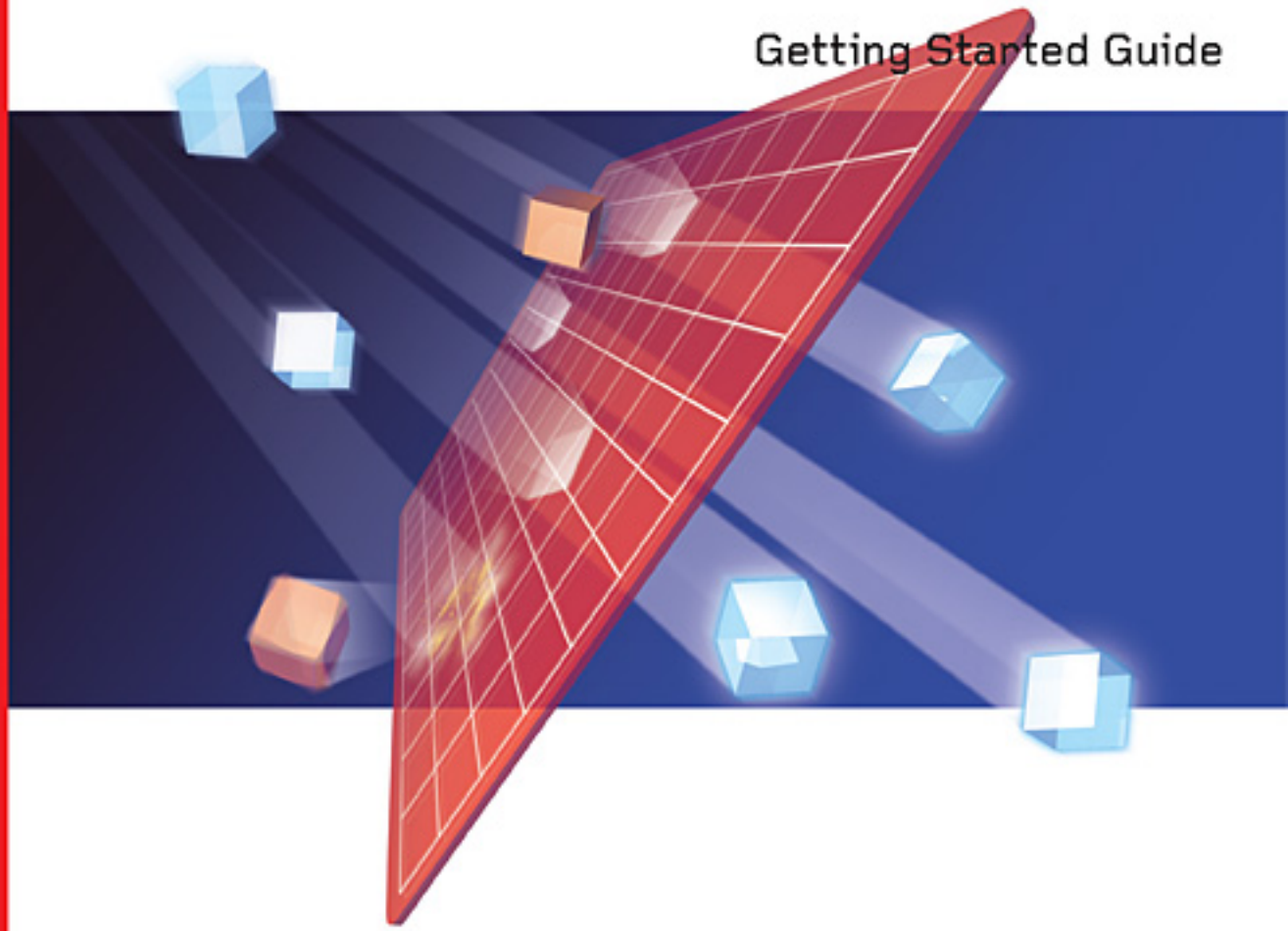
TREND MICRO™
InterScan™ WebProtect3

Integrated HTTP gateway protection

for Microsoft™ ISA Server

Getting Started Guide



TREND MICRO™

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

http://www.trendmicro.com/download/documentation/

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

Document Part No. WPEM31859/40408

Release Date: April 2004

Protected by U.S. Patent No. 5, 951, 698

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

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

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

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

Contents

Chapter 1

Introduction

InterScan WebProtect for Microsoft ISA Server protects your network from all types of computer viruses that can cross the information superhighway—the Internet—and into your network. InterScan WebProtect for Microsoft ISA continuously monitors files transferring via HTTP, effectively creating an impermeable barrier to infections from known and unknown viruses.

This chapter discusses what computer viruses are, how they attack your system, the damage they can do, and available methods used to safeguard against these potentially damaging files.

The following is only an introduction to virus types. You can access detailed, on-line information about specific viruses from the following site:
`http://www.antivirus.com/vinfo/virusencyclo/`

Topics included are:

- What is InterScan WebProtect?
- Main Features
- How InterScan WebProtect Scans Files
- About Viruses
- Using the Product Documentation

What is InterScan WebProtect?

InterScan WebProtect is a set of programs that executes on the Internet gateway. This system acts as a gateway between a LAN and the Internet system. InterScan WebProtect scans all or selected file transfer via HTTP for viruses. The program performs a user-configured action whenever it encounters an infected file (e.g., clean, quarantine, delete).

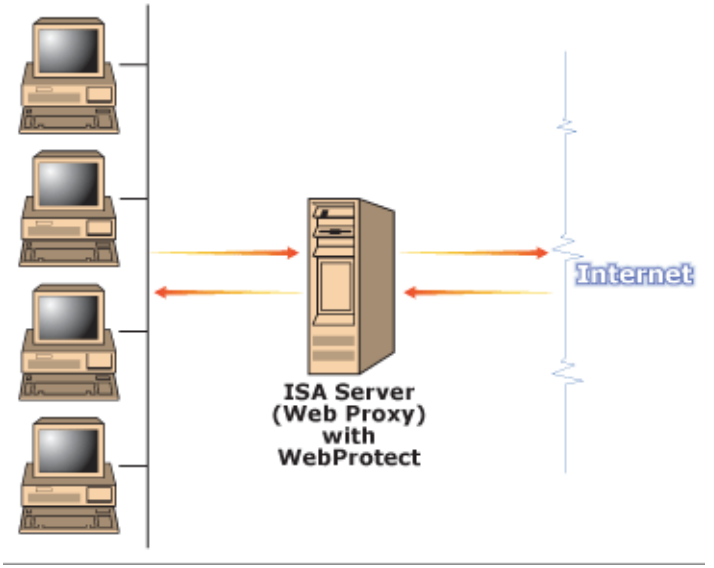


FIGURE 1-1. WebProtect scans all or selected file transfer via HTTP.

Main Features

Here are some of the main features of InterScan WebProtect:

- Integrates directly with ISA Server
- Intercepts viruses at the server before they can enter and damage your network
- Complements existing firewall systems
- Uses a Windows 2000-based virus scanning engine
- Allows you to selectively download certain MIME content-types that would otherwise be obstructed by the scanning function
- Provides a simple-to-use Web browser configuration program
- Transparent to the user
- Contains an award-winning, intelligent virus scanner designed for multi-threading operating systems
- Provides virus pattern file updates through the Internet with a single click of a button, as well as periodic, prescheduled updates
- Flexible configuration

How InterScan WebProtect Scans Files

InterScan WebProtect for Microsoft ISA Server consists of two logical components: the configuration utility and the main program.

InterScan WebProtect looks at all incoming files transferred via HTTP, places the contents into a temporary file, and invokes the virus-checking program. If the incoming file is not infected, InterScan WebProtect passes the file to the client.

If a file is infected with a virus, InterScan WebProtect performs the action you've specified in your configuration. It may delete the file, pass it to the recipient node, or isolate it for later action.

InterScan WebProtect uses its virus pattern file to detect known signature viruses by pattern matching. In addition to catching known signature viruses, the program detects and intercepts previously unknown polymorphic, or mutation, viruses.

In the case of polymorphic or mutation viruses, scanning engine of WebProtect saves the virus code in a temporary location on the WebProtect server. Here, after

decrypting, InterScan WebProtect locates the code, characterizes the mutation virus, and performs whatever action you have configured (for example, clean, quarantine).

InterScan WebProtect employs Trend Micro's generic macro virus scanning engine, MacroTrap™ to detect macro viruses. MacroTrap is a rule-base virus detection method, which detects and removes unknown as well as known macro viruses.

About Viruses

A computer virus is a program that replicates. To do so, the virus needs to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes.

Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage. Called the damage routine, or payload, the destructive portion of a virus can range from overwriting the partition table on the main system disk to scrambling the numbers in your corporate spreadsheets to just taunting you with sounds, pictures, or effects.

It's worth bearing in mind, however, that even without a "damage routine," left unabated, viruses continue to propagate—consuming system memory, disk space, slowing network traffic, and generally degrading performance. Virus code can be the source of mysterious system problems that take weeks to understand.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate—until the preordained trigger day or event when they unleash their damage routines across the network.

Whether it was written to be harmful or just annoying, a virus on your system can lead to instability and should not be allowed to remain.

Virus Writers

In the traditional scenario, a highly-technical individual, working alone, would write a virus program and then introduce it onto a computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations for virus writers.

Now, however, it takes no special skill to create a macro virus, a mass mailer, or other virus with highly disruptive potential. In fact, “virus kits” proliferate on the Internet and are available at no cost to anyone who wants to try disrupting the internet or corporate communications.

About Virus Scanning

At the root of antivirus programs such as WebProtect is both a scan engine and a comprehensive database of virus “signatures,” commonly called the virus pattern file. Together, these two components do the work of identifying and then cleaning infected files.

At its most basic, a gateway antivirus application monitors HTTP and FTP traffic between the LAN and the Internet. Whenever it detects a file type that it has been configured to scan (for example, .zip, .exe, .doc, and so on), the application copies the file to a temporary location and opens the copy for virus scanning.

If the file is clean, the application deletes the copy and releases the original for delivery to the FTP or HTTP server, which delivers the file as usual. If a virus is detected, the application takes whatever action it has been configured to take: **Clean**, **Delete**, **Quarantine**, or **Pass** (deliver anyway - this choice is not recommended). Deleted and quarantined files are not delivered to the client desktop. Files set to be cleaned are opened, the virus code removed, and the file is then reassembled.

Not all viruses, or malware, can be cleaned. For example, some viruses corrupt the host file, making in unusable. Trojans, worms, and mass mailers do not “infect” a host file and therefore cannot be cleaned. Whatever the action, all detections are written to the virus log; the administrator and/or designated others can also receive an automatic notification of the incident.

About ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, anti-spam rules, and program files via the Internet.

ActiveUpdate does not interrupt network services, or require you to reboot your servers. Updates are available on a regularly scheduled interval, or on-demand.

Updated components are also available on the Trend Micro Enterprise Solutions CD, which is issued quarterly to customers on Premium Support.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire 5-6MB pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your virus pattern file.

About Heuristic Virus Protection

The Trend Micro scan engine uses two methods for detecting viruses, worms, Trojans, and other Internet security threats: pattern matching and heuristic scanning.

