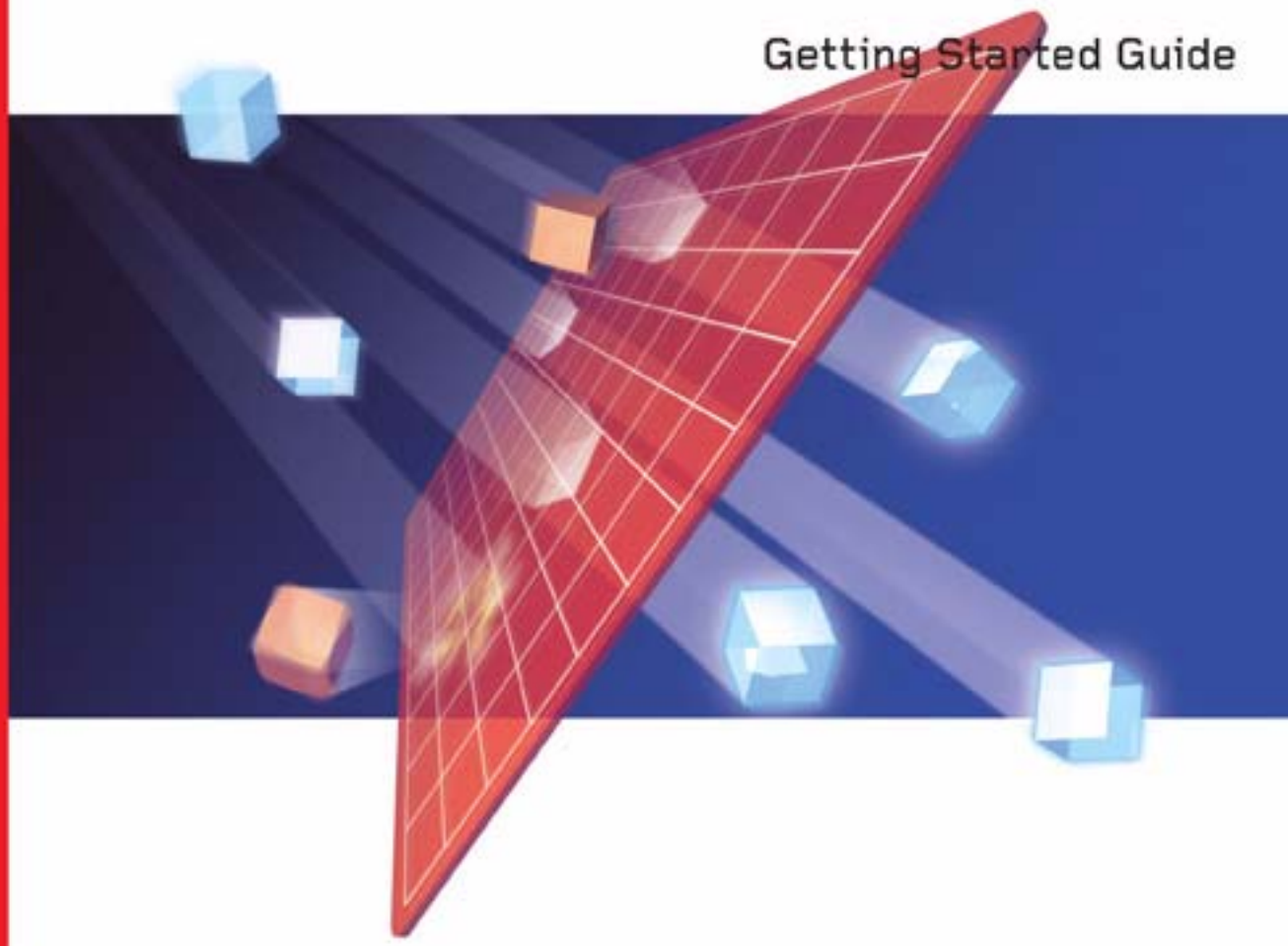
TREND MICRO™
InterScan™ WebProtect 5

Integrated HTTP gateway protection

for Microsoft™ ISA Server

Getting Started Guide



TREND MICRO™

Release Date: April, 2007

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please email us at:

docs@trendmicro.com

Your feedback is always welcome. You can evaluate this documentation on the Web at the following location:

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

Contents

Chapter 1: Introducing Trend Micro InterScan WebProtect

HTTP Security Risk Overview 1-2
- Comprehensive Web Security 1-2
- Leading Virus Protection 1-2
- Centralized Management and Coordination 1-2

Main Features 1-3
- HTTP Virus Scanning 1-3
- Configurable Deferred Scanning 1-3
- Reports and Logs 1-3
- Notifications 1-4

Updatable Program Components 1-4
- Virus Pattern File 1-5
- Spyware/Grayware Pattern File 1-6
- Scan Engine 1-7

About Hot Fixes, Patches, and Service Packs 1-9

InterScan WebProtect Documentation 1-10

Chapter 2: Installing InterScan WebProtect

Upgrade Information 2-2
- Upgrading from ISA 2004 to ISA 2006 2-2

Minimum System Requirements 2-6

Installing InterScan WebProtect 2-7
- Post Installation 2-20

Removing InterScan WebProtect 2-21

ISA Policies 2-23
Configuring ISA Policy Rules for ISWP 2-23

Chapter 3: Getting Up and Running with WebProtect

Opening the ISWP console 3-2
Obtaining an Activation Code 3-2
Obtaining a Registration Key 3-2
Activating WebProtect 3-4
Component Version Information 3-5
Proxy Settings for Updates 3-6
Manual Updates 3-8
Forced Manual Updates 3-8
Scheduled Updates 3-9
Maintaining Updates 3-11
Rolling Back an Update 3-11
Deleting Old Pattern Files 3-11
Configuring Notifications 3-12
Enabling Virus and Spyware Scanning 3-12
Configuring Proxy Settings 3-13
Setting the Database Connection 3-14
Testing InterScan WebProtect 3-16
EICAR Test File 3-16
Download Scanning 3-17
Upload Scanning 3-17

Chapter 4: Configuring InterScan WebProtect

Sending Infection Data to the World Virus Tracking Center 4-2
Changing the Management Console Password 4-3
HTTP Scanning Performance Considerations 4-5
HTTP Virus Scanning Rules 4-5
Configuring Compressed File Scanning Limits 4-9
Handling Large Files 4-10
Spyware and Grayware Scanning Rules 4-12
Setting the Scan Action for Viruses 4-14
Scan Events 4-15
Introduction to Notifications 4-15
Email Notification Settings 4-16

Notification Tokens/Parameters 4-17
Configuring Notifications 4-18

Chapter 5: Logs and Reports

Overview 5-2
Report Types 5-2
Generating Real-time Reports 5-3
Scheduled Reports 5-5
Report Settings 5-7
Introduction to Logs 5-9
Log Settings 5-11

Appendix A: Encrypting Browser-Console Communication (HTTPS)

Accessing the InterScan WebProtect Console via HTTPS A-3
Disabling Non-HTTPS Access A-3
Configurations After Changing the Console Listening Port A-4

Appendix B: Frequently Asked Questions (FAQs)

Appendix C: Maintenance Agreement

Renewing the Maintenance Agreement C-2

Chapter 1

Introducing Trend Micro InterScan WebProtect

This chapter introduces InterScan WebProtect 5.01 and explains how it helps to ensure your organization's gateway security.

Topics in this chapter include:

- Introducing how InterScan WebProtect protects against HTTP security risks
- Introducing the main ISWP benefits, its main features and what's new in the latest version
- Explaining the ISWP program architecture and the main program components, services and scheduled tasks
- Explaining the updatable program components in ISWP
- Explaining the different types of product updates available, including hot fixes, patches, and service packs

HTTP Security Risk Overview

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

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

Comprehensive Web Security

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

Leading Virus Protection

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

Centralized Management and Coordination

IT administrators can easily manage InterScan WebProtect along with other Trend Micro products within a centralized management console, Trend Micro Control Manager™ (TMCM). TMCM provides a unified view of Trend Micro software installations across the enterprise. Activities can be centrally managed. Using the URL redirect feature, the TMCM management console can access each individual

instance of the ISWP and perform ISWP policy modification through the ISWP management console.

You can view real-time or scheduled reports with enhanced graphs and charts. The end result: you can deploy an immediate, coordinated response to block any emerging risk.

Main Features

The following InterScan WebProtect features help you maintain HTTP gateway security.

HTTP Virus Scanning

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

Configurable Deferred Scanning

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

Reports and Logs

InterScan WebProtect includes many pre-configured reports to provide a summary of your gateway security status. Reports can be run for a specific time period and customized to only provide information about clients in whch you are interested.

To provide current information about your HTTP gateway security, InterScan WebProtect is pre-configured to generate spyware/grayware reports. Reports can be generated on-demand or scheduled on a daily, weekly or monthly basis.

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

Notifications

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

Updatable Program Components

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

- **ActiveUpdate:** ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of pattern files and the scan engine. ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on-demand.
- **Virus and spyware/grayware pattern files**: These are the files that contain the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, InterScan WebProtect is able to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the grayware/spyware pattern files are updated less frequently.
- **Scan engine**: This is the module that analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.

Virus Pattern File

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

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

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

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

How it Works

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

Virus Pattern File Naming

Pattern files use the following naming format:

`lpt$vpn.###`

where ### represents the pattern version (for example, 400). To accommodate pattern versions greater than 999, the InterScan WebProtect management console displays the following format:

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

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

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

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

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire pattern file (15MB - 20MB), ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software and deploy pattern files throughout your environment.

Controlled Virus Pattern Releases

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

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

Spyware/Grayware Pattern File

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

The spyware/grayware pattern file, which is stored in <Install_directory> uses the following naming format:

tmaptn.###

where ### represents the pattern version. This format accommodates pattern versions greater than 999. The ISWP management console displays the following format:

roll number.pattern version (format: xxxxx.###)

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

Scan Engine

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

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

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

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

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

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

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

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

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

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

About Scan Engine Updates

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

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

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

http://www.trendmicro.com/download/engine.asp

About Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address issues, enhance product performance, or add new features.

The following is a summary of the items Trend Micro may release:

- **Hot fix:** a work-around or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Security Patch:** a hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Patch:** a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Service Pack:** a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

You can check the Trend Micro Web site regularly to download patches and service packs:

http://www.trendmicro.com/download

All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

InterScan WebProtect Documentation

The documentation set for ISWP includes the following:

- **Getting Started Guide**—This guide helps you plan for and install the ISWP server programs and modify important default client settings.
- **Online Help Topics**—The purpose of help topics is to provide descriptions for performing the main tasks, usage advice, and field-specific information, such as valid parameter ranges and optimal values. The Help topics are accessible from the ISWP console.
- **Readme file**—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and product release history.
- **Knowledge Base**—The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site:

  http://esupport.trendmicro.com

Chapter 2

Installing InterScan WebProtect

This chapter describes the system requirements for InterScan WebProtect, and step-by-step instructions on how to install and remove the program:

- Upgrade Information
- Recommended System Requirements
- Installing InterScan WebProtect
- Removing InterScan WebProtect
- Testing InterScan WebProtect
- Configuring ISA Policies

Upgrade Information

If you are using a previous version of WebProtect you must remove it before installing InterScan WebProtect version 5.01. You cannot upgrade from ISWP version 3.x or earlier to ISWP version 5.01.

During installation, depending on the install options you have selected, Setup will prompt you for the following information:

- An Activation Code, evaluation or full, for the modules you will install (alternatively, you can Activate ISWP after installation using Web console); contact your Trend Micro reseller for an Activation Code if you do not have one
- IP address and port of the proxy server used to connect to the Internet
- IP address and port of the SMTP server you will use to relay ISWP notification messages, and the default email address to which you want those notifications sent
- IP address and port of the Trend Micro Control Manager server (if any)
- A password, to restrict access to the ISWP management console
- ISWP writes virus, spyware/grayware, and other data to a database, typically the default ISA database. If you are installing multiple instances of ISWP and want them all to share a common database, or if you want to use a SQL/MSDE database other than the default ISA one, you will need to provide the location and logon credentials of that database server.
- For installation on to an ISA Server 2004 and 2006 Enterprise Edition, the location and logon credentials of the Configuration Storage Server

Upgrading from ISA 2004 to ISA 2006

ISA server 2004 uses a database to store configurations and log data. During the installation of ISA server 2004, users can choose to install an MSDE 2000 as the database of the ISA server. By default, ISWP 5.0/5.01 will create a database in the MSDE 2000 instance that is installed along with the ISA server to store configuration and log data. When upgrading from ISA 2004 to ISA 2006, ISA will remove all other databases created in an MSDE instance. ISWP 5.0/5.01 will *not* work after upgrading without the database. Users should backup the database used by ISWP 5.0/5.01 *before* upgrading and restore it after they have upgraded successfully.

Upgrading to ISA 2006 involves the following process:

- *To backup the ISWP 5.0/5.01 database:* on page 2-3
- *To upgrade from ISA 2004 to ISA 2006:* on page 2-4
- *To restore the ISWP 5.0/5.01 database:* on page 2-4
- *To restart all ISWP 5.0/5.01 services:* on page 2-5

To backup the ISWP 5.0/5.01 database:

1. Stop all ISWP 5.0/5.01 services from Services Control Panel.

   All ISWP 5.0/5.01 services should be stopped before detaching the "ISWPDB" database. The descriptive names of ISWP services start with "Trend Micro InterScan WebProtect".

2. Detach the database named "ISWPDB" from MSSQL/MSDE using the T-SQL or Enterprise Manager method.

   To use the T-SQL detachment method:

   a. Execute the following T-SQL statement:

      ```
      EXEC sp_detach_db @dbname = 'iswpdb'
      ```

   To use the Enterprise Manager detachment method:

   a. Expand a server group, and then expand the installed ISA server.

      (Add it to the group first, if it is not in the group.)

   b. Expand **Databases**.

   c. Right-click the database "ISWPDB", and then select **All Tasks/Detach**.

   d. To terminate any existing connections from the database, click **Clear**.

   e. Click **OK**.

      The database node for the detached database is removed from the Database folder.

3. Copy the database files to a backup directory.

   a. Locate the default database files.

      The default file names of database "ISWPDB" are "iswpdb.mdf" and "iswpdb_log.LDF". They are located in default database data directory. For example:

```
C:\Program Files\Microsoft SQL Server\MSSQL$MSFW\Data
```

b. Copy both files to a backup directory.

To upgrade from ISA 2004 to ISA 2006:

1. Refer to the upgrade guide from Microsoft when upgrading.

   There are differences between the Enterprise edition and Standard edition.

2. Find the approprate instructions

   For the Enterprise edition, go to:

   http://www.microsoft.com/technet/isa/2006/Upgrade_Guide_EE.mspx

   For the Standard edition, go to:

   http://www.microsoft.com/technet/isa/2006/upgrade_guide_se.mspx

3. Restore the backup database after upgrading successfully.

To restore the ISWP 5.0/5.01 database:

1. Move the database files from the backup directory to the default database data directory. For example:

```
C:\Program Files\Microsoft SQL Server\MSSQL$MSFW\Data
```

2. Attach the database "ISWPDB" with specified database files using the T-SQL or Enterprise Manager attachment method:

   To use the T-SQL attachment method:

   Execute the following T-SQL statement.

```
EXEC sp_attach_db @dbname = N'iswpdb',
    @filename1 = N'c:\Program Files\Microsoft SQL
Server\MSSQL\Data\iswpdb.mdf',
    @filename2 = N'c:\Program Files\Microsoft SQL
Server\MSSQL\Data\iswpdb_log.ldf'
```

   To use the Enterprise Manager method of attachment:

   a. Expand a server group, and then expand the installed ISA server.

   Add it to the group first, if it is not in the group.

   b. Right-click **Databases**, and select **All Tasks/Attach Database**.

   c. Enter and select the name of the MDF (master data file) of the database to be attached. Enter or select the correct file.

For example:

```
C:\Program Files\Microsoft SQL Server\MSSQL\Data\iswpdb.mdf
```

d. Specify the database owner as "sa".

e. Click **OK**.

A database node for the newly attached database is created in the Database folder.

To restart all ISWP 5.0/5.01 services:

1. Restart all ISWP 5.0/5.01 services after database is restored.
2. If your current ISWP is release 5.0, please upgrade to ISWP 5.01.

Note: The new release ISWP of 5.01 supports ISA 2006 with improved quality.

Minimum System Requirements

Each instance of InterScan WebProtect can support roughly 500 concurrent connections, but on a system with the following software and hardware:

Hardware

- Intel® Pentium® 4 3GHz processor or equivalent
- 512MB RAM (1GB recommended)
- 1GB available disk space
- A monitor with 800x600 or greater resolution
- 10/100Mbbs network connection

Software

- Microsoft ISA Server 2004 with SP1 or SP2 or ISA Server 2006
- Microsoft Windows 2003 Server with Service Pack 1 (SP1) or Windows 2000 Server with SP4
- Microsoft Windows Server 2003 R2
- Microsoft SQL Server or Microsoft MSDE 2000 with SP3

Supported System Combinations (ISWP + Windows + ISA)

- Microsoft Windows 2003 Server, Service Pack 1, and Microsoft ISA Server 2004 or 2006 *standard*
- Microsoft Windows 2003 Server, Service Pack 1, and Microsoft ISA Server 2004 or 2006 *enterprise*
- Microsoft Windows Server 2003 R2, and Microsoft ISA Server 2004 or 2006 *enterprise*
- Microsoft Windows Server 2003 R2, and Microsoft ISA Server 2004 or 2006 *standard*
- Microsoft Windows 2000 Server, Service Pack 4, and Microsoft ISA Server 2004 or 2006 *standard*

Web Browser (for remote access):

- Microsoft Internet Explorer (IE) 6.0 with SP1 is recommended. (IE 7.0 is not supported.)

Installing InterScan WebProtect

After acquiring the InterScan WebProtect installation package, complete the following steps to install the software.

Note: If you plan to configure ISWP to use a remote database, you need to update the ISA policy *before* installation. See *ISA Policy Rule 1. Allowing ISWP to Access a Remote Database Server* on page 2-23 for details.

Running the InterScan WebProtect setup program from a folder:

1. Open the folder containing the InterScan WebProtect setup files in a Windows Explorer window.
2. Double-click the file `setup.exe` to begin installing. The Setup **Welcome** screen displays. Click **Next**.
3. The **License Agreement** screen displays. Click **I accept** to accept the license agreement and continue installing, **Print** to create a hard copy, or **I do not accept** to exit Setup.

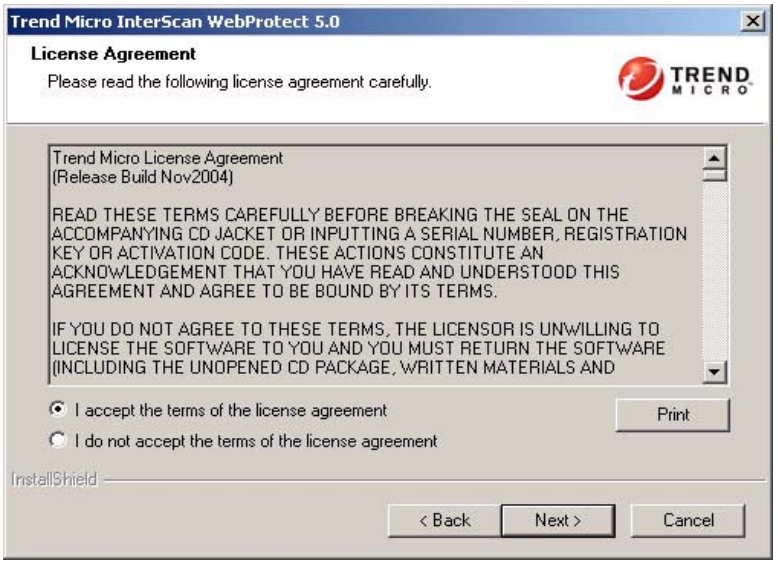


FIGURE 2-1. Click "Yes" to accept the License Agreement.

