

TREND MICRO™

# InterScan™ AntiVirus for Sendmail™

Protection from malicious code for the Internet messaging gateway

for Linux® & Solaris®

Getting Started Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the 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 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.

Trend Micro, the Trend Micro t-ball logo, InterScan, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 1998-2004 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. IAEM11988/40802

Release Date: October, 2004

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

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

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

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

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

---

# Contents

## **Chapter 1: Introducing InterScan AntiVirus**

Important features .....	1-1
Benefits .....	1-1
Getting started .....	1-2
Important terms .....	1-2
Available documentation .....	1-2
Management console .....	1-3
Navigation panel .....	1-3
Tab behavior .....	1-4
Information icon .....	1-6
Online help .....	1-7
Opening a management console from a browser .....	1-8

## **Chapter 2: Planning Your Installation**

Recommended system requirements .....	2-2
Pre-installation checklist .....	2-3
Settings migration (optional) .....	2-4
Destination directory (1/5) .....	2-4
HTTP proxy settings (2/5) .....	2-4
Product activation (3/5) .....	2-5
Notification settings (4/5) .....	2-6
Mail filter settings (5/5) .....	2-6
When to install InterScan AntiVirus .....	2-9
Example of a completed pre-installation checklist .....	2-10

### **Chapter 3: Installing InterScan AntiVirus**

Installing InterScan Antivirus .....	3-1
Evaluation version .....	3-8
Removing the evaluation-period limit .....	3-8
After installation .....	3-9
Post-installation Sendmail configuration .....	3-10
Product License screen .....	3-11
My Product Details screen .....	3-12
Removing ISAV .....	3-12

### **Chapter 4: Registering and Activating InterScan AntiVirus**

Registering InterScan AntiVirus .....	4-2
Your logon ID and password .....	4-4
After registration .....	4-4
Activating InterScan AntiVirus .....	4-5
For more information about activation and registration .....	4-6

### **Chapter 5: Updating and Testing InterScan AntiVirus**

Updating InterScan AntiVirus .....	5-1
Virus pattern file .....	5-1
Scan engine .....	5-2
Additional threats pattern file .....	5-3
Testing your installation .....	5-5

---

## **Chapter 6: Configuring InterScan AntiVirus**

Fine-tuning scanning .....	6-2
Setting action for attachments and messages .....	6-3
Setting up notifications for threats .....	6-4
Configuring inline notifications .....	6-6
Blocking files .....	6-8
Scheduling maintenance .....	6-9
Fine-tuning mail settings .....	6-9
Mail configuration settings - server .....	6-9
Mail configuration settings - disclaimer .....	6-11
Configuring alerts .....	6-11
Scheduling maintenance of log files .....	6-12
Configuring directories .....	6-13
Configuring the proxy .....	6-13

## **Chapter 7: Troubleshooting**

Issues .....	7-2
Cannot log in .....	7-2
Activation Code is invalid .....	7-2
No log or quarantine directory .....	7-2
Cannot update the pattern file .....	7-3
Management console timed out .....	7-3
Performance seems degraded .....	7-3
Virus is detected but cannot be cleaned .....	7-3
Virus scanning not working .....	7-4
Free detection tools .....	7-4
Knowledge Base .....	7-4
Virus information center .....	7-4
Global support centers .....	7-5
Before contacting technical support .....	7-6

**Appendix A: Glossary of Terms**

**Appendix B: Utilities in InterScan Antivirus**

**Appendix C: Migration Settings**

ISAV “isav.ini” file settings ..... C-2

**Appendix D: ISAV Services**

**Index**

# Introducing InterScan AntiVirus

InterScan™ AntiVirus (ISAV) provides an antivirus solution for your organization's network. You can also scan for and remove additional threats, such as spyware and dialers. And, the application is easy to install and use.

## Important features

ISAV helps you manage your network in the following ways:

- Scans for traffic containing viruses, and manages infected attachments and messages
- Scans for traffic containing other potential threats
- Blocks incoming file types that can damage your network
- Helps prevent DoS (Denial of Service) attacks by setting limits on message size
- Lets you see a summary of threats to email message activity at a glance—for today, the past week, the past month, and since ISAV was started

## Benefits

InterScan AntiVirus:

- Is easy to install with the InterScan AntiVirus installation script



- Can be configured to automatically update the virus pattern file, scan engine, and additional threats (malware) pattern file, as soon as a new version becomes available from Trend Micro
- Provides notifications to make sure you stay informed of activity, and alerts that trigger under conditions requiring attention
- Provides log files that can be purged automatically after 30 days
- Provides a user-friendly management console that includes online help to guide you through tasks

## Getting started

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

## Important terms

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

## Available documentation

The documentation for this product assumes that you are experienced with Solaris or Linux operating systems, Sendmail, and administering a network. It is also assumed that you have root privileges to manage the security applications in your network.

The documentation available for InterScan AntiVirus is:

- This document—*InterScan AntiVirus for Sendmail Getting Started Guide*
- Readme file—Contains important late-breaking information about InterScan AntiVirus
- Online Help—Two kinds of online help are available:
  - Context-sensitive screen help, which explains how to perform tasks on one screen
  - General help, which explains tasks that require action on several screens, or peripheral knowledge needed to complete tasks

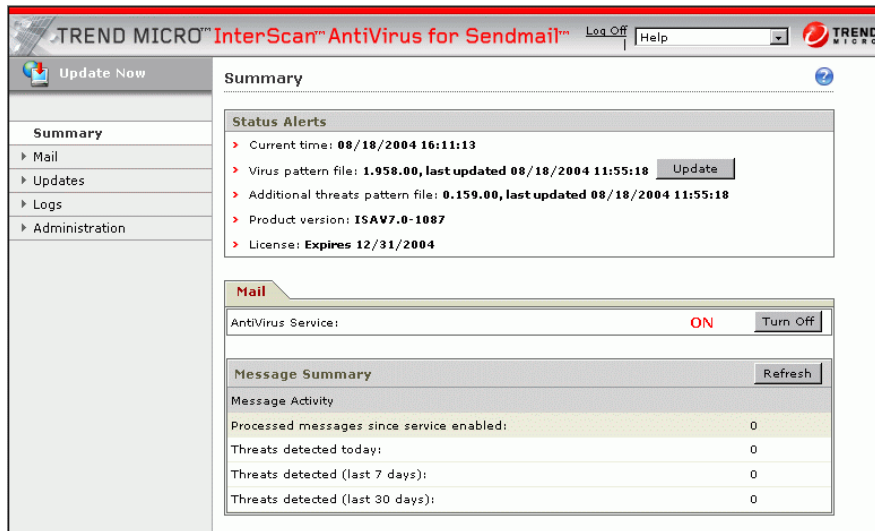
- Knowledge Base—An online database of problem-solving and troubleshooting information. Knowledge Base provides the latest information about known product issues. To access the Knowledge Base, select the Knowledge Base link in online general help, or visit:

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

## Management console

After you have successfully installed ISAV, the **Logon** screen displays. Type the password you created on the **Notification Settings** screen in the installation script. Click **Enter** to access the management console.

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

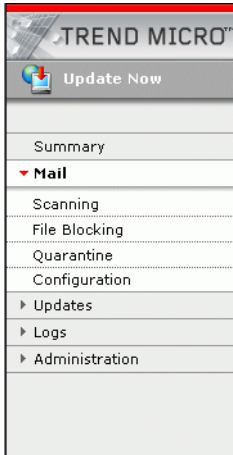


**FIGURE 1-1.** Summary screen on the InterScan AntiVirus management console

## Navigation panel

The left side of the management console is a main menu, that also serves as a navigation panel. Click a selection in the navigation panel to open its corresponding

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



**FIGURE 1-2.** Navigation panel in the ISAV console

---

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

---

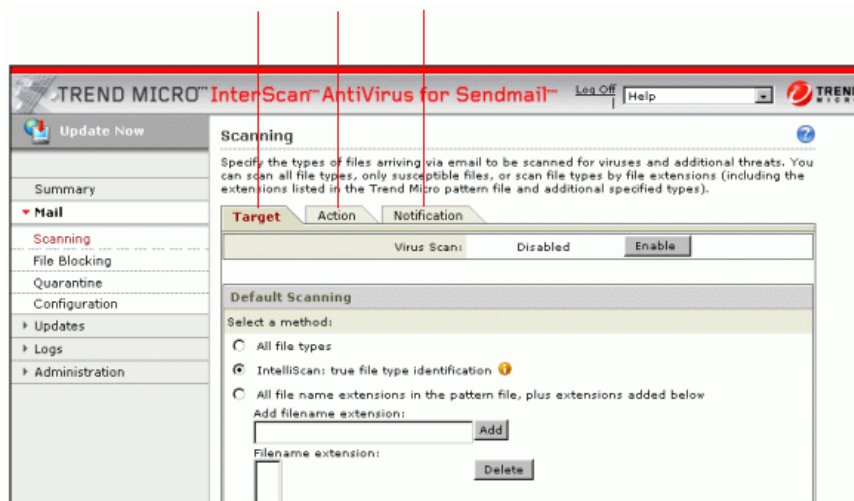
In the InterScan AntiVirus documentation, a path such as Mail > Scanning > Action, indicates that:

- The main selection in the navigation panel is Mail
- The secondary selection is Scanning
- The selected tab on the **Scanning** screen is the **Action** tab

## Tab behavior

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

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



**FIGURE 1-3. Tab behavior in InterScan AntiVirus**

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

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

The appearance of the **Save** button indicates whether saving is necessary. The **Save** button is unavailable when the screen first opens. After you perform tasks on the screen, the appearance of the **Save** button changes so the text on the button appears black instead of gray. This is an indication that a **Save** is necessary to validate the work you have done.

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

## Information icon

Some screens in the management console contain an information icon:



Position your mouse pointer over the information icon to display a popup text box with additional information, to help you make a decision or complete a task.

In the following example, moving the pointer over the information icon displays more information about additional threats that can be detected by InterScan AntiVirus:

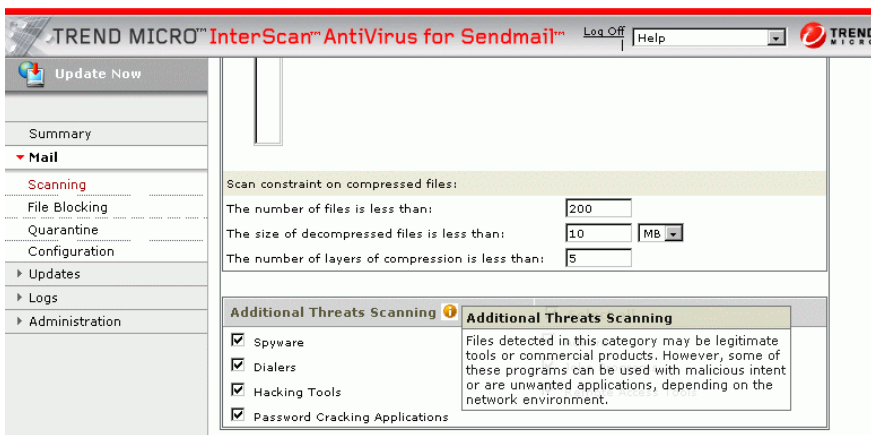


FIGURE 1-4. Information icon

## Online help

To invoke screen help, click the screen help icon:



Invoke general help by selecting the help feature in the InterScan AntiVirus banner.

