

# F-Secure Anti-Virus

for MIMESweeper

Administrator's Guide



"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:

GB2353372	GB2366691	GB2366692	GB2366693
GB2367933	GB2368233	GB2374260	

Copyright © 1993-2005 F-Secure Corporation.

Portions Copyright © 1991-2004 Kaspersky Lab.

All rights reserved.

12000073-5E16

# Contents

<b>About This Guide</b>	<b>5</b>
How This Guide Is Organized .....	6
Conventions Used in F-Secure Guides .....	7
Symbols .....	7
<b>Chapter 1 Introduction</b>	<b>9</b>
1.1 Overview .....	10
1.2 MIMESweeper Product Family .....	11
1.3 Features .....	12
<b>Chapter 2 Installation</b>	<b>13</b>
2.1 Deployment .....	14
2.2 System Requirements .....	15
2.3 Installation Steps .....	15
<b>Chapter 3 Configuration</b>	<b>19</b>
3.1 Configuring F-Secure Anti-Virus for MIMESweeper .....	20
3.2 Configuring Content Scanner Scenario .....	25
3.3 Configuring Alert Forwarding .....	28
<b>Chapter 4 Updating Virus Definition Databases</b>	<b>33</b>
4.1 Overview .....	34
4.2 Automatic Updates .....	34

4.3	Manual Updates .....	35
4.3.1	Using FSUPDATE .....	35
4.3.2	Using LATEST.ZIP .....	35
4.3.3	Updating the Virus Definition Database Remotely .....	35

## **Technical Support 37**

Overview .....	38
F-Secure Online Support Resources .....	38
Web Club .....	39
Virus Descriptions on the Web.....	39

## **About F-Secure Corporation**

# ABOUT THIS GUIDE

How This Guide Is Organized.....	6
Conventions Used in F-Secure Guides .....	7

## How This Guide Is Organized

F-Secure Anti-Virus for MIMESweeper Administrator's Guide is divided into the following chapters:

**Chapter 1. *Introduction.*** General information on F-Secure Anti-Virus for MIMESweeper and other F-Secure Anti-Virus products.

**Chapter 2. *Installation.*** Instructions on how to install and deploy F-Secure Anti-Virus for MIMESweeper.

**Chapter 3. *Configuration.*** Instructions on how to configure F-Secure Anti-Virus for MIMESweeper, Content Scanner Scenario and Alerts.

**Chapter 4. *Updating Virus Definition Databases.*** Instructions on how to keep virus definition databases up-to-date.

***Technical Support.*** Instructions on how to get technical support for problems in F-Secure Anti-Virus products.

***About F-Secure Corporation*** Describes the company background and products.

## Conventions Used in F-Secure Guides

This section describes the symbols, fonts, and terminology used in this manual.

### Symbols



**WARNING:** The warning symbol indicates a situation with a risk of irreversible destruction to data.



**IMPORTANT:** An exclamation mark provides important information that you need to consider.



**REFERENCE** - A book refers you to related information on the topic available in another document.



**NOTE** - A note provides additional information that you should consider.



**TIP** - A tip provides information that can help you perform a task more quickly or easily.

⇒ An arrow indicates a one-step procedure.

### Fonts

**Arial bold (blue)** is used to refer to menu names and commands, to buttons and other items in a dialog box.

*Arial Italics (blue)* is used to refer to other chapters in the manual, book titles, and titles of other manuals.

*Arial Italics (black)* is used for file and folder names, for figure and table captions, and for directory tree names.

Courier New is used for messages on your computer screen.

**Courier New bold** is used for information that you must type.

**SMALL CAPS (BLACK)** is used for a key or key combination on your keyboard.

[Arial underlined \(blue\)](#) is used for user interface links.

Times New Roman regular is used for window and dialog box names.

## PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

## For More Information

Visit F-Secure at <http://www.f-secure.com> for documentation, training courses, downloads, and service and support contacts.

In our constant attempts to improve our documentation, we would welcome your feedback. If you have any questions, comments, or suggestions about this or any other F-Secure document, please contact us at [documentation@f-secure.com](mailto:documentation@f-secure.com).

# 1

## INTRODUCTION

Overview.....	10
MIMEsweeper Product Family.....	11
Features .....	12

## 1.1 Overview

Malicious code, such as computer viruses, is one of the main threats for companies today. When users began to use office applications with macro capabilities to write documents and distribute them via mail and groupware servers, macro viruses started spreading rapidly.

After the millennium, the most common spreading mechanism has been the e-mail. Today about 90% of viruses arrive via e-mail. E-mails provide a very fast and efficient way for viruses to spread without any user intervention and this is why e-mail worm outbreaks, like Bagle, Sober and Mydoom, cause a lot of damage around the world.

The Internet is used by more and more people every day, which opens another, so far dormant channel, HTTP, for viruses to spread. F-Secure Anti-Virus Mail Server and Gateway products are designed to protect your company's mail and groupware servers and to shield the company network from any malicious code that travels in HTTP, FTP-over-HTTP or SMTP traffic. The protection can be implemented on the gateway level to screen all incoming and outgoing e-mail (SMTP), web surfing (HTTP) and file transfer (FTP) traffic. Furthermore, it can be implemented on the mail server level so that it not only protects inbound and outbound traffic but also internal mail traffic and public sources, such as Public Folders on Microsoft Exchange servers.

Providing the protection already on the gateway level has many advantages: the protection is easy and fast to set up and install, and it is invisible to the end users, which ensures that the system cannot be by-passed and is easy to maintain. Protecting the gateway level alone, however, is not enough to provide a complete antivirus solution; file server and workstation level protection is needed, too.

## 1.2 MIMESweeper Product Family

Clearswift, manufacturer of the MIMESweeper product family, provides complete content security solutions for email and Web traffic. With Clearswift MIMESweeper for SMTP, the company is protected against every content-based email threat from spam to employee time-wasting, circulation of pornography, breaches in confidentiality, legal liability and IT resource misuse. Clearswift MIMESweeper for Web does for web traffic what Clearswift MIMESweeper for SMTP does for SMTP: analyzes every bit of traffic and removes every kind of content threat.

F-Secure integrates antivirus protection and disinfection with Clearswift MIMESweeper for SMTP and MIMESweeper for Web, creating a complete, integrated solution to detect and disinfect the Web- or e-mail-borne viruses already at the gateway level. F-Secure Anti-Virus for MIMESweeper works together with the Clearswift products MIMESweeper for SMTP and MIMESweeper for Web.

### F-Secure Anti-Virus for MIMESweeper

F-Secure Anti-Virus for MIMESweeper provides a powerful antivirus scanning solution that tightly integrates with Clearswift MIMESweeper for SMTP and MIMESweeper for Web products giving the corporation the powerful combination of complete content security.

