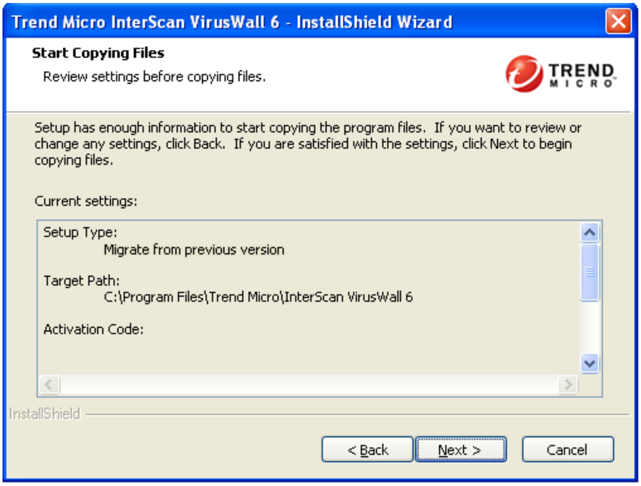
Confirm password:

Note:

Password is case sensitive and must be between 4 and 32 characters.

FIGURE 3-24. Administrator Account screen

11. When the Start Copying Files screen shown in Figure 3-25 appears, review the current settings.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current settings:

Setup Type:
Migrate from previous version

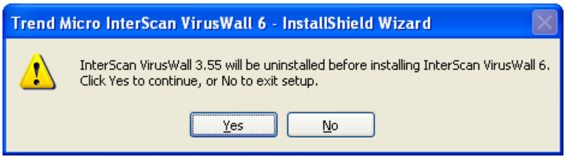
Target Path:
C:\Program Files\Trend Micro\InterScan VirusWall 6

Activation Code:

FIGURE 3-25. Start Copying Files screen

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

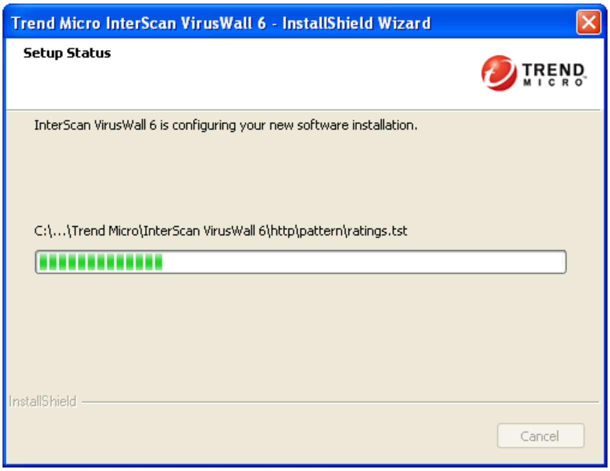
12. Click **Yes** to uninstall InterScan VirusWall 3.55 and install InterScan VirusWall 6.



InterScan VirusWall 3.55 will be uninstalled before installing InterScan VirusWall 6.
Click Yes to continue, or No to exit setup.

FIGURE 3-26. Message confirming uninstallation of ISVW 3.55

A message displays to indicate that InterScan VirusWall 3.55 is being removed. When it has been uninstalled, the Setup Status screen in Figure 3-27 appears.

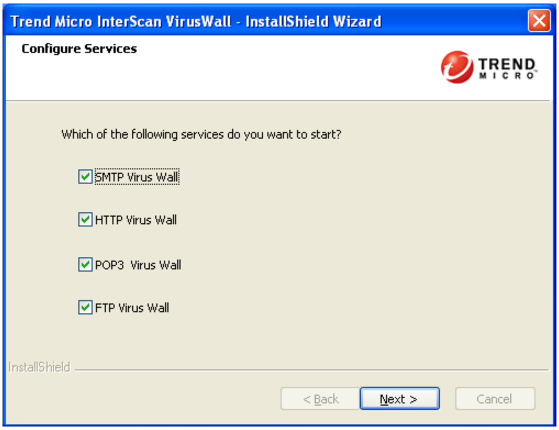


InterScan VirusWall 6 is configuring your new software installation.

C:\...\Trend Micro\InterScan VirusWall 6\http\pattern\ratings.tst

FIGURE 3-27. Setup status screen

13. When Setup is complete, the Configure Services screen shown in Figure 3-28 appears. Select the InterScan VirusWall services you want to start after the installation has finished. By default, all services are selected to start. When you have made your selections, click **Next**.



Configure Services

Which of the following services do you want to start?

☑ SMTP Virus Wall

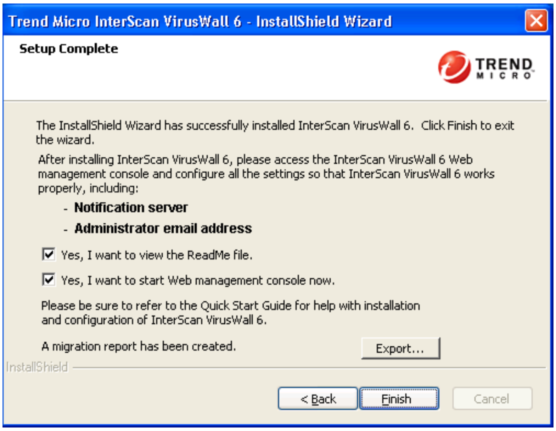
☑ HTTP Virus Wall

☑ POP3 Virus Wall

☑ FTP Virus Wall

FIGURE 3-28. Configure Services screen

14. When the Setup Complete screen shown in Figure 3-29 appears, you can do any of the following and then click **Finish**.



Setup Complete

The InstallShield Wizard has successfully installed InterScan VirusWall 6. Click Finish to exit the wizard.

After installing InterScan VirusWall 6, please access the InterScan VirusWall 6 Web management console and configure all the settings so that InterScan VirusWall 6 works properly, including:

- **Notification server**
- **Administrator email address**

☑ Yes, I want to view the ReadMe file.

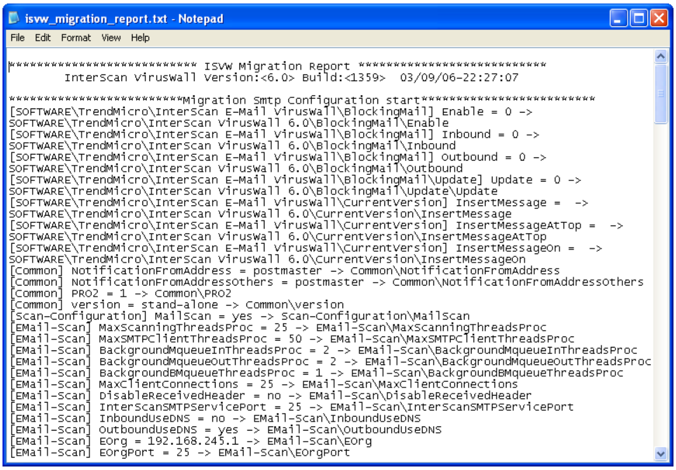
☑ Yes, I want to start Web management console now.

Please be sure to refer to the Quick Start Guide for help with installation and configuration of InterScan VirusWall 6.

A migration report has been created.

FIGURE 3-29. Setup Complete screen

- Choose to view the readme.txt file, which will display in a new window.
- Choose to start the Web management console. A Web browser window will open automatically and display the logon page for InterScan VirusWall 6.
- If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in Figure 3-30.



```
*************************** ISVW Migration Report ***************************
        InterScan VirusWall Version:<6.0> Build:<1359>  03/09/06-22:27:07

*************************Migration Smtp Configuration start*************************
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Enable = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Enable
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Inbound = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Inbound
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Outbound = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Outbound
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail\Update] Update = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Update\Update
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessage =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessage
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessageAtTop =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessageAtTop
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessageOn =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessageOn
[Common] NotificationFromAddress = postmaster -> Common\NotificationFromAddress
[Common] NotificationFromAddressOthers = postmaster -> Common\NotificationFromAddressOthers
[Common] PRO2 = 1 -> Common\PRO2
[Common] version = stand-alone -> Common\version
[Scan-Configuration] MailScan = yes -> Scan-Configuration\MailScan
[EMail-Scan] MaxScanningThreadsProc = 25 -> EMail-Scan\MaxScanningThreadsProc
[EMail-Scan] MaxSMTPClientThreadsProc = 50 -> EMail-Scan\MaxSMTPClientThreadsProc
[EMail-Scan] BackgroundMqueueInThreadsProc = 2 -> EMail-Scan\BackgroundMqueueInThreadsProc
[EMail-Scan] BackgroundMqueueOutThreadsProc = 2 -> EMail-Scan\BackgroundMqueueOutThreadsProc
[EMail-Scan] BackgroundBMqueueThreadsProc = 1 -> EMail-Scan\BackgroundBMqueueThreadsProc
[EMail-Scan] MaxClientConnections = 25 -> EMail-Scan\MaxClientConnections
[EMail-Scan] DisableReceivedHeader = no -> EMail-Scan\DisableReceivedHeader
[EMail-Scan] InterScanSMTPServicePort = 25 -> EMail-Scan\InterScanSMTPServicePort
[EMail-Scan] InboundUseDNS = no -> EMail-Scan\InboundUseDNS
[EMail-Scan] OutboundUseDNS = yes -> EMail-Scan\OutboundUseDNS
[EMail-Scan] EOrg = 192.168.245.1 -> EMail-Scan\EOrg
[EMail-Scan] EOrgPort = 25 -> EMail-Scan\EOrgPort
```

FIGURE 3-30. Sample migration report

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

<ISVW_Installation_folder>\isvw_migration_report.txt

Installing InterScan VirusWall 6 on a New Computer and Migrating ISVW 3.55 Settings to that Computer

If you will install InterScan VirusWall 6 for Windows on a computer where you have not previously installed InterScan VirusWall 6 and you want to use the configuration settings from a computer where ISVW 3.55 for Windows 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 InterScan VirusWall 6.