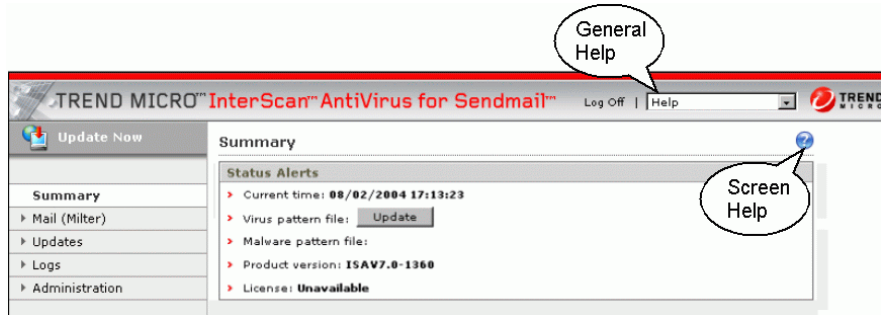


FIGURE 1-5. Help icons on InterScan AntiVirus screens

Search the online help by selecting **Contents and Index** from the general **Help** list.

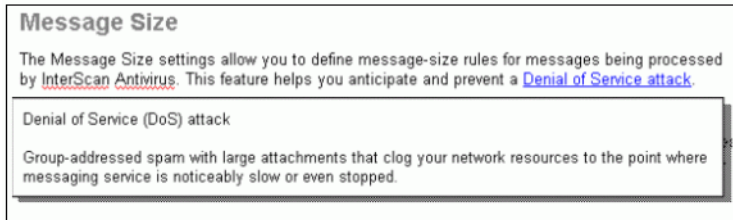
### Links in online help

The online help contains links, indicated by blue underlined text. Clicking a link either takes you to another help screen or displays a popup text box with additional information. In the following example from the online help for the **Target** tab of the **Scanning** screen, the [About IntelliScan](#) and [File Name Extensions](#) links take you to other help screens.

If you select:	Results are:
All file types	All file types are scanned.
IntelliScan: True file type identification	Only files that are most vulnerable to malicious code are scanned. For more information, see <a href="#">About IntelliScan</a> .
All file name extensions in the pattern file, plus extensions added	All file types described in <a href="#">File Name Extensions</a> , plus additional file types you have added to the <b>Filename extension</b> field are scanned.

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

In the following example, the [Denial of Service attack](#) link displays a definition for the term “Denial of Service attack”



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

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

## Opening a management console from a browser

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

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

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

# Planning Your Installation

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

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



## Recommended system requirements

Install InterScan AntiVirus on a system with:

### Hardware

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

### Supported Operating Systems

- Red Hat™ Enterprise Linux, Advanced Server 2.1
- Red Hat Enterprise Linux, Advanced Server 3.0
- SuSE™ Linux 9.0
- Solaris 8

---

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

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

---

### Software

- Sendmail™ 8.11 or 8.12 (with milter enabled)
- You must have one of the following browsers available for the Web console: (JavaScript must be enabled)
  - Netscape™ Navigator 7.1 or higher, or
  - Microsoft™ Internet Explorer 5.5 or higher

---

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

---

# Pre-installation checklist

**Pre-installation Checklist**

**Settings Migration (Optional)**

**Import Settings**  
Full path for the "intscan.ini" file \_\_\_\_\_

Destination Directory \_\_\_\_\_

**HTTP Proxy Settings (optional)**

**Use Proxy (to connect to the Internet)**  
HTTP Proxy Address \_\_\_\_\_  
HTTP Proxy Port \_\_\_\_\_

**Use Proxy Authentication**  
Proxy Authentication Username \_\_\_\_\_  
Proxy Authentication Password \_\_\_\_\_

**Product Activation**

Registration Key \_\_\_\_\_  
Activation Code \_\_\_\_\_

**Notification Settings**

Admin UI Password \_\_\_\_\_  
Admin Email Address \_\_\_\_\_  
Notification Email Server Address \_\_\_\_\_  
Notification Email Server Port \_\_\_\_\_

**Mail Filter Settings**

**Mail Filter Virus Scanning**  
Mail Filter Setting \_\_\_\_\_  
Sendmail Server IP \_\_\_\_\_  
Sendmail Server Port \_\_\_\_\_

**FIGURE 2-1. Pre-installation checklist**

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

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

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

---

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

---

## Settings migration (optional)

If you have previously used an enterprise version (3.x) of Trend Micro InterScan VirusWall™ and are migrating to InterScan AntiVirus, some of the settings in your “intscan.ini” file can be preserved if you select “y” on this screen. For a description of the settings which are kept, see Appendix C, *Migration Settings*.

## Destination directory (1/5)

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

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

```
/opt/trend/isav
```

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

---

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

---

## HTTP proxy settings (2/5)

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

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

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

## Product activation (3/5)

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

### Registration Key

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

XX-XXXX-XXXX-XXXX-XXXX

InterScan AntiVirus must be registered, using your product Registration Key, before you receive an Activation Code that allows you to begin using InterScan AntiVirus. See Chapter 4, *Registering and Activating InterScan AntiVirus*, for more information about obtaining your Registration Key, and procedures to register InterScan AntiVirus. Trend Micro recommends that you register your product before beginning the installation process.

### Activation Code

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

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

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

## Notification settings (4/5)

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

---

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

---

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

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

## Mail filter settings (5/5)

If you will *not* be using InterScan AntiVirus to scan your SMTP traffic, modify the value in the **Mail Filter Virus Scanning** field to “disabled.” However, even if you are not using InterScan AntiVirus to scan your SMTP traffic for viruses, you are prompted to specify configuration settings.

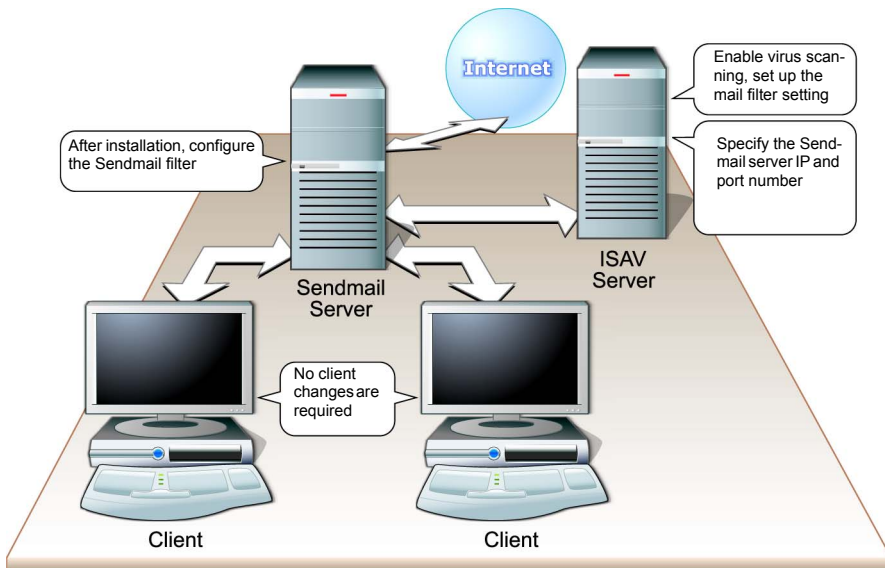
Your original configuration was probably arranged so that messages would go between the Internet and clients via Sendmail on an MTA server. When InterScan AntiVirus is added to the configuration, messages between Sendmail and the Internet are also routed through the InterScan AntiVirus server before being delivered to clients.

There are two possible installation scenarios:

- You have an existing Sendmail server, and have installed ISAV on the same server
- You have an existing Sendmail server, and have installed ISAV on another server (referred to as the ISAV server) - this second scenario is illustrated in Figure 2-2

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

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



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

You are prompted to supply the mail filter setting for Sendmail. You are also prompted to supply an IP address and server port for processing messages that have been quarantined. After installation, configure the Sendmail server as described in [Post-installation Sendmail configuration](#) starting on page 3-10.

### Socket mode versus inet mode for the mail filter setting field

On the Modify Sendmail Mail Filter Settings screen, the **Mail Filter Setting** field can be set in two different modes, depending on the installation scenario you select. These two modes are:

- Unix-domain socket mode
- IPv4 socket mode, also referred to as “inet” mode

You can use either mode if you install ISAV on the same machine as Sendmail. If you install ISAV on a different server than the server on which Sendmail is installed, *only* inet mode can be selected.

The format for *Unix-domain socket* mode is:

```
local:</directory path>/isav.sock
```

For example - local:/opt/trend/isav/tmp/isav.sock

The format for *IPv4 socket (inet)* mode is:

```
inet:<port>@<server IP>
```

For example - inet:3333@123.123.123.123

Here is an example of the Modify Sendmail Mail Filter Settings screen from the installation script. In this example, socket mode was selected in the **Mail Filter Setting** field:

```

InterScan Antivirus for Sendmail Install Script
-----
- Modify Sendmail Mail Filter Settings - (5/5)
Mail Filter Virus Scanning: enabled
Mail Filter Setting: <Please modify>
Sendmail Server IP: <Please modify>
Sendmail Server Port: 25

Do you want to modify the mail filter settings?

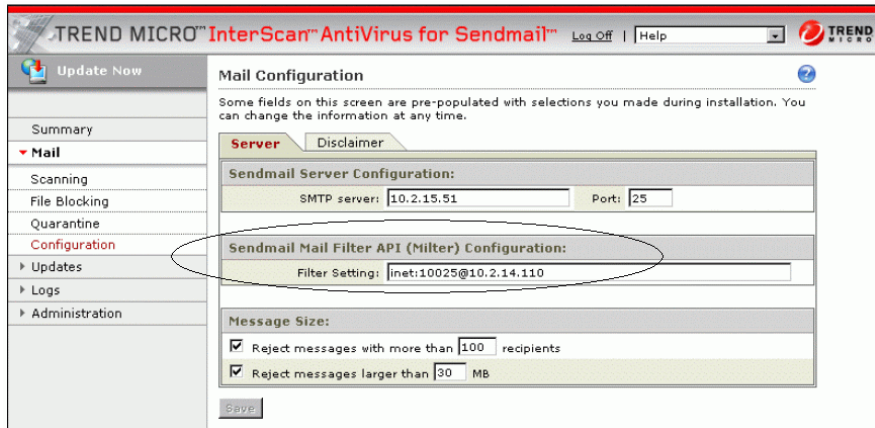
[M|m] = modify  [N|n] = next  [B|b] = back  [X|x] = exit

Please type a letter [ m ]
If you do not want to make changes, please press Enter.
Mail Filter Virus Scanning: 1=enable, 2=disable (default:1) 1
Mail Filter Setting: (For example, inet:3333@123.123.123.123)
local:/opt/trend/isav/temp/isav.sock
Sendmail Server IP: (default:123.123.123.123): 12.123.12.123
Sendmail Server Port: (default:25) 25

```

**FIGURE 2-3. Mail Filter Settings field on the Modify Sendmail Mail Filter Settings screen from the installation script**

This selection can be changed in the management console on the Server tab of the Mail Configuration screen. In the following example, inet mode was selected during installation.