There are three integration scenarios you can use with F-Secure Anti-Virus. First, the **Content Scanner scenario** provides the most effective integration and is the recommended way to set up the system. Second, the **F-Secure Anti-Virus scenario** provided by Clearswift integrates with the memory resident F-Secure Anti-Virus. Finally, when using the command line interface to F-Secure Anti-Virus, you can use the **Virus Manager scenario** provided by Clearswift. Although not as efficient a scenario as the other two presented above, in this scenario the antivirus scanner remains resident in memory, which means the command line does not reload the scanner every time.

A Content Scanner scenario needs to be created using the MIMESweeper console. This scenario determines what is scanned for viruses and what happens if a virus is found. For configuring Content Scanner Scenario, see "[Configuring Content Scanner Scenario](#)", 25.

## 1.3 Features

F-Secure Anti-Virus for MIMESweeper, as well as all other F-Secure Anti-Virus Mail Server and Gateway products, has the following features:

### Powerful and Always Up-to-date

F-Secure Anti-Virus for MIMESweeper uses the award-winning F-Secure Anti-Virus scanner to ensure the highest possible detection rate and disinfection capability. The daily virus definition database updates provide protection that is always up to date.

### Easy to Administer

F-Secure Anti-Virus for MIMESweeper can be managed either in stand-alone mode or remotely using the powerful F-Secure Policy Manager.

### Superior Protection

- High level of protection with low maintenance costs
- Superior detection rate with multiple scanning engines
- Unparalleled malicious code detection and disinfection. F-Secure Anti-Virus for MIMESweeper detects all known viruses, worms and Trojans, including Java and ActiveX viruses
- Heuristic scanning detects also unknown macro viruses
- Automatic daily virus definition database updates

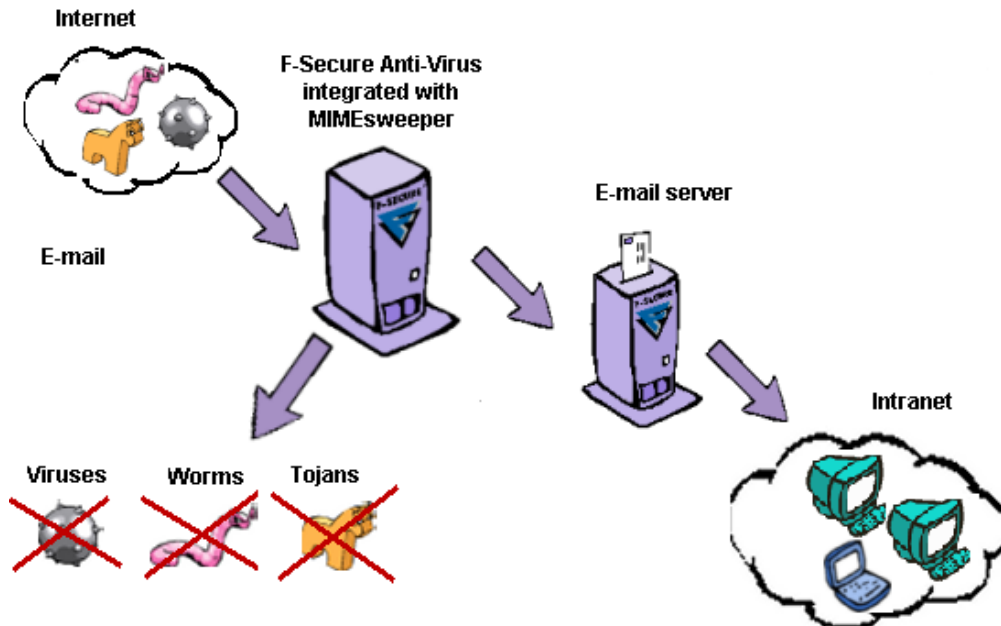
# 2

## INSTALLATION

Deployment .....	14
System Requirements .....	15
Installation Steps .....	15

## 2.1 Deployment

F-Secure Anti-Virus for MIMESweeper is always installed on the same machine where MIMESweeper for SMTP or MIMESweeper for Web is running.



## 2.2 System Requirements

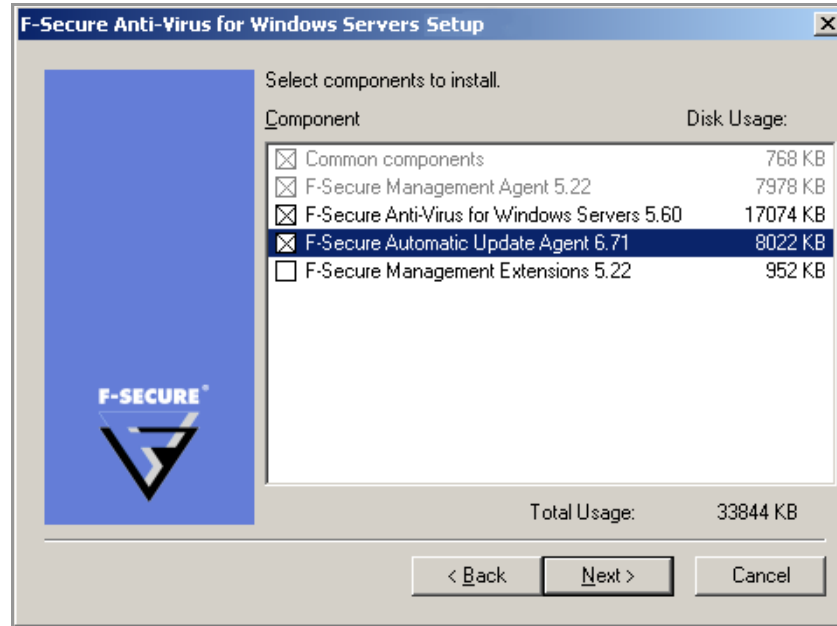
Windows 2000 Server Family:	Windows 2000 Server with the latest Service Pack; Windows 2000 Advanced Server with the latest Service Pack
Windows 2003 Server Family:	Windows Server 2003, Standard Edition with or without Service Pack 1; Windows Server 2003, Enterprise Edition with or without Service Pack 1
Clearswift MIMESweeper:	MIMESweeper™ for SMTP 5.0 MIMESweeper™ for SMTP 5.1 MIMESweeper™ for Web 5.0
Processor:	Intel Pentium processor
Memory:	256MB (Windows 2000/2003 Server)
Disk space to install:	100MB

## 2.3 Installation Steps

### To install F-Secure MIMESweeper:

1. Extract the installation archive to a temporary location in order to start the installation.
2. Read the information in the Welcome screen and click **Next** to continue.
3. Read the *Licence Agreement*. Select the **I accept the agreement** check box and click **Next** to continue.
4. Enter the keycode for F-Secure Anti-Virus for MIMESweeper. Click **Next** to continue.

