F-Secure E-mail and Server Security

Administrator's Guide

Contents

Disclaimer

"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 includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes PHP, freely available from http://www.php.net/.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes optional Microsoft SQL Server 2008 R2 SP1 Express Edition.

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

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

About This Guide

Topics:

1.1 Introduction

This guide describes how to administer F-Secure E-mail and Server Security. The solution can be licensed and deployed as F-Secure Server Security, on per-server basis, or F-Secure E-mail and Server Security, on per-user or terminal connection basis. This means that F-Secure Server Security administrators can use this guide as well.

Depending on the selected license and installed components, some product features may not be available.

Note: For more information on the licensing and the product deployment, consult F-Secure E-mail and Server Security Deployment Guide.

1.1.1 Product contents

The product can be licensed and deployed as F-Secure Server Security (Standard) or F-Secure Server Security Premium, on per-server basis, or F-Secure E-mail and Server Security (Standard) or F-Secure E-mail and Server Security Premium, on per-user or terminal connection basis.

Features with different product licenses:

Feature	F-Secure Server Security (Standard)	F-Secure Server Security Premium	F-Secure E-mail and Server Security (Standard)	F-Secure E-mail and Server Security Premium
Virus & spyware protection	X	X	X	X
DeepGuard	X	X	X	X
Web traffic scanning	X	X	X	X
Browsing protection	X	X	X	X
Anti-Virus for Microsoft Exchange			X	X
Spam Control			X	X
Offload Scanning Agent	X	X	X	X
Software Updater		X		X
Anti-Virus for Microsoft SharePoint				X
EMC CAVA support				X

1.2 How This Guide Is Organized

F-Secure E-mail and Server Security Administrator's Guide is divided into the following chapters:

Getting Started. Instructions how to use and administer the product.

Protecting the Server against Malware . Describes malware and how to protect the server against it.

Centrally Managed Administration . Instructions how to remotely administer the product when is installed in centrally managed administration mode.

Administration with Web Console . Instructions how to administer the product with the Web Console.

E-mail Quarantine Management . Instructions how you can manage and search quarantined mails.

Updating Virus and Spam Definition Databases . Instructions how to update your virus definition database.

Variables in Warning Messages . Describes variables that can be included in virus warning messages.

Sending E-mail Alerts And Reports . Instructions how to configure the product to send alerts to the administrator by e-mail.

Troubleshooting . Solutions to some common problems.

Technical Support . Contains the contact information for assistance.

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

Getting Started

Topics:

2.1 Administering the Product

The product can be used either in the stand-alone mode or in the centrally managed administration mode, based on your selections during the installation and the initial setup.

Centrally Managed Administration Mode

In the centrally managed administration mode, you can administer the product with F-Secure Policy Manager.

You still can use the Web Console to monitor the product status, start and stop the product, manage the quarantined content, and to configure settings that are not marked as **Final** in the F-Secure Policy Manager Console (settings marked as **Final** are greyed out in Web Console).

See the F-Secure Policy Manager Administrator's Guide for detailed information about installing and using the F-Secure Policy Manager components:

- F-Secure Policy Manager Console, the tool for remote administration of the product.
- F-Secure Policy Manager Server, which enables communication between F-Secure Policy Manager Console and the managed systems.

Stand-alone Mode

You can use the Web Console to administer the product; monitor the status, modify settings, manage the quarantine and to start and stop the product if necessary.

2.2 Using Web Console

You can open the Web Console in any of the following ways:

- Go to **Windows Start menu > Programs > F-Secure E-mail and Server Security > F-Secure E-mail and Server Security Web Console**
- Enter the IP address and the port number of the host where the Web Console is installed in your web browser. Note that the protocol used is https. For example: https://127.0.0.1:25023

When the Web Console login page opens, enter your user name and the password and click **Log In**. Note that you must have administrator rights to the host where the Web Console is installed.

2.2.1 Logging in for the First Time

Before you log in to the Web Console for the first time, check that javascript and cookies are enabled in the browser you use.

Note: Microsoft Internet Explorer users: The address of the Web Console, for example *https://127.0.0.1:25023/*, should be added to the `Trusted sites` in `Internet Explorer Security Options` to ensure that it works properly in every environment.

When you log in for the first time, your browser displays a Security Alert dialog window about the security certificate for the Web Console. You can create a security certificate for the Web Console before logging in, and then install the certificate during the login process.

Note: If your company has an established process for creating and storing certificates, follow that process to create and store the security certificate for the Web Console.

Create the security certificate

1. Browse to the Web Console installation directory, for example: `C:\Program Files (x86)\F-Secure\Web User Interface\bin\`
2. Locate the certificate creation utility, `makecert.bat`, and double click it to run the utility.
3. The utility creates a certificate that will be issued to all local IP addresses, and restarts the Web Console service to take the certificate into use.
4. Wait until the utility completes, and the window closes. Now you can proceed to logging in.

Log in and install the security certificate

1. Open the Web Console.
2. The Security Alert about the Web Console certificate is displayed. If you install the certificate now, you will not see the Security Alert window again.

   If you are using Internet Explorer 7, click **Continue** and then **Certificate Error**.
3. Click **View Certificate** to view the certificate information.
4. The Certificate window opens. Click **Install Certificate** to install the certificate with the Certificate Import Wizard.
5. The Certificate window opens. Click **Install Certificate** to proceed to the Certificate Import Wizard.
6. Follow the instructions in the Certificate Import Wizard.

   If you are using Internet Explorer 7, in the **Place all certificates in the following store** selection, select the **Trusted Root Certification Authorities** store.
7. If the Security Alert window is still displayed, click **Yes** to proceed or log back in to the Web Console.
8. When the login page opens, log in to the Web Console with your user name and the password.
9. The Web Console displays **Getting Started** page when you log in for the first time. You can check and configure the following information in the **Getting Started** page to complete the installation:
   - Internal domains and senders
   - E-mail alerts and reports
   - Database updates
   - Product updates

2.2.2 Modifying Settings and Viewing Statistics with Web Console

To change the product settings, open the Web Console and use the left pane to navigate the settings you want to change or statistics you want to view. For detailed explanations of all product settings, see *Administration with Web Console*.

2.2.3 Setting up Web Console for Remote Use

To access the Web Console remotely:

1. Log in to the Web Console locally on the server (**https://127.0.0.1:25023**).
2. Go to **General > Administration** and open the Web Console tab.
3. In **Allowed hosts** section, click **Add new hosts** and enter the IP address of the remote host where you want to access the server.
4. In the **Session** section, specify the length of time that a client can be connected to the server. The Web Console terminates the session and displays a warning when the session expires. The default value is 60 minutes.
5. On the remote host, open **https://<IP address of the server>:25023** to open the Web Console.

2.2.4 Setting up Web Console for Remote Use on Windows Server Core Editions

To remote access the Web Console that is installed on Microsoft Windows Server Core edition:

1. Log in to Windows Server Core with the local administrator’s account.
2. Go to the Web Console installation folder. By default, it is located in:`%ProgramFiles%\F-Secure\Web User Interface\bin`
3. Open the Web Console configuration file (`webui.cnf`) in Notepad.
4. Add the following entry to the **Connections** section: `Allowed2 = <ip_address>`

   The `ip_address` is the address of the host that you want to allow to connect to the Web Console. If you want to allow connections from any host, replace the ip address with an asterisk (*).
5. After you have changed the `webui.cnf` file, enter the following commands in the command line to restart the F-Secure Web Console daemon service:

```
net stop "F-Secure WebUI daemon"

net start "F-Secure WebUI daemon"
```

6. On the remote host, open **https://<IP address of the server>:25023** to open the Web Console.

2.3 Using F-Secure Policy Manager Console

In the centrally managed administration mode, you can administer the product with F-Secure Policy Manager Console. You can use F-Secure Policy Manager Console to create policies for product installations that are running on selected hosts or groups of hosts.

👉 **Note:** For detailed information on installing and using F-Secure Policy Manager Console, consult F-Secure Policy Manager Administrator's Guide.

2.3.1 Settings and Statistics in Centrally Managed Administration Mode

By default F-Secure Policy Manager Console is in the Anti-Virus mode where you can manage only the base component settings. To configure components that are not available in the Anti-virus mode, change F-Secure Policy Manager Console to the Advanced mode user interface.

To change the product settings in the centrally managed administration mode, follow these instructions:

1. Select the product component that you want to configure from the **Properties** pane.
2. Make sure the**Policy** tab is selected and assign values to variables under the **Settings** branch.
3. Modify settings by assigning new values to the basic leaf node variables (marked by the leaf icons) shown in the **Policy** tab of the **Properties** pane.

   Initially, every variable has a default value, which is displayed in gray. Select the variable from the **Properties** pane and enter the new value in the **Editor** pane to change it. You can either type the new value or select it from a list box.

   Click **Clear** to revert to the default value or **Undo** to cancel the most recent change that has not been distributed.

   👉 **Note:** Settings that are configured during the installation and the initial setup require that you select the Final check box from the Product View pane. For more information, see *Changing Settings That Have Been Modified During the Installation or Upgrade*.

4. After you have modified settings and created a new policy, it must be distributed to hosts. Choose **Distribute** from the **File** menu.
5. After distributing the policy, you have to wait for the product to poll the new policy file. Alternatively, click **Poll the server now** in the **Server Properties** page in the Web Console.

   For testing purposes, you may also want to change the polling intervals for incoming and outgoing packages. For more information see *F-Secure Management Agent Settings*.

To view statistics, select the **Status** tab of the**Properties** pane. Statistics are updated periodically and can be reset by choosing **Reset Statistics** on the**Policy** tab of the **Properties** pane.

To manage the quarantined content, use the Web Console. For more information, see *E-mail Quarantine Management*.

2.3.1.1 Changing Settings That Have Been Modified During the Installation or Upgrade

If you want to change a setting that has been modified locally during installation or upgrade, you need to mark the setting as **Final** in the restriction editor. The settings descriptions in this manual indicate the settings for which you need to use the **Final** restriction. You can also check in F-Secure Policy Manager Console whether you need to use the Final restriction for a setting.

Follow these instructions:

1. Select the **Policy** tab and then select the setting you want to check.
2. Select the **Status** tab to see if the setting has been modified locally.

- If the setting is grayed out in the **Status** view, then the product uses the setting from the base policy and therefore the **Final** restriction is not needed.
- If the setting is not grayed out, it has been modified locally. You must mark the setting as **Final** when you change it.

Protecting the Server against Malware

Topics:

3.1 Overview

By default, all malware types are immediately handled when they are found, so that they can cause no harm.

Virus and spyware scanning scans your local hard drives, any removable media (such as portable drives or compact disks) and downloaded content automatically by default.

3.1.1 What are Viruses and Other Malware

Malware are programs specifically designed to damage your computer, use your computer for illegal purposes without your knowledge, or steal information from your computer.

Malware can:

- take control over your web browser,
- redirect your search attempts,
- show unwanted advertising,
- keep track on the web sites you visit,
- steal personal information such as your banking information,
- use your computer to send spam, and
- use your computer to attack other computers.

Malware can also cause your computer to become slow and unstable. You may suspect that you have some malware on your computer if it suddenly becomes very slow and crashes often.

3.1.1.1 Viruses

Viruses are usually programs that can attach themselves to files and replicate themselves repeatedly; they can alter and replace the contents of other files in a way that may damage your computer.

A virus is a program that is normally installed without your knowledge on your computer. Once there, the virus tries to replicate itself. The virus:

- uses some of your computer's system resources,
- may alter or damage files on your computer,
- probably tries to use your computer to infect other computers,
- may allow your computer to be used for illegal purposes.

3.1.1.2 Spyware

Spyware are programs that collect your personal information.

Spyware may collect personal information including:

- Internet sites you have browsed,
- e-mail addresses from your computer,
- passwords, or
- credit card numbers.

Spyware almost always installs itself without your explicit permission. Spyware may get installed together with a useful program or by tricking you into clicking an option in a misleading pop-up window.

3.1.1.3 Rootkits

Rootkits are programs that make other malware difficult to find.

Rootkits hide files and processes. In general, they do this to hide malicious activity on your computer. When a rootkit is hiding malware, you cannot easily discover that your computer has malware.

This product has a rootkit scanner that scans specifically for rootkits, so malware cannot easily hide itself.

3.1.1.4 Riskware

Riskware is not designed specifically to harm your computer, but it may harm your computer if it is misused. Riskware is not strictly speaking malware. Riskware programs perform some useful but potentially dangerous functions.

Examples of riskware programs are:

- programs for instant messaging, such as IRC (Internet Relay Chat),
- programs for transferring files over the Internet from one computer to another,
- Internet phone programs, such as VoIP (Voice over Internet Protocol),
- Remote Access Software, such as VNC,
- scareware, which may try to scare or scam individuals into buying fake security software, or
- software designed to bypass CD checks or copy protections.

If you have explicitly installed the program and correctly set it up, it is less likely to be harmful.

If the riskware is installed without your knowledge, it is most likely installed with malicious intent and should be removed.

3.2 How to Scan the Server

You can scan the server for malware in real time, manually, or you can schedule a scan at set times.

Deciding which method to use depends on how powerful the server is and how high a level of protection you want. Turning on all the virus and spyware scanning features can have a noticeable effort on the server's speed if it is an older server.

Note: The following recommendations will help you to protect the server from malware in files and do not affect malware in e-mail transmissions throw Microsoft Exchange Server installed on the same computer. For detailed information about protecting your e-mail traffic and mail server see *Transport Protection* and *Storage Protection*.

3.2.1 Scan for Malware

Real-time scanning protects the server by scanning all files when they are accessed locally or remotely (over network) and by blocking access to those files that contain malware.

Real-time scanning works as follows:

1. A file is accessed locally or remotely over network.
2. The file is immediately scanned for malware before access to the file is allowed.
3. If malware is found in the file, real-time scanning removes the malware automatically before it can cause any harm.

3.2.1.1 Does real-time scanning affect the performance of my computer

Normally, you do not notice the scanning process because it takes a small amount of time and system resources. The amount of time and system resources that real-time scanning takes depends on, for example, the contents, location and type of the file.

Files that take a longer time to scan:

- Compressed files, such as .zip files.
- Files on removable drives such as CDs, DVDs, and portable USB drives.

3.2.1.2 Turn Real-Time Scanning On or Off

With the product Web Console, you can turn real-time scanning on to stop malware before it can harm your computer.

To turn real-time scanning on:

1. Go to **Server Protection > Real-time Scanning**.
2. Select **Turn on real-time scanning**.

3. Click **Apply**.

3.2.2 Include Files in Real-Time Virus Scanning

You can add file types to be included in Real-time Scanning.

No file that is excluded from scanning by either type or location is scanned even if the file is included in the list of scanned file types.

To include files:

1. Go to **Server Protection > Real-time Scanning**.
2. Under **Scan these files**, click **Configure** and select one of the following:
   - **Scan all files** to scan all files.
   - **Scan defined files** to scan only the file types that you define.
3. Define file types to scan.
   - To include a file type to be scanned, enter the three-letter file extension in the field and click **Add**.
   - To prevent a file type from being scanned, click a file type in the list. Then click **Remove**.

   File types that are defined by F-Secure in database updates are grayed out and cannot be removed.

   For example, to include executable files in the scan, type exe in the field next and click **Add**.
4. Click **OK**. **Edit Scanned File Types** dialog closes.
5. Click **Apply**.

3.2.3 Exclude Files by Location from Real-Time Virus Scanning

You can define a list of excluded folders or drives that you do not want to be scanned for viruses in real time.

Files in folders or drives that are excluded from scanning are not scanned even though they might be of a type that is included in scanned file types.

To define a list of files, folders, or drives excluded by location:

1. Go to **Server Protection > Real-time Scanning**.
2. In **Exclude from scanning**, click **Configure**.
3. Add a file, drive, or folder to exclude:
   a. Select the **Objects** tab.
   b. Select **Exclude objects**.
   c. Click **Add**.
   d. Select the file, drive, or folder that you want to exclude from virus scanning.
   e. Click **OK**.
4. Repeat the previous step to exclude other files, drives, or folders from being scanned for viruses.
5. Click **OK** to close the **Exclude from Scanning** dialog.
6. Click **Apply**.

3.2.4 Exclude Files by File Type from Real-Time Virus Scanning

You can define a list of excluded file types that you do not want to be scanned for viruses in real time.

File types on this list override the list of scanned file types. For example, if you add a file type to the list of files excluded by file type, files of that type are not scanned even if they are on the list of scanned file types.

To define a list of files excluded by file type:

1. Go to **Server Protection > Real-time Scanning**.
2. In **Exclude from scanning**, click **Configure**.
3. Exclude a file type:

a. Select the **Files** tab.
b. Select **Exclude files with these extensions**.
c. Type a file extension that identifies the type of files that you want to exclude.

   To specify files that have no extension, type '.'. You can use the wildcard '?' to represent any single character, or '*' to represent any number of characters.

   For example, to exclude executable files, type ‘`exe` ’ in the field.
d. Click **Add**.

4. Repeat the previous step for any other extension you want to be excluded from being scanned for viruses.
5. Click **OK** to close the **Exclude from scanning** dialog.
6. Click **Apply**.

The selected file types are excluded from future real-time scans.

3.2.5 Exclude Processes from Real-Time Virus Scanning

When you exclude a process from the real-time virus scan, any files it accesses are not scanned for viruses. Excluding processes can speed up the system and ensures compatibility with backup utilities and other third-party software.

To define a list of processes excluded from the real-time scanning:

1. Go to **Server Protection > Real-time Scanning**.
2. In **Exclude from scanning**, click **Configure**.
3. Add a file, drive, or folder to exclude:

   a. Select the **Processes** tab.
   b. Select **Exclude these processes**.
   c. Click **Add**.
   d. Select or directly specify the full pathname of the process executable. You cannot use wildcards in the file or path names, but you can use system environment variables, for example:

      `%ProgramFiles%\Application\app.exe`

      On x64 platforms, `%ProgramFiles%` defaults to the Program Files (x86) directory. Include `%ProgramW6432%` to add the Program Files directory to the path as an environment variable.
   e. Click **OK**.

4. Repeat the previous step to exclude other processes from being scanned for viruses.
5. Click **OK** to close the **Exclude from Scanning** dialog.
6. Click **Apply**.

Excluding a process from the scan does not exclude its child processes, so files that are accessed by them are still scanned for viruses in real time.

3.3 Scan manually

You can scan your computer manually, if you suspect that you have malware on your computer.

3.3.1 How to Select the Type of Manual Scan

You can scan your whole computer or scan for a specific type of malware or a specific location.

If you are suspicious of a certain type of malware, you can scan only for this type. If you are suspicious of a certain location on your computer, you can scan only that section. These scans will finish a lot quicker than a scan of your whole computer.

To start manually scanning your computer:

1. Go to **Server Protection > Manual Scanning**.
2. Under **New scan**, select the type of scan.

If you want to change the scanning settings, click the **Settings** tab.

3. If you selected **Choose what to scan**, click **Select**.

   A window opens in which you can select which location to scan.

4. To start scanning, click **Start**.

If no malware is detected, you will see **Finished** on the **Status** line at the upper part of the page. If malware is detected, the Scan Wizard opens.

You can also start scanning the server manually by right-clicking the product icon in the system tray.

3.3.1.1 Types of scan

You can scan your whole computer or scan for a specific type of malware or a specific location.

The following lists the different types of scan:

Scan type	What is scanned	When to use this type
Full computer scan	Your entire computer (internal and external hard drives) for viruses, spyware and riskware.	When you want to be completely sure that there is no malware or riskware on your computer. This type of scan takes the longest time to complete. It combines the quick malware scan and the hard drive scan. It also checks for items that are possible hidden by a rootkit.
Choose what to scan	A specific file, folder or drive for viruses, spyware and riskware.	When you suspect that a specific location on your computer may have malware, for example, the location contains downloads from potentially dangerous sources, such as peer-to-peer file sharing networks. Time the scan will take depends of the size of the target that you scan. The scan completes quickly if, for example, you scan a folder that contains only a few small files.
Scan hard drives	All the internal hard drives on your computer for viruses, spyware and riskware.	This type of scan goes through all the hard disks of the computer. Unlike the quick Virus and spyware scan, this scan type does not specifically go through the parts of your system that contain installed program files, but scans also all data files, such as documents, music, images, and videos. This type of scan is slow and recommended only if the Virus and spyware scan has not found any malware and if you want to be sure that the other parts of your computer do not contain malicious files.

Scan type	What is scanned	When to use this type
Virus and spyware scan	Parts of your computer for viruses, spyware and riskware.	This type of scan is much quicker than a full scan. It searches only the parts of your system that contain installed program files. This scan type is recommended if you want to quickly check whether your computer is clean, because it is able to efficiently find and remove any active malware on your computer.
Rootkit scan	Important system locations where a suspicious item may mean a security problem. Scans for hidden files, folders, drives or processes.	When you suspect that a rootkit may be installed on your computer. For example, if malware was recently detected in your computer and you want to make sure that it did not install a rootkit.

3.3.2 Clean Malware Automatically

If malware is found during the scan, you can either let the program automatically decide how to clean your computer or you can decide yourself for each item.

1. Select either of:

Option	What will happen
Handle automatically (recommended)	The program decides what to do to each malware item to automatically clean your computer.
I want to decide item by item	The program asks what you want to do to each malware item.

2. Click **Next**.
   - If you selected **Handle automatically**, a window with the results of automatic malware handling opens.

     Some malware items may have a "Not processed" status, which means that the infected file is inside an archive (for example, a zip file) and cannot be handled automatically. You can delete the infected file by opening the archive and deleting the file manually. If the content of the archive is not important, you can delete the whole archive.
   - If you selected **I want to decide item by item**, you must specify action for each detected malware.
3. Click **Finish** to close the Scan Wizard.

3.3.3 View the Results of Manual Scan

You can view a report of the scanning results after the scan is complete.

You might want to view this report because the action you selected may not always be the action that was performed. For example, if you chose to clean an infected file, but the virus could not be removed from the file, the product may have performed some other action to the file.

To view the report:

1. Go to **Server Protection > Manual Scanning** and open the **Status** tab.
2. Under **Tasks**, click **View scanning report**.

In the centrally managed administration mode, the scan report is sent to F-Secure Policy Manager. You can check it also in the F-Secure Policy Manager Console.

3.4 Scan at Set Times

You can scan your computer for malware at regular intervals, for example daily, weekly or monthly.

Scanning for malware is an intensive process. It requires the full power of your computer and takes some time to complete. For this reason, you might want to set the program to scan your computer when you are not using it.

3.4.1 Schedule a Scan

Set the program to scan your computer at regular times.

To schedule a scan:

1. Go to **Server Protection > Scheduled Scanning**.
2. Select **Turn on scheduled scanning**.
3. Select which days you would like to regularly scan for viruses and spyware:

Option	Description
Start time	Sets the time when the scan will start. You should select a time when you expect to not be using the computer.
After computer is not used for	Select a period of idle time after which the scanning starts if the computer is not used.

4. Select when you want to start the scan on the selected days.

Option	Description
Daily	To scan every day.
Weekly	To scan on selected days during the week. Select on which days to scan from the list to the right.
Monthly	To scan on up to three days a month. To select on which days: Select one of the Day options. 1. Select the day of the month from the list next to the selected day. 2. Repeat if you want to scan on another day.

5. Click **Apply**.

3.4.2 View the Results of Scheduled Scan

When a scheduled scan finishes you can check if malware were found.

To check the results of a scheduled scan:

1. Click the **Scheduled scan has finished** on the **Virus and spyware scanning** flyer.
2. Click **Show Report** to see what happened during the scan.

You can view the results of the last scan also by clicking **Server Protection > Scheduled Scanning > View scanning report** in the product Web console.

In a centrally administered mode, the scan report is sent to F-Secure Policy Manager. You can check it also in the F-Secure Policy Manager Console.

3.5 Select Files That are Scanned

You can select the types of file and parts of your computer to scan in manual and scheduled scans.

Edit manual scanning settings to select files and folders you want to scan during the scheduled scan.

Two types of lists determine which files are scanned for viruses in manual and scheduled scans:

- Scanned file types list contains either all files or a defined list of file types.
- Lists of files excluded from scanning define exceptions to the list of scanned file types. File types or locations that are on the lists of excluded files are not scanned even if they are included in the list of scanned file types.

  The lists of scanned file types and excluded files let you define which parts of your computer will be scanned in different ways:

- You can include all files, and then optionally use the exclude list to exclude drives, directories, or files that you know are safe and do not want to be scanned.
- You can define a list of file types that you want to scan, so that only these file types are scanned.

3.5.1 Include Files

You can select the file types that you want to be scanned for viruses and spyware in manual and scheduled scans.

1. Go to **Server Protection > Manual Scanning** and click the **Settings** tab.
2. Under **Scan these files**, click **Configure** and select one of the following:
   - **Scan all files** to scan all files
   - **Scan defined files** to scan only the file types that you define
3. Click Apply.

The options you selected under **Scanning** options determine which files are included in future manual and scheduled scans.

All file types or locations on the excluded items list will override the settings that you defined here. File types on the excluded items list will not be scanned even if you selected them to be scanned here.

3.5.2 Exclude Files by Location

You can define a list of excluded folders or drives that you do not want to be scanned for viruses in manual and scheduled scanning.

Files in folders or drives that are excluded from scanning are not scanned even though they might be of a type that is included in scanned file types.

To define a list of files, folders, or drives excluded by location:

1. Go to **Server Protection > Manual Scanning** and click the **Settings** tab.
2. In **Exclude from scanning**, click **Configure**.
3. Add a file, drive, or folder to exclude:
   a. Select the **Objects** tab.
   b. Select **Exclude objects**.
   c. Click **Add**.
   d. Select the file, drive, or folder that you want to exclude from virus scanning.

   e. Click **OK**.

4. Repeat the previous step to exclude other files, drives, or folders from being scanned for viruses.
5. Click **OK** to close the **Exclude from Scanning** dialog.
6. Click **Apply**.

The selected files, drives or folders are excluded from future manual and scheduled scans.

3.5.3 Exclude File Types

You can exclude files from manual and scheduled scans by their file type.

To define a list of files excluded by file type:

1. Go to **Server Protection > Manual Scanning** and click the **Settings** tab.
2. In **Exclude from scanning**, click **Configure**.
3. Exclude a file type:
   a. Select the **Files** tab.
   b. Select **Exclude files with these extensions**.
   c. Type a file extension that identifies the type of files that you want to exclude.

      To specify files that have no extension, type '.'. You can use the wildcard '?' to represent any single character, or '*' to represent any number of characters.

      For example, to exclude executable files, type ‘`exe` ’ in the field.

   d. Click **Add**.
4. Repeat the previous step for any other extension you want to be excluded from being scanned for viruses.
5. Click **OK** to close the **Exclude from scanning** dialog.
6. Click **Apply**.

The selected file types are excluded from future manual and scheduled scans.

3.5.4 View Excluded Applications

You can view applications that you have excluded from future manual and scheduled scans, and remove them from the exclude list so they will be found in future scans.

To view the applications that are excluded from scanning:

1. Go to **Server Protection > Manual Scanning** and click the **Settings** tab.
2. In **Exclude from scanning**, click **Configure**.
3. Select the **Applications** tab.

   Only spyware and riskware applications can be excluded, not viruses.

4. To restore an application so that it will be found in future manual or scheduled scans:
   a. Select the application that you want to include in the scan again.
   b. Click **Remove**.
5. Click **OK** to close the **Exclude from scanning** dialog box.
6. Click **Apply**.

3.5.5 Scan Inside Compressed Files and Folders

You can scan for viruses that hide inside compressed files.

1. Go to **Server Protection** > **Manual Scanning** and click the **Settings** tab.
2. If you want to scan archive files and folders, such as `.zip` files, select **Scan inside compressed files**.

   Compressed files take slightly longer to scan.

3. Click **OK**.

4. Click **Apply**.

3.5.6 Select the Action When Something is Found

If viruses or spyware are found and you have set the program not to automatically handle viruses and spyware, you can now select whether to clean, delete, quarantine or only block the files in which a virus or spyware was found.

This step of the Scan Wizard will be skipped if you have set the program to always handle viruses and spyware automatically during a manual or scheduled scan or if you have set the program to automatically process malware found during this scan.

When using Web Console Scan Wizard, you are shown a list of infected files and the viruses and spyware that were found in these files. To handle these viruses and spyware:

1. Select the infected files that you want to handle.

   To view additional details of the infection, click the link in the Infection column.

2. Select the action that you want to take for the selected files.

   The files are handled immediately.

3. Repeat step 2 with all the files that you want to handle.
4. Click **Finish**.

If you are using the local Scan Wizard, you will have three separate iterations for handling detected viruses, spyware and riskware. To handle viruses from your computer:

1. Select the action to take for infected files. If you want to view the additional details of the infection, click the link in the **Infection** column.
2. Click **Next** to apply the actions.
3. Click **Next** to finish.

If spyware was found during the manual or scheduled scan, the Scan Wizard continues to the spyware cleaning step.

3.5.7 Actions You Can Take in Real-Time Scanning

The **Action to take** column shows you what actions you can take for the infected files in real-time scanning.

In addition to files, the infection can be found also in a registry entry or a process.

The following actions can be taken for viruses:

Action to take	What happens to the infected files
Disinfect automatically	The product tries to disinfect the viruses in any infected files that were found during real-time scanning.
Quarantine automatically (default)	The product moves any infected files found during real-time scanning to the quarantine where it cannot harm your computer.
Rename automatically	The product renames any infected files found during real-time scanning.
Delete automatically	The product deletes any infected files found during real-time scanning.

Action to take	What happens to the infected files
Report only	The product records the detected viruses in the `logfile.log` file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications (according to the settings that are specified on the Alerts page under **General > Administration**).

The following actions can be taken for spyware:

Action to take	What happens to the infected files
Quarantine automatically	The product moves any spyware found during real-time scanning to the quarantine where it cannot harm your computer.
Remove automatically	The product removes any spyware found during real-time scanning.
Report only (default)	The product leaves any spyware that was found during real-time scanning as it is and records the detection in the logfile.log file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications (according to the settings that are specified on the Alerts page under **General > Administration**).

3.5.8 Actions You Can Take in Manual or Scheduled Scanning

The **Action to take** column shows you what actions you can take for the infected files in manual or scheduled scanning.

In addition to files, the infection can be found also in a registry entry or a process.

The following actions can be taken for viruses:

Action to take	What happens to the infected files
Ask what to do (default)	The product asks you what to do if viruses are found during manual scanning
Disinfect automatically	The product tries to disinfect the viruses in any infected files that were found during manual or scheduled scanning. It is not always possible to disinfect a virus in a file. If this is not possible, the file is quarantined (except when found on network or removable drives), so the virus cannot harm the server.
Quarantine automatically	The product moves any infected files found during manual or scheduled scanning to the quarantine where it cannot harm your computer.

Action to take	What happens to the infected files
Rename automatically	The product renames any infected files found during manual or scheduled scanning.
Delete automatically	The product deletes any infected files found during manual or scheduled scanning.
Report only	The product leaves any infected files that was found during manual or scheduled scanning as they are and records the detection in the scan report. If real-time scanning is turned off, any malware is still able to harm the server if you select this option.

The following actions can be taken for spyware:

Action to take	What happens to the infected files
Ask what to do (default)	The product asks you what to do if spyware is found during manual scanning
Quarantine automatically	The product moves any spyware found during manual or scheduled scanning to the quarantine where it cannot harm your computer.
Remove automatically	The product removes any spyware found during manual or scheduled scanning.
Report only	The product leaves any spyware that was found during manual or scheduled scanning as it is and records the detection in the scan report. If real-time scanning is turned off, any malware is still able to harm the server if you select this option.

Centrally Managed Administration

Topics:

- *Overview*
- *F-Secure Anti-Virus Settings*
- *F-Secure DeepGuard Settings*
- *F-Secure Browsing Protection Settings*
- *F-Secure Anti-Virus for Microsoft Exchange Settings*
- *F-Secure Anti-Virus for Microsoft Exchange Statistics*
- *F-Secure Anti-Virus for Microsoft SharePoint Settings*
- *F-Secure Anti-Virus for Microsoft SharePoint Statistics*
- *F-Secure Software Updater Settings*
- *F-Secure Software Updater Statistics*
- *F-Secure Content Scanner Server Settings*
- *F-Secure Content Scanner Server Statistics*
- *F-Secure Management Agent Settings*
- *F-Secure Automatic Update Agent Settings*

4.1 Overview

If the product is installed in the centrally managed administration mode, it is managed centrally with F-Secure Policy Manager Console.

Note: This chapter groups product settings and statistics by their components. Depending on the selected product license and installed components, some settings may not be available.

You can still use the Web Console to manage the quarantined content and to configure settings that are not marked as **Final** in the F-Secure Policy Manager Console (settings marked as **Final** are greyed out in Web Console).

4.2 F-Secure Anti-Virus Settings

This component protects the server from programs that may steal personal information, damage the computer, or use it for illegal purposes. You can scan the server for malware in real time, manually, or your can schedule a scan at set times.

When any type of malware is found, they are by default disabled immediately before they can cause harm.

The product scans your local hard drives, any removable media (such as portable drives or compact disks) and downloaded content automatically by default.

4.2.1 Settings for Real-Time Protection

Real-time scanning protects the computer by scanning all files when they are accessed and by blocking access to those files that contain malware.

Scanning Enabled	Enable or disable the virus scan. The virus scan scans files on the server for viruses and other malicious code.
Limit Scanning Time	Limit the time that the real-time scanning can use for scanning files.

Boot Sector Scanning

Action on Infection	Select the action on infected boot sectors.
Scan Floppy Disk Boot Sectors	When enabled, the real-time scanning scans floppy disk boot sectors when a floppy disk is accessed.
Scan at Startup	When enabled, the product scans Master Boot Records and Boot Sectors at the system startup.

File Scanning

Scan Files	Specify files that are scanned for viruses. **Scan all files** - Scan all files in the system. **Files with these extensions** - Scans only the file types that you define. **Tip:** When the scan is set to scan all files, you may want to use the Excluded

	Extensions list to exclude files with specific extensions.
Decide Action Automatically	When enabled, the product overrides the **Action on Infection** setting and decides the action automatically, depending on infection type and other factors.
Action on Infection	The following actions can be taken for viruses: **Rename Automatically** - The product renames any infected files found during real-time scanning. **Delete Automatically** - The product deletes any infected files found during real-time scanning. **Disinfect Automatically** - The product tries to disinfect the viruses in any infected files that were found during real-time scanning. **Ask After Scan (default)** - The product asks what to do after the scan. **Report Only** - The product records the detected viruses in the `logfile.log` file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications. **Quarantine Automatically** - The product moves any infected files found during real-time scanning to the quarantine where it cannot harm your computer.
Scan Network Drives	When enabled, the product scans files accessed over the network.
Scan when Renamed	When enabled, the product scans files when they are renamed.
Scan Inside Archives	Specify whether files inside compressed archive files are scanned for viruses and other malicious code.
Inclusions and Exclusions	Specify files that are scanned.

Inclusions and Exclusions

Included Extensions	Specify file extensions that should be scanned.
Included Extensions for Compressed Files	Specify file extensions of archived files that should be scanned.
Add Extensions Defined in Database Updates	Enable to add the file name extensions defined in the database update packages published by

	F-Secure Corporation to the list of extensions defined in the policy.
Excluded Extensions Enabled	Enable to exclude specified file extensions from the scan.
Excluded Extensions	Specify file extensions that should not be scanned.
Excluded Objects Enabled	Enable to exclude specified files or folders from the scan. Specify files and folders that you want to exclude in the **Excluded Objects** list.
Excluded Processes Enabled	Enable to exclude specified processes from the scan. Specify processes that you want to exclude in the Excluded Processes list. Any files accessed by the excluded process are automatically excluded from the scan.

4.2.2 Settings for Manual Scanning

You can scan the server manually, for example if you suspect that you have malware on the computer. You can scan your whole computer or scan for a specific type of malware or a specific location.

To start the manual scan, follow these instructions:

1. Go to the **F-Secure Anti-Virus / Operations / Launch Manual Scanning** branch.
2. Click **Start** in the Editor pane.

Allow Manual Scanning	Specify users who are allowed to run manual scans. **Not Allowed** - Manual scanning is not allowed. **Users with Administrative Rights** - Only users with administrative rights can start the manual scan. **All Users** - Anyone can start the manual scan.
Max Number of Scan Tasks	Specify the maximum number of simultaneous scanning tasks.
Scanning Time Limit	Limit the time that the real-time scanning can use for scanning files.

Memory Scan

Scan Binaries of Active Processes	Enable to scan the binaries of active processes when the task to scan all hard disks for viruses is executed.
Stop Active Infected Processes	If **Scan Binaries of Active Processes** setting is Enabled, stops all detected malicious processes.

Boot Sector Scanning

Action on Infection

Select the action on infected boot sectors.

Disinfect Automatically - The product tries to disinfect the viruses in any infected files that were found during the scan.

Ask After Scan - The product asks what to do after the scan.

Report only - The product records the detected viruses in the logfile.log file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications.

Scan Floppy Disk Boot Sectors

When enabled, the real-time scanning scans floppy disk boot sectors when a floppy disk is accessed.

File Scanning

Scan Files

Specify files that are scanned for viruses.

Scan All Files - Scan all files in the system.

Files with These Extensions - Scans only the file types that you define.

Tip: When the scan is set to scan all files, you may want to use the Excluded Extensions list to exclude files with specific extensions.

Action on Infection

The following actions can be taken for viruses:

Rename Automatically - The product renames any infected files found during real-time scanning.

Delete Automatically - The product deletes any infected files found during real-time scanning.

Clean Automatically - The product tries to disinfect the viruses in any infected files that were found during real-time scanning.

Ask After Scan (default) - The product asks what to do after the scan.

Report Only - The product records the detected viruses in the `logfile.log` file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications.

Quarantine Automatically - The product moves any infected files found during real-time scanning to the quarantine where it cannot harm your computer.

Scan Inside Archives

Specify whether files inside compressed archive files are scanned for viruses and other malicious code.

Inclusions and Exclusions

Included Extensions	Specify file extensions that should be scanned.
Included Extensions for Compressed Files	Specify file extensions of archived files that should be scanned.
Add Extensions Defined in Database Updates	Enable to add the file name extensions defined in the database update packages published by F-Secure Corporation to the list of extensions defined in the policy.
Excluded Extensions Enabled	Enable to exclude specified file extensions from the scan.
Excluded Extensions	Specify file extensions that should not be scanned.
Excluded Objects Enabled	Enable to exclude specified files or folders from the scan. Specify files and folders that you want to exclude in the **Excluded Objects** list.

Heuristic Scanning

Heuristic Scanning Enabled	Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

Rootkit Scanning

Rootkit Scanning Enabled	Enable or disable the rootkit scan.
Include Rootkit Scanning in Full Computer Check	Specify whether the full computer check should scan the computer for rootkits.
Report Suspicious Hidden Items in a Full Computer Check	Specify whether the product reports suspicious hidden items that it detects during the full computer check. If you include the rootkit scanning in the full computer check, suspicious hidden items are reported always.

4.3 F-Secure DeepGuard Settings

DeepGuard analyzes the content of files and behavior of programs, and blocks new and undiscovered viruses, worms, and other malicious programs that try to make potentially harmful changes to your computer.

System changes that can be dangerous include:

- system setting (Windows registry) changes,

- attempts to turn off important system programs, for example, security programs like this product, and
- attempts to edit important system files.

DeepGuard continuously watches for these changes and checks each program that attempts to change the system.

When DeepGuard detects a program attempting to make potentially harmful changes to the system, it allows the program to run in a safe-zone, unless you have specifically allowed or blocked the program.

In the safe-zone, the program cannot harm your computer. DeepGuard analyzes what changes the program tried to make, and based on this, decides how likely the program is to be malware.

DeepGuard automatically either allows or blocks the program, or asks you whether to allow or block the program, depending on how likely the program is to be malware.

DeepGuard Enabled	When DeepGuard is enabled, you can prevent suspicious programs from making potentially harmful system changes in the computer.
Action on System Modification Attempt	Select one of the following default actions if DeepGuard detects a system modification attempt. **Do Not Ask** - DeepGuard blocks unsafe applications and allows safe applications automatically without asking you any questions. **Ask When Case is Unclear** - Ask when DeepGuard detects a program trying to make potentially harmful system changes and it cannot identify whether the program is safe or unsafe. **Always Ask Permission** - DeepGuard asks you whether you want to allow or block all monitored actions, even when it identifies the application as safe.
Local Administrator Control	Specify whether the local administrator can make decisions on events that on processes that belong to another user. If **Own processes** is selected, local administrators can only permit their own processes.
Use Real-time Protection Network	Using Real-time Protection Network improves the DeepGuard detection rate of suspicious programs. For the full Real-time Protection Network policy, consult our web site: *http://www.f-secure.com/en/web/home_global/rtpn-privacy*
Enhanced Process Monitoring Enabled	When enhanced process monitoring is turned on, DeepGuard temporarily modifies running programs for maximum protection. **Note:** Enhanced process monitoring may cause problems with programs that make sure that they are not corrupted or modified.
Applications	Use the Applications list to select applications that are commonly used in your company as safe.

	To prevent a certain application from running, specify **Trusted** as **No**.

4.4 F-Secure Browsing Protection Settings

Browsing protection helps you evaluate the safety of web sites you visit and prevents you from unintentionally accessing harmful web sites.

Browsing protection shows you safety ratings for web sites that are listed on search engine results. By helping you avoid web sites that contain security threats, such as malware (viruses, worms, trojans) and phishing, you avoid the latest Internet threats that are not yet recognized by traditional antivirus programs.

There are four possible safety ratings for web sites: safe, suspicious, harmful and unknown. These safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

4.4.1 Reputation Based Protection

Browsing Protection Enabled	When Browsing Protection is enabled, you can protect your browsers from accessing harmful web sites.
Reputation Based Protection Enabled	When Reputation Based Protection is enabled, the product obtains safety information on sites and blocks access to sites that have **harmful** safety rating.

Features

Show link reputations on search results	When enabled, browsing protection ratings will be displayed for the sites listed on search engines (Google, Yahoo, etc.).
Trusted sites	If the product blocks access to a page that you trust and want to access, define the site as trusted to allow access to it.
Disallowed sites	To block access to a web site completely, define it as a disallowed site.
Allow user to continue to blocked pages	Specify whether users can open blocked pages after viewing the warning message.

4.5 F-Secure Anti-Virus for Microsoft Exchange Settings

4.5.1 General Settings

Notifications

Specify **Notification Sender Address** that is used for sending warning and informational messages to the end-users (for example, recipients, senders and mailbox owners).

Note: Make sure that the notification sender address is a valid SMTP address. A public folder cannot be used as the notification sender address.

Network Configuration

The mail direction is based on the **Internal Domains** and **Internal SMTP senders** settings and it is determined as follows:

1. E-mail messages are considered **internal** if they come from internal SMTP sender hosts and mail recipients belong to one of the specified internal domains (internal recipients).
2. E-mail messages are considered **outbound** if they come from internal SMTP sender hosts and mail recipients do not belong to the specified internal domains (external recipients).
3. E-mail messages that come from hosts that are not defined as internal SMTP sender hosts are considered **inbound**.
4. E-mail messages submitted via MAPI or Pickup Folder are treated as if they are sent from the internal SMTP sender host.

   Note: If e-mail messages come from internal SMTP sender hosts and contain both internal and external recipients, messages are split and processed as internal and outbound respectively.

   Note: On Microsoft Exchange Server 2003, internal messages which are submitted via MAPI or Pickup Folder are not delivered via transport level. Therefore, those messages do not pass Transport Protection and they are checked on the storage level only.

   Note: To scan or filter messages from internal hosts on Microsoft Exchange Server 2003, use corresponding real-time scanning settings in the storage protection section.

Internal Domains

Specify internal domains. Messages coming to internal domains are considered to be inbound mail unless they come from internal SMTP sender hosts.

Separate each domain name with a space. You can use an asterisk (*) as a wildcard. For example, ***example.com internal.example.net**

Internal SMTP Senders

Specify the IP addresses of hosts that belong to your organization. Specify all hosts within the organization that send messages to Exchange Edge or Hub servers via SMTP as Internal SMTP Senders.

Separate each IP address with a space. An IP address range can be defined as:

- a network/netmask pair (for example, 10.1.0.0/255.255.0.0),
- a network/nnn CIDR specification (for example, 10.1.0.0/16), or
- IPv6 address (for example, 1::, 2001::765d 2001::0-5, 2001:db8:abcd:0012::0/64, 2001:db8:abcd:abcd::/52, ::1).

You can use an asterisk (*) to match any number or dash (-) to define a range of numbers. For example, 172.16.4.4 172.16.*.1 172.16.4.0-16 172.16.250-255.*

Note: If end-users in the organization use other than Microsoft Outlook e-mail client to send and receive e-mail, it is

	recommended to specify all end-user workstations as Internal SMTP Senders. ☞ **Note:** If the organization has Exchange Edge and Hub servers, the server with the Hub role installed should be added to the Internal SMTP Sender on the server where the Edge role is installed. ☞ **Important:** Do not specify the server where the Edge role is installed as Internal SMTP Sender.

Lists and Templates

Match Lists

Specify file and match lists that can be used by other settings.

List name	Specify the name for the match list.
Type	Specify whether the list contains keywords, file patterns or e-mail addresses.
Filter	Specify file names, extensions, keywords or e-mail addresses that the match list contains. You can use wildcards. ☞ **Note:** To add multiple patterns to the filter, add each list item to a new line.
Description	Specify a short description for the list.

Message Templates

Specify message templates for notifications.

Template name	Specify the name for the message template.
Subject line	Specify the subject line of the notification message.
Message body	Specify the notification message text. For more information about the variables you can use in notification messages, see *Variables in Warning Messages*.

Quarantine

When the product places content to the E-mail Quarantine, it saves the content as separate files into the E-mail Quarantine Storage and inserts an entry to the Quarantine Database with information about the quarantined content.

Quarantine Storage

Specify the path to the E-mail Quarantine storage where all quarantined mails and attachments are placed.

Note: If you change the Quarantine Storage setting, select the **Final** checkbox in the **Restriction Editor** to override initial settings.

Note: During the installation, the product adjusts the access rights to the Quarantine Storage so that only the product, operating system and the local administrator can access it. If you change the Quarantine Storage setting, make sure that the new location has secure access permissions. For more information, see *Moving the E-mail Quarantine Storage*.

Retain Items in Quarantine

Specify how long quarantined e-mails are stored in the E-mail Quarantine before they are deleted automatically.

The setting defines the default retention period for all Quarantine categories. To change the retention period for different categories, configure **Quarantine Cleanup Exceptions** settings.

Delete Old Items Every

Specify how often old items are deleted from the E-mail Quarantine.

The setting defines the default cleanup interval for all Quarantine categories. To change the cleanup interval for different categories, configure **Quarantine Cleanup Exceptions** settings.

Quarantine Cleanup Exceptions

Specify separate Quarantine retention periods and cleanup intervals for infected files, suspicious files, disallowed attachments, disallowed content, spam messages, scan failures and unsafe files.

Quarantine Size Threshold

Specify the critical size (in megabytes) of the E-mail Quarantine. If the Quarantine size reaches the specified value, the product sends an alert to the administrator.

If the threshold is specified as zero (0), the size of the Quarantine is not checked.

Quarantined Items Threshold

Specify the critical number of items in the E-mail Quarantine. When the Quarantine holds the critical number of items, the product sends an alert to the administrator.

If the threshold is specified as zero (0), the amount of items is not checked.

Notify When Quarantine Threshold is Reached

Specify the level of the alert that is sent to administrator when threshold levels are reached.

Released Quarantine Message Template

Specify the template for the message that is sent to the intended recipients when e-mail content is released from the quarantine. For more information, see *Lists and Templates*.

The product generates the message only when the item is removed from the Microsoft Exchange Server store and sends it automatically when you release the item to intended recipients.

Automatically Process Unsafe Messages

Specify how often the product tries to reprocess unsafe messages that are retained in the E-mail Quarantine. Set the value to Disabled to process unsafe messages manually.

Max Attempts to Process Unsafe Messages

Specify how many times the product tries to reprocess unsafe messages that are retained in the E-mail Quarantine.

Use the Final Action on Unsafe Messages setting to specify the action that takes place if the message is retained in the Quarantine after the maximum attempts.

Final Action on Unsafe Messages

Specify the action on unsafe messages after the maximum number of reprocesses have been attempted.

Leave in Quarantine - Leave messages in the Quarantine and process them manually.

Release to Intended Recipients - Release messages from the Quarantine and send them to original recipients.

Quarantine Log Directory

Specify the path to the directory where E-mail Quarantine logfiles are placed.

Rotate Quarantine Logs Every

Specify how often the product rotates E-mail Quarantine logfiles. At the end of each rotation time a new log is created.

Keep Rotated Quarantine Logs

Specify how many rotated log files are kept.

Sample Submission

You can use the product to send samples of unsafe e-mails and new, yet undefined malware to F-Secure for analysis.

Max Submission Attempts

Specify how many times the product attempts to send the sample if the submission fails.

Resend Interval

Specify the time interval (in minutes) how long the product should wait before trying to send the sample again if the previous submission failed.

Connection Timeout

Specify the time (in seconds) how long the product tries to contact the F-Secure Hospital server.

Send Timeout

Specify the time (in seconds) how long the product waits for the sample submission to complete.

Content Scanner Server

Edit the Content Scanner Server settings to change the general content scanning options.

Max Size of Data Processed in Memory

Specify the maximum size (in kilobytes) of data to be transferred to the server via shared memory in the local interaction mode. When the amount of data exceeds the specified limit, a local temporary file will be used for data transfer.

If the option is set to zero (0), all data transfers via shared memory are disabled.

The setting is ignored if the local interaction mode is disabled.

Connection Timeout

Specify the time interval (in seconds) how long the product should wait for a response from F-Secure Content Scanner Server before it stops attempting to send or receive data.

Working directory

Specify the name and location of the working directory, where temporary files are placed.

Important:

This setting must be defined as Final with the Restriction Editor before the policies are distributed. Otherwise the setting will not be changed in the product.

Note: The installation automatically adjusts the access rights so that only the operating system and the local administrator can access files in the Working directory. If you change this setting after the installation, make sure that the new folder has secure access permissions.

Note: If F-Secure Content Scanner Server uses a proxy server when it connects to the threat detection center and the proxy server requires authentication, the proxy authentication settings can be configured with the product Web Console only. For more information, see *Proxy Server*.

4.5.2 Transport Protection

You can configure inbound, outbound and internal message protection separately. For more information about the mail direction and configuration options, see *Network Configuration*.

Attachment Filtering

Specify attachments to remove from inbound, outbound and internal messages based on the file name or the file extension.

Strip Attachments	Enable or disable the attachment stripping.
List of Attachments to Strip	Specify which attachments are stripped from messages. For more information, see *Lists and Templates*.
Use Exclusions	Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.
Action on Stripped Attachments	Specify how disallowed attachments are handled. **Drop Attachment** - Remove the attachment from the message and deliver the message to the recipient without the disallowed attachment. **Drop the Whole Message** - Do not deliver the message to the recipient at all.
Quarantine Stripped Attachments	Specify whether stripped attachments are quarantined. The default option is **Enabled**.
Do Not Quarantine These Attachments	Specify which files are not quarantined even when they are stripped. For more information, see *Lists and Templates*.
Send Notification Message to Recipient	Specify the template for the notification message that is sent to the intended recipient when disallowed or suspicious attachment is found. ☞ **Note:** Note that the notification message is not sent if the whole message is dropped.
Send Notification Message to Sender	Specify the template for the notification message that is sent to the original sender of the message when disallowed or suspicious attachment is found. For more information, see *Lists and Templates*. Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.

Do Not Notify on These Attachments

Specify attachments that do not generate notifications. When the product finds specified file or file extension, no notification is sent.

Notify Administrator

Specify whether the administrator is notified when the product strips an attachment and the alert level of the notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Virus Scanning

Specify inbound, outbound and internal messages and attachments that should be scanned for malicious code.

Note: Disabling virus scanning disables archive processing and grayware scanning as well.

Scan Messages for Viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

List of Attachments to Scan

Specify attachments that are scanned for viruses. For more information, see *Lists and Templates*.

Use Exclusions

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scan.

Heuristic Scanning

Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

By default, the heuristic scan is enabled for inbound mails and disabled for outbound and internal mails.

Note: The heuristic scan may affect the product performance and increase the risk of false malware alarms.

Attempt to Disinfect Infected Attachments

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Action on Infected Messages

Specify whether to drop the infected attachment or the whole message when an infected message is found.

Drop Attachment - Remove the infected attachment from the message and deliver the message to the recipient without the attachment.

Drop the Whole Message - Do not deliver the message to the recipient at all.

Quarantine Infected Messages

Specify whether infected or suspicious messages are quarantined.

Do Not Quarantine These Infections

Specify infections that are never placed in the quarantine. If a message is infected with a virus or worm which has a name that matches a keyword specified in this list, the message is not quarantined. For more information, see *Lists and Templates*.

Send Virus Notification Message to Recipient

Specify the template for the notification message that is sent to the intended recipient when a virus or other malicious code is found.

Note: Note that the notification message is not sent if the whole message is dropped.

Send Virus Notification Message to Sender

Specify the template for the notification message that is sent to the original sender of the message when a virus or other malicious code is found.

Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.

For more information, see *Lists and Templates*.

Do Not Notify on These Infections

Specify infections that do not generate notifications. When the product finds the specified infection, no notification is sent. For more information, see *Lists and Templates*.

Notify Administrator

Specify whether the administrator is notified when the product finds a virus in a message.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Archive Processing

Specify how the product processes inbound, outbound and internal archive files.

Note that scanning inside archives takes time. Disabling scanning inside archives improves performance, but it also means that the network users need to use up-to-date virus protection on their workstations.

Note: Archive processing is disabled when virus scanning is disabled.