**FIGURE 2-4.** Sendmail Mail Filter API (Milter) Configuration field - IPv4 socket (inet) mode configuration

## When to install InterScan AntiVirus

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

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



## Example of a completed pre-installation checklist

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

<b>Pre-installation Checklist</b>	
<b>Settings Migration (Optional)</b>	
<input checked="" type="checkbox"/> Import Settings	Full path for the "intscan.ini" file <i>opt/trend/isav/etc/iscan/intscan.ini</i> _____
	Destination Directory <i>opt/trend/isav</i> _____
<b>HTTP Proxy Settings (optional)</b>	
<input checked="" type="checkbox"/> Use Proxy (to connect to the Internet)	HTTP Proxy Address <i>123.123.123.123</i> _____
	HTTP Proxy Port <i>80</i> _____
<input type="checkbox"/> Use Proxy Authentication	Proxy Authentication Username _____
	Proxy Authentication Password _____
<b>Product Activation</b>	
	Registration Key <i>AJ-43B2-P388-WJ5T-Z9Q1</i> _____
	Activation Code <i>BV-43CZ-8TY9-D4VNA-82WE9-L7T2-WPX41</i> _____
<b>Notification Settings</b>	
	Admin UI Password <i>same2yoo2 (secure this document after completion)</i> _____
	Admin Email Address <i>admin@smtp.ourcompany.com</i> _____
	Notification Email Server Address <i>12.123.12.123</i> _____
	Notification Email Server Port <i>25</i> _____
<b>Mail Filter Settings</b>	
<input checked="" type="checkbox"/> Mail Filter Virus Scanning	Mail Filter Setting <i>inet.3333@123.123.123.123</i> _____
	Sendmail Server IP <i>123.12.123.123</i> _____
	Sendmail Server Port <i>25</i> _____

FIGURE 2-5. Example of completed pre-installation checklist

## Installing InterScan AntiVirus

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

To install InterScan Antivirus, copy and download the files from the FTP site provided by your sales representative or reseller.

### Installing InterScan Antivirus

Follow these steps to install InterScan AntiVirus.

**To start the installation process:**

---

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

---

1. From the FTP site, copy the ISAV files to the machine you plan to use as the ISAV server.

2. Locate the folder containing the installation files. The files are:

For Linux	<code>isinst isav-7.0-linux-1xxx.tgz</code>
For Solaris	<code>isinst isav-7.0-sol-1xxx.tgz</code>

3. Type the following:

```
#ls
```

The result is:

For Linux	<code>isinst isav-7.0-linux-1xxx.tgz</code>
For Solaris	<code>isinst isav-7.0-sol-1xxx.tgz</code>

4. Execute the installation as follows:

```
#sh ./isinst
```

5. The first **Install** screen displays.

```
InterScan Antivirus for Sendmail Install Script
-----

Welcome to the Trend Micro InterScan Antivirus for Sendmail
Install Script.

Be sure to consult the ReadMe.txt file before proceeding.

The install script will guide you to review default settings.
You will be able to modify them as well.

Press Enter to continue ...
```

**FIGURE 3-1. Install script Welcome screen**

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

**To respond to the installation setup script:**

1. Press **Enter** to proceed with the installation.
2. The Trend Micro **License Agreement** displays. Press **Enter** to view the full text of the license agreement. When you are finished, type **Y|y** (accept license) to proceed, or **N|n** (decline license) to stop. If you do not accept the terms in the license agreement, the installation cannot be completed.
3. When you accept the license terms, the **Settings Migration** screen displays. If you are migrating to ISAV from a legacy version of InterScan VirusWall (ISVW), you can retain some of your original ISVW configuration settings by typing **Y|y** (yes) to proceed. See Appendix C, *Migration Settings*, for a description of the parameters that are migrated to ISAV. To decline, type **N|n** (no). Press **Enter** to continue.
4. The **Choose Destination Directory** screen displays. The default directory for installation of the InterScan AntiVirus files (`/opt/trend/isav`) displays in

the **Destination Directory** field. To accept the default, type **N|n**. To change the directory, type **M|m** {modify}, and enter an alternate directory in the **Destination Directory** field - then type **N|n** to continue.

5. The **Modify Default HTTP Proxy Settings** screen displays. Respond to the prompts on this screen if you are currently using a proxy server to connect to the Trend Micro ActiveUpdate server, including the proxy server address and port number, and optional authentication user name and password. If you are not using a downstream proxy, you do not need to provide this information and can go to the next screen. Type **N|n** (next) to continue.
6. The **Product Activation** screen displays:

```
InterScan Antivirus for Sendmail Install Script
-----
- Product Activation - (3/5)
You must register online to get an Activation Code.
Go to https://olr.trendmicro.com/registration
Has the product been activated? : no
Do you want to enter the Activation Code?
[E|e] = enter code  [N|n] = next  [B|b] = back  [X|x] = exit
Please type a letter [  ]
```

**FIGURE 3-2. Product Activation screen**

- a. If you have already registered *and* activated InterScan AntiVirus, “yes” displays in the **Has the product been activated?** field. In this case, type **N|n** to continue.
- b. If you have not registered *or* activated the product, “no” displays in the **Has the product been activated?** field. To register now, go to the Trend Micro Online Registration Web site at:

<http://olr.trendmicro.com>

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

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

---

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

---

- 7.** The **Modify Notification Settings** screen displays. Type **M|m** (modify) to enter and confirm the password for the administrator account you plan to use to manage InterScan AntiVirus. Also enter the notification email address, server IP address, and port. Type **N|n** (next) to continue.
- 8.** The **Modify Sendmail Mail Filter Settings** screen displays. If you do not plan to use this feature, type **M|m** to modify the default value in the **Mail Filter Virus Scanning** field from “enabled” to “disabled.”  
If you plan to use this feature, the fields on this screen are described in detail in Chapter 2. Enter the values you recorded on your pre-installation checklist for the Sendmail filter setting, and the reprocessing server IP and port to be used for

messages that are reprocessed after being quarantined. Type **N|n** when you are finished.

```
InterScan Antivirus for Sendmail Install Script
-----
- Modify Sendmail Mail Filter Settings - (5/5)
Mail Filter Virus Scanning: enabled
Mail Filter Setting: <Please modify>
Sendmail Server IP: <Please modify>
Sendmail Server Port: 25

Do you want to modify the mail filter settings?

[M|n] = modify  [N|n] = next  [B|b] = back  [X|x] = exit
Please type a letter [  ]
```

**FIGURE 3-3. Modify Sendmail Mail Filter Settings screen**

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

```
InterScan Antivirus for Sendmail Install Script
-----
- Ready to Install -
You have selected:
Proxy:           no
Activated:       no
Mail Filter:     enabled

Proceed to the next screen to start installation.

[S|s] = start installation  [B|b] = back  [X|x] = exit
Please type a letter [  ]
```

**FIGURE 3-4.** Ready to Install screen

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

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



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

```
Please use your Web browser to view the management console on:  
http://123.123.12.12:1812  
or  
https://123.123.12.12:8443  
[root@my machine 31 isav1050]#
```

**FIGURE 3-5. User prompt for displaying management console**

---

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

---

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

## Evaluation version

You can install the evaluation version of any Trend Micro product, which allows you to try out other Trend Micro products as well. Evaluation versions are fully functional and can be installed with a temporary product Registration Key and Activation Code. Typically after 30 days, however, most of the program features will be disabled.

## Removing the evaluation-period limit

If you decide to purchase a product that you are evaluating, you do not need to reinstall. Instead, open the Trend Micro Online Registration page, enter the Registration Key you received (post-purchase) along with the other required fields,

and click **Register** to send your information to Trend Micro. Your Activation Code arrives via email, typically within twenty minutes.

## After installation

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

- Adjust the default configuration of the product to meet the needs of your organization more accurately, or
- Begin scanning for viruses immediately, using the default settings you chose during installation

Immediately after installing, you should also:

- Update the virus pattern file and scan engine
- Update the additional threats pattern file
- Confirm that virus scanning is enabled
- Customize the notification messages
- Configure the alerts
- Set up an update schedule for the virus pattern file, scan engine, and additional threats pattern file

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

## Post-installation Sendmail configuration

After you have installed ISAV, configure the Sendmail configuration file to communicate with ISAV.

### Configuring Unix-domain socket mode:

Add the following 2 lines of code to the configuration file:

```
O InputMailFilters=filterISAV
XfilterISAV, S=local:<directory path>/isav.sock, F=T, T=S:10m;R:15m;E:15m
```

For example:

```
O InputMailFilters=filterISAV
XfilterISAV, S=local:/opt/trend/isav/tmp/isav.sock, F=T, T=S:10m;R:15m;E:15m
```



### Configuring IPv4 (inet) socket mode:

Add the following 2 lines of code to the configuration file:

```
O InputMailFilters=filterISAV
XfilterISAV, S=inet:<port>@<IP address>, F=T, T=S:10m;R:15m;E:15m
```

For example:

```
O InputMailFilters=filterISAV
XfilterISAV, S=inet:10025@124.123.123.123, F=T, T=S:10m;R:15m;E:15m
```



### For both modes:

In the “Xfilter” expression:

- “F” controls the fallback method in case of an error:
  - If F = R, the connection is rejected
  - If F = T, as shown in the example, the connection is temporarily deferred
- “T” controls the timeout settings, as shown below:
  - S:xxm = timeout for sending traffic to the filter, for example, if S = 10m, the sending timeout period is 10 minutes
  - R:xxm = timeout for receiving traffic from the filter, for example, if R = 15m, the receiving timeout period is 15 minutes
  - E:xxm = timeout between sending end-of-message and reply from the Sendmail filter (in the above example, the timeout period is 15 minutes)

If Sendmail already has another filter configured, for example, a filter called “ABCD,” append the ISAV filter after the existing filter as shown in the following example:

```
O InputMailFilters=filterABCD, filterISAV
```

For more information about configuring Sendmail filter settings, go to the following Web site:

<http://www.milter.org>

---

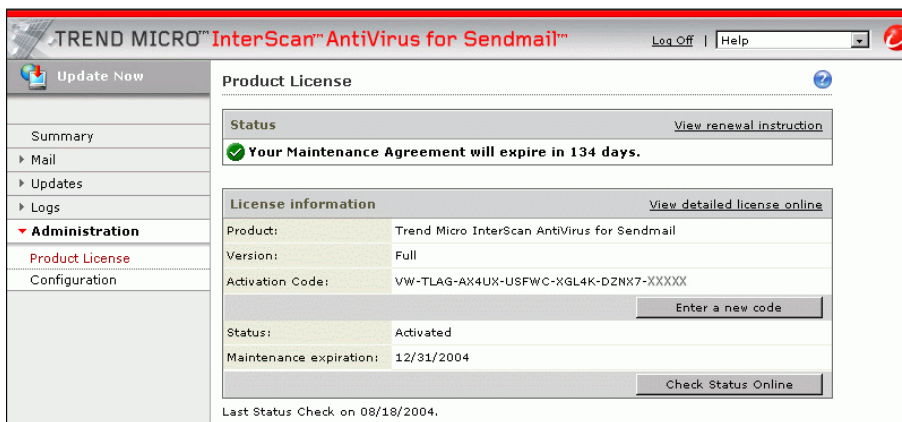
**Note:** If you use sendmail.mc, add the following line in your Sendmail configuration file:

---

```
INPUT_MAIL_FILTER(`filterISAV', `S=inet:<port>@<IP address>, F=T,
T=S:10m;R:15m;E:15m')
```

## Product License screen

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



**FIGURE 3-6.** Product License screen in the management console

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

## My Product Details screen

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

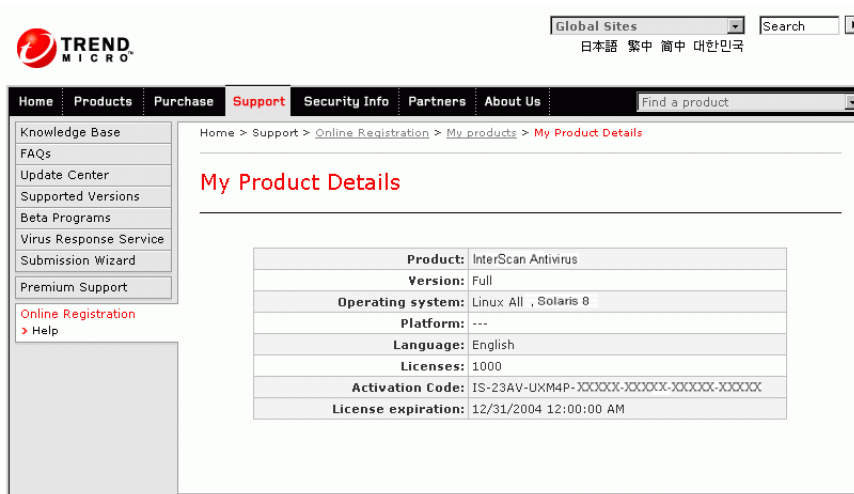


FIGURE 3-7. My Product Details screen

## Removing ISAV

To remove the software from your machine:

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

Progress: 100%

#

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

# Registering and Activating InterScan AntiVirus

This chapter describes:

- Product registration, which is required to receive product updates, including updates to the virus pattern file, scan engine, and additional threats pattern file
- Product activation, which is required to enable InterScan AntiVirus to begin scanning and blocking

After your purchase of InterScan AntiVirus concludes, you will receive a product license certificate. The certificate contains a code, either a Registration Key or an Activation Code. The codes are needed to complete the registration and activation tasks described in this chapter.