- Accept the default selection. F-Secure Automatic Update Agent is not necessary if the virus definition databases are updated through F-Secure Policy Manager. Click **Next** to continue.



- Choose the destination folder where you want to create F-Secure Anti-Virus for MIMEsweeper folders and install all files. Subfolders are created automatically for any applications, such as F-Secure Anti-Virus for Windows Servers. Click **Next** to continue.
- Select the administration method you want to use. The default installation method is the stand-alone installation. In stand-alone installation the product is managed via the local user interface. Centralized administration is used for F-Secure Policy Manager-based management. Click **Next** to continue.



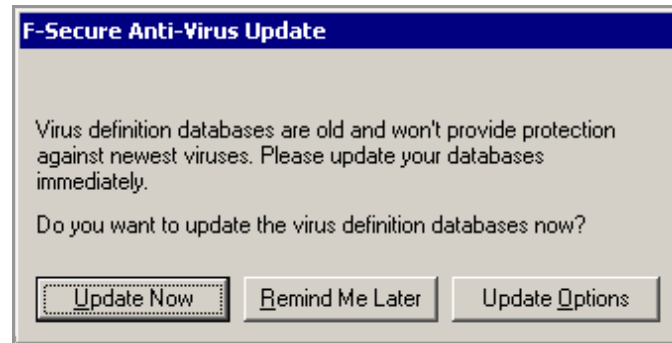
*For information on F-Secure Policy Manager, see the F-Secure Policy Manager Administrator's Guide.*

- Verify that all necessary components are listed in the F-Secure Setup screen. Click **Next** to continue.

9. After the installation is ready, read the *ReadMe-file* for any last minute notes about the product. Click **Finish** to quit the setup.
10. Click **Update Now** to update the virus definition databases.



**IMPORTANT:** Keep the virus databases up to date to ensure the best possible protection.



If the updated virus definition databases are not yet taken into use, you will see a yellow arrow on the sword-and-shield icon.



When the system recognizes the updated virus definition databases, the yellow arrow will disappear. It will reappear in the future if the databases are not updated frequently.



For more information, see <ProductNameLink>Chapter 4. [Updating Virus Definition Databases](#).



# 3

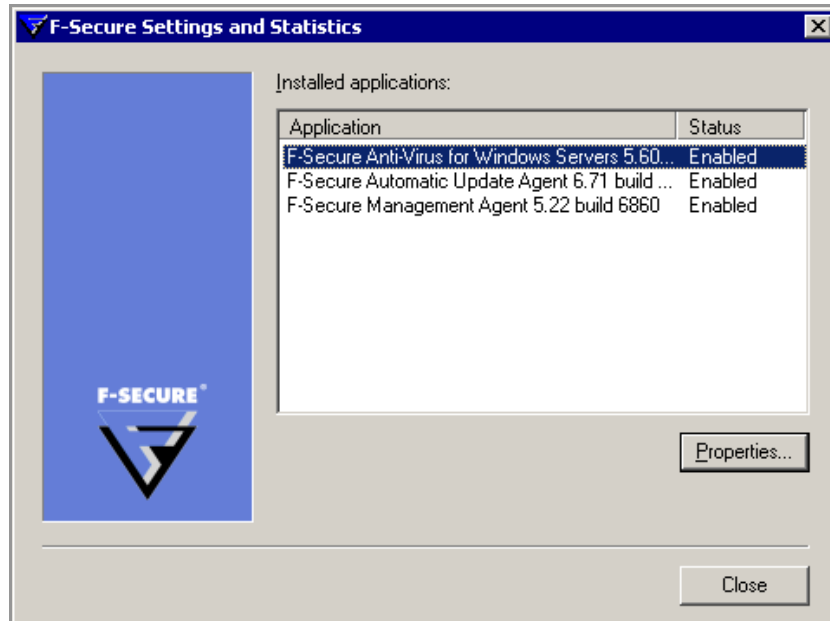
## CONFIGURATION

Configuring F-Secure Anti-Virus for MIMESweeper .....	20
Configuring Content Scanner Scenario .....	25
Configuring Alert Forwarding .....	28

## 3.1 Configuring F-Secure Anti-Virus for MIMESweeper

### To configure F-Secure Anti-Virus for MIMESweeper:

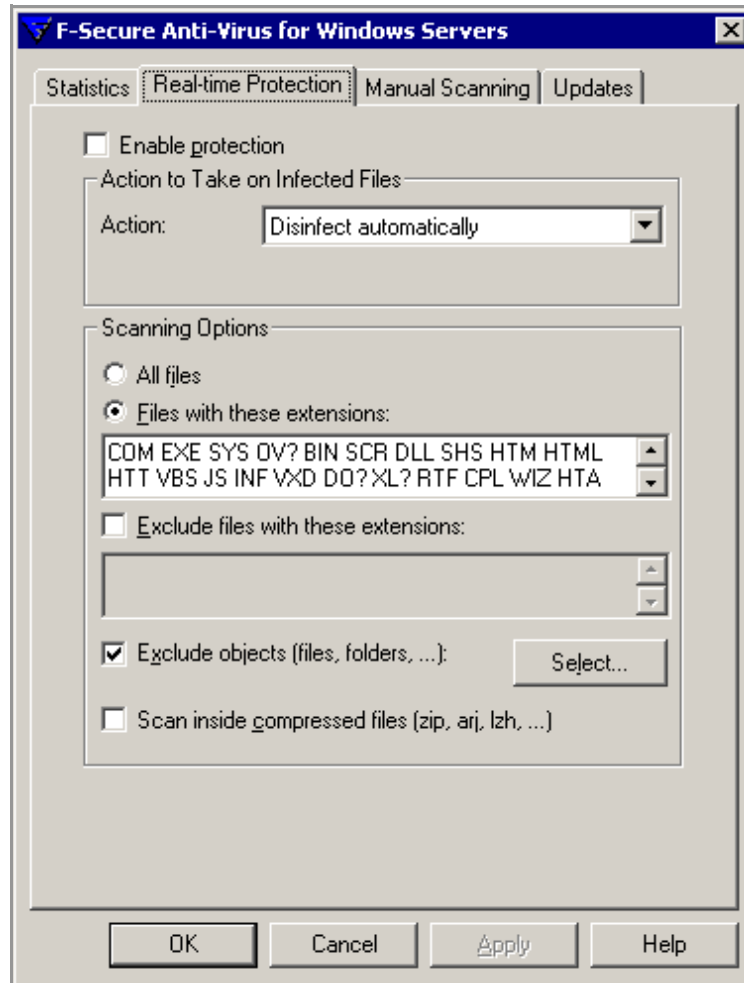
1. Double-click the blue **F-Secure** icon to open the F-Secure Settings and Statistics dialog. From here you can control all locally installed F-Secure products.



