TREND MICRO™

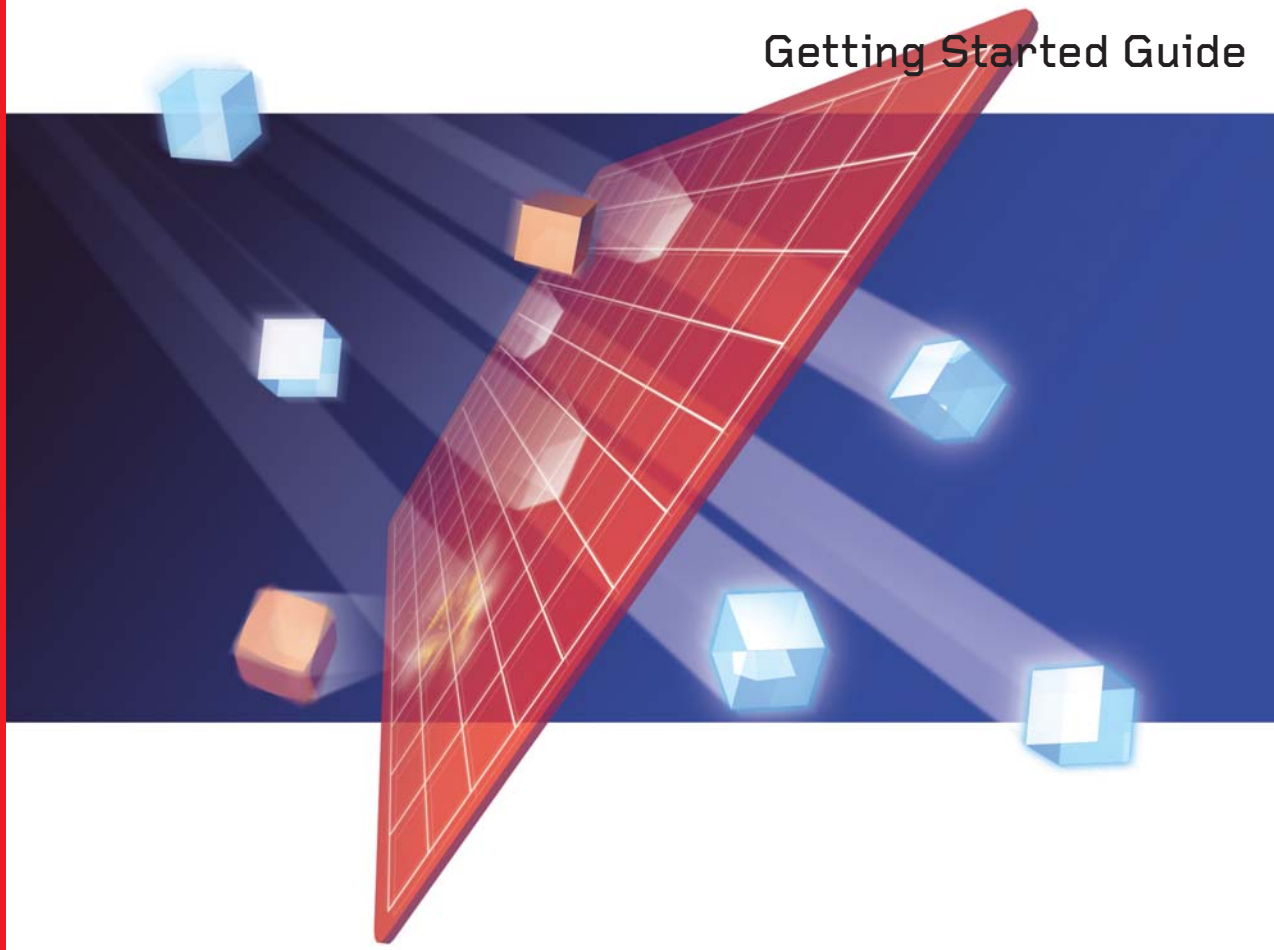
InterScan VirusWall™ 5

for Small and Medium Businesses

Integrated virus and spam protection for your Internet gateway

for Linux™

Getting Started Guide



TREND MICRO™

Document Part No. IVEM51899/40505

Release Date: July, 2004

Protected by U.S. Patent No. 5,623,6000, 5,889,943, 5,951,698, and 6,119,165

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

For technical support, please refer to Chapter 7, *Troubleshooting*, for technical support information and contact details. Detailed information about how to use specific features within the software is available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any other Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

`http://www.trendmicro.com/download/documentation/rating.asp`

Contents

Chapter 1

Introducing InterScan VirusWall for SMB

InterScan™ VirusWall™ (ISVW) for Small and Medium Businesses (SMB) provides an all-in-one antivirus and content management solution for your organization's network. For example, you do not have to install separate applications for virus protection, spam detection, or content filtering—all of these functions are available. ISVW for SMB provides protection for major traffic protocols—SMTP, HTTP, and FTP, as well as POP3 traffic, to ensure that employees don't accidentally bring in viruses from their personal email accounts. And, the application is easy-to-use.

Important features

ISVW for SMB helps you manage your network in the following ways:

- Scans for traffic containing viruses, and manages infected messages or files
- Scans for spam at low to high threshold levels, and allows you to determine how spam is handled
- Filters offensive or inappropriate content
- Blocks incoming file types that can damage your network
- Helps prevent DoS (Denial of Service) attacks by setting limits on message size
- Blocks connections to URLs or FTP sites prohibited by your corporate policies

Benefits

InterScan VirusWall for SMB:

- Is easy to install with the InterScan VirusWall for SMB installation wizard
- Allows you to fine-tune configuration of the scanning, anti-spam, and filtering features after installation
- Provides approved senders and blocked senders functionality for file and URL blocking
- Can be configured to automatically update the virus pattern file, scan engine, and spam rules and engine, as soon as a new version becomes available from Trend Micro
- Provides notifications to make sure you stay informed of activity, and alerts that trigger under conditions requiring attention
- Provides log files that are purged automatically after 30 days
- Provides a user-friendly management console that includes online help to guide you through tasks

Getting started

If you have already installed ISVW for SMB, skip chapters 2 and 3, which describe how to plan for installation, and install. If not, review the information in these two chapters, as well as the readme file, prior to installation. A setup program guides you through the installation process.

Important terms

Terms are used throughout the documentation and online help that may not be familiar to you, or may be used in an alternate way from what you might expect. A glossary of terms is available in the Glossary.

Available documentation

The documentation for this product assumes that you are experienced with Linux operating systems, and that you are at least a novice system administrator who is familiar with the basic concepts of administering a network. It is also assumed that you have superuser privileges to manage the security applications in your network.

The documentation available for InterScan VirusWall for SMB is:

- This document—*InterScan VirusWall for SMB Getting Started Guide*
- Readme file—Contains important late-breaking information about InterScan VirusWall for SMB
- Online Help—Two kinds of online help are available:
  - Context-sensitive screen help, which explains how to perform tasks on one screen
  - General help, which explains tasks that require action on several screens, or peripheral knowledge needed to complete tasks
- Knowledge Base—An online database of problem-solving and troubleshooting information. Knowledge base provides the latest information about known product issues. To access the Knowledge Base, select the Knowledge Base link in online general help, or visit:

  `kb.trendmicro.com/solutions/solutionSearch.asp`

Management console

After you have successfully installed ISVW for SMB, the **Logon** screen displays. Type the password you created on the **Administrator Account** screen in the installation script. Click **Enter** to access the management console.

Here is the appearance of the management console when you first log in.

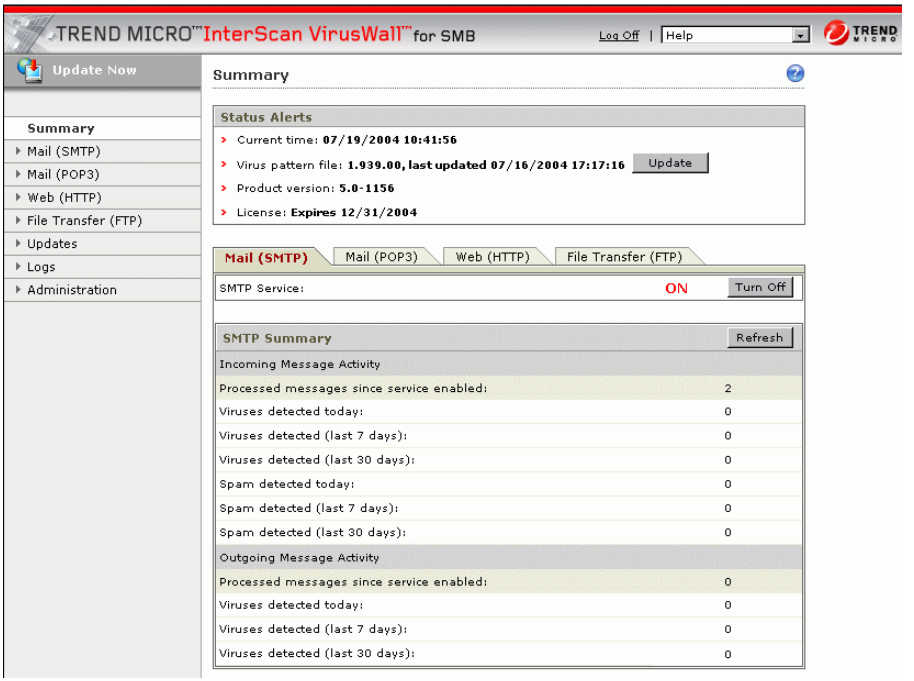


FIGURE 1-1. Summary screen on the InterScan VirusWall management console

Navigation panel

The left side of the management console is a main menu, that also serves as a navigation panel. Click a selection in the navigation panel to open its corresponding screen. A selection is compressed when the arrow is pointing right, a selection is

expanded when the arrow is pointing down.The right side of the screen does not refresh until you click a selection name on the menu.

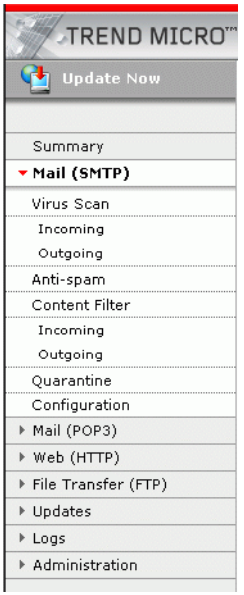


FIGURE 1-2. Navigation panel in the ISVW console

Note: Click the **Update Now** link to go directly to the **Manual Update** screen. This screen is described in Chapter 5.

In the InterScan VirusWall for SMB documentation, a path such as Mail (SMTP) > Virus Scan > Incoming > Action, indicates that:

- The main selection in the navigation panel is Mail (SMTP)
- The secondary selection is Virus Scan
- The tertiary selection is Incoming
- The selected tab on the **SMTP Incoming Virus Scan** screen is the **Action** tab

Tab behavior

The action screens for your selection display on the right side of the management console. Many of the screens have several tabs. The active tab name displays in reddish-brown; inactive tab names display in black text.

Typically the tabs are related and work together. For example, in the following figure, all three tabs are needed to configure virus scanning of incoming SMTP traffic.

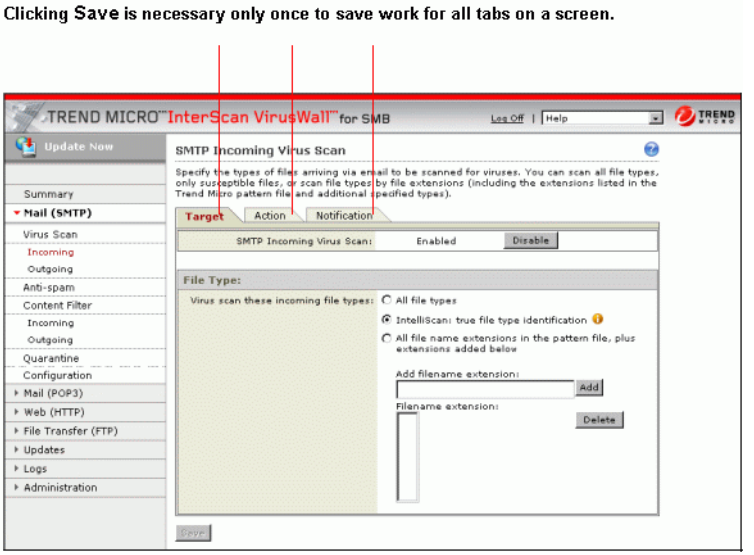


FIGURE 1-3. Tab behavior in InterScan VirusWall for SMB

- **Target**—Allows you to define the scope of activity to be acted upon
- **Action**—Allows you to define the action to be taken when a trigger event (such as an attempt to transfer an infected file via FTP) has taken place - examples of actions are clean, delete, or quarantine
- **Notification**—Allows you to compose a notification message, as well as define who is notified of the event and the action

For related tabs such as these, clicking **Save** once saves work on all three tabs.

The appearance of the **Save** button indicates whether saving is necessary. The **Save** button is unavailable when the screen first opens. After you perform tasks on the

screen, the appearance of the **Save** button changes so the text on the button appears black instead of gray. This is an indication that a **Save** is necessary to validate the work you have done.

If you try to leave a screen before you click **Save**, a message displays, prompting you to confirm whether you want to exit the screen without saving your work.

Information icon

Some screens in the management console contain an information icon. Position your mouse over the information icon to display a popup text box with additional information, to help you make a decision or complete a task.

In the following example, mousing over the information icon displays more information about IntelliScan, one of several options available for determining the type of virus scanning to be performed:

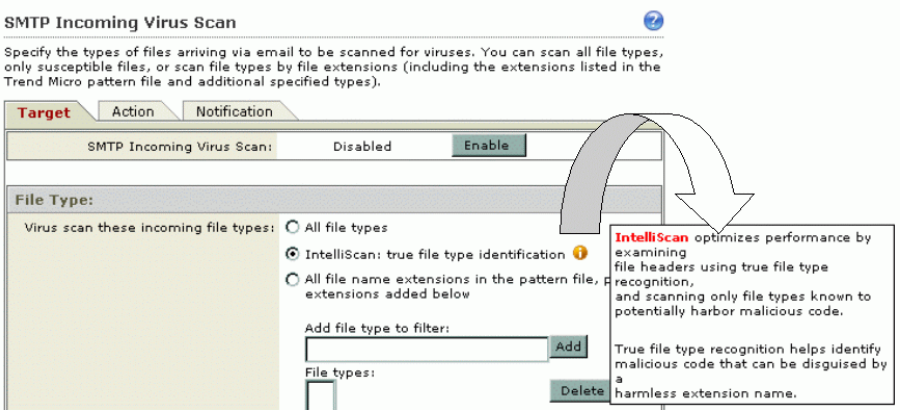


FIGURE 1-4. Information icon

Online help

Invoke general help by selecting the help feature in the InterScan VirusWall banner. To invoke screen help, click the screen help icon.