---

**Note:** Trend Micro recommends that you register and activate ISAV immediately.

---

## Registering InterScan AntiVirus

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

Your Registration Key or Activation Code can be found on your license certificate, that you should have received from Trend Micro shortly after your purchase of InterScan AntiVirus. If you do not have your license certificate, contact Trend Micro for assistance.


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

TREND MICRO SOFTWARE LICENSE CERTIFICATE

Issued to confirm the purchase by: YOUR COMPANY

Customer No: 16340  
Product Name: INTERSCAN ANTIVIRUS  
No. of License: 2443  
Reseller Name: BIZCO DISTRIBUTORS, INC.  
SKU: SEBEMVE52  
TM Program Number: 8436  
TM Reference Number: 02018533  
S/N (R/K): CJ-49N2-P388-XXXX-R8E3  
Maintenance Start Date:  
Maintenance End Date:

Customer Service and Sales Support – email [sales@trendmicro.com](mailto:sales@trendmicro.com)

 TREND MICRO™

[www.trendmicro.com](http://www.trendmicro.com)

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



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

<http://olr.trendmicro.com>

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

The screenshot shows the Trend Micro Online Registration page. At the top, there is a navigation bar with 'Home', 'Products', 'Purchase', 'Support', 'Security Info', 'Partners', and 'About Us'. A search bar is located on the right. The 'Support' menu is expanded, showing 'Knowledge Base', 'FAQs', 'Update Center', 'Versions Supported', 'Support Newsletter', 'Beta Programs', 'Submission Wizard', and 'Premium Support'. The 'Online Registration' link is highlighted in red. The main content area is titled 'Online Registration' and contains the following text: 'Thank you for using Trend Micro™ products and services. To ensure that you are eligible to receive the latest security updates and other product and maintenance services, register your products by completing the following Online Registration forms.'

The page is divided into two main sections: 'Login' and 'New customer registration:'. The 'Login' section includes a 'Login ID:' input field, a 'Password:' input field, a 'Login' button, and a 'Forgot your ID / Password?' link. The 'New customer registration:' section includes instructions: 'Complete the registration process, if you: - Have purchased Trend Micro product(s) but have never registered online - Have product evaluation CD and want to install one or more programs. Select the region where the product were purchased and your preferred language:'. Below this is a dropdown menu set to 'United States - English' and a 'Register your product' button.

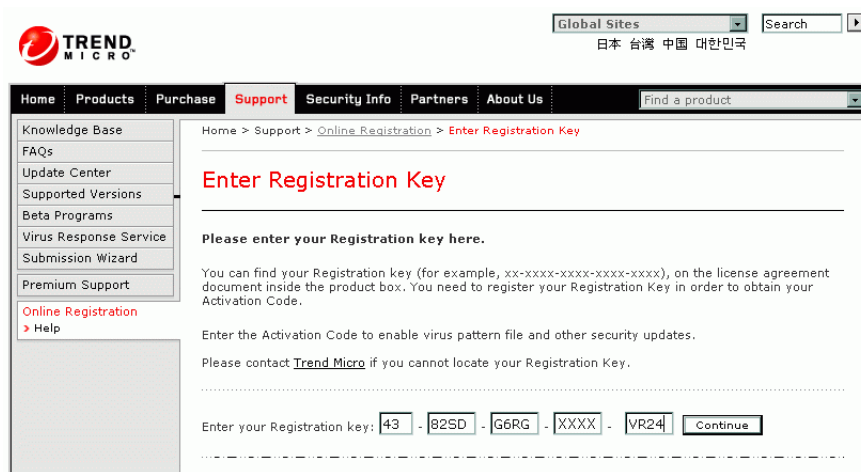
An 'Instruction:' section follows, with a link to '> Purchasing the software'. A 'Note:' states: 'As part of the registration process, Trend Micro will collect certain contact information, which may include personal data, for business reasons. Trend Micro agrees not to share this information generally with third parties other than as required to provide you directly with the services for which you or your company or organization have paid Trend Micro. For details about our information collection and use practices, please review our [Privacy Policy](#).'

At the bottom, there are links for 'Email this page' and 'Rate this page'.

**FIGURE 4-2. Trend Micro Online Registration screen**

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

The **Enter Registration Key** screen displays.



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

## Your logon ID and password

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

## After registration

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

## Activating InterScan AntiVirus

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

### To activate during installation:

Enter the Activation Code in the **Enter Activation Code** field on the **Product Activation** screen. This field appears after you type **E|e** (enter code):

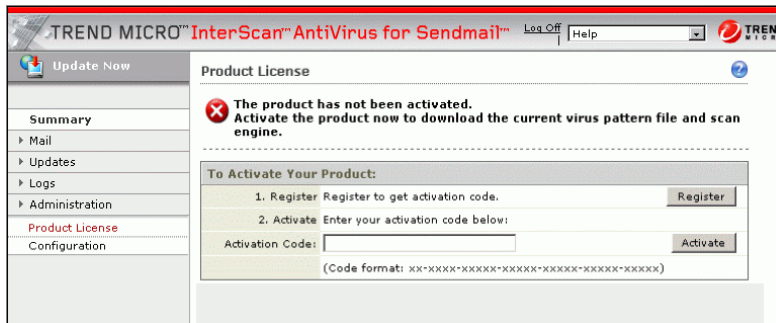
```
InterScan Antivirus for Sendmail Install Script
-----
- Product Activation - (3/5)
You must register online to get an Activation Code.
Go to https://olr.trendmicro.com/registration
Has the product been activated? : no
Do you want to enter the Activation Code?

[E|e] = enter code  [N|n] = next  [B|b] = back  [X|x] = exit
Please type a letter [ ]
```

FIGURE 4-3. Product Activation screen in installation script

**To activate after installation:**

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

**FIGURE 4-4. Product License screen**

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

Your product license enables you to receive product updates, pattern file updates, and basic technical support for one year from the date of purchase.

As soon as InterScan AntiVirus is activated, it begins scanning for viruses if you enabled virus scanning during installation. To enable scanning of other threats, such as spyware, you must select the other threats to be scanned on the Target tab of the Mail > Scanning screen. To enable file blocking, configure this feature according to your organization's communications policies. See *Configuring InterScan AntiVirus* starting on page 6-1 and the online help for more information.

**For more information about activation and registration**

View a product registration FAQ by visiting the following site:

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

---

# Updating and Testing InterScan AntiVirus

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

- Updating InterScan AntiVirus to use the most recent versions of the scanning and malware detection tools
- Testing the installation to make sure InterScan AntiVirus is detecting viruses

## Updating InterScan AntiVirus

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

- Virus pattern file
- Scan engine
- Additional threats pattern file

### Virus pattern file

Trend Micro's products draw upon an extensive database of virus "signatures," commonly called the virus pattern file. During scanning, the binary patterns of files are compared against these signatures, and the scan engine determines a file is

infected if a match is found. Since new virus pattern files are often available every week or sometimes several times a week, you should schedule automatic daily updates.

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

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

<http://www.trendmicro.com>

## Scan engine

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

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

---

**Note:** See update instructions in *Scheduled update* starting on page 5-3 or *Manual update* starting on page 5-4.

---

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

---

**WARNING!** *InterScan AntiVirus will not scan password-protected or encrypted files. SMTP password-protected or encrypted messages are delivered, but ISAV embeds a warning message to that mail, to let the user know the files were not scanned.*

---

## Additional threats pattern file

Like the virus pattern file, the additional threats pattern file uses a database of threat “signatures,” but unlike the virus pattern file, you can selectively choose which additional threats to scan in your SMTP traffic. The additional threats pattern file is updated via the Trend Micro ActiveUpdate server. A new additional threats pattern file is available every 2 weeks.

## Scheduled update

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

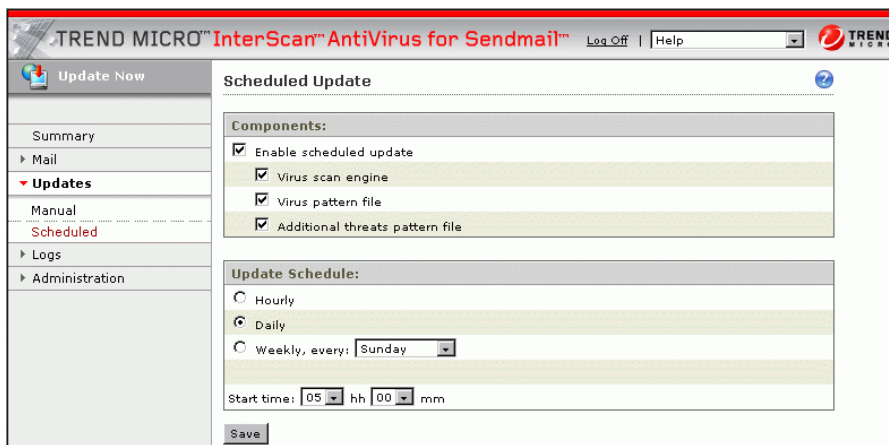


FIGURE 5-1. Scheduled Update screen

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

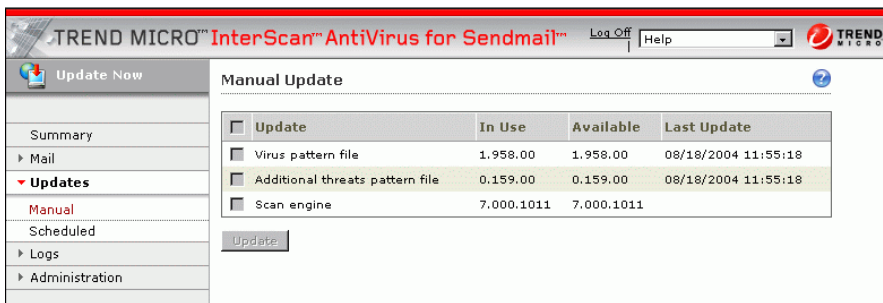
---

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

---

## Manual update

Click **Updates** > **Manual** to display the **Manual Update** screen. If an update is available for a particular component, the component can be selected. For example, the following screen shows that all components are currently up-to-date, because none of the checkboxes can be selected. Also, the “In Use” and “Available” versions for all components match.