A migration tool that allows you export the configuration settings to a file has been supplied as part of the InterScan VirusWall 6 installation package. The migration tool allows you to export the ISVW 3.55 configuration and eManager plug-in settings.

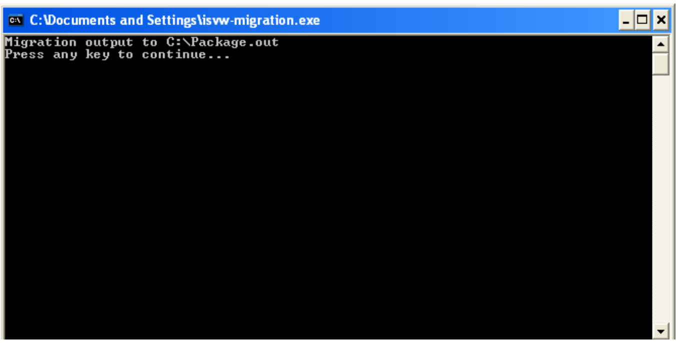
If ISVW 3.55 does not exist on the computer where you run the migration tool, InterScan VirusWall 6 issues a message and exits the installation setup.

Migrating the configuration settings to a different computer:

To install InterScan VirusWall 6 on a computer and migrate the configuration settings from another computer that has ISVW 3.55 installed, perform the following steps:

1. On the machine that contains the ISVW 3.55 installation, navigate to {Installation package}\tools\isvw-migration.exe.
2. Double-click isvw-migration.exe to export the configuration settings. If ISVW 3.55 exists, the command window shown in Figure 3-31 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.



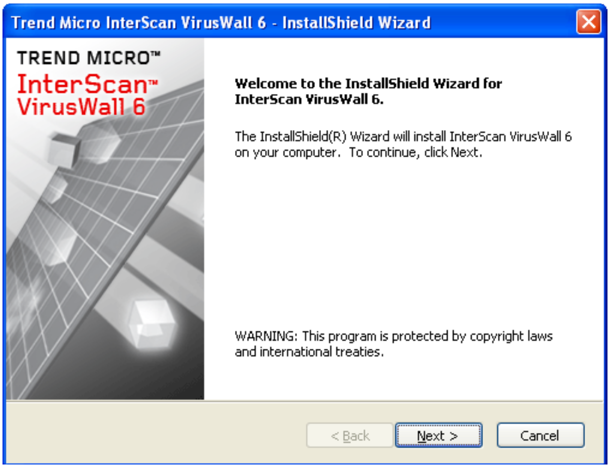
```
Migration output to C:\Package.out
Press any key to continue...
```

FIGURE 3-31. Migration Tool Export Utility screen

3. Press any key and the command window closes.
4. If you will be 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 InterScan VirusWall 6.
5. On the computer where you wish to install InterScan VirusWall 6, double-click setup.exe to start the installation process.

Note: If the InterScan VirusWall 6.01 Setup detects InterScan VirusWall 6.0 and they are the same language version, the Setup program will prompt you to confirm the build upgrade. If InterScan VirusWall 6.01 and 6.0 are different language versions, the Setup program will ask to uninstall version 6.0 before proceeding. If the Setup program detects that you have a different langauge version of InterScan VirusWall 6.01 installed, it will prompt you to uninstall the different language version and then proceed with the installation. Currently only the English version of InterScan VirusWall 6.01 is available.

6. When the Welcome screen shown in Figure 3-32 appears, click **Next**.



Welcome to the InstallShield Wizard for InterScan VirusWall 6.

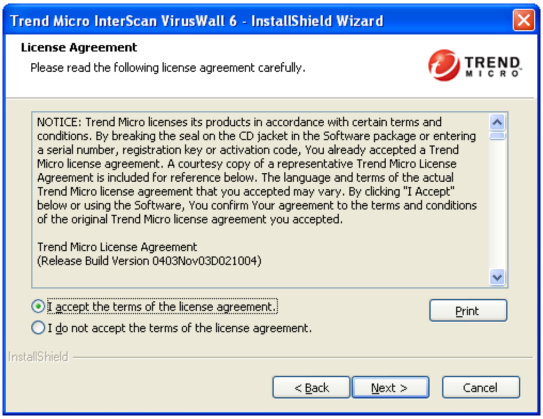
The InstallShield(R) Wizard will install InterScan VirusWall 6 on your computer. To continue, click Next.

WARNING: This program is protected by copyright laws and international treaties.

FIGURE 3-32. InterScan VirusWall Welcome screen

7. When the License Agreement screen shown in Figure 3-33 appears, read the entire license agreement and select **I accept the terms of the license agreement** to proceed with the installation. You can scroll through the entire agreement online or print it.

If you select **I do not accept the terms of the license agreement**, the installation process will terminate.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or entering a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement
(Release Build Version 0403Nov03D021004)

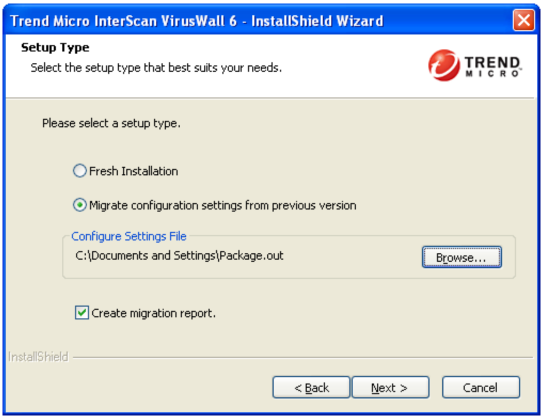
● I accept the terms of the license agreement.

○ I do not accept the terms of the license agreement.

FIGURE 3-33. License Agreement screen

8. When the Setup type screen shown in Figure 3-34 appears, select **Migrate configuration settings from previous version**. Click **Browse** to specify the location of the configuration settings file. If you do not want to create a report

that lists all the settings that were migrated, deselect **Create migration report**. Click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Please select a setup type.

○ Fresh Installation

● Migrate configuration settings from previous version

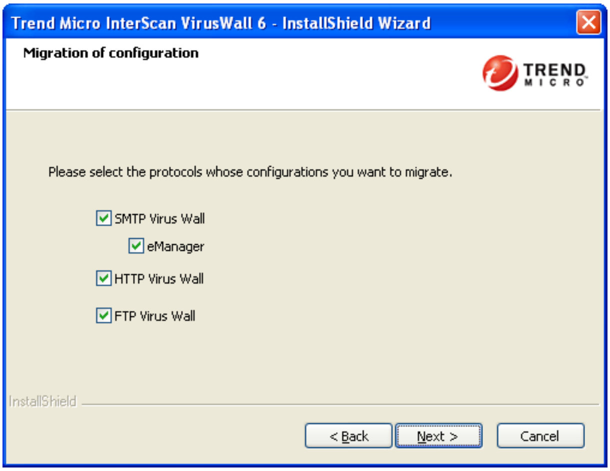
Configure Settings File

C:\Documents and Settings\Package.out

☑ Create migration report.

FIGURE 3-34. Setup Type screen with the Migrate option selected

9. When the Migration of configuration screen in Figure 3-35 appears, select the protocols whose configuration settings you want to migrate to InterScan VirusWall 6. Click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Migration of configuration

Please select the protocols whose configurations you want to migrate.

☑ SMTP Virus Wall

  ☑ eManager

☑ HTTP Virus Wall

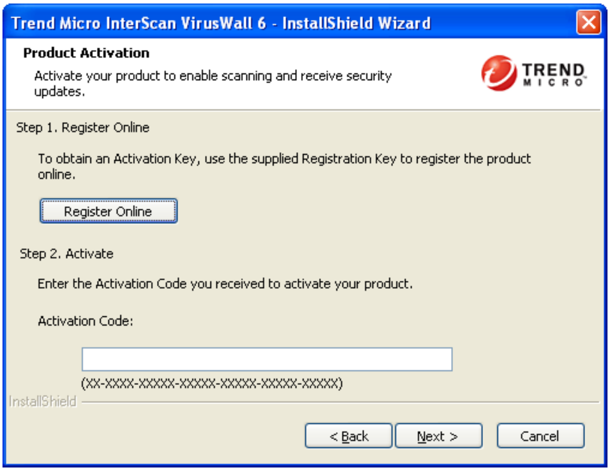
☑ FTP Virus Wall

FIGURE 3-35. Migration of configuration screen

Note: To migrate the configuration settings for eManager, select the SMTP protocol.

