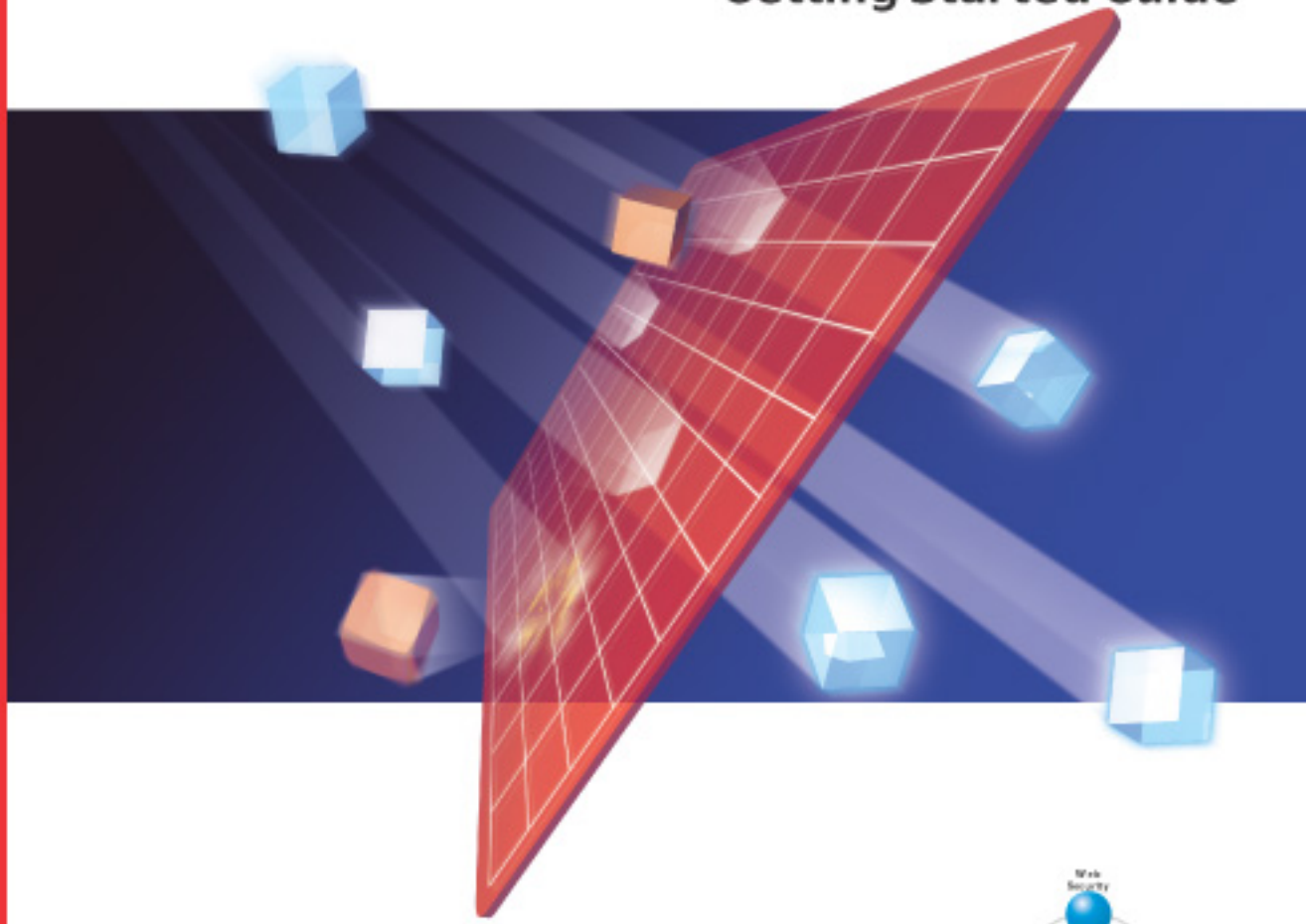
TREND MICRO™

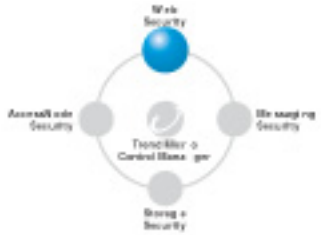
InterScan™ VirusWall™ 3

Virus protection for Internet gateways

CSP Edition

Getting Started Guide





TREND MICRO™

Document Part No. IVEM31569/30722

Release Date: August 2003

Protected by U.S. Patent No. 5623600, 5889943, 5951698 and 6119165

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

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

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

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

Table of Contents

Chapter 3: Getting Started

Chapter 4: Enabling SMTP, HTTP, and FTP Scanning

Chapter 5: Log Files and Resource Configuration

Chapter 1

Introduction

The Content Scanning Protocol (CSP) was defined and developed by Trend Micro™ to allow partner Internet firewalls to support virus scanning through Trend Micro InterScan™ VirusWall™. Customers using supported firewalls can protect their internal network from virus infections and outbreaks with InterScan VirusWall CSP Edition.

Trend Micro™ InterScan™ VirusWall CSP Edition is a comprehensive antivirus solution for the Internet gateway. It analyzes SMTP, HTTP, and FTP traffic as an intermediate step before sending messages and files on to their final destination.

This chapter explains the virus and email content threats that InterScan VirusWall can stop at the firewall and introduces the program's main features:

- Proprietary scanning protocol developed by Trend Micro™
- Secure, Web-based console
- Uses pattern recognition and rule-based technologies to detect known and unknown viruses, including macro viruses
- Provides activity logs detailing system and virus events
- Active update of the pattern file weekly, daily, or even hourly
- Configurable performance optimization
- Built-in connection to online support

Introduction to InterScan™ VirusWall™ CSP Edition

Trend Micro™ InterScan™ VirusWall™ CSP Edition is a three-in-one Internet gateway antivirus program that detects and cleans virus-infected files before they enter or exit the corporate network. InterScan VirusWall scans the following three types of traffic for viruses:

- SMTP scanner monitors inbound and outbound email messages
- HTTP scanner checks for viruses and malicious Java and ActiveX applets
- FTP scanner ensures that all file transfers made via FTP are virus-free

How Does InterScan™ VirusWall™ Work?

At its most basic, InterScan VirusWall monitors all SMTP, 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`), InterScan VirusWall extracts the file from the message body to a temporary location and opens the copy for virus checking.

If the file is clean, InterScan VirusWall deletes the copy and releases the original for delivery to the SMTP, FTP or HTTP server, which delivers the file as usual. If a virus is found, a notification is issued and InterScan VirusWall takes the action configured: Clean, Delete, Move, or Pass.

Introduction to the Content Scanning Protocol

The Content Scanning Protocol (CSP) was designed and copyrighted by Trend Micro™. This manual describes the UNIX version of InterScan VirusWall CSP Edition 1.5. CSP 1.5 adds functionality such as improved performance, increased flexibility and reliability, and enhanced error and version control handling.

Protecting Against Email Threats

InterScan™ VirusWall CSP Edition protects against the following threats to your company's messaging system.

Antivirus Protection

Virus detection is performed using Trend Micro's 32-bit scan engine and a process called pattern matching. The scan engine uses the virus pattern file to compare the files travelling through your gateway with the binary patterns of known viruses. If a virus is detected, the scan engine will attempt to clean, that is, remove the virus code from the file. Trend Micro releases new virus pattern files as new viruses are detected.

Malicious Macros

Many types of file attachments, such as executable programs and documents with embedded macros, have the potential to harbor viruses. InterScan VirusWall uses the Trend Micro™ MacroTrap™, a heuristic scanning device that can detect both known and unknown macro viruses by analyzing the macro code within the files to detect virus-like behavior.

MacroTrap performs a rules-based examination of all macro code that is saved in association with a document. Macro virus code is typically contained as a part of the invisible template (.DOT, for example, in Microsoft™ Word) that travels with the document. Trend Micro's MacroTrap checks the template for signs of unknown Macro viruses by seeking out instructions that perform virus-like activity, for example, copying parts of the template to other templates (replication), or code to execute harmful commands (destruction).