1. **Pattern matching**—as the engine checks each file, it compares the binary file data to a list of known virus "signatures" or strings of code. Pattern matching is thorough and efficient, but is limited to detecting only known viruses
2. **Heuristic scanning**—as the engine checks each file (or email message), it runs through a series of "questions" to analyze whether the file possesses the characteristics of a threat. Because heuristic scanning is an evaluative method rather than comparative, it excels in detecting undiscovered viruses and threats, including polymorphic viruses—those that change "signatures" with each new infection.

   Trend Micro heuristic scanning includes the following specialized technologies:

   - **ScriptTrap**—Detects script-based viruses including JavaScript, Visual Basic (VB) Script, HTML, and Active Server Pages (ASP) Scripts
   - **Vice Engine**—Detects new and unique Denial of Service (DoS) threats
   - **MacroTrap**—Detects unknown macro viruses—including those embedded in the following types of files: Microsoft Word, Excel, PowerPoint, Access, Visio, and Microsoft Project
   - **Softmice**—Detects complex polymorphic viruses using a 32-bit emulator to fool the virus into revealing itself in a safe and contained environment
   - **BootTrap**—Detects both boot sector and partition table viruses

About the Trend Micro Scan Engine

At the heart of all Trend Micro products lies a proprietary scan engine. Originally developed in response to the very first computer viruses the world had seen, the scan engine today is exceptionally sophisticated and capable of detecting Internet worms, mass-mailers, Trojan horse threats, phish sites (a bogus Web site designed to spoof a legitimate organization's site, in order to trick people into disclosing personal information), spyware, and network exploits, as well as viruses. The scan engine detects threats 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

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 passing through an email server to 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 that 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 manage bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes some 30 or more compression formats, including Zip, Arj, and Cab. Most Trend Micro products also allow the product administrator 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 breaking threats. 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. Occasional technological upgrades in the engine software, typically prompted by a paradigm-shift in the nature of virus threats, for example the recent rise in mixed-threats such as SQL Slammer and the so-called network viruses

In both cases, updates can be scheduled from the antivirus product to occur automatically, or they can be manually handled by the administrator in charge of security.

The Trend Micro scan engine is certified annually by international computer security organizations.

Using the Product Documentation

The documentation set for this product includes the following:

- Getting Started Guide—This Guide helps you get "up and running" by introducing WebProtect, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation using a harmless test virus. The latest version of the Guide is available in electronic form at:

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

- 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 release history.
- Online help—The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the WebProtect console.
- Knowledge Base— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://kb.trendmicro.com`

Chapter 2

Installation and Setup

This chapter describes the system requirements for InterScan WebProtect, and step-by-step instructions on how to install and remove the program. We recommend that you register your software with Trend Micro Inc. as soon as you have completed the installation.

Topics included are:

- Recommended System Requirements
- Installing InterScan WebProtect
- Removing InterScan WebProtect
- Testing InterScan WebProtect

Recommended System Requirements

To use InterScan WebProtect for Microsoft ISA Server, you will need the following hardware and software:

- Intel Pentium™ III 450MHz or higher
- Microsoft™ Windows™ 2000 Server or Windows 2000 Advanced Server with Service Pack 1 or later or Microsoft Windows 2003 Server
- Memory: 256MB of RAM
- Hard Disk: 20MB of available hard-disk space
- Microsoft ISA Server 2000
- Microsoft Internet Information Server

Installing InterScan WebProtect

Before the installation process, Trend Micro recommends stopping all running Windows programs. Moreover, you must have a full administrator's access privilege before proceeding with the installation process.

To install InterScan WebProtect:

1. You can install WebProtect from either the Trend Micro Enterprise Solutions CD or by downloading it from the Web.
   If you are installing from the Trend Micro Enterprise Solutions CD,
   a. Run the Trend Micro Enterprise Solutions CD by inserting the CD into the CD-ROM drive.
   b. Follow the prompts to continue.
   c. The **Enterprise Solutions** screen displays as shown below.

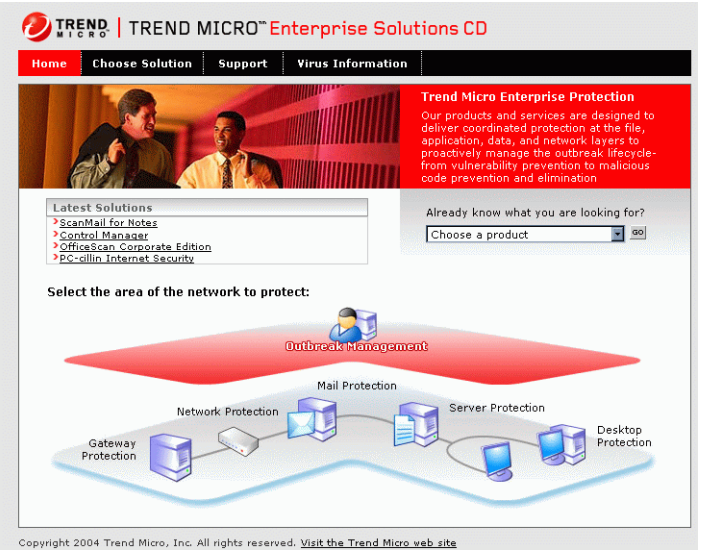


FIGURE 2-1. WebProtect must be installed on the same logical drive as the ISA Server.

If you are downloading from the Web,

a. Download or copy the WebProtect binary archive to a temporary directory on the server where you want WebProtect to run, and then extract the files.

b. Next, double-click the file **setup.exe** to begin installing.

2. Click **Next**.
3. Click **Yes** to accept the **Software License Agreement**.
4. Under the **User Information** screen, type all the necessary information in the fields provided. Click **Next** to continue.
5. The **Choose Destination Location** screen appears. The default install directory is `c:\Program Files\Trend\InterScan\WebProtect`. Click **Next** to install the program files, or click **Browse** to select another destination directory.

Note: If the InterScan WebProtect setup program detects an existing version on the system, the default program directory will be set to the existing version's program directory; however, you can choose another directory. (1) To install InterScan WebProtect in a directory different from the existing version's directory, Trend Micro recommends removing the existing version first, then continue the installation process. (2) To install InterScan WebProtect in the same directory as the existing version, you have three options: (a) Keep the configuration and overwrite all other files, (b) Overwrite all files including configuration files, or (c) Exit setup.

---

6. Next, the **Select Program Folder** screen appears. Here you can add the **InterScan WebProtect for Microsoft ISA Program Group** folder. You may select a folder from the list under **Existing Folders** or click **Next** to continue and use the default folder.
7. In the **WebProtect Configuration IP Address and IIS Port** screen, type the correct IP address of your system and the IIS Port number (80 is the default IIS port number). Click **Next**.

Note: You cannot access the **WebProtect Configuration** page if the IP address or IIS port number was not configured correctly.

---

8. Restart IIS before running **Trend InterScan WebProtect Configuration**. Click **Yes** to restart now and begin configuring the program or click **No** to configure at

a later time. You will also be prompted to restart the Web Proxy before Trend Micro InterScan WebProtect can work. Click **Yes** to restart now.

9. Click **Finish**.

Note: After completing setup, activate the ISA Application filter, also known as the HTTP redirector, on the ISA Server. This will make the firewall redirects all HTTP requests to the Web proxy to make sure that all traffic will pass through InterScan WebProtect.

Removing InterScan WebProtect

To remove InterScan WebProtect:

1. On the Windows taskbar, click **Start** > **Programs > InterScan WebProtect for ISA > Uninstall**.
2. A **Confirm File Deletion** screen appears. Click **Yes** to confirm and continue with uninstallation or click **No** to cancel the operation.

Testing InterScan WebProtect

After installing InterScan WebProtect, you must test virus scanning to verify that WebProtect is working properly.

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 whose 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.

Note: Never use real viruses to test your antivirus installation.

Obtaining the EICAR test file

You can download the EICAR test virus from the following URLs:

www.trendmicro.com/vinfo/testfiles/

www.eicar.org/anti_virus_test_file.htm

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

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

Note: To test the eicar script with InterScan WebProtect, disable any other antivirus software running on your network or computer before attempting to download the EICAR test script.

Testing HTTP Scanning

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

To test virus scanning for Web-based mail attachments:

1. Open the WebProtect console and click **Scan Configuration > HTTP Scanning** in the left-hand menu. Clear **Enable HTTP Scan**, and then click **Save**.
2. Download the test virus from the following page:
   www.eicar.org/anti_virus_test_file.htm
3. Save the test virus on your local machine.
4. Re-open the WebProtect console, select **Enable HTTP Scan** in **Scan Configuration > HTTP Scanning** in the left-hand menu, and then click **Save**.
5. Send a message with one of the test viruses as an attachment by using any Internet mail service. A warning message that shows the detection of an EICAR test virus must appear for the test to be successful.

Chapter 3

Configuring InterScan WebProtect

Once you have installed the InterScan WebProtect software on the Internet gateway, you can configure it to begin real-time scanning of file transfers via HTTP. This chapter will guide you through the configuration process.

Topics included are:

- Securing InterScan WebProtect Installation
- Opening the WebProtect Console
- Enabling HTTP Scanning
- Configuring the "Trickle" Function
- Configuring Files to Scan
- Bypassing Specific MIME Content-Types
- Setting Virus Notifications
- Setting the Scan Action for Viruses

Securing InterScan WebProtect Installation

InterScan WebProtect for Microsoft ISA requires the use of IIS and ISA Servers on the same machine. Because of this setup, unauthorized individuals may take the chance to gain access to users' Web servers.To set up security for WebProtect users using IIS and ISA Servers on the same machine, the following solutions, depending on the case, are given as follows:

CASE 1: For ISA Server installed using **Firewall** and **Integrated** modes

To avoid unauthorized Internet (external) individuals using the incoming port, perform the following solutions to block Internet users.

1. In the console tree of **ISA Management** (**Start > Programs > Microsoft ISA Server > ISA Management**), select **Access Policy** and right-click **IP Packet Filters**, then select **New > Filter**.
2. Follow the on-screen instructions to block external users from the IIS incoming port in **Local Port Number**.

CASE 2: For ISA Server installed using **Firewall**, **Cache**, and **Integrated** modes

To avoid unauthorized intranet (internal) individuals using the incoming port, either one of following identification methods can be used to authenticate users.

To use authentication control in IIS:

1. Create a Windows user account appropriate for the authentication method. If appropriate, add the account to a Windows user group.
2. Configure NTFS permissions for the directory or file for which you want to control access.
3. Go to **Start > Programs > Administrative Tools > Internet Services Manager**.
4. Under **Internet Information Services**, select a site, directory, or file and right-click and choose **Properties**. (for example, select WebProtect)
5. Select **Directory Security** and under **Anonymous access and authentication control**, click **Edit**. Then, disable **Anonymous access**.
6. Under **Authenticated access**, enable **Integrated Windows authentication**.

Note: Trend Micro recommends **Integrated Windows authentication** for high security level without exposing the IP address and internal name.

---

7. Click **OK**, then click **Apply** and click **OK** again.

To use authentication control in ISA Server:

1. In the ISA Management console tree, right-click the applicable array and then click **Properties**.
2. Under **Incoming Web Requests** or **Outgoing Web Requests**:
   a. Click **Add** to add and configure an Internet protocol (IP) address.
   b. Click **Edit** to edit the properties of an IP address.
3. Under the **Add/Edit Listeners** screen, select **Authentication > Integrated**.