**FIGURE 5-2. Manual update feature**

## Manual update, pattern file only

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



## Testing your installation

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

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

---

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

---

### To test your installation's virus scanning:

1. Go to the following URLs:

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

`http://www.eicar.org/anti\_virus\_test\_file.htm`

2. Attach the virus test file to an email message and send it to your administrator's email address.
3. Check the virus logs to see if the detection is reported in the logs. If not, contact customer support for assistance.

Visit the EICAR Web site for more information:

`http://www.eicar.org`

# Configuring InterScan AntiVirus

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

- Fine-tune scanning for viruses and additional threats
- Set action for attachments and messages that contain threats
- Set up notifications to be sent when a threat is detected
- Set up file blocking
- Schedule maintenance of quarantined attachments and messages
- Fine-tune your mail configuration settings
  - Server tab
  - Disclaimer tab
- Schedule maintenance of log files
- Configure alerts to be sent under certain conditions, such as a stopped daemon
- Configure directories for quarantined attachments and messages, and log files
- Configure the proxy for product registration and updates

## Fine-tuning scanning

If you selected “enabled” in the **Mail Filter Virus Scanning** field on the **Modify Sendmail Mail Filter Settings** screen during installation, the virus scanning daemon is running as soon as you complete ISAV installation. However, there are additional settings available on the **Mail > Scanning** screens, that allow you to further customize your SMTP controls. Start with the **Target** tab active.

### To configure SMTP scanning:

1. There are 3 virus scanning modes available:
  - Scanning all file types
  - Scanning only some messages with IntelliScan, which utilizes true file type recognition (this is the default value)
  - Scanning selected files by file name extension

To select a different scanning mode, click the appropriate button in the **Default Scanning** section of this screen.

2. After you select scanning mode, establish the parameters for compressed files that are attached to email messages. For example, to disallow compressed files that are more than 5MB in size, define the size limit in this section of the screen.
3. At the bottom of the **Mail > Scanning** screen, the **Additional Threats Scanning** section of the screen allows you to select other threats that you would like ISAV to detect. The options are:
  - Adware
  - Dialers
  - Hacking Tools
  - Joke Programs
  - Password Cracking Applications
  - RATs (Remote Access Tools)
  - Spyware

While some of these “threats” may have legitimate application in your environment, (for example, one of your company’s system administrators uses remote access tools to manage the network), it is also possible for an intruder to use such a tool to gain access to your network. Decide which additional “threats”

will be allowed. Check those that are not allowed. In the following example, ISAV will scan for all additional threats except adware and remote access tools.

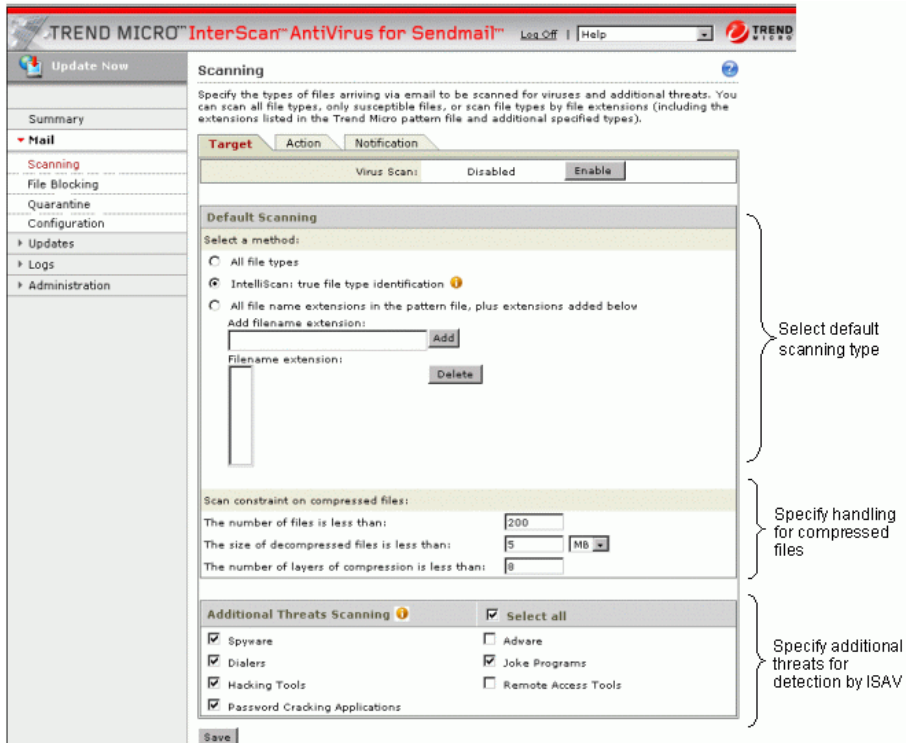


FIGURE 6-1. Mail > Scanning screen with the Target tab active

4. Click **Save** to save your work on this screen. See the online help for the **Mail > Scanning > Target** screen for more information.

## Setting action for attachments and messages

The **Action** tab of the **Mail > Scanning** screen allows you to specify what will be done with threats in attachments and messages when they have been detected by ISAV, or with compressed files that violate the filter criteria.

**To configure action for SMTP threats and violating compressed files:**

1. In the **Action for unsafe attachment** section of the **Mail > Scanning > Action** screen:
  - Select an action from the **Detected files** list for attachments that contain a threat.
  - If you selected “Clean” and the attachment cannot be cleaned, specify what should be done with an uncleanable file in the **Uncleanable files** list.
  - In the **Additional threats** list, specify an action for the additional threats that you selected for detection on the **Target** tab.

---

**Note:** “Pass” allows an attachment to be sent to the client anyway. For additional threats, if you set action to “Pass,” it is the same as allowing the additional threat to remain on your system. This action is not recommended.

---

2. In the **Action for compressed attachment** section of the **Mail > Scanning > Action** screen:
  - Select an action from the **Password protected files** list for password-protected files, which cannot be scanned by ISAV.
  - Select an action from the **Compression constraint violation files** list for compressed files that violate the criteria you selected on the **Target** tab.
3. In the **Action for unsafe messages** section of the **Mail > Scanning > Action** screen:
  - Select an action from the **Unsafe messages** list for messages that contain an attachment for which you specified “Pass” as the action
  - Select an action from the **Malformed messages** list for messages that for some reason violate safe Internet email message standards—the safest action is not to allow these messages into your network by selecting “Reject”
4. Click **Save** to save your work on this screen. See the online help for the **Mail > Scanning > Action** screen for more information.

## Setting up notifications for threats

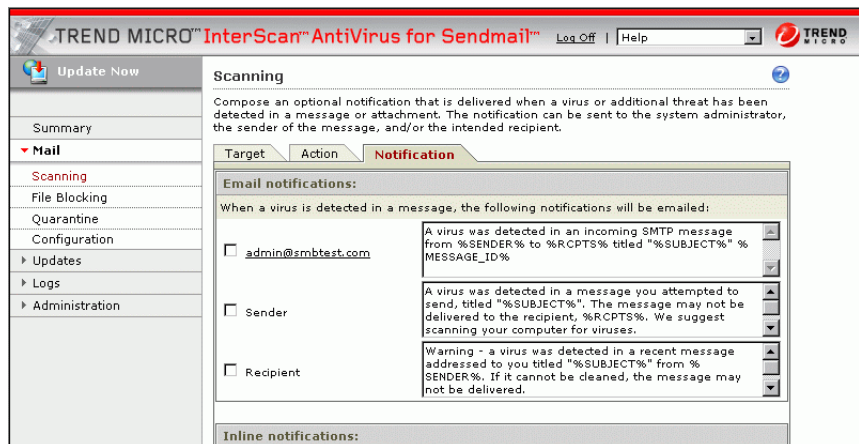
The **Notification** tab of the **Mail > Scanning** screen allows you to specify who will be notified when threats in attachments and messages have been detected by ISAV.

You can also configure inline notifications, such as “This message has been scanned by InterScan AntiVirus and is virus-free.” or “The file called %FILE\_NAME% was infected with the %VIRUS\_NAME% threat. The following action has been taken: %ACTION%.”

**Note:** The variables inside the percent (%) symbols are replaced with live data from your system, for example, “The file called Q3Results was infected with the Worm\_Ratos.A threat. The following action has been taken: Quarantine.” See the online help for detailed instructions on creating notifications using variables (also called tokens).

### To configure notifications for email message threats:

1. In the **Email notifications** section of the screen, there are three configurable recipients for notifications—the administrator, the sender, and the recipient.



**FIGURE 6-2.** Mail > Scanning screen with the Notification tab active

The administrator’s email address appears next to the first checkbox in this section. (This address was set up during installation on the **Modify Notification Settings** screen in the installation script. To change the address, go to **Administration > Configuration > Notification**.) To send a notification to the administrator when a virus or other threat is detected in an email message or attachment, check the admin address and compose your message in the text box

provided. Change the default message that appears in the text box by highlighting and typing over the default text.

2. Repeat this procedure to send a message to the sender, and/or the recipient. Leave the appropriate boxes unchecked to decline sending a notification.
3. Click **Save** to save your work on this screen. See the online help for the **Mail > Scanning > Notification** screen for more information.

## Configuring inline notifications

Inline notifications appear in the body of all messages that meet the notification criteria. Inline notifications can be created on the **Mail > Scanning > Notification** screen, or the **Mail > File Blocking > Notification** screen.

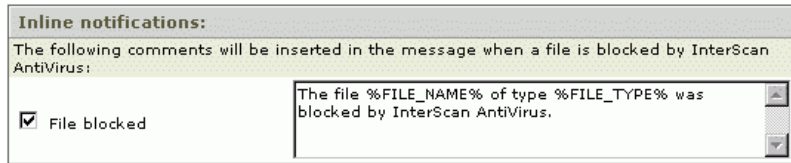
There are 3 types of inline notifications you can create:

- Virus free—A notification that appears in all messages that have been scanned by InterScan AntiVirus and found virus free
- Virus detected—A notification that appears in the message body when an attachment to the message is infected

Inline notifications:	
The following comments will be inserted in all scanned messages and viewable by recipients:	
<input type="checkbox"/> Virus free	Your mail has been scanned by InterScan AntiVirus.
<input checked="" type="checkbox"/> Virus detected	The file %FILE_NAME% was infected with the %VIRUS_NAME% computer virus. The following action has been taken: %ACTION%.