Selective Scanning of MIME Files

Multipurpose Internet Mail Extensions (MIME) extend the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers. While MIME files contribute to the richness of Internet information exchange, MIME files are often quite large and can take a while to scan. In addition, MIME file names are sometimes quite large, which also adds to scan time. InterScan VirusWall contains selections to filter out this type of mail from scanning:

- SMTP scanner can block MIME files with attachment names longer than a specified number of characters
- HTTP scanner can exempt files from scanning based on configurable MIME types and subtypes

MIME header information contains a Content-Type field, which is used to specify the nature of the data in the body of a MIME object, by giving media type and subtype identifiers. You can configure selective MIME subtypes for exemption, such as certain types of application files, for example:

```
application/x-director, application/pdf
```

In this case, x-director and pdf files are exempt from scanning, but all other MIME application types are scanned.

Scanning Based on File Type

File scanning is based on the embedded file type or description, rather than the exact extension name. For example, if you select to scan files of type `.doc`, attachments of both `.doc` and `.dot` types will be scanned because they are both Microsoft™ Office document types, according to the embedded file description.

Blocking Files from HTTP Download

HTTP file blocking can be used to prevent users from downloading file types that have the potential to harbor viruses. You can block downloads of the file types `java`, `exec`, and `com`.

Detailed Virus and System Logs

InterScan VirusWall CSP Edition contains detailed virus logs which help administrators track down virus issues. Logs can be queried by scanning type (SMTP, HTTP, and/or FTP) and sorted by date. In addition, the Advanced Query option can be used to access logs by recipient name and/or virus name.

InterScan VirusWall's system log contains information on mail processing issues. You can configure the directory to store the system logs and the number of system logs to keep.

Where to Install InterScan™ VirusWall™ CSP Edition

InterScan VirusWall checks both inbound and outbound SMTP, HTTP, and FTP traffic for viruses. It can be installed on the same machine as your existing firewall server or on a dedicated machine.

You should install InterScan VirusWall CSP Edition inside a firewall. The idea is to have InterScan VirusWall listen for new connections on port 3300, scan the SMTP, HTTP, and FTP traffic it receives, and then route scanned traffic back to the original firewall.

InterScan VirusWall can be installed in the following configurations:

- **Same machine** — some firewall servers support installation of InterScan VirusWall CSP Edition on the firewall itself

- **Dedicated machine** —if the firewall server is on another machine, you need to specify the hostname (or IP address) and port for InterScan VirusWall

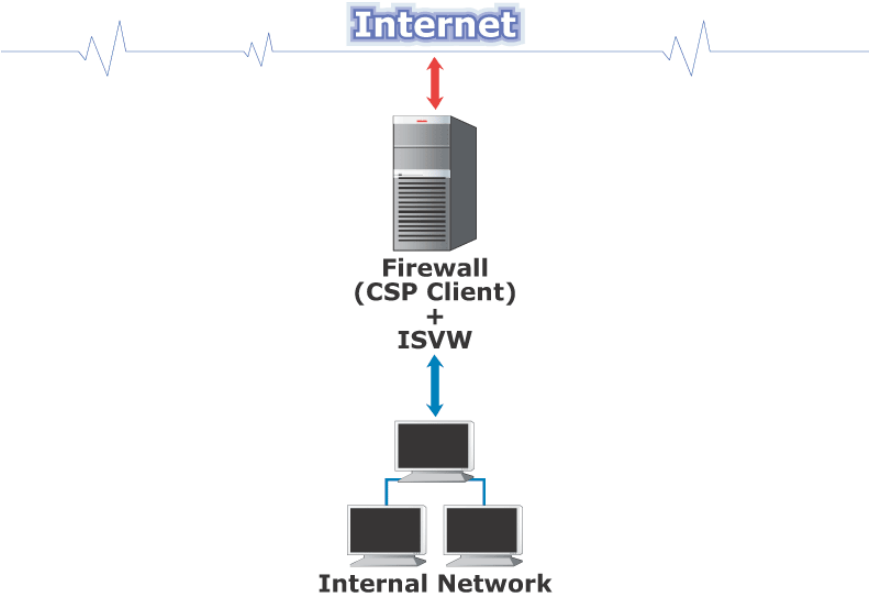


FIGURE 1-1 InterScan™ VirusWall™ CSP Edition installed on the Firewall server.

The following procedures occur in the InterScan™ VirusWall™ CSP protocol:

1. The firewall receives an application protocol (smtp, http, or ftp) request from a client and saves the request information.
2. When the firewall receives content (mail data, http response, ftp file) for this request from either the remote client (for example, http post, ftp put, smtp data) or remote server (for example, http get, ftp get), the firewall connects to the scanner over a socket and sends a scan request packet containing information in the request headers.
3. The scanner then scans the content and returns the scan result to the firewall.
4. The firewall routes the content to the receiver as usual.

The procedure is the same when the firewall is located on a dedicated machine. The only extra step required is configuring the firewall to route traffic to the InterScan VirusWall CSP Edition machine.

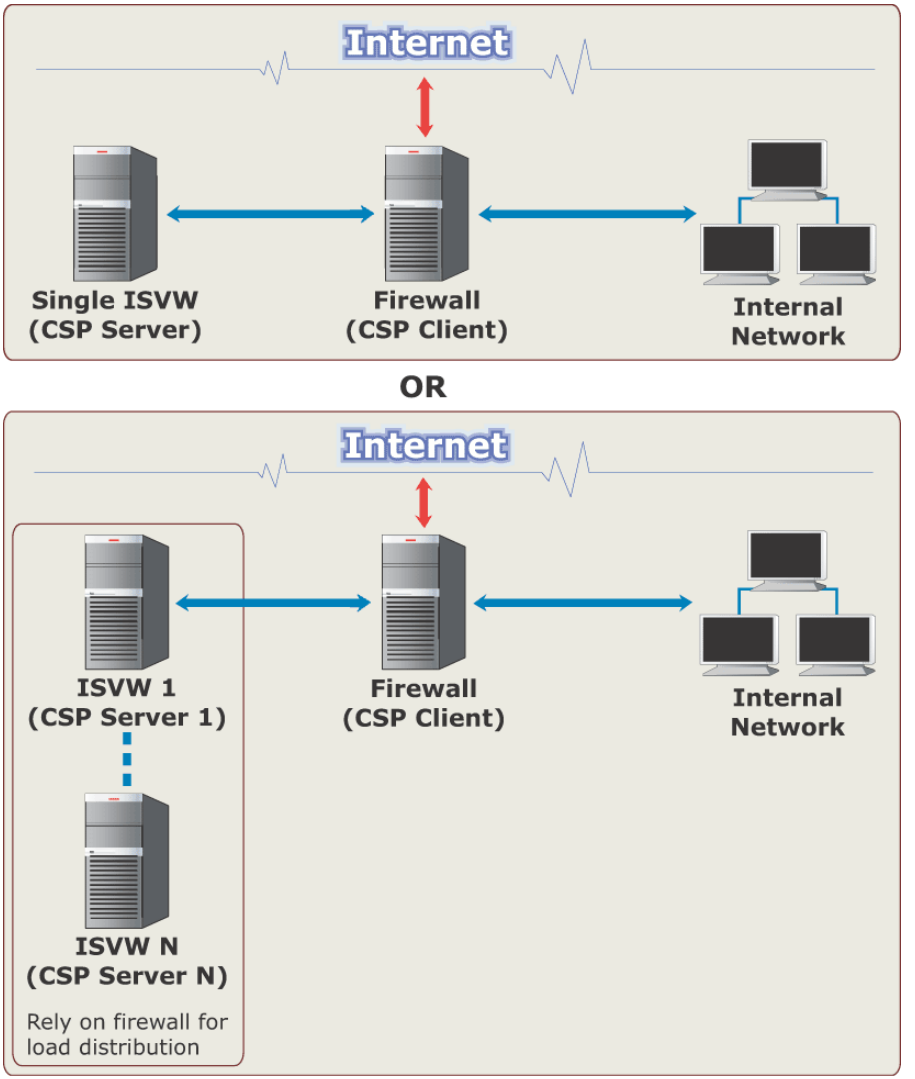


FIGURE 1-2. InterScan™ VirusWall™ CSP Edition installed on a dedicated machine, or several dedicated machines.

If the firewall has the capacity to do load balancing, you can install more than one CSP server to scan the SMTP, HTTP, and/or FTP traffic.