10. When the Product Activation screen shown in Figure 3-36 appears, do one of the following:

- If you have already registered and obtained a product activation code, then skip registration 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 you received in the Activation Code text box and click **Next**.
- Click **Next** without entering an activation code.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Product Activation

Activate your product to enable scanning and receive security updates.

Step 1. Register Online

To obtain an Activation Key, use the supplied Registration Key to register the product online.

Step 2. Activate

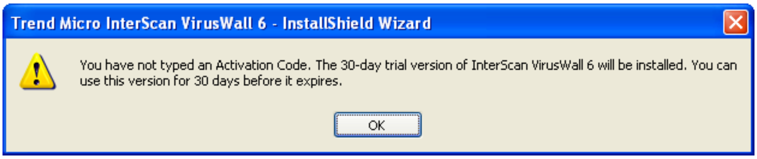
Enter the Activation Code you received to activate your product.

Activation Code:

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

FIGURE 3-36. Product Activation screen

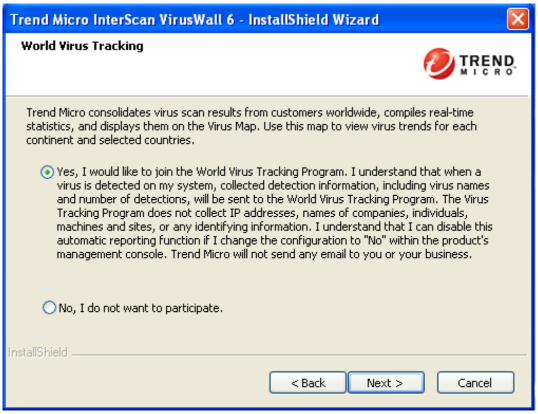
If you clicked **Next** without entering an activation code, the 30-day trial version of InterScan VirusWall 6 will be installed. Click **OK** to proceed with the installation.



You have not typed an Activation Code. The 30-day trial version of InterScan VirusWall 6 will be installed. You can use this version for 30 days before it expires.

FIGURE 3-37. Product Activation message

11. When the World Virus Tracking screen shown in Figure 3-38 appears, select whether your installation would like to participate in the Trend Micro World Virus Tracking Program, then click **Next**.



World Virus Tracking

Trend Micro consolidates virus scan results from customers worldwide, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries.

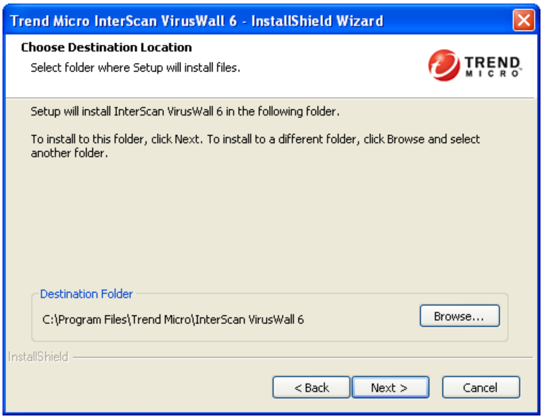
● Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, collected detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program. The Virus Tracking Program does not collect IP addresses, names of companies, individuals, machines and sites, or any identifying information. I understand that I can disable this automatic reporting function if I change the configuration to "No" within the product's management console. Trend Micro will not send any email to you or your business.

○ No, I do not want to participate.

FIGURE 3-38. World Virus Tracking screen

12. The Choose Destination Location screen shown in Figure 3-39 appears, indicating the directory path where InterScan VirusWall 6 will be installed. If you wish to change the directory path, click **Browse** and specify a different location.

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


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install InterScan VirusWall 6 in the following folder.

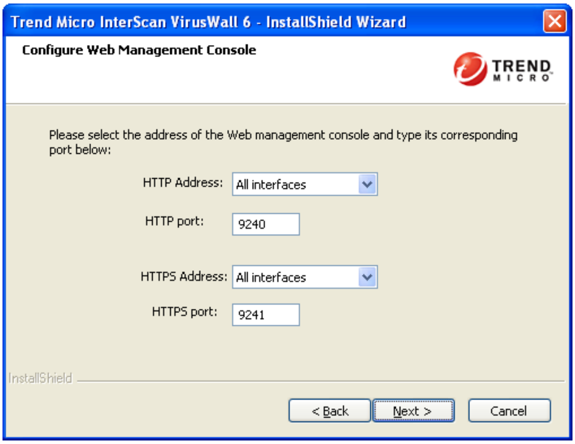
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Trend Micro\InterScan VirusWall 6

FIGURE 3-39. Choose Destination Location screen

13. When the Configure Web Management Console screen appears, specify where the Web management console will bind. Default settings are shown in Figure 3-40. Click **Next**.


Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Configure Web Management Console

Please select the address of the Web management console and type its corresponding port below:

HTTP Address: All interfaces

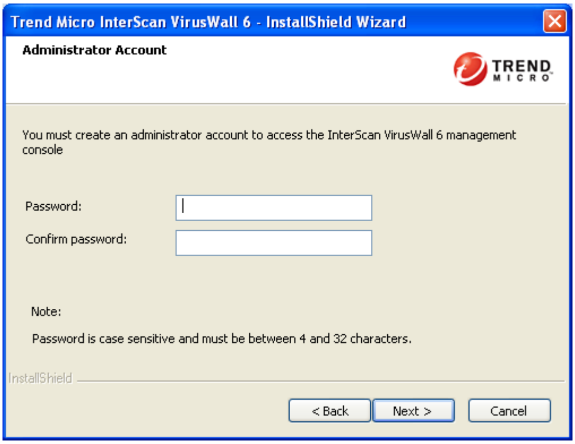
HTTP port: 9240

HTTPS Address: All interfaces

HTTPS port: 9241

FIGURE 3-40. Web Management Console Configuration screen

14. When the Administrator Account screen shown in Figure 3-41 appears, enter a 4- to 32-character password, confirm it, and click **Next**.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Administrator Account

You must create an administrator account to access the InterScan VirusWall 6 management console

Password:

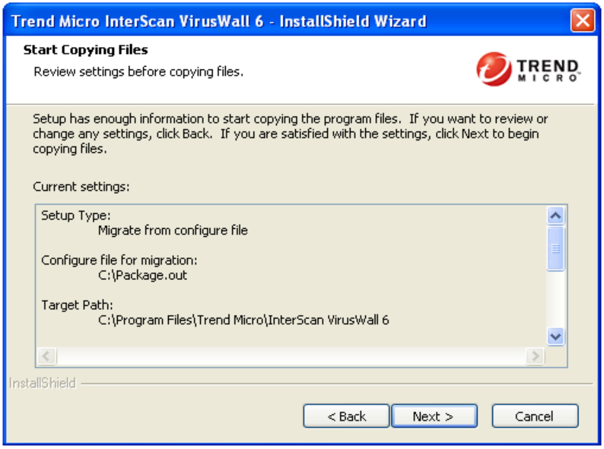
Confirm password:

Note:

Password is case sensitive and must be between 4 and 32 characters.

FIGURE 3-41. Administrator Account Password screen

15. When the Start Copying Files screen shown in Figure 3-42 appears, review the current settings.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current settings:

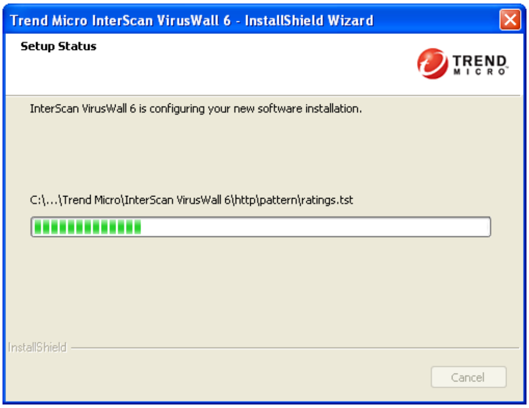
```
Setup Type:
          Migrate from configure file

Configure file for migration:
          C:\Package.out

Target Path:
          C:\Program Files\Trend Micro\InterScan VirusWall 6
```

FIGURE 3-42. Start Copying Files screen

- If the settings are correct, click **Next**.

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

The Setup Status screen shown in Figure 3-43 appears.



Trend Micro InterScan VirusWall 6 - InstallShield Wizard

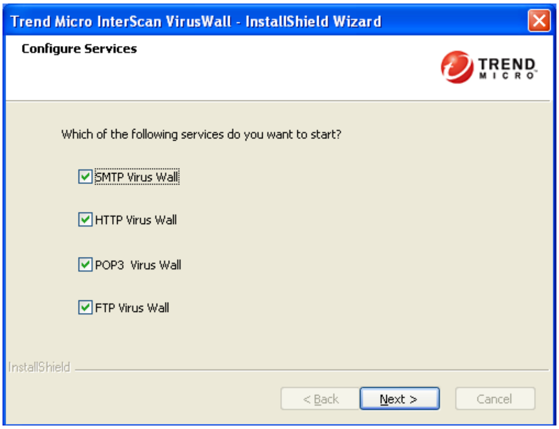
Setup Status

InterScan VirusWall 6 is configuring your new software installation.

C:\...\Trend Micro\InterScan VirusWall 6\http\pattern\ratings.tst

FIGURE 3-43. Setup Status screen

16. When Setup is complete, the Configure Services screen shown in Figure 3-44 appears. Select the InterScan VirusWall services you want to start after the installation has finished. By default, all services are selected to start. When you have made your selections, click **Next**.