**FIGURE 6-3.** Inline notifications section of the **Mail > Scanning > Notification** screen

- File blocked—A notification that appears in the message body when an attachment to the message is blocked

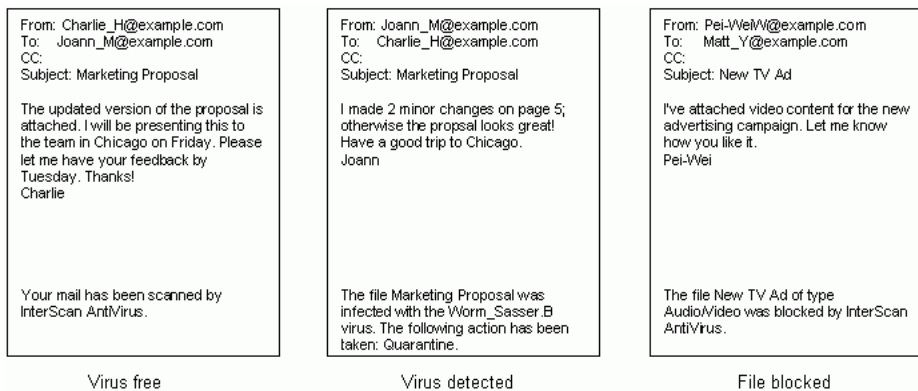


**FIGURE 6-4.** Inline notifications section of the Mail > File Blocking > Notification screen

#### To create an inline notification:

1. Check the notification to be created.
2. Type the notification text in the text box. If a default message is shown in the text box, create your own text by highlighting and typing over the default message.
3. Click **Save** to save your work. See the online help for the **Mail > Scanning > Notification** screen and the **Mail > File Blocking > Notification** screens for more information.

An example of each type of inline notification is shown below:



**FIGURE 6-5.** Examples of inline notifications



## Blocking files

By default, file blocking is not enabled until you manually configure this option. The file blocking feature helps you prevent certain types of content, by file type, from entering your network.

### To configure file blocking:

1. Select **Mail > File Blocking** to display the **File Blocking** screen.
2. On the **File** tab, select the group file types to be blocked, or select all. The options are:
  - Audio/Video
  - Compressed
  - Executable
  - Images
  - Java
  - Microsoft Office
3. On the **Action** tab, in the **Action for unsafe attachment** section of the screen, specify an action for attachments of a blocked file type in the **Detected files** list. If you select “Pass,” the attachment and message are acted upon according to the action displayed next to the **Unsafe messages** field in the **Action for unsafe messages** section of the screen.

---

**Note:** The **Action for unsafe messages** section of the screen is provided for information only. The actions for unsafe messages and malformed messages are the same as those selected on the **Action** tab of the **Scanning** screen. To change the action, click the action link on the **File Blocking** screen. The action tab of the **Scanning** screen displays, and you can change your selection.

---

4. On the **Notification** tab, create notifications for the administrator, sender, and/or recipient. You can also create an inline notification that appears in the message body when an attachment is of a blocked file type. See [Setting up notifications for threats](#) starting on page 6-4 for more information. Also see the online help for the **Mail > File Blocking - Notification** screen.

## Scheduling maintenance

You can manually update the virus pattern file by clicking the Update Now icon in the left navigation panel, by clicking **Update** on the **Summary** screen, or by selecting the virus pattern file for updating on the **Manual Update** screen. See the online help for the **Updates > Manual Update** screen for more information.

To update components on a scheduled basis, go to the **Updates > Scheduled Update** screen to set up a recurring schedule that can be hourly, daily, or weekly. Trend Micro recommends that you update at least daily. See the online help for the **Updates > Scheduled Update** screen for more information.

## Fine-tuning mail settings

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

There are two tabs on the **Mail Configuration** screen. Choose the appropriate tab to complete the following configuration:

- **Server**—Set up or modify basic connections to enable the SMTP service
- **Disclaimer**—Create an optional disclaimer that appears in the beginning or end of the message body for all outgoing messages

### Mail configuration settings - server

When you first display the **Server** tab of the **SMTP Configuration** screen, the fields are pre-populated with values you entered during installation. (After you have completed installation, all required settings that enable the SMTP protocol have been

established.) Enter new values in the fields on this screen to make changes to your SMTP configuration after installation if you choose.

The screenshot shows the 'Mail Configuration' page in the Trend Micro InterScan AntiVirus for Sendmail web interface. The page has a red header with the product name and 'Log Off' and 'Help' links. A left sidebar contains navigation options: 'Update Now', 'Summary', 'Mail' (selected), 'Scanning', 'File Blocking', 'Quarantine', 'Configuration', 'Updates', 'Logs', and 'Administration'. The main content area is titled 'Mail Configuration' and includes a note: 'Some fields on this screen are pre-populated with selections you made during installation. You can change the information at any time.' Below this are three configuration sections: 'Server' (with a sub-tab for 'Disclaimer'), 'Sendmail Mail Filter API (Milter) Configuration', and 'Message Size'. The 'Server' section has 'SMTP server' set to '10.2.15.51' and 'Port' set to '25'. The 'Milter' section has 'Filter Setting' set to 'inet:10025@10.2.14.110'. The 'Message Size' section has two checked options: 'Reject messages with more than 100 recipients' and 'Reject messages larger than 30 MB'. A 'Save' button is located at the bottom of the configuration area.

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

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

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

## Mail configuration settings - disclaimer

The **Disclaimer** tab of the **Mail Configuration** screen contains fields that allow you to create an optional disclaimer that is appended to the beginning or end of all outgoing messages.

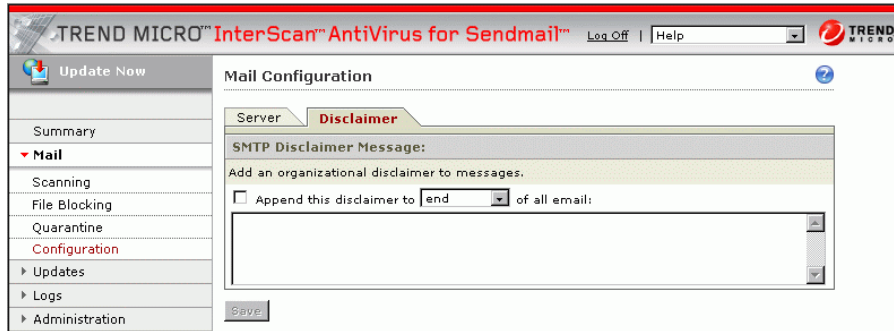


FIGURE 6-6. Mail Configuration screen - Disclaimer tab active

A sample disclaimer is shown in the online help.

## Configuring alerts

The **Alerts** tab of the **Administration > Configuration** screen allows you to configure optional notifications that alert you when the following conditions are met:

- A service has stopped for more than a specified number of minutes
- The quarantine directory is nearly full

- A scheduled update was successfully completed

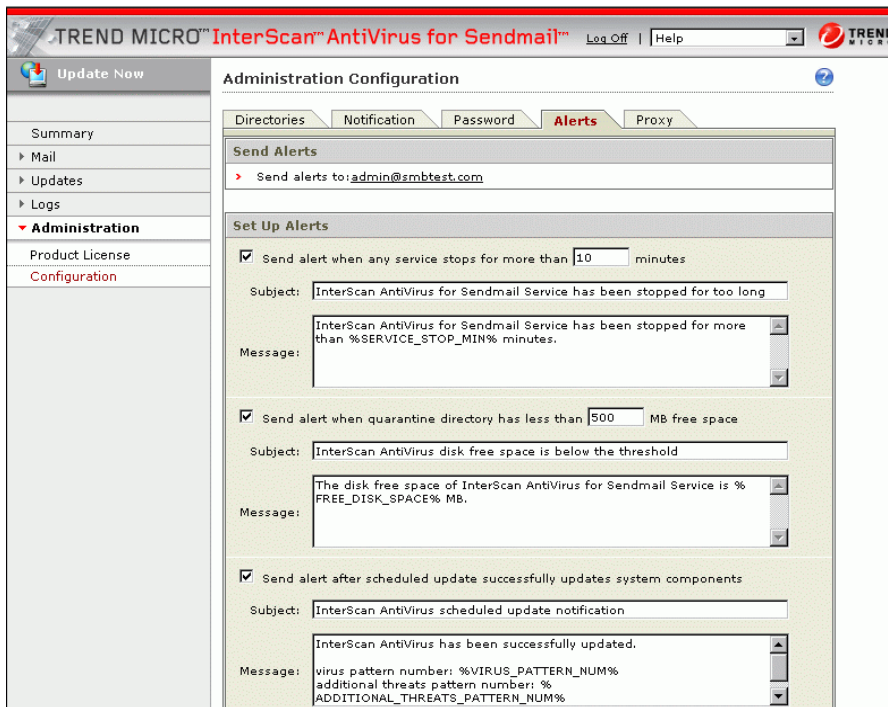


FIGURE 6-7. Alerts tab on the Administration > Configuration screen

Alerts are sent to the administrator's email address, which was set up during installation on the **Modify Notification Settings** screen in the installation script.

To change the address, go to the **Notification** tab of the **Administration > Configuration** screen. To change the password associated with the administrator's user ID, go to the **Password** tab of the **Administration > Configuration** screen.

## Scheduling maintenance of log files

Select **Logs > Maintenance** to display the **Log Maintenance** screen. Set up a schedule to automatically purge log entries after a specified number of days, weeks, or months. The default value is 30 days.

## Configuring directories

The location of the quarantine directory for infected attachments and messages, and the log directory, defaults to the following:

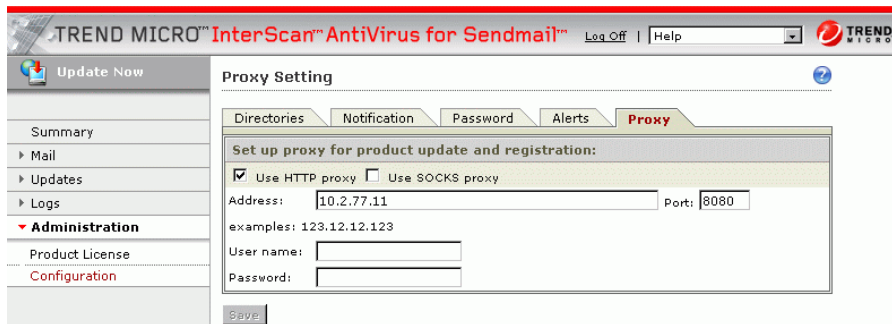
- *<destination directory selected during installation>/quarantine/attachment*
- *<destination directory selected during installation>/quarantine/message*
- *<destination directory selected during installation>/logs*

The destination directory is selected during installation, on the **Choose Destination Directory** screen. For example, if the destination directory path selected during installation is “opt/trend/isav,” the default log directory is “opt/trend/isav/log.”

You can change your selections on the **Directories** tab for the **Administration > Configuration** screen. See the online help for more information.

## Configuring the proxy

A proxy can be used to access the Trend Micro Online Registration and ActiveUpdate servers for product registration and product updates (such as downloading an updated virus pattern file to your network). All of the proxy settings are configured during installation, on the **Modify Default HTTP Proxy Settings** screen.



**FIGURE 6-8.** Administration Configuration screen - Proxy tab active

To change proxy settings, go to the **Proxy** tab of the **Administration > Configuration** screen (shown above). See the online help for more information.

---

# Troubleshooting

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

- Cannot log on
- Activation Code is invalid
- No log or quarantine directory
- Cannot update the pattern file
- Management console timed out
- Performance seems degraded
- Virus is detected but cannot be cleaned

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

To contact Trend Micro support, visit:

<http://kb.trendmicro.com>

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

## Issues

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

### Cannot log in

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

### Activation Code is invalid

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

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

### No log or quarantine directory

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



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

## Cannot update the pattern file

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

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

## Management console timed out

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

## Performance seems degraded

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

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

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

## Virus is detected but cannot be cleaned

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

<http://subwiz.trendmicro.com/SubWiz/Default.asp>

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

## Virus scanning not working

Ensure that no one has disabled the virus scanning feature on the **Mail > Scanning > Target** screen. If scanning is enabled but viruses are not being detected, contact technical support for assistance.