InterScan™ VirusWall™ CSP Edition Main Features

InterScan™ VirusWall CSP Edition includes the following features:

Management

- Advanced Performance: Its multithreaded design takes full advantage of multi-processor systems.
- Secure Web-based Management Console
- Integrated firewall/AV security solution
- Ease of management
- Transparency to corporate clients (no need to reset user proxies)
- Flexibility in re-routing SMTP, HTTP, or FTP or all three traffic types to ISVW for virus scanning
- Configurable resource optimization
- Manual or automated download of new pattern files, as well as a configuration option of how many previous pattern files to keep
- Detailed virus and system logs and automatic system log deletion
- Active registration from the InterScan VirusWall console

Scanning and Notification Features

- Macro scanning for SMTP, HTTP, and FTP traffic
- SMTP scan can block messages containing MIME files with attachment names longer than a specified number of characters
- HTTP scan allows designated MIME file types to be exempt from scanning
- HTTP scan allows blocking files by file type
- Notifies administrator, sender, and/or recipients with customizable message text when viruses are found
- Includes a Safe Stamp option to let users know when their mail has been scanned and is virus-free

Chapter 2

Installation

Installing InterScan™ VirusWall™ takes about ten minutes and should be performed from the machine where the program(s) will reside. If you are installing on a dedicated machine, allow another 10-15 minutes to configure your existing firewall to pass traffic to InterScan VirusWall.

In this chapter you will find step-by-step instructions for installing InterScan VirusWall CSP Edition. Also presented are instructions for:

- Minimum system requirements
- Starting and stopping InterScan™ VirusWall™ CSP Edition
- Opening the InterScan VirusWall Web Console
- Uninstalling InterScan VirusWall
- Installed Files
- Upgrading from the trial version

Minimum System Requirements

InterScan™ VirusWall™ CSP Edition has the following minimum system requirements:

- Solaris 7 through 9 on a Sun™ Ultra™ Sparc™ platform
- 256MB main memory (DRAM)
- Swap space should be 2 to 3 times the main memory
- 20MB disk space for InterScan VirusWall only
- At least 1GB disk space for operation (processing email messages)
- The InterScan VirusWall "temp" directory should be configured to 4 times the total number of connections (max_proc times thr_per_proc) configured. For example:

  max_proc = 25
  thr_per_proc = 5
  Average email size = 50K

  (25 X 5 X 50) X 4 = 25MB (InterScan VirusWall only)

Note: Insufficient temporary disk space may lead to program performance problems, up to and including program failure.

FireWall Support

- Lucent Brick 6.0
- NetScreen -100 and -500

Supported Internet Browsers

- IE 5.0 and above·
- Netscape 4.7 and above

Deciding Where To Install

You can install InterScan VirusWall on a dedicated server or the same machine as the firewall server, depending on the firewall type.

The following configurations are supported:

- Single CSP server with Firewall
- Multiple CSP servers with Firewall
- CSP server and Firewall on the same server

Note: A single firewall may be connected to multiple CSP servers if the firewall has the ability to perform load balancing.

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

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

In the case when firewall and CSP server is on the same machine, there is no need to transfer the data between firewall and CSP server. Instead, the firewall informs the InterScan VirusWall CSP Edition server the paths of the files.

Setup Sequence

InterScan VirusWall listens on port 3300 for SMTP, FTP, and HTTP connections, scans the traffic, then returns it to the firewall server. The SMTP server handles the actual delivery of the mail.

1. Install InterScan VirusWall on the Sparc machine.
2. Stop the Firewall server and add the InterScan VirusWall port, for example 3300.

3. Open the InterScan VirusWall configuration console (*http://hostname:8443/iscan/servlets/index.htm*).

Upgrading InterScan™ VirusWall™ CSP Edition

Note: Before Installing InterScan VirusWall CSP Edition, you must completely remove any existing version you may have.

When you remove InterScan VirusWall, the `intscan.ini` file is temporarily saved in the following directory: `/tmp/iscan_old.`

Note: If the `tmp` directory is deleted prior to reinstalling InterScan VirusWall, you will lose your previous customized values.

During the Base System installation, the script creates a new `intscan.ini` and saves your old `intscan.ini` file to the following directory: `/opt/trend/iscan/old_log_ini`. The new intscan.ini file contains default installation values.

To retain your customized `intscan.ini` values, you must manually replace the default values in the new `intscan.ini` file with your customized values. We recommend that you print out the old `.ini` file and use it to review each value in the new `.ini` file. Use any text editor to restore the old settings and save the new `.ini` file. When finished, start the InterScan VirusWall services.

Installing InterScan™ VirusWall™

The InterScan VirusWall setup includes scripts requiring superuser permission—log on as **root** before installing.

1. FTP the program files to a UNIX server and untar them.
2. From the directory containing the InterScan VirusWall installation files, type `./isinst` and press ENTER.
3. By default, InterScan VirusWall installs all available systems to subdirectories of `/opt/trend.` If you want to install to a different directory, type in the path and press ENTER.

4. The *Main Menu* appears, displaying the current system configuration.
   - None means the package is not installed. This is the typical value for first time installations.
   - Installed means the package exists on the server. Before installing the current version, be sure to uninstall any previous version.
5. Choose **1. Install InterScan VirusWall CSP Edition** to start the installation.
6. The BASE and CGI Admin are required for CSP installation. Choose option **4** to start the install of all components. Continue to follow the screen prompts to complete the installation.
7. Once the InterScan VirusWall Base and Admin systems are installed, you are prompted to enter a serial number.

   Press **Enter** without entering a serial number to install the 30-day trial version. This version of InterScan VirusWall is fully functional but will expire after 30 days, at which time it should be upgraded or removed. For information on how to buy, please refer to the following URL:

   `www.trendmicro.com/buy`
8. Once you have completed the installation, select **Exit**. InterScan VirusWall will then automatically start the services with new `intscan.ini` settings.

Opening the Web Console

After installation, InterScan VirusWall automatically starts the InterScan VirusWall daemon. Although InterScan VirusWall is configured to run on a robust set of default values, you should at least open the Web console and confirm the settings.

1. Open a Web browser, then enter the InterScan VirusWall URL followed by the port (**8443)**. The IP address can be either the domain name or number of the InterScan VirusWall machine. The port used for the Web Console is also user-configurable. For example:

   `https://domain:`*`port`*`/iscan/servlets/index.htm`
   `https://isvw.widget.com:8443/iscan/servlets/index.htm`
   `https://123.123.123.12:8443/iscan/servlets/index.htm`
2. The InterScan VirusWall console is password-protected. By default, both the user name and password are **`admin`**.

Note: The default password for the InterScan VirusWall console is blank. We recommend that you configure a password upon first use to prevent unauthorized changes to your policies. See *Changing the Management Console Password* starting on page 5-11 for more information.

The InterScan VirusWall console can be viewed through a Web browser from either the machine where the program was installed, or remotely across the network.

To view the console from another computer on the network, open ***https://<target server's IP address>:<target server's port>/iscan/servlets/index.htm*** in a Web browser. Using the target server's fully-qualified domain name (FQDN) instead of the IP address is also acceptable.

Note: As a security precaution, the InterScan VirusWall Web console times out after 20 minutes of inactivity, and automatically returns the user to the password-entry screen.

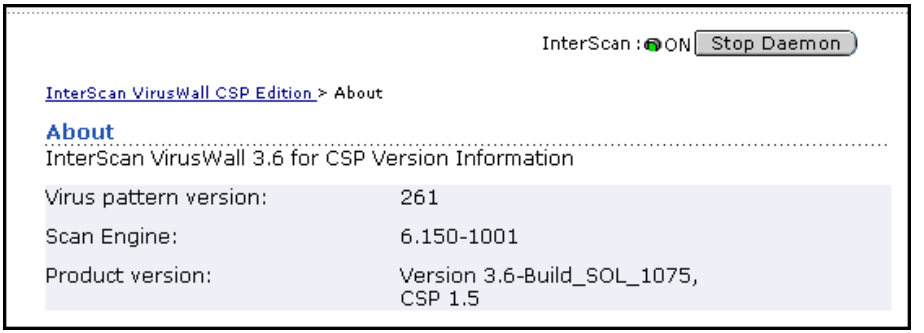


FIGURE 2-1. This InterScan VirusWall About screen, which shows the versions installed.

Starting and Stopping InterScan™ VirusWall™

By default, InterScan™ VirusWall™ CSP Edition services are enabled upon installation. The services can also be controlled, however, according to the following options:

- Enable/disable real-time SMTP, HTTP, and/or FTP scanning from the console
- Turn on/turn off the network flow to InterScan VirusWall from the console
- Turn on/turn off the network flow to InterScan VirusWall from the command line

Enabling/Disabling SMTP, HTTP, and/or FTP Scanning

To enable/disable real-time scanning from the InterScan VirusWall console,

1. From the InterScan VirusWall Web configuration menu, click **Scan**.
2. To enable or disable real-time scanning, click the respective service type:
   - **SMTP > Files to Scan**
   - **HTTP > Files to Scan**
   - **FTP > Files to Scan**
3. Click the checkbox to toggle scanning for that service.
4. Click the **Save** button.