4. The InterScan WebProtect setup program checks to ensure the server meets the minimum system requirements. Click **Next**.
5. The **Installation Folder** screen displays. Type the path where you want to install InterScan WebProtect, or click **Browse** to select a folder. The default destination is:

   ```
   C:\Program Files\Trend Micro\InterScan WebProtect\
   ```

Note: InterScan WebProtect does not support installation to a shared drive or a remote server.

6. The **Component Selection** screen displays. Select the components you want to install. Options are:
   - **Main Program**—installs the administration user interface and the basic library files necessary for InterScan WebProtect
   - **WebFilter for ISA Server**—installs the service necessary for HTTP scanning.
   - **TMCM Agent** —installs the files necessary for the Control Manager agent, to enable centralized management, updates, and consolidated logging through Control Manager. You need to install the agent if you are using Control Manager (Trend Micro's central management console). Installing InterScan WebProtect and Control Manager on the same machine is not supported.

7. Click **Next** to continue.

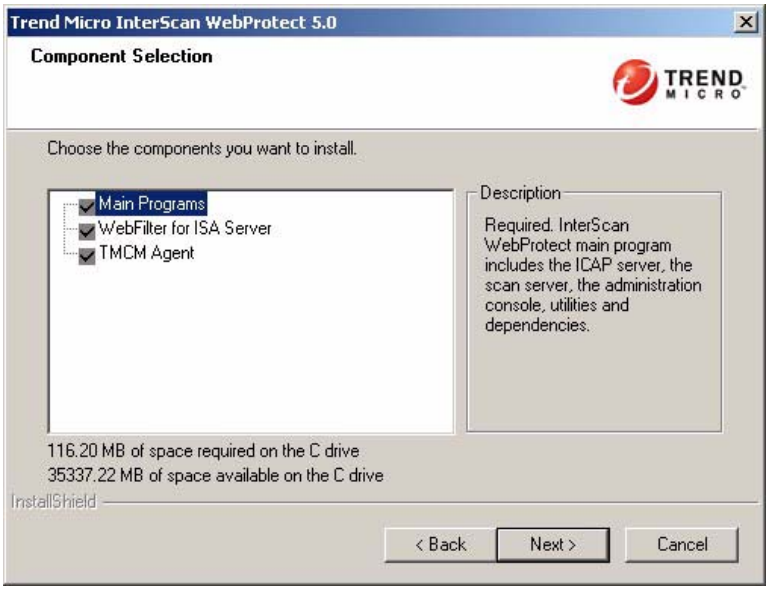


FIGURE 2-2. Select the InterScan WebProtect modules and features to install.

8. In the **Connection Settings** screen, specify how you access the Internet to activate and update the software. If Internet connections pass through a proxy server, enable **Use a proxy server to connect to Internet**, and then type the

address and port number of the proxy server. If the proxy server requires authentication, enter the **User name** and **Password**.

FIGURE 2-3. Enter proxy server (if used)) details to download pattern and program updates.

9. Next, the **Product Activation** screen displays. The Registration Keys that came with your InterScan WebProtect purchase are exchanged for Activation Codes during product registration. The Activation Codes are used to unlock full, that is, non-evaluation, versions of the InterScan WebProtect modules. Click the **Register Online** button to visit Trend Micro's online registration Web site to

register InterScan WebProtect and obtain Activation Codes. Once you have Activation Codes, enter them into appropriate fields

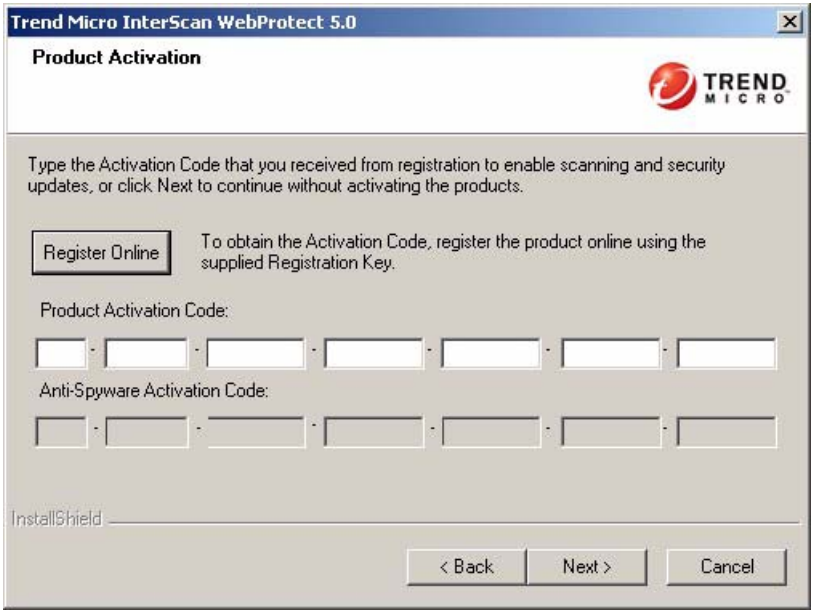


FIGURE 2-4 Enter Activation Code(s) for selected modules.

If you have the Activation Code(s), type them in the fields provided. Enter Activation Code(s) for the modules that you are installing. Alternatively, you can leave these fields blank to install evaluation versions and activate the installation from the management console after you have completed installation.

Note: Scanning capabilities, along with pattern file and scan engine updates, will be enabled after activation.

10. With customer authorization, Trend Micro collects and consolidates infection data from product installations worldwide. These transmissions contain infection data and no user-specific information is sent. This data is used to generate the Virus Map on the Trend Micro Web site

(`http://www.trendmicro.com/map/`). If you would like to participate in this program, select **Yes**. Click **Next**.

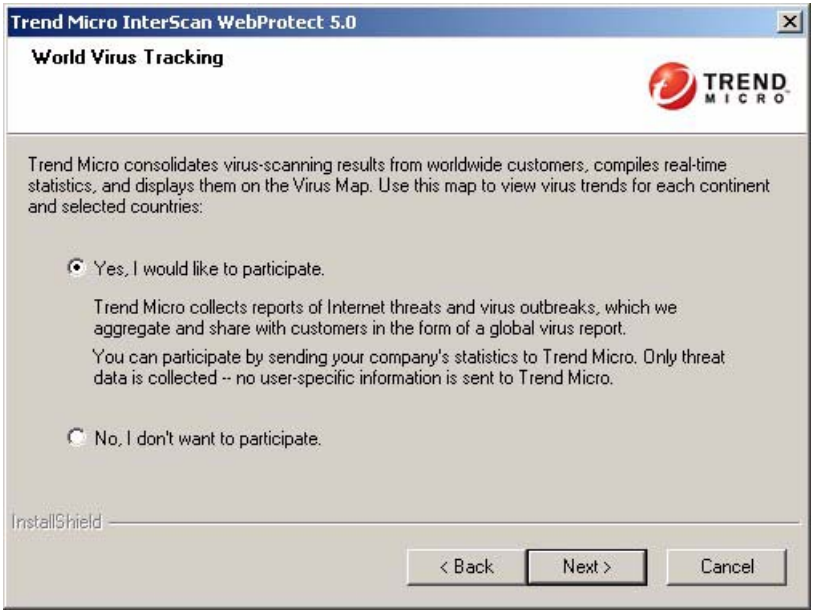


FIGURE 2-5 Select Yes to participate in World Virus Tracking.

11. Enter the password (from 4 to 32 characters) to restrict InterScan WebProtect management console access. Click **Next**.

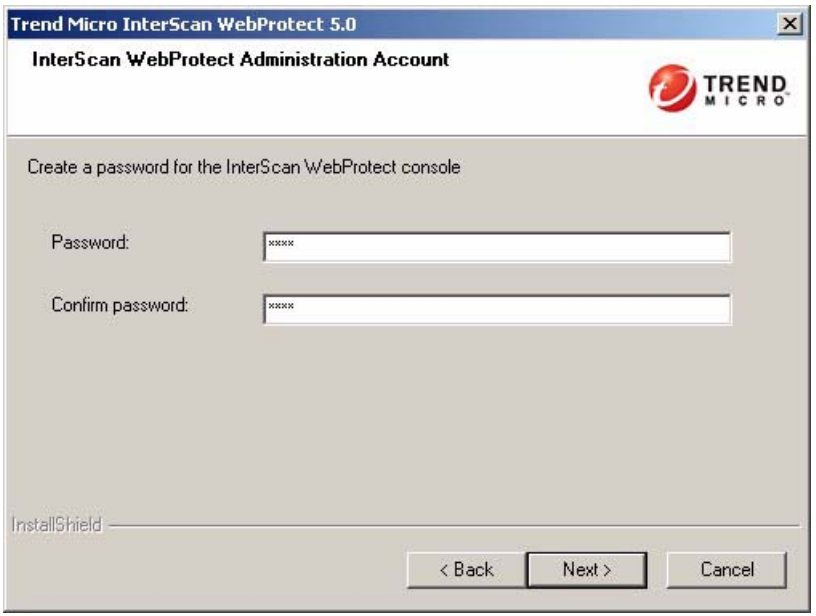


FIGURE 2-6. Review the installation choices.

12. The **Configuration Storage Server Credentials** screen appears (for ISA 2004 or 2006 Enterprise only).

13. Specify a Storage Server with login credentials. The default storage server is "hostname". Otherwise, you must manually configure credentials.

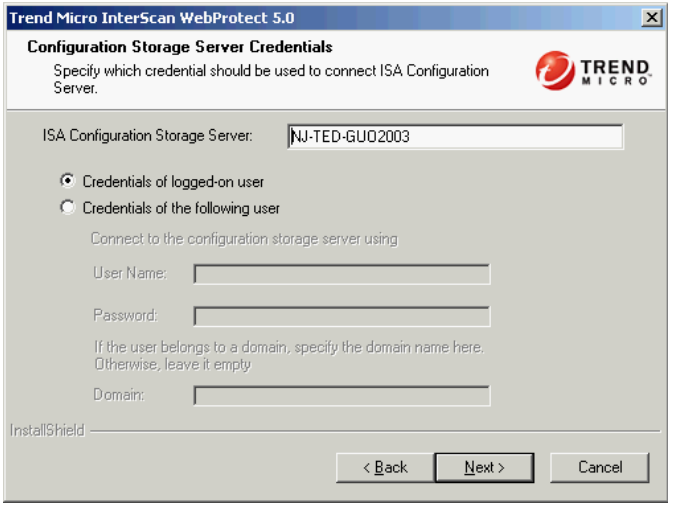


FIGURE 2-7 Does not display during ISA 2004 or 2006 *standard* version installation.

14. Choose the type of database to use to store you scan policy settings, virus, and spyware/grayware logs. The default option is to have the InterScan WebProtect setup program share the Microsoft SQL Server Desktop Engine (MSDE) with ISA. If you want to use an existing Microsoft SQL Server database, check **Other**, choose the **Database** and select the type of authentication. Click **Next**.

Note: If you plan to configure ISWP to use a remote database, you need to update the ISA policy *before* installation. See *ISA Policy Rule 1. Allowing ISWP to Access a Remote Database Server* on page 2-23 for details.

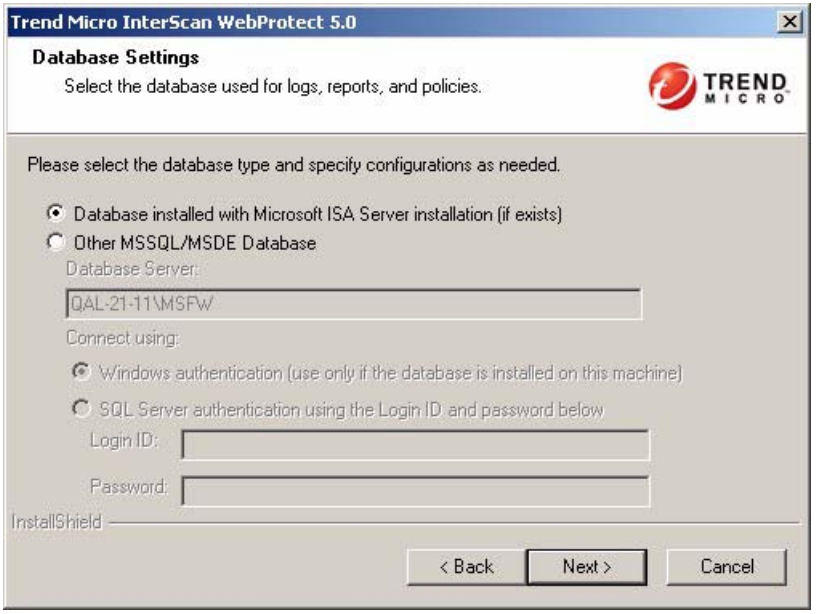


FIGURE 2-8 Select the type of database and authentication method.

15. If the database already exists at destination specified in the “Database Settings” page, the following page appears (otherwise the page is skipped).

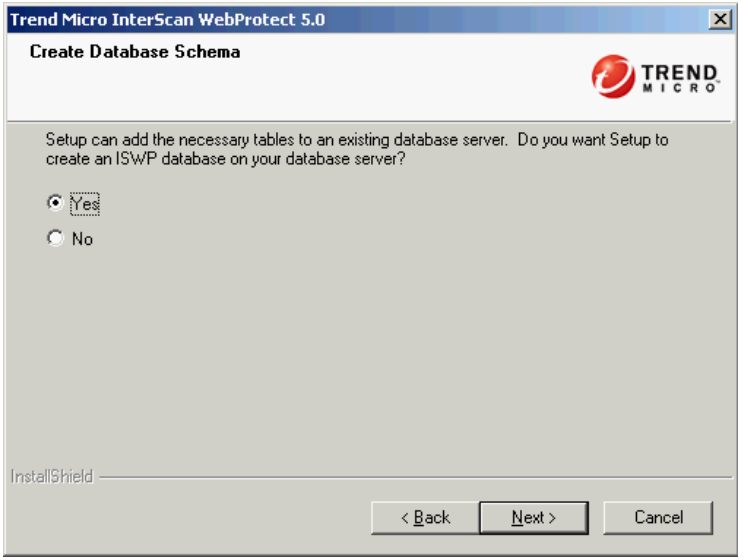


FIGURE 2-9 Create the database schema.

16. InterScan WebProtect can send notifications in response to scanning and updates.
    - For **Email**: Type the email address that should receive email notification messages
    - For **Host**: Type the IP address or domain name of the SMTP server used for sending notifications
    - For **Port:** Type the port number of the SMTP server used for sending notifications. (Generally the port number is 25.)

      The SMTP server that you specify must allow relay from the InterScan WebProtect machine, and later configure your mail server accordingly.

Note: This screen can also be left blank and configured from the ISWP console.

17. Click **Next** to continue.

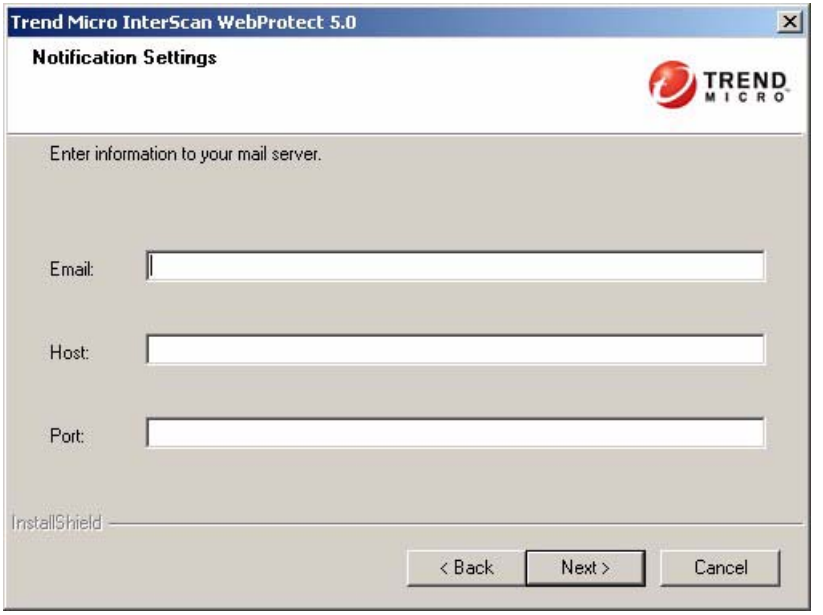


FIGURE 2-10. Enter the email address that receives notifications and information for SMTP server that sends notifications.

18. The **Control Manager Agent Setup** screen appears, as shown in Figure 2-11. Type the host name (or IP address) and the port number of the Control Manager

server, and the protocol that the TMCM server uses to publish the Central Management service: HTTPS or HTTP.

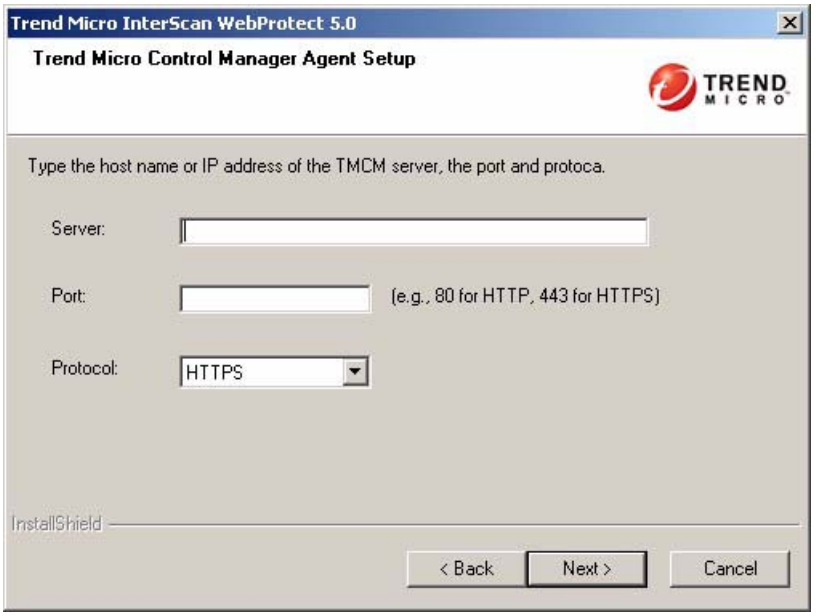


FIGURE 2-11 Enter the Control Manager server's IP address or host.

19. Click **Next** to continue.

20. Setup now has enough information to install InterScan WebProtect. Review the summary of settings in the **Settings Review** screen and then click **Next**.

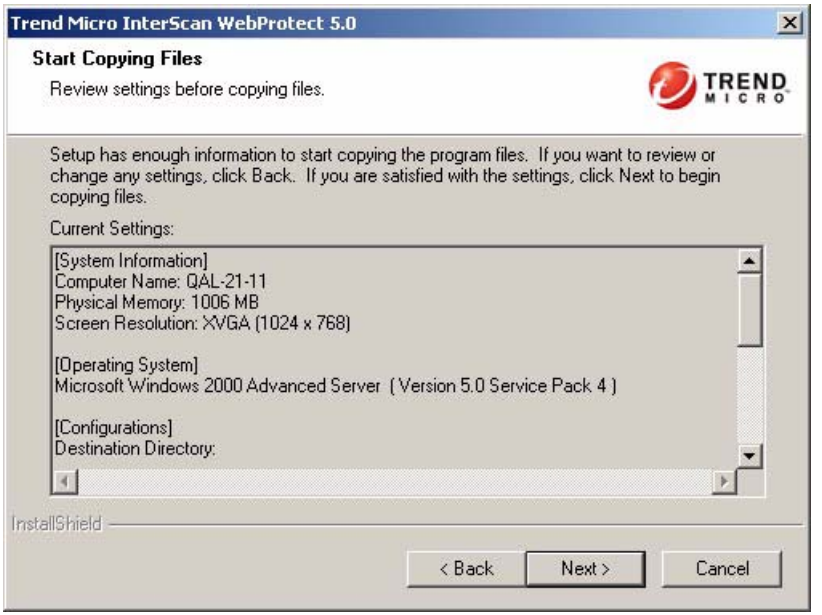


FIGURE 2-12 Review the installation choices.

21. A progress bar and status messages are displayed as the InterScan WebProtect files are copied to the target server.
22. The **InstallShield Wizard Complete** screen displays. To restart the computer, check **Yes** and then click **Finish**.