Opening the WebProtect Console

You will begin all configuration tasks from the WebProtect console, which you can access from any node on the Internet with a Web browser.

To open the WebProtect console:

1. Either select **Programs > InterScan WebProtect for ISA > WebProtect Configuration** from Windows 2000 Advanced Server **Start** menu, or start your Web browser and enter the WebProtect URL:

   ```
   http://IPaddress:port/dir/cgi-bin/webprotect.htm
   ```

   where `IP address` is your IP address, `port` is the IIS running port number and `dir` is the directory in which InterScan WebProtect for ISA Server is installed. For example:

   ```
   http://127.0.0.1:8888/WebProtect/cgi-bin/webprotect.htm
   ```

2. If password security has been set up, the **Authentication** screen appears. Type the user name and password values, and then click **OK**.

   The URL link to Web configuration will not work if one of the following conditions occurs:

   - The user used a wrong IP address during the program installation.
   - The computer's IP address was changed after installing InterScan WebProtect for ISA.
   - The computer's IIS running port number was changed.

   To resolve this issue, go to `/WebProtect/webprot.url`. Right-click `webprot.url`, and then choose **Properties**. Type the valid IP address and IIS

port number values in the fields provided, click **Apply**, and then **OK**. For example, the following URL with local computer port number 8888 is written as follows:

```
http://127.0.0.1:8888/WebProtect/cgi-bin/webprotect.htm
```

Password Management

Your password is the primary means of protecting your system from unauthorized access. 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 the dictionary
- Intentionally mis-spell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

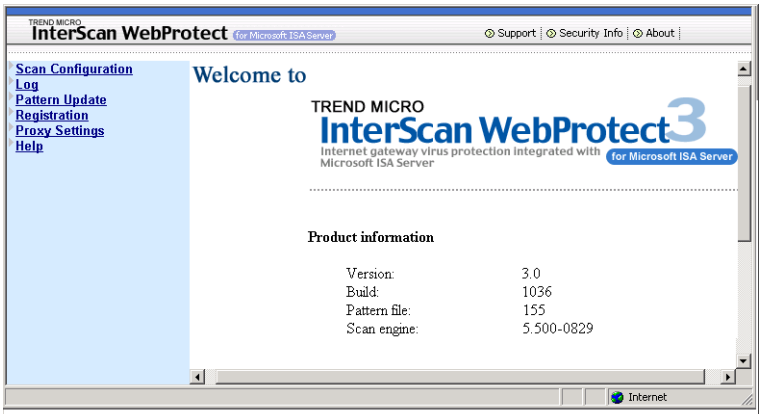


FIGURE 3-1. The WebProtect console gives you the latest product information.

Enabling HTTP Scanning

InterScan WebProtect monitors client HTTP download requests for viruses and malicious content.

To enable HTTP scanning:

1. Open the WebProtect console and select **Scan Configuration > HTTP Scanning**.
2. Select **Enable HTTP Scan**.
3. You can have WebProtect keep a log of the HTTP requests made by all client machines by enabling **Log HTTP Client Requests**.

   This log cannot be viewed from the **View Logs** page. Instead, use a text editor (such as Notepad.exe) to open and view the log file. The date, time, process and number, client IP address, GET request, and URL are recorded. You can use the viewer's search or find function to quickly locate keywords.

   The log files are kept in the root WebProtect directory and take the form of: `name.log.year.month.day`. For example,

   ```
   c:\webprotect\iscan.log.2001.12.18
   ```

4. Click **Save** to apply your changes. You need to stop and restart the Microsoft Proxy Server before the changes will take effect.
5. Click **Restore** to revert to the previous configuration settings.

Configuring the "Trickle" Function

InterScan WebProtect for Microsoft ISA Server features a "trickle" function, which solves a proxy or client browser time-out issue that can occur while scanning downloaded files.

How Does "Trickle" Work?

If the connection between InterScan WebProtect and the Internet is slow, clients may encounter time-out issues generated by the HTTP proxy server or their Web browsers when downloading large files. To solve the problem, InterScan WebProtect provides the option to "trickle" small amounts of data to the requesting client in advance of transferring the entire scanned file.

Note: Use "trickle" only if you are currently experiencing the time-out problem described above.

Because "trickle" works by advancing a small portion of data to the clients without scanning, it is theoretically possible that virus code will be among the portion of file that has been "trickled" to the client. Users should delete these files.

Data trickled to the client's hard drive will appear as a small, unusable file. Users should understand that InterScan WebProtect has not corrupted these files; rather, they have been deleted in accordance to the policy set by the administrator

With "trickle" set, clients are not notified when a file is blocked.

The predicted download time that clients receive when downloading a file will be vastly overestimated—the client browser calculates this time according to the "trickle" it is receiving; it bears no reflection on the speed at which InterScan WebProtect is receiving the file. In fact, once the file has been scanned, transfer to the client usually only takes a few seconds.

Follow the steps outlined below to configure the "trickle" function of InterScan WebProtect.

1. Open the WebProtect console and select **Scan Configuration > HTTP Scanning**.
2. Under **Configuration**, type the number of bytes you want "trickled" to clients. For example,

   Send 1024 bytes of data to client for every 512 kilobytes received

   In this example, InterScan WebProtect will release 1024 bytes of data to the client for each 512KB of the file that it receives. Once the entire file has been downloaded to the InterScan WebProtect machine and scanned, it is rapidly transferred to the requesting browser.
3. Click **Save** to apply your changes. You need to stop and restart the Microsoft Proxy Server before the changes will take effect.
4. Click **Restore** to revert to the previous configuration settings.

WARNING! *The partial delivery of file may result in a virus leak; thus, this would be a performance versus absolute security choice for you. Use this option only if you are currently experiencing an issue with timeouts.*

Configuring Files to Scan

You can configure WebProtect to check all downloads for viruses or scan only selected file types. Follow the steps outlined below to configure the **File to Scan** section of InterScan WebProtect.

1. Open the WebProtect console and select **Scan Configuration > HTTP Scanning**.
   - To scan all file types, regardless of extension, click **All files** under **File to Scan**. Scan all files is the most secure configuration (recommended setting).
   - You can skip files based on their extensions to work around performance issues with scanning all HTTP traffic. However, this is an unsafe practice and not recommended, because the extension of the file is not a reliable means of determining its content. You should skip files by extension only if it is necessary to meet the performance requirements of your environment.

     To scan only selected file types (Trend Micro does not recommend this setting), click **Only the following extensions** under **File to Scan**. Type the file types you want to scan. Delimit multiple entries with a comma. Use this option, for example, to decrease the aggregate number of files WebProtect checks, to decrease overall scan time.
2. Click **Save** to apply your changes. You need to stop and restart the Microsoft Proxy Server before the changes will take effect.
3. Click **Restore** to revert to the previous configuration settings.

Bypassing Specific MIME Content-Types

You can configure WebProtect to selectively bypass certain MIME content-types. This can be useful for streaming protocols such as Real Audio or other streaming content, for example, where the audio starts playing as soon as the beginning of the file arrives at the client computer. For these files to be scanned for viruses, however,

the entire file must first be downloaded, a condition contrary to the methods of protocol streaming. You can have WebProtect omit these file types from scanning by adding the appropriate MIME types to the list of MIME content-type to skip.

WebProtect gives you the option to exclude certain MIME content-types from being scanned; however, there is no direct approach in excluding downloaded files by extension. To address this, you can select **Only the following extensions** under **File to Scan** rather than **All files** to exclude certain extensions from being scanned and, therefore, ensure protection.

Below are the file extensions recommended to be scanned by WebProtect:

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

To bypass certain MIME content-types:

1. Open the WebProtect console and select **Scan Configuration > HTTP Scanning**.
2. Under **Scan Exceptions**, enable **Do not scan the following MIME types** to omit the listed file types from being scanned. Type the MIME content-type to bypass (for example, image, audio, application/x-director video, application.pdf, multipart). Delimit multiple entries with a comma.
3. Click **Save**.
4. Click **Restore** to revert to the previous configuration settings.

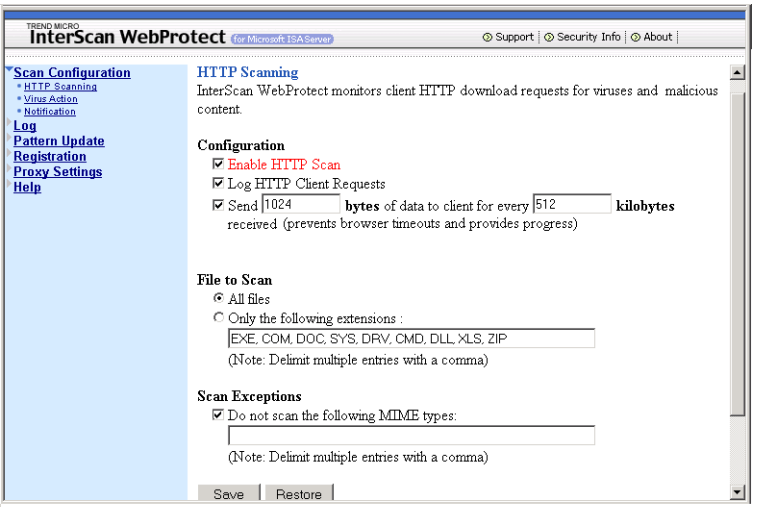


FIGURE 3-2. Delimit multiple entries with a comma.

Setting Virus Notifications

When WebProtect detects a virus, Trojan, or other malicious code in a file, which a user requested, WebProtect can automatically send a customized email message to the administrator or other individuals who should be informed to the presence of infected files. WebProtect uses the Web browser of the requesting client to notify user whenever a downloaded file is infected with a virus:

1. Open the WebProtect console and select **Scan Configuration > Notification**.

2. Under **Message properties**, type the sender's email address and subject in the fields provided.
3. Under **Notification**, enable **Notify the following** and type the recipients' email addresses. Delimit multiple entries with a comma. Type the necessary message in the **Message Text** field. For example:

   InterScan WebProtect for ISA has found a virus/malicious code in a user's HTTP traffic.
4. Under **Notification Server**, type the hostname (or IP address) and SMTP port number values in the fields provided.
5. Click **Save** to apply your changes.
6. Click **Restore** to revert to the previous configuration settings.

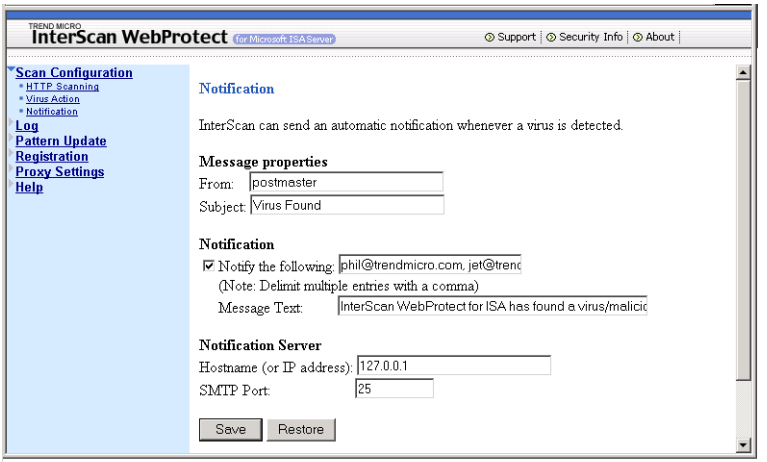


FIGURE 3-3. Make sure that you enter the correct IP address and SMTP port number of the notification server.