WARNING! *If you disable virus scanning, the flow of traffic will continue, so use these options with caution.*

Turning On/Off the Daemon from the Console

To completely stop the flow of traffic to InterScan VirusWall, you can change the traffic flow status. Go to the top right of the InterScan VirusWall console:

1. Click **Stop Daemon** to turn all scanning and network flow to InterScan VirusWall off.
2. To re-enable scanning, click **Start Daemon**.

Turning On/Off the Daemon from the Command Line

To stop/start the flow of traffic to InterScan VirusWall from the command line, enter the following:

```
% /etc/rc2.d/S99ISscsp stop
% /etc/rc2.d/S99ISscsp start
```

Uninstalling InterScan™ VirusWall™

InterScan VirusWall's uninstall scripts require superuser privileges. You must be logged on as **root** to uninstall InterScan VirusWall.

To remove InterScan VirusWall:

1. Bring up the *Main Menu* by entering `./isinst` in the directory where your InterScan VirusWall files are located.
2. Choose **Option 2**, and follow the on-screen prompts to remove the service.
3. Choose **Option 4**. **Remove All InterScan VirusWall System**.

Installed Files

InterScan VirusWall makes the following changes to your system:

Table 2-1. InterScan VirusWall CSP Edition Installed Files

Directory	*Subdirectory*	*Files/Modification*
/opt/trend (user config)	ISADMIN	ISADMIN contains the administrative program files
	ISCSP	ISCSP contains the executable daemon and a script file
	iscan iscan/virus iscan/alert	iscan contains the system and virus log files, files blocked, as well as other program files
	tmp	temporary files used

Table 2-1. InterScan VirusWall CSP Edition Installed Files

Directory	*Subdirectory*	*Files/Modification*
/etc	rc2.d	creates S99IScsp; S99IScanHttpd

Upgrading from the Trial Version

To upgrade a trial version to the full version:

1. Save the `/opt/trend/iscan/intscan.ini` file used by your trial version. This file contains configuration settings used by your trial version software.
2. Run InterScan VirusWall's install script (`./isinst`) to uninstall the trial version.
3. Run the install script again to install the software, and enter the serial number when prompted.
4. Replace the default `intscan.ini` file from your installation with your saved version and restart InterScan VirusWall.

Chapter 3

Getting Started

This chapter explains important configuration tasks to perform after installation. Topics include how to start the InterScan VirusWall configuration console and how to perform routine administrative tasks that will keep your antivirus protection up-to-date:

- Registering
  - Obtaining a serial number
  - Upgrading from the trial version
  - Configuring your proxy server settings
- Updating the pattern file immediately
- Updating the scan engine
- Scheduling pattern file and scan engine updates
- Rolling back an update

Registering Benefits

Registering your product is important because it entitles you to the following benefits:

- One year of program and pattern file updates
- One year of technical support
- Important product information

You can register over the Internet or by mail.

Note: You must register through the InterScan VirusWall CSP Edition console to obtain automatic pattern file updates.

Obtaining a Serial Number

The product serial number can be obtained:

- On the product registration card included with the software
- On the outside front cover of the product documentation
- From a Trend Micro™ sales representative at the following email address:
  `sales@trendmicro.com`

Registering InterScan™ VirusWall™ CSP Edition

Failing to enter a valid InterScan VirusWall serial number during installation will install a 30-day trial version of the program. To continue using the program after the 30-day trial period has elapsed, you must enter a valid serial number.

To enter the serial number, choose **Registration** from the left-hand frame:

1. Fill in the product serial number.
2. Fill in the user and company information, making sure to fill in the required fields, which are preceded by a red star.

3. Click **Register** to register the product, which entitles you to virus pattern updates.

Configuring Proxy Settings

If you use a proxy server to connect to the Internet, you must configure your server and authentication settings before you can register and update the pattern file.

1. To enter your proxy settings, click the **proxy settings** link on the registration screen.

   -or-

   Select **Update > Settings** from the left-hand menu to go directly to the proxy settings screen.
2. Enable the *Use a proxy server to access the Internet* option and then enter the proxy's name, port and authentication information.
3. Click the **Save** button. The new Proxy Server settings will be immediately applied in the InterScan VirusWall scheduler.

Note: As a security precaution, the proxy password is sent **only once** from the Web-based management console to the InterScan VirusWall server. When you return to the Proxy Settings screen, the *Password* field will appear blank. This is because displaying it (even as "*****") would necessitate sending the proxy user name and password between the server and browser.

Updating the Pattern File and Scan Engine

InterScan VirusWall CSP Edition blocks viruses by comparing a file's binary pattern and message content with the virus pattern file. In order to maintain the highest level of protection against the latest virus and content threats, it's important that you update your pattern file regularly. Trend Micro™ frequently updates its virus pattern file, often several times per week in response to newly-released viruses.

In addition, Trend Micro periodically updates the scan engine, which is the component that compares a file's binary structure with the virus pattern file, detects suspicious virus-like behavior and cleans viruses.

On-demand Update (Update Now)

To update the pattern file immediately:

1. Select **Update > Update Now** from the left-hand frame. Your current pattern file and the date it was downloaded will be listed.
2. Click the **Update Now** button.

Scheduled Update

InterScan VirusWall CSP Edition can automatically download updates hourly, daily or weekly. If your network has limited Internet bandwidth, you can configure updates for a time when network load is low, outside of business hours.

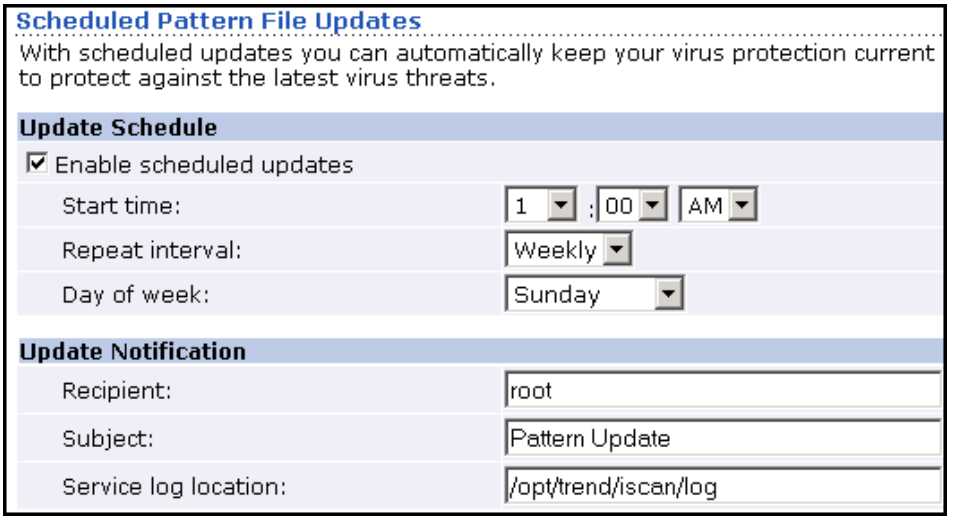


FIGURE 3-1. Scheduled Update Configuration Page

To configure a scheduled update:

1. Select **Update > Scheduled Update** from the left-hand menu.
2. Check the *Enable scheduled updates* option.

3. Configure the time and update interval.
4. Configure the recipient you want the pattern update notifications sent to. You can specify the Subject line for the notifications and the directory to store the Service logs.

Note: The new Scheduled Update settings will be immediately applied to the InterScan VirusWall Scheduler.

Updating the Scan Engine Manually

The scan engine for InterScan VirusWall is updated on a regular basis with new features and improvements. The scan engine is posted for download on the Trend Micro™ Web site and cannot be updated automatically by InterScan VirusWall CSP Edition.

Note: Use the **About** page in the Web Console to see which version of the scan engine is currently being used.

To update the scan engine:

1. Download the scan engine (libvsapi.so) from `www.trendmicro.com/download` and untar the file.
2. Using the Web Console, stop all the InterScan VirusWall scanning services (SMTP, FTP, and/or HTTP).
3. Copy the new engine file to the `/opt/trend/iscan` directory.
4. Restart the InterScan VirusWall scanning services.
5. Clean out the cache by running `./S99IScanHttpd stop`, then `./S99IScanHttpd start`.