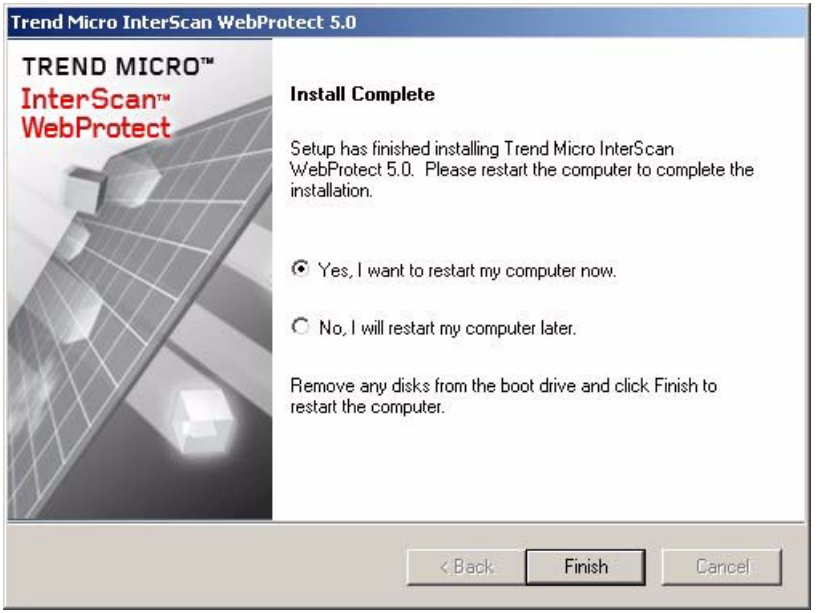


FIGURE 2-13 Restart the computer to finish Setup.

Post Installation

Trend Micro recommends that you register and activate ISWP, check for updates and setup notifications, and other automated program behavior.

You should also test you installation using the EICAR test file. See *EICAR Test File* on page 3-16 for details.

Removing InterScan WebProtect

The uninstallation program can remove InterScan WebProtect installations. It should be run from the Microsoft ISA server with the ISWP you want to remove.

To remove InterScan WebProtect from a local machine:

1. From the Windows taskbar, select **Start > Settings > Control Panel** and double-click **Add/Remove Programs**.
2. Find the **Trend Micro InterScan WebProtect 5.01** entry and click **Change/Remove**.

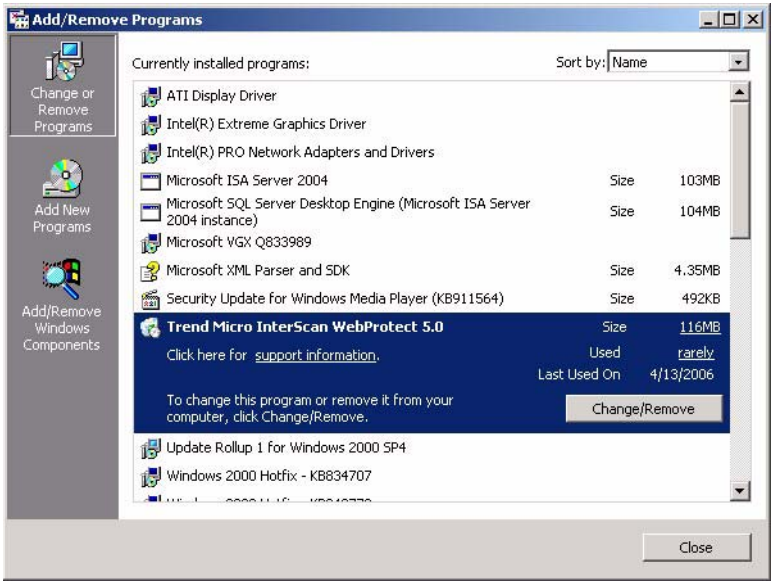


FIGURE 2-14 The Remove Programs screen from Microsoft Windows.

3. In the **Delete Database Schema** screen that appears, choose **Yes** to delete the ISWP schema if no other instances of ISWP are using the same schema.

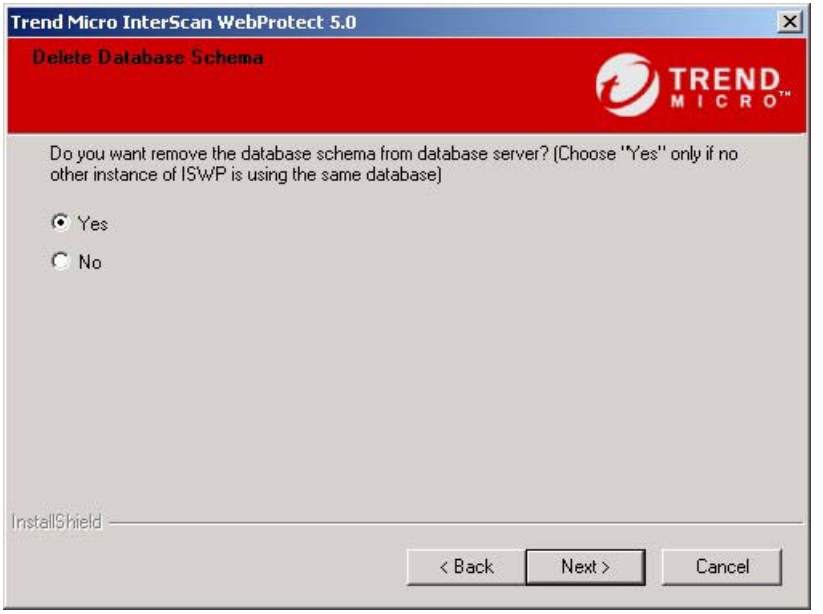


FIGURE 2-15 Choose to remove the ISWP database if no other ISWP servers are sharing it.

4. When removal concludes, the **Maintenance Complete** window displays.

ISA Policies

You may need to modify the ISA policies to allow ISWP to accept and scan traffic. For example:

- Enable HTTP/HTTPS access to Internet or proxy server
- Enable access to MSSQL/MSDE server
- Enable access port 1812 from outside for administration console
- Enable HTTP/HTTPS access to Trend Micro Control Manager server (if installed)

Configuring ISA Policy Rules for ISWP

Although, the ISWP works with the ISA Server 2004 and 2006, the server's default settings deny most ISWP access to the network. You must configure some ISA policy rules to allow communication between ISWP and network resources. Configuring these rules ensures that critical functions, such as ActiveUpdate, can occur.

Use the following sample rules for reference. You can implement other rules as needed.

ISA Policy Rule 1. Allowing ISWP to Access a Remote Database Server

To configure a remote database server for ISWP, you need to enable the access to the remote database server before installation. Generally, the remote database server is located in your internal network, so you can utilize the default system policy rule 16, which allows MSSQL access from local host to internal network.

Rule 16 is disabled by default and must be enabled manually.

Enable rule 16 as show in Figure 2-16.

FIGURE 2-16 Enable rule 16 to allow communication with remote database server.

Note: If you configure ISWP to use MSDE, enabling rule 16 is not necessary.

ISA Policy Rule 2. Allowing ISWP to Access the Trend Micro Web Site for Updates, WVTP, and Virus Information

You need to allow access to the Trend Micro Web site for:

- Updating licenses, pattern files and the scan engine
- Participating in the World Virus Tracking program (WVTP)
- looking up information about detected viruses

Modify the system policy rule 17 (shown in Figure 2-17) to allow access.

FIGURE 2-17 Allow access to the Trend Micro Web site by modifying rule 17.

Rule 17 is enabled in default settings, however you must modify the network object "System Policy Allowed Sites" to allow access to the Trend Micro Web site.

To allow access to the Trend Micro Web site:

1. Open the System Policy Allowed Sites Properties dialog box.
2. Click **Add.**

3. Type `*.trendmicro.com` as shown in Figure 2-18.

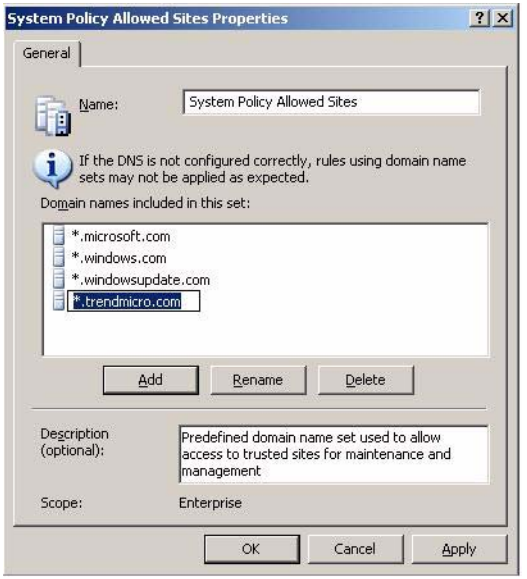


FIGURE 2-18 Add the Trend Micro Web site to the Allowed Sites.

4. Click **Apply**. Click **OK**.

Note: If you use ISA Server 2004 or 2006 Enterprise edition, the System Policy Allowed Sites rule can only be edited at the enterprise level.

ISA Policy Rule 3. Allowing Access to ISWP Web Console from Internal Network and VPN Clients

To configure ISWP remotely from your internal network or through VPN connection, you must:

- Create a new, outbound TCP protocol
- Create a policy rule to allow access through the new protocol

To allow access to ISWP web console from the internal network and VPN clients:

1. Create a new protocol. For example, use ISWP Console.
2. Create the protocol type as TCP and the direction as outbound.
3. Add a port range from 1812 to 1812 (or the port value used by your web console) as shown in Figure 2-19.

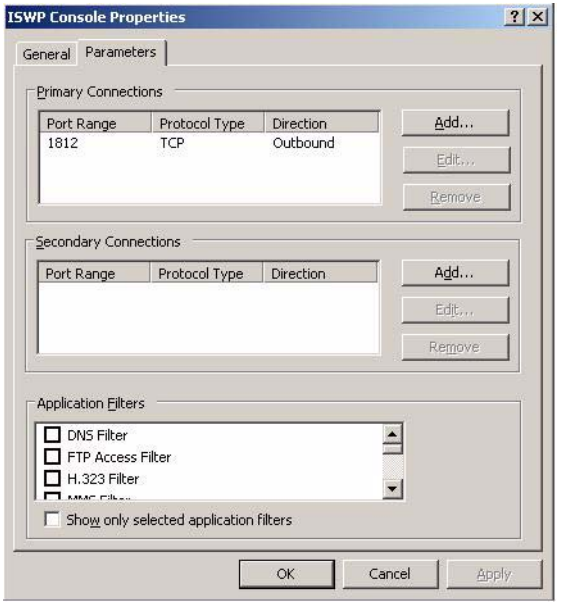


FIGURE 2-19 Create a new, outbound TCP protocol.

4. Create a policy rule that allows access to the local host from the internal network and the VPN client, using the newly created ISWP Console protocol. See the example in Figure 2-20.

FIGURE 2-20 Allow access to the local host from internal network and VPN client.

Note: If you have a TMCM server in your internal network, this rule also allows you to access the ISWP console through the URL Redirect feature of the TMCM.

ISA Policy Rule 4. Allowing ISWP to Communicate with the TMCM Server

If you have TMCM server installed, you must establish communication between the ISWP and the TMCM.

To allow the ISWP and the TMCM to communicate:

1. Go to the TMCM server properties dialog box.
2. Create a new computer set. In this example, it is named TMCM server.
3. Add the IP address of the TMCM server to the new computer set as shown in Figure 2-21.

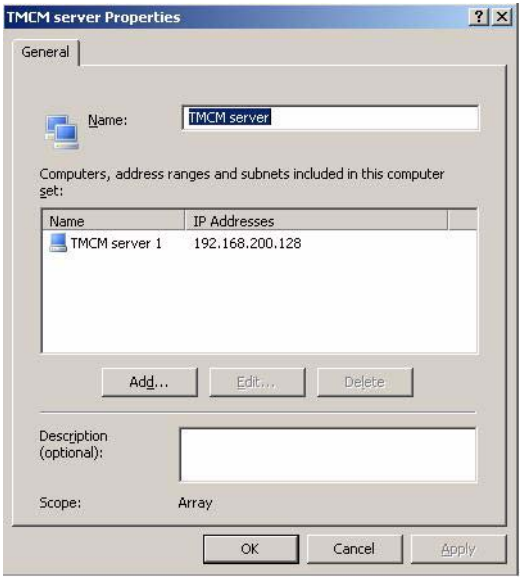


FIGURE 2-21 Add a computer set to the TMCM server properties.

4. Create two policy rules, as shown in Figure 2-22, to allow communication between the ISWP and the TMCM.

FIGURE 2-22 Create policy rules to allow communication between ISWP and TMCM.

Note: When configuring the rule "Allow access ISWP console remotely," the second rule in Figure 2-22 (rule 3) is not needed if the TMCM resides in your internal network.

ISA Policy Rule 5. Allowing the ISWP to Access the SMTP Server

ISWP sends administration email notification using the SMTP server. Usually, the SMTP server is in your internal network. System policy rule 28 allows SMTP access. It is enabled in default settings. (See an example in Figure 2-23.)

FIGURE 2-23 Allow the ISWP to access the SMTP server.

Chapter 3

Getting Up and Running with WebProtect

After installing InterScan WebProtect on the ISA server, Trend Micro recommends that you make certain configuration modifications. This chapter will guide you through the main configurations.

- Opening the ISWP console
- Obtaining an Activation Code and/or Registration Key
- Activating InterScan WebProtect
- Component version information
- Proxy settings for updates
- Manual and scheduled updates
- Update maintenance
- Configuring notifications
- Enabling virus and spyware scanning
- Configuring proxy scan settings
- Setting the database connection
- Testing InterScan WebProtect

Opening the ISWP console

1. Do one of the following:
   - From the computer where you installed InterScan WebProtect, choose **Start > Programs > Trend Micro > InterScan WebProtect > Management Console**.
   - Open a browser window and type the URL of the ISWP management console. You can either enter the URL using the qualified domain name, machine name or IP address. For example,

     `http://domain:port/index.jsp`

     `http://<machinename>:1812/index.jsp`

     `http://123.123.123.12:1812/index.jsp`
2. Type the management console password that you configured during installation and click **Enter**. The management console will open to the **Summary** page.

Obtaining an Activation Code

You automatically receive an evaluation Activation Code if you download ISWP from the Trend Micro Web site. You can use a Registration Key to obtain an Activation Code online at Trend Micro's online registration Web site (http://olr.trendmicro.com)

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solutions CD
- License Certificate (which you obtained after purchasing the product)

Registering and activating InterScan WebProtect entitles you to the following benefits:

- Updates to the virus pattern and spyware pattern files and the scan engine
- Technical support
- Easy access to the license expiration update, registration and license information, and renewal reminders

- Easy renewal of the license and update of your customer profile

Note: After registering InterScan WebProtect, you will receive an Activation Code via email. An Activation Code has 37 characters (including the hyphens) and is written in the following format: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
A Registration Key has 22 characters (including the hyphens) and is written in the following format: xx-xxxx-xxxx-xxxx-xxxx

When the full version expires, security updates will be disabled. When the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the **Product License** screen, you can obtain an Activation Code online, view renewal instructions, and verify the status of the product.

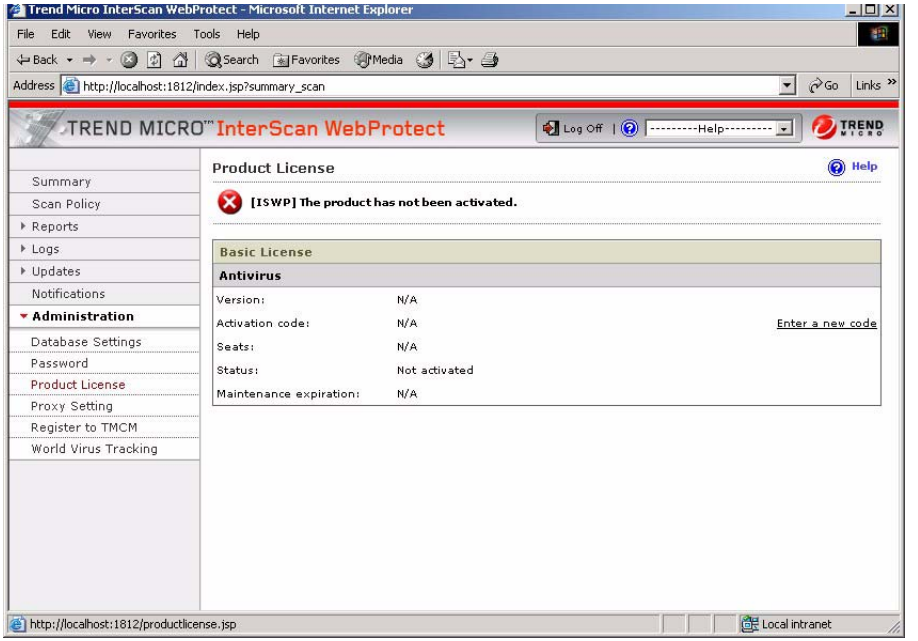


FIGURE 3-1. Review license information in the "Product License" screen.

Activating WebProtect

If you did not activate InterScan WebProtect during installation, activate the modules using the InterScan WebProtect management console after installation.

To activate installed InterScan WebProtect or update the Activation Code:

1. From the main menu, click **Administration > Product License**.
2. The **Product License** screen displays license status information for the installed InterScan WebProtect modules.
3. Click the **Enter a new code** link next to the module to activate and type in the Activation Code.

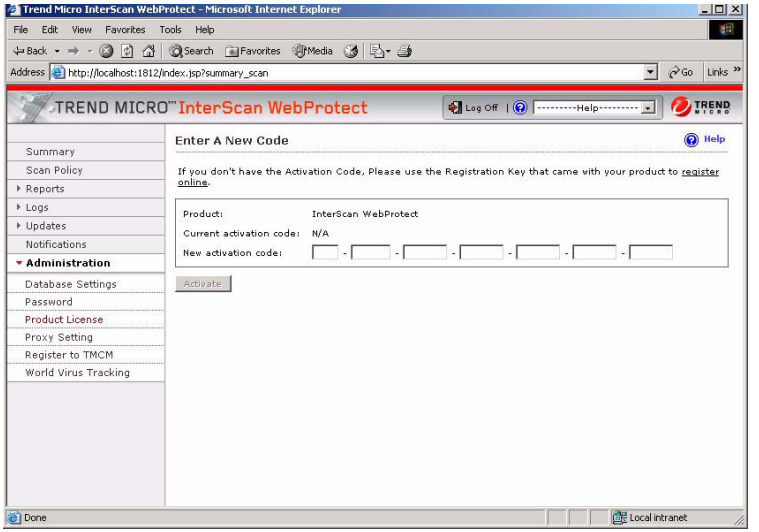


FIGURE 3-2 Enter an Activation Code for the installed module.

4. Click **Activate**.
5. Click **Product License** on the main menu to return to the **Product License** screen and repeat the steps to activate or update another module.