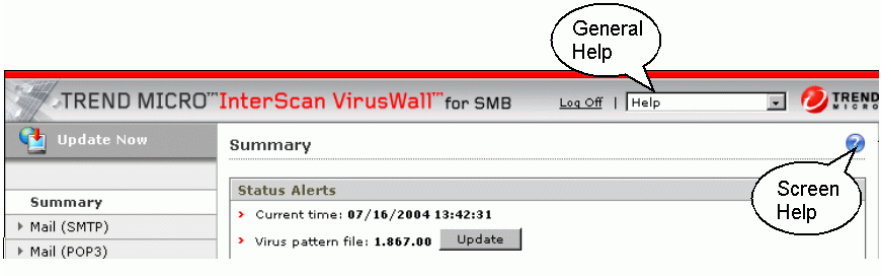
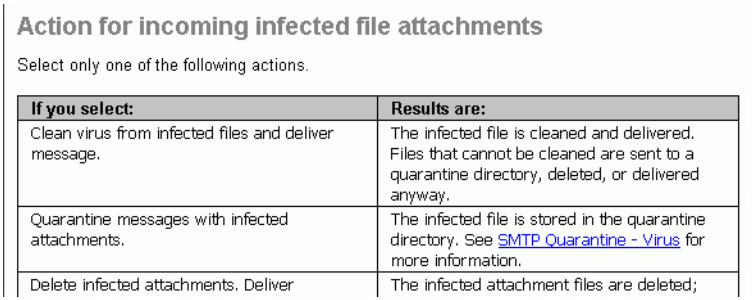


FIGURE 1-5. Help icons on InterScan VirusWall screens

Search the online help, by selecting **Contents and Index** from the general **Help** pull-down menu.

Links in online help

The online help contains links, indicated by blue underlined text. Clinking a link either takes you to another help screen or displays a popup text box with additional information. In the following example, the SMTP Quarantine - Virus link takes you to another help screen.



Action for incoming infected file attachments

Select only one of the following actions.

If you select:	Results are:
Clean virus from infected files and deliver message.	The infected file is cleaned and delivered. Files that cannot be cleaned are sent to a quarantine directory, deleted, or delivered anyway.
Quarantine messages with infected attachments.	The infected file is stored in the quarantine directory. See SMTP Quarantine - Virus for more information.
Delete infected attachments. Deliver	The infected attachment files are deleted;

FIGURE 1-6. Online help links can take you to another help screen

In the following example, the false positives link displays a definition for the term "false positive:"

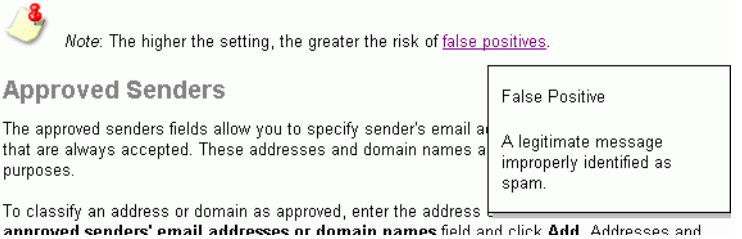


FIGURE 1-7. Online help links can display a popup text box

Most of the documentation in the online help is not repeated in this *Getting Started Guide*. Be sure to read the online help for more information about InterScan VirusWall.

Opening a management console from a browser

You can open the management console remotely from another machine using your Web browser. To log in remotely, you can either log in over HTTP, or HTTPS.

- To log in over HTTP, type http://*IP address of the SMB server*:1812, for example, http://123.123.123.123:1812
- To log in over HTTPS, type https://*IP address of the SMB server*:8443

The logon screen for the management console appears in your browser.

Chapter 2

Planning Your Installation

Before you install and configure InterScan VirusWall, there are decisions to make about how you want to implement the product in your network. This chapter serves as a pre-installation checklist, to help you:

- Consider and prepare the information you must provide to complete installation and configuration successfully, and
- Keep accurate documentation of your network configuration for such events as upgrades, troubleshooting, disaster recovery, or training new personnel

Recommended system requirements

Install InterScan VirusWall on a system with:

Hardware

- 650MHz Intel Pentium™ III-compatible or higher processor
- 512MB RAM
- Minimum 500MB free hard disk space

Supported OS

- Red Hat™ Enterprise Linux, Advanced Server 2.1
- Red Hat Enterprise Linux, Advanced Server 3.0
- Turbolinux™ 8.0 Server
- SuSE™ Linux 9.0

Note: To install ISVW-SMB on Red Hat Enterprise Linux, Advanced Server 3.0, your system must have "compact-libstdc++-7.3-2.96.122" or higher installed. This library can be found on disk 3 of the Red Hat installation CDs. Install the library using the following command:

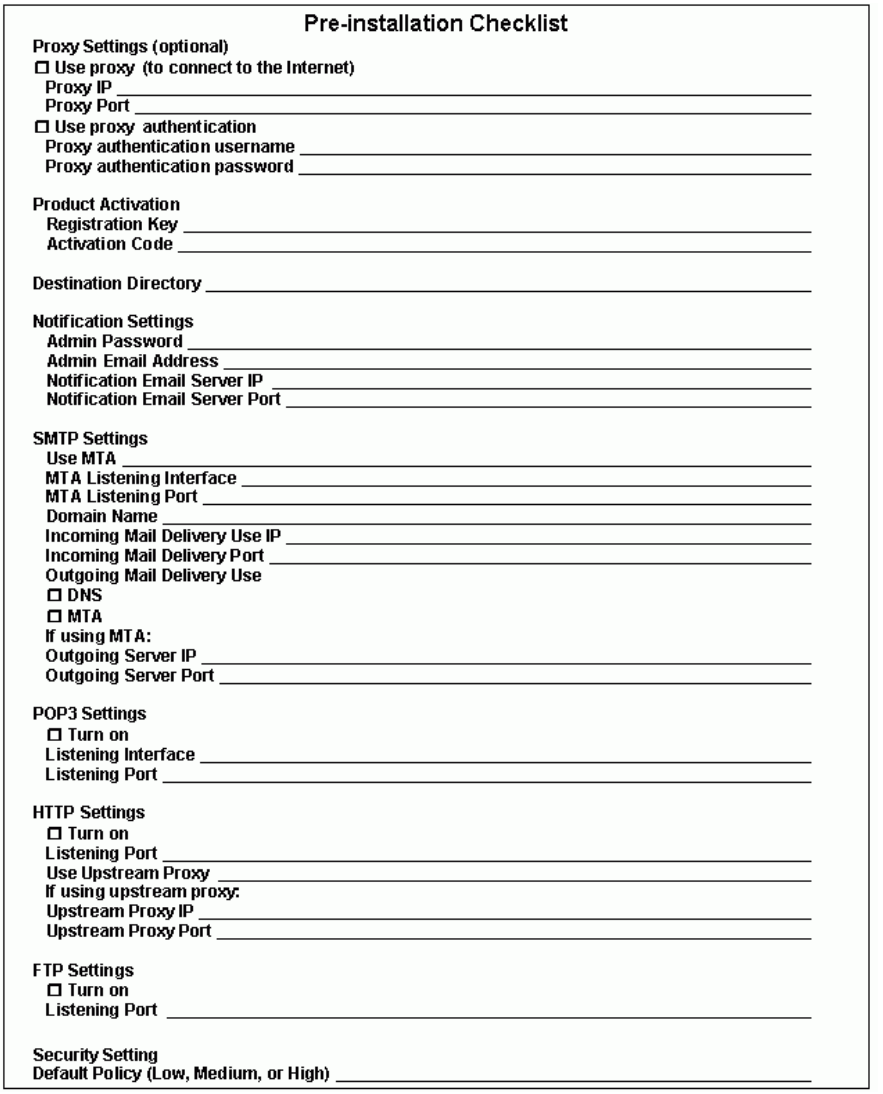
```
rpm -Uhv /mnt/cdrom/RedHat/RPMS/compat-libstdc++-7.3-2.96.122.i386.rpm
```

Software

- You must have one of the following MTA's available:
  - SendMail™ 8.11 or 8.12, or
  - Postfix 2.0.1x or Postfix 2.0.20
- You must have one of the following browsers available for the Web console: (JavaScript™ must be enabled)
  - Netscape™ Navigator 7.0 or higher, or
  - Internet Explorer 5.5 or higher

Note: The Java Runtime Environment (JRE) 1.4 or higher must be enabled to view the online help.

Pre-installation checklist



Pre-installation Checklist

Proxy Settings (optional)
☐ Use proxy (to connect to the Internet)
Proxy IP _____
Proxy Port _____
☐ Use proxy authentication
Proxy authentication username _____
Proxy authentication password _____

Product Activation
Registration Key _____
Activation Code _____

Destination Directory _____

Notification Settings
Admin Password _____
Admin Email Address _____
Notification Email Server IP _____
Notification Email Server Port _____

SMTP Settings
Use MTA _____
MTA Listening Interface _____
MTA Listening Port _____
Domain Name _____
Incoming Mail Delivery Use IP _____
Incoming Mail Delivery Port _____
Outgoing Mail Delivery Use
☐ DNS
☐ MTA
If using MTA:
Outgoing Server IP _____
Outgoing Server Port _____

POP3 Settings
☐ Turn on
Listening Interface _____
Listening Port _____

HTTP Settings
☐ Turn on
Listening Port _____
Use Upstream Proxy _____
If using upstream proxy:
Upstream Proxy IP _____
Upstream Proxy Port _____

FTP Settings
☐ Turn on
Listening Port _____

Security Setting
Default Policy (Low, Medium, or High) _____

FIGURE 2-1. Pre-installation checklist

Review each section of the checklist and record your responses. You can write your answers in the space provided, or print another copy of these pages from the following Web site:

`http://www.trendmicro.com/download/product.asp?productid=13`

An example is shown following the explanation of each section on the checklist.

WARNING! *Make sure your responses are appropriate for your environment. Responses shown in the example demonstrate the format or type of data expected, but will not necessarily be valid for your environment.*

Proxy settings (1/9)

If you have an existing proxy server for downloading the pattern file and scan engine from the Trend Micro ActiveUpdate server, you are prompted during installation to supply the IP address and port number for your existing proxy server.

If you have an existing proxy server and are required to use an authenticated logon, you must also specify an authentication user name and password.

If you are not currently using a proxy server, this information is not required and you can skip to the next section of the checklist.

Product activation (2/9)

As you are installing InterScan VirusWall, you are prompted to indicate whether the product has been activated via the registration process on the Trend Micro Online Registration Web site. You can install InterScan VirusWall, skipping both the registration and activation steps, but you cannot use the features of the product such as virus scanning until these steps are completed.

Registration Key

A product Registration Key is required to complete the product registration process. A Registration Key uses 22 characters, including hyphens, in following format:

XX-XXXX-XXXX-XXXX-XXXX

InterScan VirusWall must be registered, using your product Registration Key, before you receive an Activation Code that allows you to begin using InterScan VirusWall.

See Chapter 4, *Registering and Activating InterScan VirusWall*, for more information about obtaining your Registration Key, and procedures to register InterScan VirusWall. Trend Micro recommends that you register your product before beginning the installation process.

Activation Code

An Activation Code is required to enable scanning, receive product updates, and display the status of your license in the management console. An Activation Code uses 37 characters, including hyphens, in the following format:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

After you have completed the product registration process, you will receive your Activation Code from Trend Micro. See Chapter 4, *Registering and Activating InterScan VirusWall*, for more information about obtaining your Activation Code, and procedures to activate InterScan VirusWall.

Destination directory (3/9)

Decide which machine in your network will act as the InterScan VirusWall server. You must install directly on this machine; InterScan VirusWall cannot be installed remotely.

On the machine you have chosen, select the destination directory where InterScan VirusWall will be installed. The default selection is:

```
/opt/trend/isvw
```

If you do not want to install in the default directory path, modify the path to a directory of your choice.

Note: It is a good idea to make a record of the machine name, physical location, and IP address as well.

Notification settings (4/9)

During installation, you are prompted to enter a system administrator password to access the InterScan VirusWall management console.

Note: You *must* modify the settings on this screen.

The password should be at least eight characters in length, using a combination of alpha and numeric characters.

A notification administrator email address is also required, as well as the IP address and port of the notification email server to be used for the notifications.

SMTP settings (5/9)

If you will *not* be using InterScan VirusWall to scan your SMTP traffic, modify the value in the **Turn** field to "off." However, even if you are not using InterScan VirusWall to scan your SMTP traffic for viruses, you are prompted to specify configuration settings.

Your original configuration was probably arranged so that messages would go between the Internet and clients via a mail transfer agent (MTA) on an MTA server. When InterScan VirusWall is added to the configuration, messages between your original MTA and the Internet are routed through the InterScan VirusWall server with the ISVW server's MTA (SendMail or Postfix). However, in some organizations, the InterScan VirusWall server and ISVW MTA may replace your original MTA.

There are two possible installation scenarios:

- You have an existing MTA server, and have installed ISVW-SMB on the server that was originally functioning as your MTA
- You have an existing MTA, and have installed ISVW-SMB on another server (referred to as the ISVW server) positioned between your original MTA server and the Internet - this second scenario is illustrated in Figure 2-2

Even if the virus-scanning feature is turned off, you must complete the configuration steps to allow your SMTP traffic to flow properly.

The following figure helps illustrate the relationship between these settings and your network:

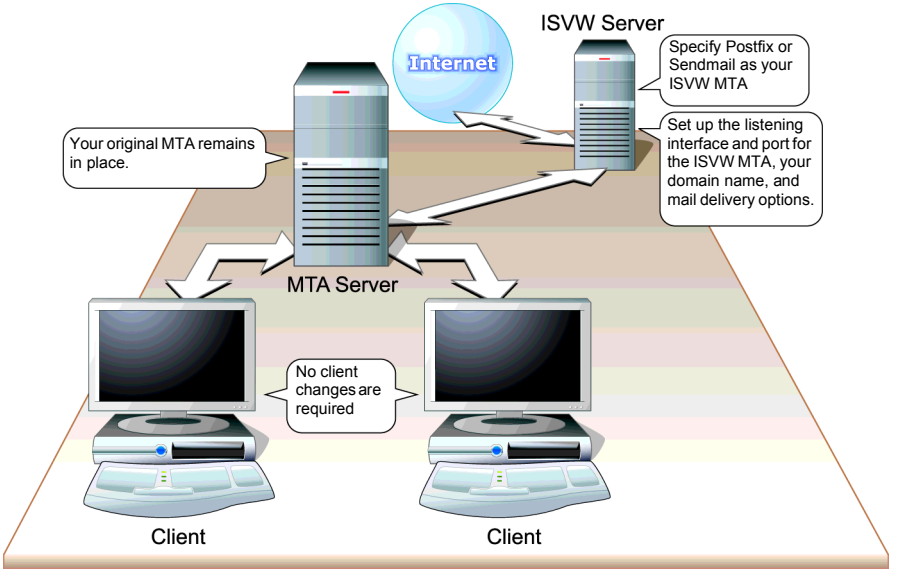


FIGURE 2-2. Configuring the InterScan VirusWall server with a Mail Transfer Agent (MTA server) for SMTP

InterScan VirusWall searches for a Mail Transfer Agent on your network. Sendmail and Postfix are both supported. When you have selected an MTA, you are prompted to supply an IP address and listening port for the MTA.

You are also prompted for the domain name of your company, such as "ourcompany.com."

The default selection for incoming mail delivery is to specify a server IP and port.

Note: Your incoming mail server IP should be the IP of the server that hosts your users mailboxes (such as Domino), with the corresponding port (usually 25).

For outgoing mail delivery, the default selection is to use DNS (Domain Name System) resolution, which provides reliable translation of names to network addresses.

POP3 settings (6/9)

If you will *not* be using InterScan VirusWall to scan your POP3 traffic, modify the value in the **Turn** field to "off." However, even if the virus-scanning feature is turned off, complete the configuration steps.