Rolling Back a Pattern File Update

After updating to a new virus pattern file, InterScan VirusWall by default keeps the last three downloaded pattern files on the server. You can change this setting in the Update > Settings screen.

Note: InterScan VirusWall always uses the pattern file with the largest three-digit pattern file number, that is, the pattern file's extension.

To roll back to a previous virus pattern file:

1. Note the version of the virus pattern file that you are currently using.

   Note: Click on **About** to see which version of the pattern file is currently being used.

2. Stop the InterScan VirusWall services.
3. Delete the file /opt/trend/iscan/lpt$vpn.###, where ### is three digits that represents the pattern file version.
4. Verify that there is another virus pattern file in the /opt/trend/iscan path whose pattern version is less than the one you deleted.
5. Restart the InterScan VirusWall services.

Chapter 4

Enabling SMTP, HTTP, and FTP Scanning

This chapter describes how to enable and configure SMTP, HTTP, and FTP scanning. Topics include:

- Macro Scan settings
- SMTP settings
  - Message insertions
  - Message ID
  - Action on viruses found in MIME attachments with long filenames
  - Selecting the file types to scan
  - Configuring notifications
  - Setting the virus actions
- HTTP and FTP settings
  - Selecting the file types to scan
  - Configuring notifications
  - Setting the virus actions

Scan Menu

SMTP, HTTP, and FTP options can be separately configured in InterScan VirusWall CSP Edition, allowing flexibility in scan options and actions on viruses found. InterScan VirusWall offers the administrator a great deal of flexibility in configuring how the program will behave. For example, you can choose which email attachment types to scan, who should be notified when a virus is discovered, what action should be taken—clean, delete, move, or pass it on to the recipient along with a warning message.

The only configuration that is applied to all types of scanning is the Macro Scan settings.

Macro Scan Settings

Macro Scan detects macros in file downloads and provides two scanning options: Quarantine and Clean. Go to the **Scan > Macro Settings** screen. Select **Enable macro scanning** to use this feature, then choose Quarantine or Clean.

- **Quarantine** removes the file if it contains a macro and places it in the Quarantine directory.
- **Clean** strips off the macro before delivering the file with the attachment.

SMTP Scanning

InterScan™ VirusWall™ scans all inbound and outbound messages for viruses. SMTP scanning is enabled by default after installing InterScan VirusWall.

InterScan VirusWall SMTP features include:

- Real-time scanning of inbound *and* outbound email traffic
- Automatic, customizable virus notifications
- Option to Clean, Quarantine, Delete or Pass infected files
- MIME Attachment name filtering based on size
- Safe Stamps
- Record Message ID in the server log

Enabling SMTP Scanning

To enable or disable InterScan™ VirusWall™ SMTP scanning:

1. In the menu on the left, click **Scan > SMTP > Files to Scan**.
2. Click **Enable SMTP scanning**:
   - A check means real-time scanning is enabled
   - No check means real-time scanning is *not* enabled

SMTP Settings

You can select several different types of notifications in messages that InterScan VirusWall scans, in addition to the regular virus notifications. Select **Scan > SMTP > Settings** to go to the SMTP settings screen, as shown below:

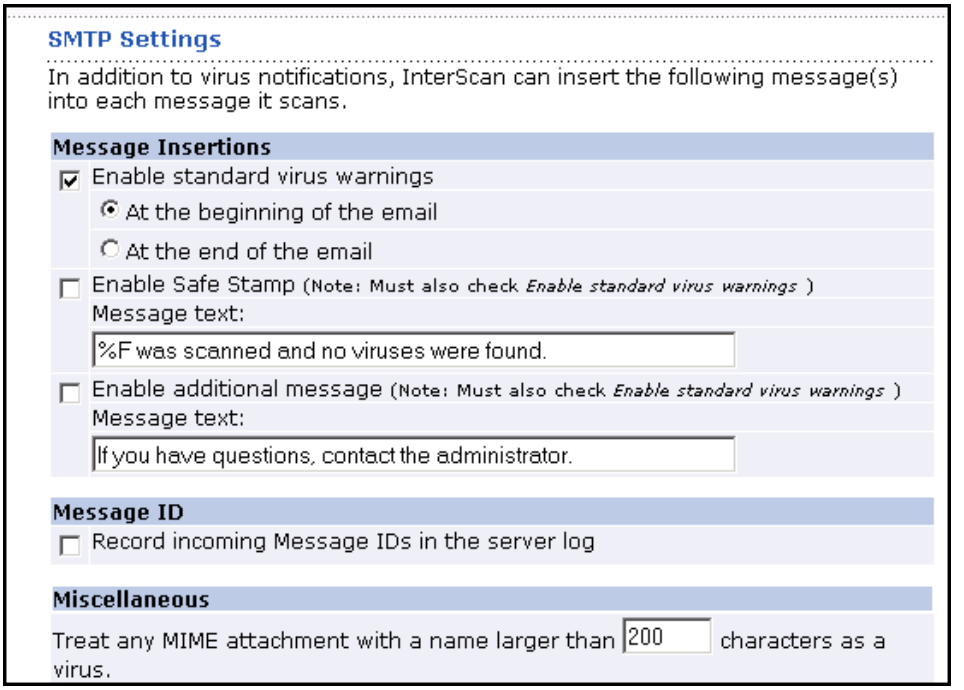


FIGURE 4-1. SMTP Settings screen, where you can enable message insertions.

Message Insertions

1. Select **Enable standard virus warnings** to insert InterScan VirusWall notifications in the original email. Then select whether to place the warnings at the beginning or the end of the email.
2. Select **Enable Safe Stamp** to have InterScan VirusWall insert a brief note in scanned messages to let users know that their email was scanned and found to be virus free.

   Insert the InterScan VirusWall variable %F if you want InterScan VirusWall to include the name of the file(s) scanned, for example:

   InterScan VirusWall checked the attached file, "Mystery.zip", and found no virus(es).

3. Check **Enable additional message** to have InterScan VirusWall send a separate email message when a virus is found. Enter your message in the message text field. The additional message is sent to the recipient(s).

Note: For this message to be sent, you must also select **Enable standard virus warnings** in the **SMTP > Notification** screen.

Message ID

InterScan VirusWall has the ability to log the Message IDs for identification purposes. To enable this feature, select **Record incoming Message IDs in the server log**.

This feature is used when InterScan VirusWall encounters unique problem cases. If a specific email causes InterScan VirusWall to crash, the Mail Transfer Agent (MTA) will recognize that InterScan VirusWall is down and attempt to resend the email after a specific period of time. The problem will recur as long as the same message is being resent.

The problem email Message ID can be identified in the log to solve this problem. Before allowing the message to pass, make sure that it is not infected.

Miscellaneous

File attachment names longer than 200 characters can cause additional scanning time that slows down the scan process. Select **Treat any MIME attachment with a name larger than ___ characters as a virus** to bypass scanning these files. You can change the number of characters to any file name length that you choose.

Selecting the Files to Scan

To select which files to scan:

- To scan all file types, regardless of extension, select **All files**. This is the most secure configuration. Compressed files are opened and all files within are scanned.

- To scan only selected file types, select **Only the following**. Only those files with extension names that are explicitly specified in the associated text box are scanned.

  ```
  .com .exe .sys .doc .xls .zip .dll
  ```

  Use this option, for example, to decrease the aggregate number of files InterScan VirusWall checks, thus decreasing overall scan times. Some file types (for example, graphics) have not been known to carry viruses.

  Note: Zip and other compressed files are only scanned if the file type is specified. Compressed files are opened and all files scanned. Infected Zip files cannot be cleaned and should be deleted or quarantined.

  There is no limit to the number or types of files you can specify here. Also, note that no wildcard (*) precedes the extension, and multiple entries are delimited by a space.

Setting Virus Notifications

Upon detecting a virus, InterScan™ VirusWall™ can send an automatic email notification to the administrator (or other users), sender, and/or recipients (inbound, and unblocked outbound mail only). The notification text is fully customizable and you can insert InterScan VirusWall fields in the message as well.

Specifying the Notification Delivery Server

In order to be able to send notifications, you need to specify the SMTP server that will deliver the notification messages. This selection is made on the **General > Settings** screen.

Note: If no notification server is specified, no notifications will be sent.

After specifying the SMTP notification server, go to **Scan > SMTP > Notification** to specify the administrator name and subject for the notification messages. You can have any email address you want appear in the **From** field of the virus notification message(s); however, only valid accounts on the SMTP server will be delivered if users attempt to "Reply to" the notification message.