Which of the following services do you want to start?

☑ SMTP Virus Wall

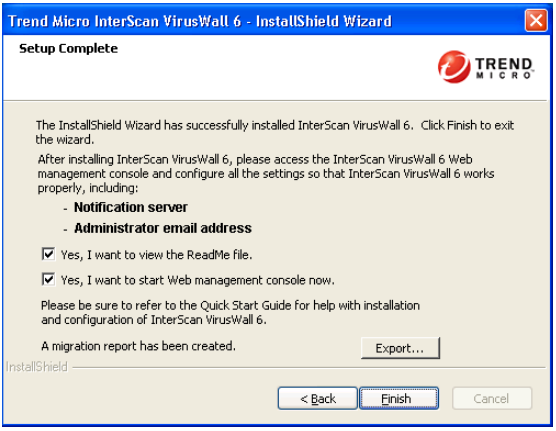
☑ HTTP Virus Wall

☑ POP3 Virus Wall

☑ FTP Virus Wall

FIGURE 3-44. Configure Services screen

17. When the Setup Complete screen shown in Figure 3-45 appears, you can do any of the following and then click **Finish**.



The InstallShield Wizard has successfully installed InterScan VirusWall 6. Click Finish to exit the wizard.

After installing InterScan VirusWall 6, please access the InterScan VirusWall 6 Web management console and configure all the settings so that InterScan VirusWall 6 works properly, including:

- **Notification server**
- **Administrator email address**

☑ Yes, I want to view the ReadMe file.

☑ Yes, I want to start Web management console now.

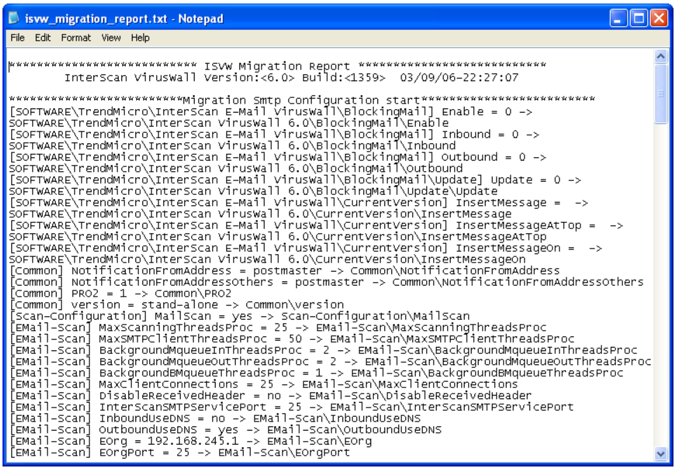
Please be sure to refer to the Quick Start Guide for help with installation and configuration of InterScan VirusWall 6.

A migration report has been created.

FIGURE 3-45. Setup Complete screen

- Choose to view the readme.txt file, which will display in a new window.

- Choose to start the Web management console. A Web browser window will open automatically and display the logon page for InterScan VirusWall 6.
- If you chose to create a migration report at the beginning of installation, click **Export**. The report will display in a new window, similar to the report shown in Figure 3-46.



```
*************************** ISVW Migration Report ***************************
        InterScan VirusWall Version:<6.0> Build:<1359>  03/09/06-22:27:07

*************************Migration Smtp Configuration start***************************
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Enable = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Enable
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Inbound = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Inbound
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail] Outbound = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Outbound
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\BlockingMail\Update] Update = 0 ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\BlockingMail\Update\Update
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessage =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessage
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessageAtTop =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessageAtTop
[SOFTWARE\TrendMicro\InterScan E-Mail VirusWall\CurrentVersion] InsertMessageOn =  ->
SOFTWARE\TrendMicro\InterScan VirusWall 6.0\CurrentVersion\InsertMessageOn
[Common] NotificationFromAddress = postmaster -> Common\NotificationFromAddress
[Common] NotificationFromAddressOthers = postmaster -> Common\NotificationFromAddressOthers
[Common] PRO2 = 1 -> Common\PRO2
[Common] version = stand-alone -> Common\version
[Scan-Configuration] MailScan = yes -> Scan-Configuration\MailScan
[EMail-Scan] MaxScanningThreadsProc = 25 -> EMail-Scan\MaxScanningThreadsProc
[EMail-Scan] MaxSMTPClientThreadsProc = 50 -> EMail-Scan\MaxSMTPClientThreadsProc
[EMail-Scan] BackgroundMqueueInThreadsProc = 2 -> EMail-Scan\BackgroundMqueueInThreadsProc
[EMail-Scan] BackgroundMqueueOutThreadsProc = 2 -> EMail-Scan\BackgroundMqueueOutThreadsProc
[EMail-Scan] BackgroundBMqueueThreadsProc = 1 -> EMail-Scan\BackgroundBMqueueThreadsProc
[EMail-Scan] MaxClientConnections = 25 -> EMail-Scan\MaxClientConnections
[EMail-Scan] DisableReceivedHeader = no -> EMail-Scan\DisableReceivedHeader
[EMail-Scan] InterScanSMTPServicePort = 25 -> EMail-Scan\InterScanSMTPServicePort
[EMail-Scan] InboundUseDNS = no -> EMail-Scan\InboundUseDNS
[EMail-Scan] OutboundUseDNS = yes -> EMail-Scan\OutboundUseDNS
[EMail-Scan] EOrg = 192.168.245.1 -> EMail-Scan\EOrg
[EMail-Scan] EOrgPort = 25 -> EMail-Scan\EOrgPort
```

FIGURE 3-46. Sample migration report

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

<ISVW_Installation_folder>\isvw_migration_report.txt

Upgrading from ISVW Windows Version 6.0

When upgrading from version 6.0 to version 6.01 the installer imports all of your previous settings.

Note: If the InterScan VirusWall 6.01 Setup detects InterScan VirusWall 6.0 and they are the same language version, the Setup program will prompt you to confirm the build upgrade. If InterScan VirusWall 6.01 and 6.0 are different language versions, the Setup program will ask to uninstall version 6.0 before proceeding. If the Setup program detects that you have a different langauge version of InterScan VirusWall 6.01 installed, it will prompt you to uninstall the different language version and then proceed with the installation. Currently only the English version of InterScan VirusWall 6.01 is available.

To start the upgrade process:

1. Double-click **setup.exe** to start the upgrade process. The Trend Micro InterScan VirusWall 6 - InstallShield Wizard screen appears.
2. Click **Next**. The Setup Status screen appears while InterScan VirusWall upgrades to version 6.01.
3. On the Update Complete screen, the installation program may prompt you to restart the computer. If prompted, choose to restart now or later and then click **Finish**

Post-Installation Tasks

After installing InterScan VirusWall 6, 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

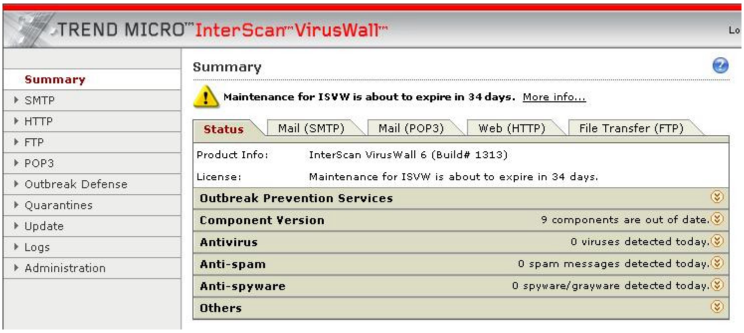
Using InterScan VirusWall 6

In this chapter, you will familiarize yourself with InterScan VirusWall 6 using the Web management console, and learn about tasks such as starting and stopping the various InterScan VirusWall 6 services, and testing key InterScan VirusWall 6 features.

Note: The online help discusses all the InterScan VirusWall 6 tasks that you can perform. It also provides a list of best practices to help you manage InterScan VirusWall 6 optimally.

InterScan VirusWall 6 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.



Summary

Maintenance for ISVW is about to expire in 34 days. More info...

Product Info: InterScan VirusWall 6 (Build# 1313)

License: Maintenance for ISVW is about to expire in 34 days.

Outbreak Prevention Services	
Component Version	9 components are out of date.
Antivirus	0 viruses detected today.
Anti-spam	0 spam messages detected today.
Anti-spyware	0 spyware/grayware detected today.
Others	

FIGURE 4-1. InterScan VirusWall 6 Web management console showing the Summary screen

Accessing the Console

After installation, InterScan VirusWall 6 automatically starts the basic services and the services you selected to start during installation. Although InterScan VirusWall 6 is configured to run on a robust set of default values, you should open the InterScan VirusWall 6 console and confirm the settings.