Component Version Information

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

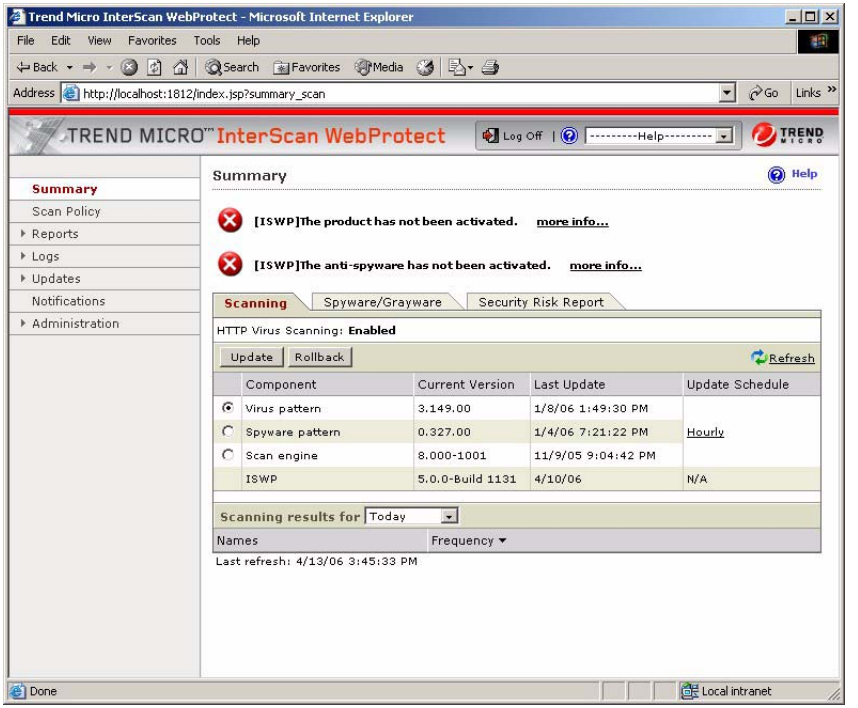


FIGURE 3-3 **Pattern file, scan engine and other component version information displays on the Summary page.**

Proxy Settings for Updates

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

To configure a proxy server for component and license updates:

1. Open the InterScan WebProtect management console and click **Administration > Proxy Setting**.
2. Select **Use an HTTP proxy server for pattern, engine, and license updates**. To supply a proxy server or port number other than the values entered during installation, type the **Proxy server name or IP address** and **Port** number in the fields.
3. If your proxy server requires authentication, type a **User ID** and **Password** in the fields provided. Leave these fields blank if your proxy server does not require you to authenticate.

4. Click **Save**.

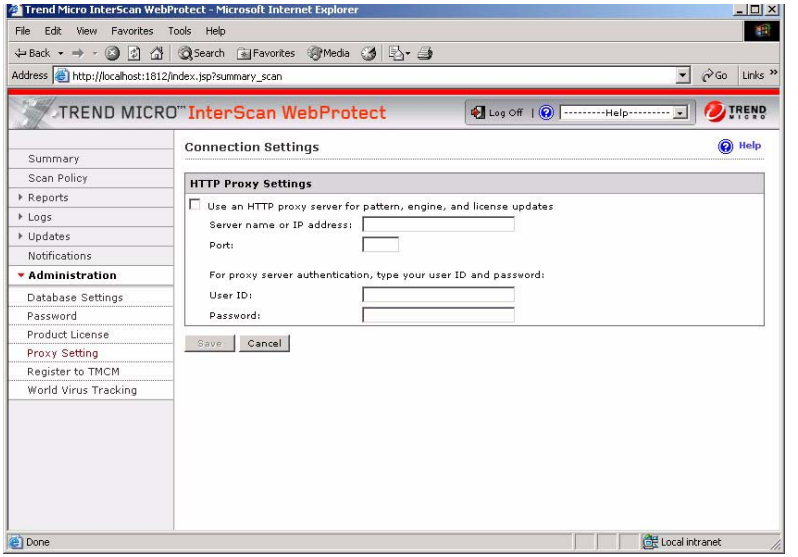


FIGURE 3-4 Configure proxy settings for update and license renewal in the Connection Settings screen.

Updating Program Components

The effectiveness of your InterScan WebProtect installation depends upon using the latest pattern files, and scan engine. Signature-based virus and spyware/grayware scanning works by comparing the binary patterns of scanned files against binary patterns of known risks in the pattern files. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly-identified risks.

New versions of the Trend Micro scan engine are updated as performance is improved and features added to address new risks.

Note: If Internet connections on your network pass through a proxy server and you did not configure your proxy information during install, click **Administration > Proxy Setting** from the main menu and enter your proxy server information.

To update the pattern files and/or scan engine:

1. Click **Summary** on the main menu and make sure the **Scanning** tab is active.
2. For all of the components listed on the **Scanning** tab, select components to update and click **Update**.

Note: If InterScan WebProtect is already using the latest version of the component and no update is available, a message prompts whether you want to force an update. Forcing an update is typically not necessary unless the components on the InterScan WebProtect server are corrupt or otherwise cannot be used.

Manual Updates

To manually update pattern files and/or scan engine:

1. Click **Summary** in the main menu.
2. On the **Scanning** tab of the **Summary** page, select the component to update and click **Update**.

Forced Manual Updates

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

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

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

Scheduled Updates

To schedule automatic pattern file and scan engine updates:

1. Click **Updates > Scheduled** from the main menu.
2. Select the update interval. Options are:
   - Every *x* minutes (select the interval, in minutes between updates)
   - Hourly
   - Daily
   - Weekly

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

---

3. Select a **Start time** for the update schedule to take effect.

4. Click **Save**.

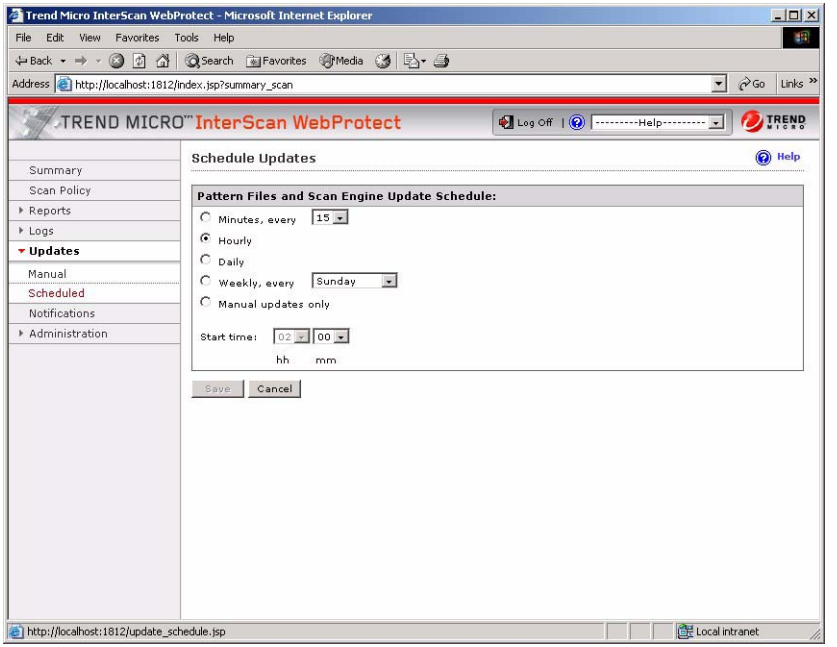


FIGURE 3-5 Configure scheduled updates for the pattern files and the scan engine.

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

Maintaining Updates

The **Scanning** tab of the **Summary** page in the InterScan WebProtect management console displays the version of the component in use, plus the time and date of the last update. Check the Summary page to verify that a manual or scheduled update has completed successfully.

InterScan WebProtect can issue notifications to proactively inform an administrator about the status of a pattern file or scan engine update.

Rolling Back an Update

InterScan WebProtect checks the program directory and uses the latest pattern file and engine library file (`vsapi32.dll`) to scan inbound/outbound traffic. It can distinguish the latest pattern file by its file extension; for example, `lpt$vpn.401` is newer than `lpt$vpn.400`.

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

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

1. Click **Summary** in the main menu. The **Scanning** tab displays by default.
2. Select the component to roll back and click **Rollback**. After the rollback, you can find the current version and date of the last update on the **Scanning** tab of the **Summary** screen.

Deleting Old Pattern Files

After updating the pattern file, InterScan WebProtect keeps old pattern files on the server so they are available to roll back. The number of pattern files kept on the server is controlled by the **Number of pattern files to keep** setting on the **Updates > Connection Settings** page.

If you need to manually delete pattern files, they can be found in the following directory:

```
<install directory>\activeupdate
```

Configuring Notifications

The InterScan WebProtect setup program prompts for an email address and SMTP server to use for update and security event notifications.

To review and modify your notification settings:

1. Click **Notifications** on the main menu.
2. Verify that the notification settings for each security and update event match the requirements of your environment.
3. Click **Send notification to...** to view and modify the email address or SMTP server to use for notifications.
4. Click Save.

Enabling Virus and Spyware Scanning

After installing InterScan WebProtect and rebooting the server, the HTTP scanning is enabled by default.

To enable or disable HTTP scanning:

1. From the main ISWP menu, click **Scan Policy**.
2. Click **Enable Virus Scanning** at the top of the screen.
3. Click the **Spyware/Grayware Scan Rule** tab to make that screen active.

4. Click **Enable Spyware/Grayware Scanning** at the top of the screen.

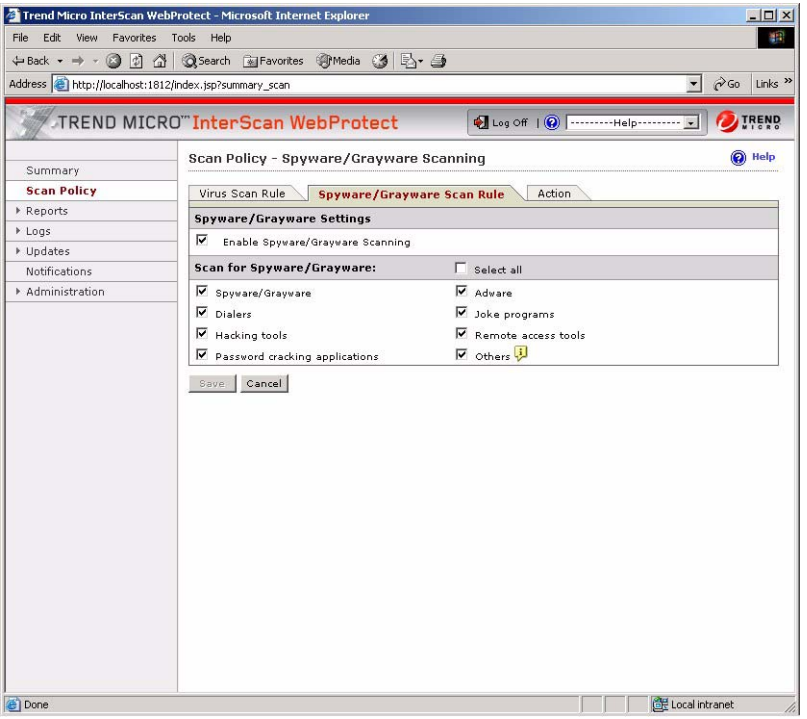


FIGURE 3-6 Enable Spyware/Grayware scanning.

Configuring Proxy Settings

Proxy settings entered during installation of ISWP can be changed in the **Administration > Proxy Setting > Connection Settings** page.

To modify your proxy settings:

1. Click **Administration > Proxy Setting** from the main menu.

2. On the **Connection Settings** page, review the existing configurations and modify if necessary.

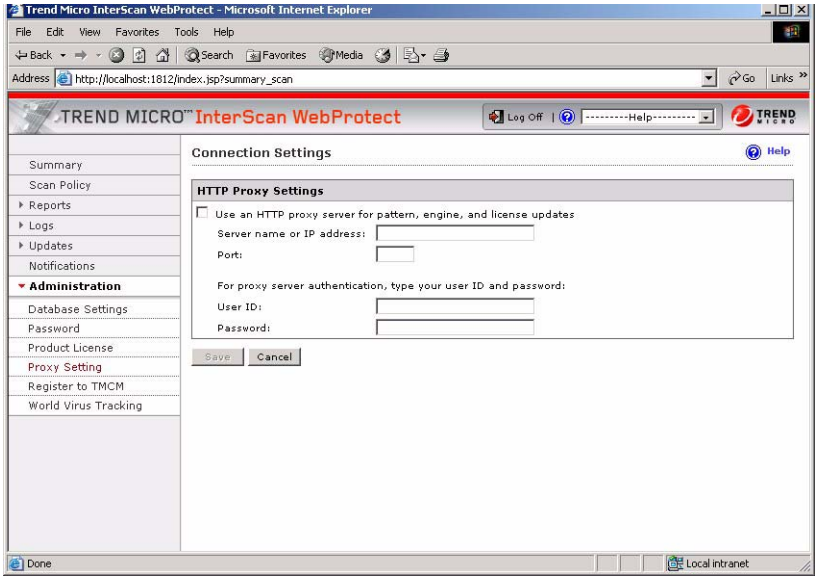


FIGURE 3-7. Enable the proxy settings if there is a proxy server between ISWP and the Internet.

Setting the Database Connection

Make sure that you set up your database appropriately under the **Database Connection Settings** section (**Administration > Database Settings**). When you are setting up a database for multiple ISWP server configurations, specify the same database for all InterScan WebProtect servers. Whether you are using MSDE or SQL Server for the database, the schema (that is, table definitions, stored procedures, and so on) used by ISWP is initialized during installation.

To configure the database connection settings (for a remote database):

1. Open the ISWP management console and click **Administration > Database Settings**

2. Under **Database Connection Settings**, the default identification method uses the ISA server's Windows authentication to access the database used by ISWP. If you are using a remote SQL server as the database, for example to support multiple instances of ISWP installed on an ISA array, provide the log in credentials.
   - **ODBC data source name**: the ODBC data source configured on the ISA server, representing either the default ISA data base, or remote SQL server.
   - **Login ID**: Admin-level credentials for the remote database and server; ISWP will read and write data, and may create/modify/delete the table schema.
   - **Password**: password for the admin-level account on the server.
3. Click **Save**.

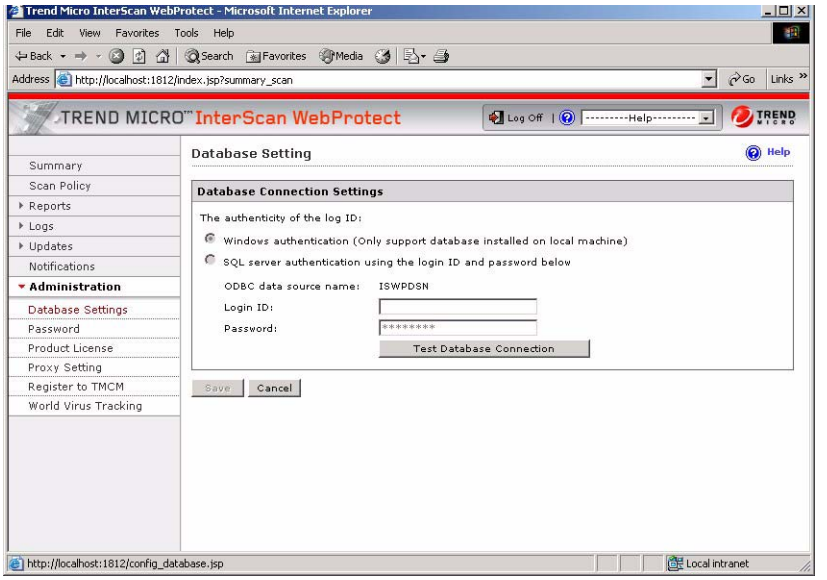


FIGURE 3-8 To verify that the database connection is working, click Test Database Connection.

Testing InterScan WebProtect

After installing InterScan WebProtect, test the following to verify that the program is working properly. Using the EICAR test virus file, there are two types of test to perform:

- Upload scanning
- Download scanning

EICAR Test File

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus software. This script is an inert text file. The binary pattern is included in the virus pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

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

Obtaining the EICAR Test File

Download the EICAR test virus from the following URLs:

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

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

Alternatively, you can create your own EICAR test virus by typing or copying the following into a text file, and then naming the file “eicar.com”:

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

Note: Flush the cache in the cache server and local browser before testing. If either cache contains a copy of the test virus, it is possible that an attempt to download the file would only retrieve the file from the cache, rather than obtaining it from the Internet, thus InterScan WebProtect would not detect the file.

Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

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

FIGURE 3-9. This warning screen shows the detection of an EICAR test virus.

Upload Scanning

Trend Micro recommends that you test virus scanning of Web-based mail attachments.

To test virus scanning of Web-based mail attachments:

1. Open the InterScan WebProtect console and **Scan Policy** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus from the following page:

   http://www.eicar.org/anti_virus_test_file.htm
3. Save the test virus on your local machine.
4. Re-open the InterScan WebProtect console, under **Scan Policy** in the main menu, select **Enable virus scanning**, and then click **Save**.

5. Send a message with one of the test viruses as an attachment by using any Internet mail service. A message similar to the following should display in your browser.

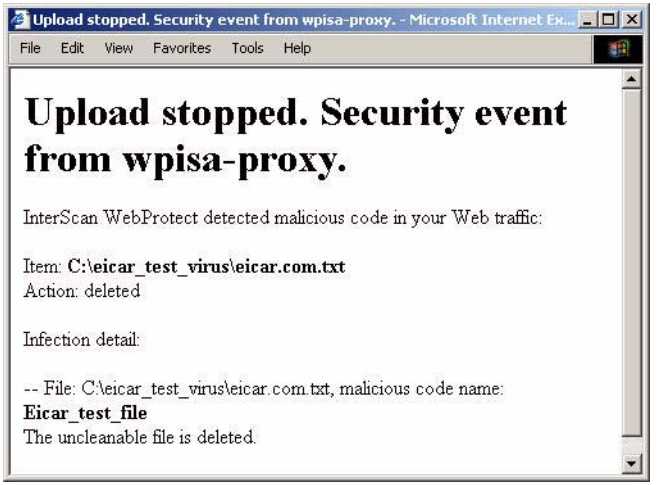


FIGURE 3-10. This warning screen shows the detection of the EICAR test virus in an Web-basedmail attachment.

Chapter 4

Configuring InterScan WebProtect

After installing InterScan WebProtect on the ISA server, you can configure it to begin real-time scanning of file transfers via HTTP. This chapter will guide you through the main configurations.

Topics included are:

- Sending Infection Data to the World Virus Tracking Center
- Changing the Management Console Password
- HTTP Scanning Performance Considerations
- HTTP Virus Scanning Rules
- Spyware and Grayware Scanning Rules
- Setting the Scan Action for Viruses
- Introduction to Notifications
- Email Notification Settings
- Notification Tokens/Parameters
- Configuring Notifications
- Pattern and Scan Engine Updates

Sending Infection Data to the World Virus Tracking Center

Trend Micro's World Virus Tracking Center provides real-time data about virus infections worldwide. After combining real-time infection data from Trend Micro product installations, Trend Micro publishes this data to the Virus Map on Trend Micro's Web site:

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

By choosing to send your InterScan WebProtect infection data to the World Virus Tracking Center, you will be contributing to Trend Micro's efforts to provide real-time infection information to its customers and the general public.

With our customers authorization, Trend Micro products send the following information to the World Virus Tracking Center via encrypted HTTPS:

- virus name
- the number of times the virus was found in the file
- the number of infected machines (always **1** for a gateway product like ISWP)
- a fake sender ID
- a fake machine ID
- the virus pattern file number in use when the virus was detected
- the ISWP product code
- the customer's country code

To send infection data to Trend Micro's World Virus Tracking Center:

1. Choose **Administration > World Virus Tracking** from the main menu.
2. Select **Yes** and click **Save**.

You can stop sending infection data to Trend Micro at any time by returning to the **World Virus Tracking Program** configuration page and selecting **No**.

Changing the Management Console Password

The management console password is the primary means to protect your InterScan WebProtect server from unauthorized changes. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess.

The following tips will help you design a safe password:

- Include both letters and numbers in your password
- Avoid words found in any dictionary, of any language
- Intentionally misspell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

To change the console password:

1. Open the ISWP console and click **Administration > Password** in the main menu.
2. Type your current password in the **Old password** field, and then type and confirm the new password.