Scan Archives	Specify whether files inside compressed archive files are scanned for viruses and other malicious code.
List of Files to Scan Inside Archives	Specify files inside archives that are scanned for viruses. For more information, see *Lists and Templates*.
Use Exclusions	Specify files that are not scanned inside archives. Leave the list empty if you do not want to exclude any files from the scan.
Max Levels in Nested Archives	Specify how many levels of archives inside other archives the product scans when **Scan Viruses Inside Archives** is enabled.
Action on Max Nested Archives	Specify the action to take on archives with nesting levels exceeding the upper level specified in the **Max Levels in Nested Archives** setting. **Pass through** - Deliver the message with the archive to the recipient. **Drop archive** - Remove the archive from the message and deliver the message to the recipient without it. **Drop the whole message** - Do not deliver the message to the recipient.
Action on Password Protected Archives	Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content. **Pass through** - Deliver the message with the password protected archive to the recipient. **Drop archive** - Remove the password protected archive from the message and deliver the message to the recipient without it. **Drop the whole message** - Do not deliver the message to the recipient.
Detect Disallowed Files Inside Archives	Specify whether files inside compressed archive files are processed for disallowed content. **Note:** Disallowed content is not processed when the archive scanning is disabled.
List of Disallowed Files to Detect Inside Archives	Specify files which are not allowed inside archives. For more information, see *Lists and Templates*.

Action on Archives with Disallowed Files

Specify the action to take on archives which contain disallowed files.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without it.

Drop the whole message - Do not deliver the message to the recipient.

Quarantine Dropped Archives

Specify whether archives that are not delivered to recipients are placed in the quarantine. For more information, see *E-mail Quarantine Management*.

Notify Administrator

Specify whether the administrator is notified when the product blocks a malformed, password protected, or overnested archive file.

Note: If the archive is blocked because it contains malware, grayware or disallowed files, the administrator receives a notification about that instead of this notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Grayware Scanning

Specify how the product processes grayware items in inbound, outbound and internal messages.

Note that grayware scanning increases the scanning overhead. By default, grayware scanning is enabled for inbound messages only.

Note: Grayware scanning is disabled when virus scanning is disabled.

Scan Messages for Grayware

Enable or disable the grayware scan.

The default value is **Enabled** for inbound messages and **Disabled** for outbound and internal messages.

Action on Grayware

Specify the action to take on items which contain grayware.

Pass Through - Leave grayware items in the message.

Drop Attachment - Remove grayware items from the message.

Drop the Whole Message - Do not deliver the message to the recipient.

Grayware Exclusion List

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan.

Quarantine Dropped Grayware

Specify whether grayware attachments are quarantined.

Do Not Quarantine This Grayware

Specify grayware that are never placed in the quarantine. For more information, see *Lists and Templates*.

Send Warning Message to Recipient

Specify the template for the notification message that is sent to the intended recipient when a grayware item is found in a message.

Note: Note that the notification message is not sent if the whole message is dropped.

Send Warning Message to Sender

Specify the template for the notification message that is sent to the original sender of the message when a grayware item is found in a message.

Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.

For more information, see *Lists and Templates*.

Do Not Notify on This Grayware

Specify the list of keywords for grayware types that are not notified about.

If the product finds a grayware item with a name that matches the keyword, the recipient and the sender are not notified about the grayware item found.

Leave the list empty if you do not want to exclude any grayware types from notifications.

Notify Administrator

Specify whether the administrator is notified when the product finds a grayware item in a message.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Content Filtering

Specify how the product filters disallowed content in inbound, outbound and internal messages.

Filter Disallowed Content

Specify whether e-mail messages are scanned for disallowed content.

Disallowed Keywords in Message Subject

Specify the list of disallowed keywords to check in e-mail message subjects. For more information, see *Using Keywords in Content Filtering*.

Disallowed Keywords in Message Text

Specify the list of disallowed keywords to check in e-mail message text. For more information, see *Using Keywords in Content Filtering*.

Action on Disallowed Content

Specify the action to take on messages which contain disallowed keywords.

Report only - Deliver the message to the recipient and notify the administrator that the scanned message contained disallowed content.

Drop the whole message - Do not deliver the message to the recipient.

Quarantine - Quarantine the message with disallowed content.

Send Notification Message to Recipient

Specify whether recipients are notified when disallowed content is found.

Send Notification Message to Sender

Specify whether the original sender is notified when disallowed content is found.

To enable the notification, select a template for the notification message. To disable the notification, leave the notification field empty.

For more information, see *Lists and Templates*.

Notify Administrator

Specify whether the administrator is notified when the product finds a message with disallowed content.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Using Keywords in Content Filtering

When the content filtering is enabled, all messages are checked against every keyword sequence that is specified in the selected list of keywords.

A keyword may contain any characters, including punctuation symbols, spaces, and other word separators. Keywords are case insensitive.

You can use ‘?’ character in a keyword to match any character in that position in the keyword and ‘*’ to match any number of characters.

Keyword examples:

example

Matches any message text or subject that contains the word ‘example’.

another example	Matches any message text or subject that contains the ‘another example’ text. Words ‘another’ and ‘example’ have to be separated with exactly one space character.
co?p?rate	Matches any message text or subject that contains - for example - words ‘corporate’ or ‘cooperate’.
another*example	Matches any message text or subject that contains words ‘another’ and ‘example’ separated with any number of characters. For example, ‘another example’ or ‘another keyword example’.

To represent ‘?’ or ‘*’ characters themselves in keywords, use ‘\?’ and ‘*’ sequences correspondingly. To represent ‘\’ character, use ‘\\’.

For example, to match the '*** SPAM ***' string, enter '*** spam ***'.

Spam Control

Spam Control settings allow you to configure how the product scans incoming mail for spam.

Note: You can configure Spam Control settings for inbound messages, and only if you have F-Secure Spam Control installed. Otherwise they will be ignored.

The threat detection engine can identify spam and virus patterns from the message envelope, headers and body during the first minutes of the new spam or virus outbreak.

Spam Filtering	Specify whether inbound mails are scanned for spam.
Spam Filtering Level	Specify the spam filtering level. All messages with the spam filtering level lower than the specified value can pass through. Decreasing the level allows less spam to pass, but more regular mails may be falsely identified as spam. Increasing the level allows more spam to pass, but a smaller number of regular e-mail messages are falsely identified as spam. For example, if the spam filtering level is set to 3, more spam is filtered, but also more regular mails may be falsely identified as spam. If the spam filtering level is set to 7, more spam may pass undetected, but a smaller number of regular mails will be falsely identified as spam.
Action on Spam Messages	Specify actions to take with messages considered as spam, based on the spam filtering level. `Quarantine` - Place the message into the quarantine folder. **Forward** - Forward the message to the e-mail address specified in the **Forward Spam Messages To E-mail Address** setting.

`Delete` - Delete the message.

Add X-Header with Spam Flag

Specify if a spam flag is added to the mail as the X-Spam-Flag header in the following format:`X-Spam-Flag:<flag>`

where `<flag>` is `YES` or `NO`

Add X-Header with Summary

Specify if the summary of triggered hits is added to the mail as X-Spam-Status header in the following format:`X-Spam-Status: <flag>, hits=<scr> required=<sfl> tests=<tests>`

where

- `<flag>` is `Yes` or `No`.
- `<scr>` is the spam confidence rating returned by the spam scanner,
- `<sfl>` is the current spam filtering level,
- `<tests>` is the comma-separated list of tests run against the mail.

Modify Spam Message Subject

Specify if the product modifies the subject of mail messages considered as spam.

The default value is **Enabled**.

Add This Text to Spam Message Subject

Specify the text that is added in the beginning of the subject of messages considered as spam.

The default value is ***** SPAM *****.

Forward Spam Messages To E-mail Address

Specify the e-mail address where messages considered as spam are forwarded when the **Action on Spam Messages** setting is set to **Forward**.

Safe Senders

Specify safe senders. Messages originating from the specified addresses are never treated as spam.

Blocked Senders

Specify blocked senders. Messages originating from the specified addresses are always treated as spam.

Safe Recipients

Specify safe recipients. Messages sent to the specified addresses are never treated as spam.

Blocked Recipients

Specify blocked recipients. Messages sent to the specified addresses are always treated as spam.

Note: The product checks the sender address from the SMTP message envelope, not from the message headers.

Max Message Size

Specify the maximum size (in kilobytes) of messages to be scanned for spam. If the size of the

	message exceeds the maximum size, the message is not filtered for spam. **Note:** Since all spam messages are relatively small in size, it is recommended to use the default value.

File Type Recognition

Select whether you want to use **Intelligent File Type Recognition** or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. Intelligent File Type Recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using Intelligent File Type Recognition strengthens the security, but can degrade the system performance.

Mail Disclaimer

When the disclaimer is enabled, a disclaimer text is added to all outbound messages.

Note: You can configure Mail Disclaimer settings for outbound messages only.

Important:

Some malware add disclaimers to infected messages, so disclaimers should not be used for stating that the message is clean of malware.

Add Disclaimer	Specify whether you want to add a disclaimer to all outbound messages.
Disclaimer	Specify the text of disclaimer that is added at the end of outbound messages.

Security Options

Configure security options to limit actions on malformed and suspicious messages.

Action on Malformed Mails	Specify the action for non-RFC compliant e-mails. If the message has an incorrect structure, the product cannot parse the message reliably. **Drop the Whole Message** - Do not deliver the message to the recipient. **Pass Through** - The product allows the message to pass through. **Pass Through and Report** - The product allows the message to pass through, but sends a report to the administrator.
Max Levels of Nested Messages	Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.

☞ **Note:** It is not recommended to set the maximum nesting level to unlimited as this will make the product more vulnerable to DoS (Denial-of-Service) attacks.

Action on Mails with Exceeding Nesting Levels

Specify the action to take on messages with nesting levels exceeding the upper level specified in the **Max Levels of Nested Messages** setting.

Drop the Whole Message - Messages with exceeding nesting levels are not delivered to the recipient.

Pass Through - Nested messages are scanned up to level specified in the **Max Levels of Nested Messages** setting. Exceeding nesting levels are not scanned, but the message is delivered to the recipient.

Quarantine Problematic Messages

Specify if mails that contain malformed or broken attachments are quarantined for later analysis or recovery.

Notify Administrator

Specify whether the administrator is notified when the product detects a malformed or a suspicious e-mail message.

☞ **Note:** Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

Trusted Senders and Recipients

You can use trusted senders and recipients lists to exclude some messages from the mail scanning and processing completely.

Trusted Senders

Specify senders who are excluded from the mail scanning and processing. For more information, see *Lists and Templates*.

Trusted Recipients

Specify recipients who are excluded from the mail scanning and processing. For more information, see *Lists and Templates*.

4.5.3 Storage Protection

Edit general Storage Protection settings to configure how mailboxes and public folders are scanned in the Exchange Store with real-time, manual and scheduled scanning.

4.5.3.1 Real-Time Scanning

The real-time scanning can automatically scan messages that have been created or received.

General

Specify which messages you want to scan during the real-time scanning.

Scan Only Messages Created Within

Specify which messages are scanned with the real-time scanning, for example; **Last hour**. **Last day**. **Last week**. Messages that have been created before the specified time are not scanned.

Note: This setting does not affect Microsoft Exchange Server 2003.

Scan Timeout

Specify how long to wait for the real-time scan result. After the specified time, the client that tries to access the scanned message gets the "virus scanning in progress" notification.

Attachment Filtering

Attachment filtering can remove attachments from messages in the Microsoft Exchange Storage based on the file name or the file extension of the attachment.

Process Mailboxes

Specify mailboxes that are filtered for attachments.

Disabled - Do not filter any mailboxes for attachments.

Process All Mailboxes - Filter attachments in all mailboxes.

Process Only Included Mailboxes - Filter attachments in the **Included Mailboxes** list.

Process All Except Excluded Mailboxes - Do not filter attachments in the **Excluded Mailboxes** list but process all other mailboxes.

Included Mailboxes

Specify mailboxes that are filtered for attachments when the **Process Mailboxes** setting is set to **Process Only Included Mailboxes**.

Excluded Mailboxes

Specify mailboxes that are not filtered for attachments when the **Process Mailboxes** setting is set to **Process All Except Excluded Mailboxes**.

Process Public Folders

Specify public folders that are filtered for attachments.

Disabled - Do not filter any public folders for attachments.

Process All Folders - Filter attachments in all public folders.

Process Only Included Folders - Filter attachments in the **Included Folders** list.

Process All Except Excluded Folders - Do not filter attachments in the **Excluded Folders** list but process all other public folders.

Included Folders

Specify public folders that are filtered for attachments when the **Process Public Folders** setting is set to **Process Only Included Folders**.

Excluded Folders

Specify public folders that are not filtered for attachments when the **Process Public Folders** setting is set to **Process All Except Excluded Folders**.

List of Attachments to Strip

Specify the list of attachments that are stripped from messages. For more information, see *Lists and Templates*.

Use Exclusions

Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from filtering.

Quarantine stripped attachments

Specify whether stripped attachments are quarantined.

Do not quarantine these attachments

Specify attachments which are not quarantined even when they are stripped.

For more information, see *Lists and Templates*.

Replacement text template

Specify the template for the text that replaces the suspicious or disallowed attachment when the attachment is removed from the message. For more information, see *Lists and Templates*.

Virus Scanning

Specify messages and attachments in the Microsoft Exchange Storage that should be scanned for malicious code.

Note: Disabling virus scanning disables archive processing and grayware scanning as well.

Scan Mailboxes

Specify mailboxes that are scanned for viruses.

Disabled - Do not scan any mailboxes.

Scan All Mailboxes - Scan all mailboxes.

Scan Only Included Mailboxes - Scan mailboxes specified in the **Included Mailboxes** list.

Scan All Except Excluded Mailboxes - Scan all mailboxes except those specified in the **Excluded Mailboxes** list.

Included Mailboxes

Specify mailboxes that are scanned for viruses when the **Scan Mailboxes** setting is set to **Scan Only Included Mailboxes**.

Excluded Mailboxes

Specify mailboxes that are not scanned when the **Scan Mailboxes** setting is set to **Scan All Except Excluded Mailboxes**.

Scan Public Folders

Specify public folders that are scanned for viruses.

Disabled - Do not scan any public folders.

Scan All Folders - Scan all public folders.

Scan Only Included Folders - Scan public folders specified in the **Included Folders** list.

Scan All Except Excluded Folders - Scan all public folders except those specified in the **Excluded Folders** list.

Important:

You need to specify the primary SMTP address for the account which is used to scan items in public folders on Microsoft Exchange 2010. The user account must have permissions to access and modify items in the public folders. For more information, see *Advanced*.

Included Folders

Specify public folders that are scanned for viruses when the **Scan Public Folders** setting is set to **Scan Only Included Folders**.

Excluded Folders

Specify public folders that are not scanned when the **Scan Public Folders** setting is set to **Scan All Except Excluded Folders**.

List of Attachments to Scan

Specify attachments that are scanned for viruses. For more information, see *Lists and Templates*.

Use Exclusions

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scan.

Attempt to Disinfect Infected Attachments

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine Infected Attachments

Specify whether infected and suspicious attachments are quarantined.

Do Not Quarantine This Infections

Specify infections that are never placed in the quarantine. For more information, see *Lists and Templates*.

Replacement Text Template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Lists and Templates*.

Archive Processing

Specify how the product processes archive files in Microsoft Exchange Storage.

Note: Archive processing is disabled when virus scanning is disabled.

Scan Archives

Specify if files inside archives are scanned for viruses and other malicious code.

List of Files to Scan Inside Archives

Specify files that are scanned for viruses inside archives.

Use Exclusions

Specify files inside archives that are not scanned. Leave the list empty if you do not want to exclude any files from the scan.

Max Levels in Nested Archives

Specify how many levels deep to scan in nested archives, if **Scan Viruses Inside Archives** is enabled.

A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.

Specify the number of levels the product goes through before the action selected in **Action on Max Nested Archives** takes place. The default setting is 3.

Action on Max Nested Archives

Specify the action to take on nested archives with nesting levels exceeding the upper level specified in the **Max Levels in Nested Archives** setting.

Pass Through - Nested archives are scanned up to level specified in the **Max Levels in Nested Archives** setting. Exceeding nesting levels are not scanned, but the archive is not removed.

Drop Archive - Archives with exceeding nesting levels are removed.

Action on Password Protected Archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Leave the password protected archive in the message.

Drop archive - Remove the password protected archive from the message.

Quarantine Dropped Archives

Specify whether archives that are not delivered to recipients are placed in the quarantine. For more information, see *E-mail Quarantine Management*.

Grayware Scanning

Specify how the product processes grayware items in Microsoft Exchange Storage.

Note: Grayware scanning is disabled when virus scanning is disabled.

Scan Messages for Grayware

Enable or disable the grayware scan.

Action on Grayware

Specify the action to take on items which contain grayware.

Report only - Leave grayware items in the message and notify the administrator.

Drop attachment - Remove grayware items from the message.

Grayware Exclusion List

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan.

Quarantine Dropped Grayware

Specify whether grayware attachments are quarantined.

Do Not Quarantine These Grayware

Specify grayware that are never placed in the quarantine. For more information, see *Lists and Templates*.

Replacement Text Template

Specify the template for the text that replaces the grayware attachment when the grayware attachment is removed from the message. For more information, see *Lists and Templates*.

File Type Recognition

Select whether you want to use **Intelligent File Type Recognition** or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. Intelligent File Type Recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using Intelligent File Type Recognition strengthens the security, but can degrade the system performance.

4.5.3.2 Manual Scanning

You can scan mailboxes and public folders for viruses and strip attachments manually at any time. To manually scan mailboxes and public folders you have specified in the settings, follow these instructions:

1. Browse to the F-Secure Anti-Virus for Microsoft Exchange / Operations / Manual Scanning branch in F-Secure Policy manager Console.
2. Click **Start**.
3. Distribute the policy.

If you want to stop the manual scan in the middle of the scanning process, click **Stop** and distribute the policy.

General

Specify which messages you want to scan during the manual scan.

Scan Mailboxes	Specify mailboxes that are scanned for viruses. **Disabled** - Do not scan any mailboxes. **Scan All Mailboxes** - Scan all mailboxes. **Scan Only Included Mailboxes** - Scan mailboxes specified in the **Included Mailboxes** list. **Scan All Except Excluded Mailboxes** - Scan all mailboxes except those specified in the **Excluded Mailboxes** list.
Included Mailboxes	Specify mailboxes that are scanned for viruses when the **Scan Mailboxes** setting is set to **Scan Only Included Mailboxes**.
Excluded Mailboxes	Specify mailboxes that are not scanned when the **Scan Mailboxes** setting is set to **Scan All Except Excluded Mailboxes**.
Scan Public Folders	Specify public folders that are scanned for viruses. **Disabled** - Do not scan any public folders. **Scan All Folders** - Scan all public folders. **Scan Only Included Folders** - Scan public folders specified in the **Included Folders** list. **Scan All Except Excluded Folders** - Scan all public folders except those specified in the **Excluded Folders** list. **Important:** You need to specify the primary SMTP address for the account which is used to scan items in public folders on Microsoft Exchange 2010. The user account must have permissions to access and modify items in the public folders. For more information, see *Advanced*.

Included Folders

Specify public folders that are scanned for viruses when the **Scan Public Folders** setting is set to **Scan Only Included Folders**.

Excluded Folders

Specify public folders that are not scanned when the **Scan Public Folders** setting is set to **Scan All Except Excluded Folders**.

Incremental Scanning

Specify which messages are scanned for viruses during the manual scan.

All Messages - Scan all messages.

Only Recent Messages - Scan only messages that have not been scanned during the previous manual or scheduled scan.

Attachment Filtering

Specify attachments that are removed from messages during the manual scan.

Strip Attachments

Enable or disable the attachment stripping.

List of Attachments to Strip

Specify which attachments are stripped from messages. For more information, see *Lists and Templates*.

Use Exclusions

Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.

Quarantine Stripped Attachments

Specify whether stripped attachments are quarantined.

Do Not Quarantine These Attachments

Specify which files are not quarantined even when they are stripped. For more information, see *Lists and Templates*.

Replacement Text Template

Specify the template for the text that replaces the infected attachment when the stripped attachment is removed from the message. For more information, see *Lists and Templates*.

Virus Scanning

Specify messages and attachments that should be scanned for malicious code during the manual scan.

Scan Messages for Viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

List of Attachments to Scan

Specify attachments that are scanned for viruses. For more information, see *Lists and Templates*.

Use Exclusions

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scan.

Heuristic Scanning

Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

Note: Heuristic scanning may affect the product performance and increase the risk of false malware alarms.

Attempt to Disinfect Infected Attachments

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine Infected Attachments

Specify whether infected or suspicious attachments are quarantined.

Do Not Quarantine These Infections

Specify infections that are never placed in the quarantine. If a message is infected with a virus or worm which has a name that matches a keyword specified in this list, the message is not quarantined. For more information, see *Lists and Templates*.

Replacement Text Template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Lists and Templates*.

Archive Processing

Specify how the product processes archive files during the manual scan.

Scan Archives

Specify if files inside archives are scanned for viruses and other malicious code.

List of Files to Scan Inside Archives

Specify files that are scanned for viruses inside archives.

Use Exclusions

Specify files inside archives that are not scanned. Leave the list empty if you do not want to exclude any files from the scan.

Max Levels in Nested Archives

Specify how many levels deep to scan in nested archives, if **Scan Viruses Inside Archives** is enabled.

A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.

Specify the number of levels the product goes through before the action selected in **Action on Max Nested Archives** takes place. The default setting is 3.

Action on Max Nested Archives

Specify the action to take on nested archives with nesting levels exceeding the upper level specified in the **Max Levels in Nested Archives** setting.

Pass Through - Nested archives are scanned up to level specified in the **Max Levels in Nested Archives** setting. Exceeding nesting levels are not scanned, but the archive is not removed.

Drop Archive - Archives with exceeding nesting levels are removed.

Action on Password Protected Archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Leave the password protected archive in the message.

Drop archive - Remove the password protected archive from the message.

Detect Disallowed Files Inside Archives

Specify whether files inside compressed archive files are processed for disallowed content.

List of Disallowed Files to Detect inside Archives

Specify files which are not allowed inside archives. For more information, see *Lists and Templates*.

Action on Archives with Disallowed Files

Specify the action to take on archives which contain disallowed files.

Pass through - Leave the archive to the message.

Drop archive - Remove the archive from the message.

Quarantine Dropped Archives

Specify whether archives that are not delivered to recipients are placed in the quarantine. For more information, see *E-mail Quarantine Management*.

Grayware Scanning

Specify how the product processes grayware items during the manual scan.

Scan Messages for Grayware	Enable or disable the grayware scan.
Action on Grayware	Specify the action to take on items which contain grayware. **Report only** - Leave grayware items in the message and notify the administrator. **Drop attachment** - Remove grayware items from the message.
Grayware Exclusion List	Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan.
Quarantine Dropped Grayware	Specify whether grayware attachments are quarantined.
Do Not Quarantine This Grayware	Specify grayware that are never placed in the quarantine. For more information, see *Lists and Templates*.
Replacement Text Template	Specify the template for the text that replaces the grayware attachment when the grayware attachment is removed from the message. For more information, see *Lists and Templates*.

File Type Recognition

Select whether you want to use **Intelligent File Type Recognition** or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. Intelligent File Type Recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using Intelligent File Type Recognition strengthens the security, but can degrade the system performance.

Advanced

Configure how to handle nested messages and specify the administrator account to scan public folders.

Max Levels of Nested Messages	Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited. **Note:** It is not recommended to set the maximum nesting level to unlimited as this will make the product more vulnerable to DoS (Denial-of-Service) attacks.

Admin User Credentials

Specify the primary SMTP address for the account which is used to scan items in public folders. The user account must have permissions to access and modify in the public folders.

Important:

The setting is used on Microsoft Exchange 2010 platform only and affects manual, realtime, and scheduled storage scanning. If you do not specify any address, public folders in Exchange Store cannot be accessed or even listed.

4.5.3.3 Scheduled Scanning

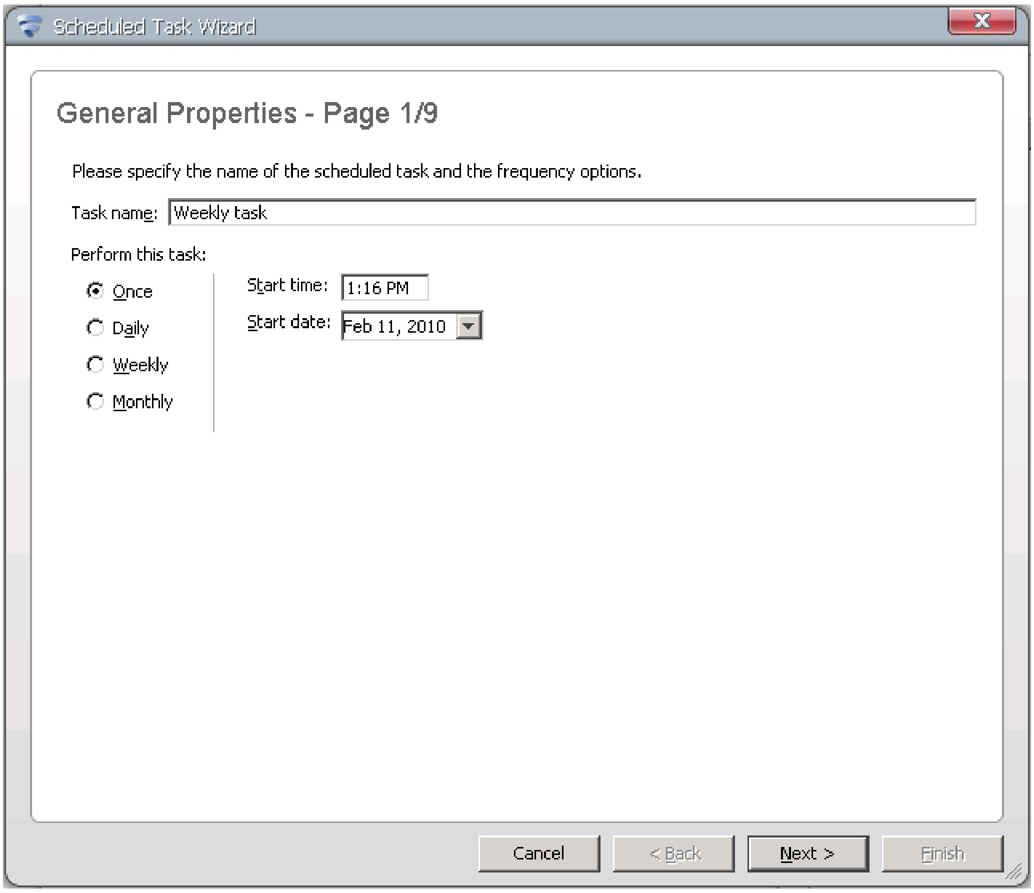
You can schedule scan tasks to scan mailboxes and public folders periodically. The scheduled scanning table displays all scheduled tasks and date and time when the next scheduled task occurs for the next time.

- To deactivate scheduled tasks in the list, clear the **Active** checkbox in front of the task. Check the checkbox to make it active again.
- Click **Add** to add a new scheduled task to the list.
- To duplicate a task, select it from the list and click **Copy**.
- To edit a previously created task, click **Edit**.
- To remove the selected task from the list, click **Clear Row**.
- Click **Clear Table** to remove all tasks from the list.
- **Force Row** enforces the current scheduled task to be active in all subdomains and hosts. **Force Table** enforces all current scheduled tasks to be active in all subdomains and hosts.

4.5.3.3.1 Creating Scheduled Task

Start the **Scheduled Task Wizard** by clicking **Add**.

General Properties



Scheduled Task Wizard

General Properties - Page 1/9

Please specify the name of the scheduled task and the frequency options.

Task name: Weekly task

Perform this task:

- ● Once
- ○ Daily
- ○ Weekly
- ○ Monthly

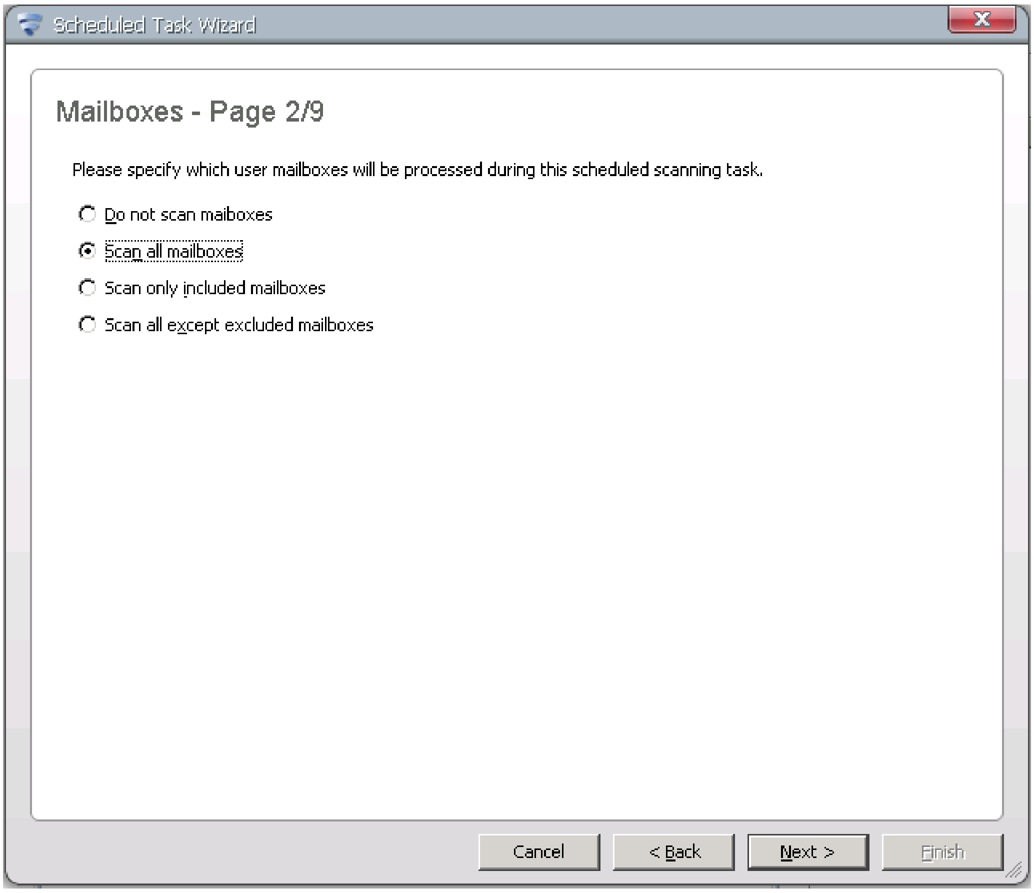
Start time: 1:16 PM

Start date: Feb 11, 2010

Enter the name for the new task and select how frequently you want the operation to be performed.

Task name	Specify the name of the scheduled operation. **Note:** Do not use any special characters in the task name.
Perform this task	Specify how frequently you want the operation to be performed. **Once** - Only once at the specified time. **Daily** - Every day at the specified time, starting from the specified date. **Weekly** - Every week at the specified time on the same day when the first operation is scheduled to start. **Monthly** - Every month at the specified time on the same date when the first operation is scheduled to start.
Start time	Enter the start time of the task in hh:mm format.
Start date	Enter the start date of the task in mm/dd/yyyy format

Mailboxes



Mailboxes - Page 2/9

Please specify which user mailboxes will be processed during this scheduled scanning task.

○ Do not scan maiboxes

● Scan all mailboxes

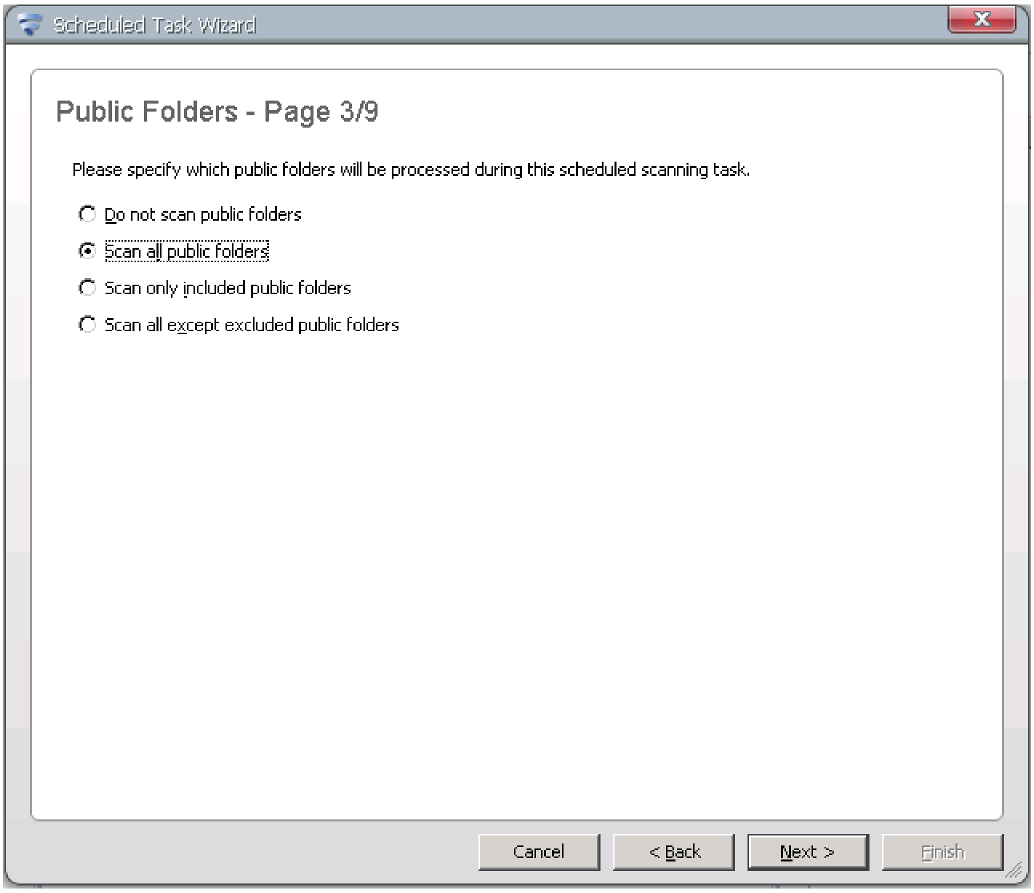
○ Scan only included mailboxes

○ Scan all except excluded mailboxes

Choose which mailboxes are processed during the scheduled operation.

Mailboxes	Specify mailboxes that are processed during the scheduled scan. **Do not scan mailboxes** - Disable the mailbox scanning. **Scan all mailboxes** - Scan all mailboxes. **Scan only included mailboxes** - Scan all specified mailboxes. Click **Add** or **Remove** to edit mailboxes that are scanned. **Scan all except excluded mailboxes** - Do not scan specified mailboxes but scan all other. Click **Add** or **Remove** to edit mailboxes that are not scanned. The format to enter the included or excluded mailbox is the username, for example: `user1`

Public Folders



Public Folders - Page 3/9

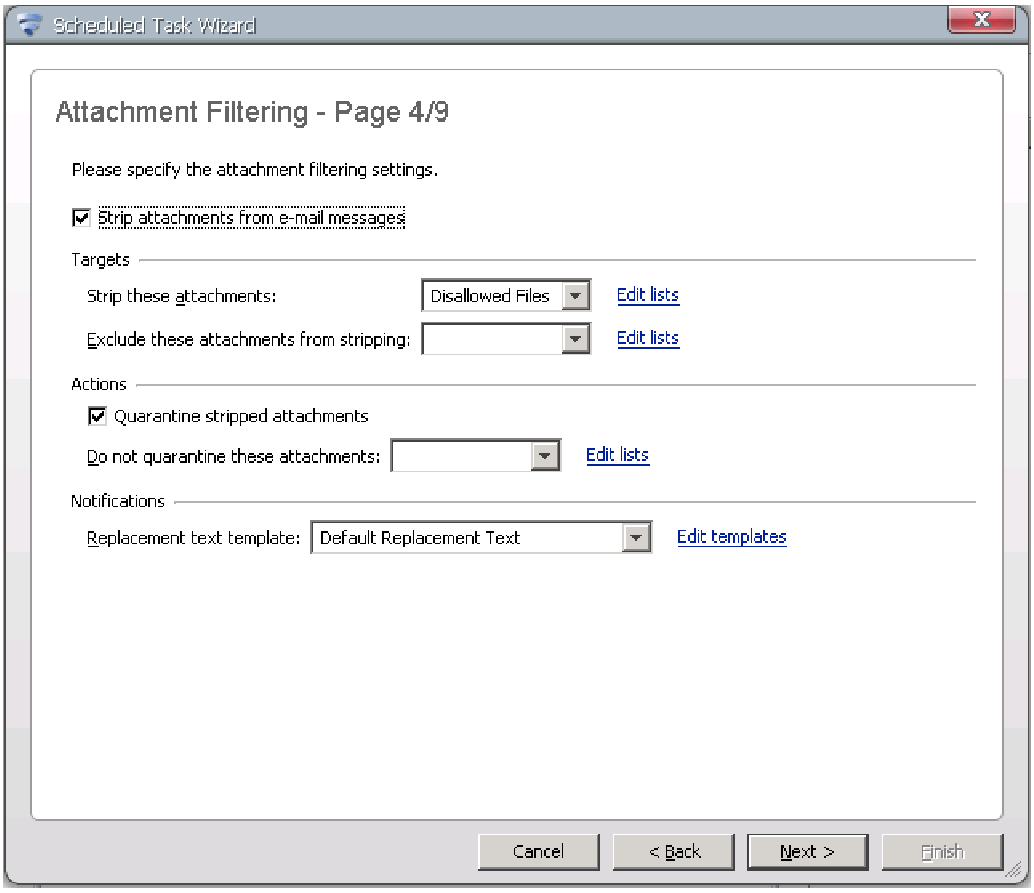
Please specify which public folders will be processed during this scheduled scanning task.

○ Do not scan public folders
● Scan all public folders
○ Scan only included public folders
○ Scan all except excluded public folders

Choose which public folders are processed during the scheduled operation.

Public folders	Specify public folders that are processed during the scheduled scan. **Do not scan public folders** - Disable the public folder scanning. **Scan all public folders** - Scan all public folders. **Scan only included public folders** - Scan all specified public folders. Click **Add** or **Remove** to edit public folders that are scanned. **Scan all except excluded public folders** - Do not scan specified public folders but scan all other. Click **Add** or **Remove** to edit public folders that are not scanned. The format to enter the included or excluded mailbox is the name of the public folder. **Important:** You need to specify the primary SMTP address for the account which is used to scan items in public folders on Microsoft Exchange 2010. The user account must have permissions to access and modify items in the public folders. For more information, see *Advanced*.

Attachment Filtering



Scheduled Task Wizard

Attachment Filtering - Page 4/9

Please specify the attachment filtering settings.

☑ Strip attachments from e-mail messages

Targets

Strip these attachments: Disallowed Files — Edit lists

Exclude these attachments from stripping: — Edit lists

Actions

☑ Quarantine stripped attachments

Do not quarantine these attachments: — Edit lists

Notifications

Replacement text template: Default Replacement Text — Edit templates

Choose settings for stripping attachments during the scheduled operation.

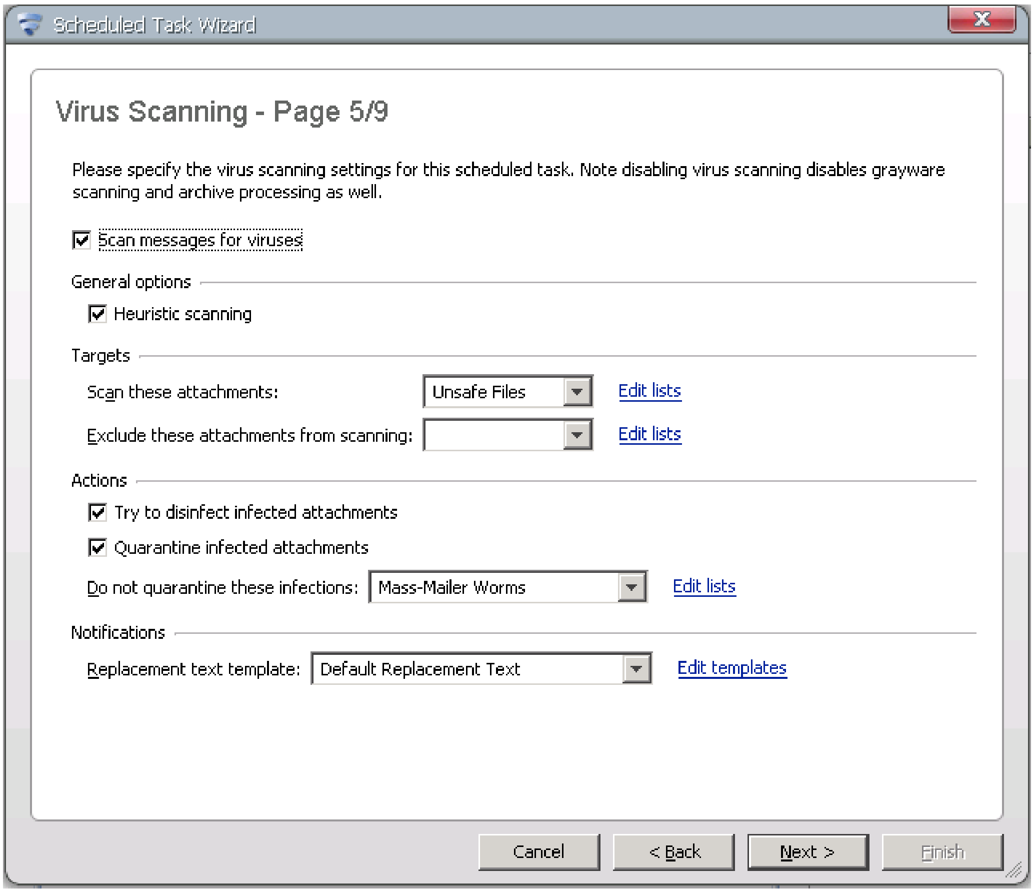
Strip attachments from e-mail messages	Enable or disable the attachment stripping.
Targets	
Strip these attachments	Specify which attachments are stripped from messages. For more information, see *Lists and Templates*.
Exclude these attachments from stripping	Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.
Actions	
Quarantine stripped attachments	Specify whether stripped attachments are quarantined.
Do not quarantine these attachments	Specify file names and file extensions which are not quarantined even when they are stripped. For more information, see *Lists and Templates*.

Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the stripped attachment is removed from the message. For more information, see *Lists and Templates*.

Virus Scanning



Virus Scanning - Page 5/9

Please specify the virus scanning settings for this scheduled task. Note disabling virus scanning disables grayware scanning and archive processing as well.

☑ Scan messages for viruses

General options

☑ Heuristic scanning

Targets

Scan these attachments: Unsafe Files — Edit lists

Exclude these attachments from scanning: — Edit lists

Actions

☑ Try to disinfect infected attachments

☑ Quarantine infected attachments

Do not quarantine these infections: Mass-Mailer Worms — Edit lists

Notifications

Replacement text template: Default Replacement Text — Edit templates

Choose settings for virus scanning during the scheduled operation.

Scan messages for viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

General Options

Heuristic Scanning

Enable or disable the heuristic scanning. The heuristic scanning analyzes files for suspicious code behavior so that the product can detect unknown malware.

Note: Heuristic scanning may affect the product performance and increase the risk of false malware alarms.

Targets

Scan these attachments

Specify attachments that are scanned for viruses. For more information, see *Lists and Templates*.

Exclude these attachments from scanning

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scanning.

Actions

Try to disinfect infected attachments

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine infected attachments

Specify whether infected or suspicious messages are quarantined.

Do not quarantine these infections

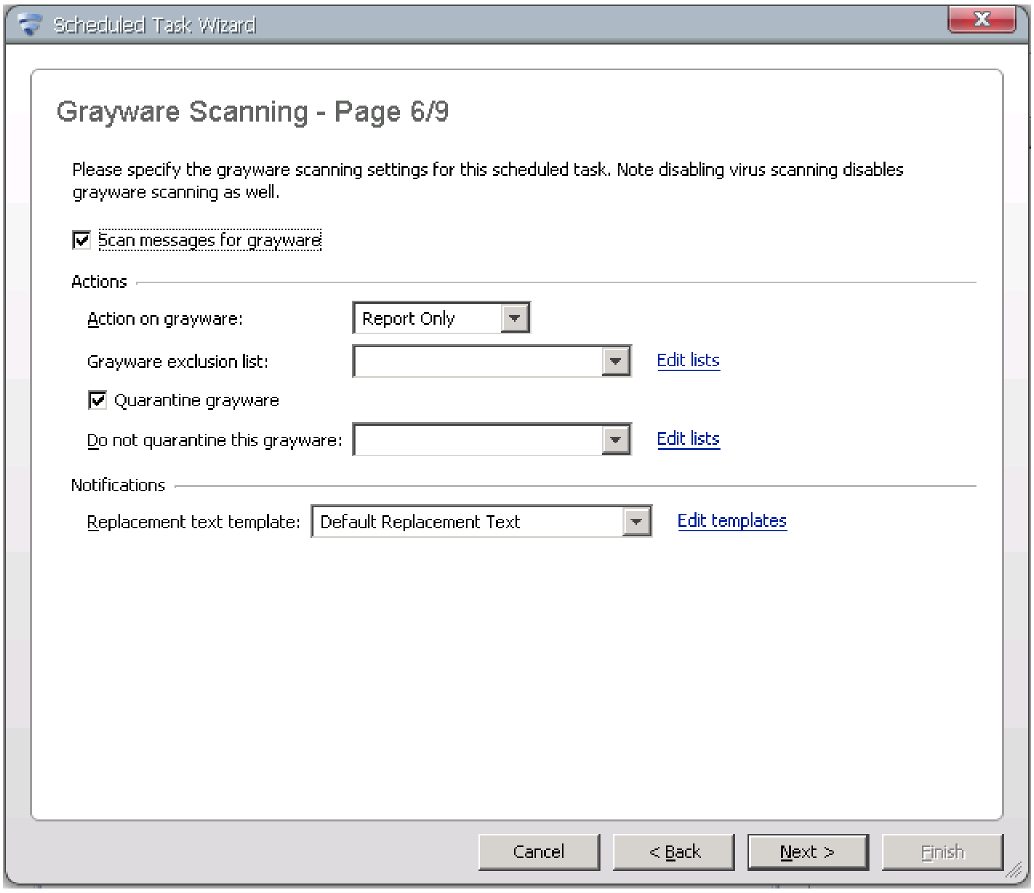
Specify infections that are never placed in the quarantine. For more information, see *Lists and Templates*.

Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Lists and Templates*.

Grayware Scanning



Grayware Scanning - Page 6/9

Please specify the grayware scanning settings for this scheduled task. Note disabling virus scanning disables grayware scanning as well.

☑ Scan messages for grayware

Actions

Action on grayware: Report Only

Grayware exclusion list:

☑ Quarantine grayware

Do not quarantine this grayware:

Notifications

Replacement text template: Default Replacement Text

Choose settings for grayware scanning during the scheduled operation.

Scan messages for grayware	Enable or disable the grayware scan.
Actions	
Action on grayware	Specify the action to take on items which contain grayware. **Report only** - Leave grayware items in the message and notify the administrator. **Drop attachment** - Remove grayware items from the message.
Grayware exclusion list	Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan. For more information, see *Lists and Templates*.
Quarantine grayware	Specify whether grayware attachments are quarantined.

Do not quarantine this grayware

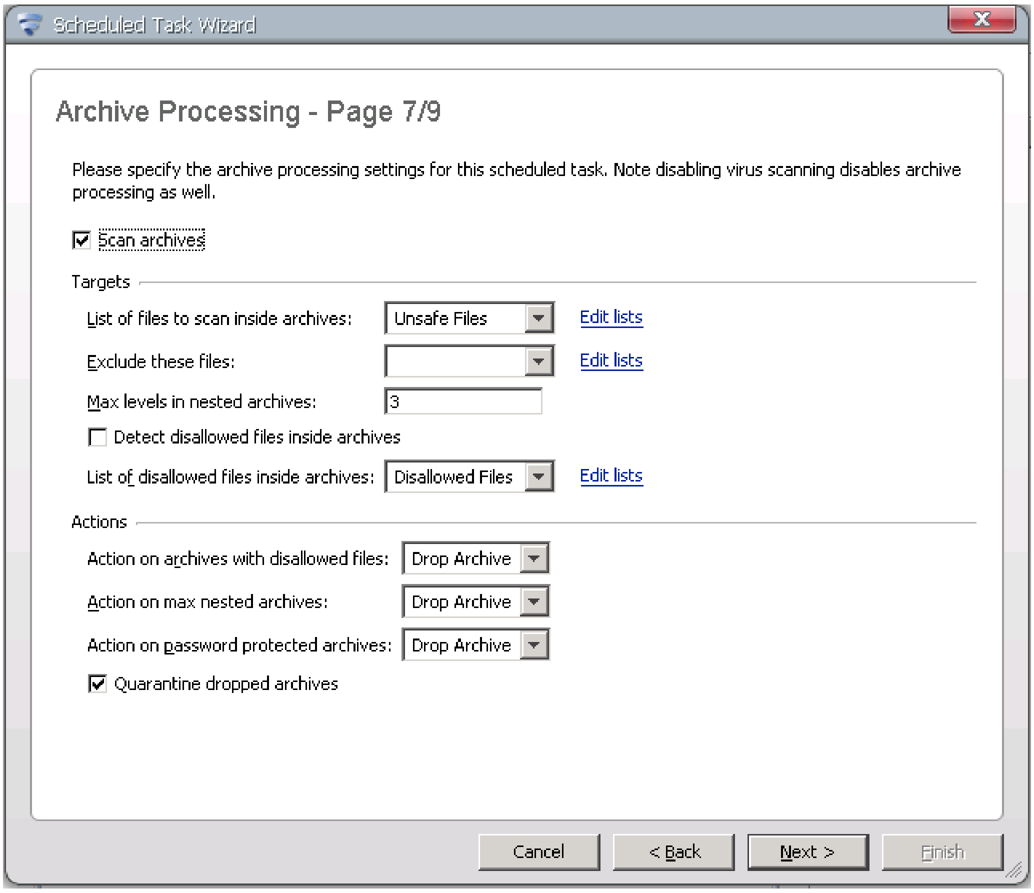
Specify grayware that are never placed in the quarantine. For more information, see *Lists and Templates*.

Notifications

Replacement text template

Specify the template for the text that replaces the grayware item when it is removed from the message. For more information, see *Lists and Templates*.

Archive Processing



Archive Processing - Page 7/9

Please specify the archive processing settings for this scheduled task. Note disabling virus scanning disables archive processing as well.

☑ Scan archives

Targets

List of files to scan inside archives: Unsafe Files — Edit lists

Exclude these files: — Edit lists

Max levels in nested archives: 3

☐ Detect disallowed files inside archives

List of disallowed files inside archives: Disallowed Files — Edit lists

Actions

Action on archives with disallowed files: Drop Archive

Action on max nested archives: Drop Archive

Action on password protected archives: Drop Archive

☑ Quarantine dropped archives

Choose settings for stripping attachments during the scheduled operation.

Scan archives

Specify if files inside archives are scanned for viruses and other malicious code.

Targets

List of files to scan inside archives

Specify files inside archives that are scanned for viruses. For more information, see *Lists and Templates*.

Exclude these files

Specify files that are not scanned inside archives. Leave the list empty if you do not want to exclude any files from the scanning.

Max levels in nesting archives

Specify how many levels of archives inside other archives the product scans when **Scan Viruses Inside Archives** is enabled.

Detect disallowed files inside archives

Specify whether files inside compressed archive files are processed for disallowed content.

Note: Disallowed content is not processed when the archive scanning is disabled.

Actions

Action on archives with disallowed files

Specify the action to take on archives which contain disallowed files.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without the archive.

Action on max nested archives

Specify the action to take on archives with nesting levels exceeding the upper level specified in the **Max Levels in Nested Archives** setting.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without it.

Action on password protected archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

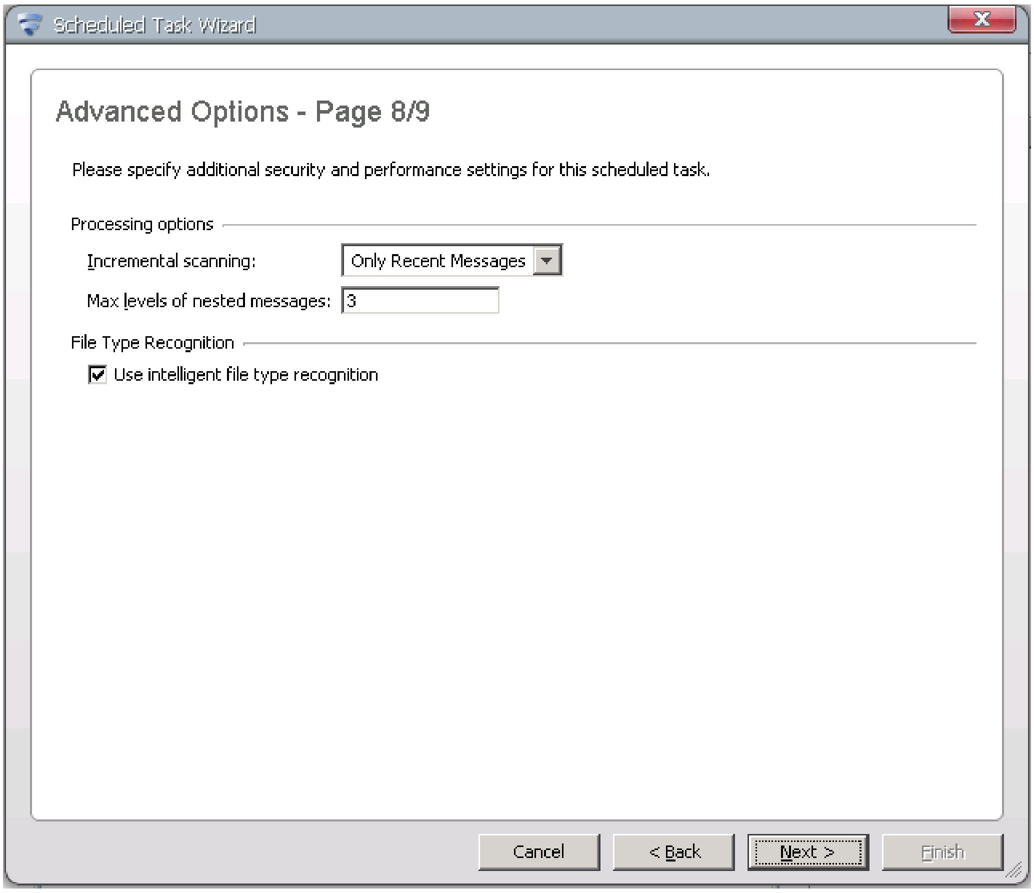
Pass through - Deliver the message with the password protected archive to the recipient.