Use any of the following browsers to access the console:

- Internet Explorer 5.5 or above
- Firefox 1.5
- Netscape 8.0
- Mozilla 1.7

To access the console:

1. Open a Web browser, then type the InterScan VirusWall 6 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.

---

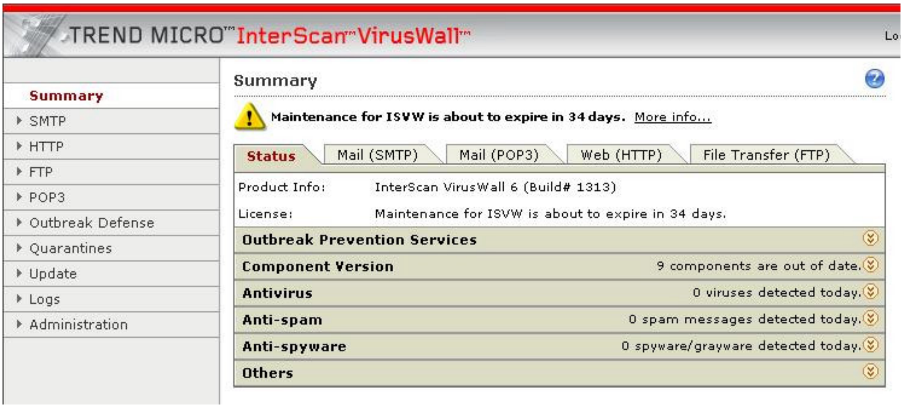
2. Type the password you specified during installation and click **Log On**. The Summary screen of the Web management console appears.

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 6 Administrator's Guide*.

Summary

The Summary menu item provides a quick overview of the status of InterScan VirusWall 6 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.



Summary

Maintenance for ISVW is about to expire in 34 days. More info...

Product Info:	InterScan VirusWall 6 (Build# 1313)
License:	Maintenance for ISVW is about to expire in 34 days.
Outbreak Prevention Services	
Component Version	9 components are out of date.
Antivirus	0 viruses detected today.
Anti-spam	0 spam messages detected today.
Anti-spyware	0 spyware/grayware detected today.
Others	

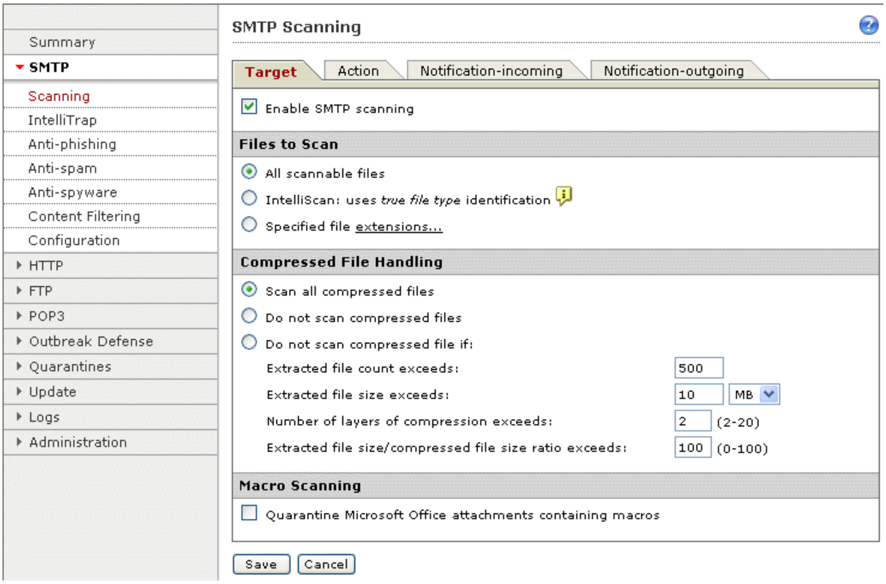
FIGURE 4-2. Summary screen

TABLE 4-1. Summary screen tabs

Tab	Available Information	Tasks
Status	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 InterScan VirusWall 6 components Roll back the previous versions of pattern files
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.



SMTP Scanning

☑ Enable SMTP scanning

Files to Scan

● All scannable files

○ IntelliScan: uses *true file type* identification

○ Specified file extensions...

Compressed File Handling

● Scan all compressed files

○ Do not scan compressed files

○ Do not scan compressed file if:

Extracted file count exceeds:	500
Extracted file size exceeds:	10 MB
Number of layers of compression exceeds:	2 (2-20)
Extracted file size/compressed file size ratio exceeds:	100 (0-100)

Macro Scanning

□ Quarantine Microsoft Office attachments containing macros

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

TABLE 4-2. Submenu items under SMTP

Submenu	Description	Tasks
Scanning	Provides real-time scanning of SMTP traffic	Enable or disable SMTP scanning 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

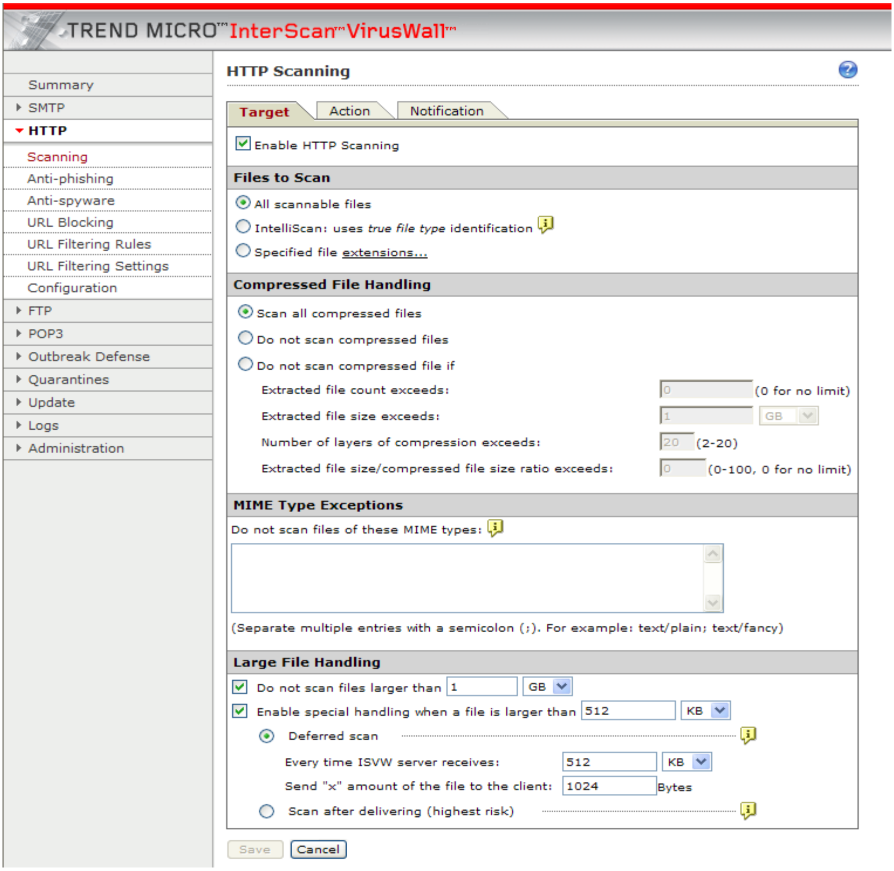
Submenu	Description	Tasks
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable SMTP IntelliTrap Determine the action to take against Bots detected by IntelliTrap (Quarantine, Delete, or Pass) Customize the notification message an administrator, 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	Detects spam messages sent through your SMTP email server	Enable or disable SMTP 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 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

Submenu	Description	Tasks
Anti-spyware	Detects spyware and allows you to perform specific actions upon it	Enable or disable SMTP 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 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 InterScan VirusWall 6 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 InterScan VirusWall 6 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.



HTTP Scanning

☑ Enable HTTP Scanning

Files to Scan

● All scannable files

○ IntelliScan: uses *true file type* identification

○ Specified file extensions...

Compressed File Handling

● Scan all compressed files

○ Do not scan compressed files

○ Do not scan compressed file if

Extracted file count exceeds: 0 (0 for no limit)

Extracted file size exceeds: 1 GB

Number of layers of compression exceeds: 20 (2-20)

Extracted file size/compressed file size ratio exceeds: 0 (0-100, 0 for no limit)

MIME Type Exceptions

Do not scan files of these MIME types:

(Separate multiple entries with a semicolon (;). For example: text/plain; text/fancy)

Large File Handling

☑ Do not scan files larger than 1 GB

☑ Enable special handling when a file is larger than 512 KB

● Deferred scan

Every time ISVW server receives: 512 KB

Send "x" amount of the file to the client: 1024 Bytes

○ Scan after delivering (highest risk)

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

TABLE 4-3. Submenu items under HTTP

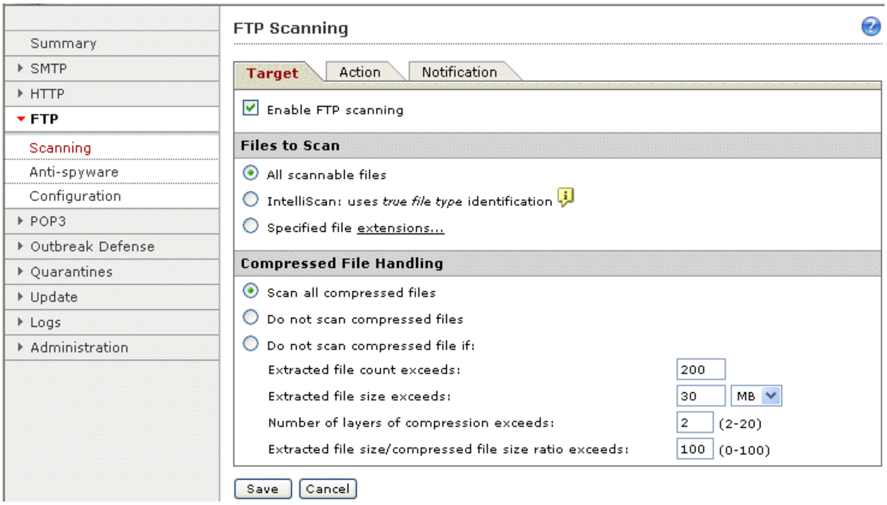
Submenu	Description	Tasks
Scanning	Lets you determine how InterScan VirusWall 6 scans HTTP traffic for viruses and other security risks in uploads and downloads	Enable or disable HTTP scanning Target the types of files to scan List MIME Type Exceptions Specify how InterScan VirusWall 6 handles large 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 InterScan VirusWall 6 detects an infected file
Anti-phishing	Lets you determine how InterScan VirusWall 6 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

Submenu	Description	Tasks
URL Blocking	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
URL Filtering Rules	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)
URL Filtering Settings	Defines how URL filtering is applied across the URL Categories in the InterScan VirusWall 6 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
Configuration	Allows you to specify configuration settings for your HTTP server	Determine if you want InterScan VirusWall 6 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.