2. Select **F-Secure Anti-Virus for Windows Servers** and click **Properties** to open the product settings.

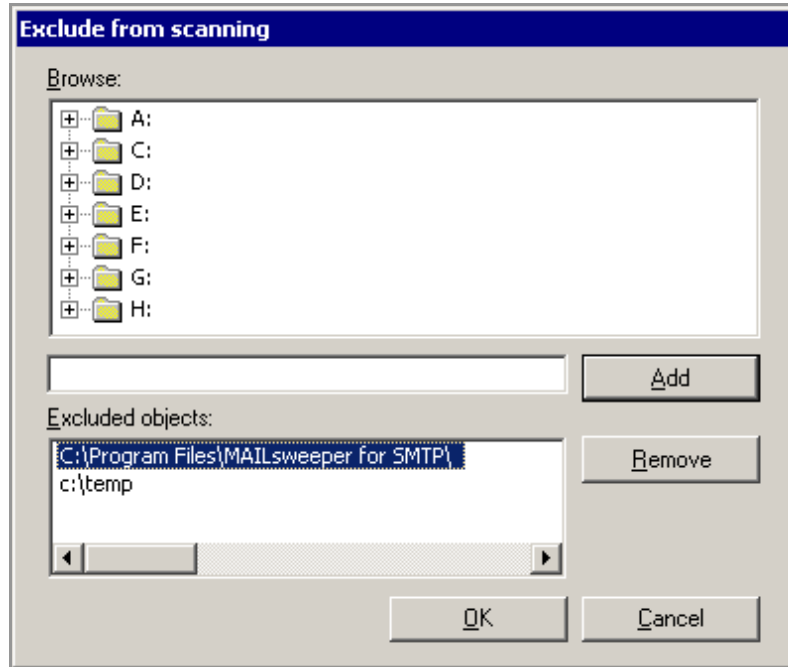
The first tab in the product settings is Statistics, where you can see the product status. The second tab, Real-time Protection, covers real-time scanning settings. F-Secure Anti-Virus for MIMESweeper does not use real-time scanning, but you can enable normal

server-level on-access file scanning from here to protect the local host. It is disabled by default for performance reasons, as the MIMESweeper servers are usually not used in file server roles.



3. Exclude the paths to MIMESweeper for SMTP and temporary directory locations to enable real-time protection in the server. This needs to be done to prevent inter-operability issues with

MIMESweeper's temporary files that are created for scanning. If these paths are not excluded, the server may fail in e-mail delivery. Click **OK** to continue.

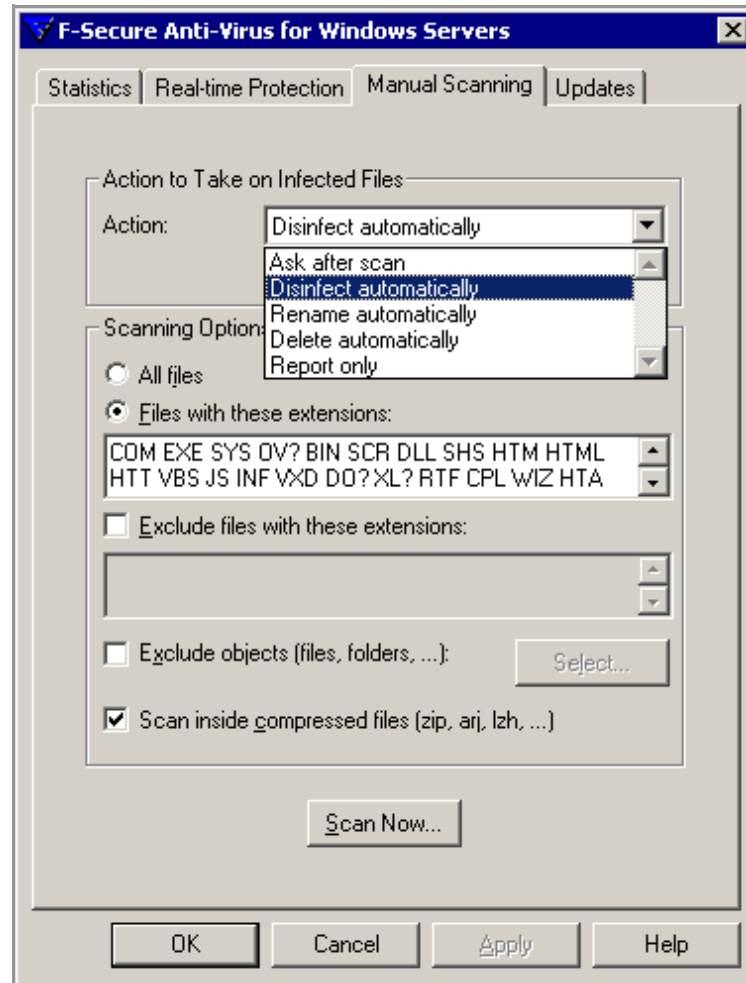


4. Configure how the e-mails are scanned in Manual Scanning. Manual Scanning is always used with F-Secure Anti-Virus for MIMESweeper. The default for 'Action to Take on Infected Files' is **Disinfect Automatically**. For 'Scanning Options' the defaults are **Files with these extensions** and **Scan inside compressed files**.