## Free detection tools

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

## Knowledge Base

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

<http://kb.trendmicro.com>

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

## Virus information center

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

<http://trendmicro.com/vinfo/default.asp>

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

- **Virus advisories**—current news about the top threats, associated risks, and the pattern file update that addresses the threat
- **Weekly Virus Report**—current news about threats that have appeared in the past week

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

## Global support centers

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

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

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

<http://www.trendmicro.com/support>

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

## Before contacting technical support

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

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

## Glossary of Terms

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

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

<b>Term</b>	<b>Explanation</b>
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, and additional threats pattern file.
additional threats	Files that may have a legitimate commercial value, or can be misused to gain unauthorized access to your computer or networking environment. Examples are adware, dialers, hacking tools, password-cracking tools, and so on.
address	Refers to a networking address (see IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to "system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of InterScan AntiVirus to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a "backdoor"; tracking mechanism on the user's computer without the user's knowledge is called "spyware."
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.

Term	Explanation
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
boot sector	A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer's operating system.
boot sector virus	A virus targeted at the boot sector (the operating system) of a computer.
browser	A program which allows a person to read hypertext, such as Internet Explorer or Netscape Navigator. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast portion of memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
cause	The reason a protective action, such as file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from an attachment file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to protocol, asking for information or action, and the server responds.

Term	Explanation
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how InterScan AntiVirus will function, for example, selecting whether to quarantine or delete a virus-infected email message.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, <i>/opt/trend/isav</i> is the default installation directory on your system.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISAV log directory is: <i>/opt/trend/isav/log</i>
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message. To see an example, click the online help for the <b>Mail Configuration - Disclaimer</b> screen.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.



Term	Explanation
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution," uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
download (noun)	Data that has been downloaded, for example, from a Web site via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or attachment.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
file name extension	The portion of a file name (such as .txt or .xml) which typically indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.

Term	Explanation
filter criteria	User-specified guidelines for determining whether a message and attachment(s), if any, will be delivered, such as: - size of the message body and attachment - file type of the attachment
filter setting	The internet port and IP address that enables Sendmail to communicate with the ISAV daemon, expressed in the following format: inet (internet):<port number>@<IP address> For example: inet:10025@123.123.123.123  For more information about configuring Sendmail filter settings, go to: <a href="http://www.milter.org">http://www.milter.org</a>
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
gateway	An interface between an information source and a Web server.
group file type	Types of files that have a common theme. There are six group file types in the InterScan AntiVirus interface, they are: - Audio/Video - Compressed - Executable - Images - Java - Documents
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hacker	See virus writer
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.

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

<b>Term</b>	<b>Explanation</b>
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—See IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of memory.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
license	Authorization by law to use InterScan AntiVirus.
license certificate	A document that proves you are an authorized user of InterScan AntiVirus.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.

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

Term	Explanation
message subject	The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. <i>Also see SMTP server.</i>
multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.
MX record	A DNS resource record type indicating which host can handle electronic mail for a particular domain.
notification ( <i>Also see action and target</i> )	A message that is forwarded to one or more of the following: <ul style="list-style-type: none"> <li>- system administrator</li> <li>- sender of a message</li> <li>- recipient of a message</li> </ul> The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an email message attachment.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data <i>leaving</i> your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. ( <i>Also see sector, which is a physical portion of a disk.</i> )
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.

Term	Explanation
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
PC	Personal Computer—A general-purpose single-user micro-computer designed to be operated by one person at a time.
polymorphic virus	A virus that is capable of taking different forms.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected email messages, email messages with infected attachments, or email affected by additional threats in an isolated directory (the Quarantine Directory) on your Inter-Scan AntiVirus server. The Quarantine Directory is typically located in the following directory path: <i>/opt/trend/isav/quarantine</i>
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.

Term	Explanation
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. <i><a href="https://olr.trendmicro.com/registration">https://olr.trendmicro.com/registration</a></i>
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNWB <i>Also see Activation Code</i>
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
removable drive	A removable hardware component or peripheral device of a computer.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
sector	A physical portion of a disk. ( <i>Also see partition, which is a logical portion of a disk.</i> )
seat	A license for one person to use InterScan AntiVirus.
Secure Password Authentication	An authentication process, by which communications can be protected, using for example, encryption and challenge/response mechanisms.
sender	The person who is sending an email message to another person or entity.



Term	Explanation
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations. Inter-Scan AntiVirus can act as the SMTP server, so that virus scanning, content filtering, and spam detection take place before the message is delivered to the recipient.
SOCKS	A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.
SOCKS proxy	The proxy used in your network for TCP traffic.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.
status bar	A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.
target (A/so see action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—One of the main protocols used in TCP/IP (Transmission Control Protocol/Internet Protocol) networks.

Term	Explanation
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
threat	An inclusive term referring to viruses, Trojans, worms, spyware, adware, dialers, joke programs, and so on.
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host <i>wombat.doc.ic.ac.uk</i> is in top-level domain "uk" (for United Kingdom).
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
trigger	An event that causes an action to take place. For example, InterScan AntiVirus detects a virus in an email message. This <i>triggers</i> the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan	A malicious program that is disguised as something benign.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
unsafe attachment	An attachment to an email message that: <ul style="list-style-type: none"><li>- contains a threat, such as a virus or additional threat,</li><li>- contains an attachment that is a blocked file type</li><li>- is password-protected and cannot be scanned</li></ul>
unsafe message	A message that contains an unsafe attachment.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, <i>www.trendmicro.com</i> . The URL maps to an IP address using DNS.

Term	Explanation
virus	<p>A computer virus is a program – a piece of executable code – that has the unique ability to infect and replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.</p> <p>In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.</p>
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a malicious computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
working directory	The destination directory in which the main application files are stored.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
zip file	A compressed archive (in other words, “zip file”) from one or more files using an archiving program such as WinZip.
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.

## Utilities in InterScan Antivirus

The following description of utilities in the ISAV application are provided for your information only. Trend Micro does not recommend changing the content of the files.

<i>Invoked by</i>	<i>File Name</i>	<i>Description</i>
manually invoked	reset_password.sh	This script resets the administrator's password to "password" - you must have root privilege to execute the script
cron daemon	TmlsuxPurgeLog	This utility cleans up outdated logs and quarantined files
cron daemon	TmlsuxUpdate	This utility manages scheduled updates

---

## Migration Settings

The table in this Appendix describes the settings in the “intscan.ini” file from a previous installation of Trend Micro InterScan VirusWall™ that can be preserved during installation of InterScan AntiVirus.

Some settings appear in the user interface and can be modified in the management console. Other settings can be modified only by changing entries in the ISAV “isav.ini” file.

---

**Note:** The “intscan.ini” file in legacy versions of InterScan VirusWall allowed for plain text entries, such as “Monday, Tuesday, Wednesday.” In InterScan Antivirus, most parameter values are expressed as numbers, for example, “0=Monday, 1=Tuesday, 2=Wednesday,” and so on.

---

## ISAV “isav.ini” file settings

ISVW Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVW: [admin] num_pattern_kept  ISAV: [admin] num_pattern_kept	Number of old pattern files kept for rollback purposes. For example, if you are currently on pattern file 833, you might want to keep 832 and even 831 in case of rollback.  <u>Valid Values</u> 1 = 1 2 = 2, and so on	N	
ISVW: [ismilter] svcport  ISAV: [milter] milter_conn	The filter setting, in the format inet:<port>@<server IP used for listening by the ISAV daemon>  <u>Valid Values</u> Must use the format described above.  This parameter is set up during installation, in the Mail Filter Setting field on the Modify Sendmail Mail Filter Settings screen.	Y	<b>Filter Setting</b> field on the Server tab of the Mail > Configuration screen
ISVW: [ismilter] verbose  ISAV: [logs] log_level	Designates whether log files display in terse or verbose mode (verbose mode includes more details).  <u>Valid Values</u> 0 = no 3 = yes	N	
ISVW: [notification] port  ISAV: [notification] smtp_server_port	Designates the port of the server to which notifications are sent.  <u>Valid Values</u> 1 - 65535  This parameter is set up during installation, in the Notification Email Server Port field on the Modify Notification Settings screen.	Y	<b>Port</b> field on the Notification tab of the Administration > Configuration screen

<b>ISVW Sendmail 3.6/ISAV Parameter Key and Name</b>	<b>Description</b>	<b>Appear in UI?</b>	<b>If in UI, Where Does it Appear?</b>
ISVW: [notification] server  ISAV: [notification] smtp_server_addr	Designates the server IP of the server to which notifications are sent.  <u>Valid Values</u> IP address format  This parameter is set up during installation, in the Notification Email Server Address field on the Modify Notification Settings screen.	Y	<b>SMTP server</b> field on the Notification tab of the Administration > Configuration screen
ISVW: [pattern update] DayOfWeek1  ISAV: [active_update] schedule_update_dd	If you select weekly for the [active_update] schedule_update_method parameter, the schedule_update_dd parameter determines the day of the week on which updates occur.  <u>Valid Values</u> 0 = Monday 1 = Tuesday 2 = Wednesday 3 = Thursday 4 = Friday 5 = Saturday 6 = Sunday  <b>Note:</b> The time of day selected for a weekly update is not migrated.	Y	<b>Weekly, every &lt;day of the week list&gt;</b> field on the Updates > Scheduled > Scheduled Update screen
ISVW: [pattern update] F requency  ISAV: [active_update] schedule_update_method	This parameter determines whether scheduled updates occur hourly, daily, or weekly.  <u>Valid Values</u> 0X00000001 = hourly 0X00000002 = daily 0X00000004 = weekly	Y	<b>Hourly/Daily/Weekly</b> radio buttons on the Updates > Scheduled > Scheduled Update screen

ISVW Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVW: [registration] reg_proxy ISAV: [proxy] proxy_addr	<p>Designates the proxy IP of the server used for communicating with the Trend Micro customer registration and ActiveUpdate servers, to register your products online, and to download updates to your virus and additional threats pattern files, and the virus scan engine.</p> <p><u>Valid Values</u> IP address format</p> <p>This parameter is set up during installation, in the Proxy IP field on the Modify Default HTTP Proxy Settings screen.</p>	Y	<b>Address</b> field on the Proxy tab of the Administration > Configuration screen
ISVW: [registration] reg_port ISAV: [proxy] proxy_port	<p>Designates the port of the proxy server used for communicating with the Trend Micro customer registration and ActiveUpdate servers, to register your products online, and download updates to your virus and additional threats pattern files, and the virus scan engine.</p> <p><u>Valid Values</u> 1 - 65535</p> <p>This parameter is set up during installation, in the Proxy Port field on the Modify Default HTTP Proxy Settings screen.</p>	Y	<b>Port</b> field on the Proxy tab of the Administration > Configuration screen