Drop archive - Remove the password protected archive from the message and deliver the message to the recipient without it.

Quarantine dropped archives

Specify whether archives that are not delivered to recipients are placed in the quarantine. For more information, see *E-mail Quarantine Management*.

Processing Options



Scheduled Task Wizard

Advanced Options - Page 8/9

Please specify additional security and performance settings for this scheduled task.

Processing options

Incremental scanning: Only Recent Messages

Max levels of nested messages: 3

File Type Recognition

☑ Use intelligent file type recognition

Choose advanced processing options for all the messages processed during the scheduled operation.

Processing options

Incremental scanning

Specify whether you want to process all messages or only those messages that have not been processed previously during the manual or scheduled processing.

Max levels of nested messages

Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.

Note: It is not recommended to set the maximum nesting level to unlimited as this will make the product more vulnerable to DoS (Denial-of-Service) attacks.

File type recognition

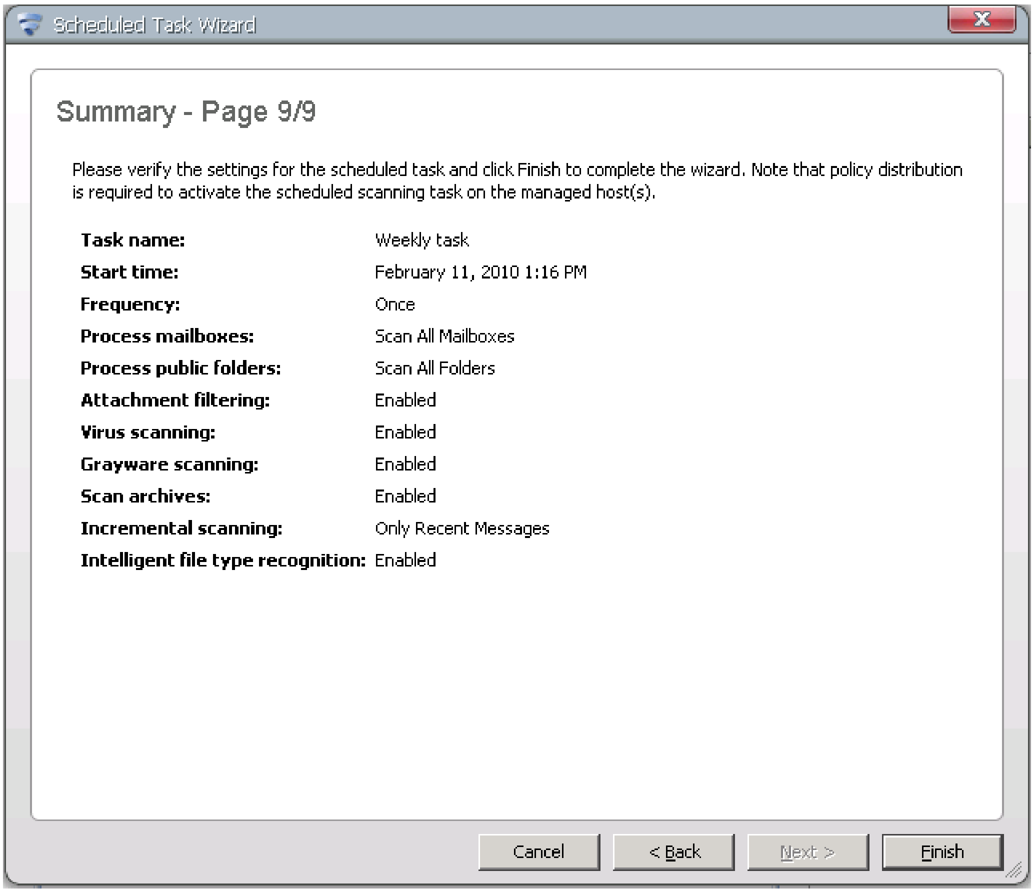
Use intelligent file type recognition

Select whether you want to use Intelligent File Type Recognition or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. Intelligent File Type Recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using Intelligent File Type Recognition strengthens the security, but can degrade the system performance.

Summary



Summary - Page 9/9

Please verify the settings for the scheduled task and click Finish to complete the wizard. Note that policy distribution is required to activate the scheduled scanning task on the managed host(s).

Task name:	Weekly task
Start time:	February 11, 2010 1:16 PM
Frequency:	Once
Process mailboxes:	Scan All Mailboxes
Process public folders:	Scan All Folders
Attachment filtering:	Enabled
Virus scanning:	Enabled
Grayware scanning:	Enabled
Scan archives:	Enabled
Incremental scanning:	Only Recent Messages
Intelligent file type recognition:	Enabled

The **Scheduled Task Wizard** displays the summary of created operation. Click **Finish** to accept the new scheduled operation and to exit the wizard.

4.6 F-Secure Anti-Virus for Microsoft Exchange Statistics

To view Anti-Virus for Microsoft Exchange statistics, open the **Status** tab from the **Properties** pane, select **F-Secure Anti-Virus for Microsoft Exchange** and open the **Statistics** subtree. It displays statistics for the host for each product installation. If a policy domain is selected, the **Status** view displays the number of hosts in the domain and which hosts are disconnected from F-Secure Policy Manager.

Resetting Statistics

You can reset statistics by using controls under the **F-Secure Anti-Virus for Microsoft Exchange / Operations** branch in the **Policy** view.

To reset transport scanning statistics, follow these instructions:

1. Go to the **Anti-Virus for Microsoft Exchange / Operations / Reset Transport Statistics / Statistics to Reset** branch.
2. Set statistics you want to reset to **Yes**.
3. Go to the **Anti-Virus for Microsoft Exchange / Operations / Reset Transport Statistics / Reset** branch.
4. Click **Start** in the Editor pane and distribute the policy.

To reset storage scanning statistics, follow these instructions:

1. Go to the **Anti-Virus for Microsoft Exchange / Operations / Reset Storage Statistics / Statistics to Reset** branch.
2. Set **Real-Time Scanning** to **Yes**.
3. Go to the **Anti-Virus for Microsoft Exchange / Operations / Reset Storage Statistics / Reset** branch.
4. Click **Start** in the Editor pane and distribute the policy.

The Status above the button displays "**Operation still in progress**" until the program reports that statistics have been reset.

4.6.1 Common

Version	Displays the version number of the product.
Previous Reset of Statistics	Displays the last date and time when the statistics were reset.
MIB Version	Displays the MIB version number.
Installation Directory	Displays the complete path where the product is installed.
Build	Displays the installed build number of the product.
Common	Displays the product name and lists all installed hotfixes.
Status	Displays whether the product is running (started), stopped, or whether the current status of the agent is unknown.

4.6.2 Transport Protection

You can view the inbound, outbound and internal message statistics separately.

Previous Reset of Statistics	Displays the date and time of the last reset of statistics.
Number of Processed Messages	Displays the total number of processed messages since the last reset of statistics.

Number of Infected Messages	Displays the number of messages with attachments that are infected and cannot be automatically disinfected.
Number of High & Medium Virus Risk Messages	Displays the number of messages that have been identified as unsafe; messages that contain patterns that can be assumed to be a part of a virus outbreak.
Number of Grayware Messages	Displays the number of messages that have been found to contain grayware.
Number of Suspicious Messages	Displays the number of suspicious content found, for example password-protected archives, nested archives and malformed messages.
Number of Stripped Attachments	Displays the number of filtered attachments.
Number of Filtered Messages	Displays the number of messages that have been found to contain disallowed keywords in the message subject or text.
Number of Spam Messages	Displays the number of messages that are classified as spam.
Last Infection Found	Displays the name of the last infection found.
Last Time Infection Found	Displays the time when the last infection was found.

4.6.3 Storage Protection

Common

Number of Mailboxes	Displays the number of currently protected user mailboxes.
Number of Public Folders	Displays the number of currently protected public folders.

Real-time and Background Scanning

Previous Reset of Statistics	Displays the date and time of the last reset of statistics.
Number of Processed Items	Displays the total number of processed items since the last reset of statistics.

Number of Infected Items	Displays the number of items that are infected and cannot be automatically disinfected.
Number of Grayware Items	Displays the number of items that have been found to contain grayware.
Number of Suspicious Items	Displays the number of suspicious content found, for example password-protected archives and nested archives.
Number of Stripped Attachments	Displays the number of attachments stripped during the real-time scan.
Last Infection Found	Displays the name of the last infection found.
Last Time Infection Found	Displays the time when the last infection was found.

Manual Scanning

Total Number of Mailboxes	Displays the total number of mailboxes in Exchange Store that the product processes during the manual scan.
Number of Processed Mailboxes	Displays the number of mailboxes that have been processed.
Total Number of Public Folders	Displays the total number of Public folders in the Exchange Store that the product processes during the manual scan.
Number of Processed Public Folders	Displays the number of public folders that have been processed.
Estimated Time Left	Displays the estimated time left to finish the current manual scan.
Elapsed Time	Displays the time that has elapsed since the manual scan was started.
Number of Processed Items	Displays the total number of processed items during the previous manual scan.
Number of Infected Items	Displays the number of items that were infected and could not be automatically disinfected during the previous manual scan.

Number of Grayware Items

Displays the number of items that have been found to contain grayware.

Number of Suspicious Items

Displays the number of suspicious content found during the previous manual scan, for example password-protected archives and nested archives.

Number of Stripped Attachments

Displays the number of filtered attachments during the previous manual scan.

Last Infection Found

Displays the name of the last infection found.

Last Time Infection Found

Displays the time when the last infection was found.

Previous Scanning

Displays the date and time of the previous manual scan.

4.6.4 Quarantine

The quarantine statistics display the total number of quarantined items, the current size of the mail quarantine storage (in megabytes), and the detailed statistics of quarantined items by category. For more information, see *E-mail Quarantine Management*.

4.7 F-Secure Anti-Virus for Microsoft SharePoint Settings

4.7.1 Real-time Protection

You can configure settings for downloaded (when they are opened from SharePoint) and uploaded (when they are saved to SharePoint) documents separetely.

4.7.1.1 Virus Scanning

Specify how the product processes viruses.

Enabled

When virus scanning is enabled, the product scans documents when they are opened (downloaded) from the SharePoint server or saved (uploaded) to the SharePoint server.

Heuristic scanning

Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

List of documents to scan

Specify documents that are scanned for viruses.

List of documents to exclude

Specify the list of documents that should not be scanned for viruses.

Notify administrator

Specify whether the administrator is notified when the product finds a virus and the alert level of the notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

4.7.1.2 Archive Processing

Specify how the product processes viruses inside archives.

Enabled

When archive processing is enabled, the product scans for viruses and other malicious code inside archives.

List of files to scan inside archives

Specify files that are scanned for viruses inside archives.

List of files to exclude from scan inside archives

Specify files inside archives that are not scanned. Leave the list empty if you do not want to exclude any files from the scan.

Max levels in nested archives

Specify how many levels deep to scan in nested archives, if archive processing is enabled.

A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.

Specify the number of levels the product goes through before the action selected in **Action on Max Nested Archives** takes place.

Action on max nested archives

Specify the action to take on nested archives with nesting levels exceeding the upper level specified in the **Max Levels in Nested Archives** setting.

Pass Through - Nested archives are scanned up to level specified in the **Max Levels in Nested Archives** setting. Exceeding nesting levels are not scanned, but the archive is not removed.

Block Archive - Archives with exceeding nesting levels are removed.

Action on password protected archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Leave the password protected archive in the message.

Block archive - Remove the password protected archive from the message.

Notify administrator

Specify whether the administrator is notified when the product detects a virus in an archive and the alert level of the notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

4.7.1.3 Grayware Scanning

Specify how the product processes grayware items.

Enabled

When grayware scanning is enabled, the product scans for grayware (adware, spyware, riskware and similar).

Note: Grayware scanning is disabled if virus scanning is disabled.

Action on grayware

Specify the action to take on items which contain grayware.

Pass through - Let users access grayware items.

Block document - Prevent users from accessing grayware items.

Notify administrator

Specify whether the administrator is notified when the product detects grayware and the alert level of the notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. The Alert Forwarding table can be found in: F-Secure Management Agent/Settings/Alerting.

4.7.2 Advanced

4.7.2.1 Content Scanner Server

Specify how F-Secure Anti-Virus for Microsoft SharePoint communicates with F-Secure Content Scanner Server.

Number of concurrent transactions

Specify the maximum number of transactions the server processes simultaneously.

Connection timeout

Specify (in seconds) how long to wait for a response from F-Secure Content Scanner Server.

Working directory

Specify where temporary files are stored. The Working directory should be on a local hard disk for the best performance. Make sure that there is enough free disk space for temporary files.

Note: This setting must be defined as Final with the Restriction Editor before the policies are distributed. Otherwise the setting will not be changed in the product.

Error handling on download

Specify how to handle error when scanning downloaded documents.

Allow - treat the document as clean;

Block - return an error to SharePoint.

Error handling on upload

Specify how to handle error when scanning uploaded documents.

Allow - treat the document as clean;

Block - return an error to SharePoint.

4.7.2.2 SharePoint

Specify how SharePoint should handle infected files.

Set **Allow download infected file** to **Warn** to display a warning about the infected file, but allow users to download them. Set it to **Block** to prevent users from downloading infected files.

4.7.2.3 Lists and Templates

Specify lists and templatest that are used with F-Secure Anti-Virus for Microsoft SharePoint. For more information, see *Lists and Templates*.

4.8 F-Secure Anti-Virus for Microsoft SharePoint Statistics

Version

Displays the version number of the product.

Previous reset of statistics

Displays the last date and time when the statistics were reset.

MIB version

Displays the MIB version number.

Installation directory

Displays the complete path where the product is installed.

Build

Displays the installed build number of the product.

Common

Displays information on installed hotfixes of the product.

Real-time protection

Real-time protection statistics are divided between downloaded and uploaded documents.

Scanned documents	Displays the total number of scanned documents.
Infected documents	Displays the number of documents that contain viruses.
Grayware documents	Displays the number of documents that contain grayware.
Suspicious documents	Displays the number of documents with suspicious content.
Failed scan requests	Displays the number of documents that could not be scanned.
Latest infection found	Displays the name of the last virus found.
Latest time infection found	Displays the time when the last virus was found.

4.9 F-Secure Software Updater Settings

Software Updater scans and reports missing updates for third-party software and deploys security updates.

Software Updater scans for Microsoft updates for the operating system and Microsoft applications, in addition to a comprehensive list of third-party applications, such as Adobe Flash, Java, OpenOffice, archive managers, media players, image viewers and so on.

Software Updater periodically checks information about software updates, compares these to software that you have installed and identifiews missing updates.

It is important to have the latest software updates installed, because many updates fix security vulnerabilities in installed products.

4.9.1 Automatic Installation

Turn on **Enable Software Updater** to install security updates automatically.

Install security updates automatically	Specify which security updates are installed automatically based on their importance. **Note:** Service packs are not installed automatically, only security updates.
Install every	Specify the day of the week when to install updates automatically, or **Every day** to install updates every day.
Install at	Specify the time of day when the automatic installation starts.

Restart after installation

Specify how to handle cases where the update requires users to restart their computer.

Ask user - users can choose when to restart the computer and they can postpone it for a while.

Force restart - the computer is restarted automatically if the update requires it.

Force restart in

Specify how long users can postpone the system restart before the computer restarts automatically.

Notify about installation

Show a flyer to users when updates are installed automatically.

Exclude software from automatic installation

Specify the name of any software that you do not want to update automatically.

Allow unsigned updates automatic installation

Some vendors do not sign their software updates. Specify whether these unsigned updates should be installed automatically.

Important: Allowing unsigned updates may decrease the level of protection. This setting applies to all updates, including any newly detected products.

4.9.2 Automatic Scanning

You can specify how often to scan for new updates. Set **Maximum rescanning period** on how often you want to scan for the latest updates.

Scanning on system startup

Scan on system startup

Turn on to scan for new updates on the system startup.

Delay

Some delay after the system startup balances computer activities and the automatic scan starts when the other system initialization tasks are ready.

Specify the delay after the system startup before starting the scan.

Randomization interval

Specify the time interval when the scan starts after the system startup. The scan starts at a random time within the interval.

Randomization interval balances upstream traffic to the server in the environments where many client computers start simulteneously.

Exclude update types from scanning

You can exclude certain applications from the automatic scanning.

Exclude security tools	Exclude security tools from scanning.
Exclude non-security updates	Exclude non-security updates from scanning.
Exclude service packs	Exclude service packs from scanning.

4.9.3 Troubleshooting

Cancel hanging installation in	Specify how long installing an update can take.
Retry hanging installation	Specify when to try to install the update again if it did no succeeed.

4.9.4 Installation Log

Specify which entries should be removed from the Installation log table.

4.9.5 Communications

Specify internet connection settings for downloading third-party software and data.

Use HTTP Proxy	Choose one of the following settings: **No** - use a direct or transparent connection to the Internet. **From AUA configuration** - use the Automatic Update Agent settings. **User-defined** - specify a proxy URL.
User-defined proxy	Specify the HTTP proxy address in the following format: `http://[user[:password]@]host:port`. For example: • http://example.com • http://example.com:8080 • http://username@example.com • http://username:password@example.com

4.10 F-Secure Software Updater Statistics

Version	Displays the version number of the product.
MIB version	Displays the MIB version number.
Installation directory	Displays the complete path where the product is installed.

Build	Displays the installed build number of the product.
Software Updater enabled	Displays the current status of Software Updater

Common

Displays information on installed hotfixes of the product.

Scanning results

Latest scanning time	Displays the latest date and time when the computer scanned for missing software updates.
Critical security updates count	Displays the number of critical security updates that are missing.
Important security updates count	Displays the number of important security updates that are missing.
Other security updates count	Displays the number of other (not critical and not important) security updates that are missing.

Installation

Latest installation time	Displays the latest date and time when the computer installed software updates.
Restart computer needed	Displays whether the computer needs to be restarted to finish the installation.

4.11 F-Secure Content Scanner Server Settings

Content Scanner Server hosts all scanning engines that the product uses to scan e-mail content that the F-Secure Anti-Virus for Microsoft Exchange component provides. Use these settings to change the general e-mail scanning options.

Important:

The Content Scanner Server settings do not affect engines that the F-Secure Anti-Virus component uses when scanning files.

4.11.1 Interface

Specify how the server will interact with clients.

IP Address	Specifies the service listen address in case of multiple network interface cards or multiple IP addresses. If you do not assign an IP address (0.0.0.0), the server responds to all IP addresses assigned to the host.

TCP Port

Specifies the TCP port that the server listens for incoming requests. The default port number is 18971. If you change this port number, you must modify the connection settings of the client accordingly, so that the client sends requests to the same port.

Accept Connections

Specifies a comma-separated list of IP addresses the server accepts incoming requests from. If the list is empty, the server accepts connections from any host.

Max Connections

Specifies the maximum number of simultaneous connections the server can accept. Value zero (0) means no limit.

Max Connections Per Host

Specifies the maximum number of simultaneous connections the server can accept from a particular host. Value zero (0) means no limit.

Send Content Timeout

Specifies how long the server should wait before it timeouts on sending data to the client.

Receive Content Timeout

Specifies how long the server should wait before it timeouts when receiving data from the client.

Keep Alive Timeout

Specifies the length of time before the server closes an inactive/idle connection. This ensures that all connections are closed if the protocol fails to close a connection.

4.11.2 Virus Scanning

Specify scanning engines to be used when F-Secure Content Scanner Server scans files for viruses, and the files that should be scanned.

Scan Engines

Scan engines can be **enabled** or **disabled**. If you want to disable the scan just for certain files, enter the appropriate file extensions to **Excluded extensions** field and separate each extension with a space. The **Excluded extensions** field supports * and ? wildcards.

Action if Engine Malfunctions

Specify how the product reacts if it cannot scan a file.

Return Scan Error - Drop the file being scanned and send a scan error.

Scan with Other Engines - Scan the file with other available scan engines.

Scan Inside Archives

Specify whether files inside compressed archive files should be scanned for viruses, if they are not excluded from scanning.

Scanning inside archives takes time. Disabling scanning inside archives improves performance, but it also means that the network users need to use up-to-date virus protection on their workstations.

Max Levels in Nested Archives

If **Scan Inside Archives** is enabled, F-Secure Content Scanner Server can scan files inside archives that may exist inside of other archives. Furthermore, these nested archives can contain other archives.

Specify the number of levels F-Secure Content Scanner Server goes through before the action selected in **Suspect Max Nested Archives** takes place. The default setting is 3.

Increasing the value increases the load on the system and thus decreases the overall system performance. This means that the system becomes more vulnerable for DoS (Denial-of-Service) attacks.

Suspect Max Nested Archives

If the amount of nested archives exceeds the value specified in the **Max Levels in Nested Archives**, the file is stopped if **Treat as Unsafe** is selected. If **Treat as Safe** is selected, the archive file is sent to the user.

Suspect Password Protected Archives

Compressed archive files can be protected with passwords. These archives can be opened only with a valid password, so F-Secure Content Scanner Server cannot scan their content. Password protected archives can be stopped by selecting **Treat as Unsafe**. If **Treat as Safe** is selected, password protected archives are delivered to recipient.

Acceptable Unpacked Size Threshold

Specify the acceptable unpacked size (in kilobytes) for archive files. If the unpacked size of an archive file exceeds this threshold, the server will consider the archive suspicious and corresponding action will be taken.

Scan Extensions Inside Archives

Enter all the extensions you want to scan inside archives.

Extensions Allowed in Password Protected Archives

Define a space-separated list of the file extensions allowed in password protected archives. Wildcards (*, ?) can be used. Example: "DO? *ML".

Max Scan Timeout	Specify the maximum time that one scanning task can last. The **Max Scan Timeout** is 10 minutes by default.

4.11.3 Virus Statistics

Select the number of most active viruses and the number of days to be displayed on the Top 10 virus list.

Time Period	Specify the time period for the most active viruses list. The product shows statistics about most active viruses detected during the specified time period. The possible value range is from 1 hour to 90 days.
Viruses to Show	Specify the number of most active viruses to be displayed for the time period specified in the '**Time Period** ' setting. The possible values are **Top 5**. **Top 10** and **Top 30**.
Mail Server Address	Specify the IP address of the mail server that is used to send e-mail.
Mail Server Port	Specify the port number of the mail server that is used to send e-mail.
E-mail Addresses for Unencrypted Reports	Specify e-mail addresses where you want to send unencrypted virus statistics reports. Separate each address with a comma or space.

4.11.4 Database Updates

Specify how you want to keep the virus definition databases up-to-date.

Verify Integrity of Downloaded Databases	Specify whether the product should verify that the downloaded virus definition databases are the original databases published by F-Secure Corporation and that they have not been altered or corrupted in any way before taking them to use.
Notify When Databases Become Old	Specify whether F-Secure Content Scanner Server should notify the administrator if virus definition databases have not been updated recently.
Notify When Databases Older Than	Specify the time (in days) how old virus definition databases can be before F-Secure Content Scanner Server sends the notification to the administrator.

4.11.5 Proxy Configuration

Specify proxy server parameters that Content Scanner Server uses when it connects to the threat detection center.

Use Proxy Server

Specify whether F-Secure Content Scanner Server uses a proxy server when it connects to the threat detection center.

Proxy Server Address

Specify the address of the proxy server.

Proxy Server Port

Specify the port number of the proxy server.

4.11.6 Advanced

Specify the location and the minimum size of the Working directory.

Working Directory

Specify where temporary files are stored. The Working directory should be on a local hard disk for the best performance. Make sure that there is enough free disk space for temporary files.

Important:

This setting must be defined as Final with the Restriction Editor before the policies are distributed. Otherwise the setting will not be changed in the product.

Note: During the setup, access rights are adjusted so that only the operating system and the local administrator can access files in the Working directory. If you make changes to Working Directory settings, make sure that the new directory has the same rights.

Working Directory Clean Interval

Specify the time after which the inactive temporary files in the Working directory are deleted. The default clean interval is 30 minutes.

Free Space Threshold

Specify when F-Secure Content Scanner Server should send a low disk space alert to the administrator. The default setting is 100 megabytes.

Max Number of Concurrent Transactions

Specify the maximum number of transactions the server processes simultaneously.

4.12 F-Secure Content Scanner Server Statistics

The **Statistics** branch in the F-Secure Content Scanner Server tree displays the version of F-Secure Content Scanner Server that is currently installed on the selected host and the location of F-Secure Content Scanner Server installation directory.

4.12.1 Server

The**Server** branch contains the following information:

Version	The version of the F-Secure Content Scanner Server.
Status	The status of F-Secure Content Scanner Server, whether it has been started and it is running or it is stopped.
Start Time	The date and time when the server was started.
Previous Reset of Statistics	The date and time of the last reset of statistics.
Number of Scanned Files	The number of files that have been scanned.
Last Database Update	The last date and time when virus definition database was updated.
Database Update Version	The currently used version of the database update. The version is shown in YYYY-MM-DD_NN format, where YYYY-MM-DD is the release date of the update and NN is the number of the update for that day.
Last Infection Found	The name of the last infection that was encountered.
Last Time Infection Found	The date and time when the last infection was found.

4.12.2 Scan Engines

The **Scan Engines** table displays the scan engine statistics and information.

Name	Displays the name of the scan engine.
Version	Displays the version number of the scan engine.
Status	Displays the status of the scan engine. The scan engine can be loaded and enabled or disabled by the administrator, or not loaded at all.
Last Database Update	Displays the last date and time when virus definition database was taken into use by the scan engine.
Database Date	Displays the date the virus signature database for the scan engine was created.
Last Infection Found	Displays the last infection found by the scan engine.

Last Time Infection Found	Displays the date and time of the last infection found by the scan engine.
Processed Files	Displays the number of files processed by the scan engine.
Infected Files	Displays the number of infected files found by the scan engine.
Disinfected Files	Displays the number of files successfully disinfected by the scan engine.
Database Version	Displays the current version of database updates used by the scan engine.

4.12.3 Common

The Common statistics branch displays the list of installed product hotfixes.

4.12.4 Spam Control

The Spam Control branch displays the following information:

Spam Scanner Version	Displays the version and build number of the Spam Scanner.
Status	Displays the status of the Spam Scanner.
Previous Reset of Statistics	Displays when the Spam Scanner statistics were reset last time.
Database Version	Displays the version of the database currently used by the Spam Scanner.
Last Database Update	Displays the date and time when the Spam Scanner database was last updated.
Number of Processed Messages	Displays the total number of e-mail messages that have been analyzed for spam.
Total Spam Statistics	These statistics show how many mail messages have been identified with each spam confidence level rating.

4.12.5 Virus Statistics

The Virus Statistics branch displays the following information:

Last Updated	Displays the date and time when the virus statistics were updated last time.
Most Active Viruses	Displays the list of most active viruses.

4.13 F-Secure Management Agent Settings

If the product is working in centrally managed administration mode, you have to make sure that it sends and receives data from F-Secure Policy Manager Server. To do this, change communications settings from F-Secure Management Agent.

Note: For detailed information on F-Secure Management Agent, see the F-Secure Policy Manager Administrator's Guide.

Communications

Host Configuration Mode	Shows whether the host is stand-alone or centrally administered.
Spool Time Limit	The maximum time the host will store the information it is unable to transmit.
Slow Connection Definition	This setting can be used to disallow F-Secure Management Agent from downloading large remote installation packages over slow network connections. F-Secure Management Agent measures the speed of the network link to F-Secure Policy Manager Server and stops the download if the minimum speed specified by this setting is not met.
Last Known Good Settings Recovery	Sets the interval how often the host tries to recover from Last Known Good (LKG) communication settings mode. If the communication settings have changed and the new settings do not work, the host enters the Last Known Good (LKG) communication settings mode and uses the old settings until the new settings have been confirmed to work.
Allow user to suspend network communications	If set to allowed, the user can temporarily suspend all network communications. **Note:** Select the **Final** checkbox in the Restriction Editor if the user is not allowed to suspend communications.
Host identification	Force the host to use a unique identity in communication or allow the use of DNS name, IP addresses, or WINS names.

Protocols

The branch contains the HTTP protocol settings used for communication between hosts and F-Secure Policy Manager.

Management Server Address	URL of the F-Secure Policy Manager Server. The URL should not have a slash at the end. For example: **http://fsms.example.com**.
Incoming Packages Polling Interval	Defines how often the host tries to fetch incoming packages (such as Base Policy files or new virus signature databases) from the F-Secure Policy Manager Server.
Outgoing Packages Update Interval	Defines how often the host tries to transmit to the administrator information that is periodically updated (such as statistics).

4.14 F-Secure Automatic Update Agent Settings

Using F-Secure Automatic Update Agent is the most convenient way to keep the virus and spam definition databases updated. It connects to F-Secure Policy Manager Server or the F-Secure Update Server automatically.

Communications

Automatic updates	Enable or disable automatic virus and spam definition updates. By default, automatic updates are enabled.
Internet connection checking	Specify whether the product should check the connection to the Internet before trying to retrieve updates. **Assume always connected** - The computer is connected to the Internet all the time. **Detect connection** - The product detects when the computer is connected to the Internet. **Detect traffic** - The product assumes that the computer is connected to the Internet only when other applications use the network. **Detect connection** is the default setting.
HTTP settings	Select whether to use an HTTP proxy when retrieving automatic updates. If F-Secure Automatic Update Agent connects to the Internet through a proxy server, specify the HTTP proxy address in the **User-defined proxy settings > Address** field. Enter the HTTP proxy server address.

PM Proxies	Specify F-Secure Policy Manager Proxies that you want to use as sources for automatic updates. If no F-Secure Policy Manager Proxies are configured, the product retrieves the latest virus definition updates from F-Secure Update Server automatically.
Intermediate server failover time	Specify (in hours) the failover time to connect to F-Secure Policy Manager Server or F-Secure Policy Manager Proxy. If the product cannot connect to any user-specified update server during the failover time, it retrieves the latest virus definition updates from F-Secure Update Server if Allow fetching updates from F-Secure Update Server is enabled.
Intermediate server polling interval	Specify (in minutes) how often the product checks one of the update sources for new updates.
Allow fetching updates from F-Secure Update Server	Specify whether the product should connect to F-Secure Update Server when it cannot connect to any user-specified update server. Specify **PM Proxies** to configure the update servers.

Administration with Web Console

Topics:

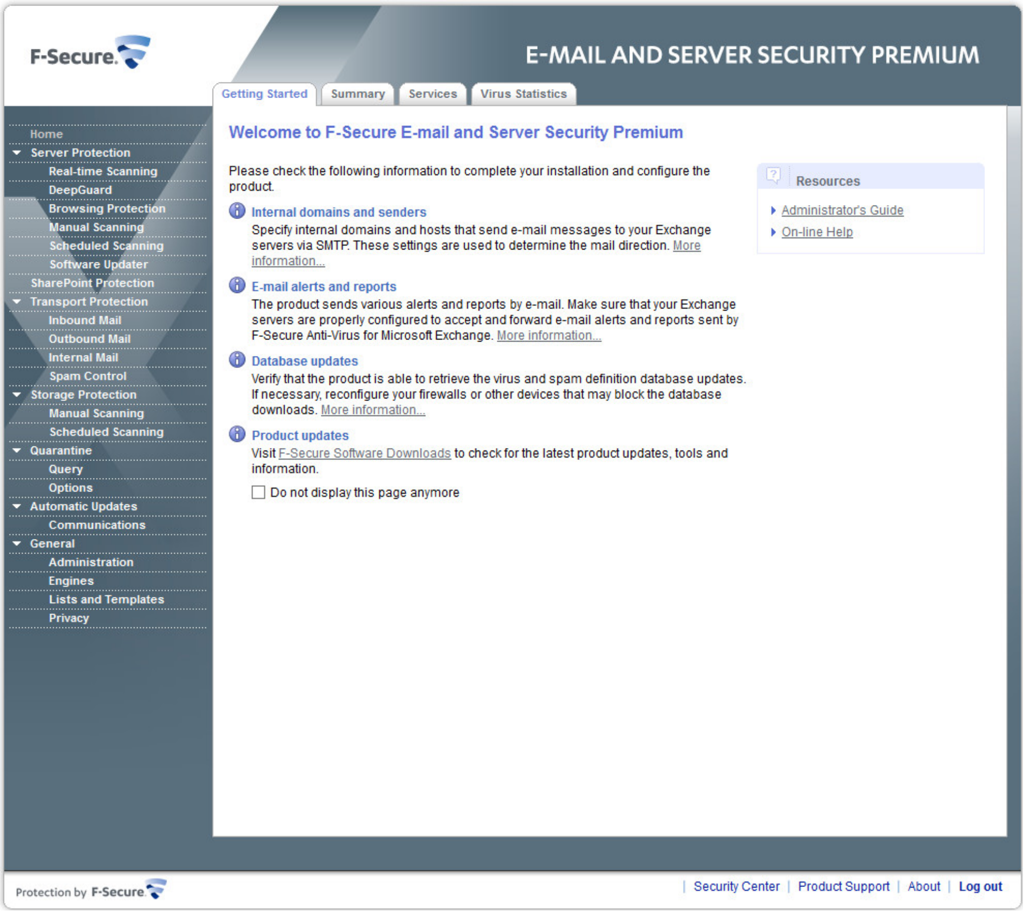
- *Home*
- *Server Protection*
- *SharePoint Protection*
- *Transport Protection*
- *Spam Control*
- *Storage Protection*
- *Quarantine*
- *Automatic Updates*
- *General Server Properties*

This section describes how to use Web Console to administer the product.

If the product is installed in the stand-alone mode, it can be administered with the Web Console.

5.1 Home

The Web Console displays **Getting Started** page when you log in for the first time.



Welcome to F-Secure E-mail and Server Security Premium

Please check the following information to complete your installation and configure the product.

Internal domains and senders
Specify internal domains and hosts that send e-mail messages to your Exchange servers via SMTP. These settings are used to determine the mail direction. More information...

E-mail alerts and reports
The product sends various alerts and reports by e-mail. Make sure that your Exchange servers are properly configured to accept and forward e-mail alerts and reports sent by F-Secure Anti-Virus for Microsoft Exchange. More information...

Database updates
Verify that the product is able to retrieve the virus and spam definition database updates. If necessary, reconfigure your firewalls or other devices that may block the database downloads. More information...

Product updates
Visit F-Secure Software Downloads to check for the latest product updates, tools and information.

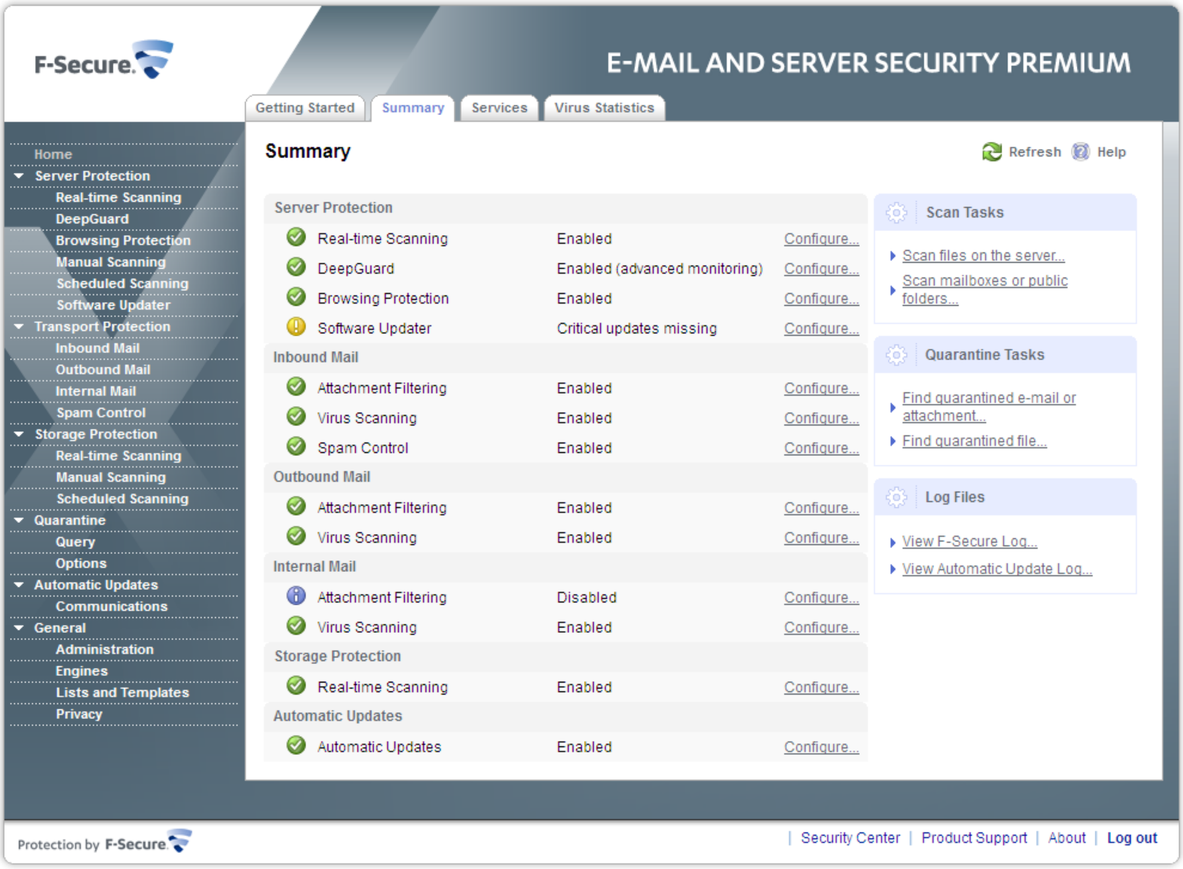
☐ Do not display this page anymore

You can check and configure the following information in the **Getting Started** page to complete the installation:

- Internal domains and senders
- E-mail alerts and reports
- Database updates
- Product updates

5.1.1 Summary

The **Summary** tab displays the current status of the product components.



Summary

Server Protection		
✓ Real-time Scanning	Enabled	Configure...
✓ DeepGuard	Enabled (advanced monitoring)	Configure...
✓ Browsing Protection	Enabled	Configure...
! Software Updater	Critical updates missing	Configure...
Inbound Mail		
✓ Attachment Filtering	Enabled	Configure...
✓ Virus Scanning	Enabled	Configure...
✓ Spam Control	Enabled	Configure...
Outbound Mail		
✓ Attachment Filtering	Enabled	Configure...
✓ Virus Scanning	Enabled	Configure...
Internal Mail		
ℹ Attachment Filtering	Disabled	Configure...
✓ Virus Scanning	Enabled	Configure...
Storage Protection		
✓ Real-time Scanning	Enabled	Configure...
Automatic Updates		
✓ Automatic Updates	Enabled	Configure...

✓	**Normal**; the feature is enabled and everything is working as it should.
ℹ	**Informational**; the feature is disabled.
!	**Warning**; the feature or an antivirus engine is disabled or virus and spam definition databases are not up-to-date.
✗	**Error**; the license has expired, the feature is not installed, all antivirus engines are disabled or a component is not loaded, F-Secure Content Scanner Server is not up and running or virus and spam definition databases are really old.

Note: If you install the product with EMC CAVA support, it should be enabled and working as it should after the installation is complete. EMC CAVA support provides Anti-Virus configuration when working in EMC CAVA environment.

Scan Tasks

Click **Scan files on the server** to manually scan files on the server for viruses and malware. For instructions, see *Manual Scanning*.

Click **Scan mailboxes or public folders** to manually scan mailboxes and public folders for viruses and strip attachments in them. For instructions, see *Manual Scanning*.

Quarantine Tasks

Click **Find quarantined e-mail or attachment** to search for the quarantined messages and attachments.

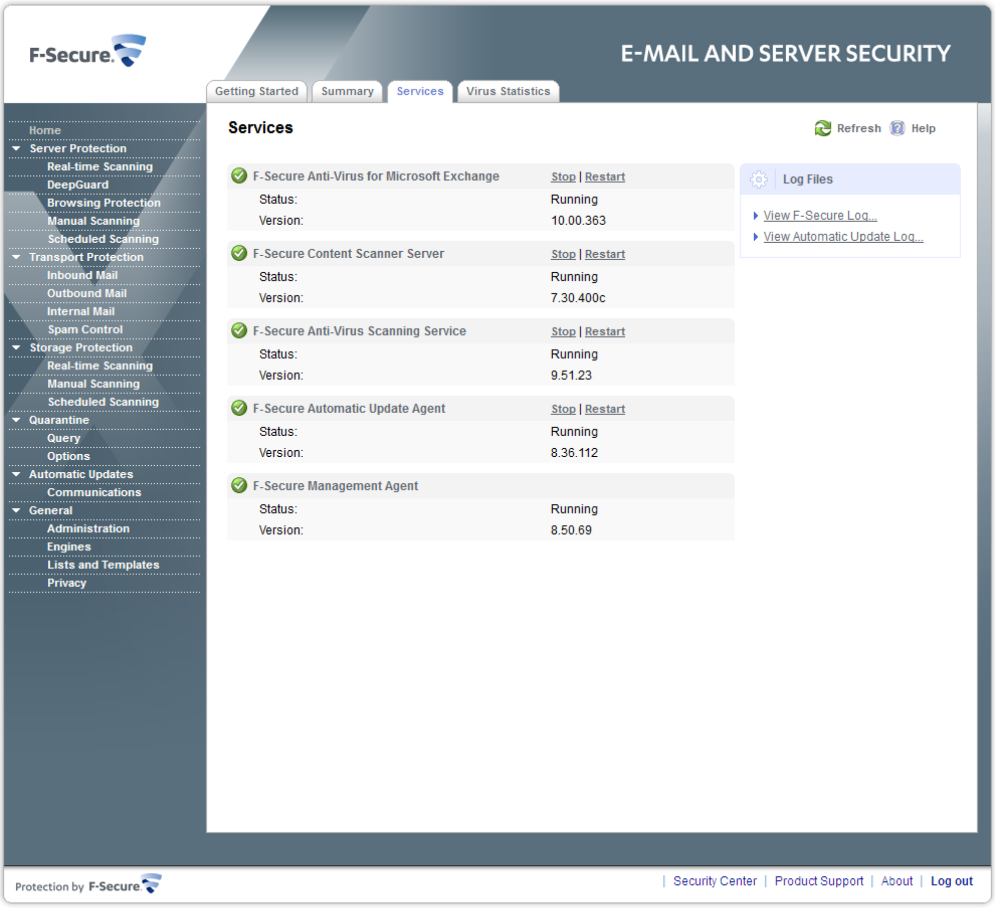
Click **Find quarantined file** to search for the quarantined file. For more information, see *Quarantined Files*.

Log Files

Click **View F-Secure Log** to view the F-Secure log file (LogFile.log) in a new Internet browser window. Click **Download** to download and save the LogFile.log for later use.

Click **View Automatic Update Log** to view the update log file.

5.1.2 Services



Services

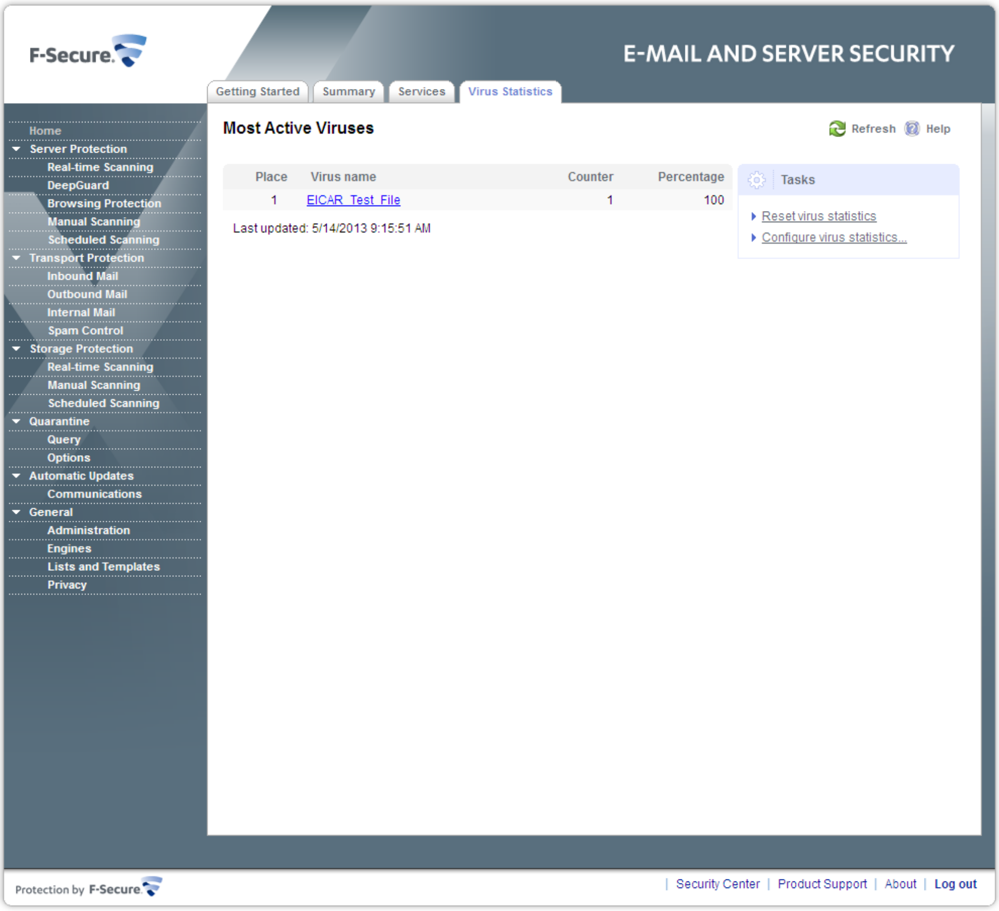
F-Secure Anti-Virus for Microsoft Exchange		Stop | Restart
Status:	Running	
Version:	10.00.363	
F-Secure Content Scanner Server		Stop | Restart
Status:	Running	
Version:	7.30.400c	
F-Secure Anti-Virus Scanning Service		Stop | Restart
Status:	Running	
Version:	9.51.23	
F-Secure Automatic Update Agent		Stop | Restart
Status:	Running	
Version:	8.36.112	
F-Secure Management Agent		
Status:	Running	
Version:	8.50.69	

Under the **Services** tab, you can start, stop, and restart services and see their current status.

Note: F-Secure Management Agent cannot be started or stopped.

5.1.3 Virus Statistics

Virus Statistics tab displays information on the most active viruses found during e-mail scanning with Transport and Storage Protection.



Most Active Viruses

Place	Virus name	Counter	Percentage
1	EICAR_Test_File	1	100

Last updated: 5/14/2013 9:15:51 AM

Note: The viruses found during file scanning with the Server Protection are not included in the statistics.

5.2 Server Protection

Server Protection protects the server from programs that may steal personal information, damage the computer, or use it for illegal purposes. You can scan the server for malware in real time, manually, or your can schedule a scan at set times.

When any type of malware is found, they are by default disabled immediately before they can cause harm.

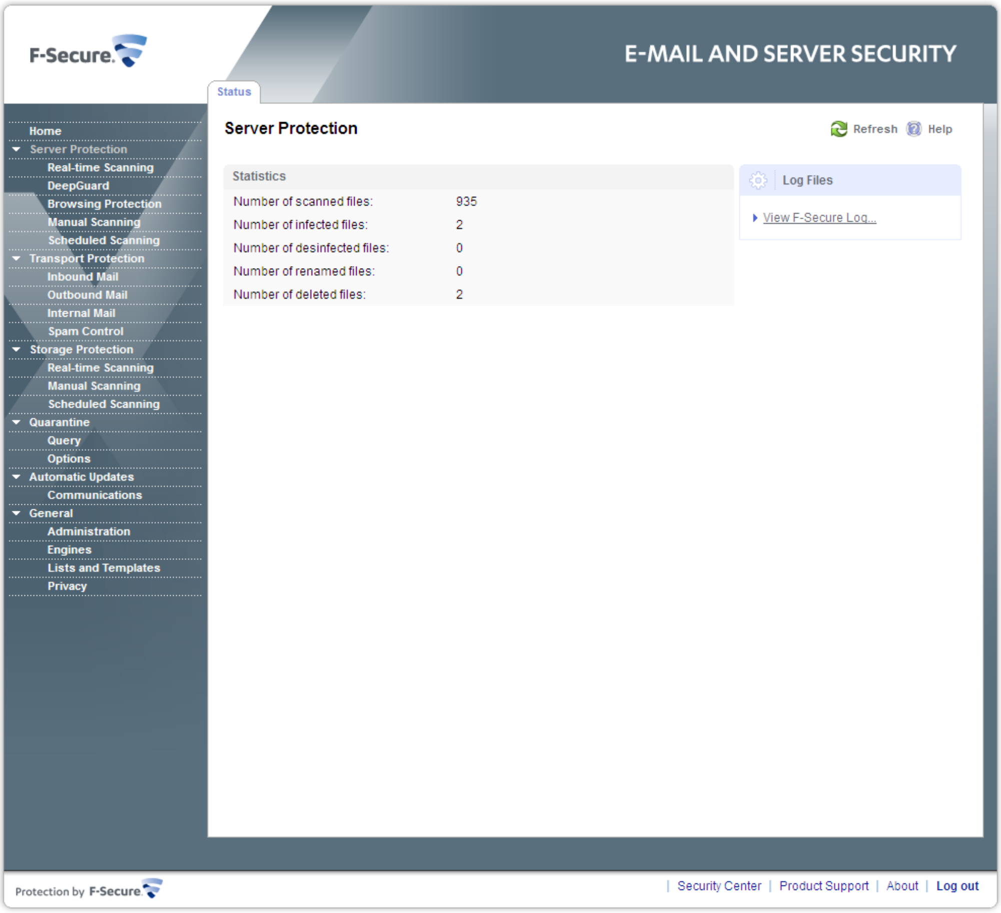
The product scans your local hard drives, any removable media (such as portable drives or compact disks) and downloaded content automatically by default.

Virus and spyware scanning also watches your computer for any changes that may indicate malware. If any dangerous system changes, for example system settings or attempts to change important system processes are found, DeepGuard stops this program from running as it is likely to be malware.

Note: These settings are used only if F-Secure virus and spyware protection component is installed with the product, otherwise these settings are not available.

Server Protection also features Software Updater, which scans and reports missing updates for third-party software and deploys security updates.

Status



Server Protection

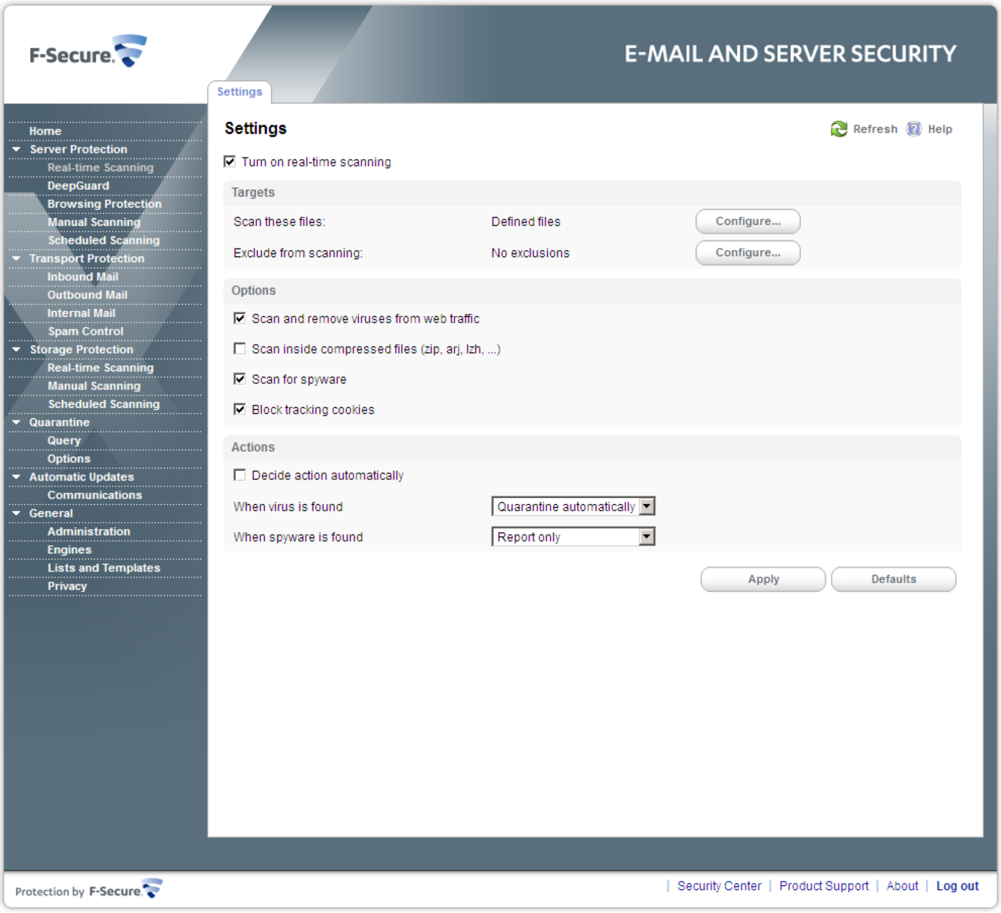
Statistics

Number of scanned files:	935
Number of infected files:	2
Number of desinfected files:	0
Number of renamed files:	0
Number of deleted files:	2

The **Status** page displays a summary of the scanned and processed files.