This screen allows you to specify some of the configuration settings required for InterScan VirusWall to process your POP3 traffic. You will be prompted to select a specific IP address, or you can select all interfaces to make POP3 service available to all interfaces.

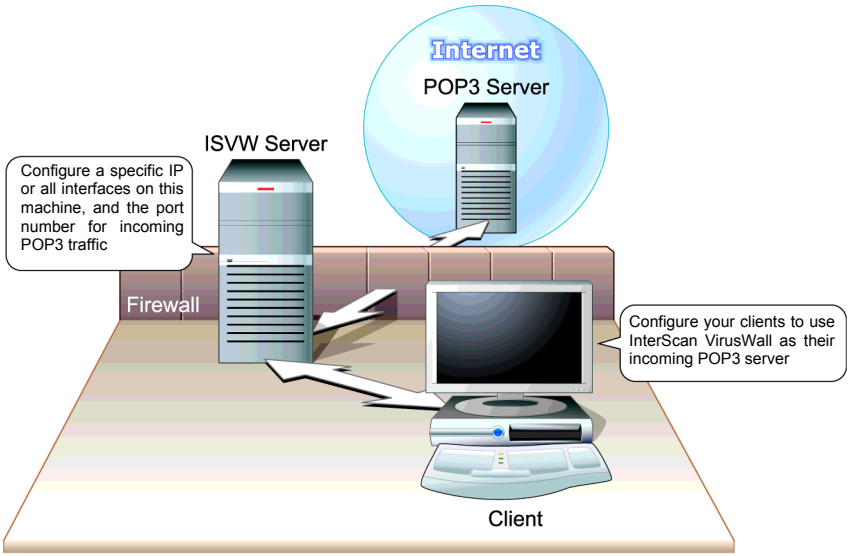


FIGURE 2-3. Configuring the InterScan VirusWall server with the POP3 IP address(es) and port for incoming POP3 traffic

HTTP settings (7/9)

If you will *not* be using InterScan VirusWall to scan your HTTP traffic, modify the value in the **Turn** field to "off." However, even if the virus-scanning feature is turned off, complete the configuration steps.

This screen allows you to specify the listening port required for InterScan VirusWall to process your HTTP traffic. You may or may not be using a firewall—it does not affect the configuration. If you are using a firewall, the ISVW server should be inside the firewall.

Your original setup was probably configured for HTTP traffic to go between clients and the Internet via a proxy/cache server. When InterScan VirusWall is added to the configuration, messages between your proxy/cache server and the Internet are routed through the InterScan VirusWall server. In addition, you may have another optional proxy between the InterScan VirusWall server and the Internet.

The following figure helps illustrate the relationship between these settings and your network:

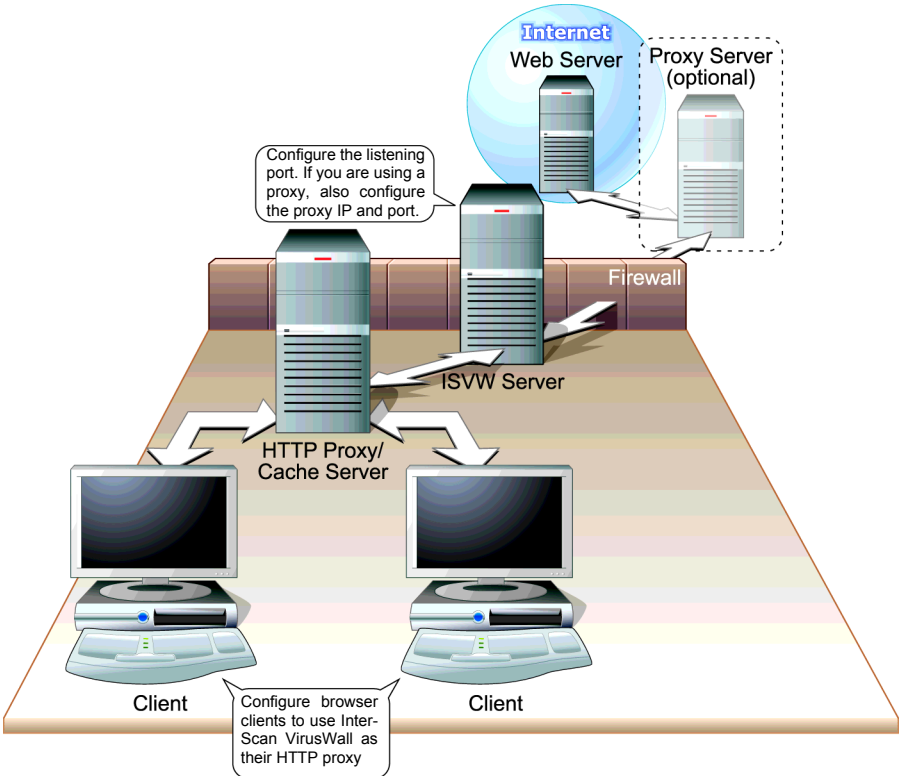


FIGURE 2-4. Configuring the InterScan VirusWall server with the HTTP listening port

If you are already using another server as an HTTP proxy, reconfigure your mail clients to go through the InterScan VirusWall server and use it as their HTTP proxy.

If you are using an upstream proxy, you will be prompted to specify the upstream proxy IP address and proxy port number.

FTP settings (8/9)

If you will *not* be using InterScan VirusWall to scan your FTP traffic, modify the value in the **Turn** field to "off." However, even if the virus-scanning feature is turned off, select an FTP listening port in the **Listening port** field.

Security level setting (9/9)

The installation script prompts you to choose a security setting for InterScan VirusWall. Choose a value of **Low**, **Medium**, or **High**. The default setting is **Medium**. The following figure describes the result of your selection:

Security Setting	Low	Medium	High
SMTP virus scan	IntelliScan	IntelliScan	Scan all file types
POP3 virus scan	IntelliScan	IntelliScan	Scan all file types
HTTP virus scan	IntelliScan	IntelliScan	Scan all file types
FTP virus scan	IntelliScan	IntelliScan	Scan all file types
Schedule Update	Weekly	Daily	Hourly

FIGURE 2-5. Security settings—low, medium, and high

These settings are described in more detail below.

Low setting

Virus scanning is performed by IntelliScan, a method of identifying which files to scan that is more efficient than scanning all files. Scheduled polling of the ActiveUpdate server for updates to the virus pattern file and scan engine occur weekly.

Medium setting

Virus scanning is performed by IntelliScan. Scheduled polling of the ActiveUpdate server for updates to the virus pattern file and scan engine occur daily.

High setting

All files are scanned for viruses. The result is the most comprehensive scanning for viruses. Scheduled polling of the ActiveUpdate server for updates to the virus pattern file and scan engine occur hourly.

Note: The **Low**, **Medium**, and **High** settings establish a default to help you get a basic configuration installed. Your selections can be changed in the management console after installation. If you are unsure which setting to select, choose **Medium**.

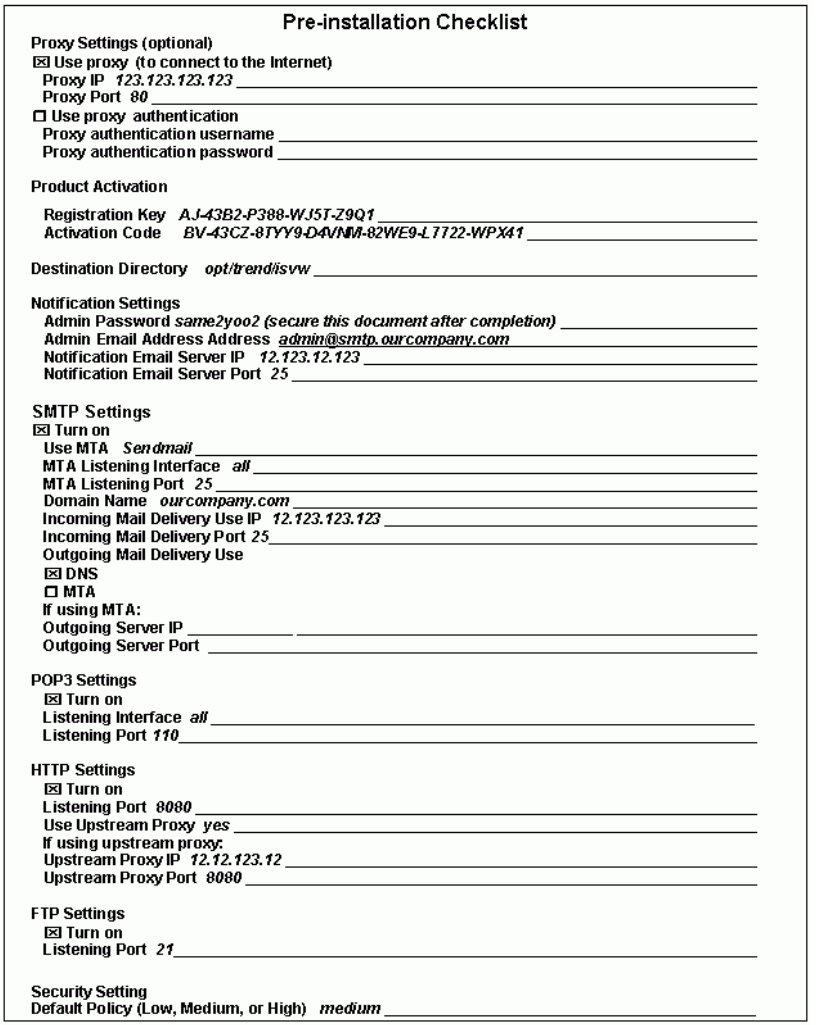
When to install InterScan VirusWall

You can install InterScan VirusWall when you are ready to supply the requested information on the pre-installation checklist. You do not have to register or activate the product to complete installation, but you will not be able to perform any scanning until you have completed these actions.

An example of a complete checklist is shown on the following page.

Example of a completed pre-installation checklist

Here is an example of a pre-installation checklist that is ready for the administrator to begin the installation:



Pre-installation Checklist

Proxy Settings (optional)
☒ Use proxy (to connect to the Internet)
Proxy IP *123.123.123.123*
Proxy Port *80*
☐ Use proxy authentication
Proxy authentication username
Proxy authentication password

Product Activation

Registration Key *AJ-43B2-P388-WJ5T-Z9Q1*
Activation Code *BV-43CZ-8TYY9-D4VNM-82WE9-L7722-WPX41*

Destination Directory *opt/trend/isvw*

Notification Settings
Admin Password *same2yoo2 (secure this document after completion)*
Admin Email Address Address *admin@smtp.ourcompany.com*
Notification Email Server IP *12.123.12.123*
Notification Email Server Port *25*

SMTP Settings
☒ Turn on
Use MTA *Sendmail*
MTA Listening Interface *all*
MTA Listening Port *25*
Domain Name *ourcompany.com*
Incoming Mail Delivery Use IP *12.123.123.123*
Incoming Mail Delivery Port *25*
Outgoing Mail Delivery Use
☒ DNS
☐ MTA
If using MTA:
Outgoing Server IP
Outgoing Server Port

POP3 Settings
☒ Turn on
Listening Interface *all*
Listening Port *110*

HTTP Settings
☒ Turn on
Listening Port *8080*
Use Upstream Proxy *yes*
If using upstream proxy:
Upstream Proxy IP *12.12.123.12*
Upstream Proxy Port *8080*

FTP Settings
☒ Turn on
Listening Port *21*

Security Setting
Default Policy (Low, Medium, or High) *medium*

FIGURE 2-6. Example of completed pre-installation checklist

Chapter 3

Installing InterScan VirusWall

The installation script prompts you through the installation of InterScan VirusWall. Before you start, be sure to read Chapter 2, *Planning Your Installation*. Complete the pre-installation checklist in that chapter.

There are two methods of installation:

- Installation from the CD
- Installation by downloading InterScan VirusWall from the Web

Installing from a CD

Follow these steps to install InterScan VirusWall from a CD.

To start the installation process:

Note: Before you begin installation, save and close other programs you may have open on your machine.

1. Log on as "root" or run the "su" command to assume root privilege.
2. Insert the CD in the CD drive.

3. Open a command prompt, and verify that the CD is properly mounted by typing the following command:

   ```
   # cd/mnt/cdrom
   ```

4. Locate the folder containing the installation files. The files are:
   - isinst
   - Isvw-5.0-en-1xxx.tgz
5. Type the following:

   ```
   #ls
   ```

   The result is:

   ```
   isinst Isvw-5.0-en-1xxx.tgz
   ```

6. Change file permission for the “isinst” file to executable as follows:

   ```
   #chmod +x./isinst
   ```

7. Execute the installation as follows:

   ```
   # ./isinst
   ```

8. The first **Install** screen displays.

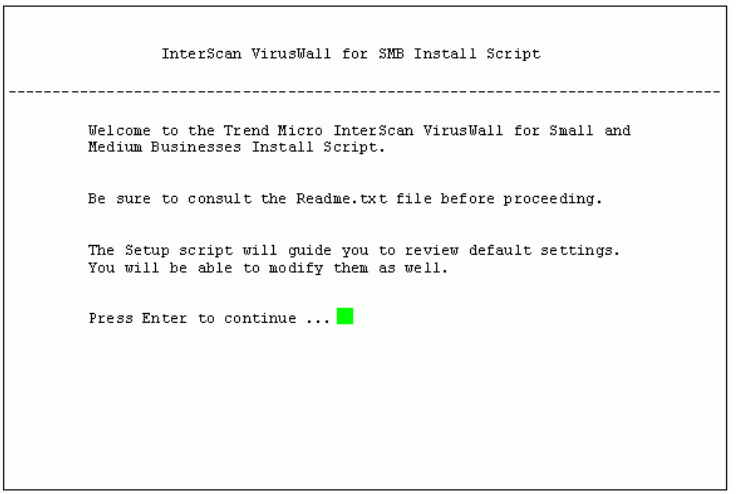


FIGURE 3-1. Install script Welcome screen

If you completed the pre-installation checklist described in Chapter 2, you will have all the information you need to respond to the prompts described in the following steps.