3. Click **Save**.

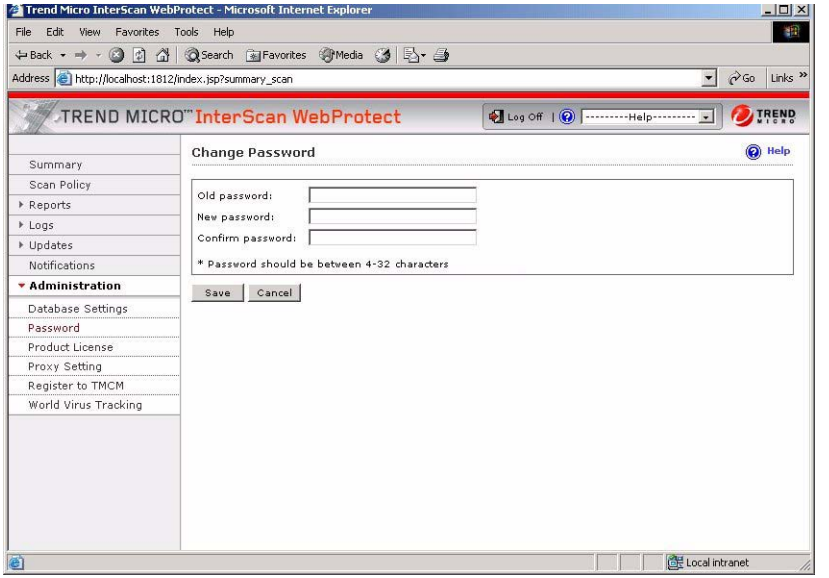


FIGURE 4-1. Passwords are case-sensitive and can contain from 4-32 characters.

HTTP Scanning Performance Considerations

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

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

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

HTTP Virus Scanning Rules

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

Scan Priorities

InterScan WebProtect scans according to the following priority:

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

Specifying File Types to Block

You can identify the types of files to block for security, monitoring or performance purposes. Blocked files are not received by the requesting client, nor are they scanned—requests to retrieve a blocked file type are not executed. You have the

option of blocking file types such as Java applets, executables, Microsoft Office documents, audio/video files, images or other files types that you configure.

To specify which file types to block:

1. While adding or editing a policy, under **Block These File Types**, select the file types to block.
2. In the **Other file types** field, type the other file types to block, using a space to delimit multiple entries.

Specifying File Types to Scan

About IntelliScan

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

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

True File Type

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

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

For example, .gif and .jpg files make up a large volume of all Web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. So, does this mean they are safe? Not entirely. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan engine and onto the network. The file could not be run until it was renamed, but IntelliScan would not stop the code from entering the network.

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

To select which file types to scan:

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

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

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

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

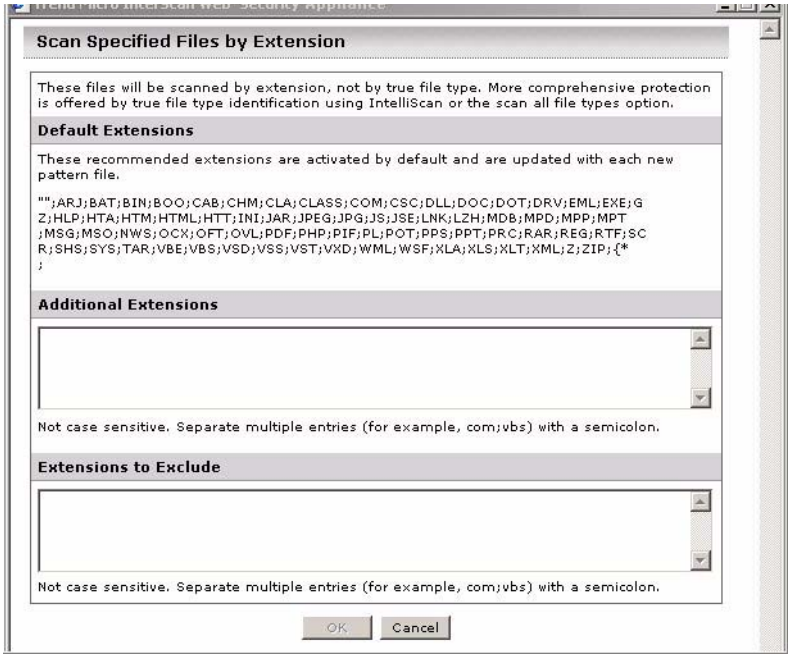


FIGURE 4-2. The recommended extensions to scan are updated with each new pattern file.

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

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

About MIME

When configured to skip scanning a file due to its MIME content-type, InterScan WebProtect will attempt to determine the file's true file type and match it to the claimed MIME type before skipping it. If the file's true file type maps to a different MIME type than indicated in the Content-type header attached to the transaction, the file will be scanned. Unfortunately, there is not always a clear mapping between file types and MIME types. If the file is smaller than 4KB, or ISWP cannot map the true file type to a MIME type, it will be skipped according to the Content-type header as configured.

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

Configuring Compressed File Scanning Limits

Compressed file scanning limits can be configured from the **Scan Policy** screen. InterScan WebProtect opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. InterScan WebProtect decompresses the files according to the configurable limits

(decompressed file count, size of the decompressed file, number of layers of compression, and the size of a decompressed is x" times the size of the compressed file).

To configure the compressed file scanning limits:

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

- **Block all compressed files**: All requests to download compressed files will not be fulfilled.
- **Block compressed files if...**: Requests to download compressed files that exceed the configured criteria will not be fulfilled. Type values for the following parameters:
  - Decompressed file count exceeds (default is 10000)
  - Size of a decompressed file exceeds (default is 2048MB)
  - Number of layers of compression exceeds (range is 1-20; default is 10)
  - Size of decompressed files is "x" times the size of compressed file (range is 1-200; default is 10)

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

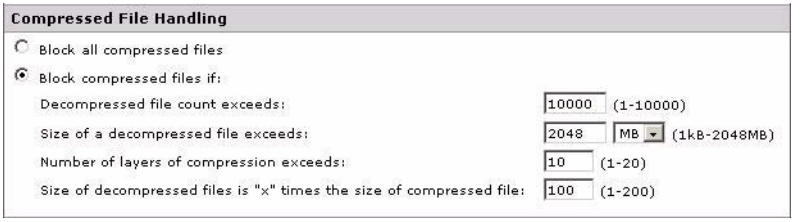


FIGURE 4-3 "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the ISWP server.

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

Handling Large Files

For larger files, a trade-off must be made between the user's experience and expectations, and maintaining security. The nature of virus scanning requires

doubling the download time (that is, the time transferring the entire file to InterScan WebProtect, scanning the file, and then transferring the entire file to the client) for large files. In some environments, the doubling of download time may not be acceptable. There are other factors such as network speed, and server capability that must be considered. If the file is not big enough to trigger large-file handling, the file will be scanned as a normal file.

When downloading a large file, the time to download the file and scan it for viruses may be long enough to cause the browser to time out. The size of file that you should consider "large" varies, depending on the hardware where InterScan WebProtect is installed, the mix of file types in the particular environment, and so on. Trend Micro recommends that files larger than 64KB (default value) be considered large and files larger than 2048MB do not have to be scanned; however, these values might vary depending on your network speed, server capability, and other factors.

Large file handling can be set from the **Scan Policy** screen.

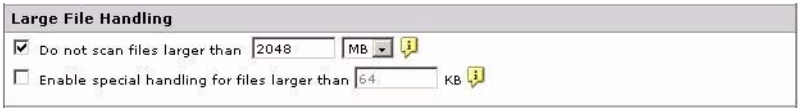


FIGURE 4-4 Configure how WebProtect handles large files.

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

To disable scanning large files:

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

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

To use large file handling for HTTP scanning:

1. Under the **Large File Handling** section, select **Enable special handling**, and then type the file size in KB to be considered a large file. The default value is 64KB.

2. Click **Save**.

Consider configuring large file handling if your users complain of browser timeouts when trying to download files.

Quarantined File Handling

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

```
C:\Program Files\Trend Micro\InterScan WebProtect\quarantine
```

When you have completed configuring the HTTP virus scanning rules on the **Scan policy** screen, move to the spyware/grayware scanning rules.

Spyware and Grayware Scanning Rules

In addition to computer viruses, the InterScan WebProtect pattern files include signatures for many other potential risks. These additional risks are not viruses since they do not replicate and spread. However, they can perform unwanted or unexpected actions, such as collecting and transmitting personal information without the user's

explicit knowledge, displaying pop-up windows, or changing the browser's home page.

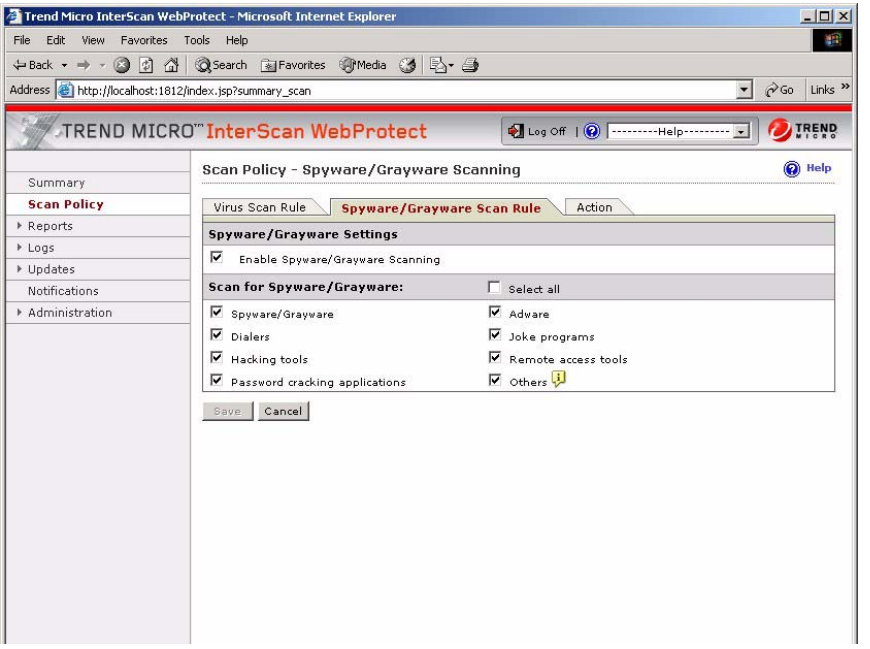


FIGURE 4-5. Select the threats for which WebProtect should scan.

Setting the Scan Action for Viruses

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

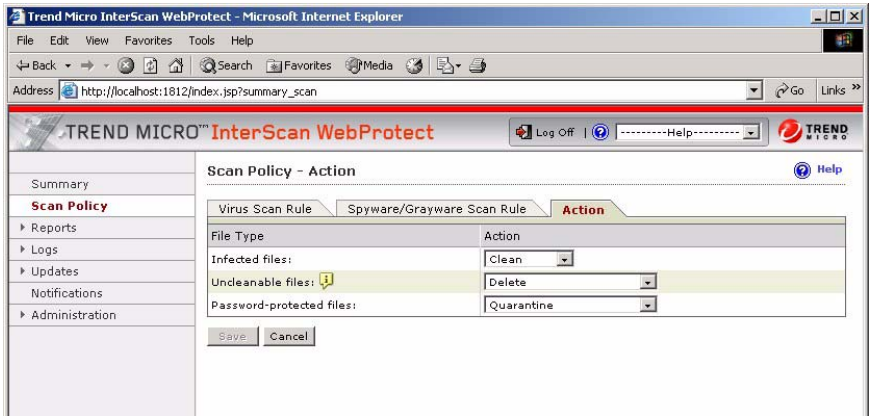


FIGURE 4-6. Choose the action you want WebProtect to take.

Scan Actions

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

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

  `C:\Program Files\Trend Micro\InterScan WebProtect\Quarantine`

  The requesting client will not receive the file. This scan action can be applied to all three of the scan events. You can optionally choose to encrypt files before sending them to the quarantine directory
- Choose **Clean** to have InterScan WebProtect automatically clean and process infected files. The requesting client will receive the cleaned file if it is cleanable, otherwise the uncleanable action is taken.

- Choose **Pass** to send the file to the requesting user. This action can be applied to the *Uncleanable files* and *Password-protected files*.

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

Scan Events

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

- **Infected files**: Files determined to be infected with a virus or other malicious code. Available actions are **Delete**, **Quarantine** or **Clean** (recommended and default action).
- **Uncleanable files**: Depending on the type of virus or malicious code infecting a file, the scan engine may not be able to clean some files. Available actions are **Delete** (recommended and default action), **Quarantine** and **Pass**.
- **Password-protected files**: Files that cannot be scanned because they are either password-protected or encrypted. The infection status of these types of files cannot be determined. Available actions are Delete, **Quarantine** (recommended and default action) and **Pass**.

Introduction to Notifications

Notifications can be issued in response to scanning, blocking and program update events. There are two types of notifications—administrator notifications and user notifications:

- **Administrator notifications** provide information about HTTP scanning, as well as pattern file and scan engine updates. InterScan WebProtect sends administrator notifications via email to addresses that you configure in **Email Settings**.
- **User notifications** occur in real-time via Web browser. You can create a simple message from the ISWP Notifications page and/or append a custom message to the ISWP default, for example to add a global disclaimer.

The messages presented in both the administrator and user notifications are configurable and can include “tokens”, or variables, to customize notification messages with information about the event. In addition, user notification messages

support HTML tags to customize the appearance of the message and provide links to other resources, such as security policy documents hosted on your intranet.

Email Notification Settings

InterScan WebProtect sends administrator notifications to email addresses that you specify. The administrator enters email settings when installing InterScan WebProtect and running the setup program, but email settings can also be modified post-installation in the management console's **Email Settings** screen.

To configure email settings for administrator notifications:

1. Click **Notifications** in the main menu.
2. In the **Notifications** screen, click the **Settings** tab.
3. Type the email address to send notifications, the sender's email address, the SMTP server, the SMTP server port and the time interval between checking the mail queue.

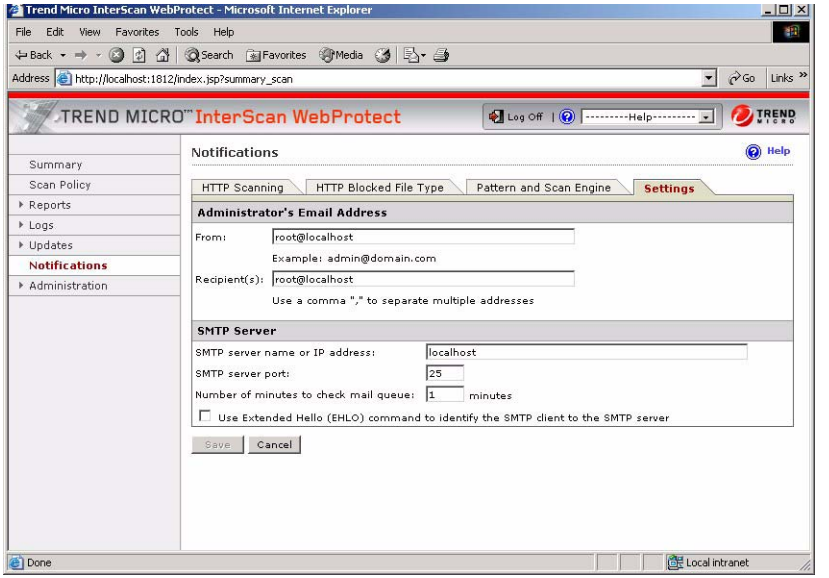


FIGURE 4-7 Configure administrator notification settings.

4. If your mail server requires ESMTP, enable **Use Extended Hello (EHLO)** for InterScan WebProtect to initial SMTP sessions using the EHLO command.
5. Click **Save**.

Notification Tokens/Parameters

To make notifications more meaningful, InterScan WebProtect can use tokens (or variables) as informational placeholders in a notification. When an event occurs, InterScan WebProtect dynamically substitutes the specific information in place of the variable, providing detailed information about that specific event.

For example, you could create a generic notification as follows:

```
A virus was detected in HTTP traffic.
```

This notification lets you know there is a problem, but does not provide any details.

Instead, you could configure the notification using variables as follows:

```
ISWP detected an Internet threat in a user's HTTP traffic. Threat
name: %V[Virus or Trojan name], Infected URL: %U[URL/URI],
Filename: %F[file name], Action taken: %A[Action], Datetime:
%Y[date and time].
```

The notification might read as follows:

```
ISWP detected an Internet threat in a user's HTTP traffic. Threat
name: TROJ_VIPERIK.A, Infected URL: http://www.example.com,
Filename: game.exe, Action taken: deleted, Datetime: May 24, 2006,
12:01 a.m.
```

With this information, administrators can obtain more security information. The notification in this example uses five variables: %V, %U, %F, %A and %Y.

The following table contains a list of tokens that can be used in notification messages and pages.

TABLE 4-1 Description of variables

Variable	Variable Meaning	How the Variable is Used
%F	file name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm

Variable	Variable Meaning	How the Variable is Used
%V	malware name (virus, Trojan, etc.)	The name of the risk detected
%A	action taken	The action taken by InterScan WebProtect
%M	moved to location	The quarantine folder location where a file was moved
%H	host name	The InterScan WebProtect host name where the event was triggered
%Y	date and time	The date and time of the triggering event
%U	URL/URI	The Web site address involved in the triggering event
%R	transfer direction	The transfer direction of the triggering event
%X	reason for blocking	The reason for blocking in the triggering event

Configuring Notifications

To configure a notification, select the types of events that will issue the notification and edit the email and browser notification messages.

Using HTML Tags in User Notifications

You can use HTML tags to format user notification messages.

HTTP Scanning

When InterScan WebProtect detects malicious code in a file requested by a client, it will issue an administrator notification via email and a user notification in the requesting client's browser.

To configure HTTP scanning notifications:

1. Click **Notifications** and then click **HTTP Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Spyware/Grayware**).

3. If you do not want to use the default notification message, highlight the default text and type your own version.

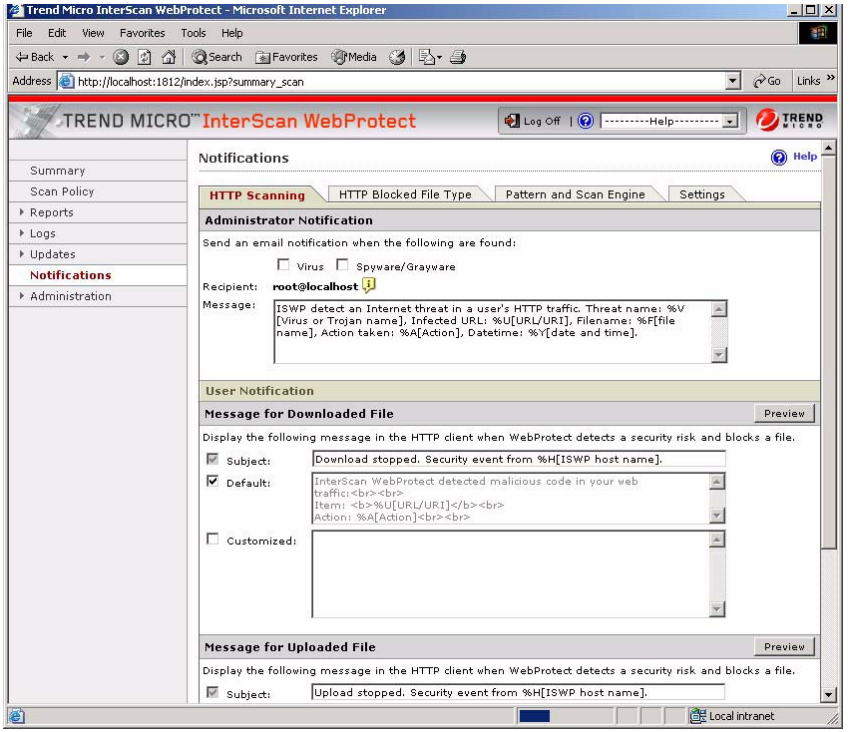


FIGURE 4-8. Configure HTTP scanning notifications.

4. Type the **Subject** to display in the browser. The default is *ISWP Security Event*.
5. For **Message for downloaded file** and **Message for uploaded file**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message.
6. Verify the notifications display correctly by clicking **Preview**.
7. Click **Save**.

HTTP Blocked File Type

When InterScan WebProtect blocks a file, it sends an administrator notification via email, and a user notification message is displayed in the requesting client's browser.

To configure HTTP file blocking notifications:

1. Click **Notifications** and then click **HTTP Blocked File Type**.
2. Under **Administrator Notification**, select **Send a message when the blocked file type is accessed**.
3. If you do not want to use the default notification message, highlight the default text and type your own version.