5.2.1 Real-time Scanning

Real-time scanning protects the computer by scanning all files when they are accessed and by blocking access to those files that contain malware.



Settings

☑ Turn on real-time scanning

Targets

Scan these files: Defined files

Exclude from scanning: No exclusions

Options

☑ Scan and remove viruses from web traffic

□ Scan inside compressed files (zip, arj, lzh, ...)

☑ Scan for spyware

☑ Block tracking cookies

Actions

□ Decide action automatically

When virus is found: Quarantine automatically

When spyware is found: Report only

Turn on real-time scanning

Enable or disable the virus scan. The virus scan scans files on the server for viruses and other malicious code.

Targets

Scan these files

Specify files that are scanned for viruses.

Scan all files - Scan all files in the system.

Scan defined files - Scans only the file types that you define.

Exclude from scanning

Specify files that are not scanned.

Applications tab lists spyware and riskware applications that have been excluded from the scan. To include the application in future scans, select it from the list and click **Remove**.

To exclude a specific file or folder, add it to the list in the **Objects** tab.

To exclude a file type, enter the three-letter file extension in the **Files** tab and click **Add**.

To exclude processes from scanning, add the process executable to the list in the Processes tab.

Note: A file that is excluded from scanning by either type or location is not scanned even if the file is included in the list of scanned file types.

Options

Scan and remove viruses from web traffic

You can scan information passing through the browser for malware, so that the server is protected from harmful web traffic.

Scan inside compressed files

Specify whether files inside compressed archive files are scanned for viruses and other malicious code.

Scan for spyware

Specify whether to scan for programs that collect personal information.

Block tracking cookies

When you block tracking cookies, web sites cannot track visited sites.

Actions

Decide action automatically

Turn on to let the product decide what to do to each malware item to automatically clean the computer.

When virus is found

The following actions can be taken for viruses:

Clean automatically - The product tries to disinfect the viruses in any infected files that were found during real-time scanning.

Quarantine automatically (default) - The product moves any infected files found during real-time scanning to the quarantine where it cannot harm your computer.

Rename automatically - The product renames any infected files found during real-time scanning.

Delete automatically - The product deletes any infected files found during real-time scanning.

Report only - The product records the detected viruses in the `logfile.log` file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications (according to the settings that are specified on the Alerts page under **General > Administration**).

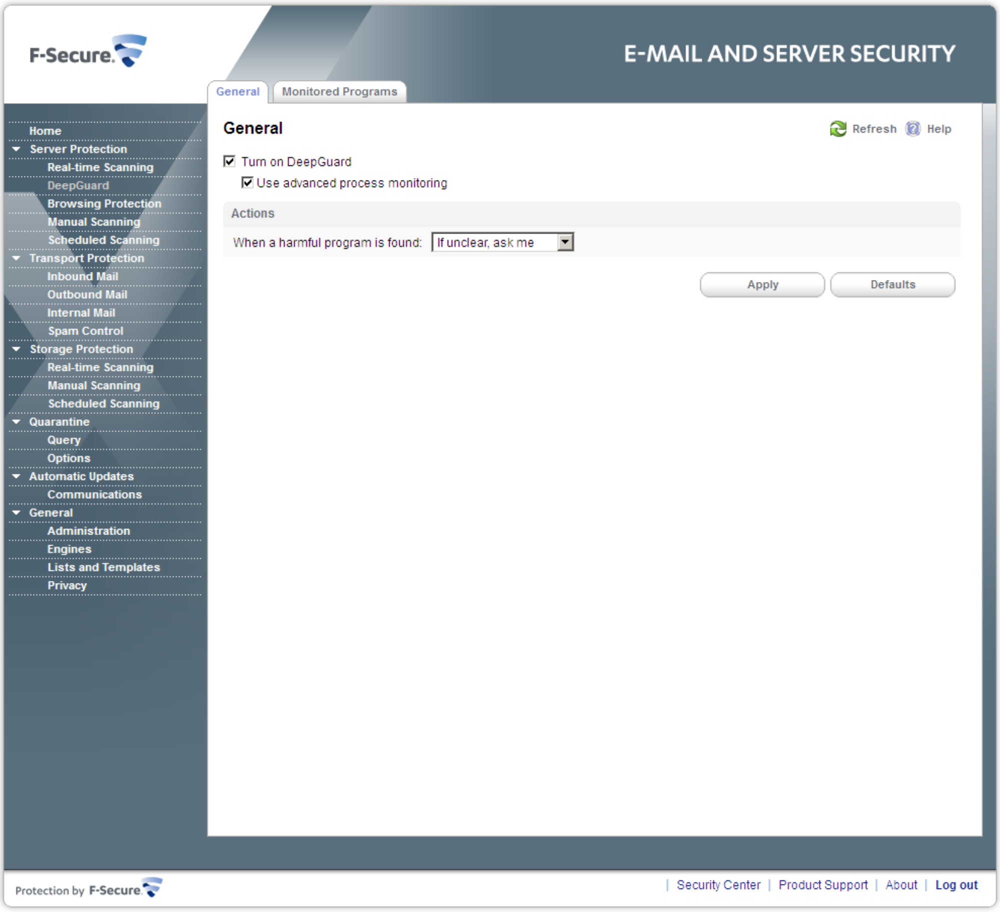
When spyware is found	The following actions can be taken for spyware: **Report only (default)** - The product leaves any spyware that was found during real-time scanning as it is and records the detection in the `logfile.log` file, sends alerts to Policy Manager, adds events to Windows Event log, and sends e-mail notifications (according to the settings that are specified on the Alerts page under **General > Administration**). **Remove automatically** - The product removes any spyware found during real-time scanning. **Quarantine automatically** - The product moves any spyware found during real-time scanning to the quarantine where it cannot harm your computer.

Excluding Processes from the Real-Time Virus Scanning

When you exclude a process from the real-time virus scan, any files that the excluded process access are not scanned for viruses. Excluding processes can speed up the system and ensures compatibility with backup utilities and other third-party software.

5.2.2 DeepGuard

DeepGuard analyzes the content of files and behavior of programs, and blocks new and undiscovered viruses, worms, and other malicious programs that try to make potentially harmful changes to your computer.



General

☑ Turn on DeepGuard

☑ Use advanced process monitoring

Actions

When a harmful program is found: If unclear, ask me

System changes that can be dangerous include:

- system setting (Windows registry) changes,
- attempts to turn off important system programs, for example, security programs like this product, and
- attempts to edit important system files.

DeepGuard continuously watches for these changes and checks each program that attempts to change the system.

When DeepGuard detects a program attempting to make potentially harmful changes to the system, it allows the program to run in a safe-zone, unless you have specifically allowed or blocked the program.

In the safe-zone, the program cannot harm your computer. DeepGuard analyzes what changes the program tried to make, and based on this, decides how likely the program is to be malware.

DeepGuard automatically either allows or blocks the program, or asks you whether to allow or block the program, depending on how likely the program is to be malware.

Note: These settings are used only if F-Secure DeepGuard is installed with the product, otherwise these settings are not available.

Turn on DeepGuard

By turning DeepGuard on, you can prevent suspicious programs from making potentially harmful system changes in the computer.

Use advanced process monitoring

When advanced process monitoring is turned on, DeepGuard temporarily modifies running programs for maximum protection.

Note: Advanced process monitoring may cause problems with programs that make sure that they are not corrupted or modified.

Actions

When a harmful program is found

Select one of the following default actions if DeepGuard detects a system modification attempt.

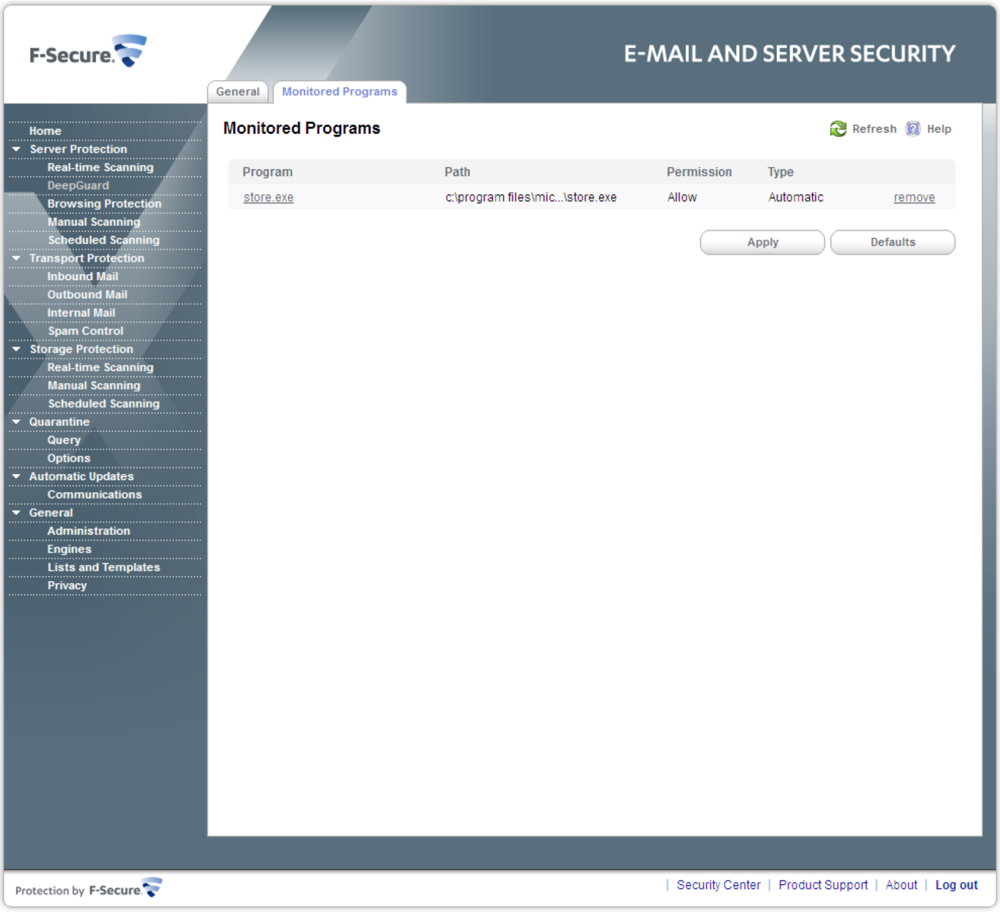
Always ask me - DeepGuard asks you whether you want to allow or block all monitored actions, even when it identifies the application as safe.

If unclear, ask me - Ask when DeepGuard detects a program trying to make potentially harmful system changes and it cannot identify whether the program is safe or unsafe.

Handle automatically - DeepGuard blocks unsafe applications and allows safe applications automatically without asking you any questions.

5.2.2.1 Monitored Programs

You can allow a blocked program by changing its permission in the **Monitored Programs** list.



Monitored Programs

Program	Path	Permission	Type	
store.exe	c:\program files\mic...\store.exe	Allow	Automatic	remove

Sometimes DeepGuard may block a safe program from running, even if you want to use the program and know it to be safe. This happens because the program tries to make system changes that might be potentially harmful.

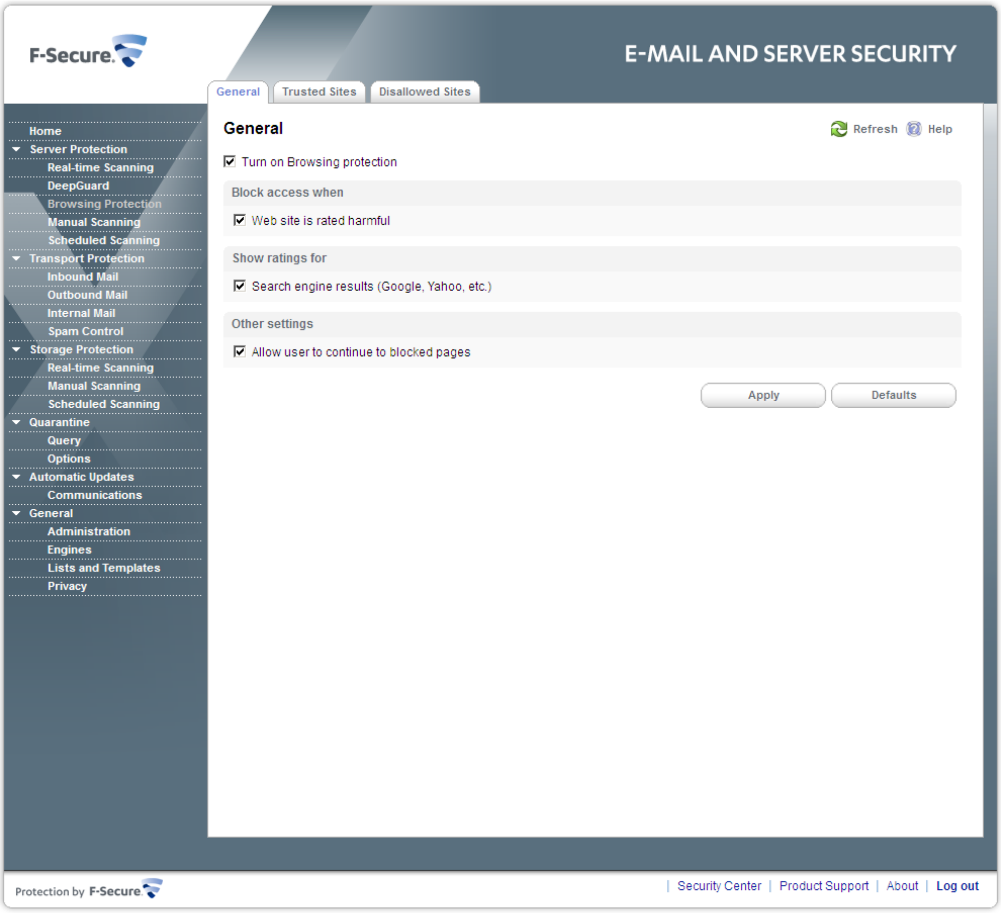
You may also have unintentionally blocked a program that you want to allow later.

To allow a program that DeepGuard has blocked, follow these instructions:

1. Click the program name you want to allow.
2. Select **Allow** and click **OK** to close the dialog.
3. Click **Apply**.

5.2.3 Browsing Protection

Browsing protection helps you evaluate the safety of web sites you visit and prevents you from unintentionally accessing harmful web sites.



General

☑ Turn on Browsing protection

Block access when

☑ Web site is rated harmful

Show ratings for

☑ Search engine results (Google, Yahoo, etc.)

Other settings

☑ Allow user to continue to blocked pages

Browsing protection shows you safety ratings for web sites that are listed on search engine results. By helping you avoid web sites that contain security threats, such as malware (viruses, worms, trojans) and phishing, you avoid the latest Internet threats that are not yet recognized by traditional antivirus programs.

There are four possible safety ratings for web sites: safe, suspicious, harmful and unknown. These safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

Note: These settings are used only if F-Secure Browsing protection component is installed with the product, otherwise these settings are not available.

Turn on Browsing protection

You will be blocked from accessing harmful websites when browsing protection is turned on.

Block access when

Web site is rated harmful

Block access to web sites that has been rated harmful.

Show ratings for

Search engine results	When selected, browsing protection ratings will be displayed for the sites listed on search engines (Google, Yahoo, etc.).
Other settings	
Allow user to continue to blocked pages	Specify whether users can open blocked pages after viewing the warning message.

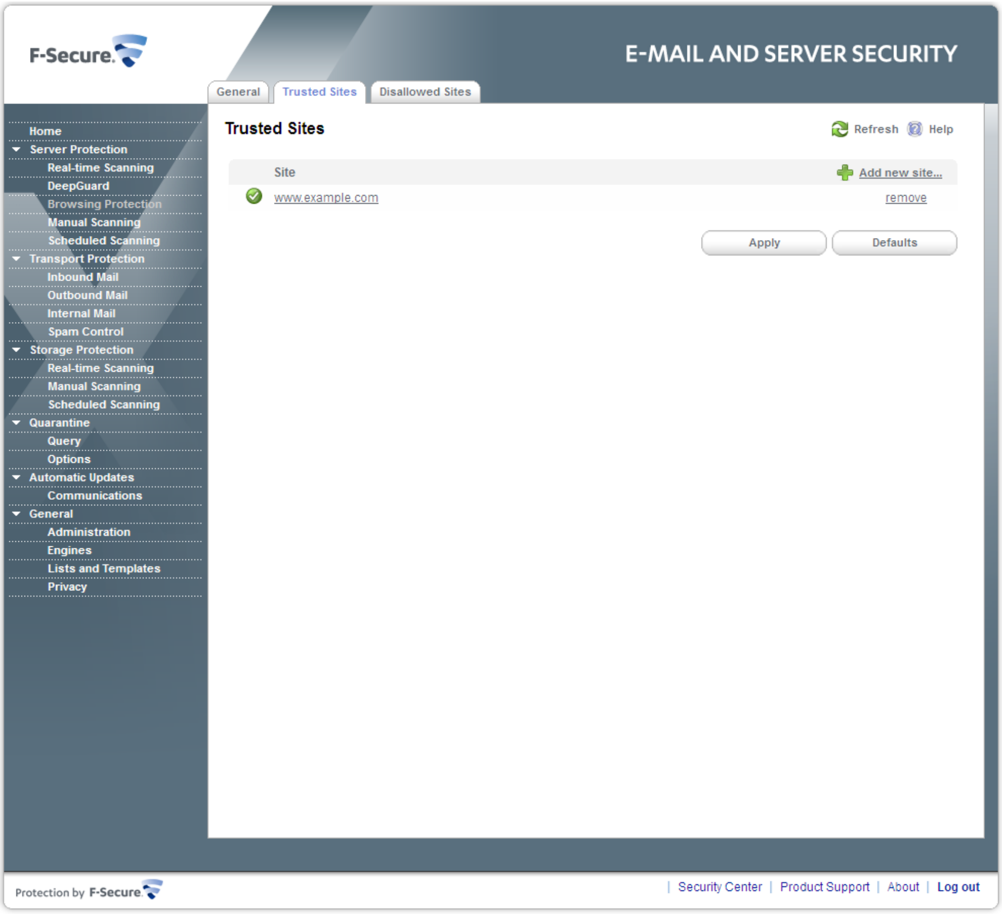
Browsing Protection Ratings

Color-coded icons show the safety rating of the current site (on the toolbar). The safety rating of each link on search engine results is also shown with the same icons. Four different color-coded icons are used:

Green	The page is safe.
Amber	The page is suspicious. Security analysis of the page indicates that it is safe, but many users have given it a low safety rating.
Red	The page is harmful.
Gray	The page has not been analyzed and no information is currently available for it.

5.2.3.1 Trusted Sites

If browsing protection blocks access to a page that you trust and want to access, you can define it as a trusted site.



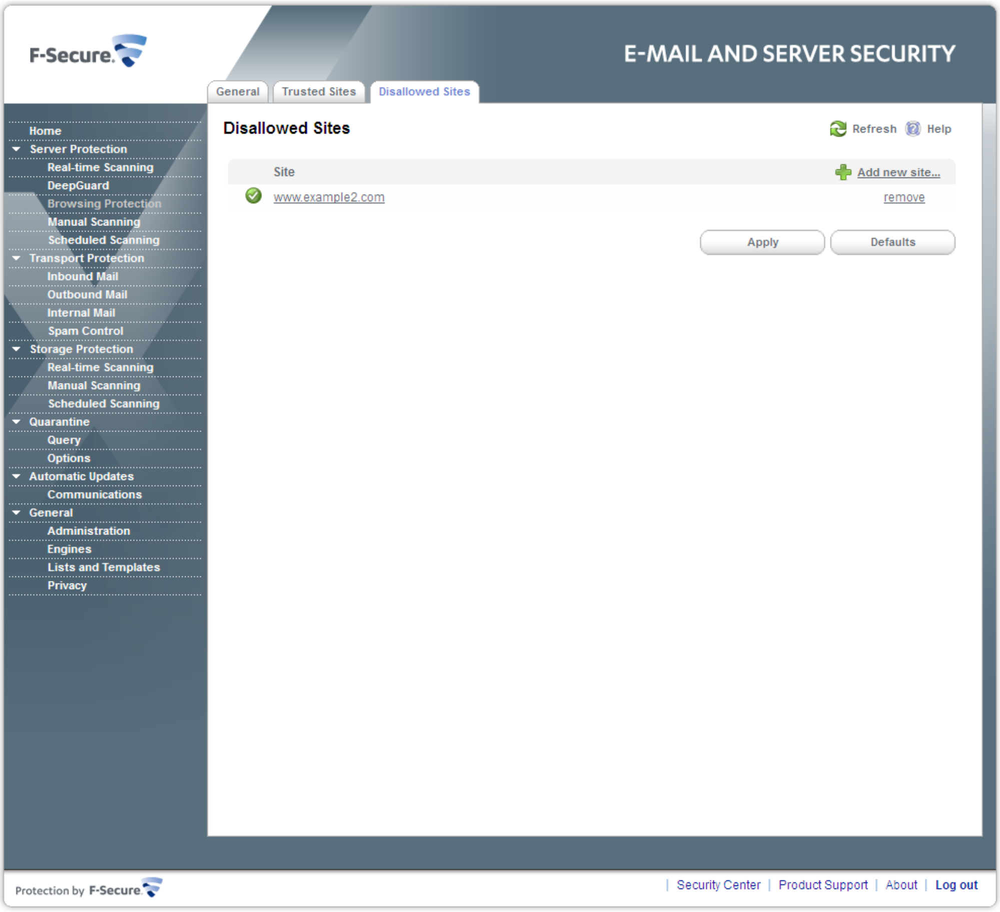
Enter the web address in the Site field to add a trusted web site.

- Use the format "www.example.com/" to allow access to the specific site, but to block access to, for example, "www.example.com.us".
- Use the format "www.example.com" to allow access to several similar addresses such as "www.example.com" and "www.example.com.us".

Note: Use this option with caution as it defines more than just the specific site as trusted. Other sites may be safe, but they can also be fake sites which may used for phishing.

5.2.3.2 Disallowed Sites

If you want to block access to a web site completely, you can define it as a disallowed site.



Disallowed Sites

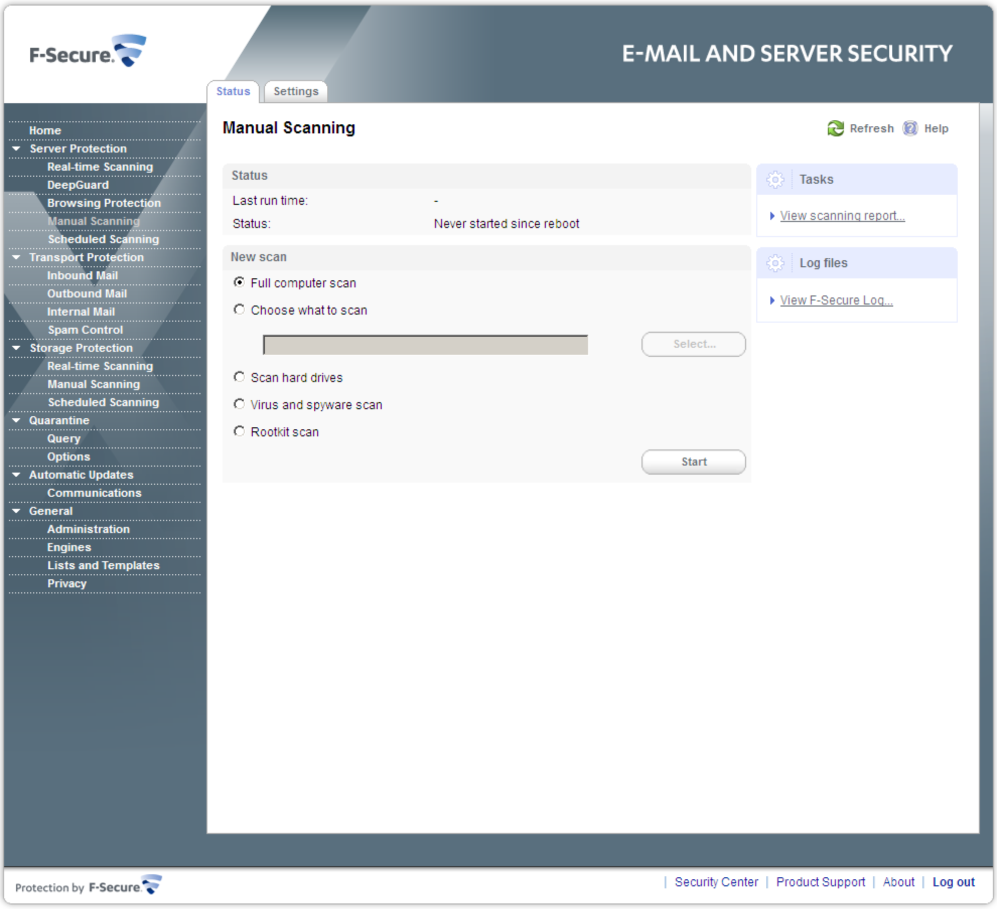
Site	
✓ www.example2.com	remove

Enter the web address in the Site field to add a disallowed web site.

- Use the format "www.example.com/" to block access to the specific site, but to allow access to, for example, "www.example.com.us".
- Use the format "www.example.com" to block access to several similar addresses such as "www.example.com" and "www.example.com.us".

5.2.4 Manual Scanning

You can scan the server manually, for example if you suspect that you have malware on the computer. You can scan your whole computer or scan for a specific type of malware or a specific location.



Manual Scanning

Status

Last run time: -

Status: Never started since reboot

New scan

● Full computer scan

○ Choose what to scan

○ Scan hard drives

○ Virus and spyware scan

○ Rootkit scan

If you are suspicious of a certain type of malware, you can scan only for this type. If you are suspicious of a certain location on your computer, you can scan only that section. These scans will finish a lot quicker than a scan of your whole computer.

New scan

To start manually scanning the server:

1. Under **New scan**, select the type of scan.

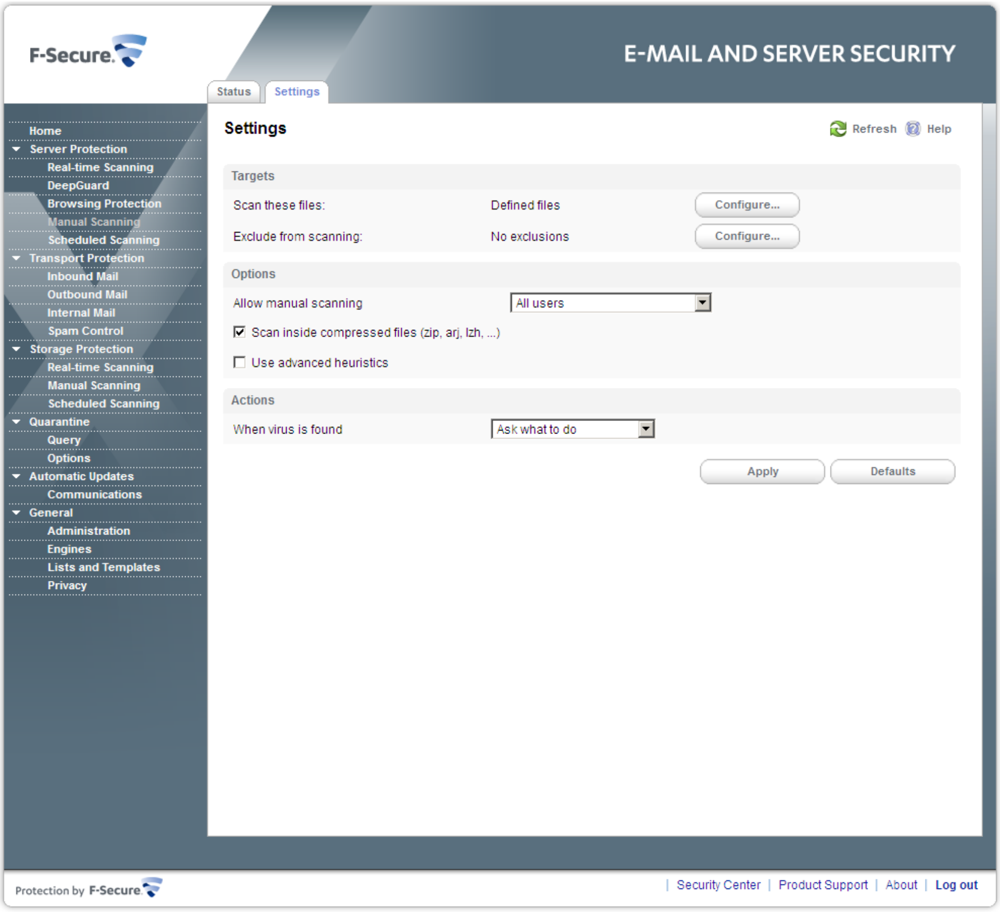
   If you want to change the scanning settings, click the **Settings** tab.

2. If you selected **Choose what to scan**, click **Select** and select which location to scan.
3. Click **Start** to start scanning. If no malware is detected, you will see "Finished" on the Status line at the upper part of the page.

Click **View scanning report** in the **Tasks** list to see the results of the last scan.

5.2.4.1 Settings

Specify settings used while running the manual file and memory scan.



Settings

Targets

Scan these files: Defined files Configure...

Exclude from scanning: No exclusions Configure...

Options

Allow manual scanning: All users

☑ Scan inside compressed files (zip, arj, lzh, ...)

☐ Use advanced heuristics

Actions

When virus is found: Ask what to do

Targets

Scan these files

Specify files that are scanned for viruses.

Scan all files - Scan all files in the system.

Scan defined files - Scans only the file types that you define.

Exclude from scanning

Specify files that are not scanned.

Applications tab lists spyware and riskware applications that have been excluded from the scan. To include the application in future scans, select it from the list and click **Remove**.

To exclude a specific file or folder, add it to the list in the **Objects** tab.

To exclude a file type, enter the three-letter file extension in the **Files** tab and click **Add**.

Note: A file that is excluded from scanning by either type or location is not scanned even if the file is included in the list of scanned file types.

Options

Allow manual scanning

Specify users who are allowed to run manual scans.

Not allowed - Manual scanning is not allowed.

Users with administrative rights - Only users with administrative rights can start the manual scan.

All users - Anyone can start the manual scan.

Scan inside compressed files

Specify whether files inside compressed archives should be scanned for malware.

Use advanced heuristics

Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

Actions

When virus is found

If malware is found during the scan, you can either let the product automatically decide how to clean the server or you can decide yourself for each item.

Ask what to do (default) - The product asks you what to do if viruses are found during manual scanning.

Clean automatically - The product tries to automatically disinfect the viruses in any infected files that were found during the scan.

It is not always possible to disinfect a virus in a file. In these cases, the file is quarantined (except when found on network or removable drives), so the virus cannot harm the server.

Quarantine automatically - The product moves any infected files that were found during the scan to the quarantine where they cannot harm the server.

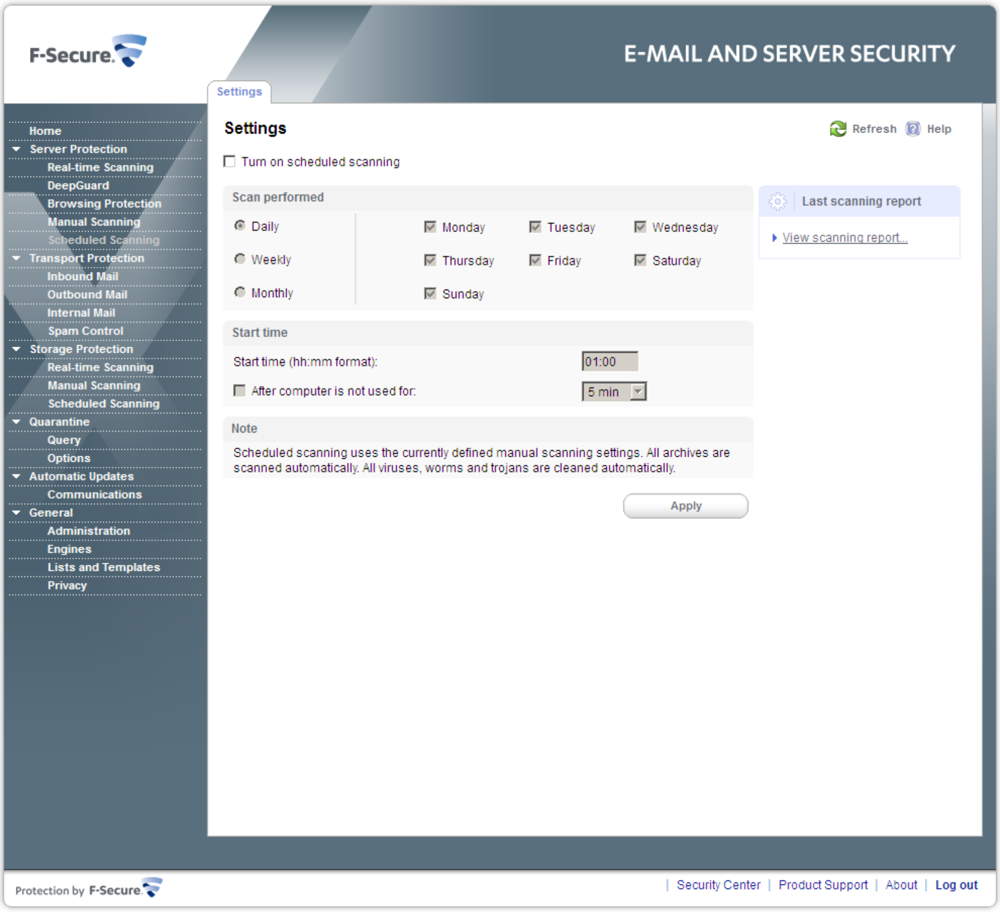
Rename automatically - The product renames any infected files that were found during the scan.

Delete automatically - The product deletes any infected files that were found during the scan.

Report only - The product leaves any infected files that were found during the scan as they are and records the detection in the scan report.

5.2.5 Scheduled Scanning

You can set the product to scan the server at regular times.



Settings

□ Turn on scheduled scanning

Scan performed

● Daily ☑ Monday ☑ Tuesday ☑ Wednesday

○ Weekly ☑ Thursday ☑ Friday ☑ Saturday

○ Monthly ☑ Sunday

Start time

Start time (hh:mm format): 01:00

□ After computer is not used for: 5 min

Note

Scheduled scanning uses the currently defined manual scanning settings. All archives are scanned automatically. All viruses, worms and trojans are cleaned automatically.

Turn on scheduled scanning	Enable or disable the scheduled virus scan.
Scan performed	Select which days you would like to regularly scan for viruses and spyware. **Daily** - Scan every day. **Weekly** - Scan on selected days during the week. Select on which days to scan from the list to the right. **Monthly** - Scan on up to three days a month.
Start time	Select when you want to start the scan on the selected days. **Start time** - The time when the scan will start. You should select a time when you expect to not be using the computer. **After computer is not used for** - Select a period of idle time after which the scanning starts if the computer is not used.

5.2.6 Managing software updates

Software Updater scans and reports missing updates for third-party software and deploys security updates.

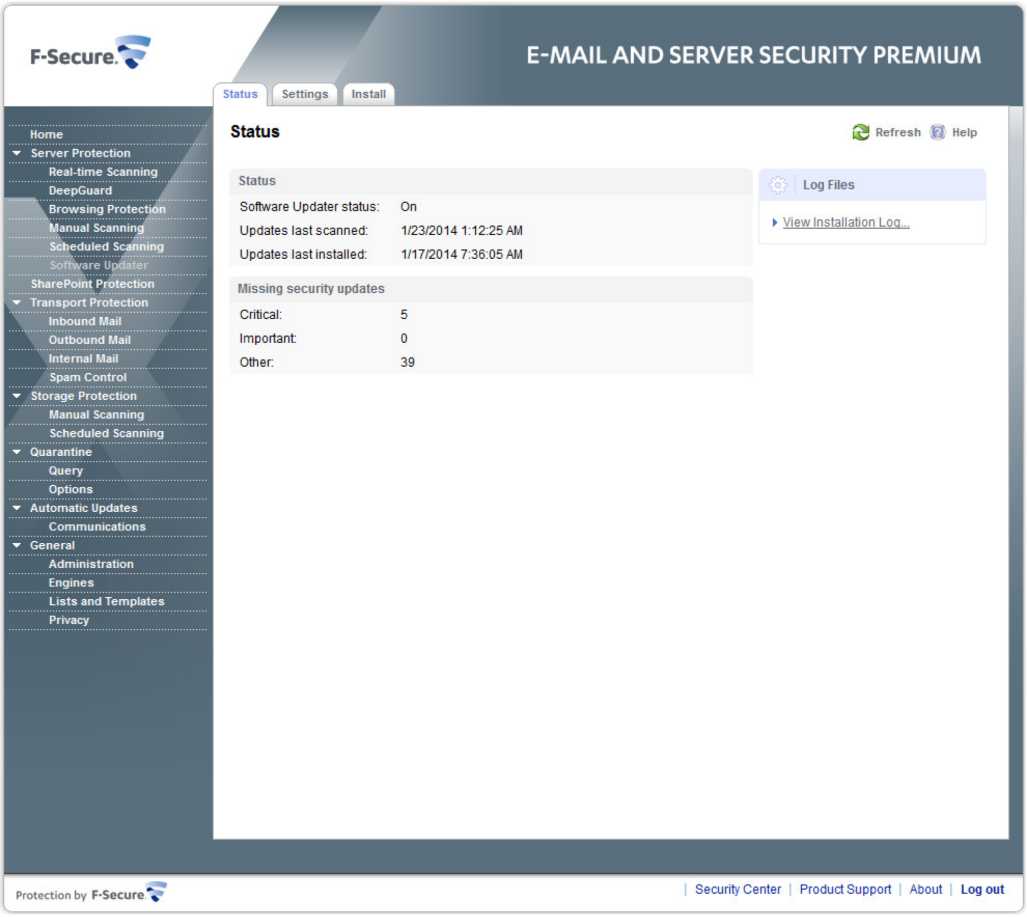
Software Updater scans for Microsoft updates for the operating system and Microsoft applications, in addition to a comprehensive list of third-party applications, such as Adobe Flash, Java, OpenOffice, archive managers, media players, image viewers and so on.

Software Updater periodically checks information about software updates, compares these to software that you have installed and identifiews missing updates.

It is important to have the latest software updates installed, because many updates fix security vulnerabilities in installed products.

5.2.6.1 Checking the status of software updates in your network

On the **Server Protection** > **Software Updater** > **Status** page, you can check the status of software updates on the server.



Status

Status

Software Updater status:	On
Updates last scanned:	1/23/2014 1:12:25 AM
Updates last installed:	1/17/2014 7:36:05 AM

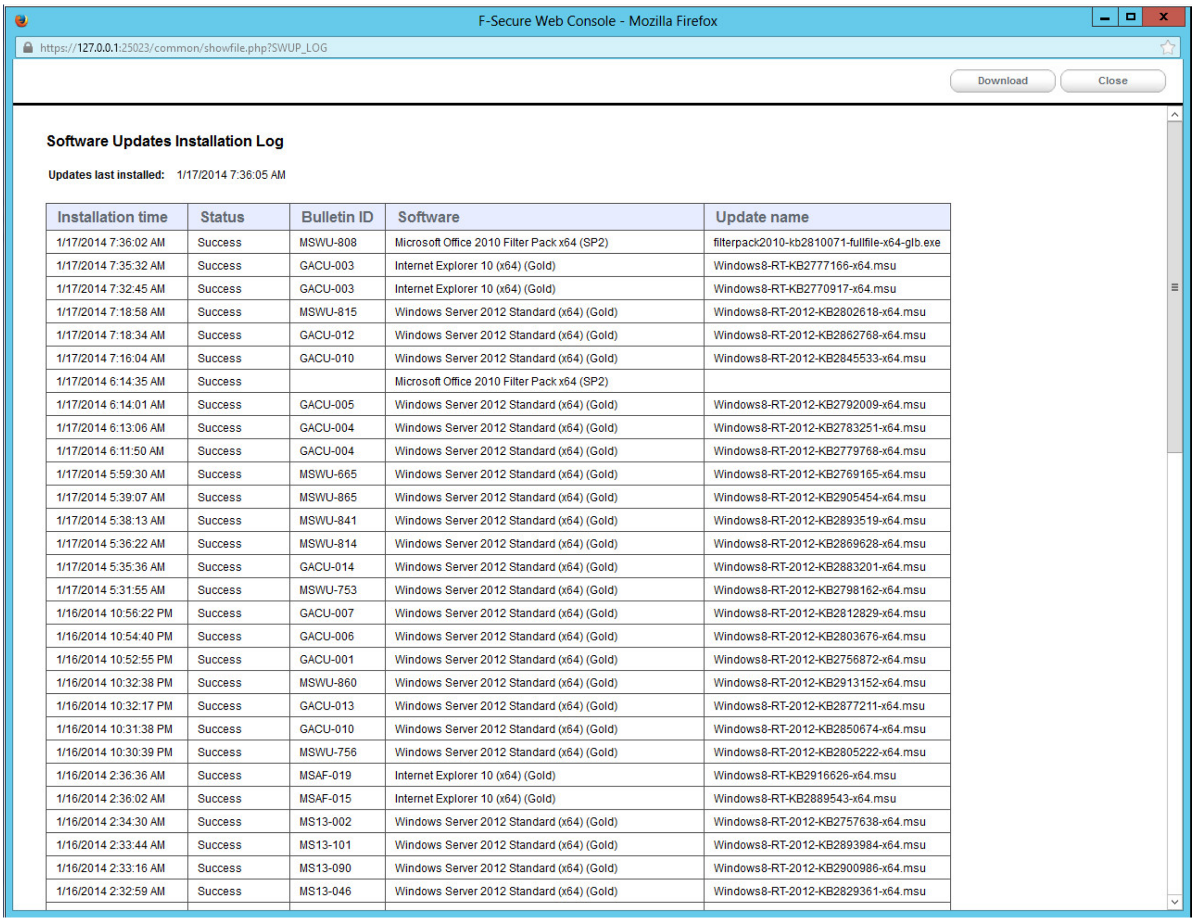
Missing security updates

Critical:	5
Important:	0
Other:	39

The **Status** page shows the number of critical, important, and other missing software updates, as well as the date when Software Updater last checked the status of installed updates and when the last updates were installed.

5.2.6.2 View Software Updater log

You can check which software updates have been installed and when in the Software Updater log.


F-Secure Web Console - Mozilla Firefox
https://127.0.0.1:25023/common/showfile.php?SWUP_LOG
Download
Close

Software Updates Installation Log

Updates last installed: 1/17/2014 7:36:05 AM

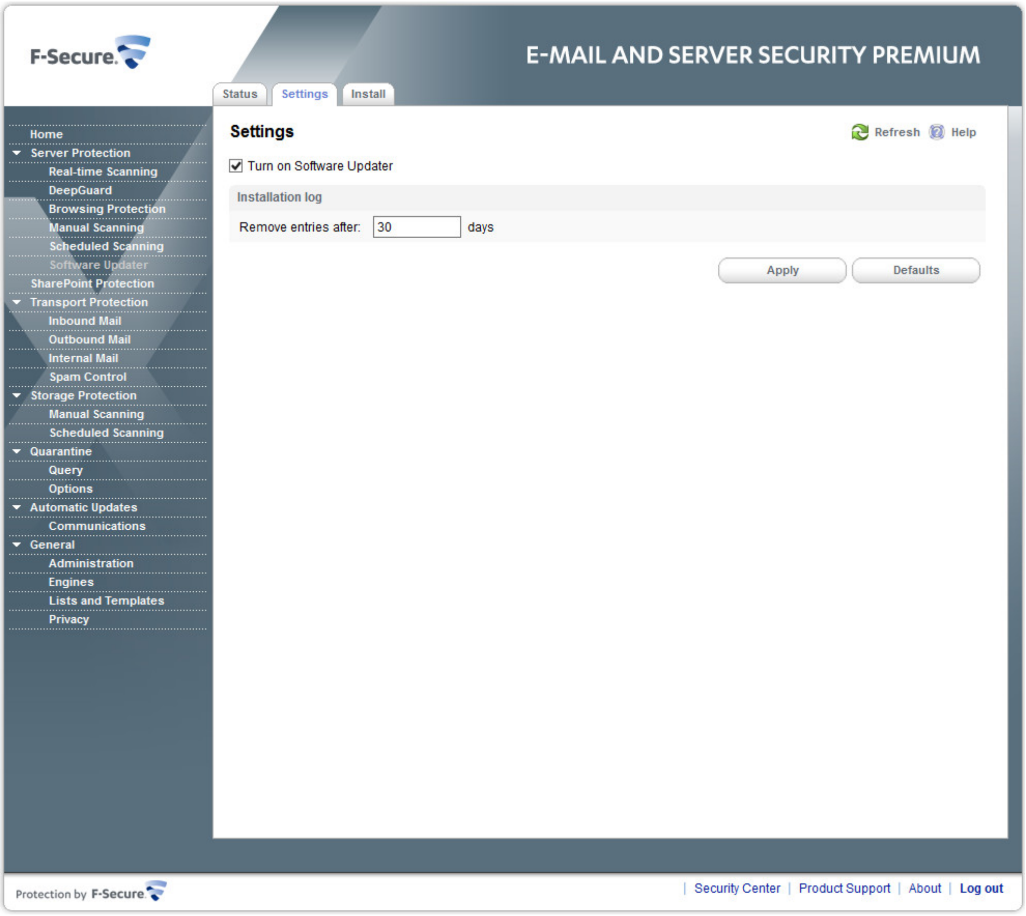
Installation time	Status	Bulletin ID	Software	Update name
1/17/2014 7:36:02 AM	Success	MSWU-808	Microsoft Office 2010 Filter Pack x64 (SP2)	filterpack2010-kb2810071-fullfile-x64-glb.exe
1/17/2014 7:35:32 AM	Success	GACU-003	Internet Explorer 10 (x64) (Gold)	Windows8-RT-KB2777166-x64.msu
1/17/2014 7:32:45 AM	Success	GACU-003	Internet Explorer 10 (x64) (Gold)	Windows8-RT-KB2770917-x64.msu
1/17/2014 7:18:58 AM	Success	MSWU-815	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2802618-x64.msu
1/17/2014 7:18:34 AM	Success	GACU-012	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2862768-x64.msu
1/17/2014 7:16:04 AM	Success	GACU-010	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2845533-x64.msu
1/17/2014 6:14:35 AM	Success		Microsoft Office 2010 Filter Pack x64 (SP2)	
1/17/2014 6:14:01 AM	Success	GACU-005	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2792009-x64.msu
1/17/2014 6:13:06 AM	Success	GACU-004	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2783251-x64.msu
1/17/2014 6:11:50 AM	Success	GACU-004	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2779768-x64.msu
1/17/2014 5:59:30 AM	Success	MSWU-665	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2769165-x64.msu
1/17/2014 5:39:07 AM	Success	MSWU-865	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2905454-x64.msu
1/17/2014 5:38:13 AM	Success	MSWU-841	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2893519-x64.msu
1/17/2014 5:36:22 AM	Success	MSWU-814	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2869628-x64.msu
1/17/2014 5:35:36 AM	Success	GACU-014	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2883201-x64.msu
1/17/2014 5:31:55 AM	Success	MSWU-753	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2798162-x64.msu
1/16/2014 10:56:22 PM	Success	GACU-007	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2812829-x64.msu
1/16/2014 10:54:40 PM	Success	GACU-006	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2803676-x64.msu
1/16/2014 10:52:55 PM	Success	GACU-001	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2756872-x64.msu
1/16/2014 10:32:38 PM	Success	MSWU-860	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2913152-x64.msu
1/16/2014 10:32:17 PM	Success	GACU-013	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2877211-x64.msu
1/16/2014 10:31:38 PM	Success	GACU-010	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2850674-x64.msu
1/16/2014 10:30:39 PM	Success	MSWU-756	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2805222-x64.msu
1/16/2014 2:36:36 AM	Success	MSAF-019	Internet Explorer 10 (x64) (Gold)	Windows8-RT-KB2916626-x64.msu
1/16/2014 2:36:02 AM	Success	MSAF-015	Internet Explorer 10 (x64) (Gold)	Windows8-RT-KB2889543-x64.msu
1/16/2014 2:34:30 AM	Success	MS13-002	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2757638-x64.msu
1/16/2014 2:33:44 AM	Success	MS13-101	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2893984-x64.msu
1/16/2014 2:33:16 AM	Success	MS13-090	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2900986-x64.msu
1/16/2014 2:32:59 AM	Success	MS13-046	Windows Server 2012 Standard (x64) (Gold)	Windows8-RT-2012-KB2829361-x64.msu

To view the Software Updater log:

1. Go to **Server Protection** > **Software Updater** > **Status**.
2. Click **View Installation Log**.
   Software Updates Installation Log shows:
   - the date when the update was installed,
   - installation status,
   - update ID,
   - updated software, and
   - the name of the update file.
3. To remove old entries from the log:
   a) Go to **Server Protection** > **Software Updater** > **Settings**.
   b) In **Remove entries after** field, enter how many days log entries stay in the installation log.

5.2.6.3 Turning Software Updater on or off

When Software Updater is on, it scans and reports missing updates for 3rd party software.



Settings

☑ Turn on Software Updater

Installation log

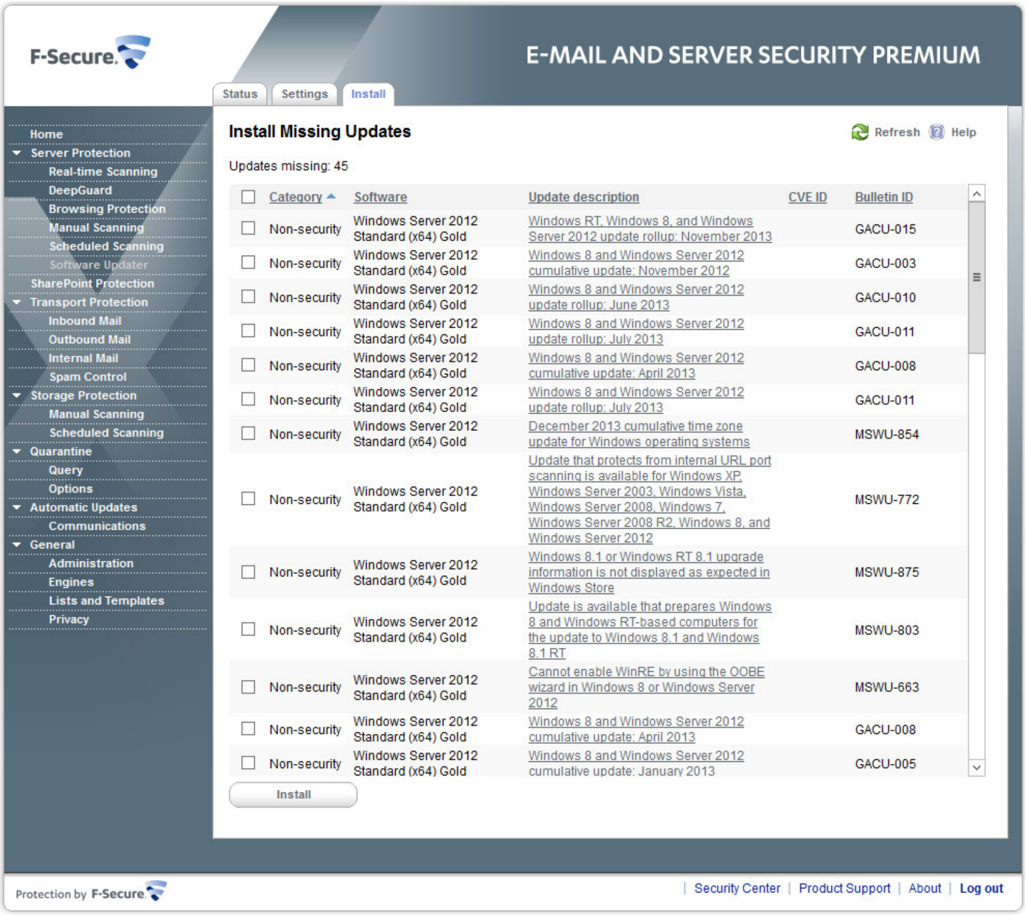
Remove entries after: 30 days

To turn Software Updater on:

1. Go to **Server Protection** > **Software Updater** > **Settings**.
2. Select **Turn on Software Updater**.
3. Click **Apply**.

5.2.6.4 Installing missing software updates

You can check the status of software updates and install missing updates manually when needed.