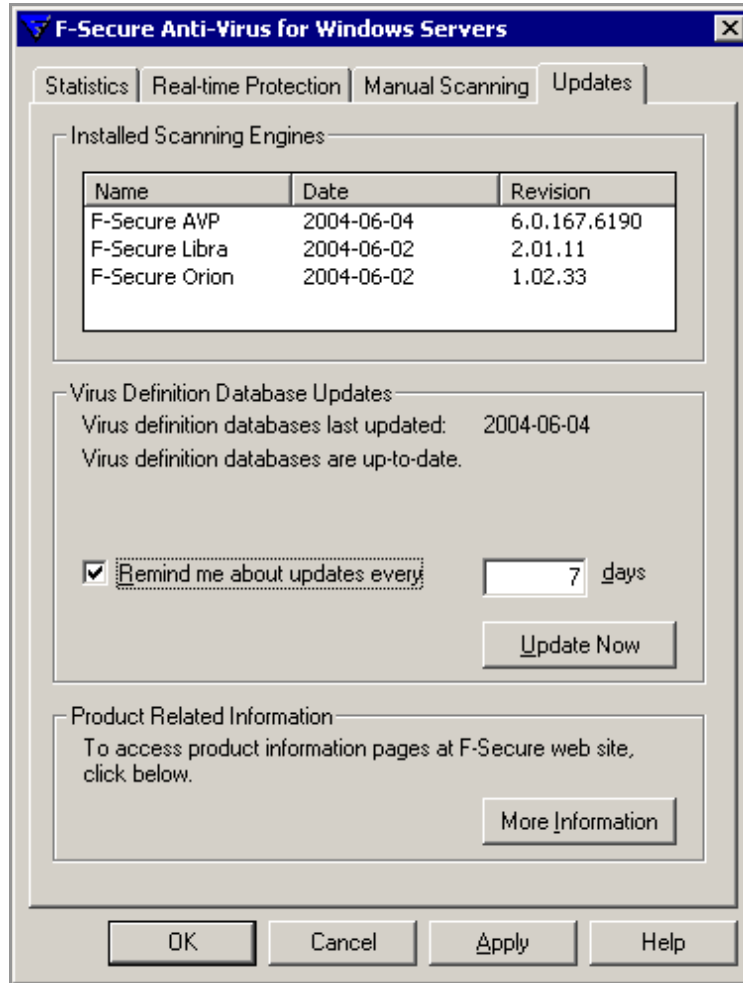
*These settings are separate from Clearswift scenario settings.*

After selecting, click **OK** to continue.



5. Define how often you want the system to remind you about the updates. Click **Update Now**→**Apply**→**OK**. If updates are not performed frequently, the product alerts the administrator after a certain time has passed since the last successful database update.

After the F-Secure Anti-Virus for MIMESweeper configuration is complete, the next task is to configure the Content Scanner Scenario for MIMESweeper for SMTP.



## 3.2 Configuring Content Scanner Scenario

### To configure Content Scanner Scenario:

1. Open the MIMESweeper for SMTP console. Make sure that the MIMESweeper installation is working and does not have any antivirus scanning scenarios.
2. Go to the Incoming Scenario and choose **New Content Scanner Scenario** in the MIMESweeper for SMTP console. This guide covers only the Incoming scenario, but the same routine can be duplicated to the Outgoing scenario as well.
3. Open the New Content Scanner Wizard and click **Next**.
4. In the New Content Scanner Wizard, select **Enabled** and **Overridable**. Overridable allows you to make sub-scenarios for different antivirus behavior. Click **Next** to continue.
5. Select **F-Secure Anti-Virus for MIMESweeper**, and click **Next**.
6. Select **Clean the detected item** to allow disinfected attachments to pass through. Annotation is optional. Click **Next** to continue.
7. Select **Strip the detected item** to allow messages to pass through when malicious code is removed from the message, and click **Next**.
  - **Cleaning.** Determines whether to attempt the disinfection of e-mails. E-mails can be annotated to state that a virus was found and successfully removed.
  - **Stripping.** If cleaning is not enabled, or fails, infected items can be removed. An e-mail can be annotated to state that infected items have been removed.

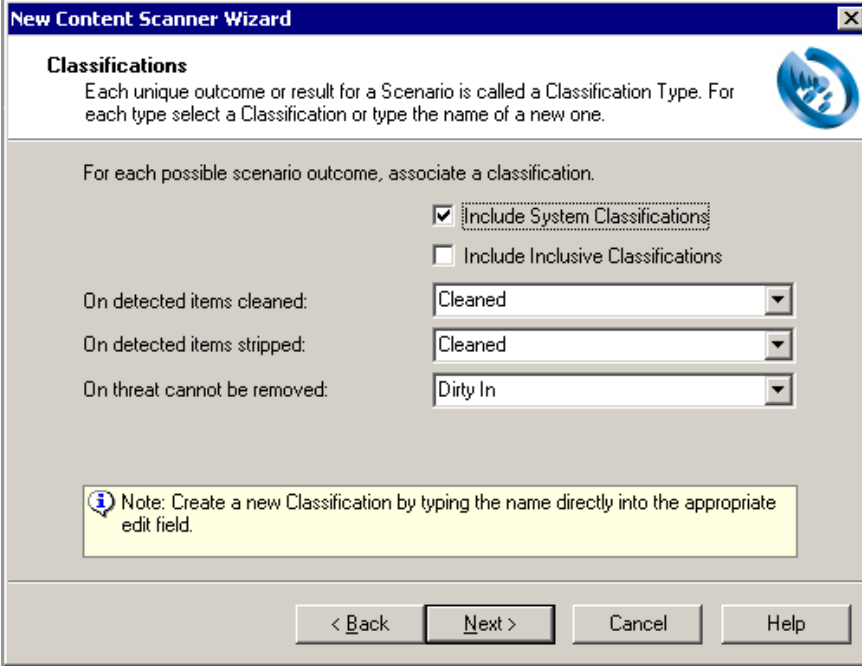
The scenario classifies e-mails depending on the F-Secure Anti-Virus scanning results.

Cleaned and Stripped e-mails are usually classified as Cleaned and they continue being processed by other scenarios.

If a virus is found, but cannot be removed, the e-mail is usually classified as Dirty, which usually results in its being quarantined. These e-mails need to be inspected manually by the administrator.

8. Select **Include System Classifications** to see all the possible classifications. **Cleaned** and **Dirty In** may not be available without this option. One way to proceed is to select **Cleaned** for the On