To respond to the installation setup script:

1. Press **Enter** to proceed with the installation.
2. The Trend Micro **License Agreement** displays. Press **Enter** to view the full text of the license agreement. When you are finished, type **Y|y** (accept license) to proceed, or **N|n** (decline license) to stop. If you do not accept the terms in the license agreement, the installation cannot be completed.
3. When you accept the license terms, the **Modify Default Proxy Settings** screen displays. Respond to the prompts on this screen if you are currently using a proxy server to connect to the Trend Micro ActiveUpdate server, including the proxy server address and port number, and optional authentication user name and password. If you are not using a downstream proxy, you do not need to provide this information and can go to the next screen. Type **N|n** (next) to continue.
4. The **Product Activation** screen displays:

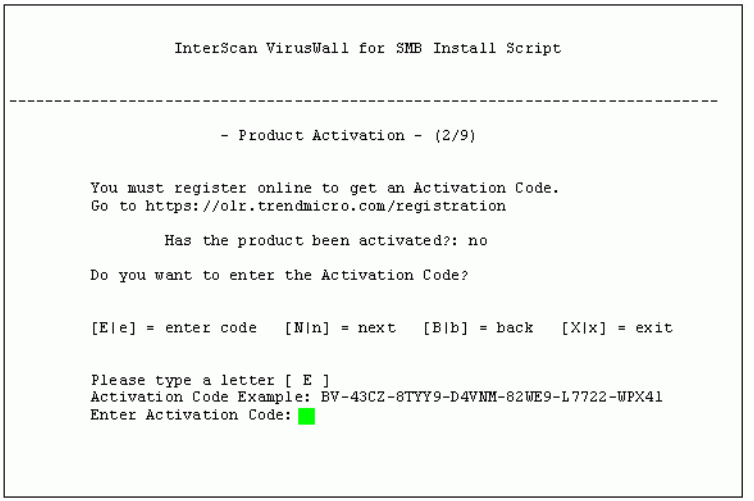


FIGURE 3-2. Product Activation screen

a. If you have already registered *and* activated InterScan VirusWall, "yes" displays in the **Has the product been activated?** field. In this case, type **N|n** to continue.

b. If you have not registered *or* activated the product, "no" displays in the **Has the product been activated?** field. To register now, go to the Trend Micro Online Registration Web site at:

`http://olr.trendmicro.com`

The Trend Micro **Online Registration** screen launches in your browser. Complete the registration process, using the Registration Key you received when you purchased the product. Your Activation Code will be sent via email, typically within 20 minutes after you complete registration. When you receive the Activation Code, follow step **c** below.

c. If you have registered and received your Activation Code, but have not yet activated the product, "no" displays in the **Has the product been activated?** field. Type **E|e** (enter code) to activate now. Enter your Activation Code in the **Enter Activation Code** field as shown in the previous figure. Type **N|n** when you are finished.

Note: After you purchase InterScan VirusWall, you will receive a license certificate that provides a code, either 22 characters or 37 characters. If you have a code that is 37 characters (including hyphens), you have an Activation Code and can skip step **b** of this process. If you have a code that is 22 characters, you must perform both steps **b** and **c**. You *can* register and/or activate now, or continue the installation without performing these steps, and do them later.

---

5. The **Choose Destination Directory** screen displays. The default directory for installation of the InterScan VirusWall files (`/opt/trend/isvw`) displays in the **Destination Directory** field. To accept the default, type **N|n**. To change the directory, type **M|m** {modify), and enter an alternate directory in the **Destination Directory** field - then type **N|n** to continue.

6. The **Modify Notification Settings** screen displays. Type **M|m** (modify) to enter and confirm the password for the administrator account you plan to use to manage InterScan VirusWall. Also enter the notification email address, server IP address, and port. Type **N|n** (next) to continue.

7. The **Modify Default SMTP Settings** screen displays. If you do not plan to use this feature, type **M**|**m** to modify the default value in the **Turn** field, and change it to "off."
   If you plan to use this feature, the fields on this screen are described in detail in Chapter 2. Enter the values you recorded on your pre-installation checklist for the MTA listening interface (IP address) and port number that InterScan VirusWall will use to listen for SMTP traffic, your mail server domain name, and your choices for SMTP message delivery options. Type **N**|**n** when you are finished.
8. The **Modify Default POP3 Settings** screen displays. If you do not plan to use this feature, type **M**|**m** to modify the default value in the **Turn** field, and change it to "off."
   If you plan to use this feature, specify the listening interface and port number to receive POP3 traffic. Type **N**|**n** to continue.
9. The **Modify Default HTTP Settings** screen displays. If you do not plan to use this feature, type **M**|**m** to modify the default value in the **Turn** field, and change it to "off."
   If you plan to use this feature, specify the listening port number to receive HTTP traffic. Also indicate whether you plan to use an upstream proxy. If so, you will be prompted to enter the proxy IP address and port. Type **N**|**n** to continue.
10. The **Modify Default FTP Settings** screen displays. If you do not plan to use this feature, type **M**|**m** to modify the default value in the **Turn** field, and change it to "off."
    If you plan to use this feature, specify the listening port number to receive FTP traffic. Type **N**|**n** to continue.
11. On the **Modify Security Level Setting** screen, select a default security setting for your network. The **Medium** setting is the default, and is recommended if you are uncertain which setting to select. These settings are described in detail in Chapter 2. Type **N**|**n** to continue.

12. The **Ready to Install** screen displays, summarizing the features you have configured.

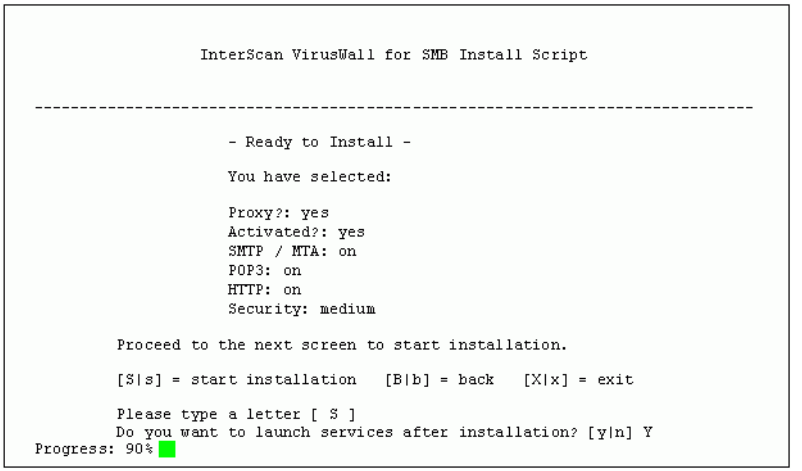


FIGURE 3-3. Ready to Install screen

Review the choices displayed. Make changes if needed by clicking **B|b** (back) to return to a screen to be changed. Otherwise, type **S|s** (start installation) to proceed.

13. You are prompted to respond to the following: **Do you want to launch services after installation?** Type **y** to launch when installation is complete. If you type **n**, you can manually launch at a later time.
14. The **Progress** field displays, advising you of the status of the loading process. When the **Progress** field displays 100%, user messages display, advising you that InterScan daemons and services are being started.

15. In a few moments, you will see the following prompt, advising you how to display the management console:

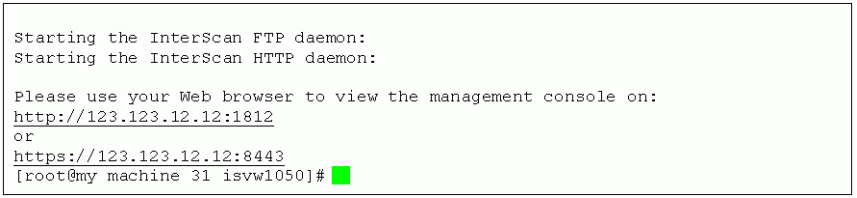


FIGURE 3-4. User prompt for displaying management console

Note: If you select HTTPS protocol, the installation script generates a default security certificate using the machine hostname as the certificate common name. You do not have to do anything further to enable the certificate.

16. Launch a browser window and type one of these URLs in the browser window. Press **Enter**. The InterScan VirusWall management console displays in your browser. Enter the password you selected (on the **Modify Notification Settings** screen during installation) in the logon screen, and click **OK**.
17. If you did not register and/or activate before or during installation, you must do so now. Otherwise, your application is fully installed and operational.

Installing by downloading from the Web

Go to the Trend Micro Web site:

`http://www.trendmicro.com`

Select InterScan VirusWall and follow the prompts to download the software.

Evaluation version

You can install the evaluation version of any Trend Micro product, which allows you to try out other Trend Micro products as well. Evaluation versions are fully functional and can be installed with a temporary product Registration Key and

Activation Code. Typically after 30 days, however, most of the program features will be disabled.

Removing the evaluation-period limit

If you decide to purchase a product that you are evaluating, you do not need to reinstall. Instead, open the Trend Micro Online Registration page, enter the Registration Key you received (post-purchase) along with the other required fields, and click **Register** to send your information to Trend Micro. Your Activation Code arrives via email, typically within twenty minutes.

After installation

When you are finished installing, if you have registered and activated InterScan VirusWall, you can:

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

Immediately after installing, you should also:

- Update the virus pattern file and scan engine
- Update the anti-spam rules and engine
- Confirm that virus scanning is enabled
- Confirm that anti-spam is enabled
- Enable and configure content-filtering to meet your organization's communications objectives
- Enable and configure URL and file blocking for HTTP and FTP
- Customize the notification messages
- Configure the alerts
- Set up an update schedule for the virus pattern file, scan engine, and anti-spam rules and engine

Post-installation steps are described in more detail in Chapter 5, *Updating and Testing InterScan VirusWall* and Chapter 6, *Configuring InterScan VirusWall*.

My Product Details screen

Verify the status of your product license anytime after installation and activation on the **Administration** > **Product License** screen.

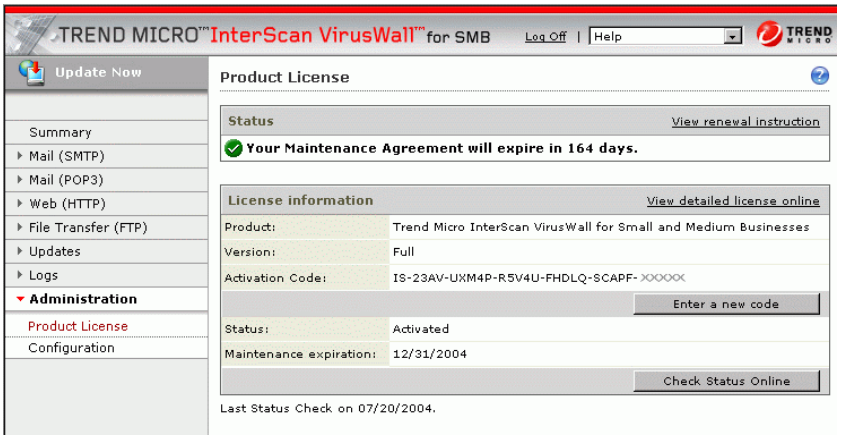


FIGURE 3-5. Product License screen in the management console

Click the View detailed license online link on the **Product License** screen to display the **My Product Details** screen, which appears in your browser.

The **My Product Details** screen displays even more information about your installation of ISVW.

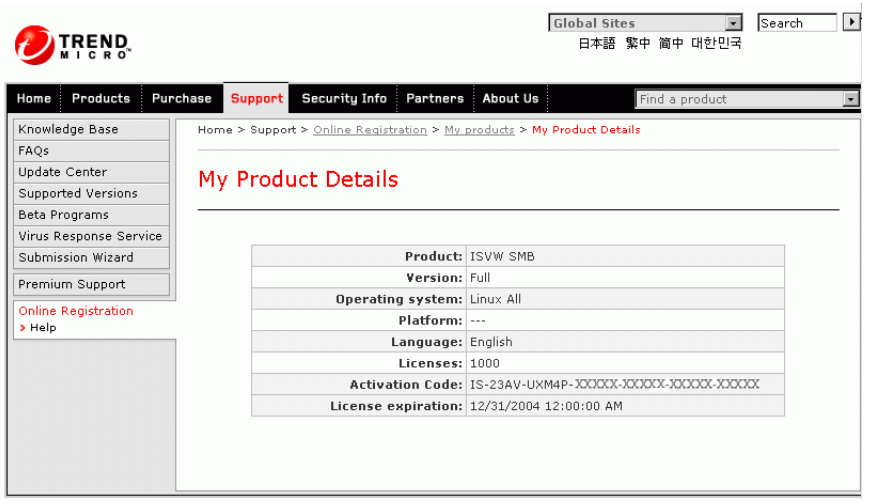


FIGURE 3-6. My Product Details screen

Removing ISVW

To remove the software from your machine:

1. Log in as root.
2. To remove InterScan VirusWall, type the following at the command line:
   ```
   # ./isinst
   ```
3. Press **Enter**. The following displays:
   ```
   Found the InterScan VirusWall installed at
   "/opt/trend/isvw".
   Do you want to uninstall it? [y|n]
   ```
4. Type y (yes) to uninstall. The following displays:
   ```
   Please wait ...
   Uninstalling ...
   Progress: 100%
   #
   ```

5. All files under the installation directory except the log files are now removed from your machine. If you do not want to retain the log files, manually delete them.

Chapter 4

Registering and Activating InterScan VirusWall

This chapter describes:

- Product registration, which is required to receive product updates, including updates to the virus pattern file, scan engine, anti-spam rules, and anti-spam engine
- Product activation, which is required to enable InterScan VirusWall to begin scanning, filtering, and blocking

After your purchase of InterScan VirusWall concludes, you will receive a product license certificate. The certificate contains a code, either a Registration Key or an Activation Code. The codes are needed to complete the following tasks.

Registering InterScan VirusWall

If you have a Registration Key, register InterScan VirusWall before proceeding. If you have an Activation Code, skip to *Activating InterScan VirusWall* starting on page 4-5.

Your Registration Key or Activation Code can be found on your license certificate, that you should have received from Trend Micro shortly after your purchase of

InterScan VirusWall. If you do not have your license certificate, contact Trend Micro for assistance.

The following example of a license certificate shows a Registration Key in the highlighted box.

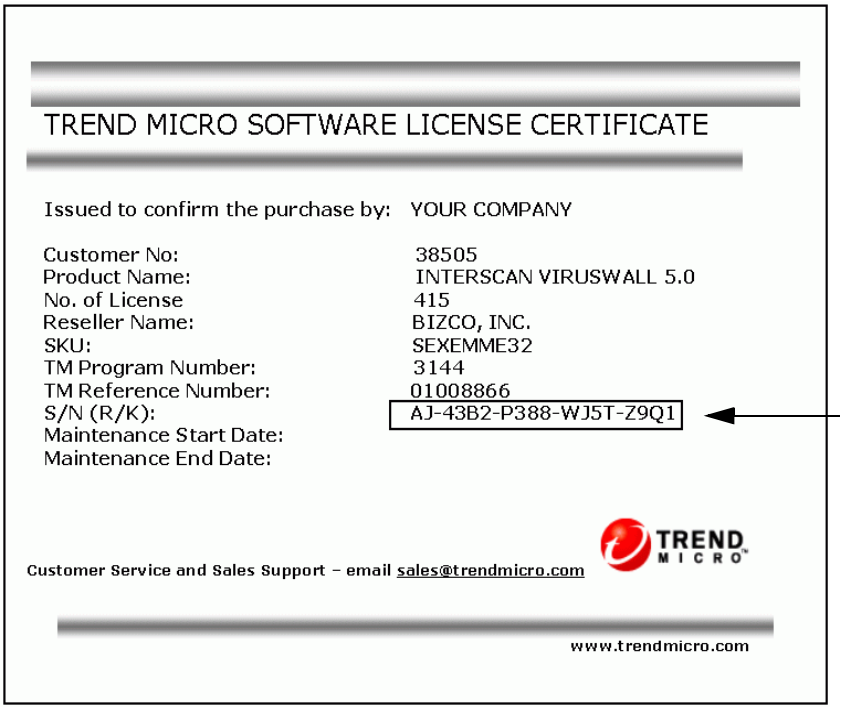


FIGURE 4-1. Code can be found on the license certificate

Assuming you have not already registered InterScan VirusWall prior to installation or during installation, register now. You will be not able to use InterScan VirusWall until the registration process is complete. Register online by visiting the following URL:

`http://olr.trendmicro.com`

The Trend Micro **Online Registration** screen displays.