Install Missing Updates

Updates missing: 45

□	Category	Software	Update description	CVE ID	Bulletin ID
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows RT, Windows 8, and Windows Server 2012 update rollup: November 2013		GACU-015
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 cumulative update: November 2012		GACU-003
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 update rollup: June 2013		GACU-010
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 update rollup: July 2013		GACU-011
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 cumulative update: April 2013		GACU-008
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 update rollup: July 2013		GACU-011
□	Non-security	Windows Server 2012 Standard (x64) Gold	December 2013 cumulative time zone update for Windows operating systems		MSWU-854
□	Non-security	Windows Server 2012 Standard (x64) Gold	Update that protects from internal URL port scanning is available for Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012		MSWU-772
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8.1 or Windows RT 8.1 upgrade information is not displayed as expected in Windows Store		MSWU-875
□	Non-security	Windows Server 2012 Standard (x64) Gold	Update is available that prepares Windows 8 and Windows RT-based computers for the update to Windows 8.1 and Windows 8.1 RT		MSWU-803
□	Non-security	Windows Server 2012 Standard (x64) Gold	Cannot enable WinRE by using the OOBE wizard in Windows 8 or Windows Server 2012		MSWU-663
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 cumulative update: April 2013		GACU-008
□	Non-security	Windows Server 2012 Standard (x64) Gold	Windows 8 and Windows Server 2012 cumulative update: January 2013		GACU-005

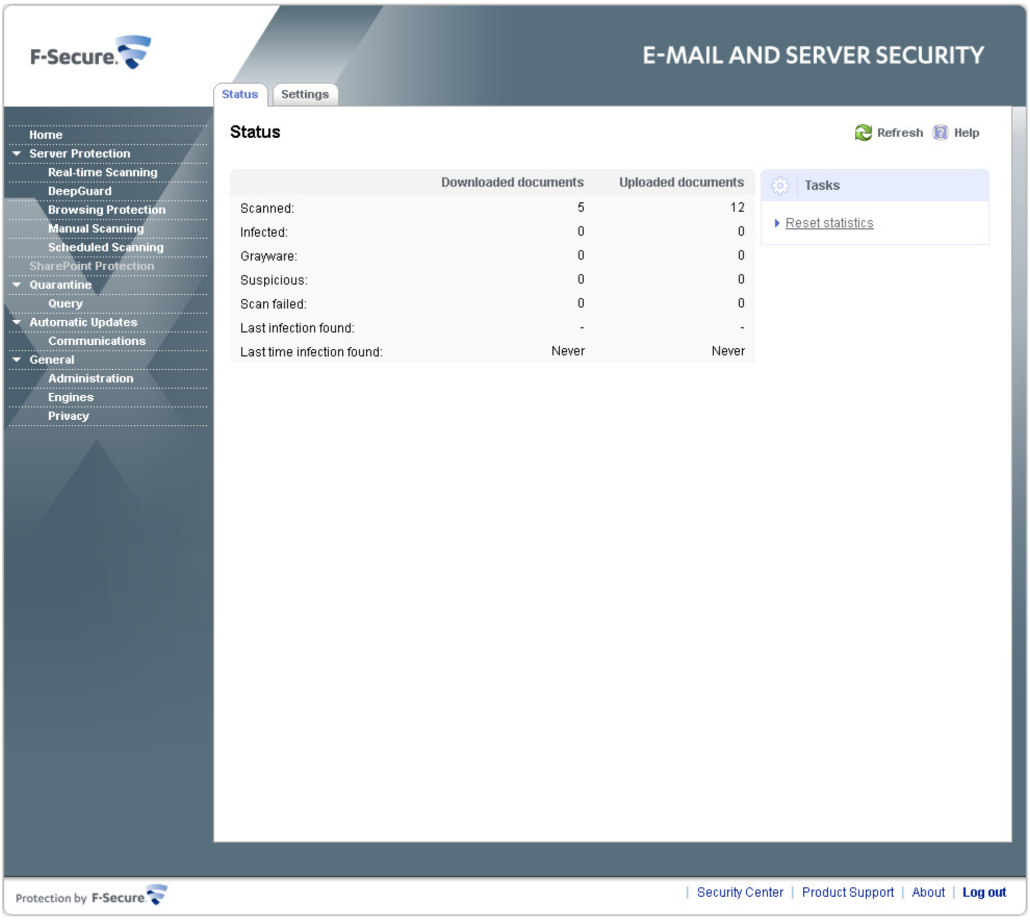
To install missing updates:

1. Go to **Server Protection** > **Software Updater** > **Install**.
   The missing updates list shows Each entry on the list includes the software in question, category, ID and description for the update.
2. Select the updates that you want to install.
3. Click **Install**.
   The product starts to download selected updates immediately.
4. After updates have been downloaded, the product installs downloaded updates.
5. Reboot the computer if the product instructs you to do so.

   Some updates require that you reboot the computer to complete the installation. The product does not force the computer to reboot, but shows the notification about the reboot when it is needed. You should reboot the computer as soon as possible.

5.3 SharePoint Protection

SharePoint Protection scans the content that is uploaded and downloaded from the SharePoint server.



Status

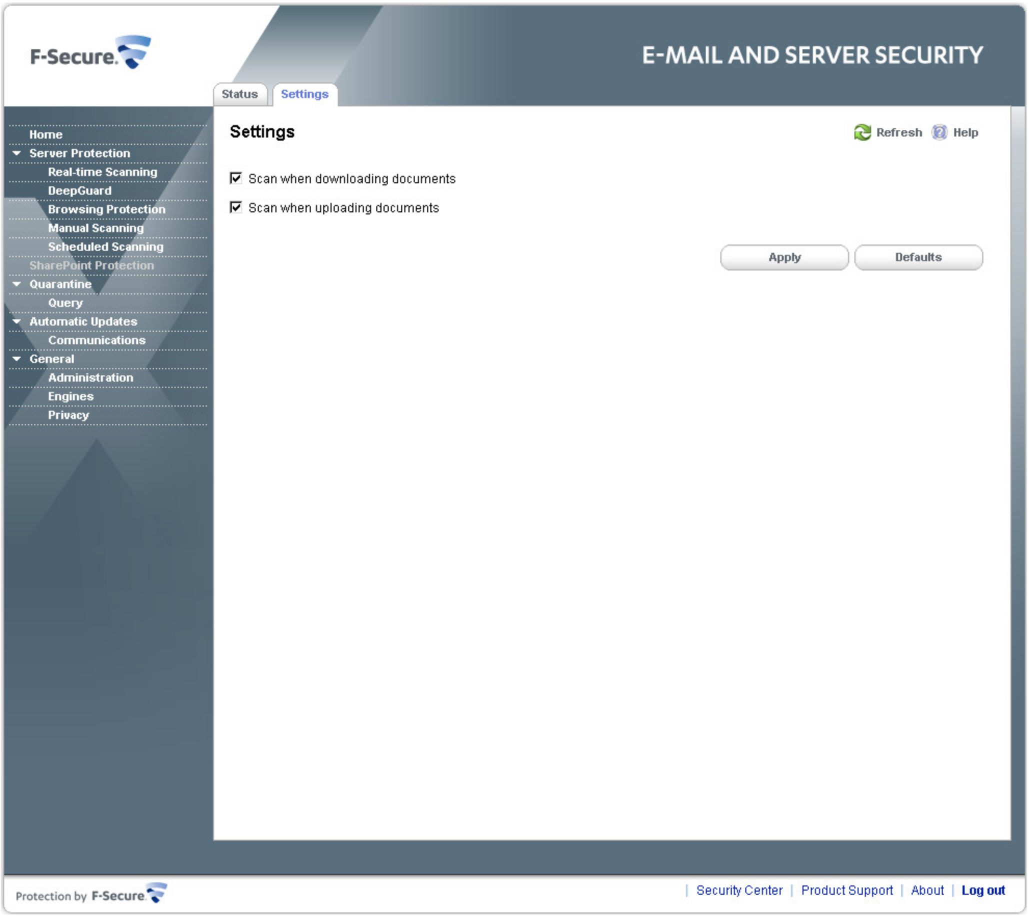
	Downloaded documents	Uploaded documents
Scanned:	5	12
Infected:	0	0
Grayware:	0	0
Suspicious:	0	0
Scan failed:	0	0
Last infection found:	-	-
Last time infection found:	Never	Never

By default, SharePoint Protection scans all uploaded and downloaded content automatically so that harmful content is not stored and cannot spread in your Sharepoint repository.

The **Status** page displays a summary of the scanned and processed files.

5.3.1 Setting up SharePoint Protection

You can choose what content SharePoint Protection scans.



Settings

☑ Scan when downloading documents

☑ Scan when uploading documents

To change SharePoint Protection settings:

1. Go to **SharePoint Protection** > **Settings**.
2. Select **Scan when downloading documents** to scan all documents that are downloaded from the SharePoint server.
3. Select **Scan when uploading documents** to scan all documents that are uploaded to the SharePoint server.

5.4 Transport Protection

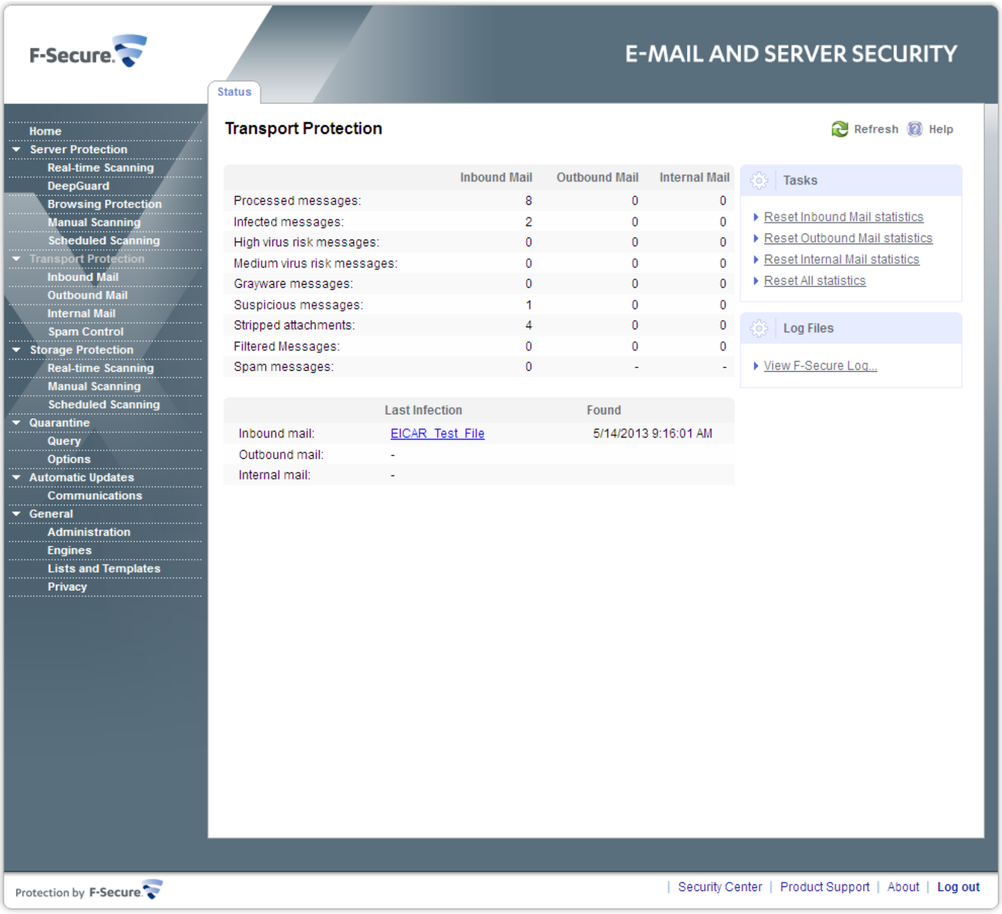
With Transport Protection, you can protect the e-mail traffic from malicious code on the transport level.

You can configure inbound, outbound and internal message protection separately. For more information about the mail direction and configuration options, see *Network Configuration*.

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.

Note: After you apply new transport protection settings, it can take up to 20 seconds for the new settings to take effect.

Status



Transport Protection

	Inbound Mail	Outbound Mail	Internal Mail
Processed messages:	8	0	0
Infected messages:	2	0	0
High virus risk messages:	0	0	0
Medium virus risk messages:	0	0	0
Grayware messages:	0	0	0
Suspicious messages:	1	0	0
Stripped attachments:	4	0	0
Filtered Messages:	0	0	0
Spam messages:	0	-	-

	Last Infection	Found
Inbound mail:	EICAR_Test_File	5/14/2013 9:16:01 AM
Outbound mail:	-	
Internal mail:	-	

The **Status** page displays a summary of the processed inbound, outbound and internal mail messages:

Processed messages

Displays the total number of processed messages since the last reset of statistics.

Infected messages

Displays the number of messages with attachments that are infected and cannot be automatically disinfected.

High & Medium virus risk messages

Displays the number of messages that have been identified as unsafe; messages that contain patterns that can be assumed to be a part of a virus outbreak.

Grayware messages

Displays the number of messages that have grayware items, including spyware, adware, dialers, joke programs, remote access tools and other unwanted applications.

Suspicious messages

Displays the number of suspicious content found, for example password-protected archives, nested archives and malformed messages.

Stripped attachments

Displays the number of filtered attachments.

Filtered messages

Displays the number of messages that have been found to contain disallowed keywords in the message subject or text.

Spam messages

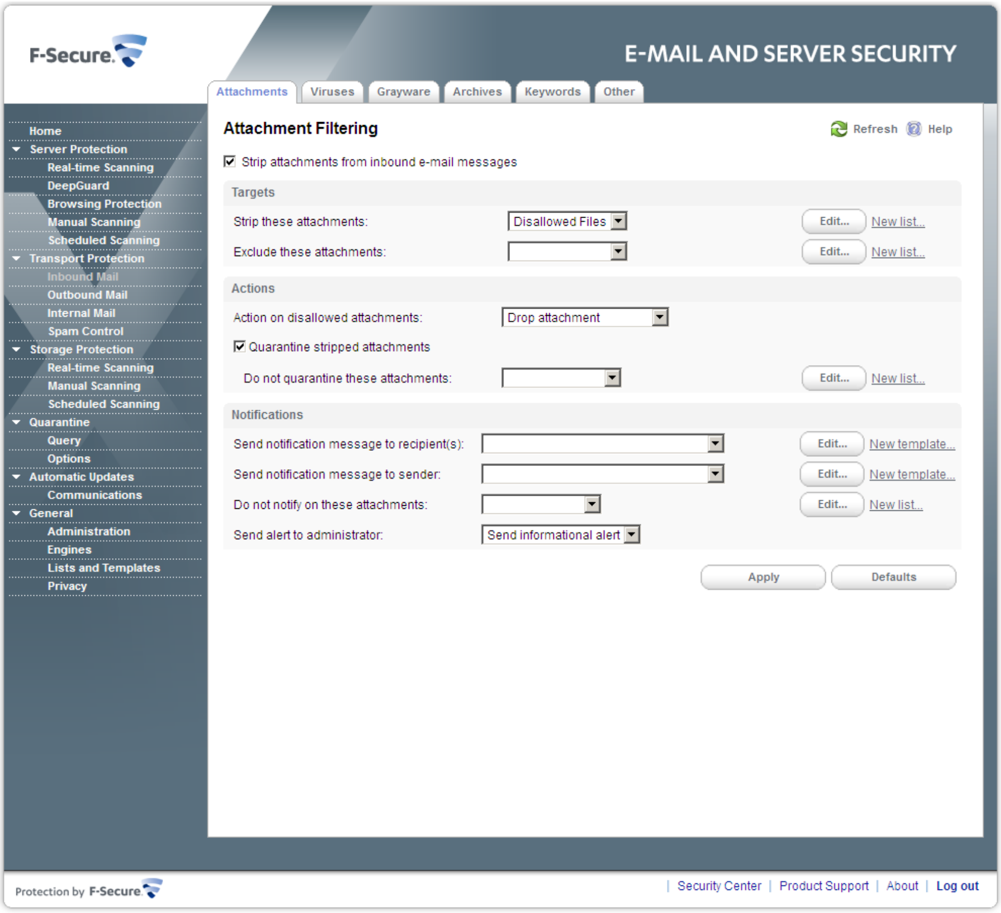
Displays the number of messages that are classified as spam.

Last Infections

Displays the name of the last infection found in inbound, outbound, and internal messages.

5.4.1 Attachment Filtering

Specify attachments to remove from inbound, outbound and internal messages based on the file name or the file extension.



Attachment Filtering

☑ Strip attachments from inbound e-mail messages

Targets

Strip these attachments: Disallowed Files

Exclude these attachments:

Actions

Action on disallowed attachments: Drop attachment

☑ Quarantine stripped attachments

Do not quarantine these attachments:

Notifications

Send notification message to recipient(s):

Send notification message to sender:

Do not notify on these attachments:

Send alert to administrator: Send informational alert

Strip attachments from e-mail messages

Enable or disable the attachment stripping.

Targets

Strip these attachments

Specify which attachments are stripped from messages. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.

Actions

Action on disallowed attachments

Specify how disallowed attachments are handled.

Drop Attachment - Remove the attachment from the message and deliver the message to the recipient without the disallowed attachment.

Drop the Whole Message - Do not deliver the message to the recipient at all.

Quarantine stripped attachments

Specify whether stripped attachments are quarantined.

Do not quarantine these attachments

Specify files which are not quarantined even when they are stripped. For more information, see *Match Lists*.

Notifications

Send notification message to recipient(s)

Specify whether recipients are notified when disallowed or suspicious attachment is found.

Note: The notification message is not sent if the whole message is dropped.

Send notification message to sender

Specify whether the original sender is notified when disallowed or suspicious attachment is found.

To enable the notification, select a template for the notification message. To disable the notification, leave the notification field empty.

For more information, see *Message Templates*.

Do not notify on these attachments

Specify attachments that do not generate notifications. When the product finds specified file or file extension, no notification is sent.

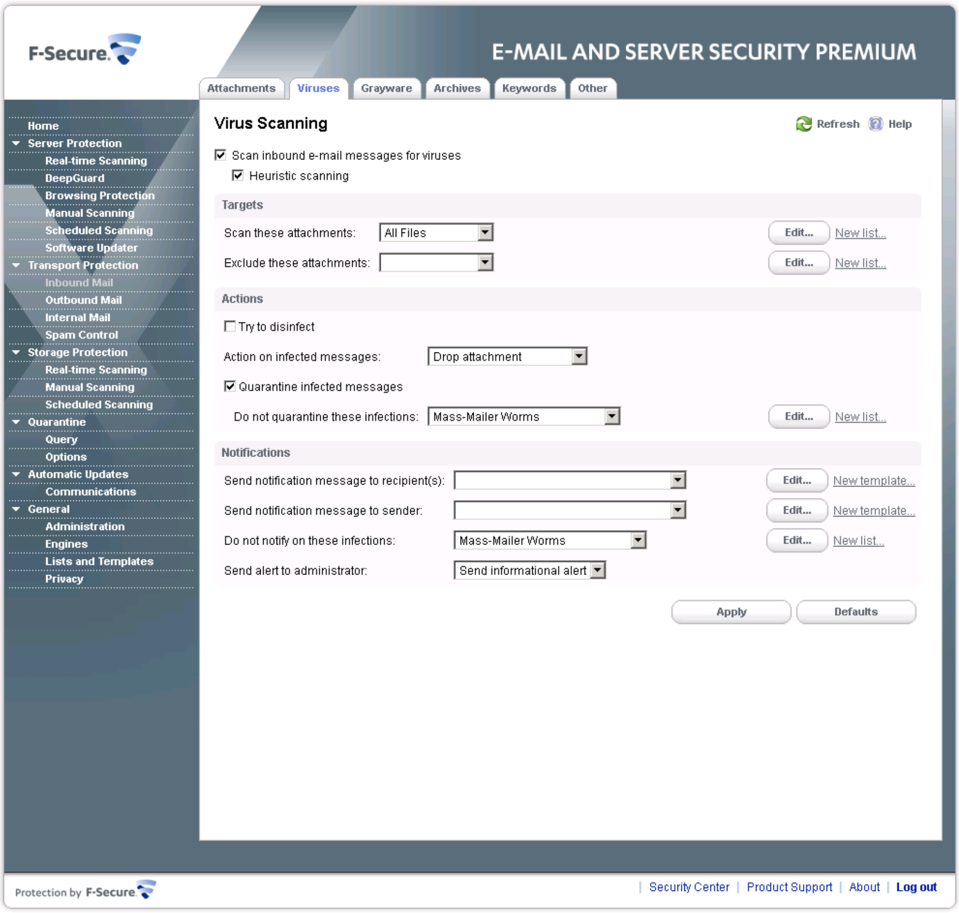
Send alert to administrator

Specify whether the administrator is notified when the product strips an attachment. If you enable the notification, specify the alert level of the notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

5.4.2 Virus Scanning

Specify inbound, outbound and internal messages and attachments that should be scanned for malicious code.



Virus Scanning

☑ Scan inbound e-mail messages for viruses

☑ Heuristic scanning

Targets

Scan these attachments: All Files

Exclude these attachments:

Actions

☐ Try to disinfect

Action on infected messages: Drop attachment

☑ Quarantine infected messages

Do not quarantine these infections: Mass-Mailer Worms

Notifications

Send notification message to recipient(s):

Send notification message to sender:

Do not notify on these infections: Mass-Mailer Worms

Send alert to administrator: Send informational alert

Note: Disabling virus scanning disables grayware scanning and archive processing as well.

Scan e-mail messages for viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

Heuristic Scanning

Enable or disable the heuristic scan. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

By default, the heuristic scan is enabled for inbound mails and disabled for outbound and internal mails.

Note: The heuristic scan may affect the product performance and increase the risk of false malware alarms.

Targets

Scan these attachments

Specify attachments that are scanned for viruses. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scanning.

Actions

Try to disinfect

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Action on infected messages

Specify whether infected messages are disinfected or dropped.

Drop Attachment - Remove the infected attachment from the message and deliver the message to the recipient without the attachment.

Drop the Whole Message - Do not deliver the message to the recipient at all.

Quarantine infected messages

Specify whether infected or suspicious messages are quarantined.

Do not quarantine these infections

Specify infections that are never placed in the quarantine. For more information, see *Match Lists*.

Notifications

Send notification message to recipient(s)

Specify whether recipients are notified when a virus or other malicious code is found.

Note: The notification message is not sent if the whole message is dropped.

Send notification message to sender

Specify whether the original sender is notified when a virus or other malicious code is found.

To enable the notification, select a template for the notification message. To disable the notification, leave the notification field empty.

For more information, see *Message Templates*.

Do not notify on these infections

Specify infections that do not generate notifications. When the product finds the specified infection, no notification is sent.

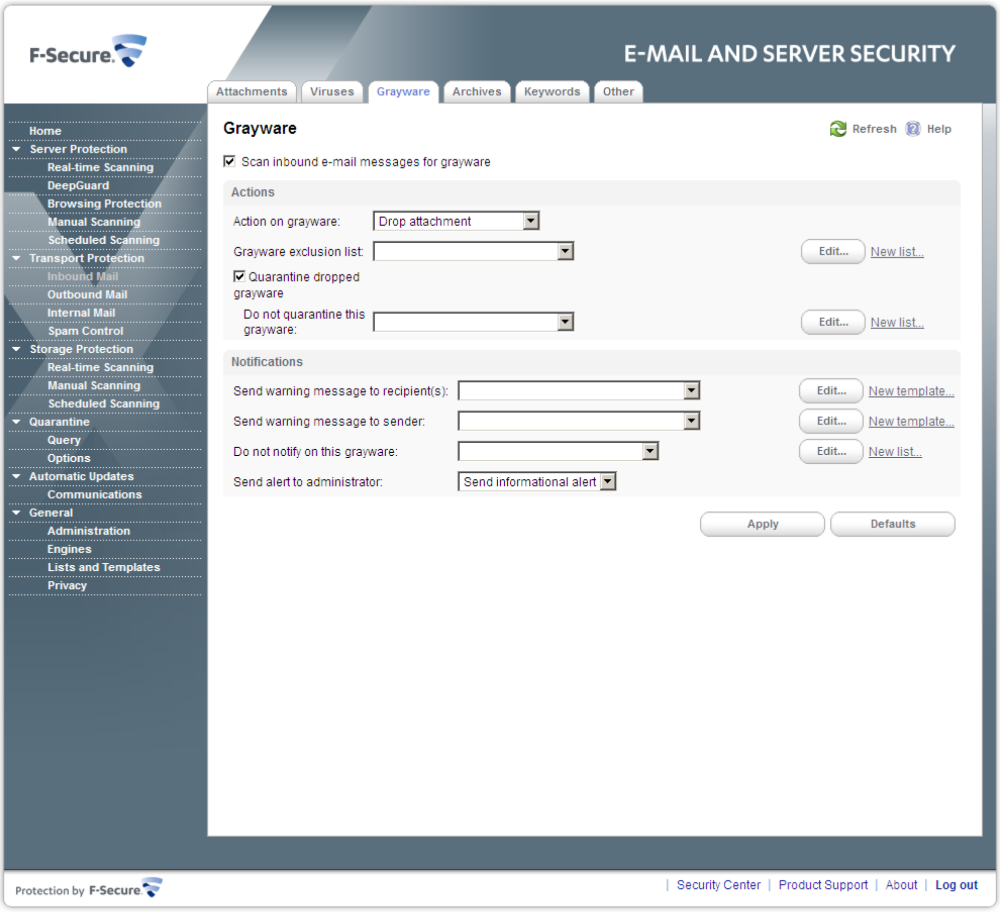
Send alert to administrator

Specify whether the administrator is notified when the product finds a virus in a message.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

5.4.3 Grayware Scanning

Specify how the product processes grayware items in inbound, outbound and internal messages.



Grayware

☑ Scan inbound e-mail messages for grayware

Actions

Action on grayware: Drop attachment

Grayware exclusion list:

☑ Quarantine dropped grayware

Do not quarantine this grayware:

Notifications

Send warning message to recipient(s):

Send warning message to sender:

Do not notify on this grayware:

Send alert to administrator: Send informational alert

Note that grayware scanning increases the scanning overhead. By default, grayware scanning is enabled for inbound messages only.

Note: Grayware scanning is disabled when virus scanning is disabled.

Scan e-mail messages for grayware

Enable or disable the grayware scan.

Actions

Action on grayware

Specify the action to take on items which contain grayware.

Pass through - Leave grayware items in the message.

Drop attachment - Remove grayware items from the message.

Drop the whole message - Do not deliver the message to the recipient.

Grayware exclusion list

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan. For more information, see *Match Lists*.

Quarantine dropped grayware

Specify whether grayware attachments are quarantined when dropped.

Do not quarantine this grayware

Specify grayware that are never placed in the quarantine. For more information, see *Match Lists*.

Notifications

Send warning message to recipient(s)

Specify the template for the notification message that is sent to the intended recipient when a grayware item is found in a message.

Note: Note that the notification message is not sent if the whole message is dropped.

Send warning message to sender

Specify the template for the notification message that is sent to the original sender of the message when a grayware item is found in a message.

Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.

For more information, see *Message Templates*.

Do not notify on this grayware

Specify a list of keywords for grayware types on which no notifications are sent.

If the product finds a grayware item with a name that matches the keyword, the recipient and the sender are not notified about the grayware item found.

Leave the list empty if you do not want to exclude any grayware types from notifications.

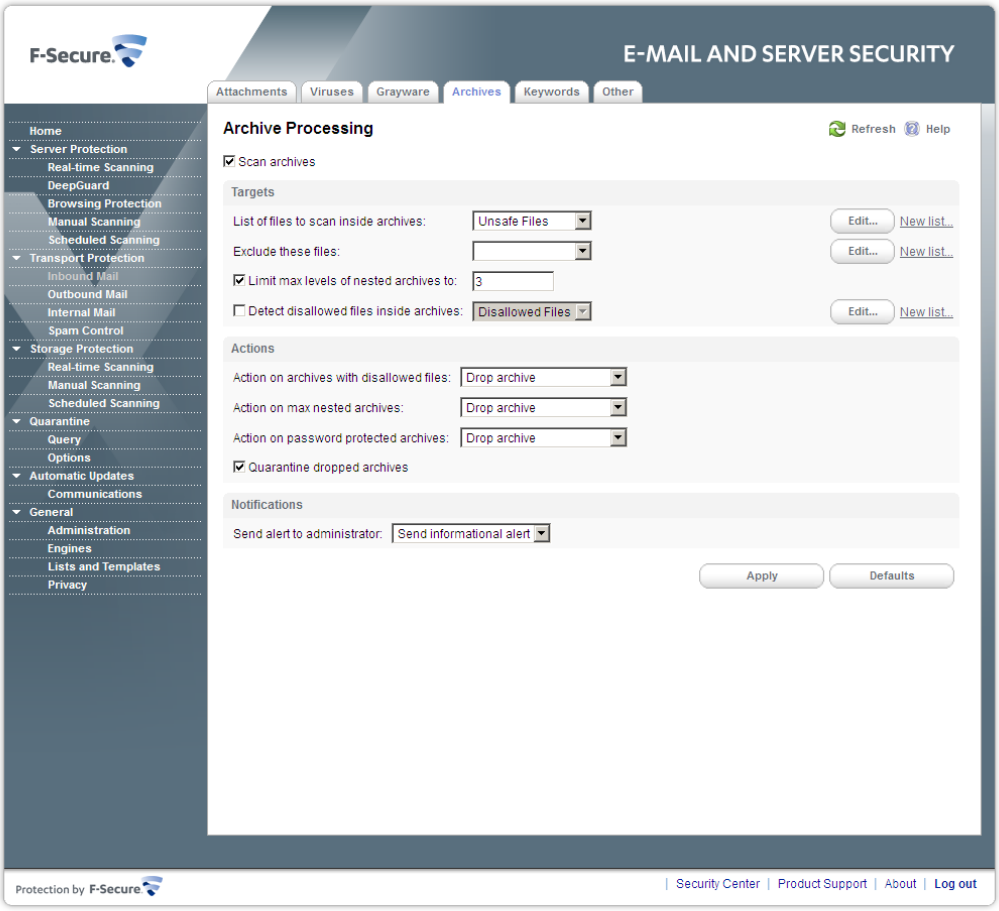
Send alert to administrator

Specify whether the administrator is notified when the product finds a grayware item in a message.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

5.4.4 Archive Processing

Specify how F-Secure Anti-Virus processes the product processes archived attachments in inbound, outbound, and internal messages.



Archive Processing

☑ Scan archives

Targets

List of files to scan inside archives: Unsafe Files

Exclude these files:

☑ Limit max levels of nested archives to: 3

☐ Detect disallowed files inside archives: Disallowed Files

Actions

Action on archives with disallowed files: Drop archive

Action on max nested archives: Drop archive

Action on password protected archives: Drop archive

☑ Quarantine dropped archives

Notifications

Send alert to administrator: Send informational alert

Note that scanning inside archives takes time. Disabling scanning inside archives improves performance, but it also means that the network users need to use up-to-date virus protection on their workstations.

Note: Archive processing is disabled when the virus scanning is disabled.

Scan archives

Specify whether files inside compressed archive files are scanned for viruses.

Targets

List of files to scan inside archives

Specify files inside archives that are scanned for viruses. For more information, see *Match Lists*.

Exclude these files

Specify files that are not scanned inside archives. Leave the list empty if you do not want to exclude any files from the scanning.

Limit max levels of nested archives

Specify how many levels of archives inside other archives the product scans when **Scan Viruses Inside Archives** is enabled.

Detect disallowed files inside archives

Specify files which are not allowed inside archives. For more information, see *Match Lists*.

Actions

Action on archives with disallowed files

Specify the action to take on archives which contain disallowed files.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without it.

Drop the whole message - Do not deliver the message to the recipient.

Action on max nested archives

Specify the action to take on archives with nesting levels exceeding the upper level specified in the **Limit max levels of nested archives** setting.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without it.

Drop the whole message - Do not deliver the message to the recipient.

Action on password protected archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Deliver the message with the password protected archive to the recipient.

Drop archive - Remove the password protected archive from the message and deliver the message to the recipient without it.

Drop the whole message - Do not deliver the message to the recipient.

The default value is **Drop archive** for inbound and outbound mail, and **Pass through** for internal mail.

Quarantine dropped archives

Specify whether archives that are not delivered to recipients are quarantined.

Notifications

Send alert to administrator

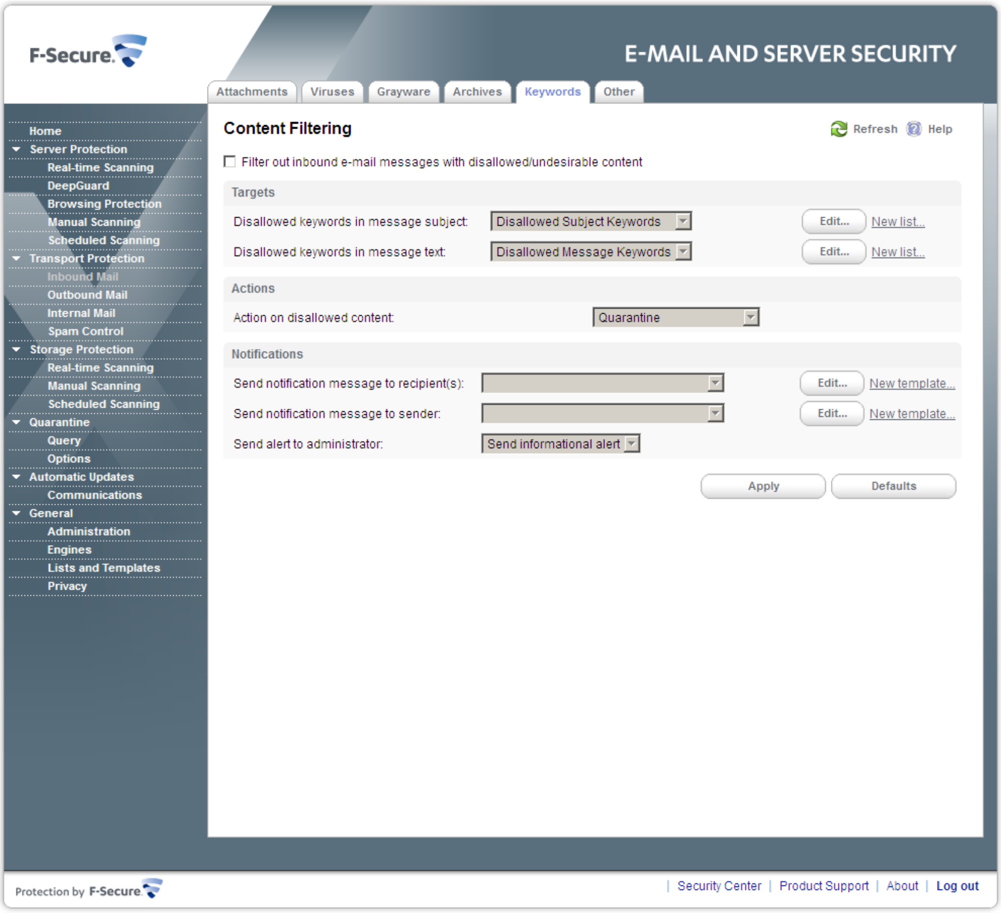
Specify whether the administrator is notified when the product blocks a suspicious overnested or password protected archive file.

Note: If the archive is blocked because it contains malware, grayware or disallowed files, the administrator receives a notification about that instead of this notification.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

5.4.5 Content Filtering

Specify how the product filters disallowed content in inbound, outbound and internal messages.



Content Filtering

□ Filter out inbound e-mail messages with disallowed/undesirable content

Targets

Disallowed keywords in message subject: Disallowed Subject Keywords

Disallowed keywords in message text: Disallowed Message Keywords

Actions

Action on disallowed content: Quarantine

Notifications

Send notification message to recipient(s):

Send notification message to sender:

Send alert to administrator: Send informational alert

Filter out e-mail messages with disallowed/undesirable content

Specify whether e-mail messages are scanned for disallowed content.

Targets

Disallowed keywords in message subject

Specify the list of disallowed keywords to check in e-mail message subjects. For more information, see *Using Keywords in Content Filtering*.

Disallowed keywords in message text

Specify the list of disallowed keywords to check in e-mail message text. For more information, see *Using Keywords in Content Filtering*.

Actions

Action on disallowed content

Specify the action to take on messages which contain disallowed keywords.

Report only - Deliver the message to the recipient and notify the administrator that the scanned message contained disallowed content.

Drop the whole message - Do not deliver the message to the recipient.

Quarantine - Quarantine the message with disallowed content.

Notifications

Send notification message to recipient(s)

Specify whether recipients are notified when disallowed content is found.

Send notification message to sender

Specify whether the original sender is notified when disallowed content is found.

To enable the notification, select a template for the notification message. To disable the notification, leave the notification field empty.

For more information, see *Message Templates*.

Send alert to administrator

Specify whether the administrator is notified when the product finds a message with disallowed content.

Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

Using Keywords in Content Filtering

When the content filtering is enabled, all messages are checked against every keyword sequence that is specified in the selected list of keywords.

A keyword may contain any characters, including punctuation symbols, spaces, and other word separators. Keywords are case insensitive.

You can use ‘?’ character in a keyword to match any character in that position in the keyword and ‘*’ to match any number of characters.

Keyword examples:

example	Matches any message text or subject that contains the word ‘example’.

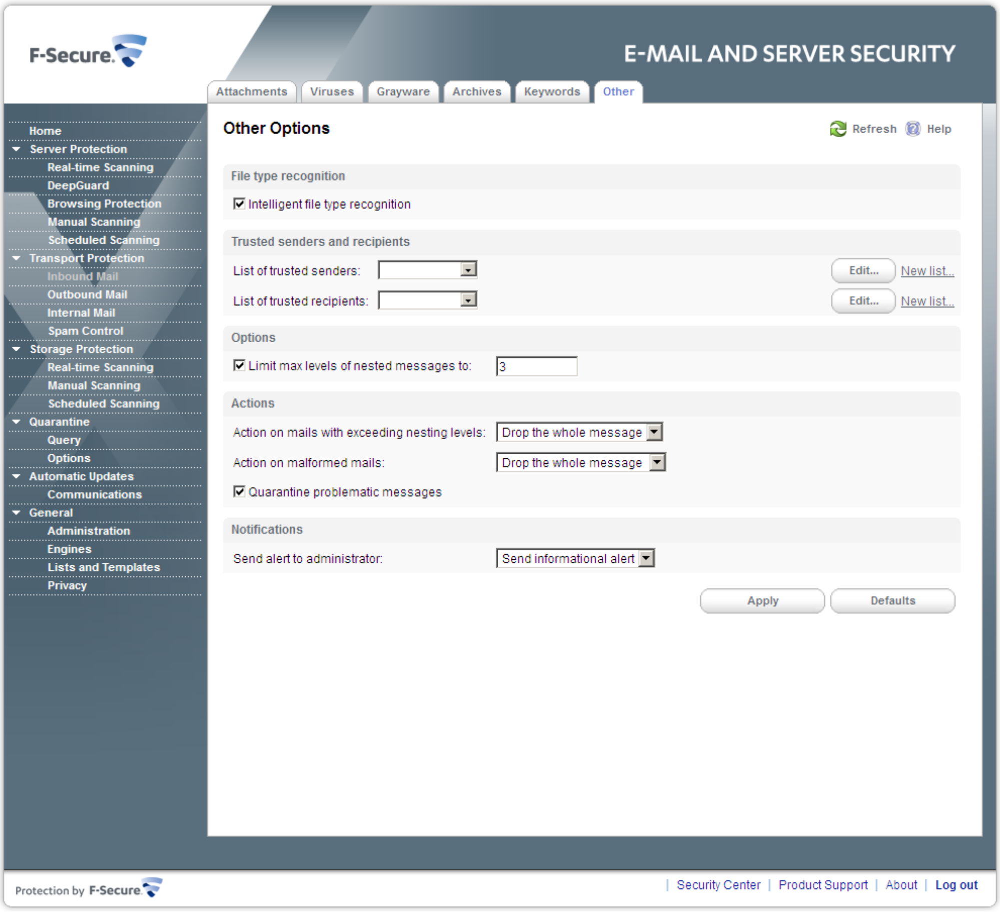
another example	Matches any message text or subject that contains the ‘another example’ text. Words ‘another’ and ‘example’ have to be separated with exactly one space character.
co?p?rate	Matches any message text or subject that contains - for example - words ‘corporate’ or ‘cooperate’.
another*example	Matches any message text or subject that contains words ‘another’ and ‘example’ separated with any number of characters. For example, ‘another example’ or ‘another keyword example’.

To represent ‘?’ or ‘*’ characters themselves in keywords, use ‘\?’ and ‘*’ sequences correspondingly. To represent ‘\’ character, use ‘\\’.

For example, to match the '*** SPAM ***' string, enter '*** spam ***'.

5.4.6 Other Options

Configure other options to limit actions on malformed and problematic messages.



Other Options

File type recognition

☑ Intelligent file type recognition

Trusted senders and recipients

List of trusted senders:

List of trusted recipients:

Options

☑ Limit max levels of nested messages to: 3

Actions

Action on mails with exceeding nesting levels: Drop the whole message

Action on malformed mails: Drop the whole message

☑ Quarantine problematic messages

Notifications

Send alert to administrator: Send informational alert

File type recognition	

Intelligent file type recognition

Select whether you want to use the intelligent file type recognition or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. The intelligent file type recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using the intelligent file type recognition strengthens the security, but can degrade the system performance.

Trusted senders and recipients

List of trusted senders

Specify senders who are excluded from the mail scanning and processing.

List of trusted recipients

Specify recipients who are excluded from the mail scanning and processing.

For more information, see *Match Lists*.

Mail disclaimer

Specify whether you want to add a disclaimer to all outbound messages.

Click **Edit disclaimer** to edit the disclaimer text.

Note: Mail disclaimer is available only for outbound messages.

Note: Some malware add disclaimers to infected messages, so disclaimers should not be used for stating that the message is clean of malware.

Options

Limit max levels of nested messages

Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.

Note: It is not recommended to set the maximum nesting level to unlimited as this will make the product more vulnerable to DoS (Denial-of-Service) attacks.

Actions

Action on mails with exceeding nesting levels

Specify the action to take on messages with nesting levels exceeding the upper level specified in the **Limit max levels of nested messages** setting.

Drop the Whole Message - Messages with exceeding nesting levels are not delivered to the recipient.

Pass Through - Nested messages are scanned up to level specified in the **Limit max levels of nested messages** setting. Exceeding nesting levels are not scanned, but the message is delivered to the recipient.

Action on malformed mails

Specify the action for non-RFC compliant e-mails. If the message has an incorrect structure, the product cannot parse the message reliably.

Drop the Whole Message - Do not deliver the message to the recipient.

Pass Through - The product allows the message to pass through.

Pass Through and Report - The product allows the message to pass through, but sends a report to the administrator.

Quarantine problematic messages

Specify if mails that contain malformed or broken attachments are quarantined for later analysis or recovery.

Mail disclaimer

Add disclaimer to processed messages

Specify whether you want to add a disclaimer to all outbound messages. Click **Edit Disclaimer** to specify the text of disclaimer that is added at the end of the messages.

The setting is available for outbound messages only.

Important:

Some malware add disclaimers to infected messages, so disclaimers should not be used for stating that the message is clean of malware.

Notifications

Send alert to administrator

Specify whether the administrator is notified when the product detects a malformed or a suspicious e-mail message.

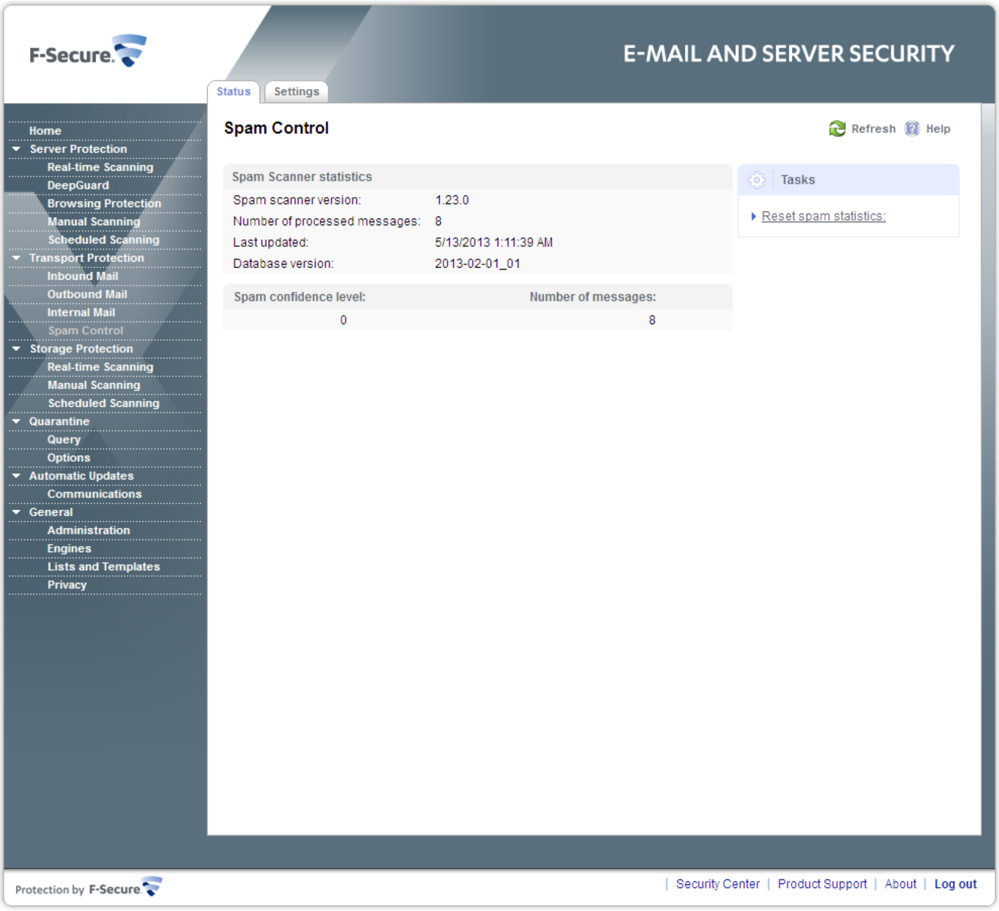
Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

5.5 Spam Control

The threat detection engine can identify spam and virus patterns from the message envelope, headers and body during the first minutes of the new spam of virus outbreak.

Note: You can configure Spam Control settings for inbound messages, and only if you have F-Secure Spam Control installed.

Status



Spam Control

Spam Scanner statistics

Spam scanner version:	1.23.0
Number of processed messages:	8
Last updated:	5/13/2013 1:11:39 AM
Database version:	2013-02-01_01

Spam confidence level:	Number of messages:
0	8

The **Status** page displays the statistics of the spam scanner:

Spam scanner version

Displays the version number of the installed spam scanner.

Number of processed messages

Displays the total number of processed messages since the last reset of statistics.

Last updated

Displays the date and time when the latest spam definition update was retrieved.

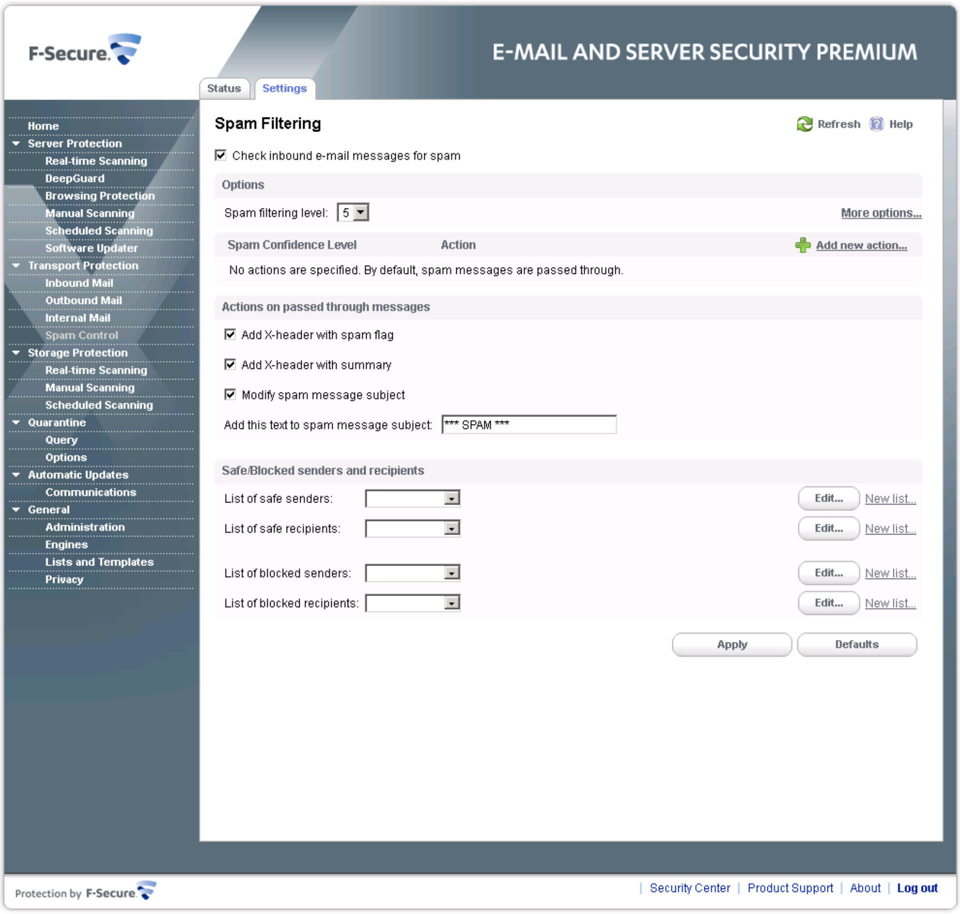
Database version

Displays the version of the installed spam definition database.

Spam confidence level / number of messages	Displays the number of messages found with specified spam confidence levels.

5.5.1 Settings

Specify how the product processes inbound spam messages.



Spam Filtering

☑ Check inbound e-mail messages for spam

Options

Spam filtering level: 5

Spam Confidence Level	Action
No actions are specified. By default, spam messages are passed through.	

Actions on passed through messages

☑ Add X-header with spam flag

☑ Add X-header with summary

☑ Modify spam message subject

Add this text to spam message subject: *** SPAM ***

Safe/Blocked senders and recipients

List of safe senders:

List of safe recipients:

List of blocked senders:

List of blocked recipients:

These settings are used only if F-Secure Spam Control is installed with the product, otherwise these settings are not available.

Check inbound e-mail messages for spam	Specify whether inbound mails are scanned for spam.

Options

Spam filtering level	Specify the spam filtering level. Decreasing the level allows less spam to pass, but more regular mails may be falsely identified as spam. Increasing the level allows more spam to pass, but a smaller number of regular e-mail messages are falsely identified as spam. For example, if the spam filtering level is set to 3, more spam is filtered, but also more regular mails may be falsely identified as spam. If the spam filtering level is set to 7, more spam may pass

undetected, but a smaller number of regular mails will be falsely identified as spam.

The allowed values are from 0 to 9.

Click **More options** to configure advanced spam filtering options:

Max message size - Specify the maximum size (in kilobytes) of messages to be scanned for spam. If the size of the message exceeds the maximum size, the message is not filtered for spam.

Forward spam messages to e-mail address - Specify the e-mail address where messages considered as spam are forwarded when the **Action** on spam messages setting is set to **Forward**.

Spam confidence level

Click **Add new action** to add a new action for messages with the spam level above the specified Spam Filtering Level.

Specify the spam level and select action to take:

`Quarantine` - Place the message into the quarantine folder.

Forward - Forward the message to the specified e-mail address.

`Delete` - Delete the message.

Actions on passed through messages

Add X-header with spam flag

Specify if a spam flag is added to the mail as the X-Spam-Flag header in the following format:`X-Spam-Flag:<flag>`

where `<flag>` is `YES` or `NO`.

Add X-header with summary

Specify if the summary of triggered hits is added to the mail as X-Spam-Status header in the following format:`X-Spam-Status: <flag>, hits=<scr> required=<sfl> tests=<tests>`

where

- `<flag>` is `Yes` or `No`.
- `<scr>` is the spam confidence rating returned by the spam scanner,
- `<sfl>` is the current spam filtering level,
- `<tests>` is the comma-separated list of tests run against the mail.

Modify spam message subject

Specify if the product modifies the subject of mail messages considered as spam.

Add this text to spam message subject

Specify the text that is added in the beginning of the subject of messages considered as spam.

	By default, the text is: *** **SPAM** ***.
Safe/Blocked senders and recipients	
List of safe senders	Specify safe senders. Messages originating from the specified addresses are never treated as spam.
List of safe recipients	Specify safe recipients. Messages sent to the specified addresses are never treated as spam.
List of blocked senders	Specify blocked senders. Messages originating from the specified addresses are always treated as spam.
List of blocked recipients	Specify blocked recipients. Messages sent to the specified addresses are always treated as spam. **Note:** The product checks the sender address from the SMTP message envelope, not from the message headers.

To use the spam detection engine, you need to make the following change to your firewall rules:

- Permit **outbound** HTTPS connections to **aspam.sp.f-secure.com** (TCP port 443)

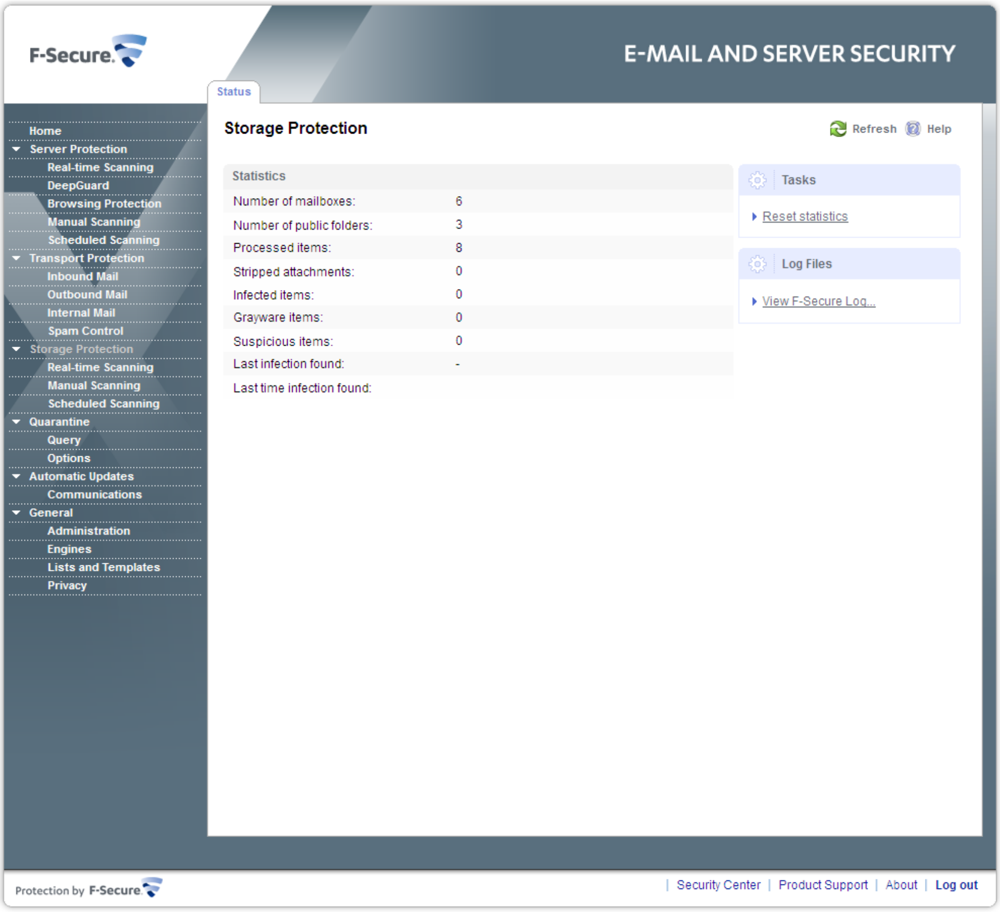
Note: Alternatively, you can use a CONNECT-capable HTTPS proxy instead of changing the firewall rules.