Alternatively, you can create an alias mail account with auto-reply and include that address in the **From** field. Users who "Reply to" the virus notification would then receive whatever information you want them to have in regards to the virus incident.

Message Properties

To specify the notification server, go to the *Message Properties* section:

1. In the **From** field, type the name of the notification server using the domain name or IP address. The default setting, *root@localhost*, can be used if your SMTP server is on the same machine as InterScan VirusWall.
2. Enter the **Subject** text line that will be sent.

Specifying the Notifications

To notify the administrator, sender, and/or recipient(s):

1. If you want to include the server name in notifications, select **Include the InterScan host name in notifications**.
2. Click the checkbox to notify the administrator, sender, and/or recipient(s).

   For the administrator, enter the email address (**root**, for example) in the associated text box. For the sender or recipients, the address is taken from the email.
3. In the **Message text** field, enter the warning message you want the administrator to receive. The following case-sensitive variables can be used in the message:
   - %A = Action taken: Detailed Description
   - %a = Action taken: Delete, Move, Pass
   - %d = Date virus was detected
   - %F = File where virus was detected

- %f = For email, identifies sender
- %v = Virus name
- %t = For email, identifies recipient
- %M = When action is move, displays the destination directory and filename
- %m = Detection method
- %h = Host name

For example:

Warning! On %d, InterScan VirusWall detected the %v virus in the file: %F. InterScan took the following action: %a.

which reads, "Warning! On **7-23-03**, InterScan VirusWall detected the **Jerusalem** virus in the file: **Word.com.** InterScan took the following action: **delete**."

Setting the Action on Viruses

You can specify one of four actions for InterScan VirusWall to take upon finding an infected file:

- Choose **Clean** to have InterScan VirusWall automatically clean and process infected files. The recipient will receive the cleaned file. Select an action in case an infected file cannot be cleaned, for example if the virus is an uncleanable virus:
  - Choose **Quarantine** to move the infected file to the Quarantine directory.
  - Choose **Delete** to reject the infected at the server.
  - Choose **Pass** to ignore the virus and deliver the file to the requesting client.
- Choose **Quarantine** to move the infected file to the Quarantine directory *without cleaning* (by default, `/opt/trend/iscan/virus`). The requesting client will not receive the file.
- Choose **Delete** to reject the infected file at the server. The requesting client will not receive the file.
- Choose **Pass** to send the infected file, along with a warning message to the client *without cleaning*.

HTTP and FTP Scanning

InterScan™ VirusWall™ can scan HTTP and FTP file transfers for viruses. InterScan VirusWall can be installed on the same machine as an existing firewall or on a dedicated machine. See *Where to Install InterScan™ VirusWall™ CSP Edition* starting on page 1-5 for illustrated examples.

InterScan VirusWall can serve as a sentry, checking all HTTP and FTP file transfers to and from the network for viruses.

Enabling HTTP and FTP Scanning

To enable or disable InterScan VirusWall HTTP and FTP scanning:

1. In the menu on the left, click **Scan > HTTP** or **FTP > Files to Scan**.
2. Select the checkbox to enable scanning or clear the checkbox to disable scanning.

Configuring FTP Files to Scan

For FTP scanning, the *Files to Scan* screen includes the same options as used for SMTP scanning. For more information, see *Selecting the Files to Scan* starting on page 4-5.

Configuring HTTP Files to Scan

For HTTP scanning, the *Files to Scan* screen includes the same options as used for SMTP and FTP scanning, with a few more options. The HTTP Files to Scan configuration screen is shown below.

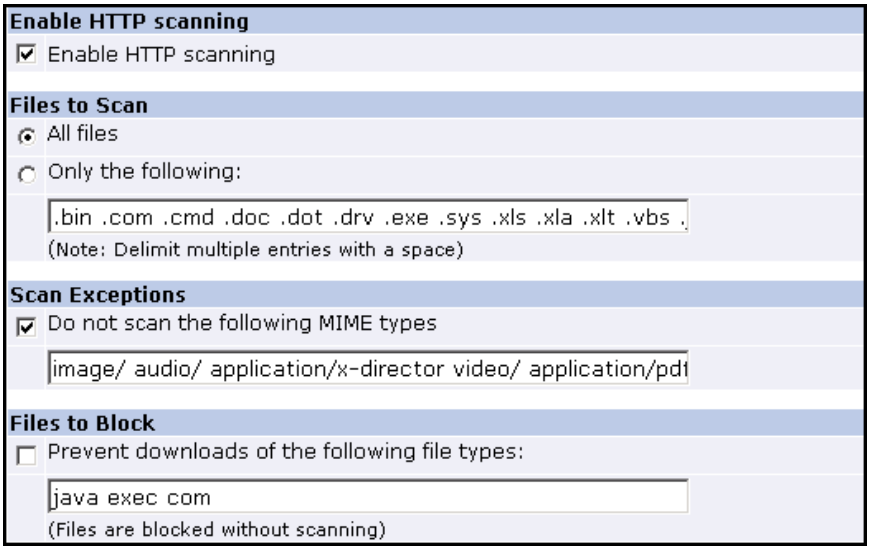


FIGURE 4-2. HTTP Files to Scan configuration screen, which also allows scan exceptions and file blocking

Files to Scan Options

The HTTP Files to Scan options are the same as the SMTP options. See *Selecting the Files to Scan* starting on page 4-5 for a description of how to configure the file types.

Scan Exceptions

MIME files usually do not contain viruses and you can exempt MIME types from HTTP scanning. In general, the top-level MIME media type is used to declare the general type of data, while the subtype specifies a specific format for that type of data. Thus, a media type of "image/xyz" is enough to tell that the data is an image, even if the user has no knowledge of the specific image format "xyz". Registered subtypes of "text", "image", "audio", and "video" should not contain embedded information that is really of a different type. Such compound formats should be represented using the "multipart" or "application" types.

To reduce scan time, you can select not to scan certain MIME types. Select **Do not scan the following MIME types** and then specify the types, such as:

```
image/ audio/ application/x-director video/ application/pdf
/multipart
```

Use a space as the separator between MIME types to exclude from scanning.

Configuring HTTP Files to Block from Download

For HTTP scanning, you can explicitly state the types of files that you want to block users from downloading.

To specify which files to block:

1. Select **Prevent downloads of the following file types**.
2. Edit the file types that you want to block. Multiple entries should be delimited by a space. Currently, the types of files that can be blocked are `java, exec,` and `com`.

Blocked files will not be allowed to pass through the server and will not be stored.

Setting the Virus Notification and Action on Viruses

For HTTP and FTP scanning, the virus actions are the same as used for SMTP scanning. The only difference in configuration is that HTTP and FTP notifications are sent only to the administrator or other designated individual. For more information, see:

- *Setting Virus Notifications* starting on page 4-6
- *Setting the Action on Viruses* starting on page 4-8

Chapter 5

Log Files and Resource Configuration

InterScan™ VirusWall™ creates two types of log files — the system logs and the virus logs. The system logs track system events such as error messages, the stopping and starting of the daemons, etc. The virus logs track all virus events.

A system log is created every day. You can specify where to keep the system logs and how many to keep.

A virus log is created each time there is a virus event. The virus logs can be queried by type of scan, recipient, virus name, and date.

Many aspects of the InterScan VirusWall resource configuration can be set from the General Configuration screen:

- Settings — set the working directory, quarantine directory, and notification server
- Main configuration — set the CSP service port and server timeouts
- Performance — resource optimization and maintenance
- Password — change the Management Console Password

Log Configuration

You can have InterScan VirusWall write its system and virus event logs to any directory you want, provided that there is sufficient disk space.

Note: If you don't regularly remove old log files from your log directory, and your InterScan VirusWall server processes high volumes of messages, the log files could consume a large amount of disk space.

1. Select **Virus Logs > Log Configuration** from the left-hand menu.

   Note: For the System and Virus logs, InterScan VirusWall adds the current date (yyyy.mm.dd) to the name.