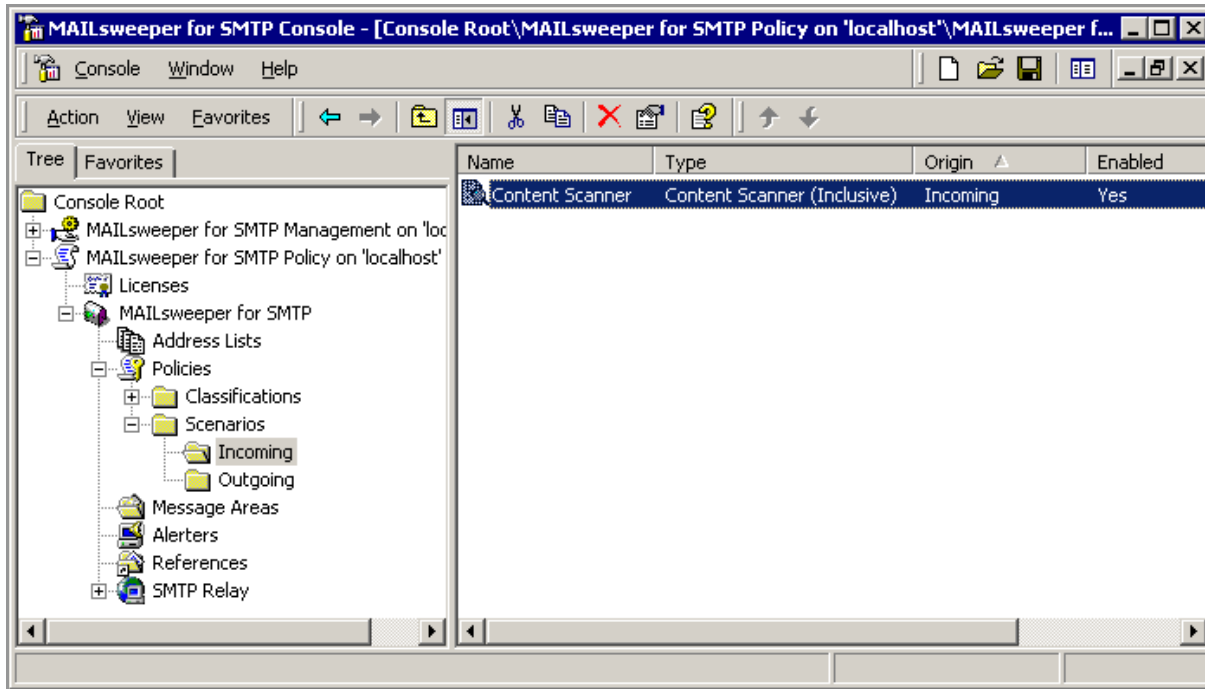
Detected Items Cleaned field and for the On Detected Items Stripped field. This classification allows the message to pass through after being disinfected. To block messages that cannot be disinfected at all, it is recommended to stop them by selecting **Dirty In** for the On Threat Cannot Be Removed field. Click **Next** to continue.



The screenshot shows a dialog box titled "New Content Scanner Wizard" with a close button in the top right corner. The main heading is "Classifications". Below the heading is a descriptive paragraph: "Each unique outcome or result for a Scenario is called a Classification Type. For each type select a Classification or type the name of a new one." To the right of this text is a circular icon with a blue and white design. Below the paragraph is the instruction: "For each possible scenario outcome, associate a classification." There are two checkboxes: "Include System Classifications" (checked) and "Include Inclusive Classifications" (unchecked). Below these are three dropdown menus: "On detected items cleaned:" (set to "Cleaned"), "On detected items stripped:" (set to "Cleaned"), and "On threat cannot be removed:" (set to "Dirty In"). At the bottom of the dialog is a yellow information box with an 'i' icon and the text: "Note: Create a new Classification by typing the name directly into the appropriate edit field." At the very bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

9. Name how the scenario shows up in the F-Secure Anti-Virus for MIMESweeper console. Content Scanner is the default name. Click **Next** to continue.
10. Check that all settings are as intended and click **Finish**.

11. Go to the MIMESweeper for SMTP Console to see the scenario you have just created.



## Testing the Scenario

To test the scenario, send an e-mail with the *ecar.com* standard antivirus test file as an attachment (see <http://www.eicar.com>). If the scenario and F-Secure Anti-Virus for MIMESweeper work correctly, you will see the results in the Recent Messages screen. In this example *ecar.com* cannot be disinfected, but it can be removed from the message and be cleaned. *Eicar.com* is not a malicious code, but for testing purposes it is detected exactly as if it was.

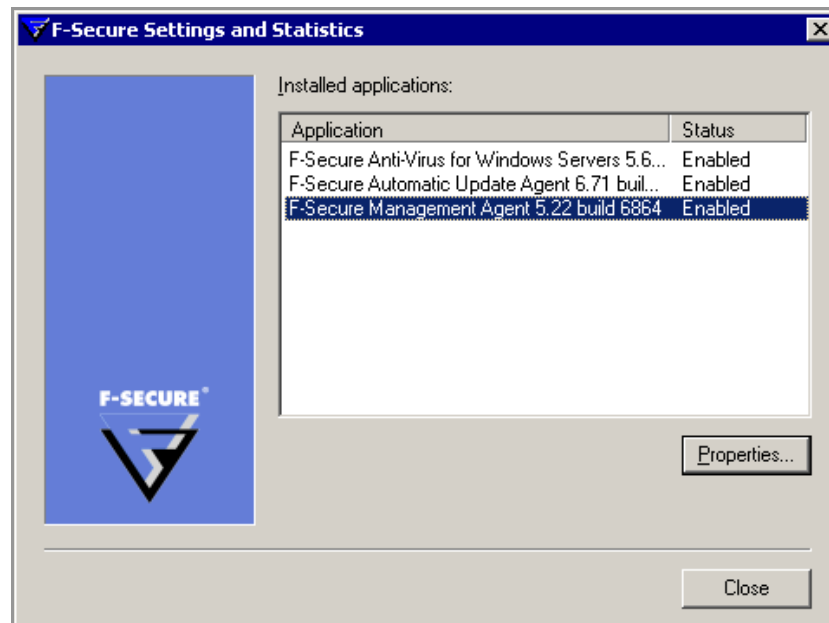
## 3.3 Configuring Alert Forwarding

Alerts are sent if the system security has been compromised, or if the program wants to notify about specific events, such as starting or stopping modules, low disk space, etc. Alerts are also sent if a program or an operation has encountered problems.

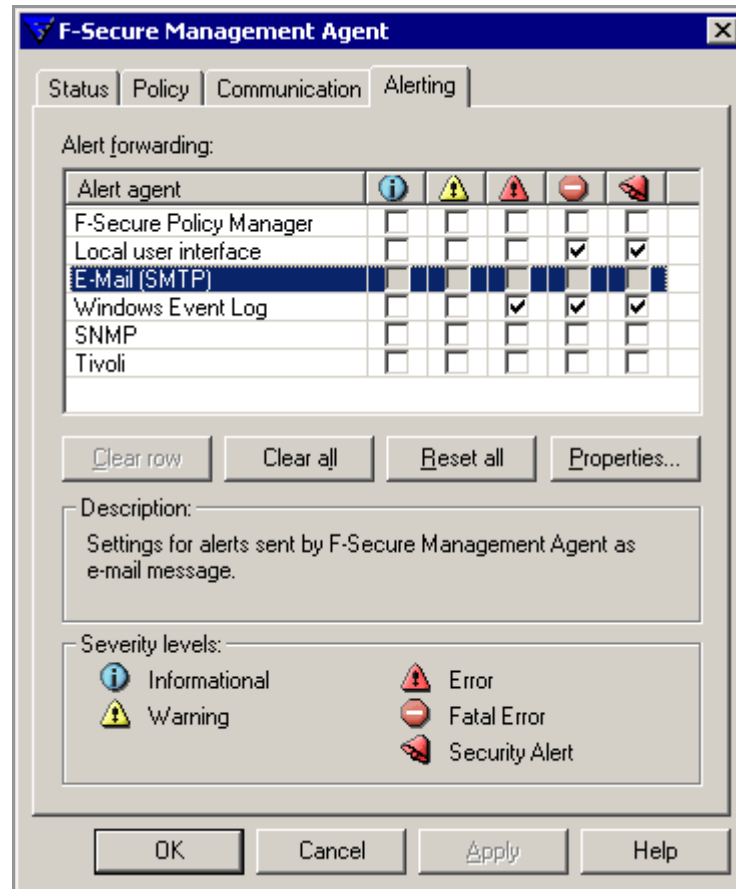
You can configure alert forwarding in stand-alone mode using the F-Secure Management Agent Local User Interface.