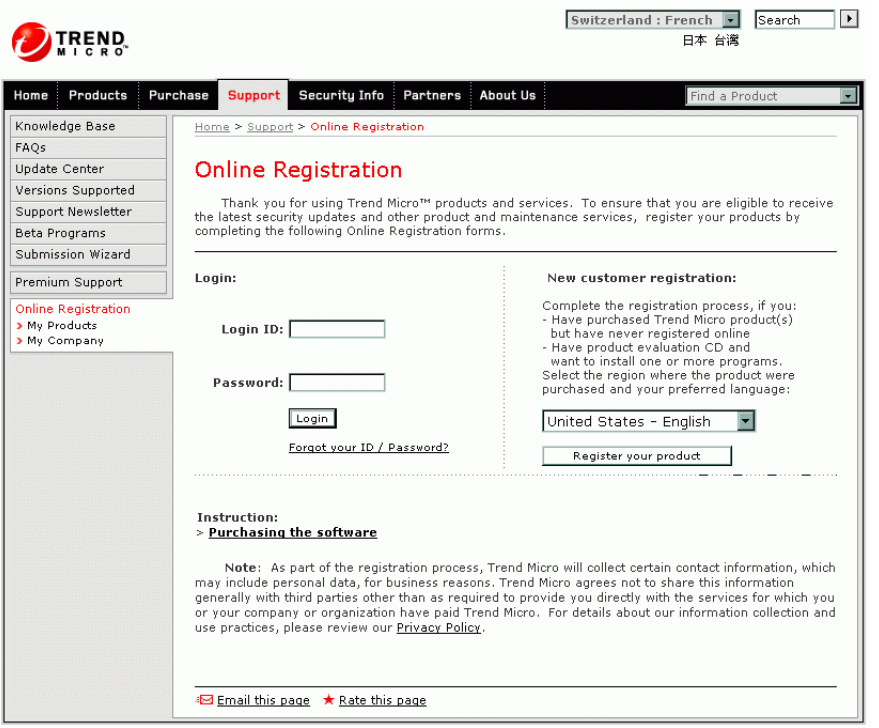
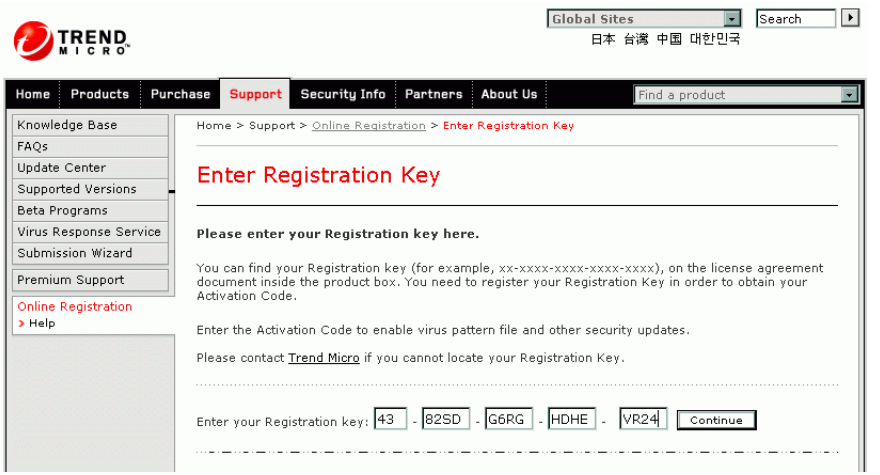


FIGURE 4-2. Trend Micro Online Registration screen

Begin in the **New customer registration** section of the **Online Registration** screen. Select your preferred language from the language pull-down, and click **Register your product**.

The **Enter Registration Key** screen displays.



Type the registration key from your license certificate and click **Continue**. Follow the prompts in the subsequent registration screens to complete the registration process.

Your logon ID and password

Some of the information you provide during registration is used to create a logon ID and password, so that next time you visit the **Online Registration** screen (for example, to update your Maintenance Agreement), you can log on as an existing customer rather than a new customer.

After registration

Shortly after you complete the registration process (typically within 20 minutes), you will receive an email message from Trend Micro that contains your Activation Code.

Activating InterScan VirusWall

Once you have your Activation Code, either received in an email message from Trend Micro following product registration, or taken directly from your license certificate, you are ready to activate InterScan VirusWall.

To activate during installation:

Enter the Activation Code in the **Enter Activation Code** field on the **Product Activation** screen.

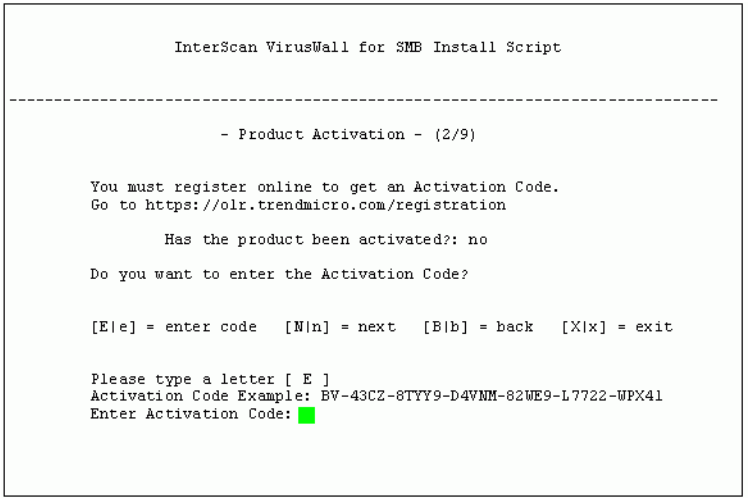


FIGURE 4-3. Product Activation screen in installation script

To activate after installation:

1. Select **Administration** > **Product License** to display the **Product License** screen.

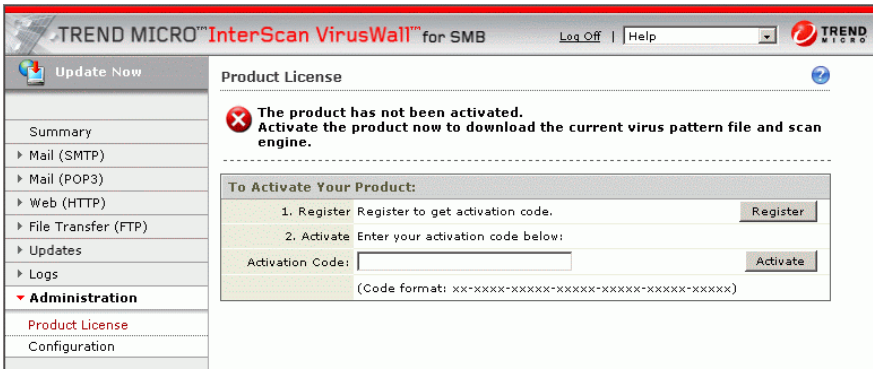


FIGURE 4-4. Product License screen

2. Enter the Activation Code in the **Activation Code** field.
3. Click **Activate**. After activation, the message at the top of the **Product License** screen changes, to let you know that activation was successful.

As soon as InterScan VirusWall is activated, it begins scanning for viruses and spam, according to the default security settings. To enable content filtering, URL, and file blocking, configure these features according to your organization's communications policies. See *Configuring InterScan VirusWall* starting on page 6-1 and the online help for more information.

For more information about activation and registration

View a product registration FAQ by visiting the following site:

`http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionId=16326`

WARNING! *Trend Micro recommends that you register and activate ISVW-SMB immediately. If you have completed installation, ISVW can begin acting as a "transparent" proxy in place of your original proxy, allowing users to access the internet without the restrictions of your original proxy.*

Chapter 5

Updating and Testing InterScan VirusWall

This chapter describes the tasks to perform immediately after completing your product activation. These include:

- Updating InterScan VirusWall to use the most recent versions of the scanning and anti-spam tools
- Testing the installation to make sure InterScan VirusWall is detecting viruses

Updating InterScan VirusWall

As soon as you finish installation of InterScan VirusWall, verify that the product is updated to use the current version of the:

- Virus pattern file
- Scan engine
- Anti-spam rules
- Anti-spam engine

Virus pattern file

Trend Micro's products draw upon an extensive database of virus "signatures," commonly called the virus pattern file. During scanning, the binary patterns of files are compared against these signatures, and the scan engine determines a file is infected if a match is found. Since new virus pattern files are available every week or sooner, you should schedule automatic weekly updates.

To reduce the bandwidth used when updating the virus pattern file, Trend Micro products use a procedure called incremental update. Rather than downloading the entire virus pattern file every time it is updated, only the new virus patterns that have been added since the last release are downloaded. The new patterns are then merged with the older virus pattern file. This greatly reduces download and deployment time.

Configure your management console to update the pattern file on a regular basis, or perform a manual update at any time. View the current version of the Trend Micro pattern file by visiting the following URL:

`http://www.trendmicro.com`

Scan engine

A virus scanning engine is the program component that does the actual work of scanning files and detecting viruses. Trend Micro releases new engine versions for a number of reasons:

1. New types of viruses have been developed that cannot be detected by the old engine.
2. Scanning performance and detection rates have been enhanced.
3. Support for virus detection of additional formats, for example, the newest Microsoft Word and Excel types, have been added.

Note: See update instructions in *Scheduled update* starting on page 5-5 or *Manual update* starting on page 5-6.

The scan engine scans UUencode, Binhex, and MIME-encoded attachments, as well as a wide variety of compressed file types.

WARNING! *InterScan VirusWall for SMB will not scan password-protected or encrypted files. SMTP and POP3 password-protected or encrypted messages are delivered, but ISVW for SMB embeds a warning message to that mail, to let the user know the files were not scanned. HTTP and FTP traffic containing a password-protected file is allowed to pass. Traffic utilizing HTTPS is not scanned, but also is allowed to pass unless the URL is blocked.*

Anti-spam rules and engine

The anti-spam rules and engine work together to detect spam in your email messages. The advanced detection technologies in the Trend Micro anti-spam engine include:

- **Heuristic rule-based scanning**—The anti-spam engine examines email messages using a heuristic (best guess) rule file, and returns a score that represents the probability that the message is spam.
- **Supports list of approved and blocked senders**—The anti-spam engine implements Trend Micro and user-defined approved senders and blocked senders. Spam filtering is bypassed for approved senders. For blocked senders, email is automatically tagged as spam. These messages also bypass heuristic and spam database scanning.
- **Uses a spam signature database**—The anti-spam engine uses the Trend Micro spam database for filtering spam messages. To help Trend Micro keep the database current, users in your network are encouraged to forward their spam email messages to Trend Micro at the following email address:

  `spam@support.trendmicro.com`

A periodic reminder displays on client desktops, as shown below, to remind users to forward spam to Trend Micro.

FIGURE 5-1. Spam and false positives reporting reminder

Forward false positive messages (messages inappropriately identified as spam) to the following email address:

`false@support.trendmicro.com`

Scheduled update

Click **Updates** > **Scheduled** to display the **Scheduled Update** screen. In the following example, the virus pattern file, virus scanning engine, anti-spam rules, and anti-spam engine are all scheduled to be updated at 5:00 A.M daily.

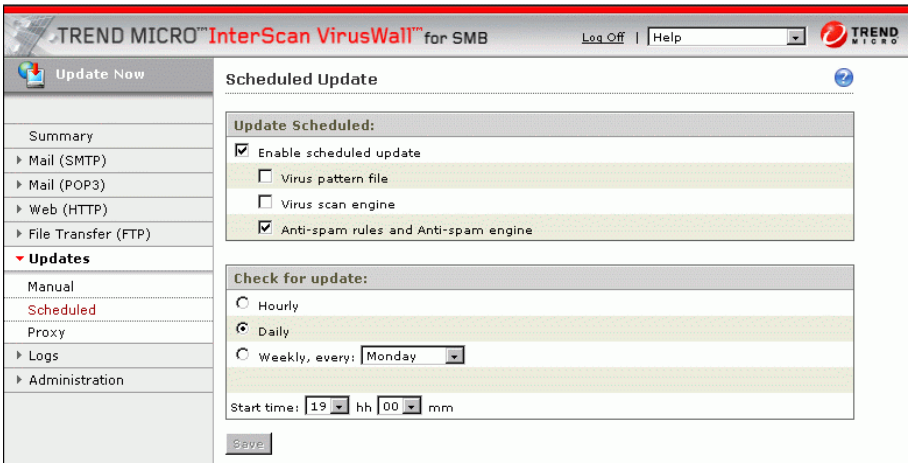


FIGURE 5-2. Scheduled Update screen

There can be several virus pattern file updates within a week. The recommended setting for the update interval is at least daily. The updates continue to occur regularly as specified until you change the update interval.

Note: ActiveUpdate is a utility common to many Trend Micro products. Connected to the Trend Micro software update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files and the scan engine as well as program files via the Internet.

Manual update

Click **Updates** > **Manual** to display the **Manual Update** screen. If an update is available for a particular component, the component can be selected. For example, the following screen shows that a more current version of the virus pattern file and scan engine is available. If the checkbox cannot be selected, as shown in the following example for the anti-spam rules and engine, the component is already current.

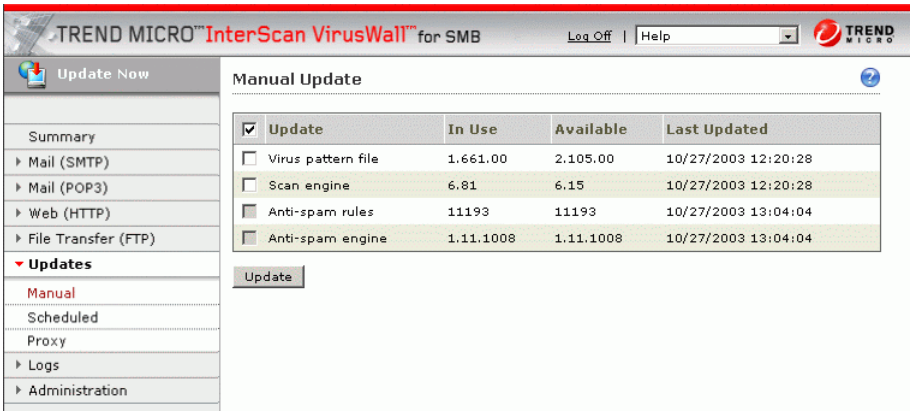


FIGURE 5-3. Manual update feature

Manual update, pattern file only

View the current virus pattern file version in the Status Alerts section of the **Summary** screen. To manually update the virus pattern file at any time, click **Update**.

Testing your installation

Trend Micro recommends testing your product and confirming that it works using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm that antivirus software is properly installed and configured.

The EICAR test script is an inert text file with a .com extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to it as if it were a virus. Use it to trigger a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

WARNING! *Never use real viruses to test your antivirus installation.*

To test your installation's virus scanning:

1. Go to the following URLs:

   `http://www.trendmicro.com/en/security/test/overview.htm`

   `http://www.eicar.org/anti_virus_test_file.htm`

2. Download the test files. In your browser window, you should see a warning message that doesn't allow you to continue the download.
3. Check the virus logs to see if the detection is reported in the logs. If not, contact customer support for assistance.