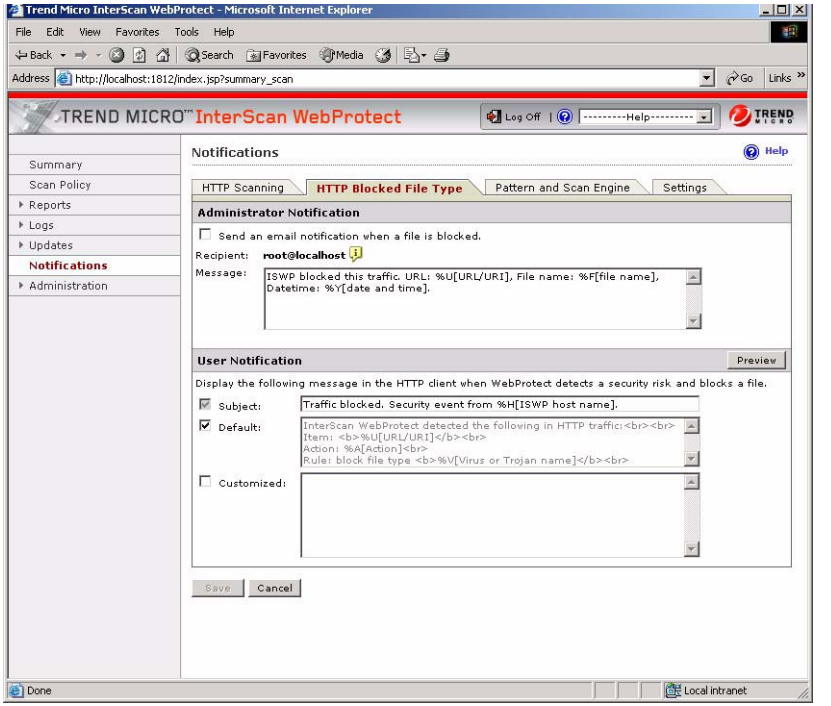


FIGURE 4-9 Configure HTTP blocked file notifications.

4. For **Subject**, type the header line to display in the browser. The default headline is *ISWP Security Event (%H)*.

5. For the **Message**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message.
6. Verify the notifications by clicking **Preview**.
7. Click **Save**.

Pattern And Scan Engine Updates

InterScan WebProtect can issue administrator notifications in response to attempts to update the virus or spyware pattern files.

To enable pattern update notifications:

1. Click **Notifications** from the main menu, then click **Pattern and Scan Engine**.

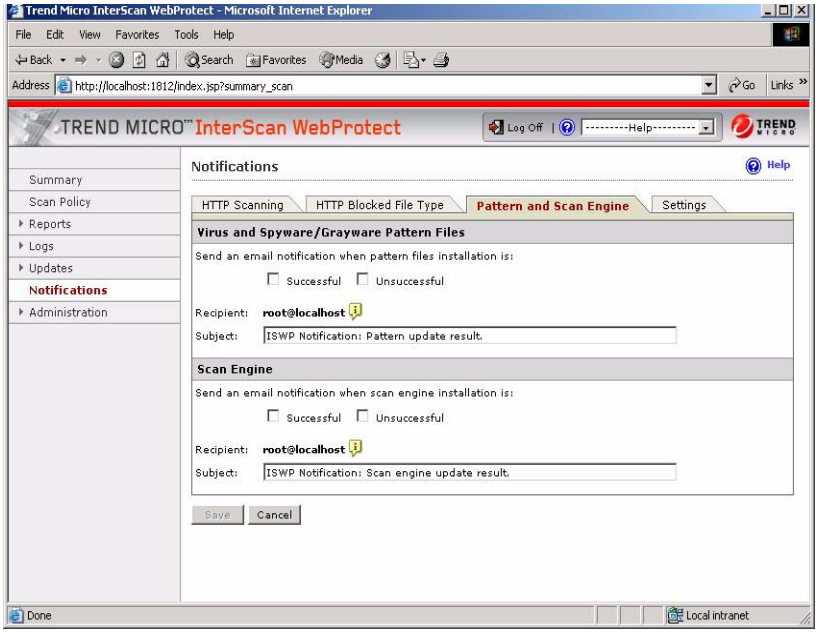


FIGURE 4-10 Configure pattern and scan engine update notifications.

2. For the pattern update attempts:

a. Select the update events that will trigger a notification. You can configure notifications for **Successful** or **Unsuccessful** update attempts.

b. Type a **Subject** for the notification message

3. Click **Save**.

Chapter 5

Logs and Reports

This chapter describes how you can get timely information about their gateway security via ISWP reports, logs and notifications.

Topics in this chapter include:

- Report Overview
  - Real-time reports
  - Scheduled reports
  - Settings
- Querying and viewing logs
- Log settings

Overview

InterScan WebProtect can generate reports about virus and malicious code detections. You can use this timely information about InterScan WebProtect program events to help optimize program settings and fine tune your organization's security policies.

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

Report Types

InterScan WebProtect uses data from reporting logs to generate reports. You can configure InterScan WebProtect to write reporting log data to both the database and text logs, or only to the database. Configure reporting log options in the InterScan WebProtect management console under **Logs > Settings**. Text logs provide backward compatibility with previous versions of InterScan WebProtect and allow further analysis of log data through custom scripts or other third-party applications. You can also use them to validate the completeness and accuracy of the data logged to the database.

Report Settings

When generating a real-time report or setting up scheduled reports, you need to specify the following information to query the reporting logs:

Report Type (Consolidated or Individual)

InterScan WebProtect can generate consolidated reports, which contain all possible reports, or just those individual reports that you select.

Options

InterScan WebProtect can present program information in either bar or line charts.

Additional Report Settings

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

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

- Send a notification email message when the scheduled report runs.
- Run the reports at a specific time and day.
- "Enable" the report to run at the scheduled time.

Generating Real-time Reports

InterScan WebProtect allows you to generate reports in real time.

To configure real-time reports:

1. Click **Reports > Real-Time Reports** in the main menu.
2. Under **Time period**, select a time period for the report (either **All Dates**, **Today**, **Last 7 days**, **Last 30 days**).

3. Click **Range** to generate a report in a given time range, and then select the **From** and **To** dates.

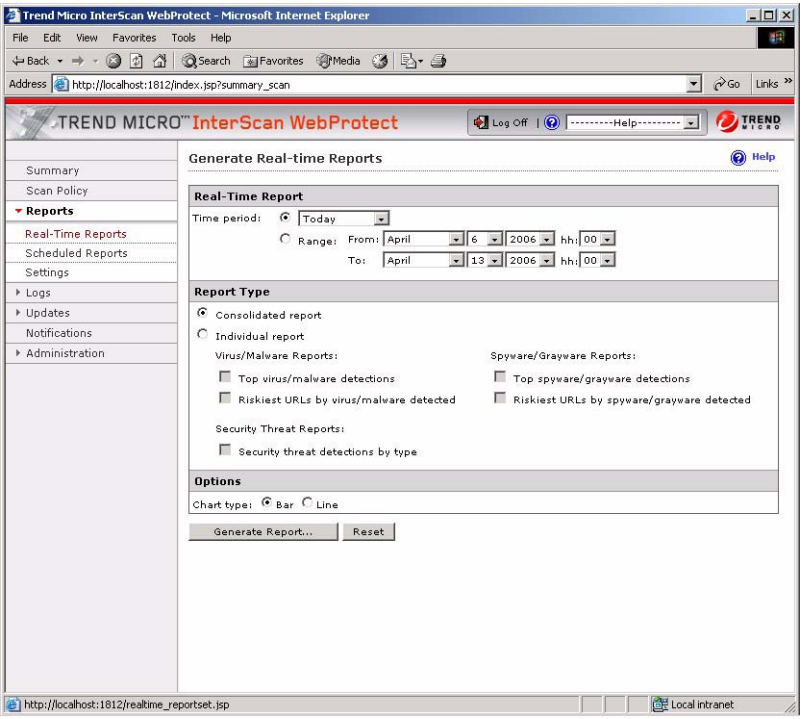


FIGURE 5-1 Generate a real-time report.

4. Under **Report Type**, select a report type:
   - **Consolidated report** (includes all InterScan WebProtect reports)
   - **Individual report** (include only the reports you select)
5. Under **Options**, select the chart type from the menu—either **Bar** or **Line**.
6. Click **Generate Report**. Click **Reset** to reset the form to the default values.

Scheduled Reports

You can configure InterScan WebProtect to generate scheduled reports on a daily, weekly, or monthly basis. To manage the large volume of reports generated, InterScan WebProtect allows you to generate only the reports that you specify and delete unnecessary scheduled reports from the archive directory.

To configure scheduled reports:

1. Click **Reports > Scheduled Reports** from the main menu.
2. Click the tab that corresponds to the frequency of scheduled report to run—either **Daily**, **Weekly** or **Monthly**.
3. Select **Enable <*Frequency*> Report**.
4. Set the time and/date to generate the scheduled report.

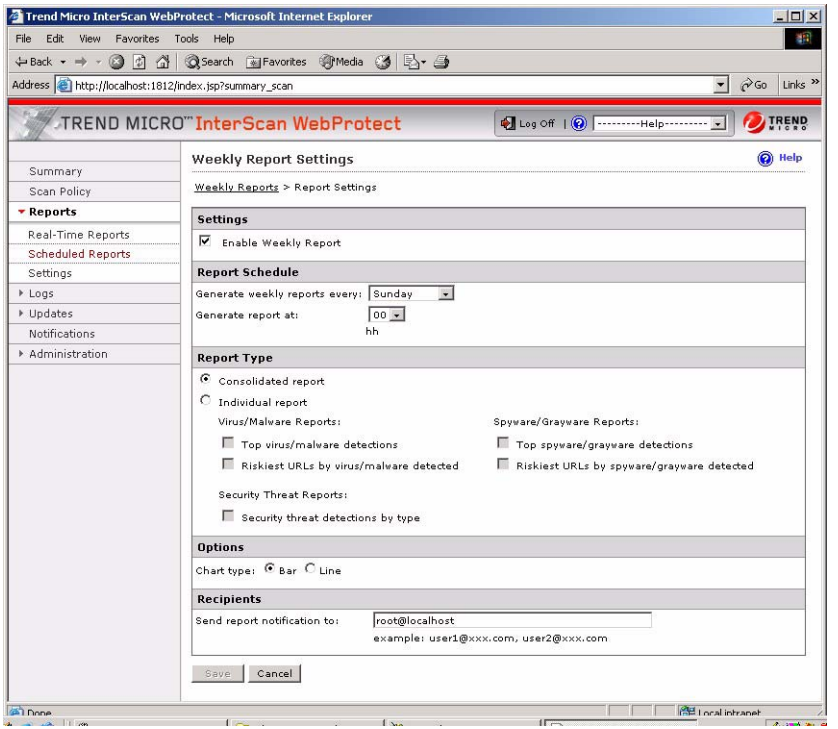


FIGURE 5-2 Scheduled Report Settings page (weekly report shown).

5. .Under **Report Type**, select the type of report to be generated:
   - **Consolidated report**.
   - **Individual report**. If you opt for the individual reports, select the type(s) of reports to include.
6. Under **Options**, select the chart type from the menu—either **Bar** or **Line**.
7. Under **Recipients**, in the **Send report notification to** field, type the email address(es) where InterScan WebProtect should send a notification when a newly generated report is ready for viewing. Separate multiple email addresses with a comma.
8. Click **Save**.

To delete scheduled reports:

1. Click **Reports > Scheduled Reports** in the main menu.
2. Click the tab that corresponds to the reports to delete—either **Daily**, **Weekly**, or **Monthly**.
3. Select the reports to remove and click **Delete**.

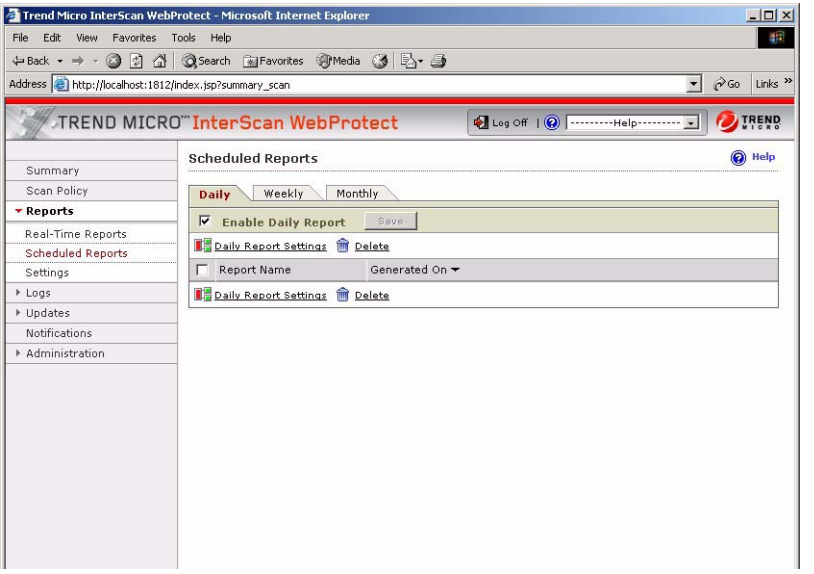


FIGURE 5-3 Delete old scheduled reports from the server.

Report Settings

InterScan WebProtect allows you to customize the number of records shown in different reports. For example, you can configure the number of "Top virus/malware detections. By default, ISWP reports include the top ten for each category (except for Security Threat Reports, which includes five.)

You can configure InterScan WebProtect to archive scheduled reports. The default path for archiving reports is `<install directory>\report` but can be modified. The default configuration is to archive 60 daily reports, 20 weekly reports and 4 monthly reports before deleting them from the server, but you can configure the number of scheduled reports to save.

To customize the report data maintenance settings:

1. Click **Reports > Settings** in the main menu.

2. Under **Customize the Number of Records**, type the number of records to include in each of the reports.

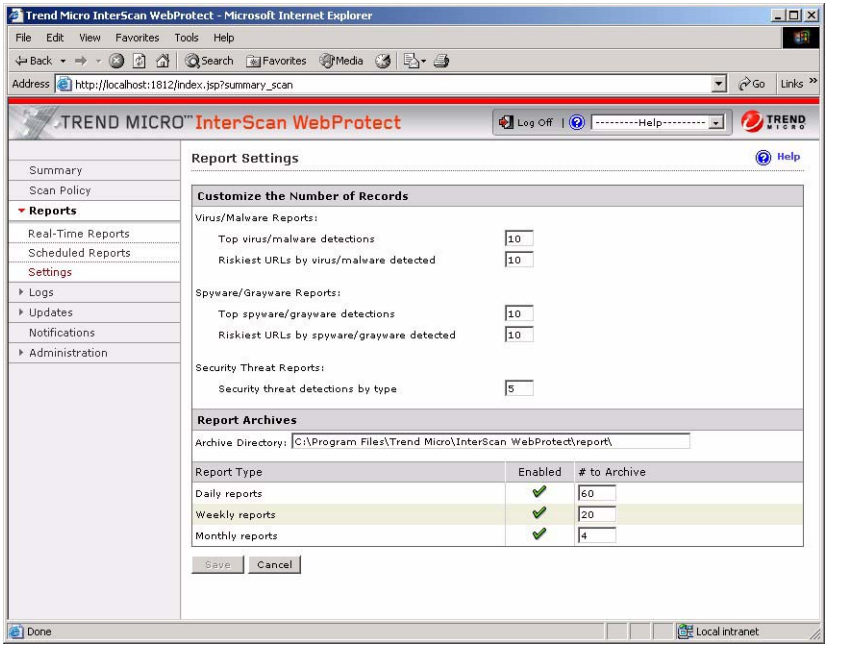


FIGURE 5-4 Customize the reports.

3. Under **Report Archives**, type the following information in the fields provided:
   a. **Archive Directory** to save the reports

      `<install directory>\report`

   b. Number of scheduled reports to save:
      - **Daily reports** (default is 60)
      - **Weekly reports** (default is 20)
      - **Monthly reports** (default is 4)
4. Click **Save**.

Note: When changing the **Archive Directory**, the folder must exist on the InterScan WebProtect server before it is entered into the **Report Settings** page. In order to view reports already generated, copy them over to the new folder.

Introduction to Logs

Reporting logs provide security threat information and can be viewed from the InterScan WebProtect management console. The database stores all log data. It may optionally also be stored in text log files to permit additional data analysis using customer scripts, and provides redundancy to verify the database is properly updated. Trend Micro recommends using the database as the only storage location for log data.

Virus Log

The virus log contains information about viruses that InterScan WebProtect has detected.

To view the virus log:

1. Click **Logs > Virus Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).
   - Click **Range** to view the virus log in a given time range, then select the start and end dates.

3. Under **Viruses**, select the virus(es) for which you want to view log entries. Click **Add** (or **Add All** for all viruses listed). To remove virus(es) from the right list box, click **Remove** (or **Remove All** for all viruses listed).

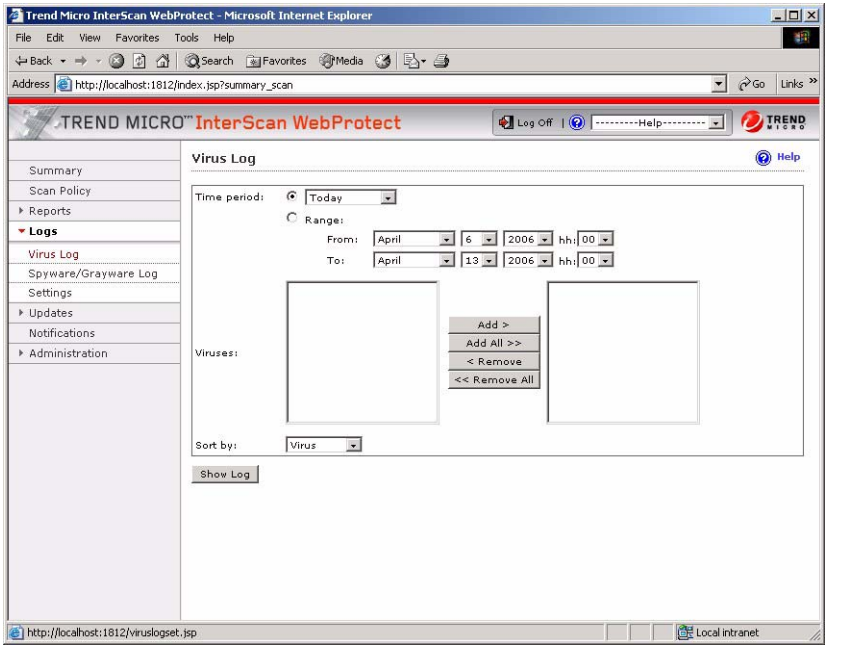


FIGURE 5-5 Filter virus log queries by the virus name.

4. Under the **Sort by** section, select a sort option to sort the display log (Virus, Date, Action, File Name).
5. Click **Show Log**. The **Virus Log** screen displays.
6. Click **Refresh** to update the screen.

Spyware/Grayware Log

The spyware/grayware log contains information about spyware/grayware detected by InterScan WebProtect, including the name of the spyware/grayware, date, action, and file name affected.

To view the spyware/grayware log:

1. Click **Logs > Spyware/Grayware Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).
   - Click **Range** to select a time range, then select the start and end dates.
3. Under **Grayware**, select the spyware/grayware for which you want to view log entries. Click **Add** (or **Add All** for all grayware listed). To remove grayware from the right list box, click **Remove** (or **Remove All** for all viruses listed).
4. Under the **Sort by** section, select a sort option (Grayware, Date, Action, and File Name).
5. Click **Show Log**. The **Spyware/Grayware Log** viewing screen displays.
6. Click **Refresh** to update the display.

Log Settings

From the **Log Settings** screen, you can configure:

- Number of days to keep the system logs (default is 7)
- Number of days to store logs in the database (default is 30)
- Database log update interval (in seconds): (default is 30)

Log File Folder Locations

You can configure the folders for the reporting logs and the system logs. The default location is:

```
<install directory>\Log
```

A folder must exist on the ISWP server before it can be configured as the log file location. InterScan WebProtect verifies the folder's accessibility after a folder path is entered, and an error message displays if the folder is not accessible.