Setting the Scan Action for Viruses

See *To set the scan actions:* starting on page 3-12 for the procedure of setting action on viruses. InterScan WebProtect for Microsoft ISA Server can be configured to perform one of four actions (**Clean**, **Quarantine**, **Delete**, **Pass**) whenever a virus is detected. You can specify the action for HTTP scanning to take upon finding an infected file (recommended action setting is **Clean**):

- Choose **Quarantine** to move, without cleaning, the infected file to the quarantine directory. The requesting client will not receive the file.
- Choose **Delete** to delete the infected file at the server. The requesting client will not receive the file.
- Choose **Clean** to have HTTP scanning automatically clean and process infected files. The requesting client will receive the cleaned file if it is cleanable.
- Choose **Pass** to send the uncleanable file (Trend Micro does not recommend this choice, because it may allow infected files into your network).

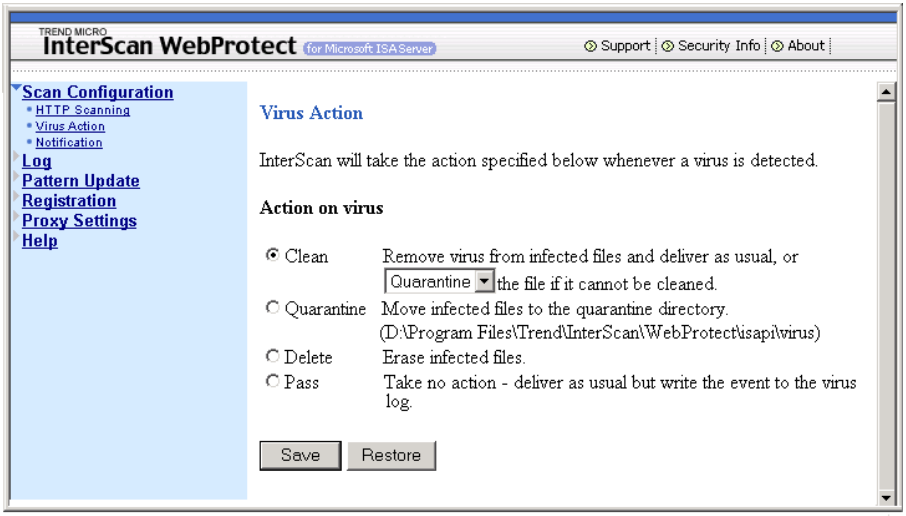


FIGURE 3-4. Infected files that cannot be cleaned, due to corruption for example, can be passed on, quarantined, or deleted.

To set the scan actions:

1. Open the WebProtect console and select **Scan Configuration > Virus Action**.
2. Specify the action for WebProtect to take when it detects an infected file:
   - Choose **Clean** to remove the virus code from infected files and deliver as usual. The drop-down menu displays the available options for uncleanable files. If you choose **Clean** you must also designate what action WebProtect should take on infected files that cannot be cleaned: **Quarantine**, **Delete**, or **Pass**.
   - Click **Quarantine** to move the infected files to the quarantine directory

     `C:\Program Files\Trend\InterScan\WebProtect\isapi\virus.`
   - To erase infected files, select **Delete**.
   - To take no action and deliver as usual but write the event to the virus log, click **Pass**.
3. Click **Save**.
4. Click **Restore** to revert to the previous configuration settings.

What Does the User See?

Users who attempt to download an infected file are informed of the action WebProtect took. A log including the virus name, user and Host IP addresses, and other details are recorded.

The following screen illustrates what the user sees if the file they are downloading has a virus and **Action on virus** has been set to **Quarantine**:

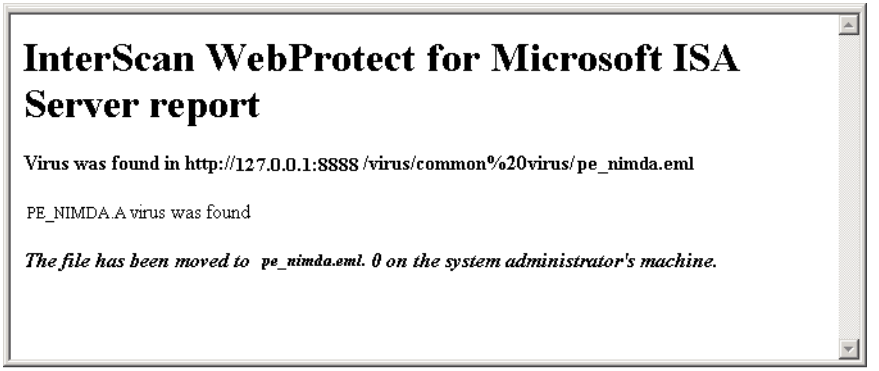


FIGURE 3-5. This type of message appears when you are downloading infected files.

Chapter 4

Managing Logs

InterScan WebProtect creates and saves an activity log that records two classes of information: virus logs and server logs. The **virus log file** contains detailed data about virus-infected files the program has detected. The **server log file** records the times and dates of program startup and shutdown as well as virus pattern file loading and updates (see *Updating the Virus Pattern File* starting on page 5-1 for a description of the virus pattern file).

Topics included are:

- Virus Log File Data
- Viewing Virus Log Files
- Viewing the Server Log
- Deleting Log Files

Virus Log File Data

The **virus log** includes information about all infected files received. You can display the entries of all or selected log files in several different formats. The format options include:

- Sort logs by date, virus name, action on virus, infected file, source
- Display log files for all dates, just today, the past week, the past month, or for a range of dates
- Display log files for all users or just for specified users
- Display log files for all viruses or only specified viruses

Viewing Virus Log Files

To view the virus log files:

1. Open the WebProtect console and select **Log > View Virus Log**.
2. Under **Display**, sort logs according to the criteria shown on the pull-down menu.

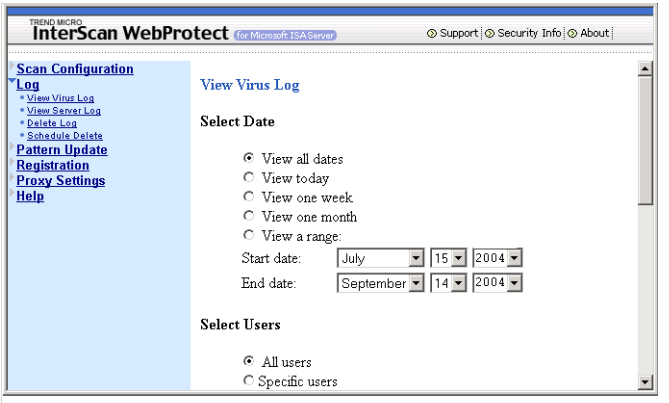


FIGURE 4-1. "View all dates" and "All users" are the default settings.

3. The selections listed under **Select Date** let you specify the dates for the log files you want to examine. Your options include:
   - **View all dates**, to display all the logs available
   - **View today**, to display just the current day's log file
   - **View one week**, to display log files for the past seven days
   - **View one month**, to display log files for the past 31 days
   - **View a range**, to select log files for a given range of dates. Select the start and end dates for the range in the corresponding pull-down menus for the month, day, and year.
4. If you want to view the log files for all users on your network, select **All users** under **Select Users**. Otherwise, select **Specific users** and choose the user names from the list.
5. To view log files for all viruses detected, select **All viruses** under **Select Viruses**. If you would prefer to see the logs for just certain viruses, select **Specify Viruses** and choose the names of individual viruses from the list.
6. Click **Restore** to revert to the previous settings, or click **View Log** to save the settings and display the log as you have just configured it.

Click the link under the **Virus** field to view the information on a virus listed.

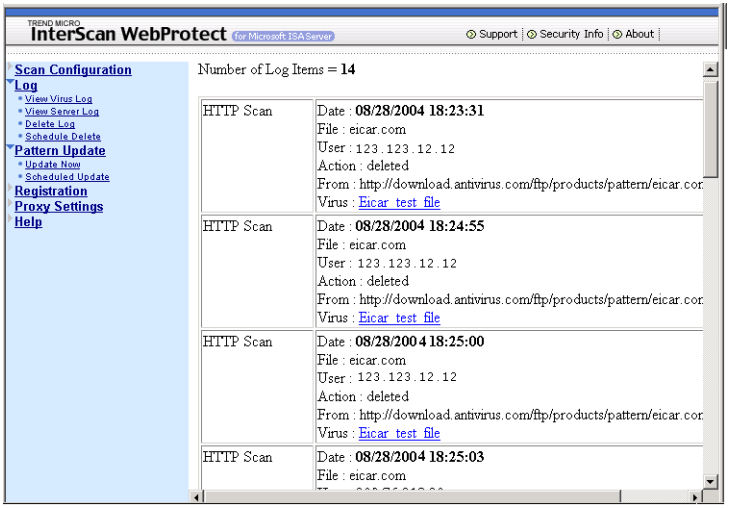


FIGURE 4-2. The Virus Activity Log screen contains information on the number of log items and HTTP Scan's descriptions.

Viewing the Server Log

InterScan WebProtect maintains a **Server Log**, which keeps a record of the date and exact time for the following program events:

- virus pattern file updates
- virus pattern file loading
- InterScan WebProtect startup
- InterScan WebProtect shutdown

To view the server log:

1. Open the WebProtect console and select **Log > View Server Log**.
2. In the **View Server Log** screen, select one of the following options:
   - **View all dates**, to display all the logs available
   - **View today**, to display just the current day's log file
   - **View one week**, to display log files for the past seven days

- **View one month**, to display log files for the past 31 days
- **View a range**, to select log files for a given range of dates. Specify the start and end dates for the range in the corresponding pull-down menus for the month, day, and year.

3. Click **Restore** to revert to the previous settings, or click **View Log** to save the settings and display the log as you have just configured it.

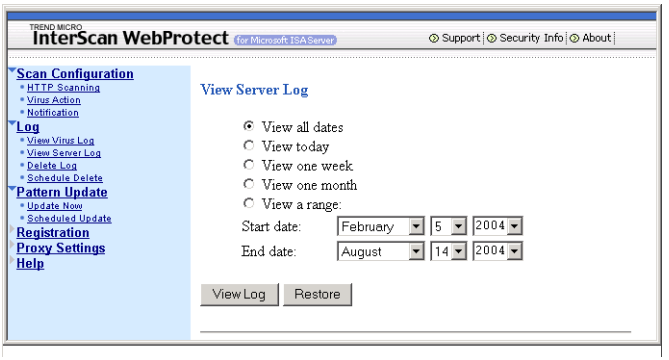


FIGURE 4-3. "View all dates" is the default setting.

Additional data is displayed at the top of the **Server Log** screen, including the number of times (since installation) the program has been started up and shut down,

the dates of the last startup and shutdown, and the total number of times the virus pattern file has been updated.