Visit the EICAR Web site for more information:

`http://www.eicar.org`

Chapter 6

Configuring InterScan VirusWall

As soon as you have completed installation and activation, InterScan VirusWall begins scanning your network traffic for viruses and spam. However, you must configure additional settings in InterScan VirusWall to:

- Enable clients to retrieve their mail using POP3 protocol
- Use FTP service
- Filter content
- Block access to certain URLs
- Block HTTP and FTP transfers
- Fine-tune your SMTP settings
  - Server tab
  - Connection tab
  - Disclaimer tab
  - Incoming Mail tab
  - Relay Control tab
- Fine-tune spam filtering
- Set up approved and blocked sender lists

Configuring the POP3 client

Whether or not your organization's messaging policies allow users to retrieve mail from a POP3 server, you should configure your network to enable scanning of incoming POP3 mail. Otherwise, your network is vulnerable if a user decides to do so regardless of the policy.

Configuring Outlook Express to enable POP3 scanning

Launch Outlook Express and select **Tools** > **Accounts**. The **Internet Accounts** screen displays. Click **Add** > **Mail**. The Internet Connection Wizard launches.

To configure the client in Outlook Express:

1. Type the client's user name, such as *John Smith*, on the **Your Name** screen in the Internet Connection Wizard. Click **Next**.
2. Type the user's email address, such as *John_Smith@anycompany.com*, on the **Internet E-mail Address** screen. Click **Next**.
3. The **E-mail Server Names** screen displays. Do the following:
   a. Select POP3 in the **My incoming mail server is a ...** field. (Choices are POP3, IMAP, or HTTP.)
   b. Type the address for the incoming mail (POP3) server in the **Incoming mail (POP3, IMAP, or HTTP) server** field.
   c. Type the address for the ISVW server in the **Outgoing mail (SMTP) server** field. Click **Next**.

Note: For steps b and c, you can use fully qualified domain name format as shown in the following example, or IP address.

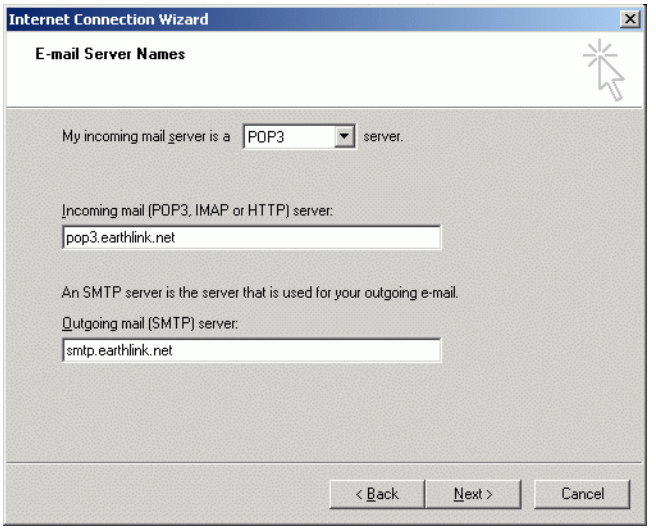


FIGURE 6-1. Microsoft Outlook Express client configuration for POP3

4. On the **Internet Mail Logon** screen:
   a. Type the account name the client will use to retrieve POP3 mail in the **Account name** field. The format must be *name*, followed by # and then the *POP3 server name*, for example:

      vsanchez#pop3.earthlink.net

   b. Type a password for the client's POP3 mail account. Check **Remember password** if appropriate for the client.

   c. If the POP3 server requires authentication, select **Log on using Secure Password Authentication (SPA)**. Click **Next**.

5. Click **Finish** on the **Congratulations** screen. Now when you view the **Internet Accounts** screen again, the POP3 connection appears, similar to the following example.

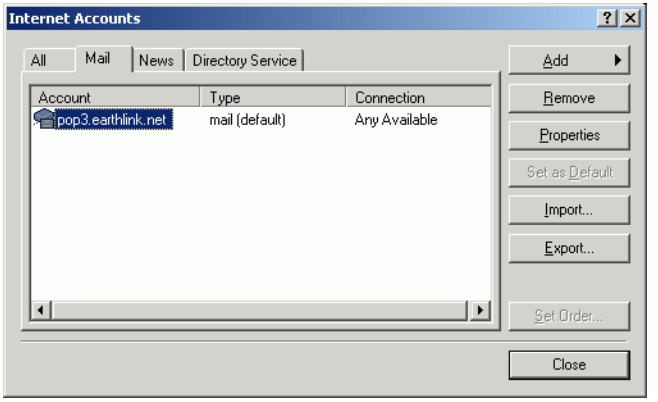


FIGURE 6-2. Outlook Express client configuration for POP3

Note: This configuration must be set up on each client utilizing POP3 in your network.

Configuring FTP service

By default, FTP service is ready to use in stand-alone mode. If you want to use ISVW as a proxy for FTP service, configure the FTP settings on the **FTP Configuration** screen.

To display this screen, click **File Transfer (FTP)** > **Configuration**:

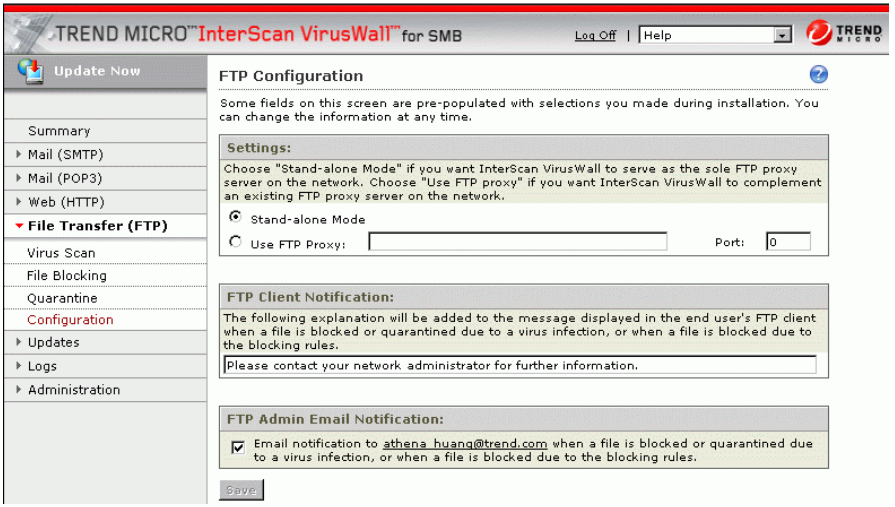


FIGURE 6-3. FTP Configuration screen

Click the online help icon for instructions to configure your FTP service, and create FTP notifications.

Content filtering

Content filtering allows you to implement policies to help your organization meet objectives related to:

- **Human Resources management**—for example, the company has a policy that employees may not use company email resources to harass others
- **Legal issues**—for example, the company has a policy that prohibits employees from leaking confidential information

If you have not previously used a content filtering application in your organization, you may want to meet with your organization's Human Resources, Legal, and other interested groups to solicit their ideas about how to implement the content filter. You may start with a baseline of words and phrases from your initial assessment, and add more words and phrases on an ongoing basis. Your goal is to implement content

filtering in a way that will help reduce legal liability, and increase employee productivity.

If you are using both SMTP and POP3 protocols for messaging, and you want to filter only incoming email messages, set up content filtering on the **Target** tab of the following screens:

- **Mail (SMTP) > Content Filter > Incoming**
- **Mail (POP3)** > **Content Filter**

To filter outgoing SMTP messages, also set up content filtering on the **Target** tab for the **Mail (SMTP)** > **Content Filter** > **Outgoing** screen.

Note: POP3 messages are incoming only, so no outgoing configuration is required for POP3 content.

All three screens have a similar design and purpose, which is to:

- Allow you to define a maximum message size, to help prevent Denial of Service attacks
- Define words that if found in the message subject, result in triggering an action (as defined on the Action tab)
- Define words that if found in the message body, result in triggering an action
- Define words that if found in an attachment file name, trigger an action
- Identify attachment group file types for scanning

On the **Content Filter** screens, make entries for the message subject and body filter criteria, and the attachment filter criteria. Here is an example for the message subject and body filter. The word “hate” has been added to the subject filter, and the phrase

"I'll get you" has been added to the message body filter. These entries remain in the content filter until you delete them.

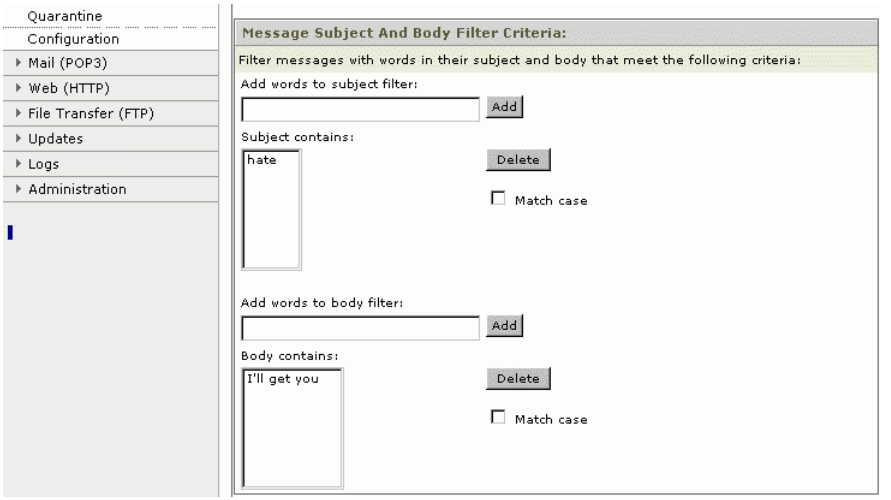


FIGURE 6-4. Setting up content filtering criteria for message subject and body

Attachments are scanned if:

- The attachment file type is selected for scanning, and/or
- A text string match is found in the attachment name

To set up words or phrases for filtering in the attachment file name, scroll down to the Attachment Filter Criteria portion of the screen, and type the text in the **Add words to attachment filter** field. In the following example, the word "sushi," representing a confidential project code-name, has been added to the filter.

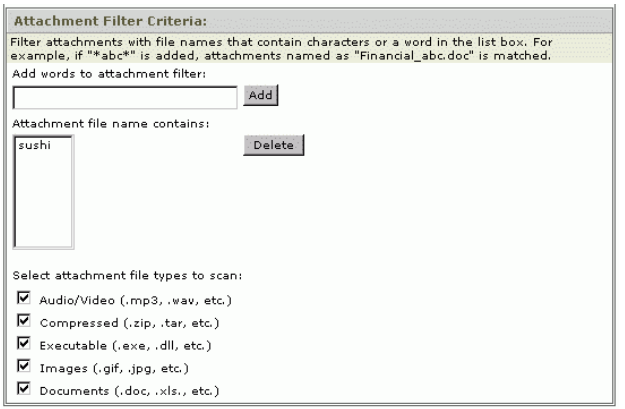


FIGURE 6-5. Setting up content filter criteria for attachment subject

The example also shows that all attachment file types should be scanned, so all the following file names would trigger an action:

- *InstallProjectSushi.exe*
- *MakingSushi.doc*
- *ProjectSushiLogo.jpg*
- *SushiRecipes.zip*
- *SushiBarRecordings.mp3*

An email message and/or attachment that meets *any one* of these filtering criteria will be acted upon, according to the action you specify in the **Action** tab of the **Content Filter** screen.

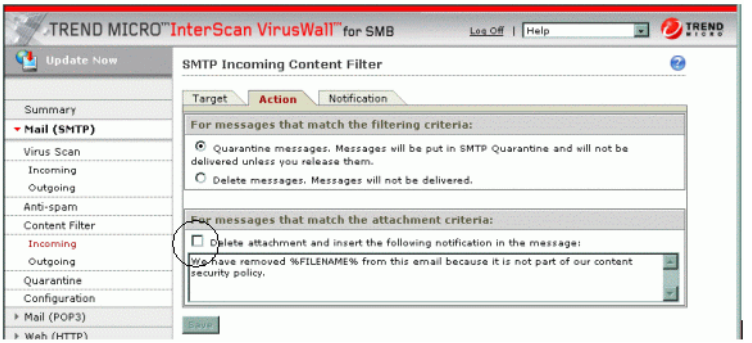


FIGURE 6-6. Action tab on SMTP Incoming Content Filter screen

The options for SMTP messages and their attachments, as shown in the previous figure, are:

- **Quarantine**—The message, with attachments if applicable, is sent to the Quarantine directory, not the recipient.
- **Delete**—The message, with attachments if applicable, is deleted. The recipient typically receives a notification that the message was deleted.

The options for POP3 messages and their attachments are:

- **Delete**—The message, with attachments if applicable, is deleted. The recipient typically receives a notification that the message was deleted.
- **Deliver**—The message, with attachments if applicable, is delivered to the recipient anyway.

If you select **Delete attachment and insert the following notification in the message**, on the **SMTP Incoming Content Filter** screen, the **SMTP Outgoing Content Filter** screen, or the **POP3 Content Filter** screen, attachments are always deleted regardless of the action selected for the message.

Blocking URLs

The URL blocking feature helps you prevent employees from accessing prohibited Web sites. For example, suppose you want to block some sites because they are dating services, online shopping services, or other offensive sites. Further, suppose you want to block any URL containing the characters "shop," "singles," or "porn." You also want to exclude "Singlestop Financials," your company's accounting service, and "Learning Tree Workshops," a consulting organization that your company uses for employee training.

To configure the HTTP URL Blocking screen for this example:

1. Select **Web (HTTP)** > **URL Blocking** to display the **HTTP URL Blocking** screen.
2. On the **URL** tab, in the **Add URL** field, type the URLs you want to block. Assume you have been having problems with employees spending time on commercial Web sites, and want to block the following URLs:
   - www.singles-matchup.com (an online dating service)
   - www.homeshoppersite.com (an online shopping service)
   - www.girlsnthings.com (a pornography site)
   - www.nazisunite.com (a racial hatred site)
   - www.casinos-ontheweb.com (an online gambling service)

   Click **Add** after each entry, to move the URL to the **Blocked URLs** field.
3. To block any URLs containing the words "singles," "shop," "girls," "porn," "nazi," or "casino." In the **Block connections to URLs containing these text strings** field, add these words, one at a time. Click **Add** after each entry, to move the words to the **Blocked URLs containing following text strings** field.
4. To create an exception for "Singlestop Financials" and "Learning Tree Workshops," add "singlestop" and "workshop" in the **Add text string** field (in the **Allow connections to URLs containing these text strings** section of the screen). Type these words, one at a time. Click **Add** after each entry.