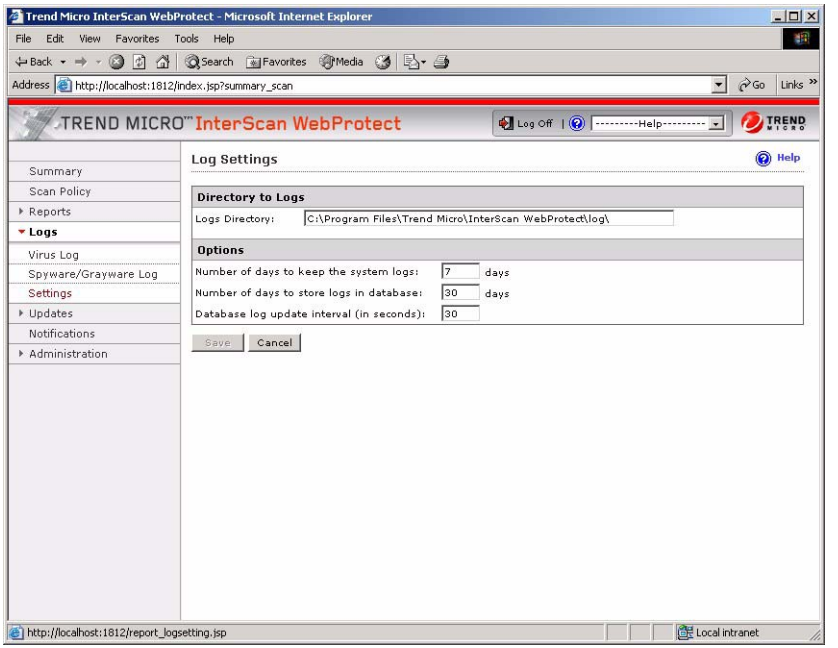


FIGURE 5-6 Configure log settings.

Appendix A

Encrypting Browser-Console Communication (HTTPS)

To prevent the interception of configuration data when it travels from the management console to the server, InterScan WebProtect can use the secure HTTPS protocol. Tomcat, the Web server that InterScan WebProtect uses, operates only on JKS format keystores, which is Java's standard "Java KeyStore" format, and is the format created by the keytool command-line utility. You can find the executable keytool in the following directory:

```
[Install_directory]\AdminUI\jre\bin\keytool.exe
```

The default install directory is:

```
C:\Program Files\Trend Micro\InterScan WebProtect
```

To learn more, see the ISWP online help. See the topics "Enable HTTPS Connection to the ISWP Console" and "Disable HTTP Access to the ISWP Console" in the Best Practices section.

To create a new keystore that contains a single self-signed certificate:

1. Execute the following from a terminal command line:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keystore
   .\mykeystore
   ```

2. Follow the prompts and use `ISWP50` as the password.

   The file `mykeystore` is generated in the current working directory.

3. Copy `mykeystore` to the Tomcat base directory.

   `[Install_directory]\AdminUI\tomcat` or to the set base directory in the CATALINA_HOME environment variable.

4. Copy and insert the following block under the `<Service name="Tomcat-Standalone">` section in the `server.xml` file located in the following file:

   `[Install_directory]\AdminUI\tomcat\conf\server.xml`

```
<Connector
className="org.apache.catalina.connector.http.HttpConnector"
port="8443"
minProcessors="5"
maxProcessors="32"
enableLookups="true"
acceptCount="0" debug="0"
scheme="https" secure=”true”>
<Factory
className="org.apache.catalina.net.SSLServerSocketFactory"
clientAuth="false" protocol="TLS"
keystoreFile="mykeystore"
keystorePass="ispw50"/>
</Connector>
```

   Note: If the filename used with keytool is something other than `mykeystore`, modify the `keystoreFile` entry shown above. If the password typed during the keytool prompts is something other than `iswp50`, modify the `keystorePass` entry as shown above.

5. Restart the Trend Micro InterScan WebProtect Console service to enable the certificate.
   Go to **Start > Settings > Control Panel > Administrative Tools > Component Services** and select **Trend Micro InterScan Web Protect Console** under the **Services (Local)** branch. On the toolbar menu, click the **Restart Service** button.

Accessing the InterScan WebProtect Console via HTTPS

To encrypt configuration data as it passes from the Web-based console to the server, you must alter the URL to use the HTTPS protocol and specify port 8443 instead of port 1812. Type the URL for encrypted communication (HTTPS) in the following format:

```
https://{SERVER-IP}:8443/index.jsp
```

```
https://123.123.123.12:8443/index.jsp
```

where `SERVER-IP` is the IP address of the server. For comparison, the URL used for non-encrypted communication (HTTP) is:

```
http://{SERVER-IP}:1812/index.jsp
```

```
http://123.123.123.12:1812/index.jsp
```

Disabling Non-HTTPS Access

Once you have enabled HTTPS to encrypt browser-console communication, you can disable non-HTTPS access to avoid the possibility of having your configuration data intercepted.

To disable non-HTTPS access:

1. Edit the Tomcat HTTP configuration file:

   ```
   <Install_directory>\AdminUI\tomcat\conf\server.xml
   ```

2. Delete the following nodes:

   ```
   <Connector
   className="org.apache.coyote.tomcat4.CoyoteConnector"
   port="1812" minProcessors="5" maxProcessors="32"
   enableLookups="true" redirectPort="8443"
   acceptCount="0" debug="0" connectionTimeout="600000"
   useURIValidationHack="false" disableUploadTimeout="true" />
   ```

3. Go to **Start > Settings > Control Panel > Administrative Tools > Component Services** and select **Trend Micro InterScan Web Security Suite Console** under

the **Services (Local)** branch. On the toolbar menu, click the **Restart Service** button.

After making these changes, the InterScan WebProtect Web console is accessible via

```
https://<ISWP_server_IP>:8443/index.jsp
```

Configurations After Changing the Console Listening Port

If the management console's listening port is changed, for example, to disable HTTP access, two configuration parameters in the `intscan.ini` file must be modified to continue using a scanning progress page.

Under the `[HTTP]` section of the `intscan.ini` file, change the following default parameters to reflect the new port and/or protocol:

```
[http]
iscan_web_server=1812
iscan_web_protocol=http
```

For example, if disabling HTTP after enabling HTTPS access to the management console, change the configuration parameters to the following:

```
[http]
iscan_web_server=8443
iscan_web_protocol=https
```

In addition, two parameters in the `[Product_Info]` section of the `product.ini` file need to be modified when InterScan WebProtect is configured to use HTTPS:

```
WebProtocol=https
WebPort=[user defined https port, e.g., 8443]
```

Appendix B

Frequently Asked Questions (FAQs)

The following FAQs apply to the current version of WebProtect.

Question 1: Why I can't get email notifications if one of my recipients in mail list is invalid?

Answer: Email notifications can vary, depending upon your mail system. Some mail systems will reject all recipients if there is one invalid email address, and some mail systems will accept it and deliver it to valid users. If it does occur, please check your recipients' list.

Question 2: Why does the Web manage console work abnormally sometimes?

Answer: If Web console IP is not in the trusted site list in IE, the access to WebProtect Web UI is blocked. WebProtect 5.01 WEB UI needs to be supported by scripts. Please reduce the IE security level or add WebProtect 5.01 (as a URL instead of a name) into the trusted site list.

Question 3: A database named as "WebProtectdb" exists, but the content inside is corrupt. Why can I still install WebProtect using it?

Answer: It is a limitation of installation program. If install WebProtect 5.01 to a corrupt database, it will cause WebProtect 5.01 to work abnormally. If you are sure that database is corrupt, change it during installation.

Question 4: Why wasn't the license renewed at any time during the grace period?

Answer: WebProtect conducts the scheduled license check to decide whether it is time to do an online license update or not. The checking action takes place under the following conditions:

- One day before the license expiration date (LED)
- 30 days or multiple of 30 days before LED
- 30 days or multiple of 30 days after LED but within grace period
- Every day after LED and beyond grace period

Question 5: Why is the content encapsulated by a pair of "[ ]" in message template always removed from the message in UI?

Answer: WebProtect reserves "[ ]" for comments to help users understand the notification message. Please do not use them for content that should appear in the notification message.

Question 6: If I configure access for Web console via https only, then I cannot access Web console through a UI-redirect from TMCM Server. Why?

Answer: When registering to the TMCM, the Control Manager Agent will send a URL for WebProtect Web UI to enable the URL-redirect. The string is composed as follows: `[protocol]://[FQDN]:[port]/.`

The [FQDN] is found in the Windows API; [protocol] and [port] are found in the product.ini file. You should manually configure two keys: WebPort and WebProtocol in the product.ini file. For example, WebPort=8443, WebProtocol=https. Then restart Control Manager Agent service. If you have configured NAT, please refer Question 11 for more details.

Question 7: Why isn't the WebFilter debug log deleted after uninstalling ISWP?

Answer: The debug log is disabled by default. Trend Micro only uses it for maintenance. To delete them, the user must remove them manually.

Question 8: Why does the report function generate an empty report folder if the ISWP Web console is configured for https access only?

Answer: You avoid the empty report folder, manually configure the following two keys: iscan_web_server, iscan_web_protocol in the intscan.ini file.

For example:

```
iscan_web_server=8443
iscan_web_protocol=https
```

Question 9: Why isn't a status change of the product updated to TMCM server if there are network problems?

Answer: The status has been stored in temporary files and will be sent again after WebProtect logs on to TMCM Server again.

Question 10: Why can't WebProtect register to the TMCM Server if the IIS server (on which the TMCM server relies) needs authentication?

This feature is not supported in current release. Please enable TMCM server's IIS "anonymous visit" option.

Question 11: Why doesn't the URL redirect function when WebProtect accesses TMCM by NAT?

Answer: If you want to enable NAT, please configure the following records: WebProtocol (ISWP WebUI's protocol) and WebPort (Port published on NAT device for ISWP WebUI) in the product.ini file. The IPAddressList (IP of NAT device) in the Agent.ini file. For example:

```
<Product.ini>
   WebProtocol=http
   WebPort=888
<Agent.ini>
   IPAddressList=10.10.10.10
```

Question 12: Why can't I use commas, semicolons and spaces as delimiters at the same time?

Answer: We don't support multi-delimiters in current release. Please use following rules:

1. Use comma for separating email recipients when configuring them in the UI pages.
2. The semicolon is regarded as delimiter in the text areas on the page accessed from **Scan Policy > Virus Scan Rule > Scan these file types (if not blocked) > Specified file extensions...**
3. A space is used as delimiter in the following two cases:

a. The text field next to "Other file types" accessed at **Scan Policy > Virus Scan Rule > Block these file types**

b. The text area that is beneath **Scan Policy > Virus Scan Rule > MIME Type Exceptions**.

Question 13: What are the basic traffic flow processing steps?

Answer: It depends on whether the traffic is incoming or outgoing. The traffic flow when downloading is:

Internet > ISA > WebProtect > ISA > Client

The flow reverses when uploading.

Question 14: Who delivers the data to the client, ISA or WebProtect?

Answer: WebProtect is a plug in for ISA. When WebProtect scans the data delivered from ISA, it returns the data back to ISA and then ISA delivers it to client.

Question 15: Do I need to modify the proxy settings of browser while using WebProtect?

Answer: No, you do not need to modify your browser proxy settings.

Question 16: Does WebProtect scan the inbound and outbound traffic?

Answer: Yes, WebProtect scans both inbound and outbound traffic.

Question 17: Can WebProtect scan HTTPS? What about FTP or FTP over HTTP?

WebProtect supports scanning of the following protocols:

- HTTP
- FTP over HTTP
- WebMail
- OWA

Question 18: Where are the files for customized notification messages located on the ISA server?

Answer: The customized notification message files are stored under `<product directory> \config\*.txt`

Question 19: What is included in antivirus scanning?

Answer: Antivirus scanning includes viruses, macro viruses, Trojans and worms.

Question 20: How many concurrent clients are supported per WebProtect instance?

Answer: WebProtect supports up to 500 concurrent connections per WebProtect instance.

Question 21: How do I setup and use a secure connection (HTTPS) to the WebProtect console?

Answer: The Web Console supports both standard HTTP and secure HTTPS connections. By default, it is configured only for HTTP. The following sections describe the procedure for setting up secure connections.

Generating an HTTPS Certificate

Before a browser can attach successfully to the WebProtect 5.01 console using the HTTPS protocol, a Windows user with administrator privileges must first generate a security certificate for use by the HTTPS protocol.

To generate the certificate:

1. Logon to the Windows server running WebProtect 5.01 with administrator privileges.
2. Select **Start > Run** and type cmd in the text field to create a command line window.
3. Change to the directory `<INSTDIR>\adminui\jre\bin`.
4. Type the following command (all on one line):

```
keytool -genkey -alias tomcat -keyalg RSA -keystore .\mykeystore
```

   This command generates (the -keygen argument) and RSA-style security key (the -keyalg RSA argument) for use with tomcat (the -alias tomcat argument), storing the key in the file mykeystore in the current directory. The program asks you several questions when generating the certificate:

   - **A password** — This is a password that is assigned to the key.
   - **First and last name** — (Optional) Type your first and last name.
   - **Organizational unit** — (Optional) Type your organizational unit (for example “sales”).

- **Organization** — (Optional) Type your organization's name.
- City or Locale - (Optional) Type the city of your organization's headquarters.
- State or Province - (Optional) Type the state or province of your organization's headquarters.
- Two-letter country code - (Optional) Type the two-letter ISO country code of your organization's country code.

After these questions are answered, the program prints a summary of the answers that it reads and asks if it is OK to generate the certificate. If you made a mistake, answer "no," and the program starts over with the First Name value. Otherwise, answer "yes." By entering the following command, the program generates the certificate mykeystore to the Tomcat base directory:

```
copy mykeystore ..\..\tomcat
```

5. Use a text editor (not a word processor) and open the file `<Install Directory>\adminui\tomcat\conf\server.xml`
6. Locate the section of the file that begins with:

```
<Service name="Tomcat-Standalone">
```

This is the beginning of the Tomcat configuration section.

7. Insert the following text below the line shown in Step 6:

```
<Connector
className="org.apache.catalina.connector.http.HttpConnector"
port="8443" minProcessors="5" maxProcessors="32"
enableLookups="true" acceptCount="0" debug="0" scheme="https"
secure="true">
<Factory
className="org.apache.catalina.net.SSLServerSocketFactory"
clientAuth="false" protocol="TLS" keystoreFile="mykeystore"
keystorePass="iswp50"/>
</Connector>
```

These lines create a new entry in the Tomcat configuration, allowing a connection to the console application on port 8443 using the secure HTTPS protocol. The connection gets the key from the file mykeystore, which is protected with a password of "iswp50". All of this information came from the keytool command in Step 4.

Note: When the filename used with keytool is other than mykeystore, modify the keystoreFile entry shown above. If the password typed during the keytool prompts is other than iwss20, modify the keystorePass entry as shown above.

8. Save the changes and close the file.
9. Manually configure two keys (i.e. iscan_web_server and iscan_web_protocol) in the intscan.ini file. Configure two keys (i.e. WebProtocol and WebPort) in the product.ini file. For example

```
iscan_web_protocol=http, iscan_web_server=1812,
WebProtocol=http, WebPort=1812
```

Note: If you have configured NAT, then the WebPort in the product.ini file should be set to a published NAT port.

10. Restart the Trend Micro InterScan WebProtect Console service. To do this:
    a. Select **Start > Programs > Administrative Tools > Services**.
    b. Right-click on Trend Micro InterScan WebProtect Console.
    c. Select **Restart**.

Disabling non-HTTPS Connections

To disable HTTP connections to the WebProtect 5.01 console service:

1. Login to the WEBPROTECT 5.01 server using a Windows account with administrator privileges.
2. Use a text editor (not a word processor) to edit the file: <INSTDIR>\adminui\tomcat\conf\server.xml
3. Locate and delete the following entry from the file:

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnecto"
port="1812" minProcessors="5" maxProcessors="75"
enableLookups="true" redirectPort="8443" acceptCount="100"
debug="0"connectionTimeout="20000" useURIValidationHack="false"
disableUploadTimeout="true" />
```

The above entry allows connections to the console application through port 1812, redirecting the connection to the console application at port 8443. Removing this entry prevents connections through port 1812.

4. Save the changes and close the file
5. Restart the Trend Micro InterScan WebProtect Console service. To do this:
   - Select **Start > Programs > Administrative Tools > Services**.
   - Right-click on **Trend Micro InterScan WebProtect Console**.
   - Select **Restart**.

Question 22: How can I change the port console that UI uses?

1. Log on to the WebProtect 5.01 server using a Windows account with Administrator privileges.
2. Use a text editor (not a word processor) to edit the following file:
   `<install directory>\adminui\tomcat\conf\server.xml`
3. Locate the following entry from the file:

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnecto"
port="1812" minProcessors="5" maxProcessors="32"
nableLookups="true" redirectPort="8443" acceptCount="0"
debug="0"connectionTimeout="20000" useURIValidationHack="false"
disableUploadTimeout="true" />
```

4. Change the port=1812 to port=xxxx (xxxx is the port you want to set.)
5. Save the changes and close the file.
6. Manually configure two keys (i.e. `iscan_web_server` and `iscan_web_protocol`) in `intscan.ini` file, then configure two keys (i.e. WebProtocol and WebPort) in `product.ini` file. For example:

   ```
   iscan_web_protocol=http, iscan_web_server=1812,
   WebProtocol=http, WebPort=1812
   ```

   Note: If you have configure NAT, then WebPort in product.ini should be published NAT port.

7. Restart the Trend Micro InterScan WebProtect Console service. To do this:
   - Select **Start > Programs > Administrative Tools > Services**

- Right-click on Trend Micro InterScan WebProtect Console
- Select **Restart**

Question 23: What kind of DB does WebProtect install? MSDE or something else?

Answer: WebProtect does not install a database during installation. Users should install MSDE/SQL 2000 by themselves or use MSDE bounded in ISA.

Question 24: How to configure the ODBC setting on WebProtect?

Answer: Please update the values of these keys in database section of intscan.ini.