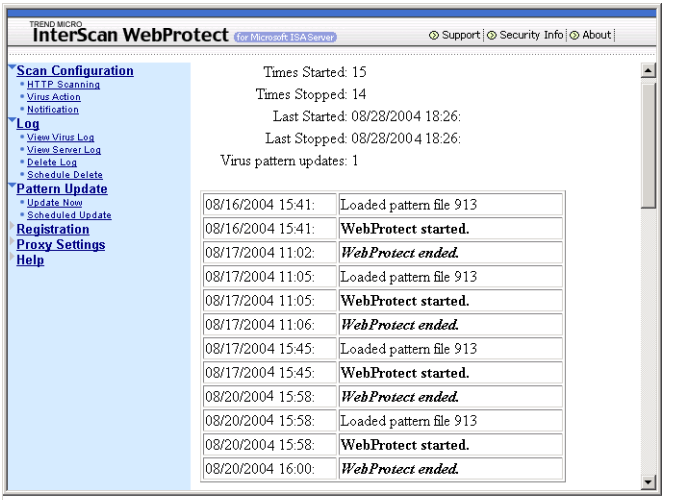


FIGURE 4-4. The Server Log gives you various activities information with the corresponding date and time.

Deleting Log Files

Because InterScan WebProtect creates and saves new log data every day, this accumulating data may eventually take up a lot of disk space. If some or all are no longer useful to you, you can delete them, either manually or automatically.

Deleting Log Files Manually

First make certain that you have looked over the log files and are sure which ones you want to delete.

To delete log files manually:

1. Open the WebProtect console and select **Log > Delete Log**. The **Log Maintenance** screen appears.
2. Under **Delete Logs**, you have the option of deleting all logs or a specific log.

To delete all, click **All logs**. To clear log files for selected dates only, click **Specific logs**. Next, highlight the log file(s) to delete (click the entries, while holding the **Ctrl** key for multiple selection).

3. Click **Delete**.
4. Click **Restore** to revert to the previous settings.

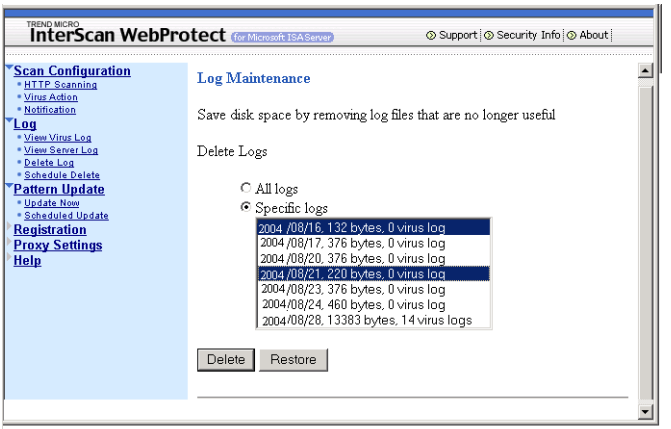


FIGURE 4-5. Save disk space by removing log files that are no longer useful in the Log Maintenance screen.

Note: The deleted files will be listed in the **Delete Log** screen until you refresh it.

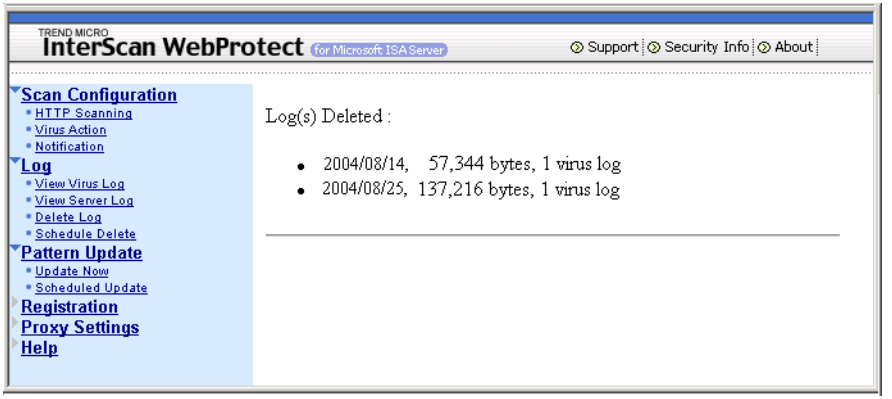


FIGURE 4-6. Descriptions of the log(s) deleted are shown in the Deleted log files message display.

Deleting Log Files Automatically

Instead of deleting old log files manually, you can set the program to do it for you at regular intervals. This feature is especially useful if your system handles a large volume of file traffic.

To enable automatic log file deletion:

1. Open the WebProtect console and select **Log > Schedule Delete**. The **Configure Autodelete** screen appears.
2. Select **Enable Autodelete**. In the field provided, type the number of days you want to retain the log files before deleting them. If you enter one (1) in this field, the program will save logs for the current day and the day before. The maximum number of days you can type is 90.

3. Click **Save**.
4. Click **Restore** to revert to the previous settings.

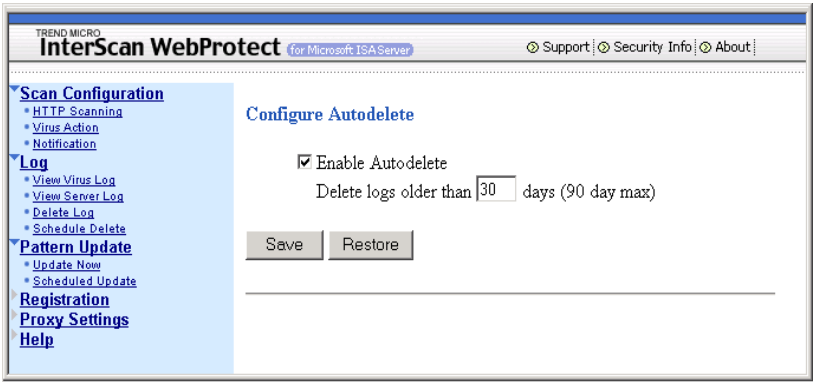


FIGURE 4-7. "Configure Autodelete" screen allows deletion of log files after a specified number of days.

Chapter 5

Updating the Virus Pattern File

This chapter describes InterScan WebProtect's virus pattern file and tells you how to update the file manually or automatically. Instructions for registering your InterScan WebProtect software (by mail or by using the Web browser user interface) are given early in the chapter. You will need to complete software registration before obtaining updated versions of the virus pattern file.

Topics included are:

- Registering for Virus Pattern File Updates
- Renewing Your Maintenance Agreement
- Updating the Virus Pattern File
  - Updating the Virus Pattern File Manually
  - Scheduling Automatic Virus Pattern File Updates
- Proxy Settings

Registering for Virus Pattern File Updates

Updating your copy of the virus pattern file is easy once you register your InterScan WebProtect software with Trend Micro Inc. Just download the updated version from the Internet. You can update the file immediately or configure InterScan WebProtect for Microsoft ISA Server to automatically download the updated pattern file weekly or monthly.

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

You can register your InterScan WebProtect over the Internet.

To register over the Internet:

1. Go to the WebProtect console and click **Registration**.
2. Enter all of the requested information and click **Register** to register your InterScan WebProtect program. To revert to the previous settings, click **Restore**.

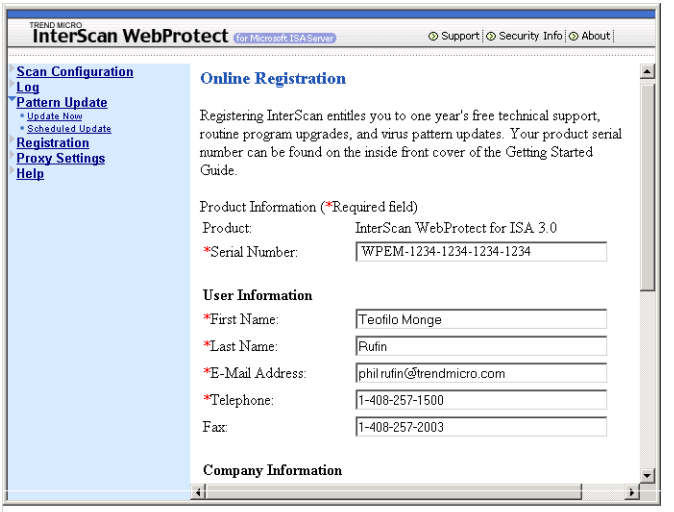


FIGURE 5-1. Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your 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. Your 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 discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

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

Renewing Your 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 your 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 your protection for a year, will be sent by post to the primary company contact listed in your company's Registration Profile.

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

`https://olr.trendmicro.com`

You are prompted to enter a login ID and password. To view your Registration Profile, type the login ID and password created when you first registered your product with Trend Micro (as a new customer), and click **Login**.

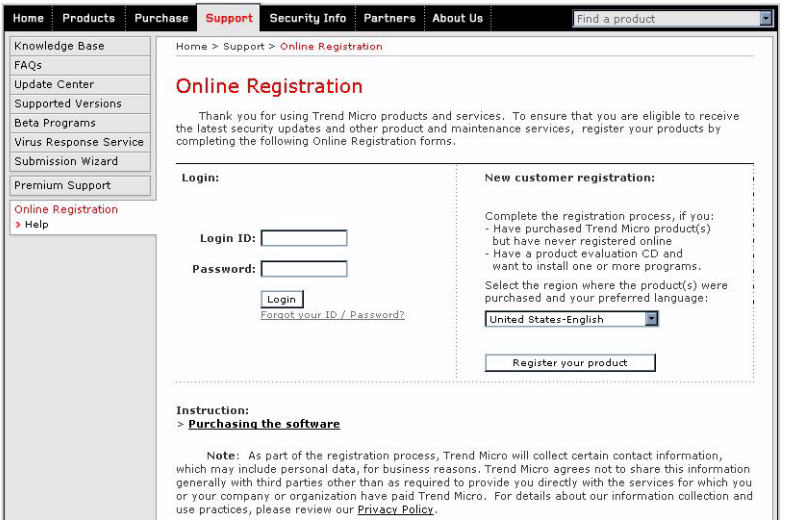


FIGURE 5-2. Trend Micro Online Registration screen, used to enter or update your Registration Profile.

Updating the 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 threats such as Trojan horses, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly pernicious threat is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature (see *About ActiveUpdate* starting on page 1-5 for details) 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, etc. to get the latest file. Trend Micro recommends that you schedule automatic updates to occur no less often than weekly, and this is the default setting for all products that are shipped. 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 all the new viruses 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. Since each virus contains a unique "signature" or string of tell-tale characters that distinguish 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.

Note: ActiveUpdate also supports incremental updates. Rather than download the entire five or six megabyte file each time, the ActiveUpdate feature can download only the portion of the file that is new and append it to the existing pattern file. Especially for networks running hundreds of individual desktop products, ActiveUpdate can save considerable bandwidth.

Pattern files use the following naming format:

`lpt$vpn.###`

where ### stands for the pattern version (for example, 400).

To distinguish a given pattern file with the same pattern version and a different build number, and to accommodate pattern versions greater than 999, the WebProtect for ISA Server 3.1 console displays the following format:

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

- `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

- `build number`—this represents the patch or special release number and contains two digits

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (sometimes several times per week), and recommends you to set a daily automatic update. Updates are available to registered WebProtect users.