5.6 Storage Protection

Configure Storage Protection settings to specify how e-mail messages and attachments in selected mailboxes and public folders should be scanned.

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.

Status



Storage Protection

Statistics	
Number of mailboxes:	6
Number of public folders:	3
Processed items:	8
Stripped attachments:	0
Infected items:	0
Grayware items:	0
Suspicious items:	0
Last infection found:	-
Last time infection found:	

The **Status** page displays a summary of the protected mailboxes and public folders and infections found.

Number of mailboxes

Displays the number of currently protected user mailboxes.

Number of public folders

Displays the number of currently protected public folders.

Processed items

Displays the total number of processed items since the last reset of statistics.

Stripped attachments

Displays the number of attachments filtered based of their file name or the file extension.

Infected items

Displays the number of items that are infected and cannot be automatically disinfected.

Grayware items

Displays the number of grayware items, including spyware, adware, dialers, joke programs, remote access tools and other unwanted applications.

Suspicious items

Displays the number of suspicious content found, for example password-protected archives and nested archives.

Last infection found

Displays the name of the last infection found.

Last time infection found

Displays the time when the last infection was found.

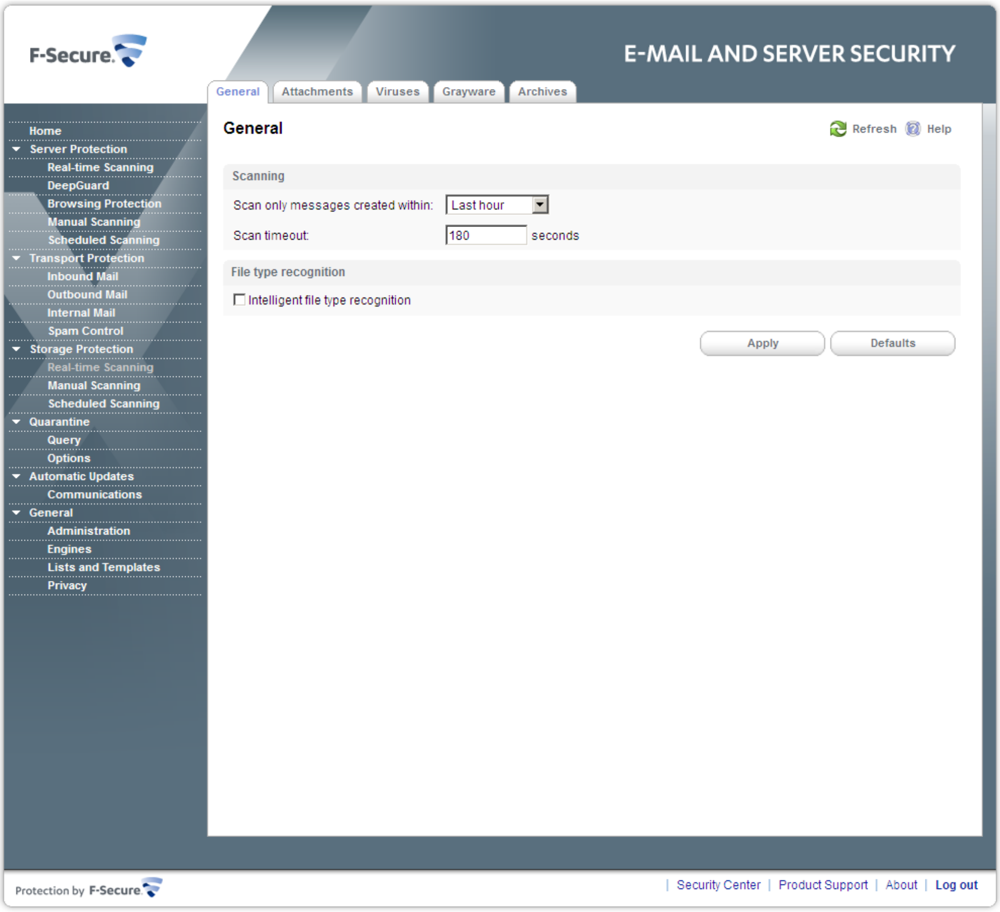
5.6.1 Real-Time Scanning

The real-time scanning can automatically scan messages that have been created or received.

Note: The real-time scanning of mailboxes and public folders is not supported in Microsoft Exchange Server 2013.

5.6.1.1 General

Real-time scanning scans messages in mailboxes and public folders for viruses.



General

Scanning

Scan only messages created within: Last hour

Scan timeout: 180 seconds

File type recognition

☐ Intelligent file type recognition

Scanning

Scan only messages created within

Specify which messages are scanned with the real-time scanning, for example; **Last hour**. **Last day**. **Last week**. Messages that have been created before the specified time are not scanned.

Note: This setting is not available with Microsoft Exchange Server 2003.

Scan timeout

Specify how long to wait for the real-time scan result. After the specified time, the client that tries to access the scanned message gets the "virus scanning in progress" notification.

File Type Recognition

Intelligent file type recognition

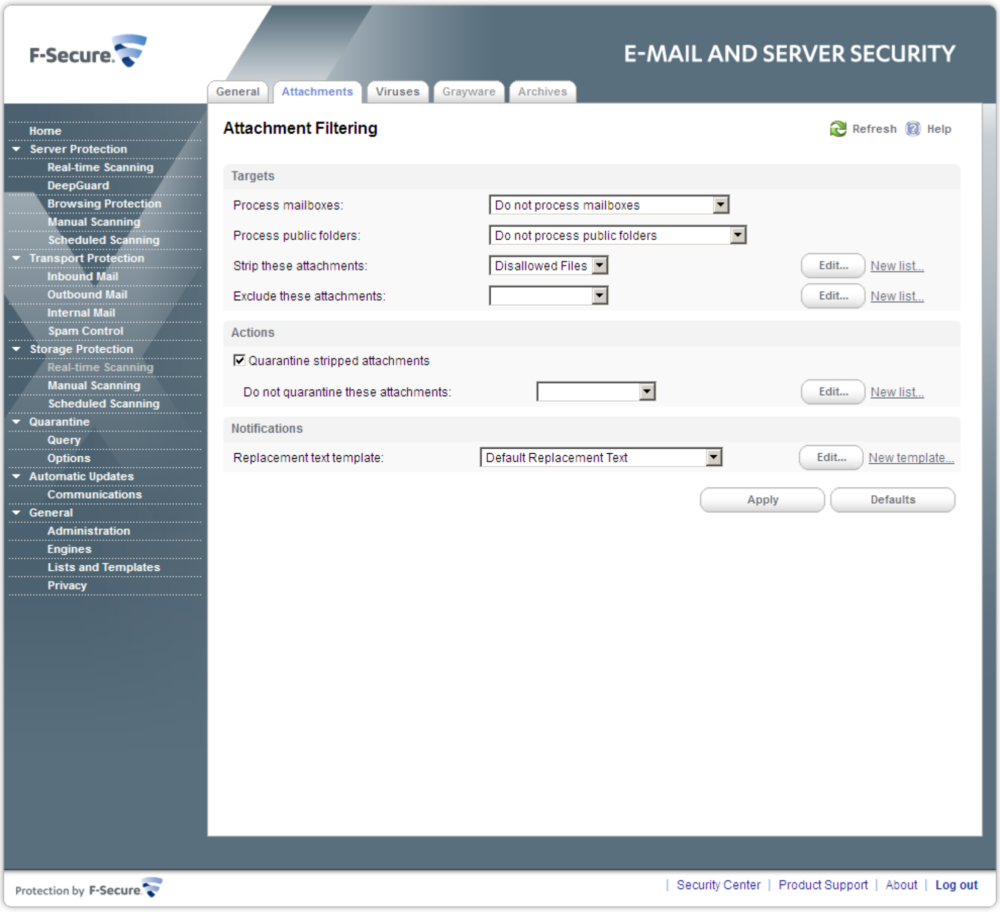
Select whether you want to use the intelligent file type recognition or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. The intelligent file type recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using the intelligent file type recognition strengthens the security, but can degrade the system performance.

5.6.1.2 Attachment Filtering

Attachment filtering can remove attachments from messages in the Microsoft Exchange Storage based on the file name or the file extension of the attachment.



Attachment Filtering

Targets

Process mailboxes: Do not process mailboxes

Process public folders: Do not process public folders

Strip these attachments: Disallowed Files

Exclude these attachments:

Actions

☑ Quarantine stripped attachments

Do not quarantine these attachments:

Notifications

Replacement text template: Default Replacement Text

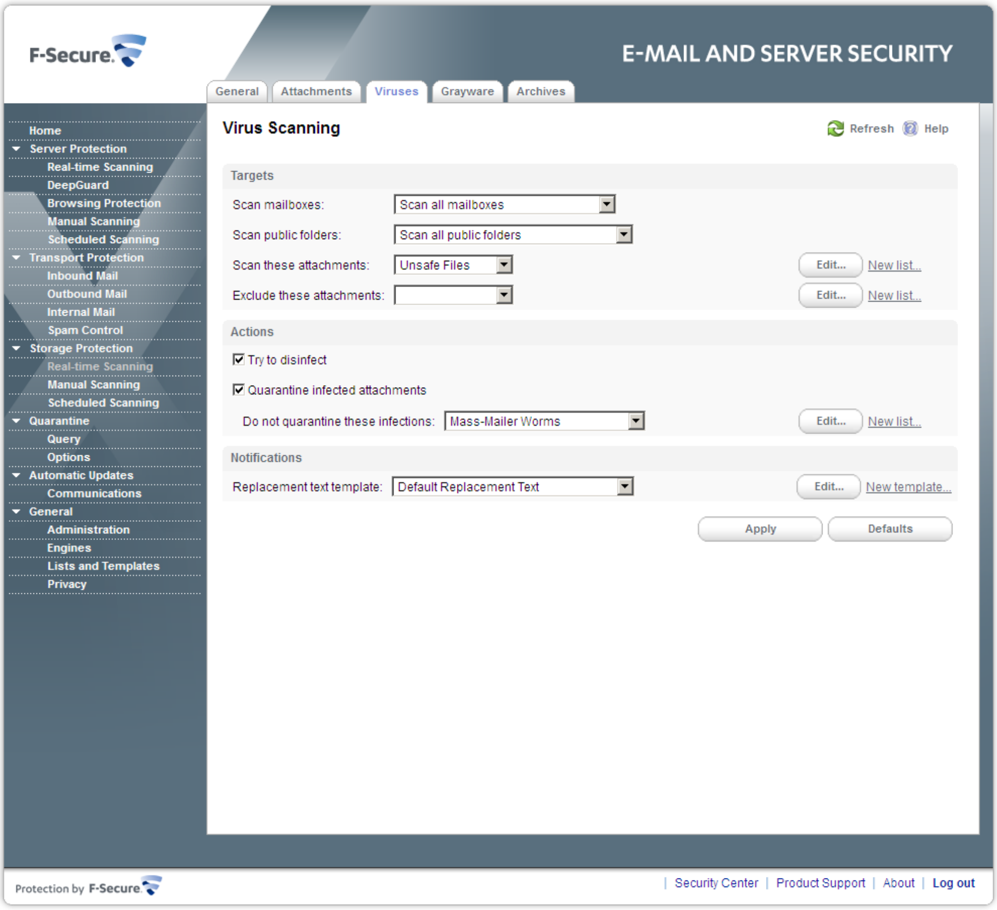
Targets	
Process Mailboxes	Specify mailboxes that are filtered for attachments. **Do not process mailboxes** - Do not filter any mailboxes for attachments. **Process all mailboxes** - Filter attachments in all mailboxes. **Process only included mailboxes** - Filter attachments in specified mailboxes only. Click **Edit** to add or remove mailboxes that are processed. **Process all except excluded mailboxes** - Do not filter attachments in specified mailboxes but process all other mailboxes. Click **Edit** to add or remove mailboxes that should not be processed.
Process Public Folders	Specify public folders that are filtered for attachments. **Do not process public folders** - Do not filter any public folders for attachments. **Process all public folders** - Filter attachments in all public folders. **Process only included public folders** - Filter attachments in specified public folders only. Click **Edit** to add or remove public folders that are processed. **Process all except excluded public folders** - Do not filter attachments in specified public folders but process all other public folders. Click **Edit** to add or remove public folders that should not be processed.
Strip these attachments	Specify which attachments are removed from messages. For more information, see *Match Lists*.
Exclude these attachments	Specify attachments that are not removed from messages even if they match to the match list rule. Leave the list empty if you do not want to exclude any attachments from filtering.
Actions	
Quarantine stripped attachments	Specify whether stripped attachments are quarantined.
Do not quarantine these attachments	Specify attachments which are not quarantined even when they are stripped. For more information, see *Match Lists*.

Notifications

Replacement text template	Specify the template for the text that replaces the suspicious or disallowed attachment when the attachment is removed from the message. For more information, see *Message Templates*.

5.6.1.3 Virus Scanning

Specify messages and attachments in the Microsoft Exchange Storage that should be scanned for malicious code.



Virus Scanning

Targets

Scan mailboxes: Scan all mailboxes

Scan public folders: Scan all public folders

Scan these attachments: Unsafe Files

Exclude these attachments:

Actions

☑ Try to disinfect

☑ Quarantine infected attachments

Do not quarantine these infections: Mass-Mailer Worms

Notifications

Replacement text template: Default Replacement Text

Targets

Scan mailboxes	Specify mailboxes that are scanned for viruses. **Do not scan mailboxes** - Disable the mailbox scanning. **Scan all mailboxes** - Scan all mailboxes. **Scan only included mailboxes** - Scan all specified mailboxes. Click **Edit** to add or remove mailboxes that should be scanned. **Scan all except excluded mailboxes** - Do not scan specified mailboxes but scan all other. Click **Edit** to

add or remove mailboxes that should not be scanned.

Scan public folders

Specify public folders that are scanned for viruses.

Do not scan public folders - Disable the public folder scanning.

Scan all folders - Scan all public folders.

Scan only included public folders - Scan all specified public folders. Click **Edit** to add or remove public folders that should be scanned.

Scan all except excluded public folders - Do not scan specified public folders but scan all other. Click **Edit** to add or remove public folders that should not be scanned.

Important:

You need to specify Administrator's mailbox setting to list and scan public folders on Microsoft Exchange 2010 platform. For more information, see *General*.

Scan these attachments

Specify attachments that are scanned for viruses. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scanning.

Actions

Try to disinfect

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine infected attachments

Specify whether infected attachments are quarantined.

Do not quarantine these infections

Specify virus and malware infections that are never placed in the quarantine. For more information, see *Match Lists*.

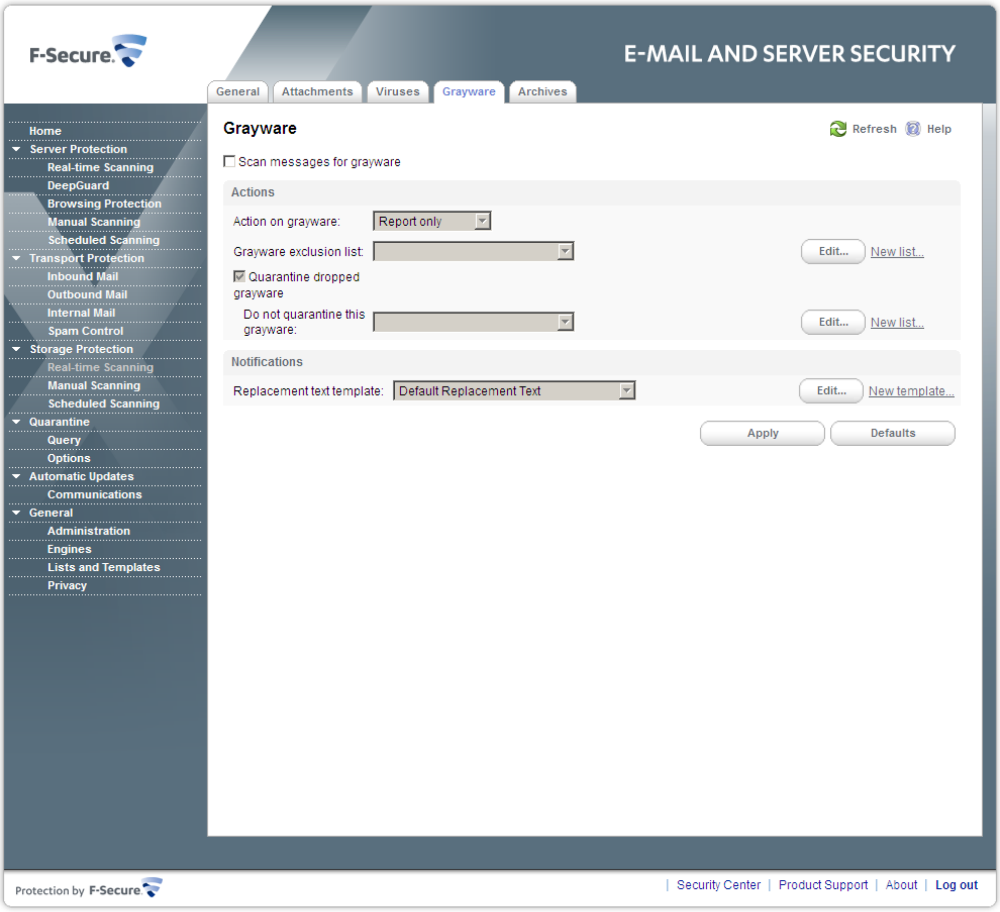
Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Message Templates*.

5.6.1.4 Grayware Scanning

Specify how the product processes grayware items during real-time mail storage scanning.



Grayware

□ Scan messages for grayware

Actions

Action on grayware: Report only

Grayware exclusion list:

☑ Quarantine dropped grayware

Do not quarantine this grayware:

Notifications

Replacement text template: Default Replacement Text

Scan messages for grayware

Enable or disable the grayware scan.

Actions

Action on grayware

Specify the action to take on items which contain grayware.

Report only - Leave grayware items in the message and notify the administrator.

Drop attachment - Remove grayware items from the message.

Grayware exclusion list

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan. For more information, see *Match Lists*.

Quarantine dropped grayware

Specify whether grayware attachments are quarantined when dropped.

Do not quarantine this grayware

Specify grayware that are never placed in the quarantine. For more information, see *Match Lists*.

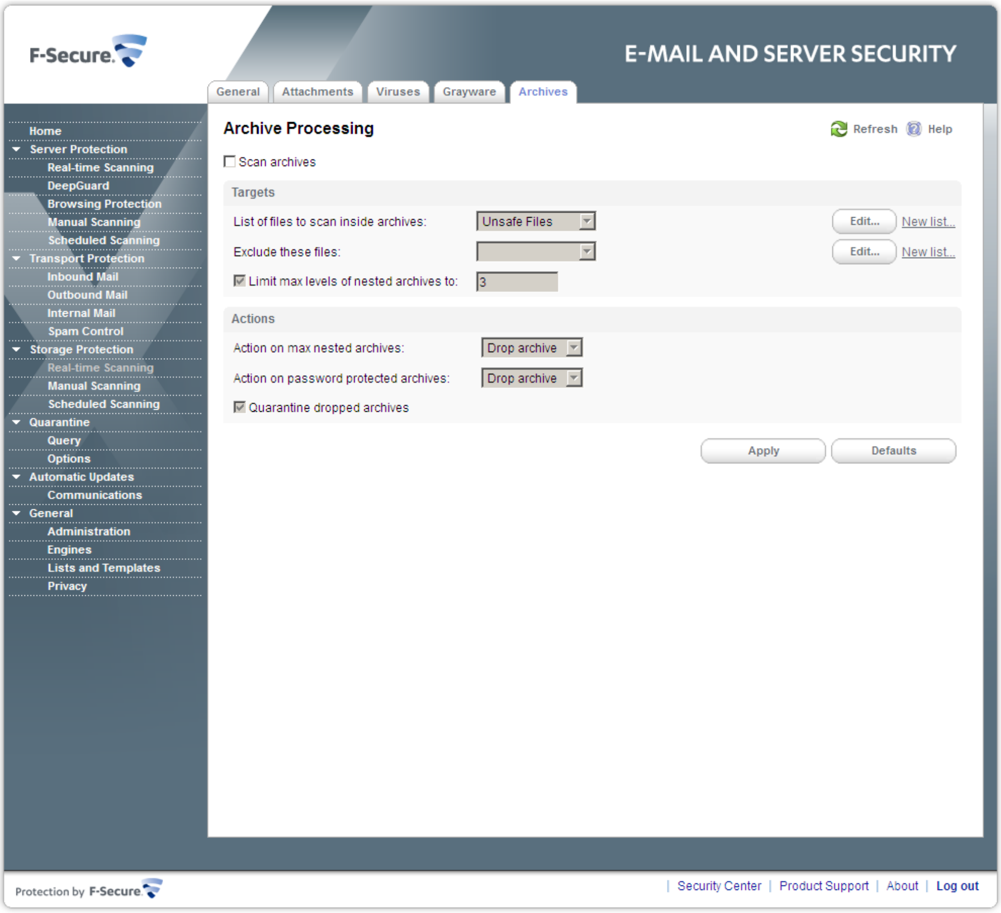
Notifications

Replacement text template

Specify the template for the text that replaces the grayware item when it is removed from the message. For more information, see *Message Templates*.

5.6.1.5 Archive Processing

Specify how the product processes archive files during the real-time e-mail storage scanning.



Archive Processing

☐ Scan archives

Targets

List of files to scan inside archives: Unsafe Files

Exclude these files:

☑ Limit max levels of nested archives to: 3

Actions

Action on max nested archives: Drop archive

Action on password protected archives: Drop archive

☑ Quarantine dropped archives

Scan archives

Specify if files inside archives are scanned for viruses and other malicious code.

Targets

List of files to scan inside archives

Specify files that are scanned for viruses inside archives.

Exclude these files

Specify files inside archives that are not scanned. Leave the list empty if you do not want to exclude any files from the scanning.

Limit max levels of nested archives

Specify how many levels deep to scan in nested archives, if **Scan archives** is enabled.

A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.

Specify the number of archive levels the product goes through. The default setting is 3.

Actions

Action on max nested archives

Specify the action to take on nested archives with nesting levels exceeding the upper level specified in the **Limit max levels of nested archives** setting.

Pass Through - Nested archives are scanned up to level specified in the **Limit max levels of nested archives** setting. Exceeding nesting levels are not scanned, but the archive is not removed.

Drop archive - Archives with exceeding nesting levels are removed.

Action on password protected archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Leave the password protected archive in the message.

Drop archive - Remove the password protected archive from the message.

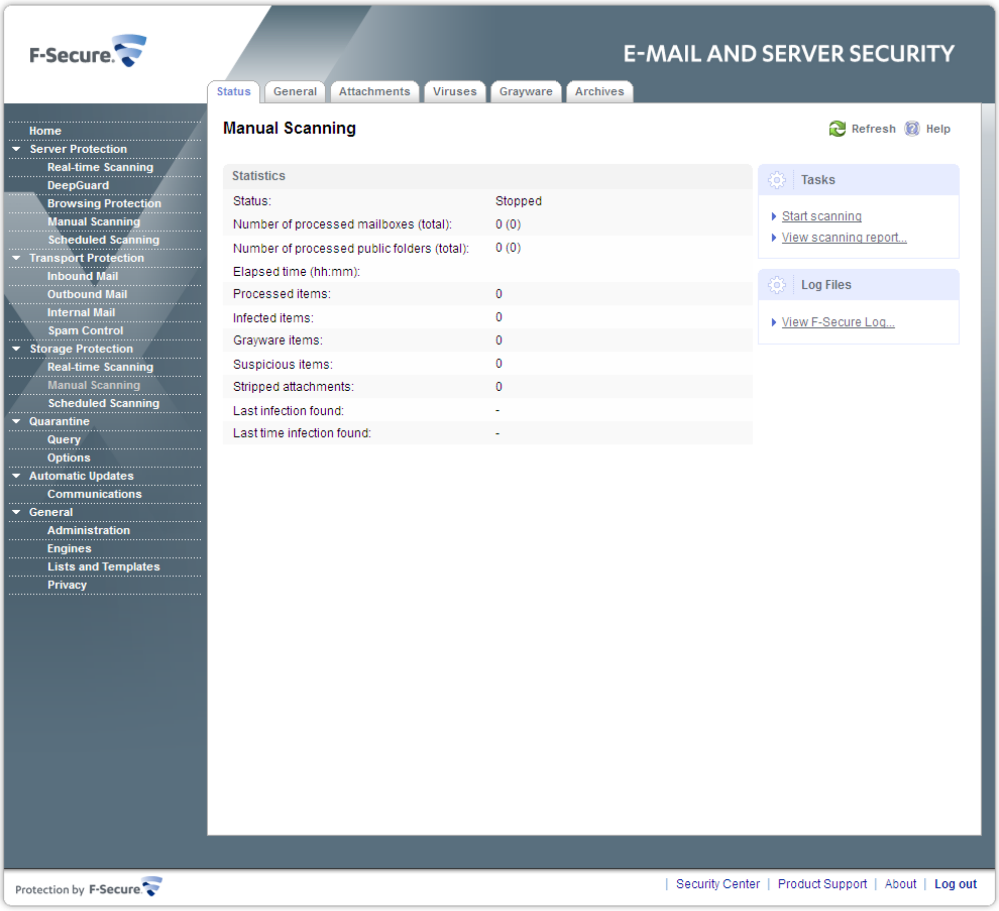
Quarantine dropped archives

Specify whether archives that are not delivered to recipients are placed in the quarantine.

5.6.2 Manual Scanning

You can scan mailboxes and public folders for viruses and strip attachments manually at any time.

Status



Manual Scanning

Statistics

Status:	Stopped
Number of processed mailboxes (total):	0 (0)
Number of processed public folders (total):	0 (0)
Elapsed time (hh:mm):	
Processed items:	0
Infected items:	0
Grayware items:	0
Suspicious items:	0
Stripped attachments:	0
Last infection found:	-
Last time infection found:	-

The **Status** page displays a summary of the messages processed during the latest manual e-mail storage scan:

Status

Displays whether the manual scan is running or stopped.

Number of processed mailboxes

Displays the number of mailboxes that have been scanned and the total number that will be scanned when the manual scan is complete.

Number of processed public folders

Displays the number of public folders that have been scanned and the total number that will be scanned when the manual scan is complete.

Estimated time left

Displays the time left when the manual scan is running.

Elapsed time

Displays how long it has been since the manual scan started.

Processed items	Displays the number of items processed during the scan.
Infected items	Displays the number of infected items found.
Grayware items	Displays the number of grayware items found, including spyware, adware, dialers, joke programs, remote access tools and other unwanted applications.
Suspicious items	Displays the number of suspicious content found, for example password-protected archives and nested archives.
Stripped attachments	Displays the number of filtered attachments.
Last infection found	Displays the name of the last infection found.
Last time infection found	Displays the date when the last infection was found.

Note: If the manual scan scans an item that has not been previously scanned for viruses and the real-time scan is on, the scan result may appear on the real-time scan statistics.

Tasks

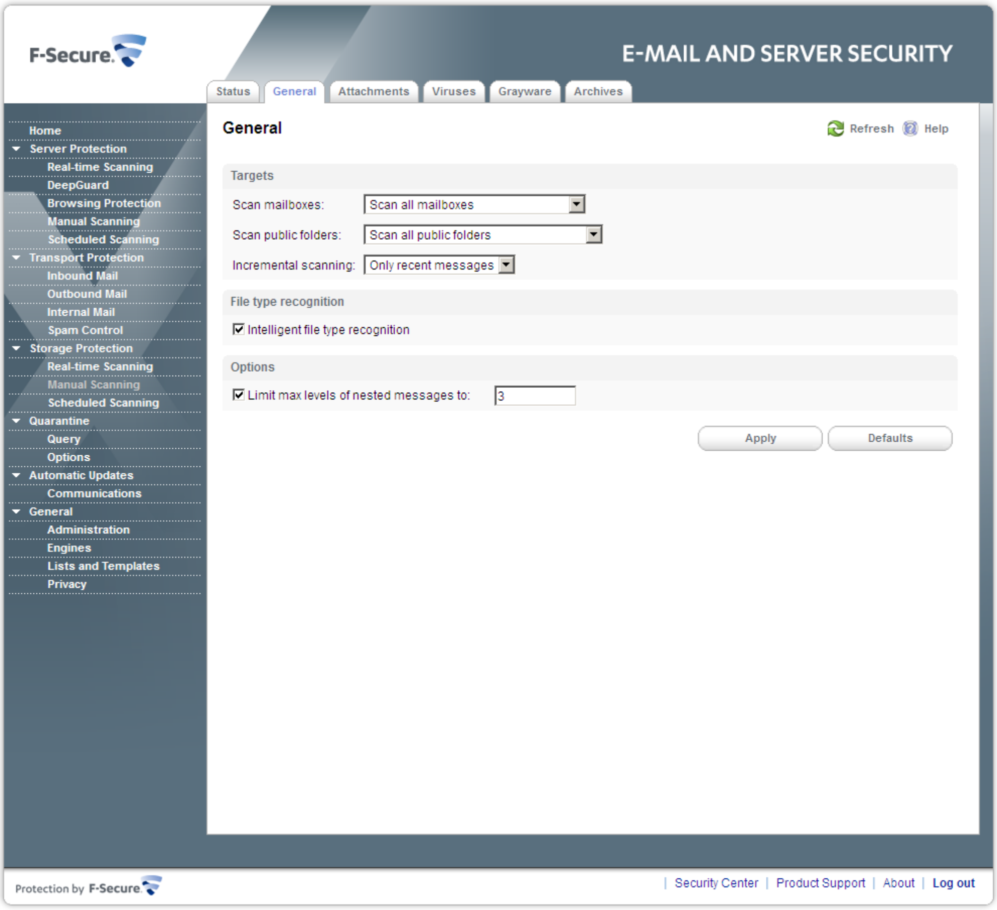
Click **Start scanning** to start the manual scan.

Click **Stop scanning** to stop the manual scan.

Click **View scanning report** to view the latest manual scan report.

5.6.2.1 General

Specify which messages you want to scan during the manual scan.



General

Targets

Scan mailboxes: Scan all mailboxes

Scan public folders: Scan all public folders

Incremental scanning: Only recent messages

File type recognition

☑ Intelligent file type recognition

Options

☑ Limit max levels of nested messages to: 3

Targets

Scan mailboxes

Specify mailboxes that are scanned for viruses.

Do not scan mailboxes - Do not scan any mailboxes during the manual scan.

Scan all mailboxes - Scan all mailboxes.

Scan only included mailboxes - Scan all specified mailboxes. Click **Edit** to add or remove mailboxes that should be scanned.

Scan all except excluded mailboxes - Do not scan specified mailboxes but scan all other. Click **Edit** to add or remove mailboxes that should not be scanned.

Scan public folders

Specify public folders that are scanned for viruses.

Do not scan public folders - Do not scan any public folders during the manual scan.

Scan all folders - Scan all public folders.

Scan only included public folders - Scan all specified public folders. Click **Edit** to add or remove public folders that should be scanned.

Scan all except excluded public folders - Do not scan specified public folders but scan all other. Click **Edit** to add or remove public folders that should not be scanned.

Important:

You need to specify Administrator's mailbox setting to list and scan public folders on Microsoft Exchange 2010 platform. For more information, see *General*.

Incremental Scanning

Specify which messages are scanned for viruses during the manual scan.

All messages - Scan all messages.

Only Recent Messages - Scan only messages that have not been scanned during the previous manual or scheduled scan.

File Type Recognition

Intelligent file type recognition

Select whether you want to use the intelligent file type recognition or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. The intelligent file type recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using the intelligent file type recognition strengthens the security, but can degrade the system performance.

Options

Limit max levels of nested messages

Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.

Advanced

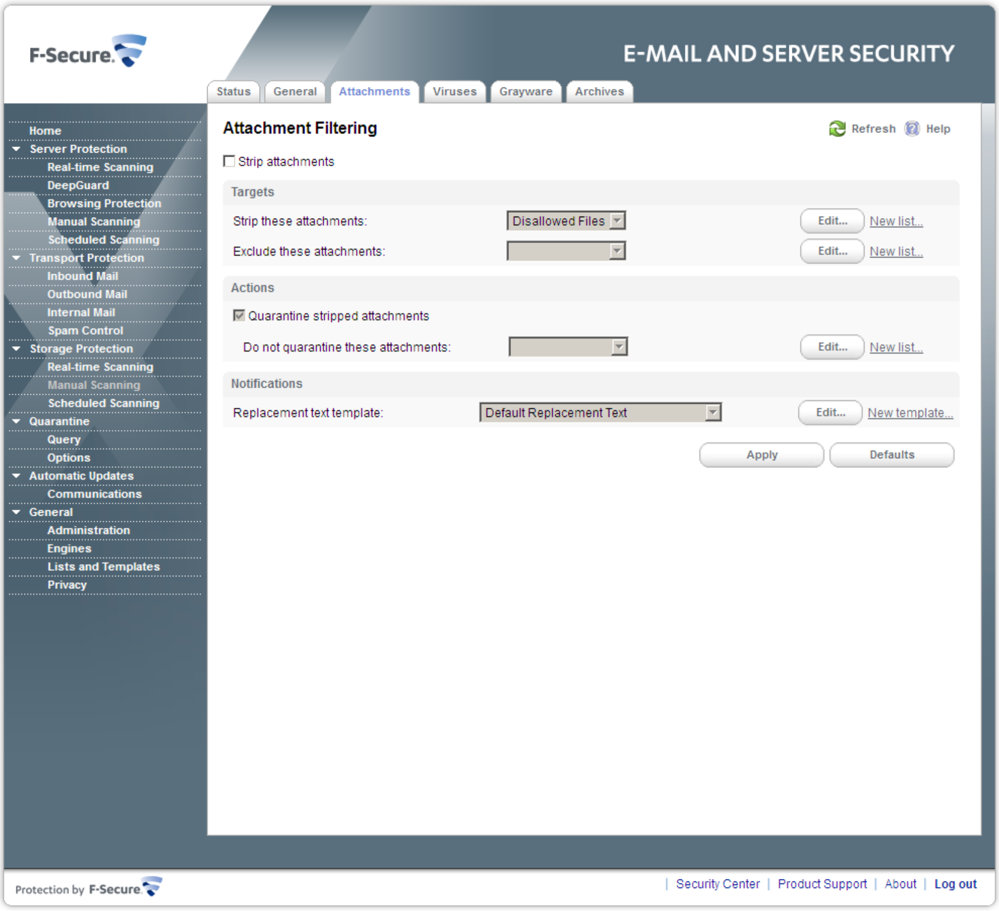
Administrator's mailbox

Specify the primary SMTP address for the account which is used to scan items in public folders. The user account must have permissions to access and modify items in the public folders.

Note: The setting is used on Microsoft Exchange 2010 platform only and affects manual, realtime, and scheduled storage scanning. If you do not specify any address, public folders in Exchange Store cannot be accessed or even listed.

5.6.2.2 Attachment Filtering

Specify attachments that are removed from messages during the manual scan.



Attachment Filtering

□ Strip attachments

Targets

Strip these attachments: Disallowed Files — Edit... New list...

Exclude these attachments: — Edit... New list...

Actions

☑ Quarantine stripped attachments

Do not quarantine these attachments: — Edit... New list...

Notifications

Replacement text template: Default Replacement Text — Edit... New template...

Strip attachments

Enable or disable the attachment stripping.

Targets

Strip these attachments

Specify which attachments are stripped from messages. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.

Actions

Quarantine stripped attachments

Specify whether stripped attachments are quarantined.

Do not quarantine these attachments

Specify files which are not quarantined even when they are stripped. For more information, see *Match Lists*.

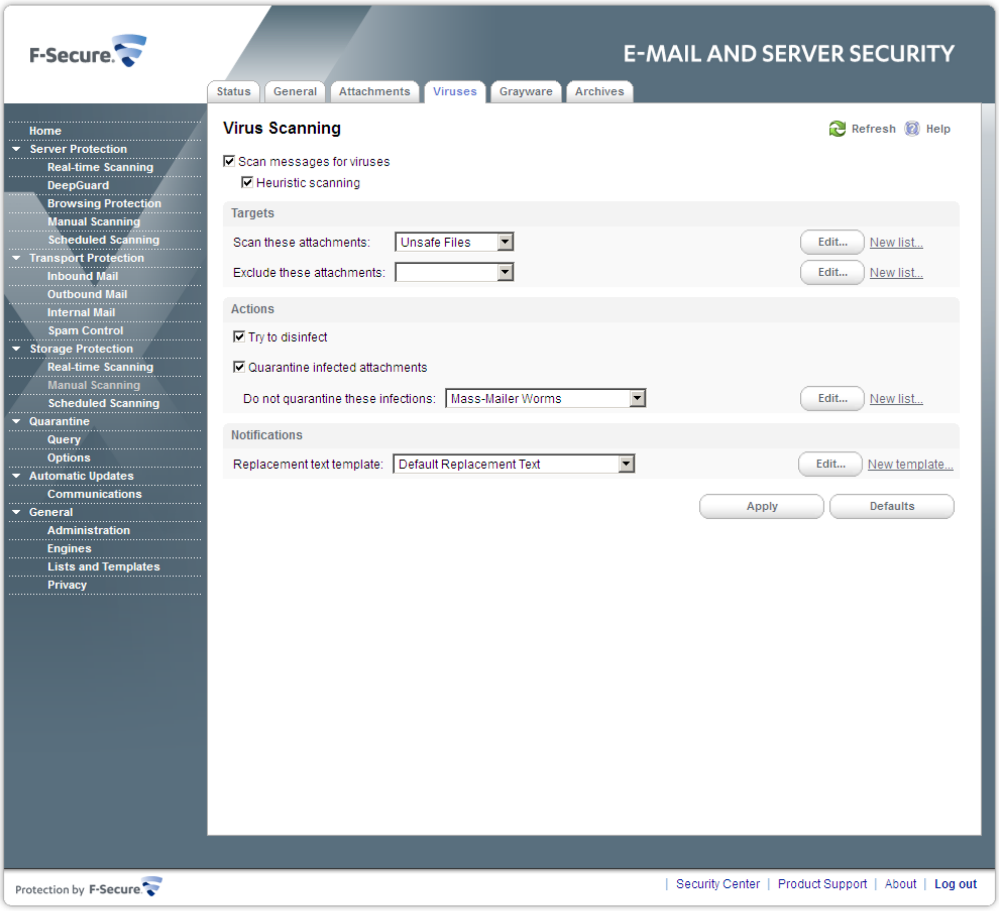
Notifications

Replacement Text Template

Specify the template for the text that replaces the infected attachment when the stripped attachment is removed from the message. For more information, see *Message Templates*.

5.6.2.3 Virus Scanning

Specify messages and attachments that should be scanned for malicious code during the manual scan.



Virus Scanning

☑ Scan messages for viruses

☑ Heuristic scanning

Targets

Scan these attachments: Unsafe Files

Exclude these attachments:

Actions

☑ Try to disinfect

☑ Quarantine infected attachments

Do not quarantine these infections: Mass-Mailer Worms

Notifications

Replacement text template: Default Replacement Text

Scan messages for viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

Note: Disabling virus scanning disables grayware scanning and archive processing as well.

Heuristic Scanning

Enable or disable the heuristic scanning. The heuristic scan analyzes files for suspicious code behavior so that the product can detect unknown malware.

Note: The heuristic scan may affect the product performance and increase the risk of false malware alarms.

Targets

Scan these attachments

Specify attachments that are scanned for viruses. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scanning.

Actions

Try to disinfect

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine infected attachments

Specify whether infected or suspicious attachments are quarantined.

Do not quarantine these infections

Specify virus and malware infections that are never placed in the quarantine. For more information, see *Match Lists*.

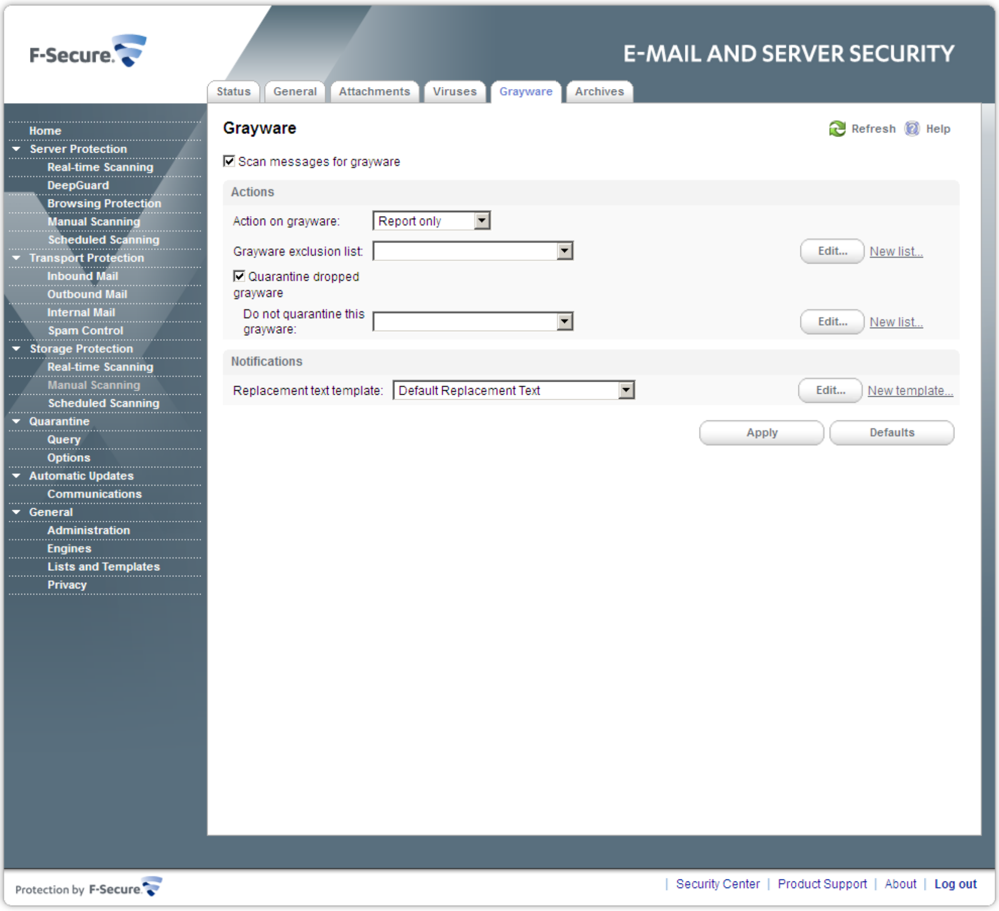
Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Message Templates*.

5.6.2.4 Grayware Scanning

Specify how the product processes grayware items during the manual scan.



Grayware

☑ Scan messages for grayware

Actions

Action on grayware: Report only

Grayware exclusion list:

☑ Quarantine dropped grayware

Do not quarantine this grayware:

Notifications

Replacement text template: Default Replacement Text

Scan messages for grayware

Enable or disable the grayware scan.

Actions

Action on grayware

Specify the action to take on items which contain grayware.

Report only - Leave grayware items in the message and notify the administrator.

Drop attachment - Remove grayware items from the message.

Grayware exclusion list

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan. For more information, see *Match Lists*.

Quarantine dropped grayware

Specify whether grayware attachments are quarantined when dropped.

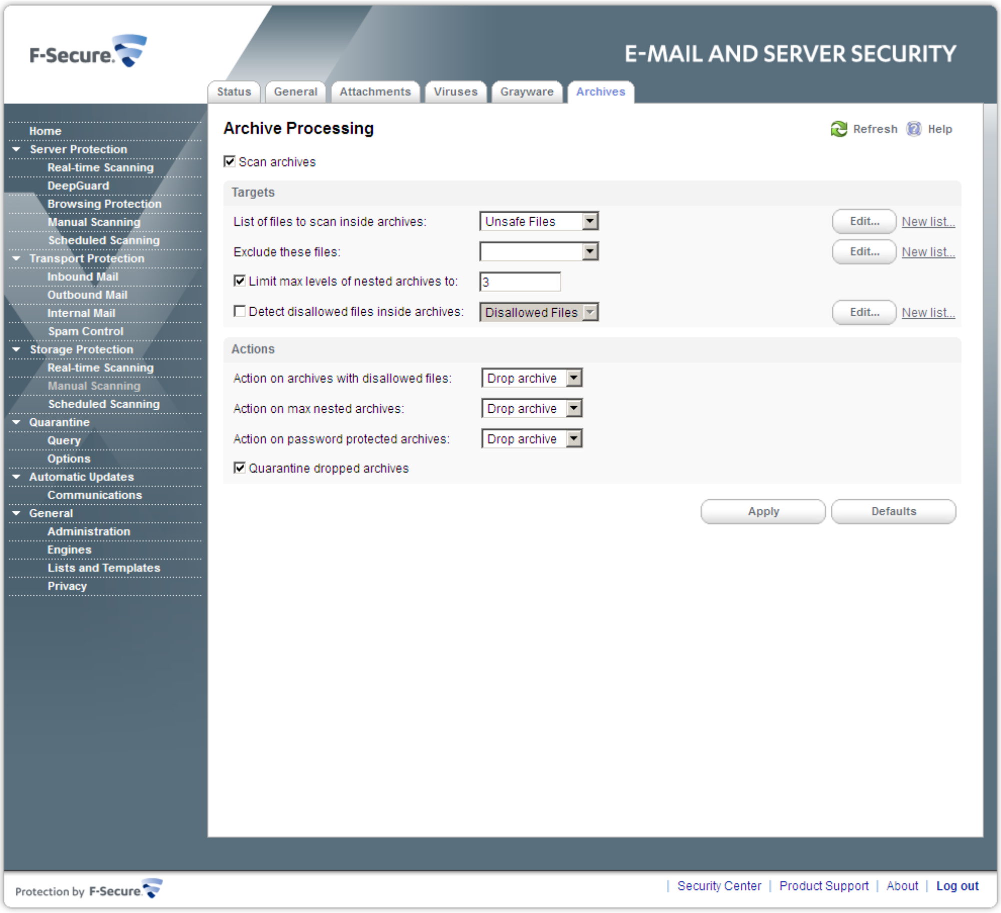
Do not quarantine this grayware	Specify grayware that are never placed in the quarantine. For more information, see *Match Lists*.

Notifications

Replacement text template	Specify the template for the text that replaces the grayware item when it is removed from the message. For more information, see *Message Templates*.

5.6.2.5 Archive Processing

Specify how the product processes archive files during the manual scan.



Archive Processing

☑ Scan archives

Targets

List of files to scan inside archives: Unsafe Files

Exclude these files:

☑ Limit max levels of nested archives to: 3

☐ Detect disallowed files inside archives: Disallowed Files

Actions

Action on archives with disallowed files: Drop archive

Action on max nested archives: Drop archive

Action on password protected archives: Drop archive

☑ Quarantine dropped archives

Scan archives	Specify if files inside archives are scanned for viruses and other malicious code.

Targets

List of files to scan inside archives	Specify files inside archives that are scanned for viruses. For more information, see *Match Lists*.

Exclude these files

Specify files that are not scanned inside archives. Leave the list empty if you do not want to exclude any files from the scanning.

Limit max levels of nested archives

Specify how many levels of archives inside other archives the product scans when **Scan archives** is enabled.

Detect disallowed files inside archives

Specify whether files inside compressed archive files are processed for disallowed content.

If you want to detect disallowed content, specify files that are not allowed. For more information, see *Match Lists*.

Actions

Action on archives with disallowed files

Specify the action to take on archives that contain disallowed content.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message and deliver the message to the recipient without it.

Drop the whole message - Do not deliver the message to the recipient at all.

Action on max nested archives

Specify the action to take on archives with nesting levels exceeding the upper level specified in the **Limit max levels of nested archives** setting.

Pass through - Deliver the message with the archive to the recipient.

Drop archive - Remove the archive from the message.

Action on password protected archives

Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content.

Pass through - Deliver the message with the archive to the recipient.

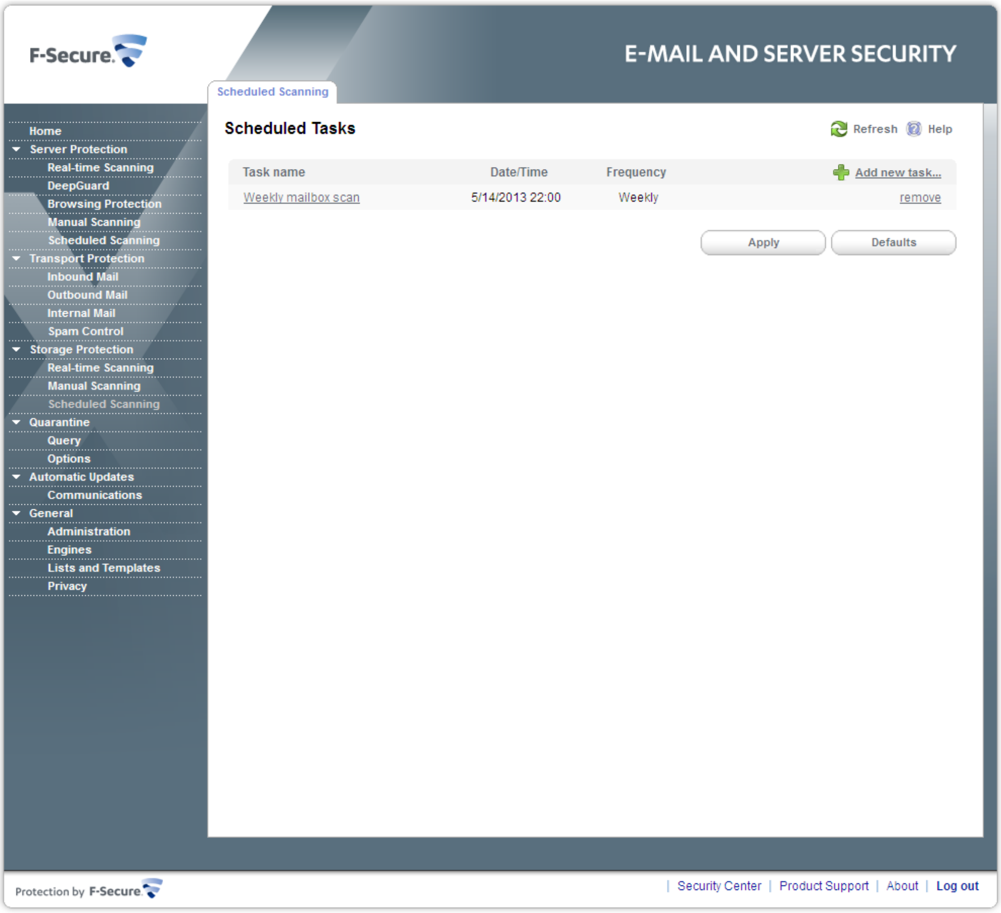
Drop archive - Remove the password protected archive from the message.

Quarantine dropped archives

Specify whether archives that are not delivered to recipients are placed in the quarantine. For more information, see *Match Lists*.

5.6.3 Scheduled Scanning

The **Scheduled Tasks** list displays the scheduled tasks that scan e-mail storage and date and time when they occur for the next time.



Scheduled Tasks

Task name	Date/Time	Frequency	Add new task...
Weekly mailbox scan	5/14/2013 22:00	Weekly	remove

Click **Add new task** to create a new scheduled operation.

Click the scheduled task name to edit it or **Remove** to completely remove it.