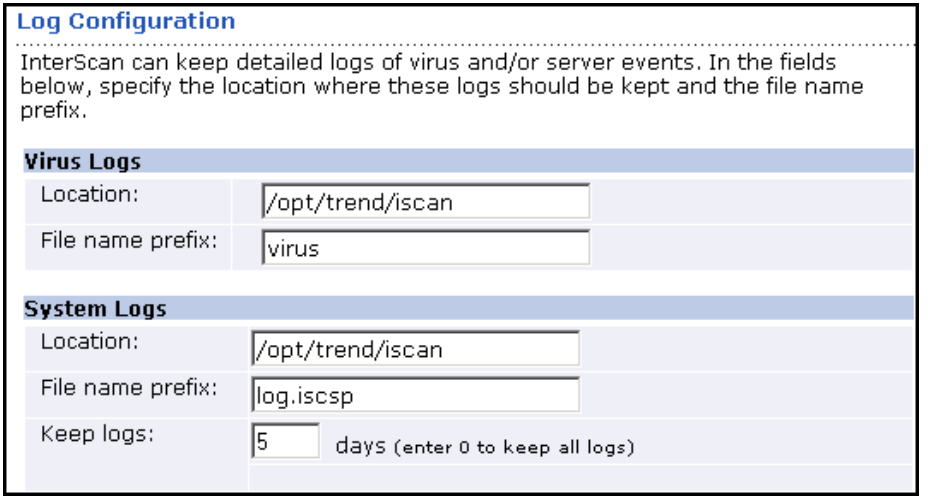


FIGURE 5-1. Virus Log Configurations screen with the default values displayed.

2. Configure the virus log settings:
   a. Specify the directory where you want the virus logs kept, which is `/opt/trend/iscan` by default.

b. Specify the file name prefix, which is "virus" by default.

3. Configure the system log settings:
   a. Specify the directory where you want the system logs kept, which is `/opt/trend/iscan` by default.
   b. Specify the file name prefix, which is "log.iscsp" by default.
   c. Specify the number of days that you want the system logs to be retained.
4. Click **Save** to write your changes.

Note: You must restart the InterScan VirusWall service to apply your new Log settings.

Viewing the System Log Files

System logs retain important information about security and program events for your InterScan VirusWall installation. New system logs are written each day. You can configure how many system logs to keep in the Log Configuration screen. See 5the previous section for more details.

Note: The system logs cannot be viewed through the Web interface. You must use an editor, such as VI, to view the system logs.

The system logs are named according to the following convention:

```
log.iscsp.2003.07.23
```

which can be read as *InterScan VirusWall System Log for July 23, 2003*.

Configuring the System Log Detail Level

The system log contains two levels of logging detail: default and verbose. The virus log contains only the default logging level. The system log levels are set directly in the `/opt/trend/iscan/intscan.ini` file; there is no interface support for changing the default log level.

- **Default** logging tracks error messages and notes whenever a daemon is stopped or started
- **Verbose** logging tracks all program details and should be used only temporarily, and only if problems are encountered

---

Note: If you use InterScan VirusWall's Verbose logging mode, be sure that you have specified a directory with plenty of disk space, for example 256 or more megabytes.

Viewing the Virus Logs

InterScan VirusWall provides two screens for viewing the virus logs: Virus Query and Advanced Virus Query. The Virus Query is the fastest and displays log records by protocol (SMTP, HTTP, and/or FTP) and date. With the Advanced Virus Query, you can also query log files by recipient name and/or virus name. This option can be useful when you have many files infected with viruses.

Virus Query

To view virus log files from the console:

1. Click **Virus Logs > Virus Query** in the left navigator.
2. Select the Protocol(s) whose logs you want to view from the list — HTTP, FTP, and/or SMTP.
3. Choose the date **Range**. If you would like to specify the exact dates, select **Specified date range** and then select the Start and End dates.
4. Choose whether to **Sort logs by** date, virus name, or user.
5. Click **View Logs** to display the logs you have selected. InterScan VirusWall extracts the data from the virus log files according to your criteria and displays the results. Virus logs include the following data:
   - Event Date—date and time the virus was discovered
   - Protocol—SMTP, HTTP, or FTP
   - From—the originating domain, IP Address, or sender
   - To—the intended recipient (for email)

- Virus Name
- Action Taken on the virus-infected file
- Infected File name and location

Virus names that appear in blue are linked to the encyclopedia on *www.trendmicro.com*. Double-click a linked name to learn more.

Advanced Virus Query

The Advanced Virus Query gives you the same options as the Virus Query, with the additional options to query files by recipient name and/or virus name.

To view virus log files by recipient name and/or virus name:

1. Click **Virus Logs > Virus Query** in the left navigator.
2. Select the Protocol(s) whose logs you want to view from the list — HTTP, FTP, and/or SMTP.
3. Select All recipients or only designated recipients. Names available will only include those users who have received virus-infected files.
4. Select All viruses or only designated recipients. Only the names of viruses that have been detected on your network will be shown.
5. Choose the date **Range**. If you would like to specify the exact dates, select **Specified date range** and then select the Start and End dates.
6. Choose whether to **Sort logs by** date, virus name, or user.
7. Click **View Logs** to display the logs you have selected.

Viewing the Virus Logs from the Command Line

Alternatively, you can view virus log files from the command line:

1. The log files are written by default to the `/opt/trend/iscan` directory.
2. The virus logs are named according to the following convention:

   `virus.log.2003.07.23`

   which can be read as *InterScan VirusWall Log for July 23, 2003*.

Deleting the Virus Log Files

InterScan VirusWall does not automatically remove virus log entries. Left unchecked, logs will grow until they consume all disk space. You can delete unwanted virus logs manually.

To delete virus log files from the console:

1. Click **Virus Logs** > **Delete Logs**.
   - To delete all log files, click **All logs**.
   - To delete selected log files, click **Specific logs** and select the logs you want to delete.
2. Click **Delete** to carry out the action.

To delete virus log files from the command line:

1. Go to the `/opt/trend/iscan/virus` directory.
2. Delete virus log files that you no longer need.

General Configuration Settings

The General section of the Configuration menu provides settings that control notifications, queue directories and the management console's password.

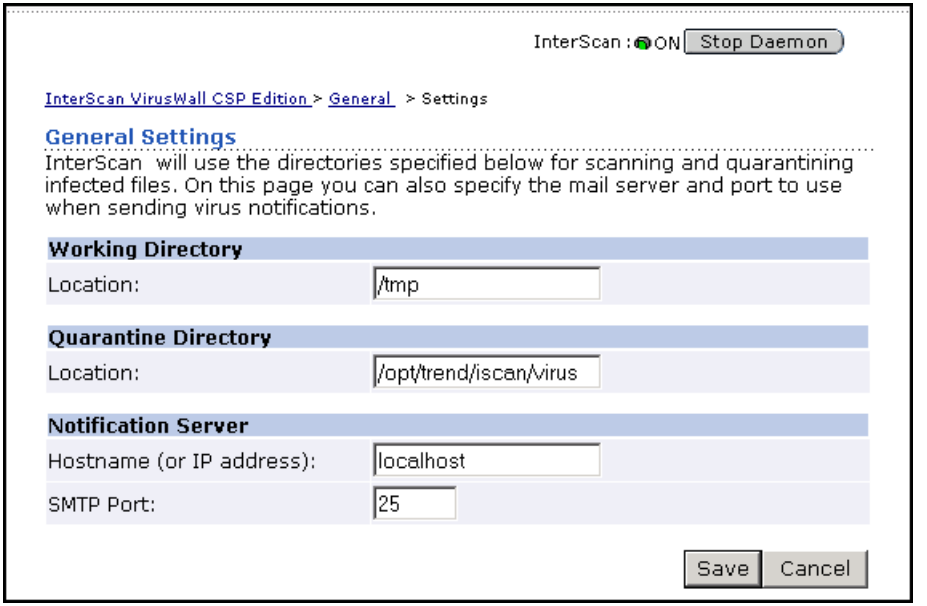


FIGURE 5-2. General Configuration Settings screen with the default values displayed.

Setting the Working Directory

By default, InterScan VirusWall uses the `/tmp` directory to scan for viruses. When InterScan VirusWall receives a file (any type that it is configured to scan), it places a copy in a temporary directory for scanning. The directory location is configurable. Be sure to specify a directory with at least 256MB available free space.

Setting the Quarantine Directory

By default, InterScan VirusWall uses the `/opt/trend/iscan/virus` directory to store files that have been quarantined due to viruses. Be sure to specify a directory with at least 256MB available free space.

Designating the Notification Server

You can be notified when a virus is detected, a policy is updated or the system requires attention via email. By default, the Notification Server's Hostname is **localhost**. Enter the hostname or IP address in this field.