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

Updating the Virus Pattern File Manually

The virus pattern file can be updated manually or you can use scheduled updates to have InterScan WebProtect stay current with the latest virus pattern file. If you use a proxy server to access the Internet, you need first to configure the Proxy Settings before updating WebProtect. To update the virus pattern file manually, go to the main menu and select **Pattern Update > Update Now**. The **Update** screen appears.

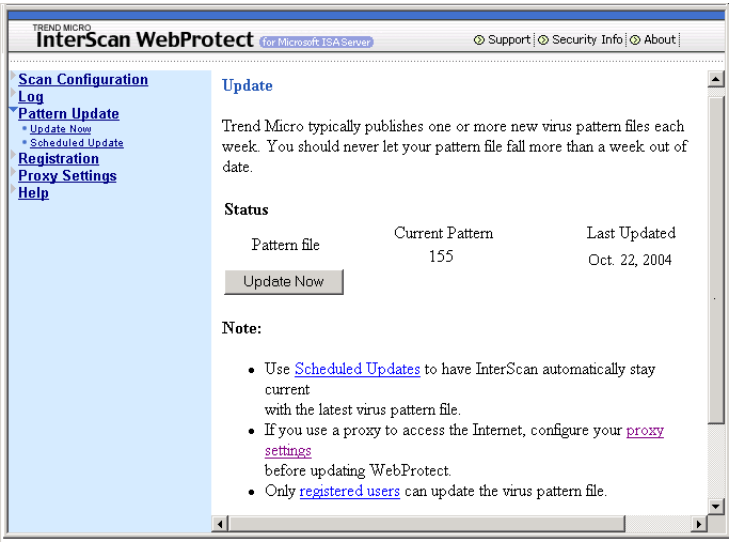


FIGURE 5-3. Always update the virus pattern file.

If the virus pattern file on your server is already up-to-date, the following message appears:

```
Pattern file is up to date.
```

Otherwise, a **Downloading Pattern** screen appears, which displays the update status, the version number of the new virus pattern file, and the version number you are replacing.

InterScan WebProtect displays a confirmation message to verify that the download was completed successfully.

Scheduling Automatic Virus Pattern File Updates

To enable scheduled updates:

1. Open the WebProtect console and select **Pattern Update > Scheduled Update**. The **Scheduled Pattern File Updates** screen appears.
2. Select **Enable Scheduled updates**.
3. Under **Start Time**, select the time of day that the virus pattern file needs to be updated.

   Under **Repeat interval**, you can choose **Daily** or **Weekly** from the drop-down menu.

   Under **Day of week**, select the day of the week for updates
4. Click **Restore** to revert to the previous setting.
5. Click **Save** to save and activate the new configuration.

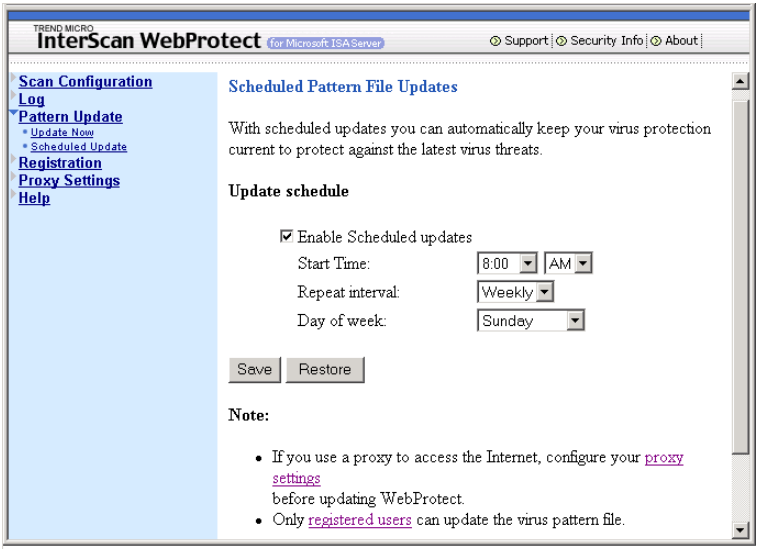


FIGURE 5-4. Configure the proxy settings if you are using a proxy server to access the Internet.

Proxy Settings

WebProtect needs the proxy information in order to connect to Trend Micro's update server for pattern file updates and to send your initial registration information.

To use a proxy server:

1. Open the WebProtect console and click **Proxy Settings**.
2. Enter the IP address (or server name) and service port of the proxy server in the fields provided. For proxy authentication, type the user name and password for verifications.
3. Click **Restore** to revert to the previous settings.
4. Click **Save** to save and activate the new configuration.

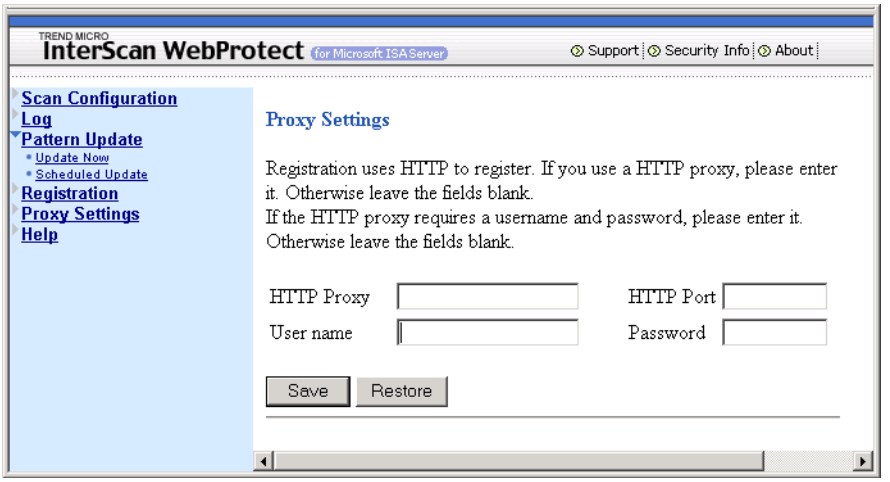


FIGURE 5-5. Make sure that you enter the correct proxy name and port number.

Chapter 6

Technical Support and Security Information

A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support 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.

If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users.

- To view a list of the worldwide support offices, go to:

  `www.trendmicro.com/support`

- To get the latest Trend Micro product documentation, go to:

  `www.trendmicro.com/download/`

In the United States, Trend Micro representatives can be reached via phone, fax, or email. Our Web site and email addresses follow:

www.trendmicro.com
support@trendmicro.com

For regional contact information and the specific technical support numbers for all the regional and worldwide offices, open the WebProtect console and click **Support**.

General US phone and fax numbers follow:

```
Voice:          +1 (408) 257-1500 (main)
Fax:            +1 (408) 257-2003
```

Our US headquarters is located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```

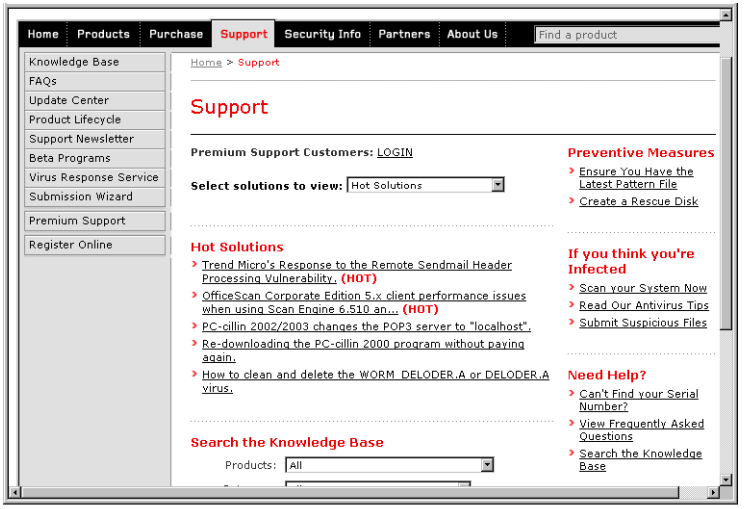


FIGURE 6-1. Trend Micro Technical Support site.

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988 by Steve Chang, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway–gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of threats to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop

viruses and other malicious code from a central point, before they ever reach the desktop.

To make this possible, TrendLabs (see *TrendLabs* starting on page 6-9 for more details) provides continuous 24 x 7 coverage to Trend Micro customers around the world.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia–a global organization with more than 1,800 employees in 25 countries.

Trend Micro products are sold directly, and through a network of corporate, value-added resellers and service providers. For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

`http://www.trendmicro.com`

Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

`http://www.trendmicro.com/en/about/contact/overview.htm`

Note: The information on this Web site is subject to change without notice.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

`http://kb.trendmicro.com`

About Scan Engine Updates

By storing the most time-sensitive virus information in external data files such as the virus pattern file, the anti-spam database, and outbreak protection policies, Trend Micro is able to minimize the number of scan engine upgrades 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`

FIGURE 6-2. Where to find the current version of the scan engine

Knowledge Base

Trend Micro Knowledge Base is an online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://kb.trendmicro.com

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

For top solutions for InterScan WebProtect, visit the following site:

http://kb.trendmicro.com/solutions/default.asp?show=prod&cmbProductTopSoln=40

Known Issues

Known issues are features in your WebProtect software that may temporarily require a workaround. Known issues are typically documented in the Readme document you received with your product. Readme files for Trend Micro products can also be found in the Trend Micro Update Center:

`http://www.trendmicro.com`

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com/solutions/`

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojan horse programs, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com`

Click **Submit a suspicious file/undetected virus**. The following screen displays.

FIGURE 6-3. Submission Wizard screen

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file to identify and

characterize any threats it may contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

If you prefer to communicate by email message, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers
- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters
- Read about TrendLabs, Trend Micro's global antivirus research and support center

To open Security Information:

1. Open the WebProtect console.
2. Click **Security Info**.

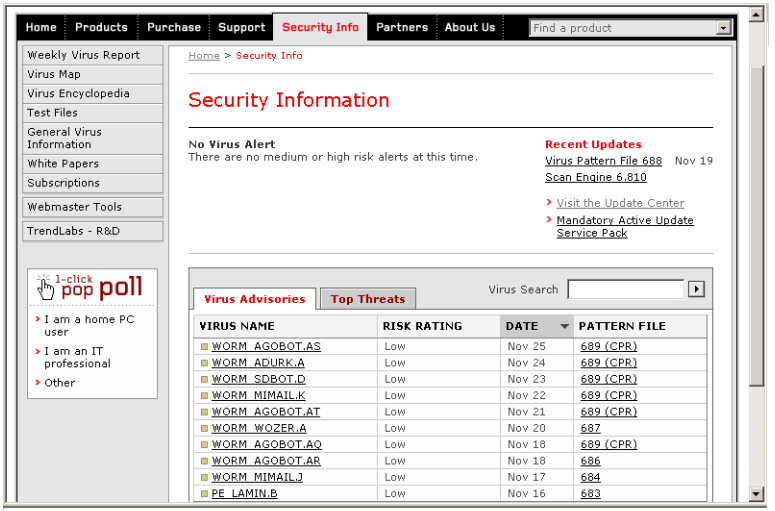


FIGURE 6-4. A multitude of virus and product information is available from the Security Information Center.