FTP Scanning

☑ Enable FTP scanning

Files to Scan

● All scannable files

○ IntelliScan: uses *true file type* identification

○ Specified file extensions...

Compressed File Handling

● Scan all compressed files

○ Do not scan compressed files

○ Do not scan compressed file if:

Extracted file count exceeds: 200

Extracted file size exceeds: 30 MB

Number of layers of compression exceeds: 2 (2-20)

Extracted file size/compressed file size ratio exceeds: 100 (0-100)

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

TABLE 4-4. Submenu items under FTP

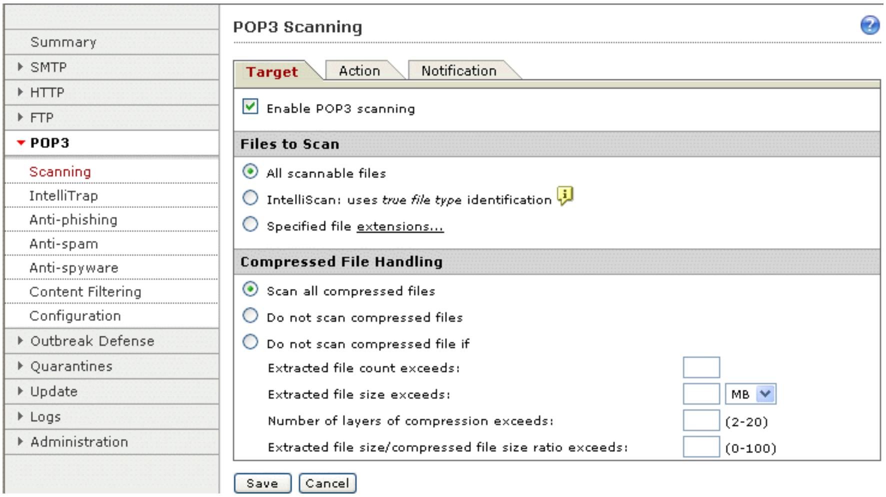
Submenu	Description	Tasks
Scanning	Checks all or specified types of files for viruses and other malware, including individual files within a compressed volume	Enable or disable FTP scanning Determine the files you want to scan Designate if and how attached compressed files are scanned Specify the action 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

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.



POP3 Scanning

☑ Enable POP3 scanning

Files to Scan

● All scannable files

○ IntelliScan: uses *true file type* identification

○ Specified file extensions...

Compressed File Handling

● Scan all compressed files

○ Do not scan compressed files

○ Do not scan compressed file if

Extracted file count exceeds:

Extracted file size exceeds: MB

Number of layers of compression exceeds: (2-20)

Extracted file size/compressed file size ratio exceeds: (0-100)

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

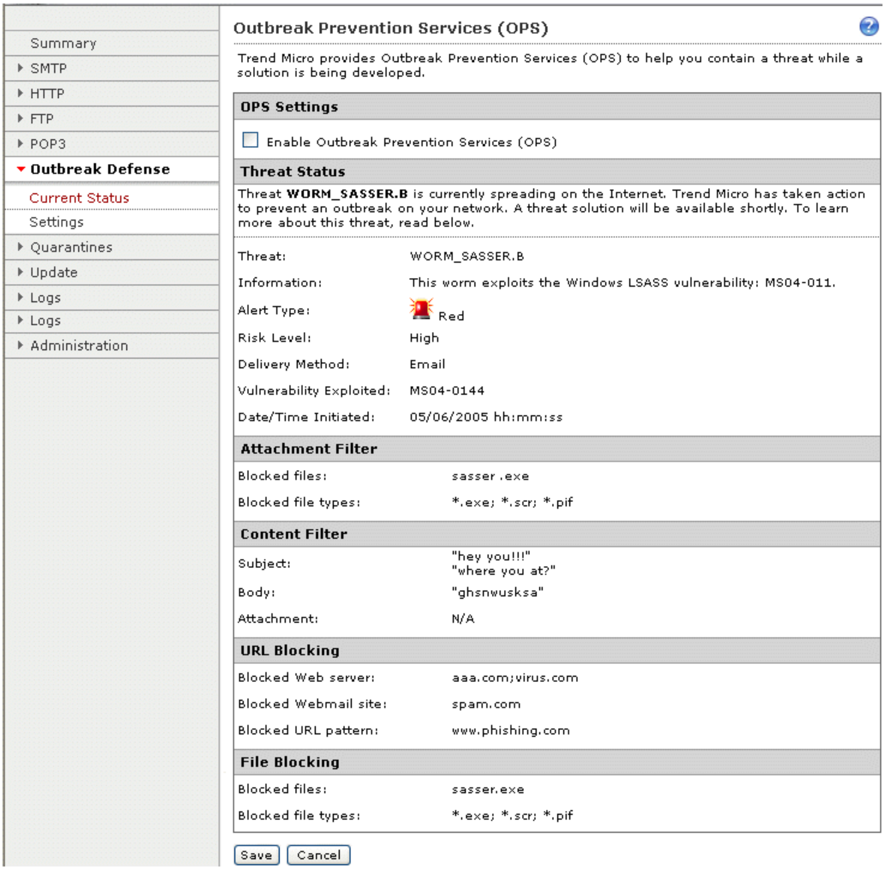
Submenu	Description	Tasks
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable POP3 IntelliTrap Take action on Bots detected by IntelliTrap (Quarantine, Delete, or Pass) Determine the action to take against Bots detected by IntelliTrap (Quarantine, 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

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 InterScan VirusWall 6's POP3 proxy server handles POP3 traffic	Specify the POP3 IP address the InterScan VirusWall 6 POP3 proxy server binds to Specify the number of simultaneous local connections allowed, the port POP3 clients will use to connect to InterScan VirusWall 6 (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.



Outbreak Prevention Services (OPS)

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

OPS Settings

□ Enable Outbreak Prevention Services (OPS)

Threat Status

Threat **WORM_SASSER.B** is currently spreading on the Internet. Trend Micro has taken action to prevent an outbreak on your network. A threat solution will be available shortly. To learn more about this threat, read below.

Threat:	WORM_SASSER.B
Information:	This worm exploits the Windows LSASS vulnerability: MS04-011.
Alert Type:	Red
Risk Level:	High
Delivery Method:	Email
Vulnerability Exploited:	MS04-0144
Date/Time Initiated:	05/06/2005 hh:mm:ss

Attachment Filter

Blocked files:	sasser .exe
Blocked file types:	*.exe; *.scr; *.pif

Content Filter

Subject:	"hey you!!!" "where you at?"
Body:	"ghsnwusksa"
Attachment:	N/A

URL Blocking

Blocked Web server:	aaa.com;virus.com
Blocked Webmail site:	spam.com
Blocked URL pattern:	www.phishing.com

File Blocking

Blocked files:	sasser.exe
Blocked file types:	*.exe; *.scr; *.pif

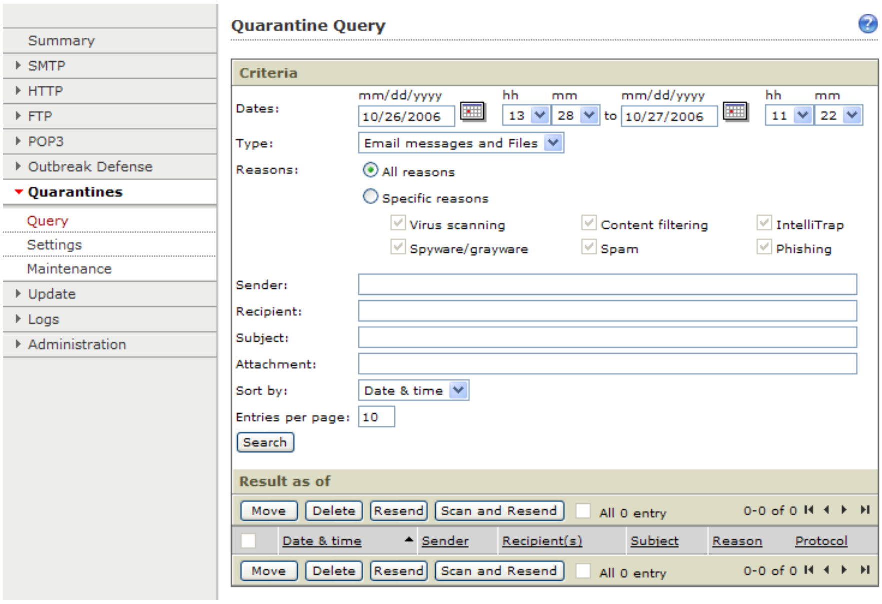
FIGURE 4-7. Outbreak Defense Current Status screen

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
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 InterScan VirusWall 6.