The **SMTP Port** is the port the Notification Server uses for SMTP traffic. The default value is 25: the standard SMTP port specification. This value is configurable, but in most circumstances it should not be changed.

Note: To apply the new Notification settings, you must restart the InterScan VirusWall service.

Main Configuration

Setting the CSP Service Port

As a rule of thumb, install InterScan VirusWall inside a firewall and on the firewall side of your existing SMTP server. The firewall directs traffic to InterScan VirusWall on port 3300, InterScan VirusWall scans the SMTP, FTP, and HTTP traffic it receives, and then routes the scanned traffic back to the firewall. The firewall then routes the traffic for delivery.

Note: Ordinarily, you should keep the CSP Service Port set to 3300.

Connection Settings

Connection settings can be established to avoid having processes wait indefinitely for a reply from either server or firewall. Set the following options:

1. Server timeout— InterScan VirusWall listens on the CSP service port for incoming traffic from the firewall. If the firewall does not respond before the timeout, InterScan VirusWall will drop the connection. By default, the timeout is 120 seconds.

2. Keep alive interval—InterScan VirusWall maintains a connection with the firewall by sending a command to test the firewall status periodically. By default, the keep alive interval is 120 seconds.

Performance Settings

You can fine-tune InterScan VirusWall's performance by making adjustments to the resource settings.

Resource Optimization

To optimize resources, you can configure the number of processes spawned upon startup and the refresh rate of slave processes. In addition, you can limit the total number of slave processes InterScan VirusWall will use at any one time, and the total number of threads for a given slave.

By default when InterScan VirusWall is started, it creates two slave processes to handle the existing traffic load. Depending on your system resources and traffic load levels, you may want to increase the number of initial slave processes.

To fine-tune the InterScan VirusWall resources:

1. Designate the number of **Initial slave processes**. The default is 2.

   Note: There is no maximum allowed value. However, entering too large of a number can result in wasted system resources.

2. Designate the **Maximum slaves per master**. The default is 25.

   Whenever the maximum number of child processes is reached, InterScan VirusWall will stop spawning new threads; additional messages are rejected (the originating client will typically make multiple attempts to send the message before bouncing it back to the sender as undeliverable; in most cases, InterScan VirusWall will be free to accept one of these subsequent redeliveries).

3. Designate the **Maximum threads per slave**. The default is 5.

Resource Maintenance

InterScan VirusWall will automatically generate slave processes as needed to accommodate traffic spikes. As the spikes taper off, excess slave processes are left idle. As a matter of "good housekeeping", InterScan VirusWall extinguishes slave processes after a set number of threads have been generated and destroyed, thus ensuring that idle resources do not inadvertently remain active.

Choosing the right regeneration time is important. On the one hand, the accumulation of a lot of idle slave processes means system resources are being wasted. On the other hand, existing slave processes can respond more rapidly to sudden increases in the work load than spawning new processes to accommodate the additional load.

To fine-tune the way that InterScan VirusWall maintains the resources:

1. Designate the number of threads for **Regenerate slave after every ___ threads**. The default is 500 threads, meaning that after 500 threads have been generated and extinguished, the slave process itself is extinguished and a new one generated (a new slave is only spawned if needed). Setting this number too low can result in needlessly brief cycles.

   Note: Specifying a value of zero (0) means that idle slave processes are never extinguished.

2. Designate the number of seconds for **Regenerate slave if idle more than ___ seconds**. The default is 3600 seconds, that is, one hour. In specifying a value, choose a number that represents a balance between the need to create new processes and the unwanted accumulation of idle processes.

   A value of zero means the number of available processes will always equal your highest usage spikes, no matter how brief or infrequent they may be. A value of just a few seconds means InterScan VirusWall will have to create new processes just about every time there is a change in the work load.

Changing the Management Console Password

Access to the InterScan VirusWall management console can be restricted via a password to prevent unauthorized changes.

Note: The default console password after InterScan VirusWall is installed is **admin**. If you forget your password, please contact a Trend Micro™ technical support engineer for instructions on how to reset it. The other option is to uninstall your software, and then reinstall it.

To configure or change the management console's password:

1. Select **General > Password** from the left-hand frame.
2. Enter the existing password, and then enter and confirm your new password.
3. The new password will take effect immediately after clicking **Save**.

Chapter 6

Getting Virus and Technical Support Information

The Trend Micro™ Web site has a wealth of information on the latest security threats, such as spam and offensive email that can interfere with your company's productivity. Visit the Trend Micro™ Virus Information Center to find information on spam, viruses, and malicious code threats. Also on the Trend Micro Web site, visit Knowledge Base, Trend Micro's online database of common answers to technical questions.

This chapter contains information on the following topics:

- Testing InterScan™ VirusWall™ CSP Edition
- Trend Micro's Virus Information Center
- Using HouseCall, an online antivirus application that runs in your Web browser
- Trend Micro's online Knowledge Base
- Technical support contact information
- TrendLabs™

Testing InterScan™ VirusWall™

Once InterScan™ VirusWall™ has been installed, we recommend that you test it to get familiar with the configuration and see how the program works.

The European Institute of Computer Antivirus Research, along with antivirus vendors, has developed a test file that can be used for checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose signature has been included in the Trend Micro™ virus pattern file. You can download the file from Trend Micro at:

`www.trendmicro.com/vinfo/testfiles/`

Once on your machine, you can use the test virus in email to test SMTP scanning, and also in files to check FTP and HTTP file transfers.

Accessing the Virus Information Center

Comprehensive security information is available over the Internet at our antivirus center:

`www.trendmicro.com/vinfo`

Use the **Virus Information Center** to find out about:

- Which viruses and malicious mobile code are currently "in the wild," or actively circulating
- Computer virus hoaxes
- Trend Micro's Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- A safe computing guide

To access Trend Micro's Virus Information Center from the InterScan™ VirusWall™ Web console, select **Security Info** in the menu bar at the top of the screen.

Knowledge Base

Trend Micro™ provides Knowledge Base, an online Knowledge Database filled with answers to common questions.

Use Knowledge Base, for example, if you are having trouble receiving program file updates and want to find out what you can do to solve the problem. Or, say you're getting an error message—search Knowledge Base using the text of message to find out what is causing the error and how to fix it.

The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro™ support engineer who will investigate the issue and respond as soon as possible.

To access Trend Micro's support database, open a Web browser and enter the following URL:

`kb.trendmicro.com/solutions/`

The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are unable to find an answer, however, select **Submit Question** and fill out the requested information. A Trend Micro™ support engineer will investigate the issue for you.

Trend Micro System Cleaner

Trend Micro System Cleaner helps 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 the Trend Micro System Cleaner on your system.

There are two versions of Trend Micro System Cleaner. Both are free, and are described below.

- Trend Micro System Cleaner (TSC) works in conjunction with HouseCall, PC-cillin, and OfficeScan. Whereas these applications let you clean or delete infected files, TSC not only detects and removes Trojans, it also rids your system of dropped code and restores settings that were altered as the result of the attack.

- Trend Micro System Cleaner Package was developed specifically for users without Trend Micro products, and offers the same benefits as TSC. The System Cleaner Package is provided as a public service, and can be downloaded free from the Trend Micro Web site.

Both versions support the following:

- Terminates all malware instances in memory
- Removes malware registry entries
- Removes malware entries from system files

Additionally, the Trend Micro System Cleaner Package:

- Scans for and deletes all malware copies in all local hard drives

For more information, visit www.trendmicro.com/download/tsc.asp

Contacting Technical Support

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.

If you need help, or just have a question, please feel free to contact us. We also welcome your comments. Trend Micro can be reached via telephone, fax, email, regular mail or through our Web site at:

```
www.trendmicro.com/support
```

To access technical support from the InterScan™ VirusWall™ Web console:

1. Click the **Support** link at the top of the main screen. You will be linked to the Trend Micro Technical Support Information screen.
2. Scroll down to select the closest office

Speeding Up Your Support Call

It will speed up your problem resolution if you have the following details on hand:

- InterScan VirusWall product version including the CSP version and build number

- Pattern file and scan engine versions
- OS version
- Network type
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- Detailed description of the installation environment
- Exact text of any error message given
- Steps to reproduce the problem

TrendLabs™

TrendLabs™ is Trend Micro's global complex of antivirus research and support centers. It's located on three continents, with a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- SolutionBank, Trend Micro's online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Index

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

For Sales:
Tel: +1-800-228-5651 (US and Canada)
Tel: +1-408-257-1500 (outside US and Canada)
Fax: +1-408-257-2003