TrendLabs

TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila,

Taipei, Munich, Paris, and Irvine, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Damage Cleanup Services

Trend Micro Damage Cleanup Services help restore your Windows system after a Trojan attack. A Trojan, like a virus, attacks your system (but unlike a virus, a Trojan cannot self-replicate).

When a Trojan is executed, you will likely experience unwanted system problems in operation, and sometimes loss of valuable data. These are indications that you should run Trend Micro Damage Cleanup Services on your system.

Two versions of Damage Cleanup Services are available at no charge–one for Trend Micro customers, and one for the general public. Download Damage Cleanup Services from the following Web site:

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

Both versions support the following:

- Terminates malware instances in memory
- Removes malware registry entries
- Removes malware entries from system files
- Scans for and deletes malware copies in local hard drives

Troubleshooting

Obtain the latest troubleshooting information for InterScan WebProtect at the following site:

http://kb.trendmicro.com/solutions/default.asp?show=prod&cmbProductTopSoln=40

The following issues are the top 20 Knowledge Base solutions for InterScan WebProtect for ISA:

Problem (1): Users are unable to manually update the Scan Engine of InterScan WebProtect 3.0 for Microsoft ISA Server and the following message is being received:

```
vsapi32.dll is being used
```

Solution (1): Resolve this issue using the following procedure:

1. Disable the InterScan WebProtect Filter from the ISA Management MMC snap-in.
2. When the ISA Server Warning appears, select **Save the changes and restart the service(s)**.
3. Download the latest VSAPI or Scan Engine for WebProtect from Trend Micro's www.antivirus.com.
4. Extract the new vsapi32.dll file into the `\Winnt\system32` folder, overwriting or replacing the existing file.
5. Enable the InterScan WebProtect Filter or reboot the WebProtect machine.

Problem (2): How can the virus pattern file for InterScan WebProtect 3.0 for Microsoft ISA Server be updated using the Main Window?

Solution (2): Resolve this issue using the following procedure on the InterScan WebProtect machine:

1. Open the WebProtect console and click **Registration**.
2. Fill up the registration form and click **Register**.

   The product serial number can be found:

   - On the product registration card included with the software.

- On the outside front cover of the printed product documentation.
- By writing to a Trend Micro sales representative at sales@trendmicro.com.

3. After registration has been successfully completed, click **Pattern Update > Update Now**.
4. Click **Update Now**.

Note: Users must register over the Internet to be able to receive or download pattern file, scan engine, and product updates.

Problem (3): Users of InterScan WebProtect for ISA 3.1 have old pattern files inside the InterScan WebProtect folder.

Users did the following:

- Deleted the `AU_Temp` directory (`D:\Program Files\Trend\InterScan\WebProtect\cgi-bin\AU_Temp`)
- Deleted the Internet Explorer cache.
- Edited the `Server.ini` file and changed the `MergeCount` value: `MergeCount=0`.
- Performed another update.
- Set up the Internet Guest account `IUSER_` to have at least a "write" permission on the `\Program Files\Trend\Interscan\WebProtect` folder.

Solution (3): To resolve the problem, apply hot fix 1017. You find more information about this hot fix in the Readme file. Refer to Solution 19175 of Knowledge Base for hot fix 1017 attachment

Contact Trend Micro Technical Support to request for this hot fix. Premium Support Program (PSP) clients can contact their Technical Account Manager (TAM) directly.

NOTICE: This hot fix was developed as a workaround or solution to a customer-reported problem. As such, this hot fix has received limited testing and has not been certified as an official product update. Consequently, THIS HOT FIX IS PROVIDED “AS-IS.” TREND MICRO MAKES NO WARRANTY OR PROMISE ABOUT THE OPERATION OR PERFORMANCE OF THIS HOT FIX NOR DOES

IT WARRANT THAT THIS HOT FIX IS ERROR-FREE. TO THE FULLEST EXTENT PERMITTED BY LAW, TREND MICRO DISCLAIMS ALL IMPLIED AND STATUTORY WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

To install Hot Fix 1017:

1. Copy the `Patchw32.dll` hot fix file to the `\cgi-bin` directory.
2. Perform the pattern update.

Problem (4): The following system message appears after clicking **Update Now** under **Pattern Update > Manual Update** of the WebProtect console:

```
"FAIL - CreateFile()"
```

WebProtect is running on a Windows 2000 Environment.

Solution (4): To resolve this issue, check and modify the permissions of the WebProtect folder.

The Internet Guest account `IUSER_<servername>` needs to have at least a "write" permission to the `<root>\Program Files\Trend\Interscan\WebProtect` folder.

Note: Refer to Solution 10181 of Knowledge Base for more information on setting the permissions on the WebProtect folder.

Problem (5): When initiating a large download sized at several hundred MB, Microsoft ISA starts downloading the file, and it appears in the `%systemroot%\winnt\temp` directory as a file called `wp-virXXX.tmp`. Once the download is finished in the ISA box, InterScan WebProtect 3.0 scans the file before ISA serves the file to the user.

Before, `api _tempnam()` was used to generate the temporary file name with `\[WebProtect Program Directory]\isapi` passed as the parameter for the temporary file directory. However, this call would generate the `wp-virXXX.tmp`

under the `%systemroot%\winnt\temp` if the TMP environment variable is not configured or if the directory specified by TMP does not exist.

By default, the Windows NT environment does not have a pre-defined TMP environment variable. But in Windows 2000, `%System%\temp` is defined as the default TMP. So for Windows NT, the `wp-virXXX.tmp` file is created in the WebProtect program directory, but under `%System\temp` in Windows 2000.

Solution (5): Resolve this issue using the following procedure:

1. Refer to Solution ID: 10726 of Knowledge Base and download the attached `isapivir.zip`, which contains an updated `isapivir.dll` file.
2. Follow the installation instructions outlined in the ReadMe.txt file included in `isapivir.zip`.

   With this update, InterScan WebProtect will now generate the temporary file under the `\Program Files\Trend\Interscan\Webprotect\Isapi` directory.

Note: Since the new API only accepts 3 characters, the new temporary file name used will be wp-XXX.tmp, instead of wp-virXXX.tmp.

Problem (6): How to disable the InterScan WebProtect Filter from the ISA Management

Solution (6): Perform the following:

1. Open the ISA Management Console.
2. Go to **Servers and Arrays > Extensions > Web Filters**.
3. On the right pane of the WebProtect console, highlight **Interscan WebProtect Filter** and go to **Properties**.
4. Under **General**, clear **Enable this filter**.
5. Click **Apply**.
6. Enable **Save the changes** and restart the service(s).
7. Click **OK**.

Problem (7): How to apply a Controlled Pattern Release (CPR) to InterScan WebProtect 3.0 for MS ISA server?

A CPR is a pre-release version of a Trend Micro virus protection database. It is designed to provide customers with advanced protection against the latest computer viruses and serve as an emergency patch during a virus threat or outbreak.

A CPR has received only preliminary testing and has not yet been approved for release in accordance with Trend Micro's quality assurance procedures.

Solution (7): Apply the Controlled Pattern Release by doing the following:

1. Go to the **Controlled Pattern Release** screen.
2. Read the disclaimer. If you agree to the terms and conditions of using the Controlled Pattern File Release, click **I Accept**.
3. Download the Controlled Pattern Release (CPR) file to a temporary directory.
4. Stop the WWW service. From the Windows desktop, click **Start > Settings > Control Panel**.
   - For Windows NT users, double-click **Services**.
   - For Windows 2000 users, click **Administrative Tools > Services**.
5. Extract the pattern file (`lptxxx.zip`, where "xxx" is the version number) to the `\Progfiles\Trend\InterScan\WebProtect` directory.
6. Open the WebProtect console and click **Pattern Update > Update Now**. Users should see the new pattern file in the **Update Now** screen.
7. Start the WWW service. From the Windows desktop, click **Start > Settings > Control Panel**.
   - For Windows NT users, double-click **Services**.
   - For Windows 2000 users, click **Administrative Tools > Services**.

Problem (8): What to check when the New Pattern File Numbering Format (NPF) Service Pack for InterScan WebProtect for ISA 3.0 cannot be installed. This service pack provides support for the new pattern file numbering format.

Note: Version 3.1 supports the new pattern file numbering format.

Solution (8): Troubleshoot WebProtect using the following procedure:

1. Check the installation log of the service pack and see which file(s) the installer failed to update. The installation log file is `$iswp_dir\Temp\PatchBackup\3.00\yyyymmdd\Installation.log`.
2. Manually install the files using this procedure:
   a. Shut down the following services:
      - World Wide Web Publishing Service (Web service of the Internet Information Server)
      - Microsoft Web Proxy (proxy service of ISA)
   b. Extract the executable file of the service pack to a temporary directory.
   c. Go to the `$sp_directory\PatchFiles\ENU` directory.
   d. Locate the patch-files that were not copied onto the server and manually copy them.
      - `\%WINNT%: OS' system directory.`
      - `\cgi-bin: $iswp_dir\cgi-bin`
      - `\isapi: $iswp_dir\isapi`
      - `help: $iswp_dir\help`
   e. Restart the Web service of the IIS and the proxy service of ISA to load the patch-files.

To confirm that the NPF Service Pack of ISWP for ISA Server 3.0 was correctly installed, open the WebProtect console and click **About**. It must contain the following information:

```
Product information:

Version: 3.0

Build: 2008

Pattern file: 1.xxx.00

Scan engine: 6.810-1005

Serial number: aaaa.bbbb.cccc.dddd.eeee

This product is licensed to:
```

where xxx is the version of the latest pattern file in the `$iswp` directory.

If the problem was not resolved by the above-mentioned procedure, contact Trend Micro Technical Support and provide them the following:

- `$iswp_dir\Temp\PatchBackup\PatchHistory.txt`
- `$iswp_dir\Temp\PatchBackup\3.00\`
- Version and build number of ISWP
- System information of the operating system (that is, platform name and SP level)

Problem (9): After the EICAR test virus is detected by InterScan WebProtect 3.0 for Microsoft ISA Server, no mail notification was received by the designated SMTP address even though it has already been configured earlier.

Solution (9): Resolve this issue using the following procedure on the InterScan WebProtect machine:

1. Open the WebProtect console and click **Scan Configuration > Notification**.
2. Under **Notification**, enable **Notify the following**.

   Check and make sure that the correct, full email address(es) of the intended recipient(s) is correctly listed in **Notify the following**. Multiple recipients must be delimited using a comma or ",".
3. Under **Notification Server**, check and make sure that the correct Hostname (or IP address) and SMTP Port information has been entered.
4. Click **Save** to store any new settings.
5. In the Windows desktop, open the Service Control Manager by clicking **Start > Programs > Administrative Tools > Services**.
6. Highlight the Microsoft Web Proxy service and click **Restart Service**.

Problem (10): Scheduled update of the pattern file or scan engine is not working for InterScan WebProtect 3.0 for ISA. However, **Update Now** is working properly.

Solution (10): This issue generally occurs when the **Scheduler** process is not running on the ISA server machine. **Scheduler** calls the update process when the computer time (hour) equals the scheduled hour configured in the WebProtect console.

Scheduler is only a process and has no service associated with it. It is dependent on the ISA service, and by default, should automatically load when the **Microsoft ISA server control** service starts.