After you complete these steps, the screen appears as follows:

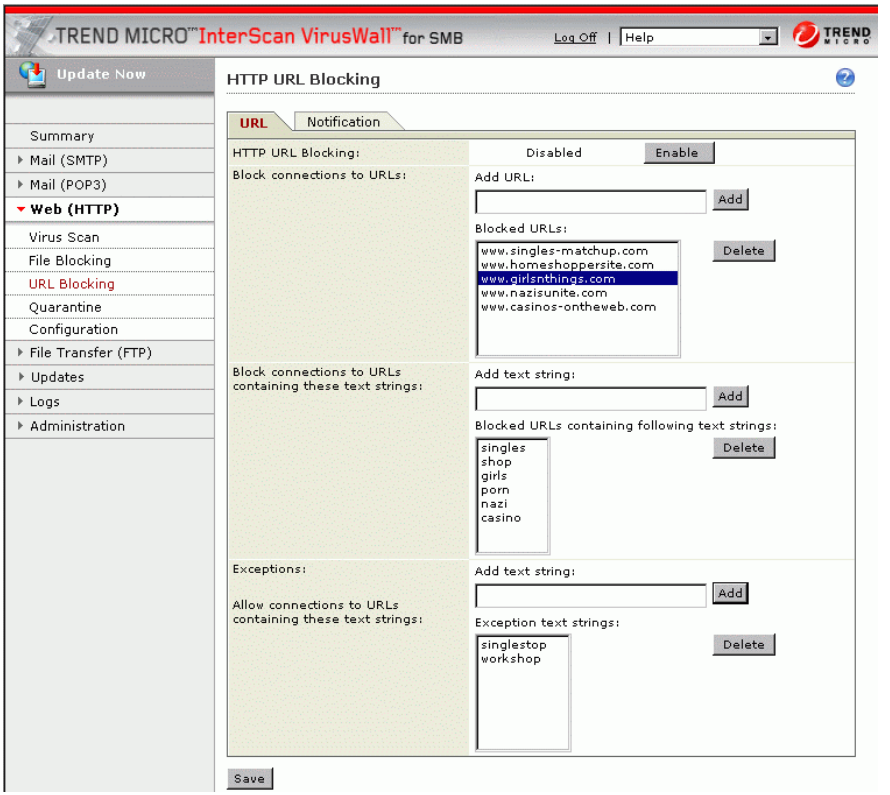


FIGURE 6-7. Setting up HTTP URL blocking

When employees attempt to access blocked sites, they are not able to view the site. A notification displays in their browser.

Blocking HTTP or FTP transfers

This feature is available to prevent employees from transferring certain types of files using HTTP and FTP service during work time. For example, suppose your company

does not allow downloading of music, both because of legal issues as well as employee productivity issues.

To block HTTP download via HTTP, select **Web (HTTP)** > **File Blocking** to display the **HTTP File Blocking** screen.

On the **File** tab of the **HTTP File Blocking** screen, block transferring of music files by selecting Audio/Video, as shown in the following example:

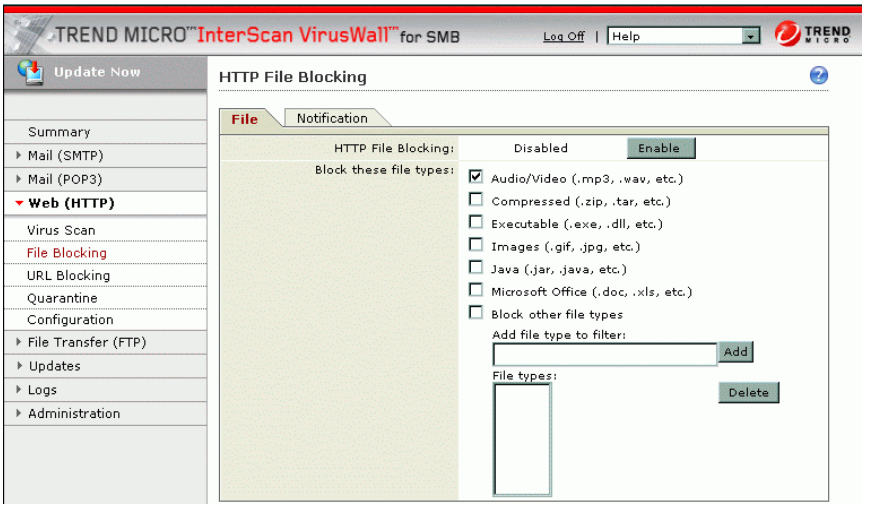


FIGURE 6-8. Setting up HTTP file blocking

To block file transfer via FTP, select **File Transfer (FTP)** > **File Blocking t**o display the **FTP File Blocking** screen.

On the **File** tab, make the same selection on the **FTP File Blocking** screen, to block the Audio/Video file types.

In the following example, two more file types, *com* and *vbs*, are also blocked:

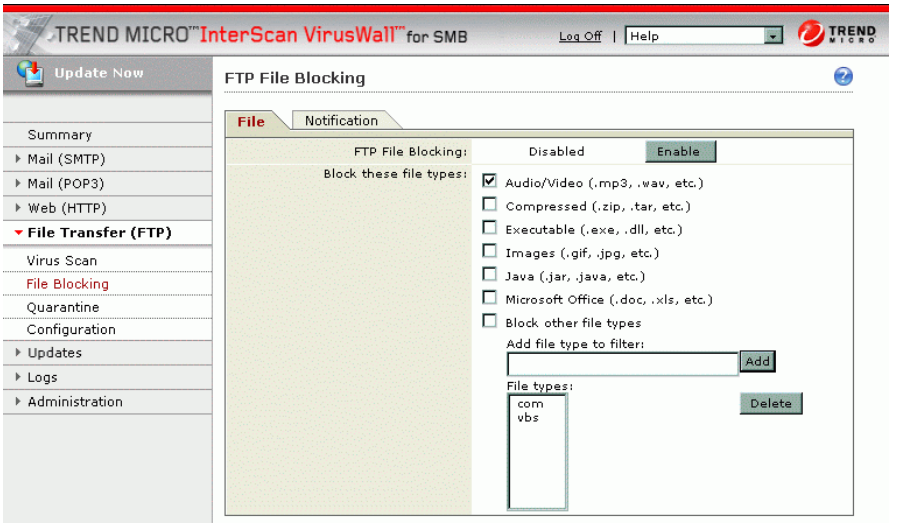


FIGURE 6-9. Setting up FTP file blocking

When users attempt to transfer a file that you have designated as blocked, they receive a standard notice in their browser or FTP client that this file cannot be transferred.

To add a notification message of your own composition, see the online help for the **Notification** tab for the **File Transfer (FTP)** > **File Blocking** > **FTP File Blocking** screen.

Fine-tuning SMTP settings

The installation script prompts you to supply the basic settings needed to set up the SMTP protocol. You are ready to begin scanning SMTP traffic with InterScan VirusWall after installation and activation. However, the tabs on the **Mail (SMTP)** > **Configuration** screen contain fields that allow you to customize additional SMTP settings.

There are five tabs on the **SMTP Configuration** screen:

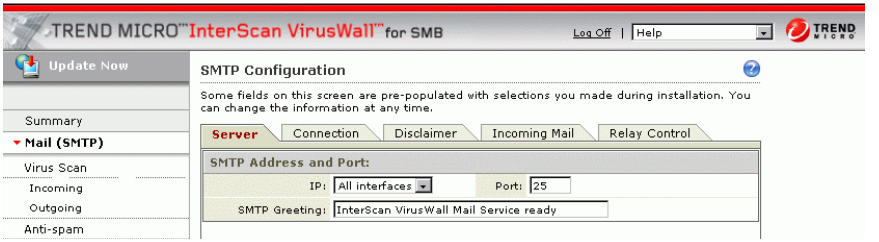


FIGURE 6-10. SMTP Configuration - Server

Choose the appropriate tab to complete the following configuration:

- Server—Set up basic connections to enable the SMTP service
- Connection—Create settings that allow you to define servers (by IP address) from which you will accept incoming SMTP messages
- Disclaimer—Create an optional disclaimer that appears in the beginning or end of the message body for all outgoing messages
- Incoming Mail—Create settings that allow you to define domains you consider incoming for the purpose of virus scanning and content filtering
- Relay Control—Identify trusted hosts that are allowed to relay messages via your SMTP server

SMTP configuration settings - server

When you first display the **Server** tab of the **SMTP Configuration** screen, the fields are pre-populated with values you entered during installation. (After you have completed installation, all required settings that enable the SMTP protocol have been established.) Enter new values in the fields on this screen to make changes to your SMTP configuration after installation if you choose.

The **Incoming Message Size** section of this screen allows you to configure two message size rules that are *not* set up during installation. These rules let you:

- Reject messages addressed to more than a specified number of recipients, and
- Reject messages larger than a set number of MB

The fields are optional, but are recommended, to help prevent Denial of Service attacks on your network.

SMTP configuration settings - connection

The fields on the **Connection** tab of the **SMTP Configuration** screen allow you to:

- Accept SMTP messages from all server IP addresses except those you define in the exception list, or
- Deny SMTP messages from all server IP addresses except those you define in the exception list

If you want a more *inclusive* acceptance policy, meaning you want to accept email from most senders with a few exceptions, select **Accept** and define the exceptions—IP addresses from which you will not accept SMTP traffic. If you want a more *exclusive* acceptance policy, select **Deny**, which will disallow SMTP traffic from all servers except those you add to the **Exception list** field.

SMTP configuration settings - disclaimer

The **Disclaimer** tab of the **SMTP Configuration** screen contains fields that allow you to create an optional disclaimer that is appended to the beginning or end of all outgoing messages. A sample disclaimer is shown in the online help.

SMTP configuration settings - incoming mail

The **Incoming Mail** tab of the **SMTP Configuration** screen contains fields that allow you to specify domains from which you will always accept incoming messages. This feature is similar to the **Connection** tab, except that you are specifying domain names rather than IP addresses.

These fields are optional, as are the fields on the **Connection** tab, but are provided to allow you to refine the SMTP traffic you will allow in your network. The option to screen by both IP (on the **Connection** tab) and by domain (on the **Incoming Mail** tab) is available, because MTAs may use different rules for filtering traffic.

For example, the following figure illustrates that a message sent from a server in the domain “example.org” with IP address “123.123.123.123” is successfully delivered under the traffic evaluation rules for MTA 1, but not MTA 2.

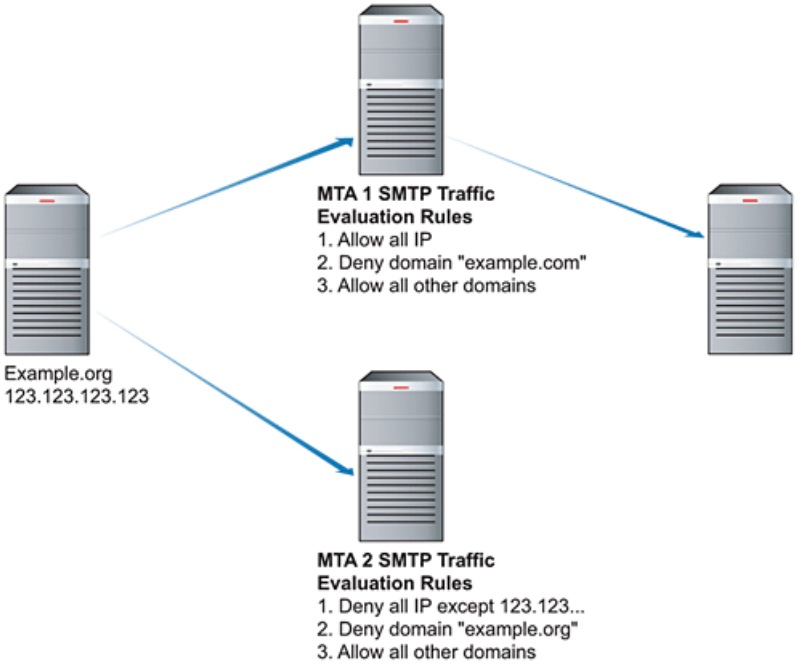


FIGURE 6-11. SMTP configuration settings - incoming mail

SMTP configuration settings - relay control

Relaying is a process of utilizing bandwidth from other networks to move an email message to a final delivery point. If an SMTP server is set up to allow relaying, either intentionally or by accident, *anyone* can connect to the SMTP server and send email.

This practice:

- Slows down the legitimate business traffic for the relaying server, because it has to handle relaying traffic as well as legitimate traffic
- Allows senders of spam mail to utilize an unprotected server for relaying spam, which could result in a lawsuit

Further, the risk of having an open relay is that your server could get blacklisted, which means email messages from your company would be rejected by mail servers all over the world.

To rule out this problem, ISVW is *already* configured to prevent relaying of traffic through your network. The **Relay Control** tab of the **Mail (SMTP)** > **Configuration** > **SMTP Configuration** screen states that InterScan VirusWall does not allow other hosts to use your server as a relay, unless you identify them as trusted.

You can allow trusted domains, such as a subsidiary or a joint venture partner, to relay traffic by configuring the domain name in the Trusted Domains section of this screen.

To allow a trusted domain to relay through your network:

1. Enter the domain name in the **Add domain** field.
2. Click **Add**. The domain name displays in the **Trusted domains** field.

The following example shows that three domains have been added as trusted domains—tellsitall.com, sales.tellsitall.com, and finance.tellsitall.com.

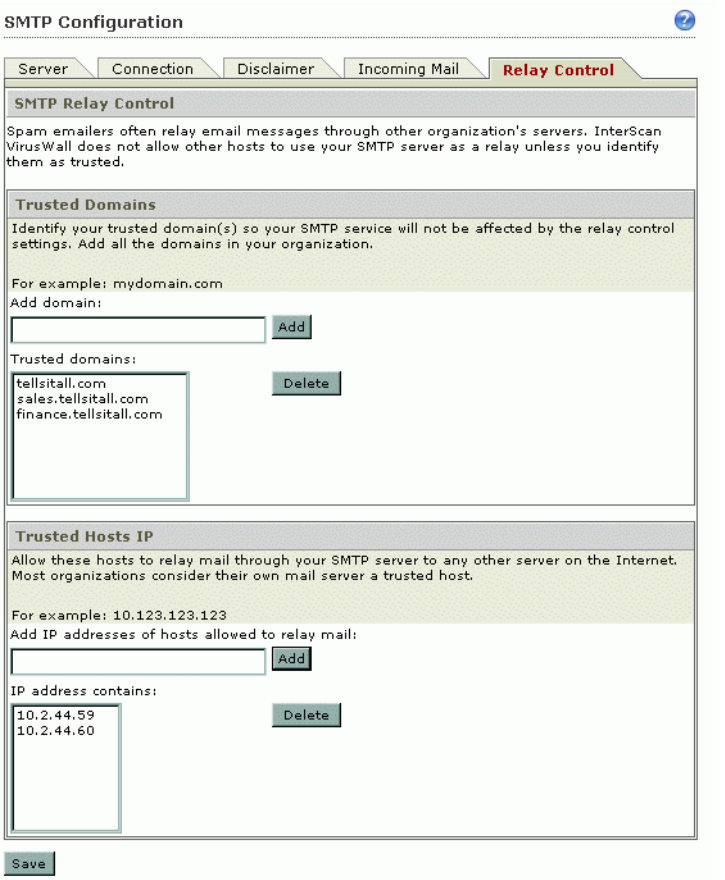


FIGURE 6-12. SMTP configuration - relay control tab

To allow a trusted host to relay through your network:

1. Enter the host IP address in the **Add IP address of hosts allowed to relay mail** field.

2. Click **Add**. The host IP address displays in the **IP address contains** field. The example shows that two IP addresses have been added as trusted hosts—10.2.44.59, and 10.2.44.60.

Only domains or hosts added to the Trusted sections of this screen are allowed to use the ISVW server as a relay. Relay attempts from other organizations are blocked.

Fine-tuning spam filtering

If you are getting too many false positives, to decrease the number, set the spam threshold setting to **Low**. Conversely, you may be getting complaints from users that they are still getting too much spam. In this case, adjust the threshold from **Low** to **Medium**, or **Medium** to **High**.