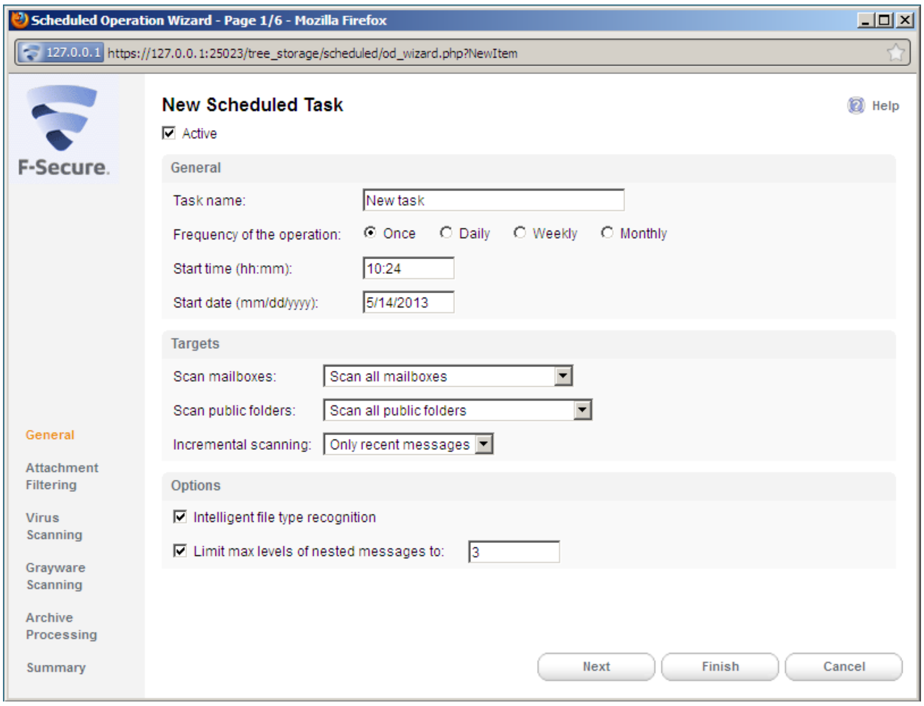
5.6.3.1 Creating Scheduled Task

How to create a scheduled scanning task.

To start the **Scheduled Operation Wizard**, click **Add new task** in the **Scheduled Scanning** page.

5.6.3.1.1 Specify Scanning Task Name and Schedule

Enter the name for the new task and select how frequently you want the operation to be performed.



Scheduled Operation Wizard - Page 1/6 - Mozilla Firefox

127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem

F-Secure.

General

Attachment Filtering

Virus Scanning

Grayware Scanning

Archive Processing

Summary

New Scheduled Task

Help

☑ Active

General

Task name: New task

Frequency of the operation: ● Once ○ Daily ○ Weekly ○ Monthly

Start time (hh:mm): 10:24

Start date (mm/dd/yyyy): 5/14/2013

Targets

Scan mailboxes: Scan all mailboxes

Scan public folders: Scan all public folders

Incremental scanning: Only recent messages

Options

☑ Intelligent file type recognition

☑ Limit max levels of nested messages to: 3

Next Finish Cancel

Active

Specify whether you want the scheduled scanning task to be active immediately after you have created it.

General

Task name

Specify the name of the scheduled operation.

Note: Do not use any special characters in the task name.

Frequency of the operation

Specify how frequently you want the operation to be performed.

Once - Only once at the specified time.

Daily - Every day at the specified time, starting from the specified date.

Weekly - Every week at the specified time on the same day when the first operation is scheduled to start.

Monthly - Every month at the specified time on the same date when the first operation is scheduled to start.

Start time

Enter the start time of the task in hh:mm format.

Start date

Enter the start date of the task in mm/dd/yyyy format

Targets

Scan mailboxes

Specify mailboxes that are scanned for viruses.

Do not scan mailboxes - Disable the mailbox scanning.

Scan all mailboxes - Scan all mailboxes.

Scan only included mailboxes - Scan all specified mailboxes. Click **Edit** to add or remove mailboxes that should be scanned.

Scan all except excluded mailboxes - Do not scan specified mailboxes but scan all other. Click **Edit** to add or remove mailboxes that should not be scanned.

Scan public folders

Specify public folders that are scanned for viruses.

Do not scan public folders - Disable the public folder scanning.

Scan all folders - Scan all public folders.

Scan only included public folders - Scan all specified public folders. Click **Edit** to add or remove public folders that should be scanned.

Scan all except excluded public folders - Do not scan specified public folders but scan all other. Click **Edit** to add or remove public folders that should not be scanned.

Important:

You need to specify Administrator's mailbox setting to list and scan public folders on Microsoft Exchange 2010 platform. For more information, see *General*.

Incremental scanning

Specify whether you want to process all messages or only those messages that have not been processed previously during the manual or scheduled processing.

Options

Intelligent file type recognition

Select whether you want to use the intelligent file type recognition or not.

Trojans and other malicious code can disguise themselves with filename extensions which are usually considered safe to use. The intelligent file type recognition can recognize the real file type of the message attachment and use that while the attachment is processed.

Note: Using the intelligent file type recognition strengthens the security, but can degrade the system performance.

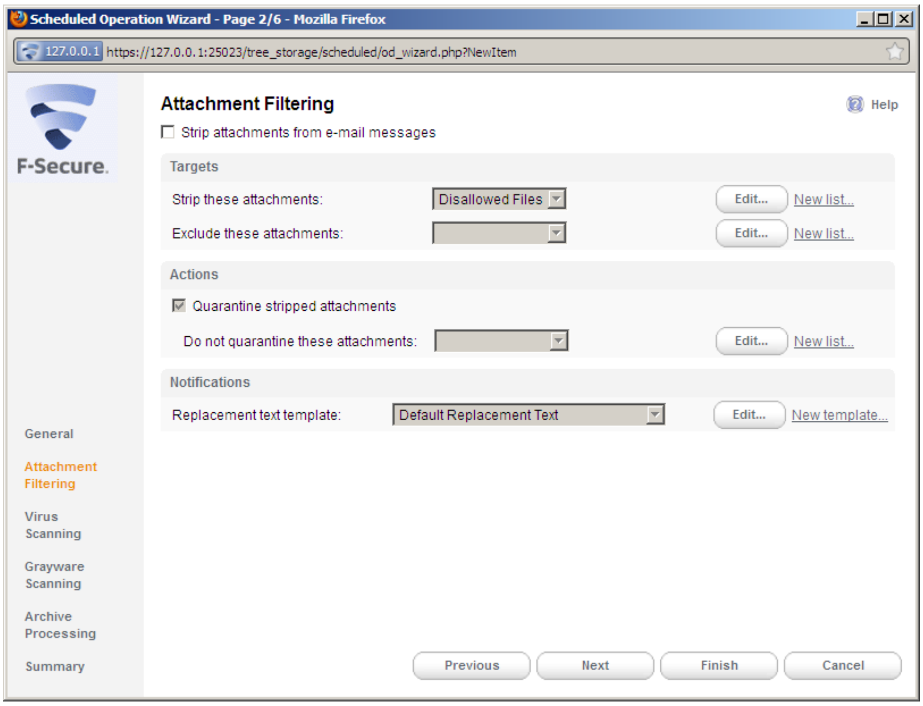
Limit max levels of nested messages

Specify how many levels deep to scan in nested e-mail messages. A nested e-mail message is a message that includes one or more e-mail messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.

Note: It is not recommended to set the maximum nesting level to unlimited as this will make the product more vulnerable to DoS (Denial-of-Service) attacks.

5.6.3.1.2 Specify Attachment Filtering Options

Choose settings for stripping attachments during the scheduled operation.



Scheduled Operation Wizard - Page 2/6 - Mozilla Firefox

127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem

Attachment Filtering

☐ Strip attachments from e-mail messages

Targets

Strip these attachments: Disallowed Files

Exclude these attachments:

Actions

☑ Quarantine stripped attachments

Do not quarantine these attachments:

Notifications

Replacement text template: Default Replacement Text

Strip attachments from e-mail messages

Enable or disable the attachment stripping.

Targets

Strip these attachments

Specify which attachments are stripped from messages. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering.

Action

Quarantine stripped attachments

Specify whether stripped attachments are quarantined.

Do not quarantine these attachments

Specify files which are not quarantined even when they are stripped. For more information, see *Match Lists*.

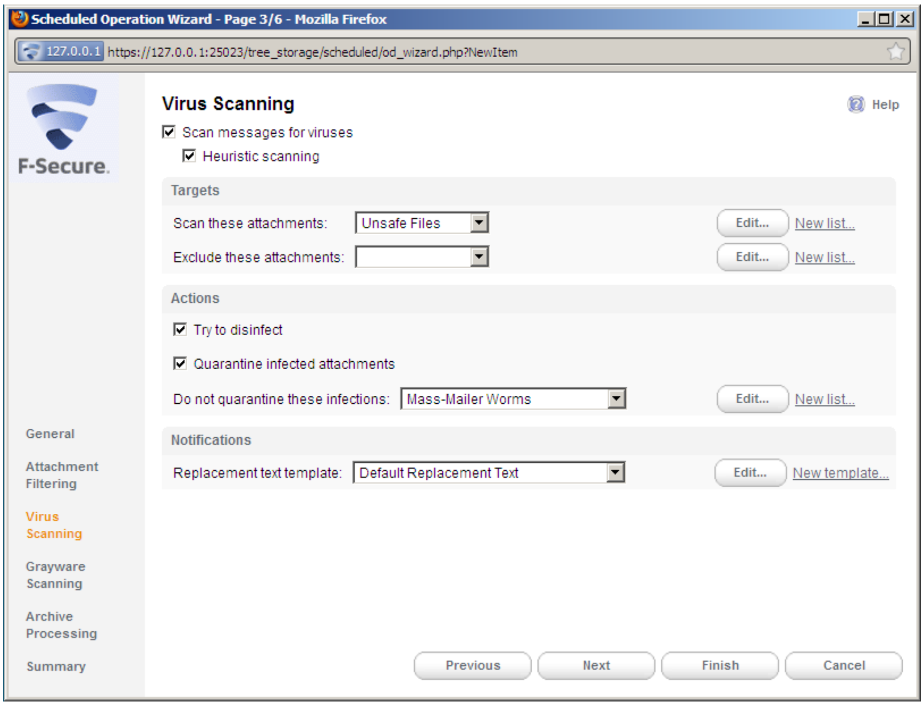
Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the stripped attachment is removed from the message. For more information, see *Message Templates*.

5.6.3.1.3 Specify Virus Scanning Options

Choose how mailboxes and public folders are scanned for viruses during the scheduled operation.



Scheduled Operation Wizard - Page 3/6 - Mozilla Firefox

127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem

Virus Scanning

☑ Scan messages for viruses

☑ Heuristic scanning

Targets

Scan these attachments: Unsafe Files

Exclude these attachments:

Actions

☑ Try to disinfect

☑ Quarantine infected attachments

Do not quarantine these infections: Mass-Mailer Worms

Notifications

Replacement text template: Default Replacement Text

Scan messages for viruses

Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code.

Note: If you disable the virus scan, grayware scanning and archive processing are disabled as well.

Heuristic Scanning

Enable or disable the heuristic scanning. The heuristic scanning analyzes files for suspicious code behavior so that the product can detect unknown malware.

Note: Heuristic scanning may affect the product performance and increase the risk of false malware alarms.

Targets

Scan these attachments

Specify attachments that are scanned for viruses. For more information, see *Match Lists*.

Exclude these attachments

Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scanning.

Actions

Try to disinfect

Specify whether the product should try to disinfect an infected attachment before processing it. If the disinfection succeeds, the product does not process the attachment further.

Note: Disinfection may affect the product performance.

Note: Infected files inside archives are not disinfected even when the setting is enabled.

Quarantine infected messages

Specify whether infected or suspicious messages are quarantined.

Do not quarantine these infections

Specify infections that are never placed in the quarantine. For more information, see *Match Lists*.

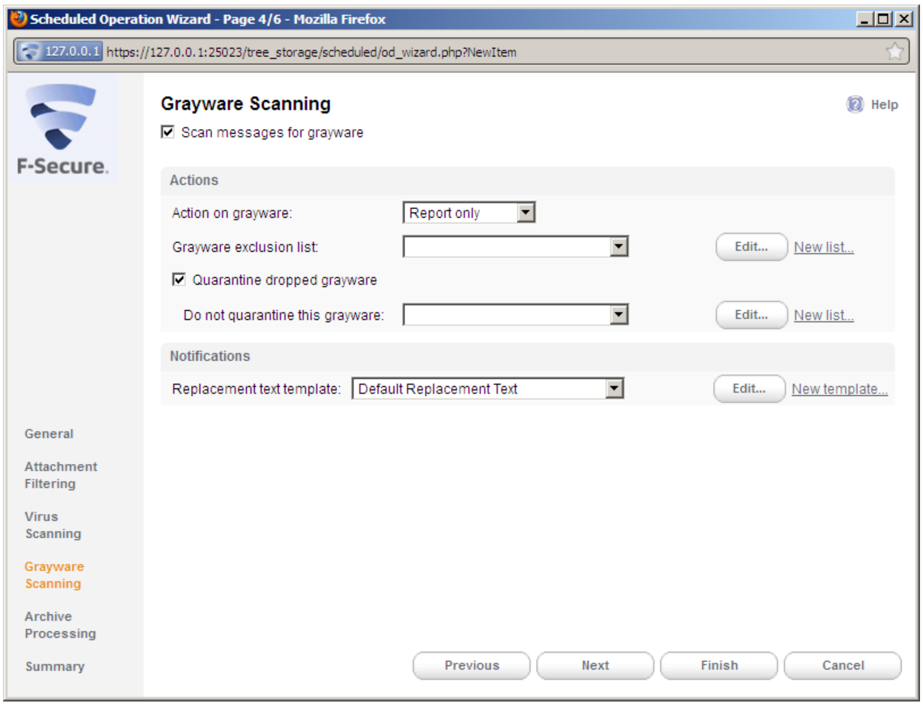
Notifications

Replacement text template

Specify the template for the text that replaces the infected attachment when the infected attachment is removed from the message. For more information, see *Message Templates*.

5.6.3.1.4 Specify Grayware Scanning Options

Choose settings for grayware scanning during the scheduled operation.



Scheduled Operation Wizard - Page 4/6 - Mozilla Firefox

127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem

Grayware Scanning

☑ Scan messages for grayware

Actions

Action on grayware: Report only

Grayware exclusion list:

☑ Quarantine dropped grayware

Do not quarantine this grayware:

Notifications

Replacement text template: Default Replacement Text

Scan messages for grayware

Enable or disable the grayware scan.

Actions

Action on grayware

Specify the action to take on items which contain grayware.

Report only - Leave grayware items in the message and notify the administrator.

Drop attachment - Remove grayware items from the message.

Grayware exclusion list

Specify the list of keywords for grayware types that are not scanned. Leave the list empty if you do not want to exclude any grayware types from the scan. For more information, see *Match Lists*.

Quarantine dropped grayware

Specify whether grayware attachments are quarantined when dropped.

Do not quarantine this grayware

Specify grayware that are never placed in the quarantine. For more information, see *Match Lists*.

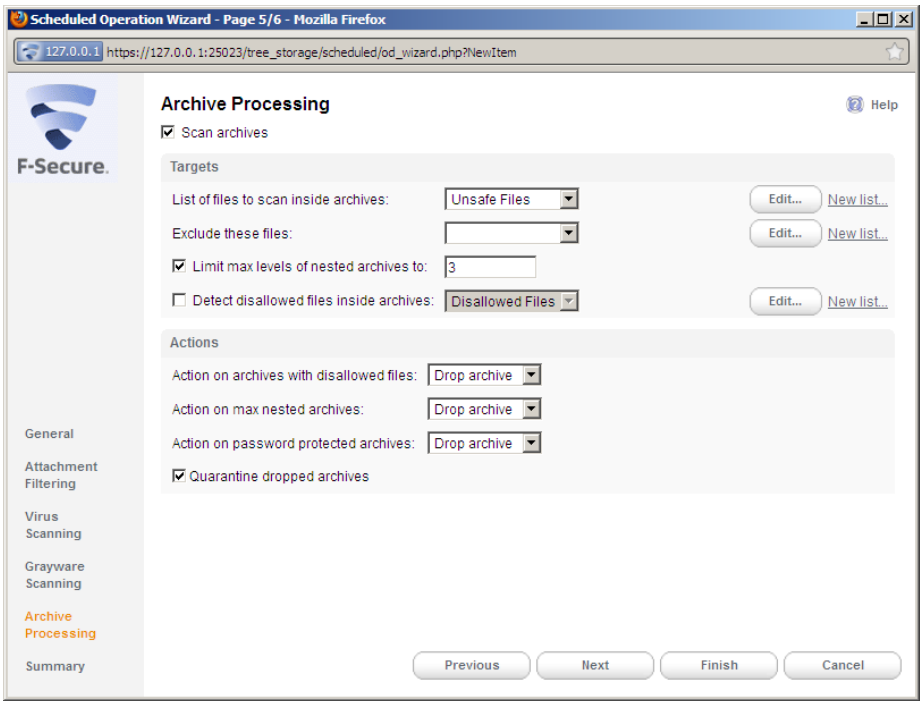
Notifications

Replacement text template

Specify the template for the text that replaces the grayware item when it is removed from the message. For more information, see *Message Templates*.

5.6.3.1.5 Specify Archive Processing Options

Choose settings for archive processing during the scheduled operation.



Scheduled Operation Wizard - Page 5/6 - Mozilla Firefox

127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem

Archive Processing

☑ Scan archives

Targets

List of files to scan inside archives: Unsafe Files

Exclude these files:

☑ Limit max levels of nested archives to: 3

□ Detect disallowed files inside archives: Disallowed Files

Actions

Action on archives with disallowed files: Drop archive

Action on max nested archives: Drop archive

Action on password protected archives: Drop archive

☑ Quarantine dropped archives

Scan archives

Specify if files inside archives are scanned for viruses and other malicious code.

Targets

List of files to scan inside archives

Specify files inside archives that are scanned for viruses. For more information, see *Match Lists*.

Exclude these files

Specify files that are not scanned inside archives. Leave the list empty if you do not want to exclude any files from the scanning.

Limit max levels of nested archives

Specify how many levels of archives inside other archives the product scans when **Scan archives** is enabled.

Detect disallowed files inside archives

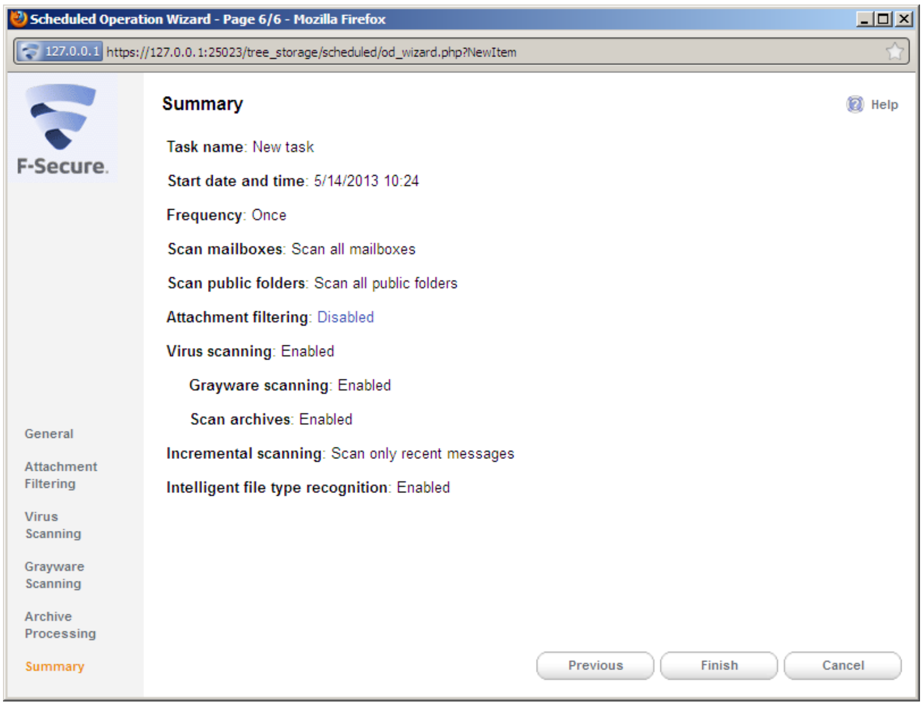
Specify files which are not allowed inside archives. For more information, see *Match Lists*.

Actions

Action on archives with disallowed files	Specify the action to take on archives which contain disallowed files. **Pass through** - Deliver the message with the archive to the recipient. **Drop archive** - Remove the archive from the message and deliver the message to the recipient without it.
Action on max nested archives	Specify the action to take on archives with nesting levels exceeding the upper level specified in the **Limit max levels of nested archives** setting. **Pass through** - Deliver the message with the archive to the recipient. **Drop archive** - Remove the archive from the message and deliver the message to the recipient without it.
Action on password protected archives	Specify the action to take on archives which are protected with passwords. These archives can be opened only with a valid password, so the product cannot scan their content. **Pass through** - Deliver the message with the password protected archive to the recipient. **Drop archive** - Remove the password protected archive from the message and deliver the message to the recipient without it.
Quarantine dropped archives	Specify whether archives that are not delivered to recipients are placed in the quarantine.

5.6.3.1.6 Finish

The **Scheduled Operation Wizard** displays the summary of created operation.


Scheduled Operation Wizard - Page 6/6 - Mozilla Firefox
127.0.0.1 https://127.0.0.1:25023/tree_storage/scheduled/od_wizard.php?NewItem
F-Secure.
Help
General
Attachment Filtering
Virus Scanning
Grayware Scanning
Archive Processing
Summary
Previous
Finish
Cancel

Summary

Task name: New task

Start date and time: 5/14/2013 10:24

Frequency: Once

Scan mailboxes: Scan all mailboxes

Scan public folders: Scan all public folders

Attachment filtering: Disabled

Virus scanning: Enabled

Grayware scanning: Enabled

Scan archives: Enabled

Incremental scanning: Scan only recent messages

Intelligent file type recognition: Enabled

Click **Finish** to accept the new scheduled operation and to exit the wizard.

5.7 Quarantine

Quarantine is a safe repository for detected items that may be harmful. Quarantined items cannot spread or cause harm to your computer.

The product can quarantine malware, spyware, riskware, and unwanted e-mails to make them harmless. You can restore files and e-mail messages from the quarantine later if you need them.

The product uses two separate quarantine repositories:

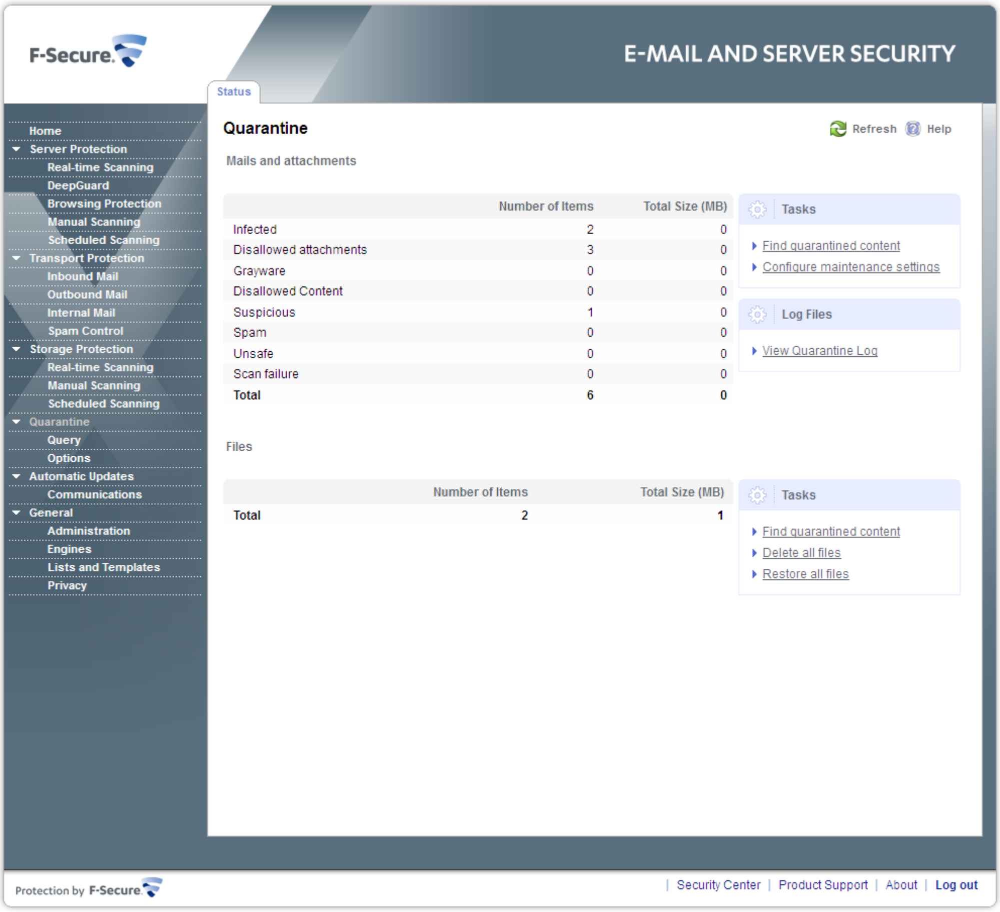
- File Quarantine - quarantines malicious files that are detected on the server with Server Protection security level. The repository is stored on the same Microsoft Windows Server where the product is installed.
- E-mail Quarantine - quarantines e-mail messages and attachments that F-Secure Anti-Virus for Microsoft Exchange component detects with Transport and Storage Protection security levels. Since Transport Protection and Server Protection may be installed on different Microsoft Windows Servers running Microsoft Exchange Server, the E-mail Quarantine is handled through an SQL database and may be installed on a dedicated server.

> **Note:** For additional information on different deployment scenarios for the product and how to install the E-mail Quarantine, consult F-Secure E-mail and Server Security Deployment Guide.

The Quarantine management is divided into two different parts:

- Quarantine-related configuration, and
- the management of the quarantined content, for example searching for and deleting quarantined content.

Status



Quarantine

Mails and attachments

	Number of Items	Total Size (MB)
Infected	2	0
Disallowed attachments	3	0
Grayware	0	0
Disallowed Content	0	0
Suspicious	1	0
Spam	0	0
Unsafe	0	0
Scan failure	0	0
Total	6	0

Files

	Number of Items	Total Size (MB)
Total	2	1

The **Quarantine Status** page displays a summary of the quarantined messages, attachments and files and their total size:

Mails and attachments

Infected

Displays the number of messages and attachments that are infected.

Disallowed attachments

Displays the number of messages that contained attachments with disallowed files.

Grayware

Displays the number of messages that have grayware items, including spyware, adware, dialers, joke programs, remote access tools and other unwanted applications.

Disallowed content

Displays the number of messages that have been found to contain disallowed keywords in the message subject or text.

Suspicious	Displays the number of suspicious content found, for example password-protected archives, nested archives and malformed messages.
Spam	Displays the number of messages that are classified as spam.
Unsafe	Displays the number of messages that have been identified as unsafe; messages that contain patterns that can be assumed to be a part of a spam or virus outbreak
Scan failure	Displays the number of files that could not be scanned, for example severely corrupted files.

E-mail Quarantine Tasks

Click **Find quarantined content** to search for the quarantined e-mails and attachments.

Click **Configure maintenance settings** to configure settings for automatic reprocessing and cleanup items in E-mail Quarantine.

Click **View Quarantine Log** to view E-mail Quarantine log file.

Files	
Total	Displays the number of files found on the server that have been quarantined.

File Quarantine Tasks

Click **Find quarantined content** to view general information on quarantined files in the File Quarantine.

Click **Delete all files** to delete all the quarantined files from the File Quarantine.

Click **Restore all files** to all the items from the File Quarantine. Restored items are moved back to their original location in your computer.

Important:

Do not restore any items from the quarantine unless you are sure that the items pose no threat.

5.7.1 Query

You can use Query pages to search and manually handle the quarantined content.

Quarantined Mails and Attachments

With the Quarantine Query page, you can create different queries to search quarantined e-mails and file attachments from the E-mail Quarantine database.

Quarantined Files

You can view the general information on the quarantined items in the Quarantined Files page. The page displays a list of the first 100 items with the type of the quarantined items, their name, and the path where the files were installed.

To delete quarantined items, select items that you want to remove and click **Delete**. Deleting an item in the quarantine removes it permanently from your computer.

If you need a quarantined item, you can restore it from the File Quarantine. Restored items move back to the original location in the computer. Select the quarantined items you want to restore and click **Restore**.

- In general, you can delete quarantined malware.
- In most cases, you can delete quarantined spyware. It is possible that the quarantined spyware is part of a legitimate software program and removing it stops the actual program from working correctly. If you want to keep the program on your computer, you can restore the quarantined spyware.
- Quarantined riskware can be a legitimate software program. If you have installed and set up the program by yourself, you can restore it from the quarantine. If the riskware is installed without your knowledge, it is most likely installed with malicious intent and should be deleted.

Important:

Do not restore any items from the quarantine unless you are sure that the items pose no threat.

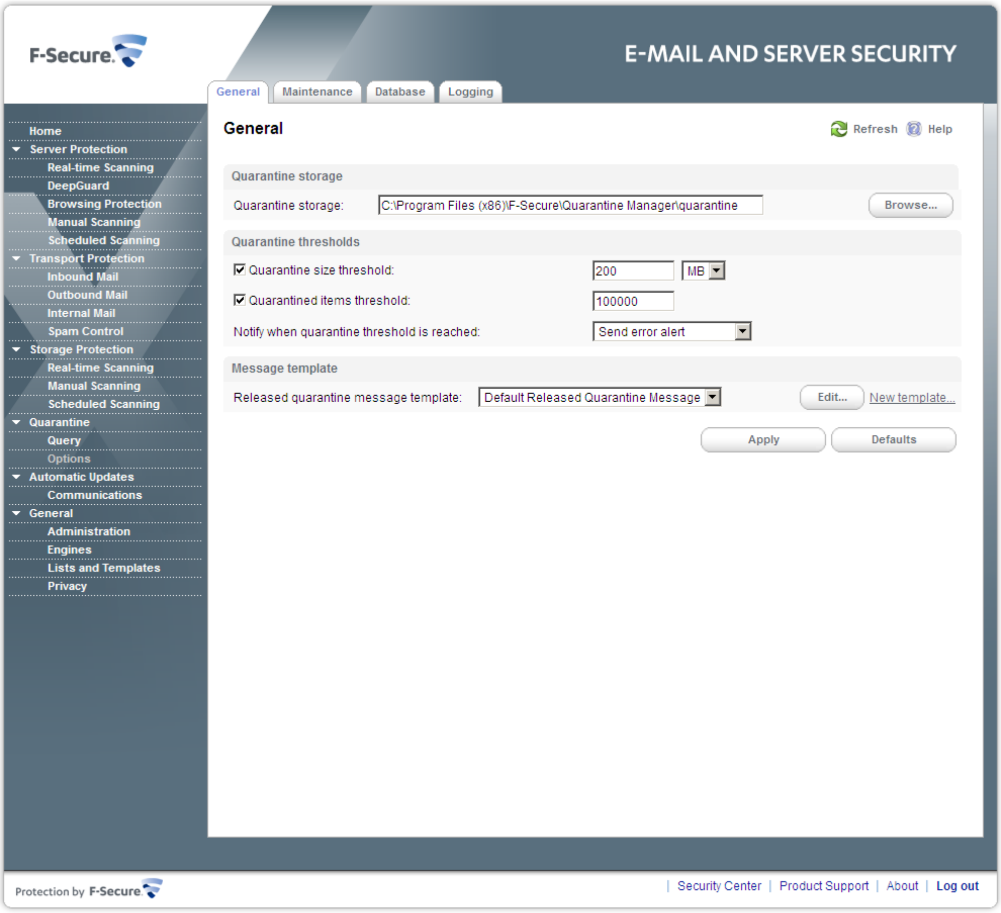
5.7.2 Options

You can configure the E-mail Quarantine storage location and threshold, how quarantined e-mail messages and attachments are processed and quarantine logging options.

Note: All the described options affect the E-mail Quarantine only.

5.7.2.1 General

When the product places content to the Quarantine, it saves the content as separate files into the Quarantine Storage and inserts an entry to the Quarantine Database with information about the quarantined content.



General

Quarantine storage

Quarantine storage: C:\Program Files (x86)\F-Secure\Quarantine Manager\quarantine

Quarantine thresholds

☑ Quarantine size threshold: 200 MB

☑ Quarantined items threshold: 100000

Notify when quarantine threshold is reached: Send error alert

Message template

Released quarantine message template: Default Released Quarantine Message

Quarantine storage

Quarantine storage

Specify the location of the E-mail Quarantine storage.

Before you change the location, see *Moving the E-mail Quarantine Storage*.

Note: Make sure that F-Secure Anti-Virus for Microsoft Exchange service has write access to this directory. Adjust the access rights to the directory so that only the F-Secure Anti-Virus for Microsoft Exchange service and the local administrator can access files in the Quarantine.

Quarantine thresholds

Quarantine size threshold

Specify the critical size (in megabytes) of the E-mail Quarantine storage. If the specified value is reached, the product sends an alert. The default value is 200. If zero (0) is specified, the size of the Quarantine is not checked. The allowed value range is from 0 to 10240.

Quarantined items threshold

Specify the critical number of items in the Quarantine storage. If the specified value is reached or exceeded, the product sends an alert. If zero (0) is specified, the number of items in the Quarantine storage is not checked. The default value is 100000 items.

Notify when quarantine threshold is reached

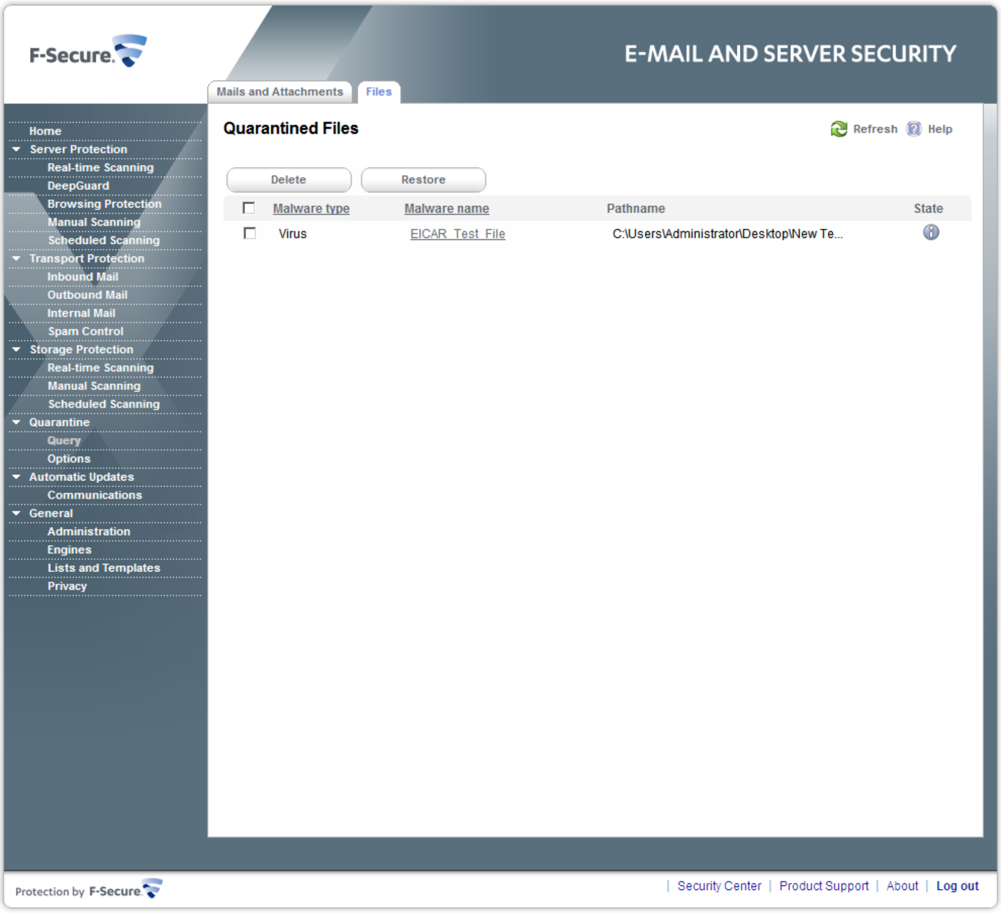
Specify how the administrator should be notified when the Quarantine Size Threshold and/or Quarantined Items Threshold are reached. No alert is sent if both thresholds are set to zero (0).

Message template

Released quarantine message template

Specify the template for the message that is sent to the intended recipients when e-mail content is released from the quarantine. For more information, see *Message Templates*.

5.7.2.2 Quarantine Maintenance



Quarantined Files

□	Malware type	Malware name	Pathname	State
□	Virus	EICAR_Test_File	C:\Users\Administrator\Desktop\New Te...	

When quarantined content is reprocessed, it is scanned again, and if it is found clean, it is sent to the intended recipients.

When removing quarantined messages from the quarantine, the product uses the currently configured quarantine retention and cleanup settings.

Reprocess unsafe messages

Automatically reprocess unsafe messages

Specify how often the product tries to reprocess unsafe messages that are retained in the E-mail Quarantine.

Set the value to Disabled to process unsafe messages manually.

Max attempts to process unsafe messages

Specify how many times the product tries to reprocess unsafe messages that are retained in the E-mail Quarantine.

Final action on unsafe messages

Specify the action on unsafe messages after the maximum number of reprocesses have been attempted.

Leave in Quarantine - Leave messages in the E-mail Quarantine and process them manually.

Release to Intended Recipients - Release messages from the E-mail Quarantine and send them to original recipients.

Quarantine retention and cleanup

Retain items in quarantine

Specify how long quarantined items should be retained in the E-mail Quarantine before they are deleted.

Use the **Quarantine Cleanup Exceptions** table to change the retention period for a particular Quarantine category.

Delete old quarantined items

Specify how often the storage should be cleaned of old quarantined items.

Use the **Quarantine Cleanup Exceptions** table to change the cleanup interval for a particular Quarantine category.

Exceptions

Specify separate quarantine retention period and cleanup interval for any Quarantine category. If retention period and cleanup interval for a category are not defined in this table, then the default ones (specified above) are used.

Active - Enable or disable the selected entry in the table.

Quarantine category - Select a category the retention period or cleanup interval of which you want to modify. The categories are:

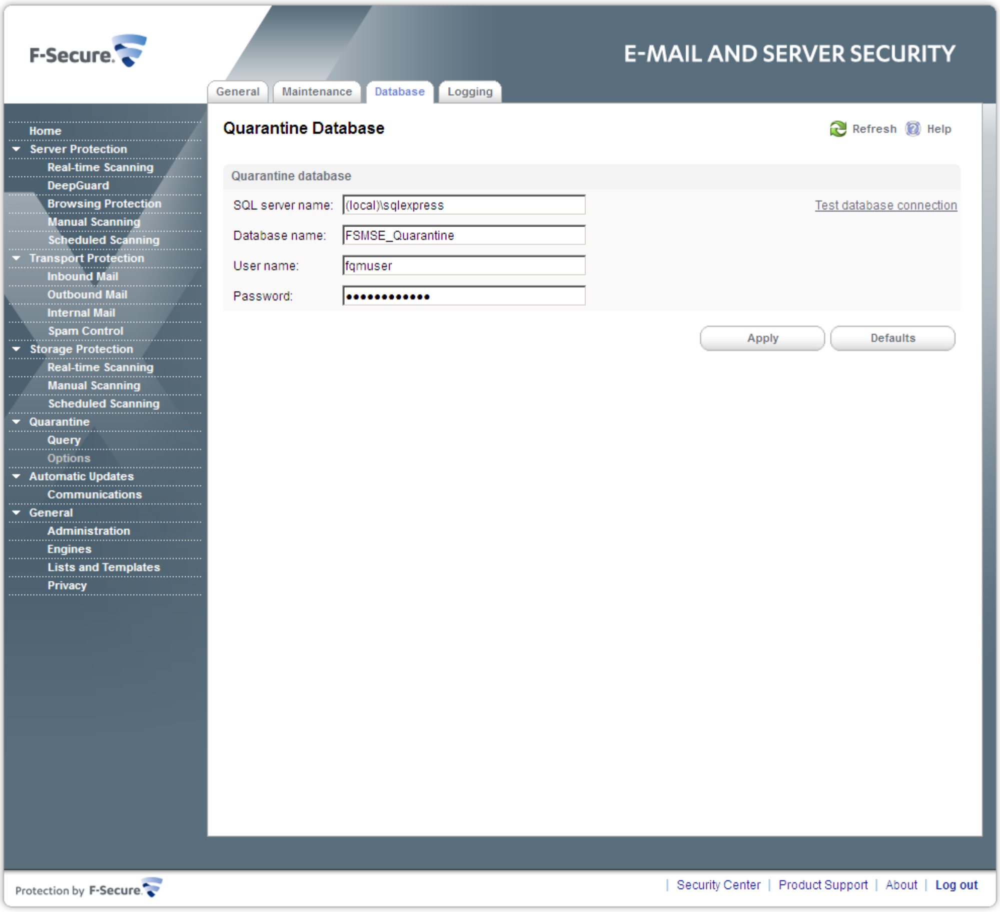
- Infected
- Suspicious
- Disallowed attachment
- Disallowed content
- Spam
- Scan failure
- Unsafe
- Grayware

Retention period - Specify an exception to the default retention period for the selected Quarantine category.

Cleanup interval - Specify an exception to the default cleanup interval for the selected Quarantine category.

5.7.2.3 Quarantine Database

You can specify the database where information about quarantined e-mails is stored and from which it is retrieved.



Quarantine Database

Quarantine database

SQL server name: (local)\sqlexpress

Database name: FSMSE_Quarantine

User name: fqmuser

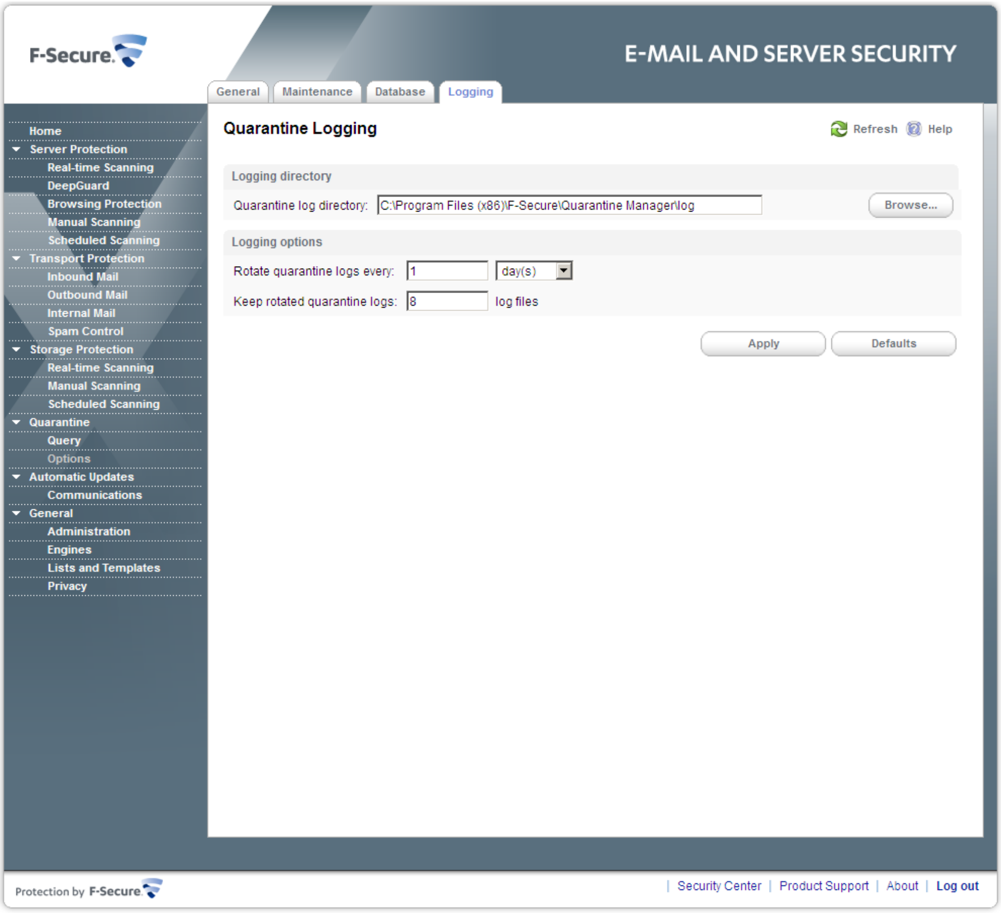
Password: ••••••••••••

Quarantine database	
SQL server name	The name of the SQL server where the database is located.
Database name	The name of the quarantine database. The default name is `FSMSE_Quarantine`.
User name	The user name the product uses when accessing the database.
Password	The password the product uses when accessing the database.

Click **Test database connection** to make sure that you can access the quarantine database with the configured user name and password.

5.7.2.4 Quarantine Logging

Specify where the product stores E-mail Quarantine log files.



Quarantine Logging

Logging directory

Quarantine log directory: C:\Program Files (x86)\F-Secure\Quarantine Manager\log

Logging options

Rotate quarantine logs every: 1 day(s)

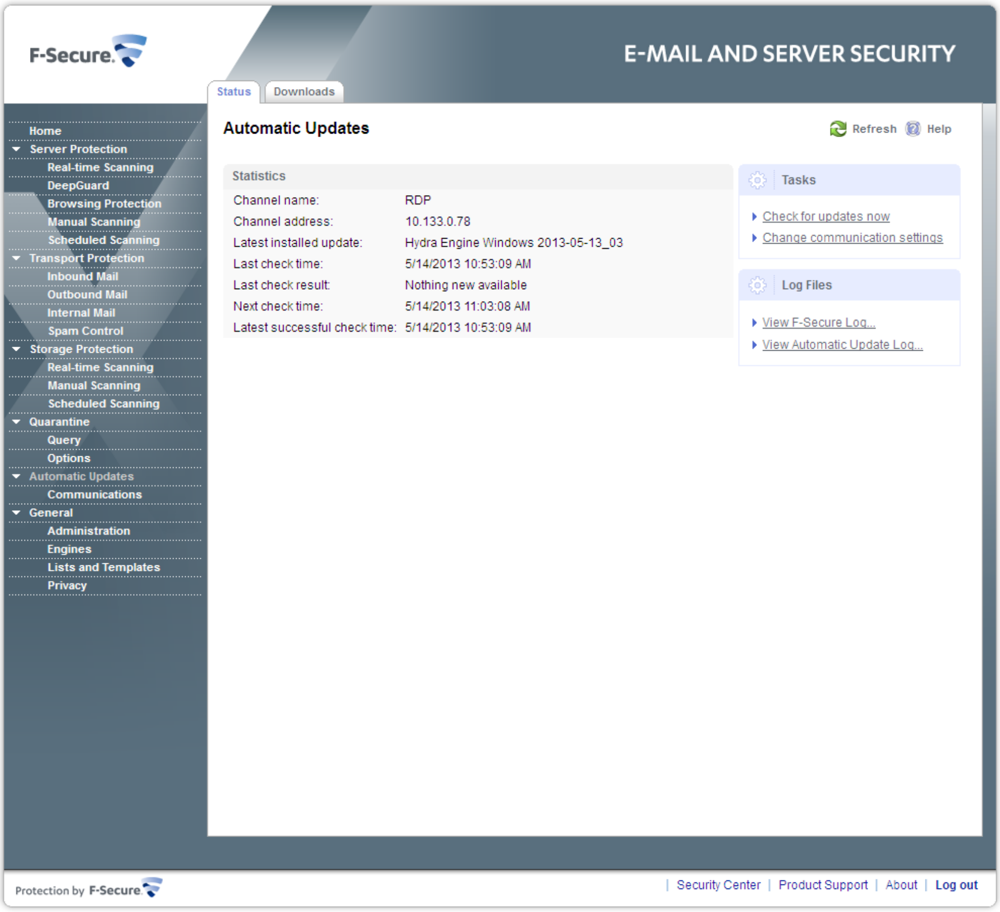
Keep rotated quarantine logs: 8 log files

Logging directory	
Quarantine log directory	Specify the path for E-mail Quarantine log files.
Logging options	
Rotate quarantine logs	Specify how often the product rotates Quarantine log files. At the end of each rotation time a new log file is created.
Keep rotated quarantine logs	Specify how many rotated log files should be stored in the Quarantine log directory.

5.8 Automatic Updates

With F-Secure Automatic Update Agent, virus and spam definition database updates are retrieved automatically when they are published to F-Secure Update Server.

Status



Automatic Updates

Statistics

Channel name:	RDP
Channel address:	10.133.0.78
Latest installed update:	Hydra Engine Windows 2013-05-13_03
Last check time:	5/14/2013 10:53:09 AM
Last check result:	Nothing new available
Next check time:	5/14/2013 11:03:08 AM
Latest successful check time:	5/14/2013 10:53:09 AM

The Status page displays information on the latest update.

Channel name
Displays the channel from where the updates are downloaded.

Channel address
Displays the address of the Automatic Updates Server.

Latest installed update
Displays the version and name of the latest installed update.

Last check time
Displays the date and time when the last update check was done.

Last check result
Displays the result of the last update check.

Next check time	Displays the date and time for the next update check.
Last successful check time	Displays the date and time when the last successful update check was done.

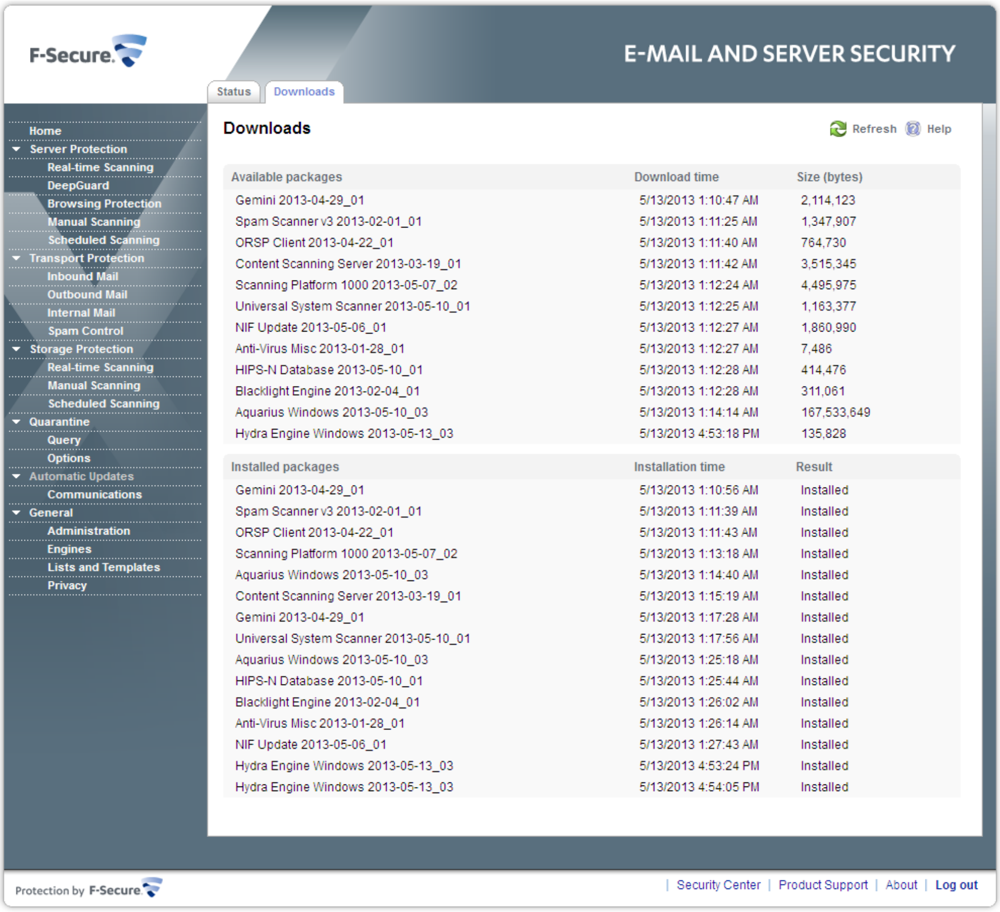
Tasks

Click **Check for updates now** to check that the product is using the latest database updates. If the virus and spam databases are not up-to-date, updates are downloaded automatically.

Click **Change communication settings** to configure how the product connects to F-Secure Update Server. For more information, see *Automatic Updates General Settings*.

5.8.1 Downloads

The Downloads page displays information about downloaded and installed update packages.