Resolve this issue using the following procedure:

1. Open the Windows Task Manager and check if the **Scheduler** process is running.
2. If the process is NOT running, stop the **Microsoft ISA Server Control** service, which will stop all other services dependent on it.

   This can be accomplished from the Control Manager Services List.
3. Manually restart all the services stopped in the previous step, including the **Microsoft ISA Server Control** service.
4. Check the Task Manager again if the **Scheduler** process is running.

   If the process is still NOT running, the scheduler.exe file may be corrupted or missing.
5. Download the attached scheduler.zip from Solution ID: 10977 of Knowledge Base and extract its contents into the `\[WebProtect Program Directory]\utils` folder, overwriting any existing files.
6. Restart the **Microsoft ISA** services.

Problem (11): Streaming media allows a user to view or hear a portion of a media file without completely downloading it. This type of traffic need not be processed by InterScan WebProtect 3.0 for ISA and should be skipped to prevent buffering or slow response on the client side.

Solution (11): Ensure that your system meets the following requirements to identify the correct MIME type and add it to Interscan WebProtect's exclusion list.

Applying Build 1040

Build 1040 and above has two new parameters so that administrators can specify the streaming media files for exclusion. These are the following.

```
SkipScanStreamingMedia=yes/no
```

```
SkipScanStreamingMediaType=useragent:mimetype
```

Ensure that the current WebProtect installation is running build 1040 at the very least. Contact Trend Micro Technical Support to request for this build.

Note: Trend Micro carefully evaluates if the customers' issues and environment matches what each hot fix or build number is intended for. This helps ensure that our customers receive only those hot fixes or build applicable to their situation.

Using a Sniffer

With the use of a sniffer, capture the traffic from a Web proxy client to the ISA server. You can download a free sniffer at the Ethereal Network Analyzer site.

Ethereal has a function to trace or follow a TCP stream. Use this function to locate both the request and response packet that can help you identify the user agent and MIME type.

Modifying Intscan.ini

After identifying the correct MIME type, modify intscan.ini and add the new parameters with the specified MIME type and user agent. Here is an example:

```
SkipScanStreamingMedia=yes

SkipScanStreamingMediaType=NSPLAYER:video/x-ms-asf
```

Restarting the Service

Restart the Web proxy service of ISA. The stream should display normally now.

You can download a video file that shows how you can implement these steps. Here is the necessary information:

```
FTP address: ftp-download.trendmicro.com.ph/Gateway/jeff/

Username: ftpuser

Password: ftp-trend

Filename: 14667.zip
```

Note: You can find commonly used video/ and audio/ MIME subtypes at the Microsoft TechNet Web site.

However, since some Web servers use MIME types other than the ones listed in this site, it is important for administrators to know how to identify the correct MIME type using a network sniffer.

Problem (12): Trend Micro's WebProtect v3.0 is deployed with Microsoft's Internet Security & Acceleration Server (ISA).

When a download manager like Gozilla and Getright are used to download a file, MS-ISA reports that the actual downloaded data is bigger than the actual size of the file. This usually leads to issues with the traffic-reporting software.

Solution (12): Web Protect sends trickle data to the client while downloading files. Since a traffic-reporting software counts all data sent from a connection stream, the trickled data, as well as the original size of data, are counted as one. Therefore, the reported file size is greater than actual size of the original file. The downloaded data will have the same size as the original file. The downloaded file is not corrupted.

Problem (13): When a user tries to save configuration changes to InterScan WebProtect 3.0 for Microsoft ISA Server in the WebProtect console, the following message appears:

```
Error: Unable to save configuration data
```

Solution (13): When Interscan WebProtect v3.0 is installed, by default, the anonymous account does not have the necessary permission on the WebProtect program folder. But the client has options to resolve this issue:

Option 1 (Do not allow anonymous access)

1. Open the IIS management console.
2. Right-click **Default Web Site** and select **Properties**.
3. Click **Security**, and then click **Edit**.
4. Clear **Allow anonymous access**.
5. Click **OK**.

Note: IIS will prompt the user/administrator for a user account when WebProtect's console is opened.

Option 2 (Allow anonymous access)

1. Open Windows Explorer.
2. Look for the WebProtect program file. This is usually in `< root >\Program Files\Trend\Interscan\WebProtect`.
3. Add the Internet Guest account, `IUSR_<server name>`, and give full permission to this account.

Note: Option 2 is not a secure option, but is the most convenient.

Problem (14): There are cases that even after registering their WebProtect 3.0 for ISA server, messages indicating that the 30-day trial or evaluation period has expired are still be received or displayed.

Solution (14): Resolve this issue using the following procedure:

1. Backup the WebProtect config file as a precautionary measure, which by default is:

`C:\Program Files\Trend\Interscan\WebProtect\intscan.ini`

2. Remove InterScan WebProtect for ISA server.
3. Reinstall WebProtect for ISA server, entering a valid serial number when prompted during installation.
4. Register the product using the **Registration** page of the WebProtect console.

Problem (15): How to upgrade from InterScan WebProtect (ISWP) for ISA server 3.0 to version 3.1.

Note: The installer requires that the server be restarted after the installation. Schedule your resources accordingly.

Solution (15): Upgrade ISWP for ISA server 3.0 to version 3.1 using this procedure:

1. Back up the `$iswp_dir/intscan.ini` file before running the setup program as it contains your serial number, which you will use during upgrade process. Backing up will also be useful when you need to roll back from 3.1 to 3.0 as it contains your original settings.
2. Copy the installation files from the Trend Micro Web site or install the media to a directory on the target server.

   You can find the serial number information in the **[Registration]** section of the `intscan.ini` file as shown below:

   ```
   [Registration]

   Serial=aaaa.bbbb.cccc.dddd.eeee
   ```

3. Run the setup program and follow the wizard to upgrade ISWP for ISA Server 3.0 to version 3.1.

   The wizard provides you with three upgrade options:

   - Option 1: Keep the configuration and overwrite all other files
   - Option 2: Overwrite all files including configuration files
   - Option 3: Exit setup

   Choose the first option if you wish to preserve settings from version 3.0. If you wish to use the default settings of version 3.1, choose option 2. To cancel the upgrade, select the third option.
4. Restart the ISA server.

To confirm that ISWP for ISA Server 3.0 has been upgraded to version 3.1, open the WebProtect console and click **About**. It must contain the following information:

```
Product Information:

Version: 3.1

Build: 1017

Pattern file: 1.xxx.00

Scan engine: 6.810-1005

Serial number: aaaa.bbbb.cccc.dddd.eeee

This product is licensed to: OS' registration information
```

where `xxx` is the version of the latest pattern file in the `$iswp` directory.

Problem (16): The Microsoft ISA server uses InterScan WebProtect for ISA 3.x or lower to scan HTTP traffic. At the same time, Web-Server publishing is enabled in ISA to publish the content of Internet Information Server (IIS).

Is it possible for WebProtect to scan the HTTP traffic that is coming in and going out of the IIS? Can WebProtect protect the IIS from viruses that exploit IIS vulnerabilities such as Code Red?

Solution (16): InterScan WebProtect cannot scan the HTTP traffic for the Web-Publishing service of ISA; therefore, it could not protect the actual Web server from viruses such as Nimda and Code Red.

InterScan WebProtect for ISA only acts as a plug-in for the ISA server and the only HTTP traffic that it scans are those that are being routed to it by the ISA.

ISA uses a different connection for the HTTP access rules and for the Web-Publishing service. The only HTTP traffic that is being routed to WebProtect falls under the "HTTP access rules".

To protect the IIS server from Code Red and Nimda, use ServerProtect. This antivirus software protects the actual server and all programs it is running. With ServerProtect, files being written to the IIS will be subjected to scanning.

Problem (17): When installing InterScan WebProtect 3.x for Microsoft ISA, the following message is received:

```
Event ID 14146: ISA Server failed to load Web Filter DLL
D:\ISAServer\..\InterScan\WebProtect\isapi\isapivir.dll.
```

The error code shown in the **Data** area of the **Event** properties indicates the cause of the failure.

Solution (17): Resolve this issue by installing InterScan WebProtect in the ISA folder or in an ISA sub-directory. This will allow the WebProtect Web Filter path to be properly registered and the `isapivir.dll` file can be successfully loaded.

For more information, visit Microsoft's support.microsoft.com: Article Q244223.

Problem (18): When WebProtect for ISA is enabled, HTTP downloads are drastically slow. This is reflected on the estimated download time for large files.

Solution (18): The estimated download time may not be accurate. What happens is that ISA proxy downloads the file and sends the file to WebProtect for virus scanning. Then, the file is sent back to the ISA proxy for delivery to the workstation.

WebProtect holds the file until it is scanned entirely, afterwards it returns the file to ISA. So, if the file is quite large, it might take a while before the workstation receives the file.

It is also possible that at the start of a download, the data transfer is slow; but once the whole file is scanned for viruses, only then can data transfer speed up.

The administrator/user may want to download a test file and see if the estimated download time is accurate or not.

If the estimated download time is accurate (which confirms slow download), perform the instructions below:

1. Open the WebProtect console and click **Scan configuration**.
2. Enable **HTTP scanning**.
3. Locate for the "trickle function" utility. This field reads: "send xxxx bytes of data for every yyy kb data received".
4. The trickle function allows WebProtect to send some part of a file to the workstation (without being scanned), so that browser time-outs can be prevented. By default, the trickle function is set to:

   ```
   send 1024 bytes of data for every 512 kb of data received.
   ```

5. Set the values above, to: "send 100 bytes of data for every 50kb of data received". See if the problem persists.
6. If the problem persists; make trials to find values that will optimize download time.

Problem (19): The administrator would not like other users to browse the Internet, if the WebProtect filter is not loaded into ISA. Thus, the administrator would like the Web Proxy service to stop, if WebProtect is not loaded.

Solution (19): Stopping the Web proxy service if WebProtect is not loaded, can be done by using the monitoring feature of ISA.

1. Under **Monitoring Configuration** of ISA, select **ALERTS**.
2. Create a new alert for WebProtect, or use the existing alert **Component Load Fail**.
3. If the administrator would only like to receive an alert from WebProtect and other related Web Filters, select Web Filter from the list of components.
4. Set the action to **Stop Selected Services**, and then select **Web Proxy**.

   This will stop the Web Proxy service if a Web Filter component is not loaded.

Note: The rule above will apply to any Web Filter that fails to load, not only InterScan WebProtect for ISA.

Problem (20): Is Interscan WebProtect for ISA Server capable of detecting viruses during file transfer using MSN Instant Messenger?

Solution (20): No, infected file transfers via Microsoft Network or MSN Instant Messenger cannot be detected by InterScan WebProtect or ISWP for ISA Server.

MSN file transfers occur on a different port besides port 80, which is used by WebProtect for ISA Server to check/scan for viruses.

Resolve this issue by using InterScan WebProtect in combination with other Trend Micro enterprise antivirus solutions.

Index

P

R

S

T

U

V

W

Trend Micro Incorporated
10101 N. De Anza Blvd.
Cupertino, CA., 95014 USA
www.trendmicro.com

For Sales:
Tel: +1-408-257-1500 (outside US and Canada)
Fax: +1-408-257-2003

Item Code: WPEM31859/40408