```
[database]
dsn=WebProtectDSN
db=WebProtect
user=sa
dbServer=127.0.0.1\WebProtect
jdbcUrl=jdbc:odbc:WebProtectDSN
```

Question 25: Where does WebProtect store logs, reports, and configuration settings?

1. Virus logs and spyware/grayware logs are stored in the tb_violation table; reports are generated through query the logs.
2. The scan policy (not all configuration settings) is stored in the tb_rule table.
3. The other configurations are stored in the following files:
   - `intscan.ini`
   - `IWSSPIProtocolIcap.pni`
   - `IWSSPIScanVsapi.dsc`

Question 26: Does WebProtect support working with an existing MSDE or SQL server?

Answer: Yes, it does. It can be configured during installation

Question 27: What should I need to do if I changed the user name or password of the database?

Answer: You can change user name in the .ini file, but password should be changed through Web UI, since the password is encrypted before saving into .ini file

Question 28: How can I recover or reset WebProtect console password?

Answer: Delete the password file: “prd.password”, and the console password is restored to “admin”.

Question 29: How can I initiate debug logging? Where are debug logs stored and in what format?

Answer: You can start debug logging by changing the debuglevel key value in the registry. (5 is the most detailed.) Or you can open debug log by CDT. The debug logs are stored in the $ProductDir\debug. The debug log follows Trend Micro standards.

Question 30: Does WebProtect support the ISA appliances provided by third party vendors?

Answer: We do not support them.

Question 31: How are old pattern files deleted? Do we have an “auto-delete”? Where are pattern files stored?

Answer: Old patterns will be deleted automatically, the pattern files is stored in $ProductDir\activeupdate.

Question 32: How many pattern files are kept by default? Do we support Scan Engine Rollback?

Answer: WebProtect will keep three virus patterns and three spyware patterns. It also supports Scan Engine Rollback.

Question 33: What will users see when they access a web page containing a blocked file type? Is the entire web page blocked, or just the file, such as a Java applet?

Answer: The web page containing a blocked file type will display without showing the blocked file type.

Question 34: How can I decrypt encrypted quarantine files?

1. Download the vsencode.zip at: (http://solutionfile.trendmicro.com/SolutionFile/11435/en/vsencode.zip)
2. Extract the contents to the ISWP Quarantine directory. The following files appear:

```
forencrypt.ini
readme.txt
```

```
VSAPI32.DLL
VSEncode.exe
```

3. Open for editing the `forencrypt.ini` file and type the path of the quarantine directory. For example:

```
C:\Program Files\Trend Micro\InterScan
WebProtect\quarantine\*.*
```

4. Open a command prompt at the directory where you downloaded the vsencode.zip. file and type the following:

```
VSEncode -d [-debug] -i forencrypt.ini
```

Parameters

-d: decrypts files in the specified folder defined in the "ini" file

-debug: generates the debug log and output in client system root

5. All encrypted files in the quarantine directory will be decrypted and the log, VSEncrypt.log, (or VSEncDbg.log for debug mode) is created.

WARNING! *Decrypted files are likely to be dangerous. Viruses can infect the server. Trojans can drop their payload, worms may propagate, and spyware can open backdoors to the server. Use caution. Delete or re-encrypt the files as soon as possible.*

Question 35: What kinds of events that are logged?

Answer: These events are logged:

- Update license result
- ActiveUpdate result
- Main service start/stop
- Main service fatal error

Question 36: How can we test report notifications without waiting for the next scheduled event?

Answer: Modify the system time and restart the windows task schedule.

Question 37: Is a report notification sent to the recipient, or the report itself?

Answer: Scheduled reports will notify those entities listed in the email list in Scheduled Report setting with a URL for accessing the report.

Question 38: What happens if a report is specified for a longer time frame than the logs keep? (For example, a six-months report in a 30-day log archive). Is a notification sent, or how does user know?

Answer: The system will delete the expired report automatically according to the setting in the **Reports > Settings** page.

Question 39: Can you use multiple WebProtect servers together with TM Control Manager?

Answer: Yes, the TMCM supports multiple WebProtect 5.01 servers.

Question 40: What's the difference between clicking Updates > Manual in the menu and Update in the manual Update page? How about for Rollback?

Answer: The only difference is showing the latest version or not.

Question 41: What are the variable that can be used in WebProtect notifications (and anywhere else)? For example, %u, %f, %u.

Answer: WebProtect 5.01 supports the following tokens:

- %U [URI]
- %A [Action]
- %Y [date]
- %V [Virus name]
- %F [file name]
- %H [host name]
- %M [quarantine path]
- %R [transfer direction]
- %X [reason for block]

Note: The message headers of user notification only support parsing the token %H [host name].

Question 42: What ports does WebProtect use?

Answer: The following table shows the WebProtect's port number usage:

Port Number	Usage
25	For email notifications
80	For HTTP access to TMCM server, ActiveUpdate server, PR server
443	For HTTP access to TMCM server, AU server, PR server
563	For HTTP access to TMCM server, AU server, PR server
1344	For ICAP server
1433	For Microsoft SQL Server
1812	For HTTP access to web console
8443	For HTTPS access to web console

TABLE B-1 WebProtect Port Number Usage

Question 43: What WebProtect services run under Windows?

Answer: The following WebProtect services run under Windows:

- Trend Micro InterScan WebProtect (Main service)
- Trend Micro InterScan WebProtect Console
- Trend Micro InterScan WebProtect Log to Database
- Trend Micro InterScan WebProtect Notification Delivery Service
- Trend Micro InterScan WebProtect TMCM Agent

Question 44: If scanning is halted (service crash, intentionally disabled, etc.), how does the user know?

Answer: It can be monitored through TMCM Server.

Question 45: How can I install a TM Control Manager agent? Where is it located?

Answer: It will be installed by default. You only need to register it to TMCM Server on WEB Console or during installation.

Question 46: Are reports archived in the database, or are they stored in the directory? What are the names and type of report files?

Answer: Reports are stored in a user-defined directory configured in **Reports > Settings**.

Scheduled reports are stored in Daily/Weekly/Monthly->report.<year>.<month>.<day>, including several files.

Question 47: What file extensions are used in the Virus Scan Policy for the following categories: Java applets, executables, Microsoft Office documents, audio/video files, images, other file types?

Answer: File extensions by category are:

Category	Extensions
Java applets	java, class
Executables	binhex, com, core, dcr, exe, exec, grp, hpexe, lisp, lnk, mac, netlm, netpd, netuni, novhlp, risc, swf
Microsoft Office documents	afc, afm, cdr, doc, hlp, fm, mscal, msdoc, msexl, msmdb, mso, msppt, msproj, mswri, pdf, ps, rtf
Audio/video files	afc, aif, afs, av, avs, iff, maud, midi, mng, mp3, mpeg, mprg, qtm, ra, rmf, scm, sf, smf, voc, wav
Images	bw, cgm, eps, fh9, gif, jpeg, picture, ras, tga, tiff
Other true type file groups	
Compressed files	arj, bin, bzip2, com16, cpio, gzip, lha, mscab, mscomp, rar, tar, teleimg, zip
Encoded files	base64, uuencode
Others	bnd, mmdf, msft, sbf, type, elf, tnef

Question 48: Why can't I download pattern files from alternative server when I block compressed files?

Answer: This is because the data package is compressed and blocked. To solve the problem, you need to add the update server into the registry key at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan
WebProtect\ISA2004WebFilter\SkipHDR
```

Question 49: Is security compromised if I can access the ISWP database via MS SQL Enterprise managers by connection to MSDE DB via <instance>\WPFW?

Answer: Yes it is. Since WebProtect uses the same database with ISA Server and a separate SQL data resource, the database is accessible by SQL console. Trend Micro recommends that the customer should to manage the security of the database via a strong password.

Question 50: When I uninstall ISWP, the ISA generates a WebFilter Start error message. It says: "WebFilter Trend Micro InterScan WebProtect WebFilter is not installed." Other files of WebProtect are totally removed. Is it all right?

Answer: The uninstall is fine. This is a normal warning message from the ISA Server while WebProtect is uninstalling.

Question 51: Why is the same real-time report generated even after I have modified the report settings?

Answer: There are two possible reasons this happens. The page may have been cached by IE or by your ISA server. Try the following solutions:

- **a.** Empty your IE cache, and then generate the report again.
- **b.** If the ISA cache has been enabled, you should add a new cache rule on the ISA server that makes the ISA server avoid caching the content for ISWP. For instructions on creating a cache rule, please refer to the ISA document "Configure Cache Rules."

Question 52: Why can't I use the WebProtect Configure Console from the TMCM Web UI?

Answer: If you use NAT between ISWP and TMCM, please refer **Question 11:** *Why doesn't the URL redirect function when WebProtect accesses TMCM by NAT?* on page B-3. Otherwise, you can change your network settings of TMCM Web client to avoid this. There are two methods. One is to change the Web proxy of the machine to an

ISA server. The other is to change the gateway setting, pointing the gateway to an ISA server.

Question 53: Do I have the latest pattern file?

Answer: To find out which version or pattern file you have, go to the main ISWP menu, click **Summary**. The virus pattern, spyware, and scan engine versions and update schedules appears.

To find out the latest available patterns, open a Web browser to the Trend Micro Update Center at: http://www.trendmicro.com/download/

For specific updates try the following links:

- For Virus and Spyware pattern files, go to: http://www.trendmicro.com/download/pattern.asp
- For Scan engine updates, go to: http://www.trendmicro.com/download/engine.asp#prod_16
- For ISWP builds, go to: http://www.trendmicro.com/download/product.asp?productid=16

Question 54: How are log files named?

Answer: ISWP automatically logs all Internet-threat incidents, mail deliveries, pattern file and other updates, and reports. Logs can be kept on the local ISWP server, or posted to the ISWP database (for faster reporting, file management considerations, or to aggregate data for a multi-ISWP environment).

Naming convention:

- HTTP Log—http.log.yyyymmdd
- Mail Delivery Log—mail.log.yyyymmdd
- Update Log—update.log.yyyymmdd

Question 55: What can I do if a pattern file is corrupt?

There may be occasion to revert, or rollback, ISWP to a previous version a pattern file or the scan engine. The two most common reasons for a rollback are:

- False positive—a harmless file (or group of files) is incorrectly detected as unwanted
- Corrupted files—transmission of the pattern introduced an error

Rollbacks are only supported for registered versions of ISWP.

ISWP automatically retains the three most recent pattern files (and scan engine versions), in addition to the current one. Older versions are automatically removed from the ISA server.

To rollback to a previous version of one or more data files:

1. From the main ISWP menu, click **Summary**.
2. Select the component you want to rollback from the list that appears.
3. Click the **Rollback** button.
4. After prompted, to see the rollback results, click the **Back** button to return to the **Summary** page and see the results in the Current Version and Last Update column.

Question 56: What is Spyware?

Spyware includes software programs and technologies (called “bots”) that seek to surreptitiously collect data and transmit it back to a host source.

The category of spyware and other grayware threats includes adware, Internet cookies, Trojans, and surveillance tools. The type of information collected by spyware ranges from the relatively innocuous (a history of visited Web sites) to the downright alarming (credit card and Social Security numbers, bank accounts, and passwords).

The majority of Spyware/Grayware comes embedded in a “cool” software package which a user finds on a Web site and downloads. You can configure ISWP to scan these downloads, and if the file matches one of the pattern files, you can have ISWP block it. Some spyware programs are part of a legitimate program. Others are purely illicit. The network administrator must determine whether a given class of software is something he or she wants to allow on the network, or something they want ISWP to block at the gateway.

Growing hazard

Increasingly, users are installing more and more malicious types of spyware without their knowledge, either as a “drive-by download”, or as the result of clicking some option in a deceptive pop-up window. What concerns corporate security departments is that the more sophisticated types of spyware can be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email

and other applications. In some cases, spyware can even capture screenshots or turn on Web cams.

Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls related to spyware are forcing corporations of all sizes to take action. Spyware can represent both a security and system management nightmare.

Question 57: Why doesn't the ISWP status icon in the TMCM change during an off-hour?

Answer: The status icon is not designed to change during off-hours. The TMCM is behaving correctly, even when the status icon does not change during the off-hour.

Question 58: I have Web Protect but I have not purchased a license for anti-spyware. However, I am still receiving email notifications that say: "Spyware pattern: ERROR: The anti-spyware has not been activated. ActiveUpdate is disabled." Can this be disabled without effecting other notifications, including notifications for regular pattern and scan engine updates?

Answer: Users can disable or enable notification email messages for anti-spyware pattern updates by changing the "sypware_ptn_notify" parameter in the "intscan.ini" found at "\Trend Micro\InterScan WebProtect". Once the parameter is configured to "no", email notifications for anti-spyware pattern updates will not be sent.

Question 59: I have upgraded from Web Protect 5.0 to 5.01, but I can't rollback the pattern and engine immediately. Is there a way to rollback the pattern and scan engine?

Answer: Users can move the following directories from "\Trend Micro\InterScan WebProtect" to "\Trend Micro\InterScan WebProtect\AU_data" as a workaround.

- AU_log
- AU_temp
- AU_Cache

After moving the directories, follow the steps in *What can I do if a pattern file is corrupt?* on page B-16 to rollback.

Question 60: Can I have a desktop anti-virus product (e.g. OfficeScan) installed on the same ISA server where WebProtect is installed?

Answer: Yes, but you need to configure your desktop anti-virus product to exclude ISWP working directories from real-time and on-demand scanning by the desktop anti-virus product. For instance, if you have OfficeScan installed on the ISA server with ISWP, you need to exclude following directories:

- ISWP installed directory. The default is:
  `<DISK ROOT>\Program Files\Trend Micro\InterScan WebProtect\`
- Folder for ISWP to locate scanning temporary files:
  `<WINDOWS ROOT>\Documents and Settings\NetworkService\Local Settings\Temp`

Question 61: I have upgraded WebProtect from 5.0 (with hotfix 1167 or from the 5.01 Beta build) to 5.01. Why can't I receive spyware update notifications when I perform scheduled updates? (I still receive engine and virus updates notifications.)

Answer: Users can enable notification email messages for anti-spyware pattern updates by changing the "sypware_ptn_notify" parameter in the intscan.ini file found at "\Trend Micro\InterScan WebProtect". Once the parameter is configured to "yes", email notifications for anti-spyware pattern updates will be sent.

Appendix C

Maintenance Agreement

A Maintenance Agreement is a contract between the customer and Trend Micro, regarding the right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Note: The Maintenance Agreement expires. The License Agreement does not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending expiry. You can update the Maintenance Agreement by purchasing renewal maintenance from the reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

`https://olr.trendmicro.com/registration/`

Renewing the Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If the Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending protection for a year, will be sent by post to the primary company contact listed in your organization's Registration Profile.

To view or modify your organization's Registration Profile, log on to the account at the Trend Micro online registration Web site:

`http://olr.trendmicro.com`

You are prompted to enter a logon ID and password.

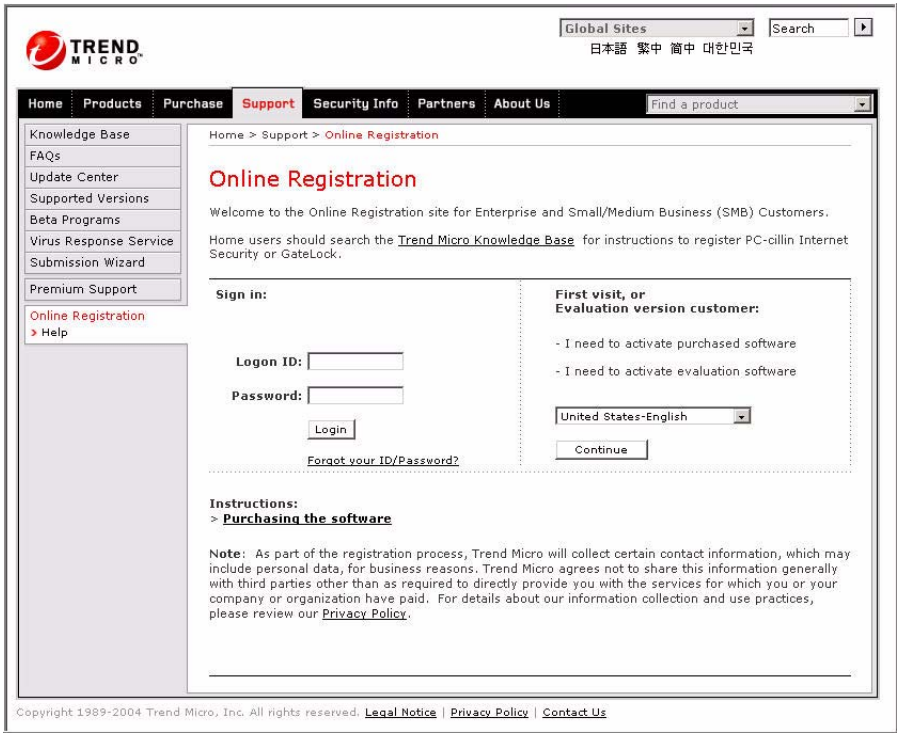


FIGURE C-1. Renew the license agreement at the Trend Micro Online Registration site

To view the Registration Profile, type the logon ID and password created when you first registered the product with Trend Micro (as a new customer), and click Login.

Index

A

Access
  internal network 2-25
  remote database 2-23
  SMTP server 2-28
  TMCM server 2-27
  Trend Micro Web site 2-24
  VPN clients 2-25
  web console 2-25
activation 2-10
Activation Code(s) 2-11
  format 3-3
  obtaining 3-2
  status 3-3
ActiveUpdate
  incremental updates 1-6
Administrator's Guide 1-10

C

cache servers
  flushing 3-10
communication
  encrypting 3-16
compressed files
  handling 4-10
  security settings 4-10
Control Manager 1-2
controlled pattern releases (CPRs) 1-6
  installing 1-6

D

database
  and log files 5-2
  connection settings 3-14
  testing connection 3-15
delete 5-6
documentation 1-10

E

EICAR test file 3-16
ESMTP 4-17

F

false alarm 3-11
FAQs B-1
file blocking
  notification 4-20
file types 4-6
  blocking 4-5–4-6
forced updates 4-22
Frequently Asked Questions B-1

H

HTTP
  file types to block 4-5
  file types to scan 4-6
  service 2-9
HTTP proxy
  settings 3-13
HTTP scanning
  compressed files 4-9
  file blocking 4-5
  files to scan 4-6
  large files 4-10
  notifications 4-18
  priority 4-9
  quarantine 4-12
  scan actions 4-14
  scan events 4-15
  security settings 4-10
  skipping files 4-5
HTTPS
  Web console A-1, A-3

I

ICSA certification 1-8
incremental pattern file updates 1-6
installation
  shared drive not supported 2-8
Installation and Deployment Guide 1-10

IntelliScan 4-6
ISA Policies 2-23
  configuring 2-23
iscan_web_protocol A-4
iscan_web_server A-4
IWSS
  features 1-3
  testing 3-16, A-4

K

keytool.exe A-1
Knowledge Base 1-10

L

large file handling
  HTTP 4-10
License Agreement 2-8, C-1
listening port A-4
log files
  URL blocking log 5-10
log settings 5-11
logs 1-3
  folders 5-11
  introduction 5-9
lpt$vpn.xyz 3-11

M

main program 2-9
Maintenance Agreement C-1
  renewal C-2
  renewing C-2
management console
  password 4-3
Microsoft SQL Server Desktop Engine (MSDE) 2-14
MIME-type 4-8–4-9
mixed threats 1-2

N

notifications 1-3–1-4, 2-16, 3-12
  administrator vs. user 4-15
  configuring 4-18
  email settings 4-16
  ESMTP support 4-17
  introduction 4-15
  tokens 4-17
  using HTML tags 4-18
  using variables in 4-17

O

online help 1-10

P

password 4-3
  setting 2-13
  tips for creating 4-3
pattern files 1-4–1-5
  deleting 3-11
  manually deleting 3-11
  several on server 1-6
  version numbering 1-5
pattern matching 1-5
proxy
  settings 3-6
proxy server
  settings 2-9, 4-22

R

readme file 1-10
RealAudio 4-8
registration
  benefits 3-2
  URL C-1–C-2
Registration Key 3-2
Registration Keys 3-2
  format 3-3
Registration Profile C-2
Remote database access 2-23
removing 2-21
reports 1-3
  archiving 5-7
  chart types 5-2
  consolidated vs. individual 5-2
  customizing 5-7–5-8
  daily 5-5
  deleting scheduled 5-6
  real-time 5-3
  scheduled 5-5
  settings 5-2–5-3
  types 5-2
rollback 4-22

S

scan engine 1-4, 1-7
  events that trigger an update 1-8
  ICSA certification 1-8
  updates to 1-8
  updating 1-8
  URL to find current version 1-8
scanning
  select file types 4-7
setup.exe 2-7
SolutionBank-see Knowledge Base 1-10
spyware/grayware
  reports 1-4
  scanning rules 4-12
spyware/grayware log 5-10
system requirements 2-6

T

testing
  download scanning 3-17
  upload scanning 3-17
tokens in notifications 4-17
Tomcat
  HTTPS A-1, A-3
TrendLabs 1-2
true file type 4-6

U

updates 3-7
  components 1-4, 3-5
  disabling scheduled updates 3-9
  forced 3-8
  forcing 3-8
  incremental 1-6
  manual 3-8
  notifications 4-21
  proxy settings 3-6
  rolling back 3-11
  scheduled 3-9
Upgrading 2-2
  Backing up the database 2-3
  ISA 2004 to ISA 2006 2-2
  ISA 2004 to ISA 2006 details 2-4
  Restarting services 2-5
  Restoring the database 2-4
URLs
  registration C-1–C-2
  scan engine version 1-8

V

variables
  using in notifications 4-17
virus
  "in the wild" 1-7
  "in the zoo" 1-7
  action 4-14
  pattern file, published 1-6
virus log 5-9
Virus Map 2-11, 4-2
virus scanning 1-3
  deferred scanning 1-3
virus signatures
  see virus pattern file
vsapi32.dll 3-11

W

World Virus Tracking Center 2-11, 4-2
  data sent 4-2