ISVW Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVW: [registration] use_proxy  ISAV: [proxy] use_proxy	Designates whether you will use your existing HTTP proxy to communicate with the Trend Micro ActiveUpdate server, to download updates to your virus and additional threats pattern files, and the virus scan engine.  <u>Valid Values</u> 0 = no 1 = yes  This parameter is set up during installation, in the Use Proxy field on the Modify Default HTTP Proxy Settings screen.	Y	<b>Use HTTP proxy</b> field on the Proxy tab of the Administration > Configuration screen
ISVW: [scan_configuration] extract_limit_size  ISAV: [VSAPI] decompress_size	The flag for the decompress_size_limit parameter (which determines the maximum size in megabytes for a compressed file before it is blocked by ISAV - see the following parameter below).	N	
ISVW: [scan_configuration] extract_limit_size  ISAV: [VSAPI] decompress_size_limit	This parameter determines the maximum size in megabytes (MB) for a compressed file before it is blocked by ISAV.  <u>Valid Values</u> 0 - 1000M	Y	<b>The size of decompressed files is less than:</b> field on the Mail > Scanning screen
ISVW: [scan_configuration] multi_scan_times  ISAV: [virus_filter] multiple_scan_times	This parameter determines the number of times ISAV will re-scan an infected file. For example, ISAV may find and clean a virus in an attachment during the first scan. If this value is set to 5, ISAV will recheck the attachment to verify that the file is now clean. If a second threat is found, ISAV will clean and recheck again, until the file is clean or the maximum value below is attained.  <u>Valid Values</u> 1 - 15	N	

ISVV Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVV: [scan_configuration] sml_scan  ISAV: [milter] virus_filter	This parameter determines whether virus scanning is enabled.  <u>Valid Values</u> 0 = no 1 = yes  This parameter is set up during installation, in the Mail Filter Virus Scanning field on the Modify Sendmail Mail Filter Settings screen.	Y	<b>Virus Scan</b> field on the Target tab of the Mail > Scanning screen
ISVV: [smtp] admin_addr  ISAV: [admin] email_address	This parameter sets the administrator's email address for notifications.  <u>Valid Values</u> format is: <admin name> @<email server address>  This parameter is set up during installation, in the Admin Email Address field on the Modify Notification Settings screen.	Y	<b>Administrator's default email address</b> displayed next to the first checkbox in the Email notifications section of the Notification tab for the the Mail > Scanning screen
ISVV: [smtp] admin_msg  ISAV: [notification] email_virus_detected_admin_msg	This parameter points to the location of a file that contains the text of the notification sent to the administrator when "Detected files" is triggered on the Mail> Scanning > Action screen.  <u>Valid Values</u> Text string	N	

<b>ISVW Sendmail 3.6/ISAV Parameter Key and Name</b>	<b>Description</b>	<b>Appear in UI?</b>	<b>If in UI, Where Does it Appear?</b>
ISVW: [smtp] extensions  ISAV: [virus_filter] scan_extension	This parameter controls the filename extensions that are scanned, in addition to those already in the Trend Micro virus pattern file, if the user selects "All file name extensions in the pattern file, plus extensions added below" as the default scanning method on the Mail > Scanning > Target screen.  <u>Valid Values</u> Text strings indicating the extension(s) to be scanned	Y	<b>Filename extension</b> field on the Target tab of the Mail > Scanning screen
ISVW: [smtp] from_addr  ISAV: [notification] sender	The email address that will be used to send notifications that the message was infected or blocked.  <u>Valid Values</u> Text string indicating the email address, in the following format: <name>@<IP address>	N	
ISVW: [smtp] level  ISAV: [virus_filter] scan_level	This parameter determines the default scanning method for virus scanning.  <u>Valid Values</u> 0 = Scan all file types 1 = Scan with IntelliScan 2 = Scan by file name extension	Y	<b>The All file types, IntelliScan, and All file name extensions...</b> radio buttons on the Target tab of the Mail > Scanning-screen
ISAV: [message] max_size	The flag for the max_size_limit parameter (which determines the maximum size in megabytes for a message before it is blocked by ISAV - see the following parameter below).  <u>Valid Values</u> 0 = message is blocked 1 = message is accepted	N	<b>The text box</b> displayed next to the administrator's email address checkbox in the Email notifications section of the Notification tab on the the Mail > Scanning screen

ISVV Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVV: [smtp] msg_size ISAV: [message] max_size_limit	This parameter allows you to specify the maximum message size in megabytes (MB) to be accepted in your network.  <u>Valid Values</u> 1 - 999	Y	The <b>Reject messages larger than</b> field on the Server tab of the Mail > Configuration screen
ISVV: [smtp] notify_admin ISAV: [notification] email_virus_detected_admin	This parameter determines whether a notification is sent to the administrator when a threat is detected.  <u>Valid Values</u> 0 = no 1 = yes	Y	The <b>checkbox</b> displayed next to the administrator's default email address in the Email notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] notify_sender ISAV: [notification] email_virus_detected_sender	This parameter determines whether a notification is sent to the sender of a message when a threat is detected.  <u>Valid Values</u> 0 = no 1 = yes	Y	The <b>Sender checkbox</b> displayed in the Email notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] notify_user ISAV: [notification] email_virus_detected_recipient	This parameter determines whether a notification is sent to the recipient of a message when a threat is detected.  <u>Valid Values</u> 0 = no 1 = yes	Y	The <b>Recipient checkbox</b> displayed in the Email notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] rlocation ISAV: [notification] inline_msg_location	This parameter determines whether an inline notification (virus free, virus detected, or file blocked) is inserted at the beginning or end of the message body.  <u>Valid Values</u> 0 = beginning 1 = end  <b>Note:</b> This setting is not the same as the "Append this disclaimer to" field on the Disclaimer tab of the Mail > Configuration screen.	N	

ISVV Sendmail 3.6/ISAV Parameter Key and Name	Description	Appear in UI?	If in UI, Where Does it Appear?
ISVV: [smtp] safe_message  ISAV: [notification] inline_virus_free_msg	This parameter points to the location of a file that contains the text of the "virus free" inline notification message.  <u>Valid Values</u> Text string	Y	The <b>text box</b> displayed next to the Virus free checkbox in the Inline notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] safe_stamp  ISAV: [notification] inline_virus_free	This parameter controls the text of the "virus free" inline notification message.  <u>Valid Values</u> 0 = no 1 = yes	Y	The <b>Virus free checkbox</b> in the Inline notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] sender_msg  ISAV: [notification] email_virus_detected_sender_msg	This parameter points to the location of a file that contains the text of the notification sent to the sender when "Detected files" is triggered on the Mail> Scanning > Action screen.  <u>Valid Values</u> Text string	Y	The <b>text box</b> displayed next to the Sender checkbox in the Email notifications section of the Notification tab on the Mail > Scanning screen
ISVV: [smtp] user_msg  ISAV: [notification] email_virus_detected_recipient_msg	This parameter points to the location of a file that contains the text of the notification sent to the recipient when "Detected files" is triggered on the Mail> Scanning > Action screen.  <u>Valid Values</u> Text string	Y	The <b>text box</b> displayed next to the Recipient checkbox in the Email notifications section of the Notification tab on the Mail > Scanning screen

## ISAV Services

The table in this Appendix describes how to start, stop, restart, and check the status of ISAV-related services. The services are:

- **Admin Console**—This service supports the management console; without this service, you cannot configure ISAV from the user interface
- **Notification Service**—This service is responsible for email notifications and alerts; if this service is off, no alerts or notifications are sent by ISAV
- **ISAV Mail Filter**—This service interacts with Sendmail to scan SMTP traffic for malicious content; if this service is off, you cannot process email messages

There are four arguments for each service command. The arguments are:

- **start**—Starts the service
- **stop**—Stops the service
- **restart**—Stops and starts the service
- **status**—Verifies whether the service is running

### Commands to Manage ISAV Services

Service	Command
Admin Console	/etc/init.d/isuid {stop start restart status}
Notification Service	/etc/init.d/isnotd {stop start restart status}
ISAV Mail Filter	/etc/init.d/isavd {stop start restart status}

# Index

## A

- activating InterScan AntiVirus 4-5
- Activation Code 2-5
  - format of 2-5
- activation of ISAV 2-5
- additional threats pattern file 5-3
- alerts
  - configuring 6-11
- attachments
  - setting action for infected 6-3
- available documentation 1-2

## B

- benefits of using InterScan AntiVirus 1-1
- blocking files 6-8

## C

- configuring
  - alerts 6-11
  - directories 6-13
  - inline notifications 6-6
  - mail disclaimer 6-11
  - mail server settings 6-9
  - notifications 6-4
  - proxy 6-13

## D

- directories
  - configuring 6-13

## E

- Enter Registration Key screen 4-4

## F

- features of InterScan AntiVirus 1-1
- file blocking 6-8
- fine-tuning scanning 6-2

## G

- glossary 1-2, A-1

## I

- inet mode 2-7
- inline notifications
  - configuring 6-6
  - examples of 6-7
- installation 3-1
  - destination directory for ISAV 2-4
  - post-installation steps 3-9
  - removing ISAV 3-12
  - testing 3-9
  - when to install 2-9
- installation planning 2-1
- installation script 1-2
- IPv4 socket (inet) mode 2-7

## K

- kb.trendmicro.com/solutions/solutionSearch.asp 7-4
- Knowledge Base 1-3, 7-4

## L

- license certificate 4-2
- log files
  - maintenance 6-11
- logon ID and password-Online Registration screen 4-3–4-4

## M

- mail configuration
  - disclaimer 6-11
  - fine-tuning settings 6-9
  - server 6-9
  - settings 6-9
- mail filter settings
  - IPv4 socket (inet) mode 2-7
  - Unix-domain socket mode 2-7
- maintenance of pattern file
  - manual update 6-9
  - scheduling periodic 6-9
- management console 1-3
- management console-opening from browser 1-8
- messages
  - setting action for infected 6-3
- migration settings C-1
- My Product Details screen 3-12

## **N**

- navigation panel 1-3
- notifications for threats
  - setting up 6-4

## **O**

- online help 1-7
  - context-sensitive 1-2
  - general help 1-2
  - search feature 1-7
- Online Registration screen 4-3
- opening a management console from a browser 1-8

## **P**

- pre-installation checklist 2-3
- Product License screen 3-11
- proxy
  - configuring 6-13

## **R**

- Readme file 1-2
- recommended system requirements 2-2
- registering InterScan AntiVirus 4-2
- Registration Key 2-5
  - format of 2-5
  - where to find 4-2
- registration of ISAV 2-5

## **S**

- Safe Computing Guide 7-5
- scan engine
  - defined 5-2
- scanning
  - fine-tuning 6-2
- scheduling log file maintenance 6-11
- setup script 3-3
- support
  - contacting 7-6
  - global support centers 7-5

## **T**

- tab behavior 1-4
- test files 7-5
- TrendLabs 7-5
- troubleshooting 7-1
  - Activation Code not valid 7-2

- cannot update pattern file 7-3
- logon difficulties 7-2
- management console timed out 7-3
- no log directory 7-2
- no quarantine directory 7-2
- performance degraded 7-3
- virus detected but not cleaned 7-3
- virus scanning not working 7-4

## **U**

- Unix-domain socket mode 2-7
- updating
  - scan engine 5-1
  - virus pattern file 5-1
- URLs
  - documentation download site 1-i, 2-4
  - documentation evaluation site 1-ii
  - EICAR site 5-5
  - EICAR test script site 5-5
  - Knowledge Base site 1-3, 7-4
  - pattern file version on Trend Micro site 5-2
  - product registration site 4-3
  - registration and activation solution site 4-6
  - registration FAQ site 4-6
  - Trend Micro support site 7-2, 7-5
  - Trend Micro Virus Submission Wizard site 7-3
  - Virus Information Center site 7-4
- utilities in InterScan Antivirus B-1

## **V**

- virus advisories 7-4
- Virus Encyclopedia 7-5
- Virus Information Center 7-4
- Virus Map 7-5
- virus pattern file
  - defined 5-1
- Virus Primer 7-5
- virus risk ratings 7-5

## **W**

- Webmaster tools 7-5
- Weekly Virus Report 7-4