Quarantine Query

Criteria

Dates: mm/dd/yyyy 10/26/2006 hh 13 mm 28 to mm/dd/yyyy 10/27/2006 hh 11 mm 22

Type: Email messages and Files

Reasons:
● All reasons
○ Specific reasons
☑ Virus scanning ☑ Content filtering ☑ IntelliTrap
☑ Spyware/grayware ☑ Spam ☑ Phishing

Sender:

Recipient:

Subject:

Attachment:

Sort by: Date & time

Entries per page: 10

Result as of

□ All 0 entry 0-0 of 0

□	Date & time	Sender	Recipient(s)	Subject	Reason	Protocol

□ All 0 entry 0-0 of 0

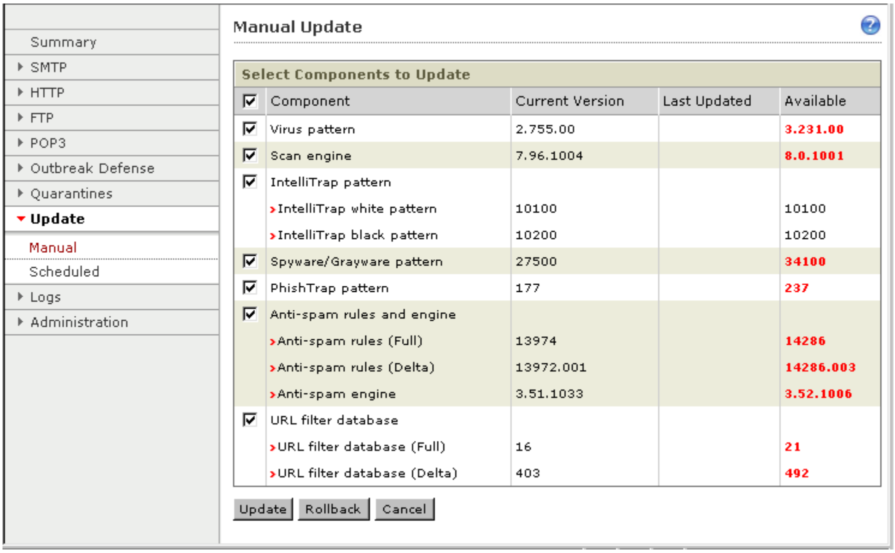
FIGURE 4-8. Quarantine Query screen

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 InterScan VirusWall 6 deletes them	Delete quarantined files Schedule automatic deletion times

Update

Because new malicious programs and offensive Web sites are developed and launched every day, InterScan VirusWall 6 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 InterScan VirusWall 6 ActiveUpdate server directly, then downloads the updates either manually or on a schedule.



Manual Update

Select Components to Update

☑	Component	Current Version	Last Updated	Available
☑	Virus pattern	2.755.00		3.231.00
☑	Scan engine	7.96.1004		8.0.1001
☑	IntelliTrap pattern			
	›IntelliTrap white pattern	10100		10100
	›IntelliTrap black pattern	10200		10200
☑	Spyware/Grayware pattern	27500		34100
☑	PhishTrap pattern	177		237
☑	Anti-spam rules and engine			
	›Anti-spam rules (Full)	13974		14286
	›Anti-spam rules (Delta)	13972.001		14286.003
	›Anti-spam engine	3.51.1033		3.52.1006
☑	URL filter database			
	›URL filter database (Full)	16		21
	›URL filter database (Delta)	403		492

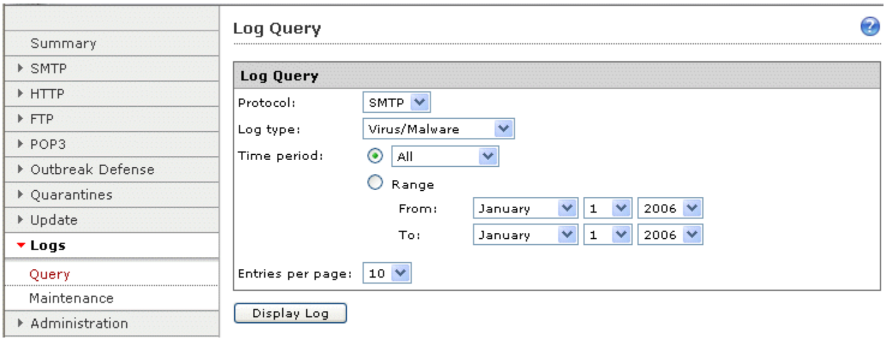
FIGURE 4-9. Manual Update screen

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 InterScan VirusWall 6 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 InterScan VirusWall 6 has detected.



Log Query

Log Query

Protocol: SMTP

Log type: Virus/Malware

Time period: ● All

○ Range

From: January 1 2006

To: January 1 2006

Entries per page: 10

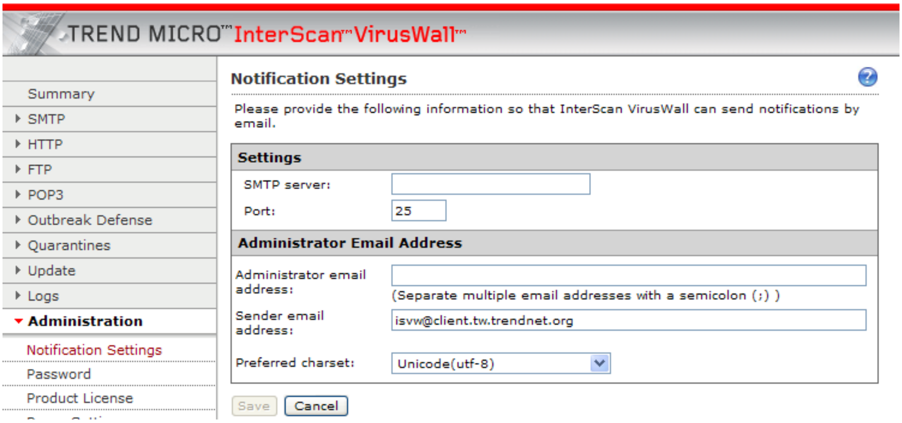
FIGURE 4-10. Log Query screen

TABLE 4-9. Submenu items under Logs

Submenu	Description	Tasks
Query	Lets you query the automatic logging feature in InterScan VirusWall 6	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

Administration

The Administration menu item allows you to manage the notification settings, password, license, and proxy settings of your InterScan VirusWall 6 installation. It also allows you to take part in Trend Micro's World Virus Tracking Program.



Notification Settings

Please provide the following information so that InterScan VirusWall can send notifications by email.

Settings

SMTP server:

Port: 25

Administrator Email Address

Administrator email address:
(Separate multiple email addresses with a semicolon (;))

Sender email address: isvw@client.tw.trendnet.org

Preferred charset: Unicode(utf-8)

FIGURE 4-11. Notification Settings screen

TABLE 4-10. Submenu items under Administration

Submenu	Description	Tasks
Notification Settings	Determines the settings that will be used when sending email notifications from InterScan VirusWall 6	Specify the following settings: • SMTP server • Port • Administrator email address • Preferred character set for receiving notifications • Sender's email address for notifications
Password	Allows you to change the password you use to log on to InterScan VirusWall 6	Specify the old password, the new password, and a new password confirmation to change your current password

TABLE 4-10. Submenu items under Administration

Submenu	Description	Tasks
Product License	Displays information about your maintenance agreement and product license for InterScan VirusWall 6	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
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 6

By default, all InterScan VirusWall 6 services you selected during installation are automatically started following installation. Each service can also be individually controlled by enabling or disabling real-time scanning for a given service.

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.

To restart all services:

1. From the **Control Panel**, click **Administrative Tools** > **Services** to open the Services window.
2. Navigate to **Trend Micro InterScan VirusWall 6** and click **Restart**.

   Trend Micro InterScan VirusWall 6 is typically set to **Automatic Startup**.