### To configure alert forwarding:

1. Double-click the left **F-Secure** icon and select **Options** to start the F-Secure Settings and Statistics.
2. Select **F-Secure Management Agent** from the dialog and click **Properties**.

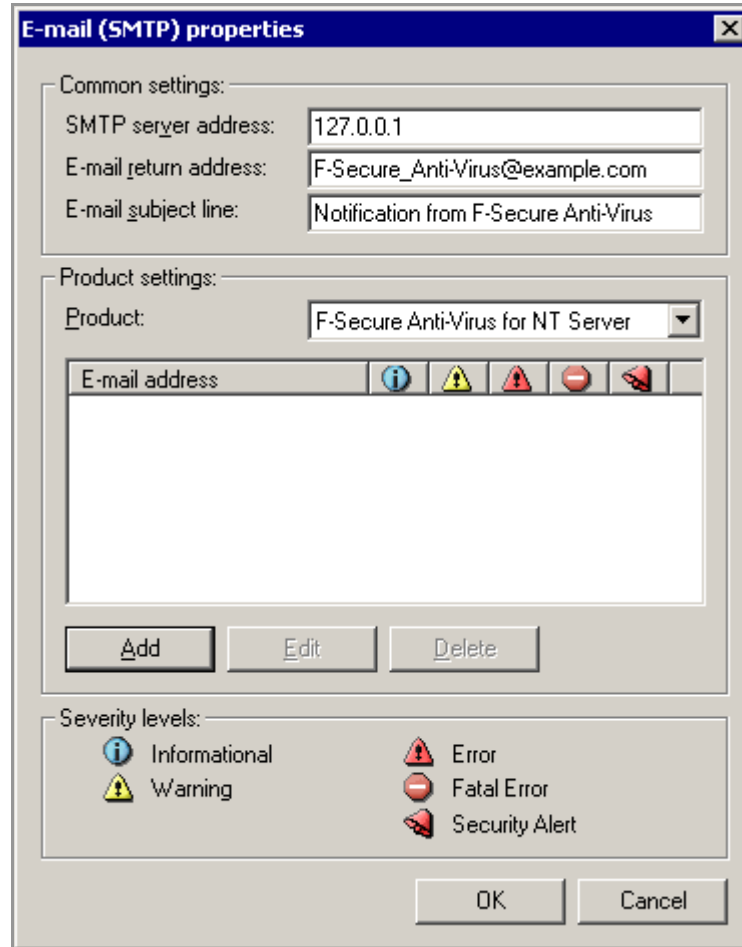


3. Select the **E-Mail (SMTP)** row. If no e-mail alerts are defined, there are no check marks on that line. The greyed boxes need to be modified in the next dialog. Click **Properties** to continue.



4. Click **Add** to make a new e-mail delivery rule in Product Settings. The Common Settings are used in all Product Settings rows. This is used to send alerts to administrators for possible actions. The E-mail return address does not need to be a valid mailbox, but should be routed to an administrator mailbox if someone replies to the e-mail, or if there


has been a problem in the delivery. The product is F-Secure Anti-Virus for Windows 2000/2003 Server. This dialog shows all F-Secure products that are installed to this system.

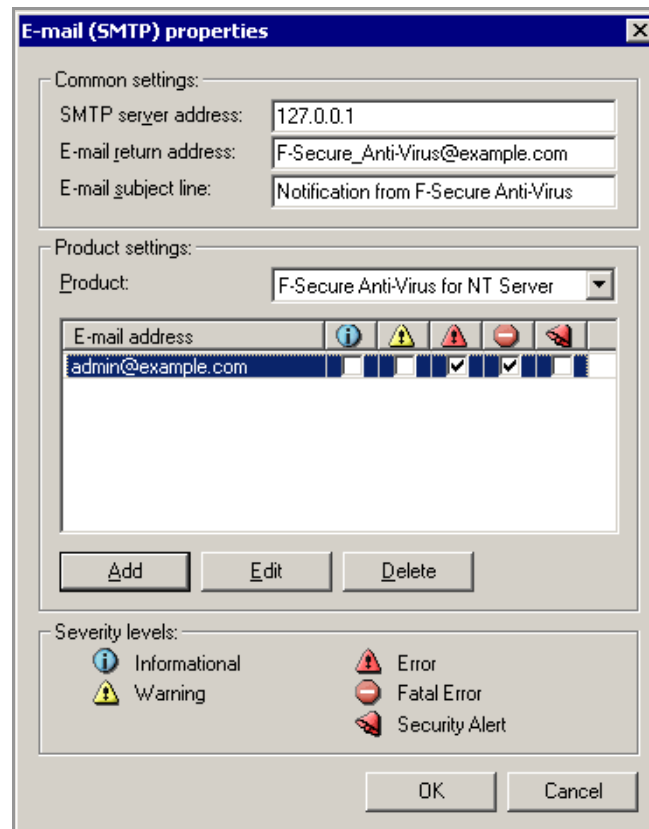


5. Choose an appropriate administrator e-mail address where the alerts are sent to. If you wish to send them to multiple administrators, choose an alias e-mail distribution list, or make multiple entries to the list. Do not enter more than one address in this dialog. Click **OK** to continue.

- Choose which alerts are sent to the e-mail address. The Severity levels define what the icons mean. Click **OK** when finished.

Now the E-Mail (SMTP) row shows the severity levels which have been configured to be logged. In this example they are sent by e-mail to an administrator.

 You can also specify an alert to be sent to Windows Event Log or as SNMP, if you have installed the Management Extensions module.