The following example shows the Threshold section of the **POP3 Anti-spam** screen. To display this screen, click **Mail (POP3)** > **Anti-spam**. The **POP3 Anti-spam** screen displays. The anti-spam filter threshold is set on the **Target** tab, as shown below:

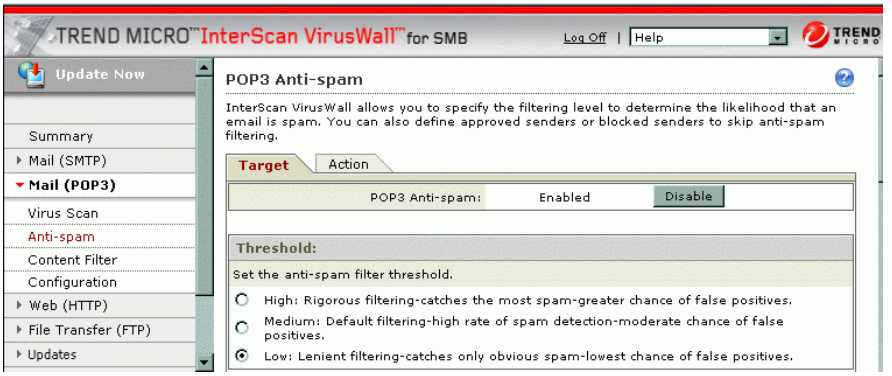


FIGURE 6-13. Adjusting the spam settings on the POP3 Anti-spam screen

A similar section exists on the **SMTP Incoming Anti-spam** screen. To adjust settings for the SMTP Incoming Anti-spam screen, click **Mail (SMTP)** > **Anti-spam**. The **SMTP Incoming Anti-spam** screen displays. Configure the threshold on the **Target** tab.

Approved/blocked senders list

You can reduce demand on the spam engine by setting up a list of:

- Approved senders—senders whose messages are never filtered for spam because they are always accepted
- Blocked senders—senders whose messages are not filtered for spam because they are never accepted

Setting up an approved senders list also helps reduce the incidence of false positives. For example, employee newsletters are often falsely identified as spam. To prevent a flood of false positives whenever your employee newsletter is mailed, add the employee newsletter address to your approved senders list.

See the anti-spam online help screens for more information.

Chapter 7

Troubleshooting

This chapter is provided to help you troubleshoot. Information is provided for the following situations:

- Cannot log on
- Activation Code is invalid
- No log or quarantine directory
- Cannot update the pattern file
- Cannot create a spam stamp identifier
- Unacceptable number of false positives
- Cannot accept any false positives
- Unacceptable amount of spam
- Management console timed out
- Performance seems degraded
- Virus is detected but cannot be cleaned

In addition, other information resources are described in this chapter, such as the Trend Micro Knowledge Base containing thousands of solutions, the Virus Information Center, free scanning tools, and more.

To contact Trend Micro support, visit:

`http://kb.trendmicro.com`

Click the appropriate Contact Support link for your region, to view the telephone number to call.

Issues

The following describes issues you might encounter with ISVW, as well as possible causes and suggested solutions.

Cannot log in

You entered an administrator password when you installed InterScan VirusWall with the installation script. You must use the password you created during installation to log in. Passwords are case-sensitive—be sure you have entered the characters correctly.

Activation Code is invalid

If you are attempting to activate InterScan VirusWall and get an error message about the Activation Code, there are several possible explanations.

- Verify that you entered the Activation Code correctly. The hyphens are required.
- If you are entering an Activation Code for a trial version, and the trial period has expired, you cannot activate the product until you purchase the software and register. After registration, you will receive a valid Activation Code via email, typically within 20 minutes.
- If the problem is not a typing error or an evaluation version of the license, contact technical support for assistance.

No log or quarantine directory

If InterScan VirusWall cannot find the directory path for the log or quarantine directories, you will get an error message. If you know the directories already exist, verify that they have not been moved or renamed.

If they do not already exist, create a sub-directory in the selected directory path, and create the path. Then go back to what you were doing prior to the error message and try again. If you are still unsuccessful, contact Trend Micro technical support for assistance.

Cannot update the pattern file

If the pattern file is out of date, and you are unable to update it, the most likely cause is that your Maintenance Agreement has expired. Check the status on the **Summary** screen. If the date shown in the **License** field is in the past, you cannot update the pattern file until you renew your Maintenance Agreement.

Another possible cause is that the Trend Micro ActiveUpdate server is temporarily down. Try to update again in a few minutes.

Cannot create a spam stamp identifier

A spam stamp identifier is a message that appears in the email message subject. For example, for a message entitled Q3 Report, if the spam stamp identifier is defined as "Spam:," the message subject would appear as "Spam:Q3 Report."

If you are having problems creating a spam identifier, make sure you are using only English upper and lowercase characters, digits 0-9, or the following set of special characters:

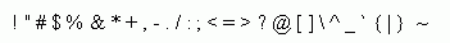


FIGURE 7-1. Special characters for spam stamp identifier

If you attempt to use characters other than those specified, you will not be able to use the spam identifier for your SMTP and POP3 messages.

Unacceptable number of false positives

Your spam filtering threshold may be set at a level that is too aggressive for your organization. Try a lower setting in the Threshold fields on the **SMTP Anti-spam** screen and the **POP3 Anti-spam** screen.

Also, if users in your network are receiving newsletters, this type of message tends to trigger a high number of false positives. Add the newsletter email address or domain name to the approved senders list to bypass spam filtering on these messages.

Cannot accept any false positives

Some organizations, such as banks and other financial institutions, cannot risk any message being identified as a false positive. In this case, disable the anti-spam feature for SMTP and POP3.

Unacceptable amount of spam

You may have set your spam filtering threshold at a level that is too lenient for your organization. Try a higher setting in the Threshold fields on the **SMTP Anti-spam** screen and the **POP3 Anti-spam** screens.

Management console timed out

If you leave the management console active and there is no activity detected for approximately 10 minutes, your session is timed out. Log in again to resume work. Unsaved changes to your work are lost. If you are called away, it's best to save your work and log off until your return.

Performance seems degraded

If the system is slow, and you are receiving an excessive number of alerts, such as the message queue is continuously backed up or a daemon has stopped, possible causes are:

- You have exceeded the allowed number of connections
- You have exceeded the ISVW default limits

To resolve this issue, you may want to install a faster CPU or more memory.

Virus is detected but cannot be cleaned

If you think you are infected with a virus that does not respond to cleaning, go to the following URL:

`http://subwiz.trendmicro.com/SubWiz/Default.asp`

This link takes you to the Trend Micro Submission Wizard, which includes information on what to do, including how to submit your suspected virus to TrendLabs for evaluation.

Virus scanning not working

Ensure that no one has disabled the virus scanning feature, on the SMTP Incoming, SMTP Outgoing, POP3, HTTP, and FTP Virus Scan screens. If scanning is enabled but viruses are not being detected, contact technical support for assistance.

Free detection tools

Trend Micro provides several tools, at no charge, to the public.

Knowledge Base

You are welcome to search for more information in the Trend Micro online Knowledge Base. The Support URL is:

`http://kb.trendmicro.com`

The Knowledge Base search engine allows you to refine your search, by entering product name, problem category (such as hardware, installation, and so on), and keywords. There are thousands of solutions available in the Knowledge Base, and more are added weekly.

Virus information center

Comprehensive security information is available from the Trend Micro free Virus Information Center. The URL is:

`http://trendmicro.com/vinfo/default.asp`

In the Virus Information Center, you can find information about the following:

- **Virus advisories**—current news about the top threats, associated risks, and the pattern file update that addresses the threat
- **Weekly Virus Report** —current news about threats that have appeared in the past week
- **Virus Map**—a description of threats by location worldwide
- **Virus Encyclopedia**—a compilation of knowledge about all known viruses
- **Test files**—a test file for testing InterScan VirusWall, and instructions for performing the test
- General virus information, including:
  - **Virus Primer**—an introduction to virus terminology and a description of the virus life cycle
  - **Safe Computing Guide**—a description of safety guidelines to reduce the risk of virus infections
  - **Risk ratings**—a description of how viruses are classified as Very Low, Low, Medium, or High threats to the global IT community
- **White papers**—that explain such concepts as the real cost of a virus outbreak or how to manage email content security
- **Webmaster tools**—free virus information updates and tools
- **TrendLabs**—the ISO 9002-certified virus research and product support center

Global support centers

If you need to contact a technical support center, the Support URL contains links to the global support centers, by region. The regions are:

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- US & Canada

Telephone numbers are available for each contact center. The URL is:

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

To contact the US technical support center, call 1-888-608-1009, between 5 A.M. and 5 P.M., Pacific Standard Time.

Before contacting technical support

Before you contact technical support, check the documentation and online help to see if it contains the answer you are looking for. If you have checked the documentation, as well as Knowledge Base, and still need help, be prepared to give the following information to speed the resolution of your problem:

- Product Activation Code
- Version number of the product
- Version number of the pattern file and scan engine
- Version of your operating system
- Number of users
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- Detailed description of the install environment
- Exact text of the error message, if you received one
- Steps to reproduce the problem

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your InterScan VirusWall software after completion of the registration process. InterScan VirusWall will not be operable until product activation is complete. Activate during installation on the **Product Activation** screen, or after installation (in the management console) on the **Administration** > **Product License** screen.
Activation Code	A 37-character code, including hyphens, that is used to activate InterScan VirusWall. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.

Term	Explanation
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to “system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of InterScan VirusWall to manage notifications and alerts.
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
anti-relay	Mechanisms to prevent hosts from “piggybacking” through another host’s network.
anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other “nuisance” mail.
anti-spam rules and engine	The Trend Micro tools used to detect and filter spam.
antivirus	Computer programs designed to detect and clean computer viruses.
approved sender	A sender whose messages are always allowed into your network.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.

Term	Explanation
audio/video file	A file containing sounds, such as music, or video footage.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
blocked sender	A sender whose messages are never allowed to enter your network.
boot sector	A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer's operating system.
boot sector virus	A virus targeted at the boot sector (the operating system) of a computer.
browser	A program which allows a person to read hypertext, such as Internet Explorer or Mozilla. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast portion of memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.

Term	Explanation
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to protocol, asking for information or action, and the server responds.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how InterScan VirusWall will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, */opt/trend/isvw* is the default installation directory on your system.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW Quarantine directory is: */opt/trend/isvw/config*
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.

Term	Explanation
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution," uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
download (noun)	Data that has been downloaded, for example, from a Web site via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

Term	Explanation
file name extension	The portion of a file name (such as .txt or .xml) which typically indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
filter criteria	User-specified guidelines for determining whether a message and attachment(s), if any, will be delivered, such as: - size of the message body and attachment - presence of words or text strings in the message subject - presence of words or text strings in the message body - presence of words or text strings in the attachment subject - file type of the attachment
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
group file type	Types of files that have a common theme. There are six group file types in the InterScan VirusWall interface, they are: - Audio/Video - Compressed - Executable - Images - Documents
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hacker	*See* virus writer
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.

Term	Explanation
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.
HouseCall	A free virus scanning and cleaning product from Trend Micro. HouseCall can detect and clean viruses found on your hard drive, but HouseCall does not provide real-time protection. In other words, HouseCall can help you to discover and clean up an existing problem, but will not prevent future ones, nor will HouseCall protect against worms, or mass-mailing programs. For preventive protection, you need InterScan VirusWall.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software.
IMAP	Internet Message Access Protocol—A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders (mailboxes), in a way that is functionally equivalent to local mailboxes.
incoming	Email messages or other data routed *into* your network.
installation script	The setup program used to install InterScan VirusWall.
IntelliScan	IntelliScan is a Trend Micro scanning technology that examines file headers using true file type recognition, and scans only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.

Term	Explanation
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
license	Authorization by law to use InterScan VirusWall.
license certificate	A document that proves you are an authorized user of InterScan VirusWall.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.

Term	Explanation
log storage directory	Directory on your InterScan VirusWall machine that stores the log files. This directory is set up on the **Directories** tab of the **Administration Configuration** screen.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
KB	Kilobyte—1024 bytes of memory.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
management console	The InterScan VirusWall user interface.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
match case	*See* case-matching.
MB	Megabyte—1024 kilobytes of data.
message	An email message, which includes the message subject in the message header, and the message body.
message body	The content of an email message.
message queue	The number of messages waiting to be scanned.
message size	The number of KB or MB occupied by a message and its attachments.

Term	Explanation
message subject	The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.
MX record	A DNS resource record type indicating which host can handle electronic mail for a particular domain.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.

Term	Explanation
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
PC	Personal Computer—A general-purpose single-user microcomputer designed to be operated by one person at a time.
polymorphic virus	A virus that is capable of taking different forms.
POP3	Post Office Protocol, version 3—A messaging protocol that allows a client computer to retrieve electronic mail from a server via a temporary connection, for example, a mobile computer without a permanent network connection.
POP3 server	A server which hosts POP3 email, from which clients in your network will retrieve POP3 messages.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected email messages, email messages with infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your InterScan VirusWall server. The Quarantine Directory is typically located in the following directory path: */opt/trend/isvw/quarantine*
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.

Term	Explanation
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
removable drive	A removable hardware component or peripheral device of a computer.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
rule-based	Describes the anti-spam engine, which is based on a set of rules for determining whether an email message should be considered spam. When the anti-spam engine examines an email message, it searches for matches between the mail contents and the entries in the rules files.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
seat	A license for one person to use InterScan VirusWall.
Secure Password Authentication	An authentication process, by which communications can be protected, using for example, encryption and challenge/response mechanisms.
sender	The person who is sending an email message to another person or entity.

Term	Explanation
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations. InterScan VirusWall can act as the SMTP server, so that virus scanning, content filtering, and spam detection take place before the message is delivered to the recipient.
SOCKS4	A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.
spam	Unsolicited email messages meant to promote a product or service.
stamp	To place an identifier, such as “Spam,” in the subject field of an email message.
status bar	A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

Term	Explanation
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
trigger	An event that causes an action to take place. For example, InterScan VirusWall detects a virus in an email message. This *triggers* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan	A malicious program that is disguised as something benign.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
trusted domain	A domain from which InterScan VirusWall will always accept messages, without considering whether the message is spam. For example, a company called Gold Standard Finance, Inc. has a subsidiary called Gold Standard Finance-Japan, Inc. Messages from goldstandardfinance-japan.com are always accepted into the goldstandardfinance.com network, without checking for spam, since the messages are from a known and trusted source.
trusted host	A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.

Term	Explanation
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect and replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a malicious computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
wildcard	In InterScan VirusWall, the term is used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Term	Explanation
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.

Appendix B

Scripts in InterScan VirusWall

The following description of scripts utilized in the ISVW application are provided for your information only. Trend Micro does not recommend changing the content of the script files.

Invoked by	*File Name*	*Description*
cron daemon	cleanfile.sh	This script manages regular cleanup of HTTP temp files
cron daemon	cleanscan.sh	This script manages regular cleanup of FTP temp files
cron daemon	CM_clearlog_agent.sh	This script manages regular cleanup of CM (Control Manager) logs
cron daemon	ISpurgefile.sh	This script manages cleanup of log files, temp files, reg-server log files, old pattern files, and other logs
cron daemon	ISupdate.sh	This script manages scheduled updates of the pattern files and scan engine

Invoked by	*File Name*	*Description*
cron daemon	purgefile.sh	This script manages cleanup of HTTP logs, virus logs, the URL blocking log, and notification delivery log
manually invoked	reset_password.sh	This script resets the administrator's password to "password" - you must have root privilege to execute the script

Index

V

W