Testing InterScan VirusWall 6

After installation, test your InterScan VirusWall 6 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 InterScan VirusWall 6 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 InterScan VirusWall 6's virus clean/deletion features. InterScan VirusWall 6 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-FILE!
$H+H*
```

To test InterScan VirusWall 6 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 InterScan VirusWall 6 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.

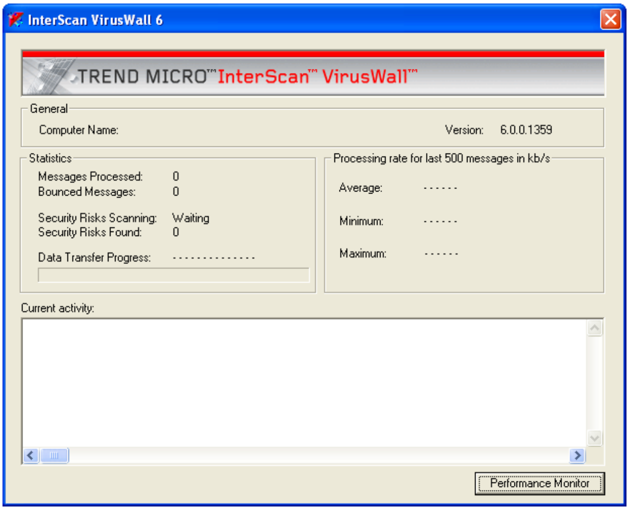
   The Quarantine Query Results panel shows the date and time the email was quarantined, the sender and recipient email addresses, the subject of the email, and the reason it was quarantined.

Using Real-time Scan Monitor

The InterScan VirusWall 6 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 6 > InterScan VirusWall 6 Real-time Scan Monitor**. When you send email through SMTP, real-time statistics and activity information are shown in the monitor panel.


InterScan VirusWall 6
TREND MICRO™ InterScan™ VirusWall™
General
Statistics
Processing rate for last 500 messages in kb/s
Current activity:
Performance Monitor

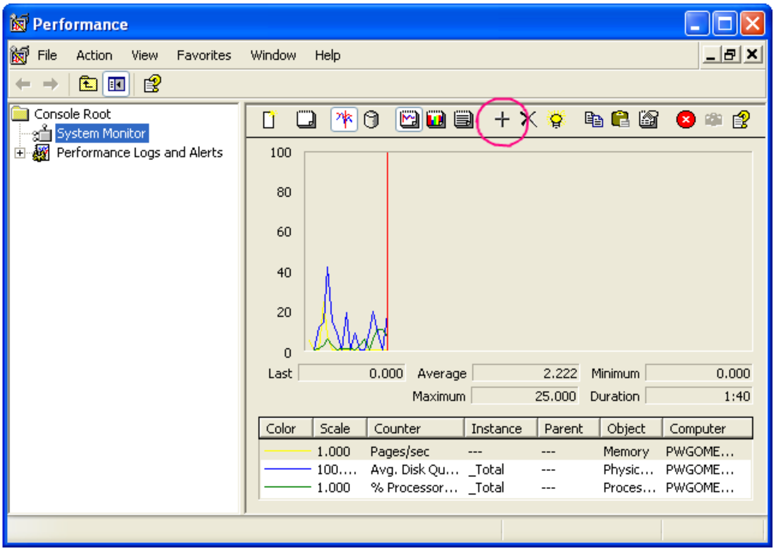
Computer Name:
Version: 6.0.0.1359

Messages Processed: 0
Bounced Messages: 0
Security Risks Scanning: Waiting
Security Risks Found: 0
Data Transfer Progress: - - - - - - - - - - - - - -

Average: - - - - - -
Minimum: - - - - - -
Maximum: - - - - - -

FIGURE 4-12. The InterScan VirusWall 6 Real-time Scan Monitor

2. Click **Performance Monitor** to open the Windows Performance Monitor.



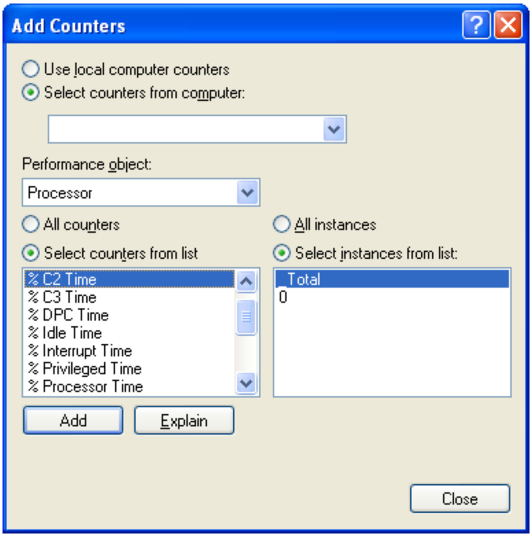
Last 0.000 Average 2.222 Minimum 0.000
Maximum 25.000 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
—	1.000	Pages/sec	---	---	Memory	PWGOME...
—	100....	Avg. Disk Qu...	_Total	---	Physic...	PWGOME...
—	1.000	% Processor...	_Total	---	Proces...	PWGOME...

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.



Add Counters

○ Use local computer counters

● Select counters from computer:

Performance object: Processor

○ All counters

● Select counters from list

% C2 Time
% C3 Time
% DPC Time
% Idle Time
% Interrupt Time
% Privileged Time
% Processor Time

○ All instances

● Select instances from list:

_Total
0

FIGURE 4-14. The Add Counters screen

2. Select the **Select counters from computer** option and then select the computer where InterScan VirusWall 6 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 ISVW 6.

If your problem is not included in the list of issues provided in this chapter, refer to the Administrator's Guide. If you need further assistance, see *Obtaining Technical Support* on page 5-7.

Troubleshooting

Issue	Explanations, Possible Causes and Solutions
Unsuccessful installation	• System requirements are not satisfied. See *System Requirements* on page 2-2. • If the operating system version or service pack is not satisfied, installation will not proceed. • There is insufficient space on the target disk. You need at least 2GB of hard disk space to install ISVW 6. Free up some disk space or install ISVW on a server with sufficient disk space. • A previous version of ISVW other than version 3.55 may already be installed. Uninstall ISVW first, and then run Setup again. • 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.

Issue	Explanations, Possible Causes and Solutions
Failure to migrate configuration settings during installation	• Failure to migrate from file occurs when you are installing ISVW 6 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 *Migrating the configuration settings to a different computer:* on page 3-21. • Install ISVW 6 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 6 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 *Migrating the configuration settings to a different computer:* on page 3-21. • Install ISVW 6 again on the machine. To re-install ISVW 6, see *Installing on the same host and migrating the configuration settings:* on page 3-11. • If you have satisfied the above requirements and migration still fails, contact Trend Micro Support.
100% CPU utilization right after installation	This normally happens because ISVW 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.

Issue	Explanations, Possible Causes and Solutions
Issues after upgrading from ISVW 3.55 with eManager 3.52 to ISVW 6	• The eManager 3.52 plug-in may still be installed after upgrading because other machines with ISVW 3.55 are still using the plug-in. It is possible for several ISVW 3.55 installations to share the same eManager 3.52 plug-in. • All content filter settings were migrated but all of them may be disabled upon upgrade because: • In version 3.55, the service "InterScan eManager Content Management" is disabled while doing migration. • In eManager 3.52, the "Attachment Filter > Enable attachment filter" option is disabled while doing migration. • ISVW 6 does not support the migration of email management rules. You need to define these rules again. • Migration of anti-spam rules is not supported. ISVW uses eManager 6 to support the content filtering feature, and the anti-spam feature is provided by Trend Micro Anti-spam Engine 3.52. • The Configuration window of ISVW 3.55 is still open after the upgrade. Stop the process manually from Windows Task Manager, and then remove all files under the path where ISVW 3.55 was installed. • Some folders under the installation folder of eManager 3.55 still exist after the upgrade. Manually delete these folders.
Cannot stop or start a service	• If you cannot stop a service after following the procedure in *Starting and Stopping InterScan VirusWall 6* on page 4-22: • Go to **Control Panel** > **Administrative Tools** > **Services**, right-click the service and then click **Stop**. • If this does not work, Go to **Control Panel** > **Administrative Tools** > **Services**, right-click the service and then click **Properties**. In the General tab, go to **Startup type:** and choose **Manual**. Restart the system. After restart, the status becomes "Stopped". • If you cannot start a service after following the procedure in *Starting and Stopping InterScan VirusWall 6* on page 4-22, call Trend Micro Technical Support.

Issue	Explanations, Possible Causes and Solutions
Cannot update license	• Activate your product before you update your license. • Do not use an evaluation-version of ISVW to update your license. • If you encounter a system or program exception error in the backend online update license server, please wait for a few minutes and try again. If you are still experiencing problems, contact Trend Micro Technical Support. • If you cannot update your license because of an incorrect server URL restored 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, please check the network status. If you are using a proxy server, check if the server can connect to the Product Registration server. If you are still experiencing problems, contact Trend Micro Technical Support.
Problems with activation	• The Activation Code used is invalid. • Do not use your full-version or evaluation-version Activation Code to activate the product again. • The evaluation-version or full-version Activation Code you used has expired. • Do not use an evaluation-version Activation Code if you installed a full version, and vice versa. • If activation still fails, contact Trend Micro Support.

Issue	Explanations, Possible Causes and Solutions
Web management console issues	• If the Web management console does not display normally after typing some Chinese/Japanese characters in a text box, check the encoding of the browser. For Internet Explorer, go to View > Encoding and select UTF-8 so that web UI can display DBCS characters (such as Chinese/Japanese) correctly. • If the Web management console does not open, check the machine where ISVW is installed. Make sure 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 6 installations are eligible for technical support. If your ISVW 6 is not registered, there is no way to recover your password.

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
- If you are not able to find an answer in the documentation or the Knowledge Base, 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