# 4

## UPDATING VIRUS DEFINITION DATABASES

Overview.....	34
Automatic Updates .....	34
Manual Updates .....	35

## 4.1 Overview

It is of the utmost importance that you keep the virus definition database up-to-date. This section describes how you can regularly update the virus definitions. Information about the latest virus database update can be found at: <http://www.F-Secure.com/download-purchase/updates.shtml>.

## 4.2 Automatic Updates

With F-Secure Automatic Update Agent, virus definition database updates are automatically retrieved when they are published. When a new virus is found, F-Secure provides a new virus definition database update and sends it to F-Secure Anti-Virus for MIMESweeper using an intelligent UDP-based polite protocol or HTTP protocol. F-Secure Automatic Update Agent transfers updates to F-Secure Anti-Virus for MIMESweeper automatically and transparently.

You can install and use F-Secure Automatic Update Agent together with licensed F-Secure antivirus and security products. F-Secure Automatic Update Agent is used only for receiving updates and related information on F-Secure antivirus and security products. F-Secure Automatic Update Agent may not be used for any other purpose or service.

### Using F-Secure Automatic Update Agent

F-Secure Automatic Update Agent user interface provides information about downloaded virus definition database updates. To access the F-Secure Automatic Update Agent user interface, open the F-Secure Anti-Virus for MIMESweeper user interface and select **F-Secure Automatic Update Agent**. In centrally managed installations, you can change these settings by using F-Secure Policy Manager Console.

## 4.3 Manual Updates

You can update your virus definition database manually. You can do it with the program called FSUPDATE, by downloading the *LATEST.ZIP* file, or by updating the database remotely.

### 4.3.1 Using FSUPDATE

The FSUPDATE is a program that automatically updates the virus definition database. The FSUPDATE can be downloaded from: <http://www.F-Secure.com/download-purchase/updates.shtml>. Run *FSUPDATE.exe* on the host. The update process takes approximately one minute.

### 4.3.2 Using LATEST.ZIP

You can update the virus definition database by downloading the *LATEST.ZIP* archive from: <http://www.F-Secure.com/download-purchase/updates.shtml>. Unzip the archive and copy the files to the communication directory.

### 4.3.3 Updating the Virus Definition Database Remotely

**Follow these instructions to update the virus definition database remotely:**

1. Run F-Secure Policy Manager Console.
2. Choose **Import Virus Signature Database** from the **Tools** menu.
3. Browse to the location where you saved the *LATEST.ZIP* file and click **Open**.
4. Click **Import**. The new virus definition database will be automatically transferred to Communication Directory.



# Technical Support

Overview.....	38
F-Secure Online Support Resources.....	38

## Overview

F-Secure Technical Support is available through F-Secure support web pages, e-mail and by phone. Support requests can be submitted through a form on F-Secure support web pages directly to F-Secure support.

## F-Secure Online Support Resources

F-Secure support web pages can be accessed at <http://support.f-secure.com/>. All support issues, frequently asked questions and hotfixes can be found on the support pages. If you have questions about F-Secure Anti-Virus for MIMESweeper that are not covered in this manual or on the F-Secure support web pages, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For technical assistance, contact your local F-Secure Business Partner. Send your e-mail to: [Anti-Virus-<country>@f-secure.com](mailto:Anti-Virus-<country>@f-secure.com). Example: [Anti-Virus-Norway@f-secure.com](mailto:Anti-Virus-Norway@f-secure.com)

If there is no authorized F-Secure Anti-Virus Business Partner in your country, you can submit a support request directly to F-Secure. There is an online "Web submit form" accessible through the F-Secure support web pages on the "Contact Support" page. Fill in all the fields and describe the problem as accurately as possible. Include the FSDiag report taken from the problematic server with the support request.

FSDiag report can be gathered by running the F-Secure Diagnostic Tool (*FSDiag.exe*) on the server that is running F-Secure Anti-Virus for MIMESweeper. This tool gathers basic information about hardware, operating system, network configuration and installed F-Secure and third-party software.

You can run the *FSDiag.exe* utility under the *F-Secure\Common* folder. The tool generates a file called *FSDiag.tar.gz*.

Include the following information with your support request:

- Version numbers of F-Secure Management Agent, F-Secure Anti-Virus for MIMESweeper, and possibly the version numbers of F-Secure Policy Manager Server and F-Secure Policy Manager

Console if you use the centralized administration method. Include the build number if available. Also include the version number of the Clearswift MIMESweeper for SMTP or MIMESweeper for Web.

- Description how F-Secure components are configured.
- The name and the version number of the operating system on which F-Secure products and protected systems are running. Include also the build number and Service Pack number.
- The version number and the configuration of your mail servers. If possible, describe your network configuration and topology.
- A detailed description of the problem, including any error messages displayed by the program, and any other details that could help us replicate the problem.
- Logfile.log from the machines running F-Secure products. This file can be found under *Program Files\F-Secure\Common*. If you are sending the FSDiag report you do not need to send the *Logfile.log* separately, because it is already included in the FSDiag report

## Web Club

The F-Secure Web Club provides assistance and updated versions of F-Secure products. To connect to the Web Club, go to: <http://www.F-Secure.com/anti-virus/webclub/corporate/>.

## Virus Descriptions on the Web

F-Secure Corporation maintains a comprehensive collection of virus-related information on its Web site. To view the Virus Information Database, connect to: <http://www.F-Secure.com/virus-info/>.



# About F-Secure Corporation

F-Secure Corporation is the fastest growing publicly listed company in the antivirus and intrusion prevention industry with more than 50% revenue growth in 2004. Founded in 1988, F-Secure has been listed on the Helsinki Stock Exchange since 1999. We have our headquarters in Helsinki, Finland, and offices in USA, France, Germany, Italy, Sweden, the United Kingdom and Japan. F-Secure is supported by service partners, value added resellers and distributors in over 50 countries. F-Secure protection is also available through mobile handset manufacturers such as Nokia and as a service through major Internet Service Providers, such as Deutsche Telekom, France Telecom and Charter Communications. The latest real-time virus threat scenario news are available at the F-Secure Antivirus Research Team weblog at <http://www.f-secure.com/weblog/>.

## Services for Individuals and Businesses

F-Secure services and software protect individuals and businesses against computer viruses and other threats coming through the Internet or mobile networks. Our award-winning solutions include antivirus and desktop firewall with intrusion prevention, antispam and antispymware solutions. Our key strength is our proven speed of response to new threats. For businesses our solutions feature a centrally-managed and well-integrated suite of solutions for workstations and servers alike. Focused partners offer security as a service for companies that do not wish to build in-house security expertise.

Visit our website at <http://www.f-secure.com/products/> to learn more about our products and services.





**F-SECURE®**



[www.f-secure.com](http://www.f-secure.com)