Downloads

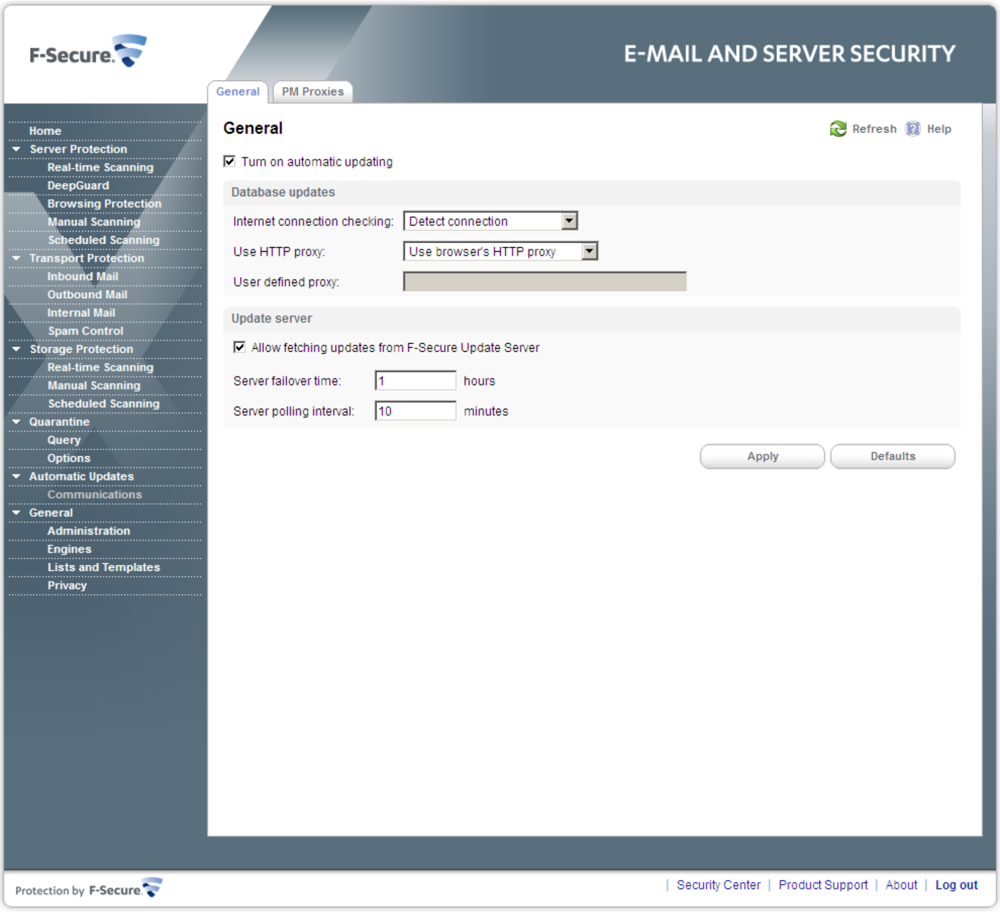
Available packages	Download time	Size (bytes)
Gemini 2013-04-29_01	5/13/2013 1:10:47 AM	2,114,123
Spam Scanner v3 2013-02-01_01	5/13/2013 1:11:25 AM	1,347,907
ORSP Client 2013-04-22_01	5/13/2013 1:11:40 AM	764,730
Content Scanning Server 2013-03-19_01	5/13/2013 1:11:42 AM	3,515,345
Scanning Platform 1000 2013-05-07_02	5/13/2013 1:12:24 AM	4,495,975
Universal System Scanner 2013-05-10_01	5/13/2013 1:12:25 AM	1,163,377
NIF Update 2013-05-06_01	5/13/2013 1:12:27 AM	1,860,990
Anti-Virus Misc 2013-01-28_01	5/13/2013 1:12:27 AM	7,486
HIPS-N Database 2013-05-10_01	5/13/2013 1:12:28 AM	414,476
Blacklight Engine 2013-02-04_01	5/13/2013 1:12:28 AM	311,061
Aquarius Windows 2013-05-10_03	5/13/2013 1:14:14 AM	167,533,649
Hydra Engine Windows 2013-05-13_03	5/13/2013 4:53:18 PM	135,828

Installed packages	Installation time	Result
Gemini 2013-04-29_01	5/13/2013 1:10:56 AM	Installed
Spam Scanner v3 2013-02-01_01	5/13/2013 1:11:39 AM	Installed
ORSP Client 2013-04-22_01	5/13/2013 1:11:43 AM	Installed
Scanning Platform 1000 2013-05-07_02	5/13/2013 1:13:18 AM	Installed
Aquarius Windows 2013-05-10_03	5/13/2013 1:14:40 AM	Installed
Content Scanning Server 2013-03-19_01	5/13/2013 1:15:19 AM	Installed
Gemini 2013-04-29_01	5/13/2013 1:17:28 AM	Installed
Universal System Scanner 2013-05-10_01	5/13/2013 1:17:56 AM	Installed
Aquarius Windows 2013-05-10_03	5/13/2013 1:25:18 AM	Installed
HIPS-N Database 2013-05-10_01	5/13/2013 1:25:44 AM	Installed
Blacklight Engine 2013-02-04_01	5/13/2013 1:26:02 AM	Installed
Anti-Virus Misc 2013-01-28_01	5/13/2013 1:26:14 AM	Installed
NIF Update 2013-05-06_01	5/13/2013 1:27:43 AM	Installed
Hydra Engine Windows 2013-05-13_03	5/13/2013 4:53:24 PM	Installed
Hydra Engine Windows 2013-05-13_03	5/13/2013 4:54:05 PM	Installed

5.8.2 Communications

Specify how the product connects to F-Secure Update Server.

Automatic Updates General Settings



General

☑ Turn on automatic updating

Database updates

Internet connection checking: Detect connection

Use HTTP proxy: Use browser's HTTP proxy

User defined proxy:

Update server

☑ Allow fetching updates from F-Secure Update Server

Server failover time: 1 hours

Server polling interval: 10 minutes

Edit **General settings** to select whether you want to use automatic updates and how often the product checks for new updates.

Turn on automatic updating	Enable and disable the automatic virus and spam database updates. By default, automatic updates are enabled.
Internet connection checking	Specify whether the product should check the connection to the Internet before trying to retrieve updates.
Use HTTP Proxy	Select whether HTTP proxy should be used. **No HTTP proxy** - HTTP proxy is not used. **Use browser's HTTP proxy** - Use the same HTTP proxy settings as the default web browser. **Manual configure HTTP proxy** - Define the HTTP proxy. Enter the proxy address in the **User defined proxy** field.

Update Server

Allow fetching updates from F-Secure Update Server

Specify whether the product should connect to F-Secure Update Server when it cannot connect to any user-specified update server. To edit the list of update sources, see *Policy Manager Proxies*.

Server failover time

Define (in hours) the failover time to connect to F-Secure Policy Manager Server or F-Secure Policy Manager Proxy.

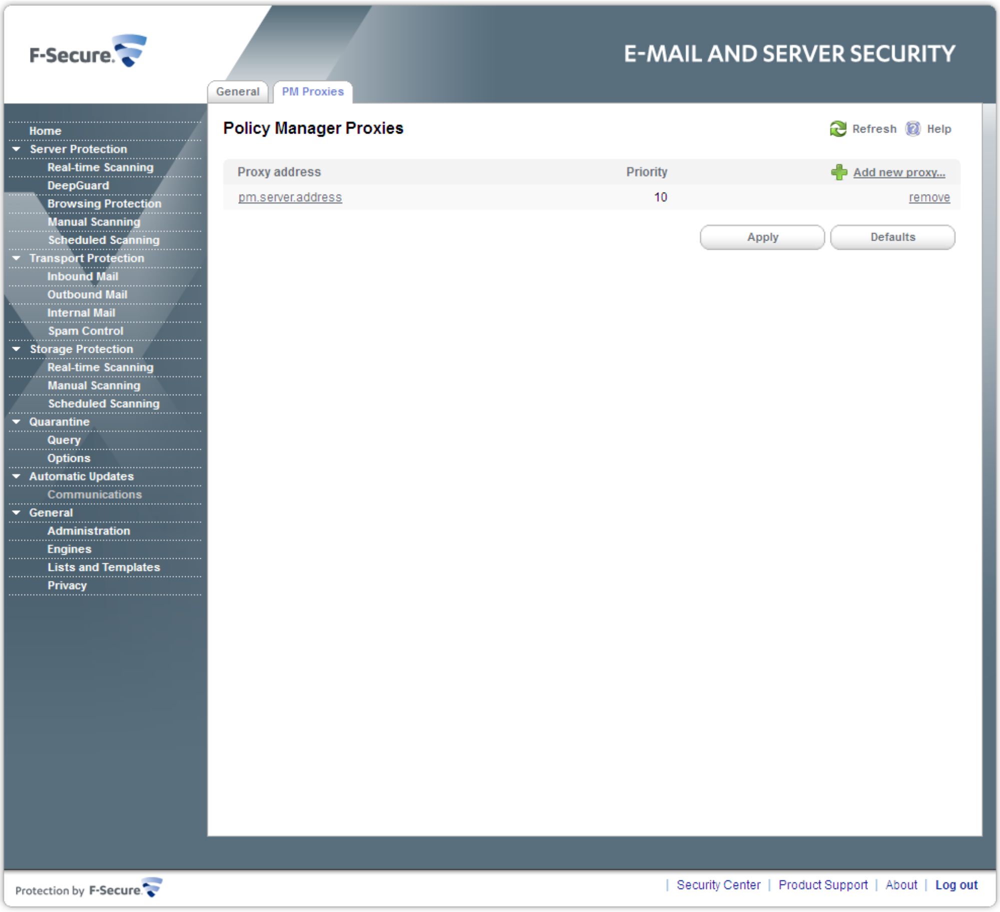
If the product cannot connect to any user-specified update server during the failover time, it retrieves the latest virus definition updates from F-Secure Update Server if Allow fetching updates from F-Secure Update Server is enabled.

Server polling interval

Define (in minutes) how often the product checks F-Secure Policy Manager Proxies for new updates.

5.8.2.1 Policy Manager Proxies

Edit the list of virus definition database update sources and F-Secure Policy Manager proxies.



Policy Manager Proxies

Proxy address	Priority	
pm.server.address	10	remove

If no update servers are configured, the product retrieves the latest virus definition updates from F-Secure Update Server automatically.

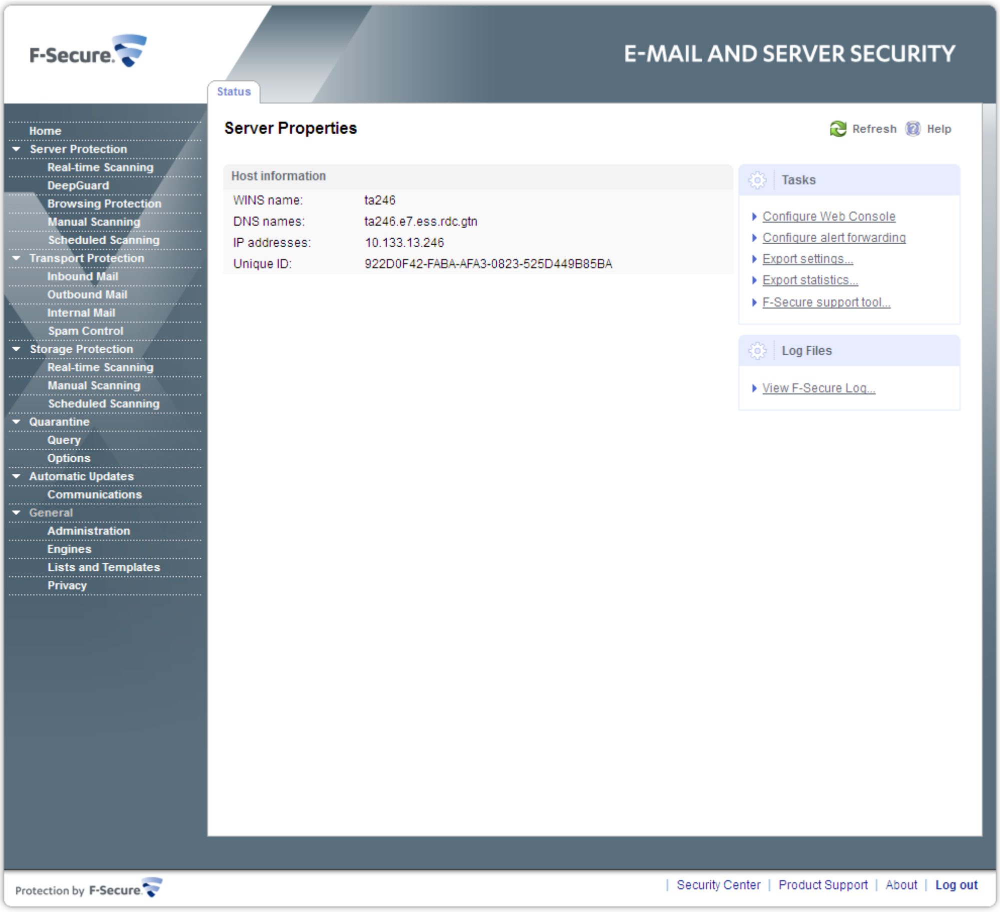
To add a new update source address to the list, follow these instructions:

1. Click **Add new proxy** to add the new entry to the list.
2. Enter the URL of the update source.
3. Edit the priority of the update source.

   The priority numbers are used to define the order in which the host tries to connect servers. Virus definition updates are downloaded from the primary sources first, secondary update sources can be used as a backup.

   The product connects to the source with the smallest priority number first (1). If the connection to that source fails, it tries to connect to the source with the next smallest number (2) until the connection succeeds.
4. Click **OK** to add the new update source to the list.

5.9 General Server Properties



Server Properties

Host information

WINS name:	ta246
DNS names:	ta246.e7.ess.rdc.gtn
IP addresses:	10.133.13.246
Unique ID:	922D0F42-FABA-AFA3-0823-525D449B85BA

The **Host information** displays the following details of the host:

- WINS name
- DNS names
- IP addresses
- Unique ID

In the centralized management mode, the page displays the following details of the F-Secure Policy Manager:

- Management server
- Last connection
- Policy file counter

- Policy file timestamp

Tasks

Click **Configure Web Console** to configure how you connect to the Web Console. For more information, see *Web Console*.

Click **Configure alert forwarding** to set where alerts are sent according to their severity level. For more information, see *Alerts*.

Click **Export settings** to open a list of all product settings in a new Internet browser window.

Click **Export statistics** to open a list of all product statistics in a new Internet browser window.

Note: To print current settings or statistics, click **Download** to download and save settings and statistics as a file.

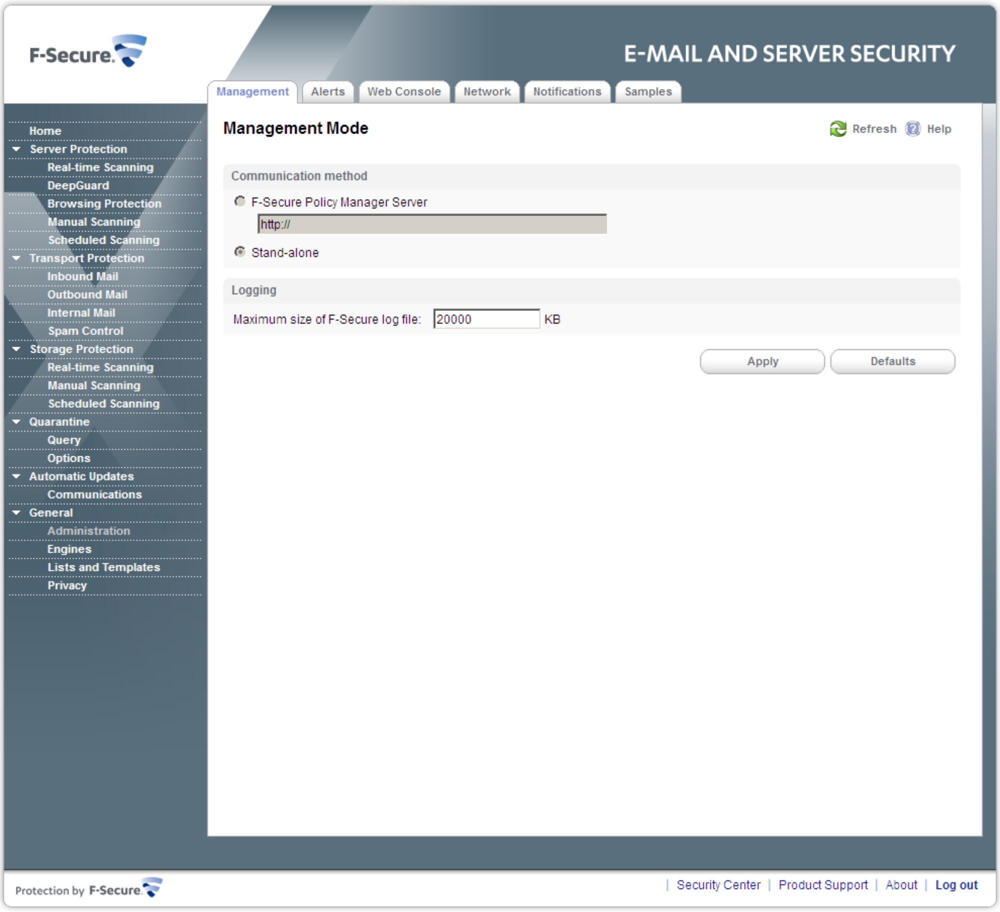
Click **F-Secure support tool** to run the F-Secure Support Tool utility to gather a report for F-Secure Technical Support.

5.9.1 Administration

Configure Administration settings to

- change the product management mode,
- specify where and how alerts are sent,
- configure the Web Console,
- define the network configuration and SMTP address for e-mail notifications, and
- specify how the samples of unsafe e-mails should be sent to F-Secure.

5.9.1.1 Management Mode



Management Mode

Communication method

○ F-Secure Policy Manager Server

http://

● Stand-alone

Logging

Maximum size of F-Secure log file: 20000 KB

Communication method

If you use F-Secure Policy Manager Server, specify the URL of F-Secure Policy Manager Server. Do not add a slash at the end of the URL.

For example: “**http://fsms.example.com**.

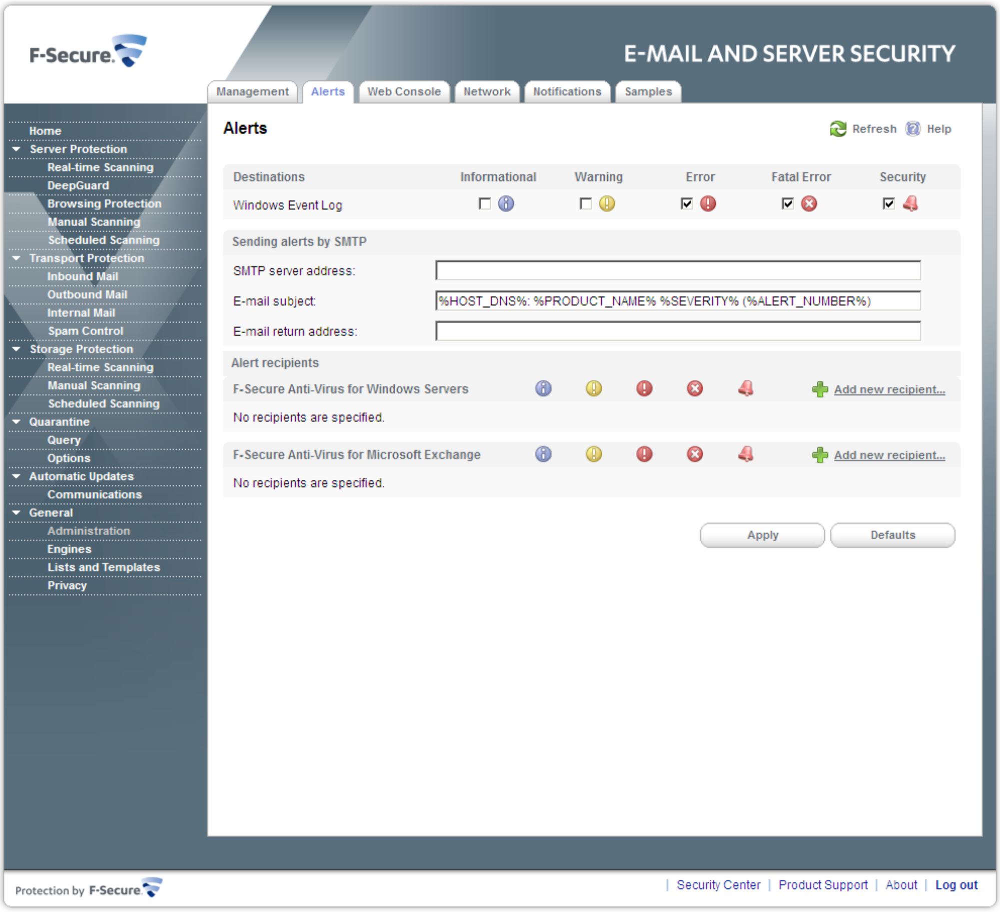
Note: F-Secure Policy Manager Server is not available if the product is installed in the stand-alone mode.

Logging

Specify the maximum file size of the F-Secure log file.

5.9.1.2 Alerts

You can specify where an alert is sent according to its severity level.



Alerts

Destinations	Informational	Warning	Error	Fatal Error	Security
Windows Event Log	□	□	☑	☑	☑

Sending alerts by SMTP

SMTP server address:

E-mail subject: %HOST_DNS%: %PRODUCT_NAME% %SEVERITY% (%ALERT_NUMBER%)

E-mail return address:

Alert recipients

F-Secure Anti-Virus for Windows Servers — Add new recipient...

No recipients are specified.

F-Secure Anti-Virus for Microsoft Exchange — Add new recipient...

No recipients are specified.

You can send the alert to any of the following:

- F-Secure Policy Manager
- Windows Event Log

If you choose to forward alerts to e-mail, specify the SMTP server address, alert message subject line and the return address of the alert e-mail.

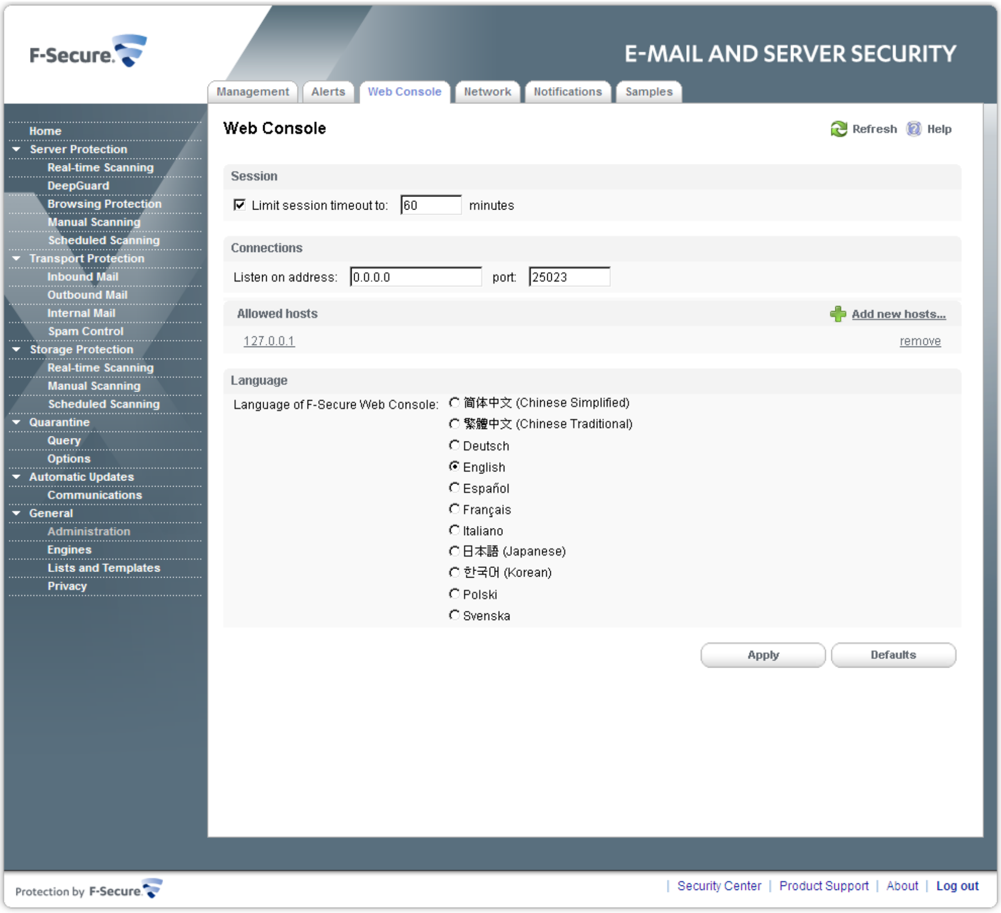
To forward alerts to an e-mail, follow these instructions:

1. Click **Add new recipient** to add a new entry in the Alert recipients table.
2. Type the e-mail address of the alert recipient.
3. Select which product component alerts you want to forward.
4. Select the types of alerts that are to be sent to this address.
5. Click **Apply**.

Note: Informational and warning-level alerts are not sent to F-Secure Policy Manager Console by default. If you use the centrally managed administration, it is recommended to have all alerts sent to F-Secure Policy Manager Console.

5.9.1.3 Web Console

Change Web Console settings to configure how you connect to the Web Console.



Web Console

Session

☑ Limit session timeout to: 60 minutes

Connections

Listen on address: 0.0.0.0 port: 25023

Allowed hosts

127.0.0.1

Language

Language of F-Secure Web Console:
○ 简体中文 (Chinese Simplified)
○ 繁體中文 (Chinese Traditional)
○ Deutsch
● English
○ Español
○ Français
○ Italiano
○ 日本語 (Japanese)
○ 한국어 (Korean)
○ Polski
○ Svenska

Session	
Limit session timeout	Specify the length of time a client can be connected to the Web Console server. When the session expires, the Web Console terminates the session and displays a warning. The default value is 60 minutes.
Connections	
Listen on address	Specify the IP address of the Web Console Server.
Port	Specify the port where the server listens for connections. The default port is 25023.

Allowed hosts

Specify a list of hosts which are allowed to connect to the Web Console.

To add a new host in the list, click **Add new hosts** and enter the IP address of the host.

To edit the host entry, click the IP address.

To delete the entry, click **remove** at the end of the host entry row.

Language

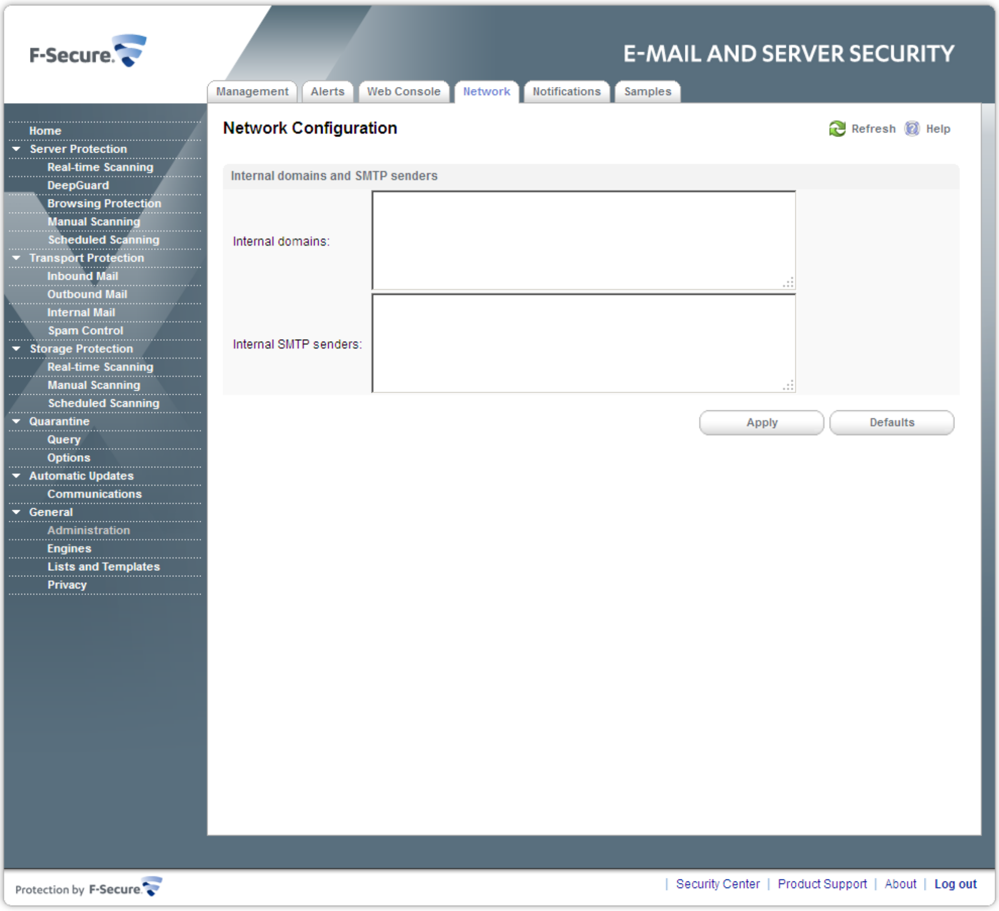
Specify the language that you want to use.

Note: Reload the Web Console after you change the language to take the new language into use.

5.9.1.4 Network Configuration

Specify internal and external domains.

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.



The mail direction is based on the **Internal domains** and **Internal SMTP senders** settings and it is determined as follows:

1. E-mail messages are considered **internal** if they come from internal SMTP sender hosts and mail recipients belong to one of the specified internal domains (internal recipients).

2. E-mail messages are considered **outbound** if they come from internal SMTP sender hosts and mail recipients do not belong to the specified internal domains (external recipients).
3. E-mail messages that come from hosts that are not defined as internal SMTP sender hosts are considered **inbound**.
4. E-mail messages submitted via MAPI or Pickup Folder are treated as if they are sent from the internal SMTP sender host.

Note: If e-mail messages come from internal SMTP sender hosts and contain both internal and external recipients, messages are split and processed as internal and outbound respectively.

Note:

On Microsoft Exchange Server 2003, internal messages which are submitted via MAPI or Pickup Folder are not delivered via transport level. Therefore, those messages do not pass Transport Protection and they are checked on the storage level only.

To scan or filter messages from internal hosts on Microsoft Exchange Server 2003, use corresponding real-time scanning settings in the storage protection section.

Internal Domains

Specify internal domains.

Separate each domain name with a space. You can use an asterisk (*) as a wildcard. For example, ***example.com internal.example.net**

Internal SMTP senders

Specify the IP addresses of hosts that belong to your organization. Specify all hosts within the organization that send messages to Exchange Edge or Hub servers via SMTP as Internal SMTP Senders.

Separate each IP address with a space. An IP address range can be defined as:

- a network/netmask pair (for example, 10.1.0.0/255.255.0.0),
- a network/nnn CIDR specification (for example, 10.1.0.0/16), or
- IPv6 address (for example, 1::, 2001::765d 2001::0-5, 2001:db8:abcd:0012::0/64, 2001:db8:abcd:abcd::/52, ::1).

You can use an asterisk (*) to match any number or dash (-) to define a range of numbers. For example, 172.16.4.4 172.16.*.1 172.16.4.0-16 172.16.250-255.*

Note: If end-users in the organization use other than Microsoft Outlook e-mail client to send and receive e-mail, it is recommended to specify all end-user workstations as Internal SMTP Senders.

Note: If the organization has Exchange Edge and Hub servers, the server with the Hub role installed should be added to the Internal SMTP Sender on the server where the Edge role is installed.

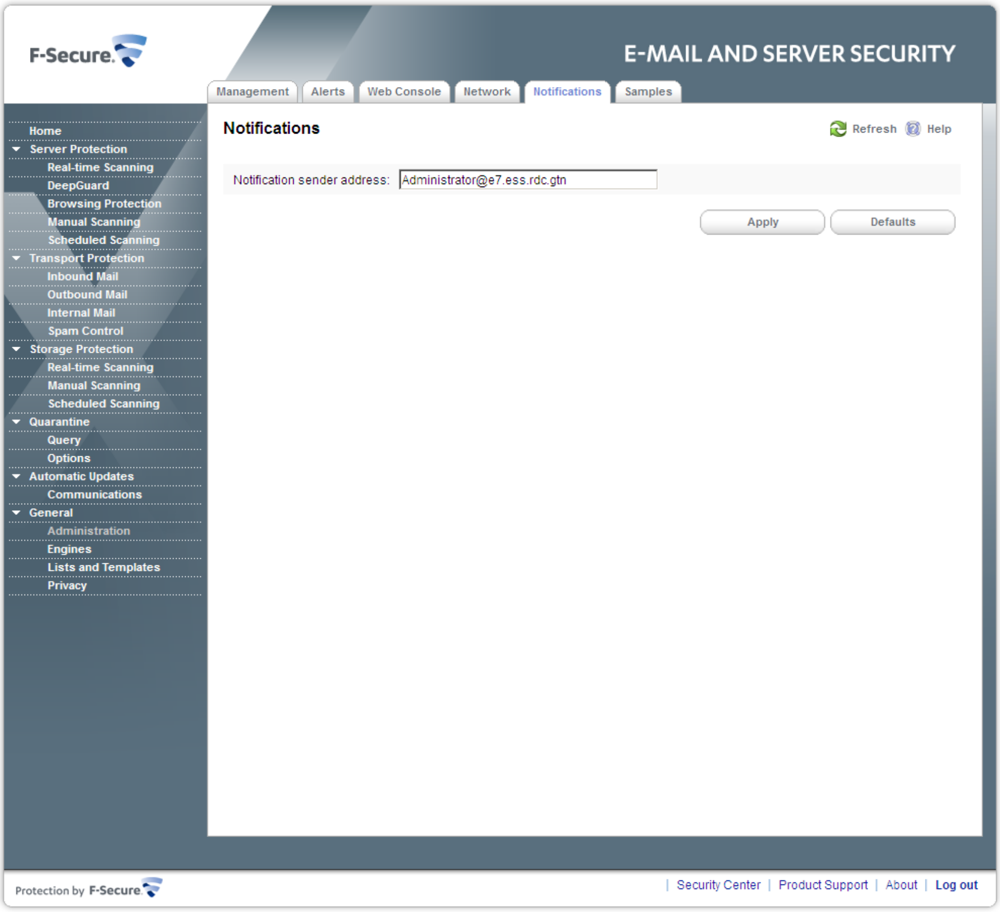
Important:

Do not specify the server where the Edge role is installed as Internal SMTP Sender.

5.9.1.5 Notifications

Specify address that is used for sending notifications to end-users.

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.



Notifications

Notification sender address: Administrator@e7.ess.rdc.gtn

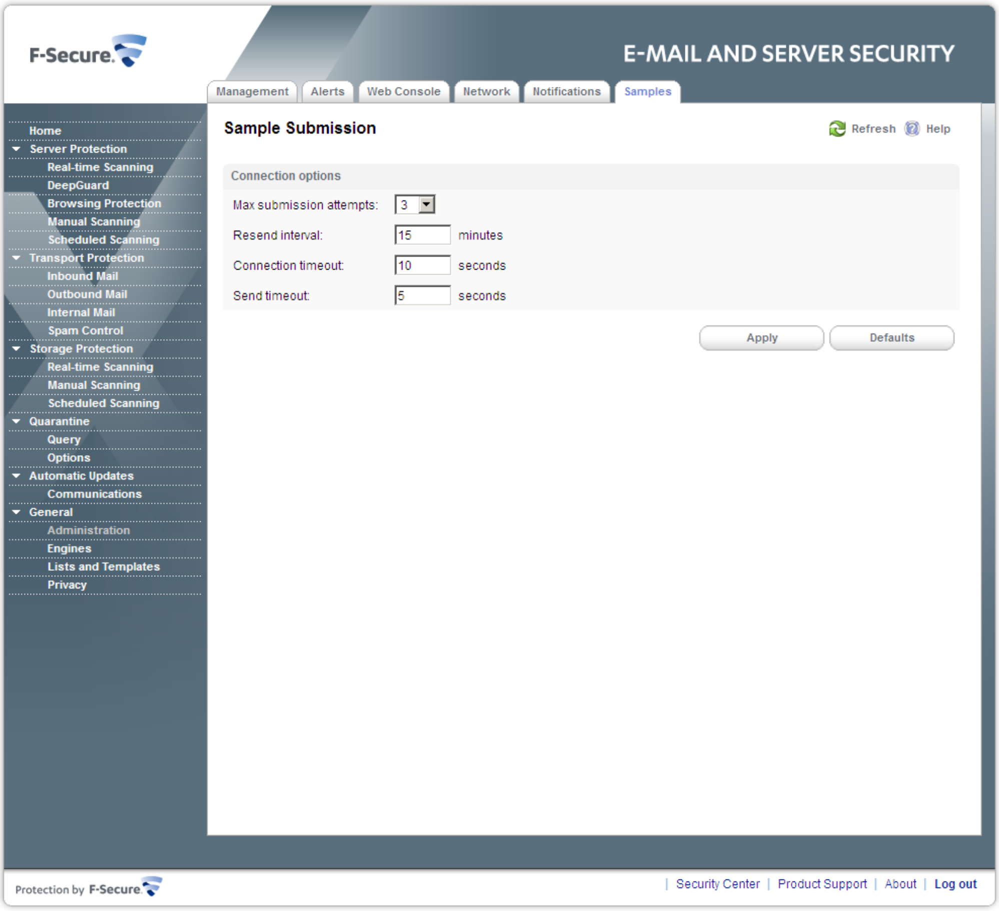
Specify **Notification Sender Address** that is used to send warning and informational messages to the end-users (for example, recipients, senders and mailbox owners).

Note: Make sure that the notification sender address is a valid SMTP address. A public folder cannot be used as the notification sender address.

5.9.1.6 Sample Submission

You can use the product to send samples of quarantined e-mails and new, yet undefined malware to F-Secure for analysis.

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.



Sample Submission

Connection options

Max submission attempts: 3

Resend interval: 15 minutes

Connection timeout: 10 seconds

Send timeout: 5 seconds

Max submission attempts

Specify how many times the product attempts to send the sample if the submission fails.

Resend interval

Specify the time interval (in minutes) how long the product should wait before trying to send the sample again if the previous submission failed.

Connection timeout

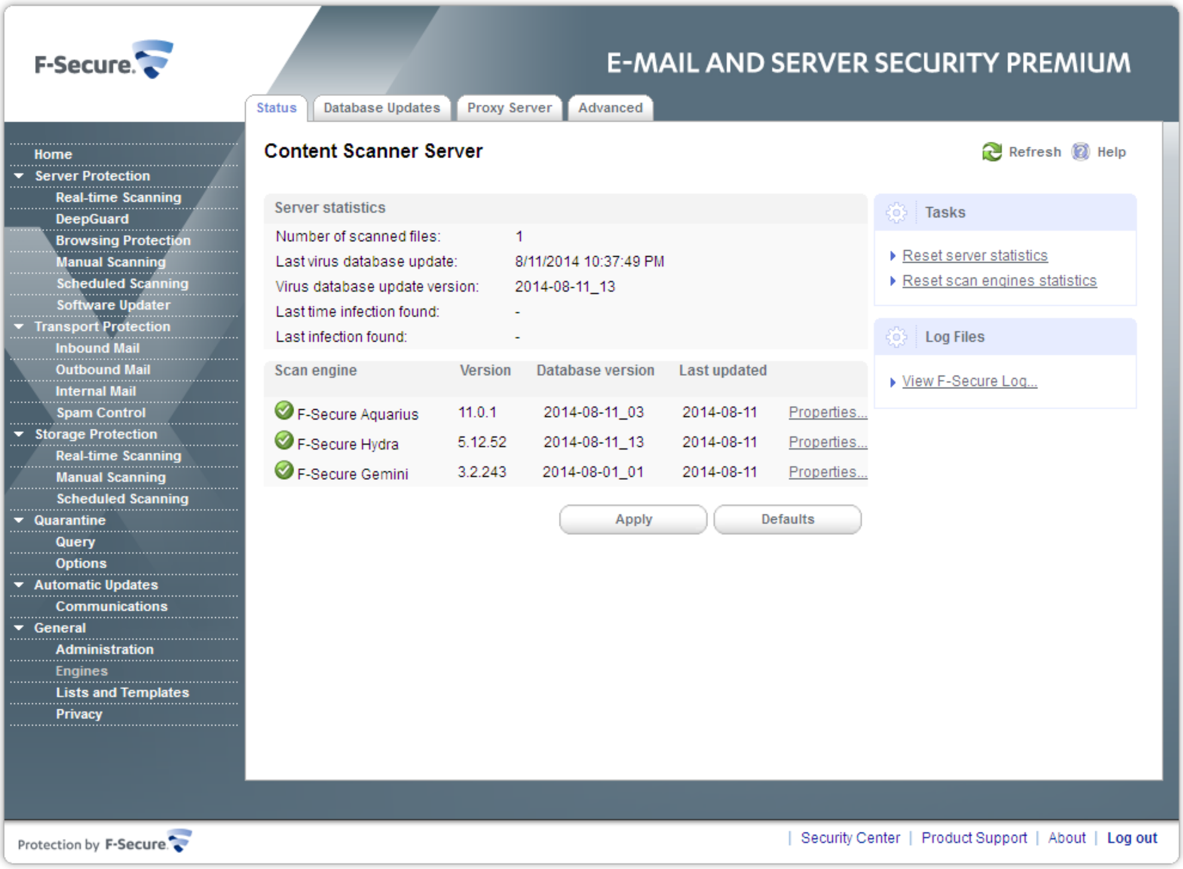
Specify the time (in seconds) how long the product tries to contact the F-Secure Hospital server.

Send timeout

Specify the time (in seconds) how long the product waits for the sample submission to complete.

5.9.2 Engines

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.



Content Scanner Server

Server statistics

Number of scanned files:	1
Last virus database update:	8/11/2014 10:37:49 PM
Virus database update version:	2014-08-11_13
Last time infection found:	-
Last infection found:	-

Scan engine	Version	Database version	Last updated	
✓ F-Secure Aquarius	11.0.1	2014-08-11_03	2014-08-11	Properties...
✓ F-Secure Hydra	5.12.52	2014-08-11_13	2014-08-11	Properties...
✓ F-Secure Gemini	3.2.243	2014-08-01_01	2014-08-11	Properties...

Content Scanner Server

Content Scanner Server hosts all scanning engines that are used when scanning e-mail content. The page displays the server statistics and the current status of the e-mail content scanning engines.

Server Statistics

Number of scanned files
The number of files that have been scanned.

Last virus database update
The last date and time when the virus definition database was updated.

Virus database update version
The version number of the virus definition database.

Last time infection found
The date and time when the last infection was found.

Last infection found
The name of the last infection that was found.

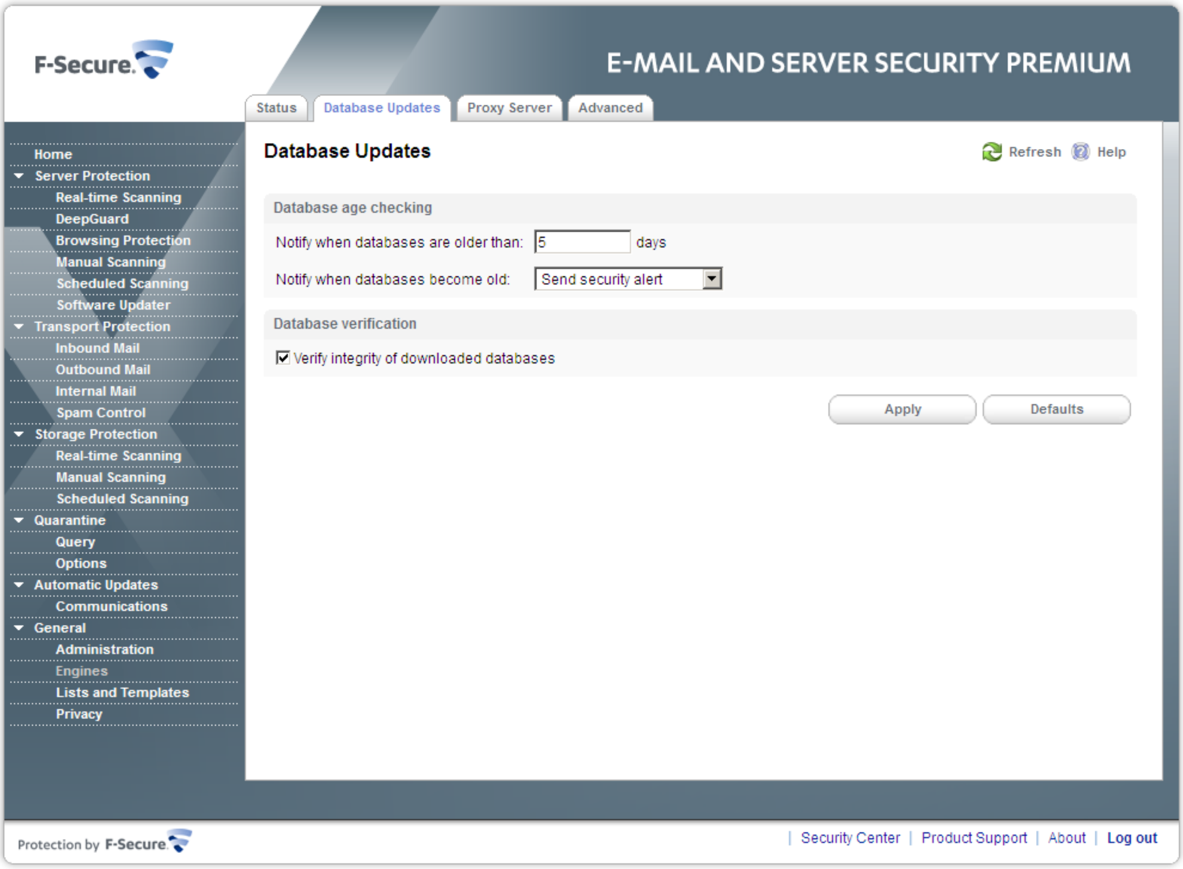
Scan Engines

The **Scan Engines** list displays e-mail content scanning engines and their database updates.

If you want to disable the scan for certain files with a specified scan engine, click **Properties** and enter the file extensions you want to exclude from the scan.

5.9.2.1 Database Updates

Configure Database Update options to set notification alerts when virus and spam definition databases are outdated.



Database Updates

Database age checking

Notify when databases are older than: 5 days

Notify when databases become old: Send security alert

Database verification

☑ Verify integrity of downloaded databases

Database age checking

Notify when databases are older than

Specify when virus definition databases are outdated. If databases are older than the specified amount of days, F-Secure Content Scanner Server sends an alert to the administrator.

Notify when databases become old

Specify the alert F-Secure Content Scanner Server service should send to the administrator when virus definition databases are not up-to-date.

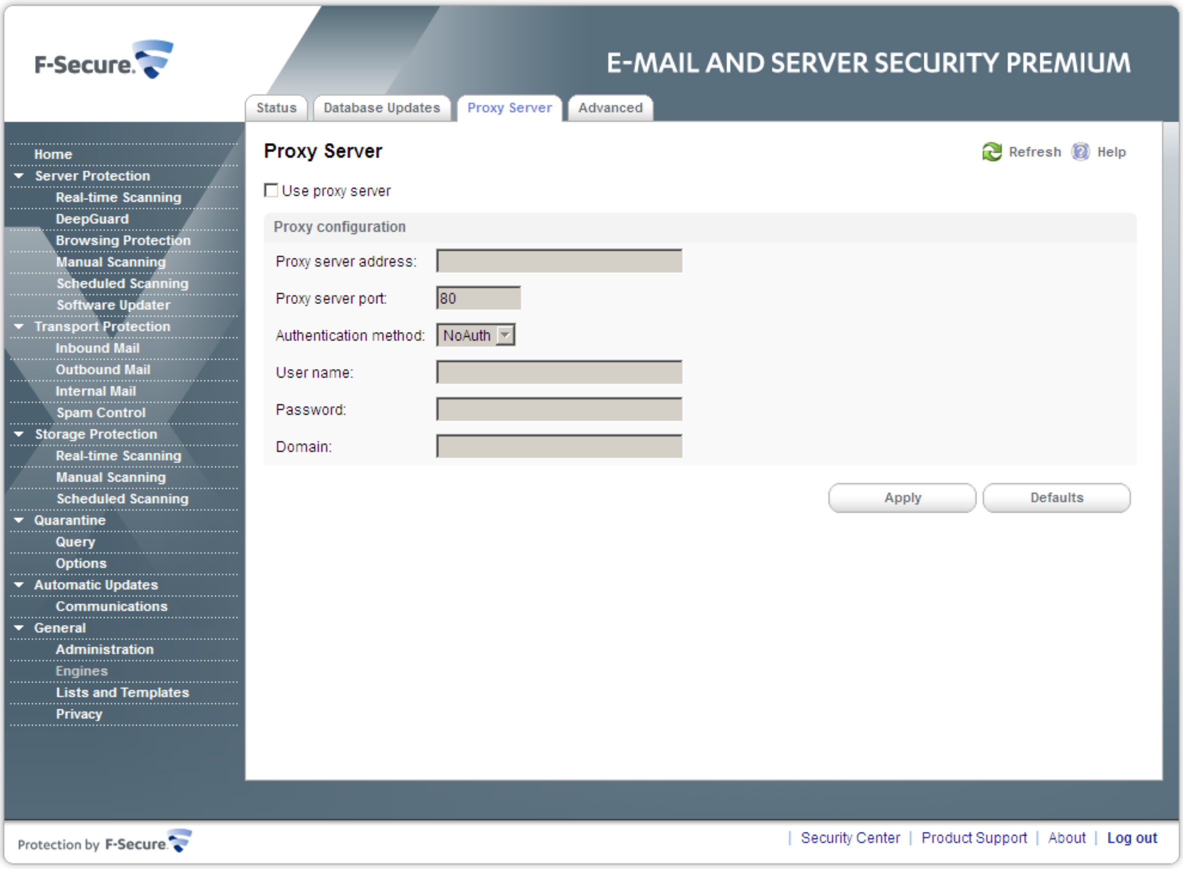
Note: Configure the Alert Forwarding table to specify where the alert is sent based on the severity level. For more information, see *Alerts*.

Database verification

Verify integrity of downloaded databases	Specify whether the product verifies that the downloaded virus definition databases are the original databases published by F-Secure Corporation and that they have not been altered or corrupted in any way before taking them to use.

5.9.2.2 Proxy Server

The product can use a proxy server to connect to the threat detection center.



Proxy Server

□ Use proxy server

Proxy configuration

Proxy server address:

Proxy server port: 80

Authentication method: NoAuth

User name:

Password:

Domain:

Use proxy server	Specify whether to use a proxy server when the product connects to the threat detection center.
Proxy configuration	
Proxy server address	Specify the address of the proxy server.
Proxy server port	Specify the port number of the proxy server.
Authentication method	Specify the authentication method to use to authenticate to the proxy server. **NoAuth** - The proxy server does not require authentication.

Basic - The proxy uses the basic authentication scheme.

NTLM - The proxy uses NTLM authentication scheme.

User name

Specify the user name for the proxy server authentication.

Password

Specify the password for the proxy server authentication.

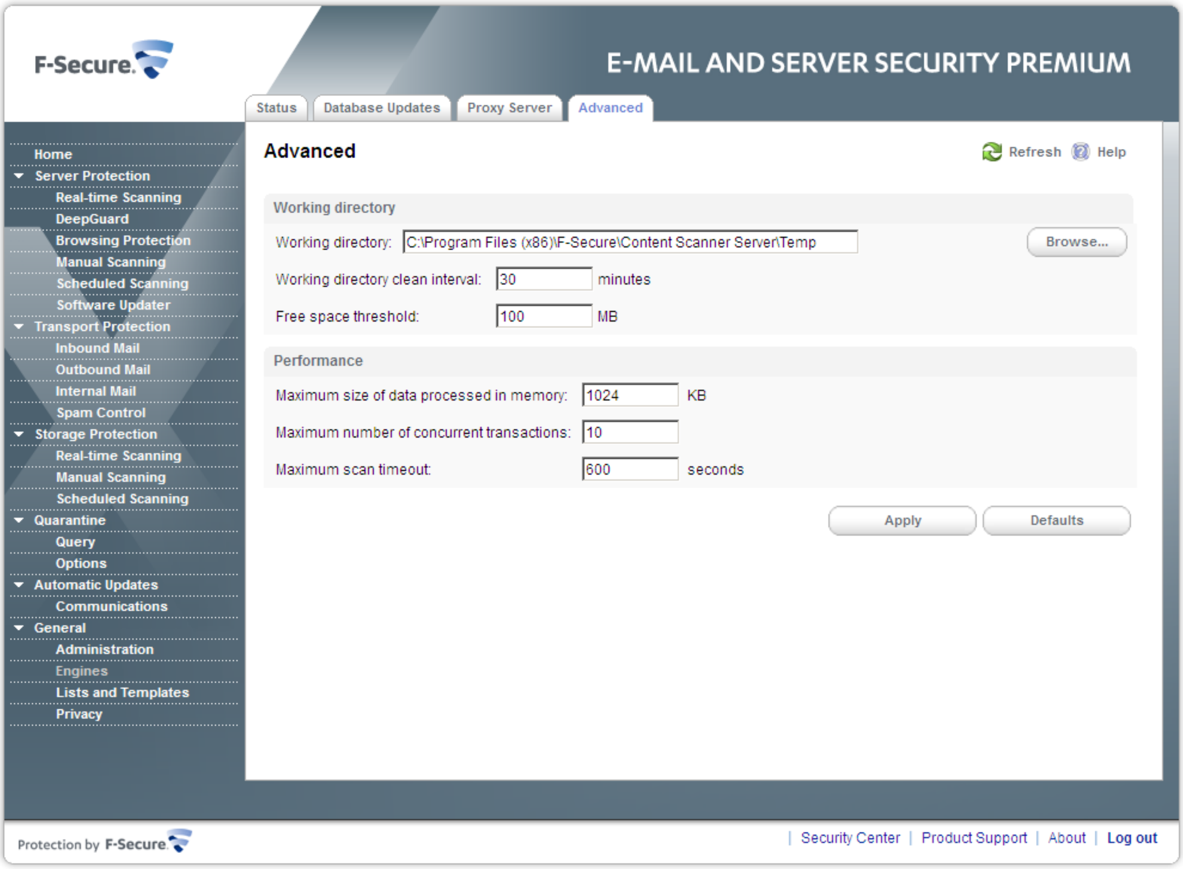
Domain

Specify the domain name for the proxy server authentication.

Note: The proxy authentication settings can be configured with the product Web Console only.

5.9.2.3 Advanced

Configure **Advanced** options to set the working directory and optimize the product performance.



Advanced

Working directory

Working directory: C:\Program Files (x86)\F-Secure\Content Scanner Server\Temp

Working directory clean interval: 30 minutes

Free space threshold: 100 MB

Performance

Maximum size of data processed in memory: 1024 KB

Maximum number of concurrent transactions: 10

Maximum scan timeout: 600 seconds

Working directory

Working directory

Specify the working directory. Enter the complete path to the field or click **Browse** to browse to the path you want to set as the new working directory.

Working directory clean interval

Specify how often the working directory is cleaned of all files that may be left there. By default, files are cleaned every 30 minutes.

Free space threshold

Set the free space threshold of the working directory. F-Secure Content Scanner Server sends an alert to the administrator when the drive has less than the specified amount of space left.

Performance

Maximum size of data processed in memory

Specify the maximum size (in kilobytes) of data to be transferred to the server via shared memory in the local interaction mode. When the amount of data exceeds the specified limit, a local temporary file will be used for data transfer.

If the option is set to zero (0), all data transfers via shared memory are disabled.

The setting is ignored if the local interaction mode is disabled.

Maximum number of concurrent transactions

Specify how many files the product should process simultaneously.

Maximum scan timeout

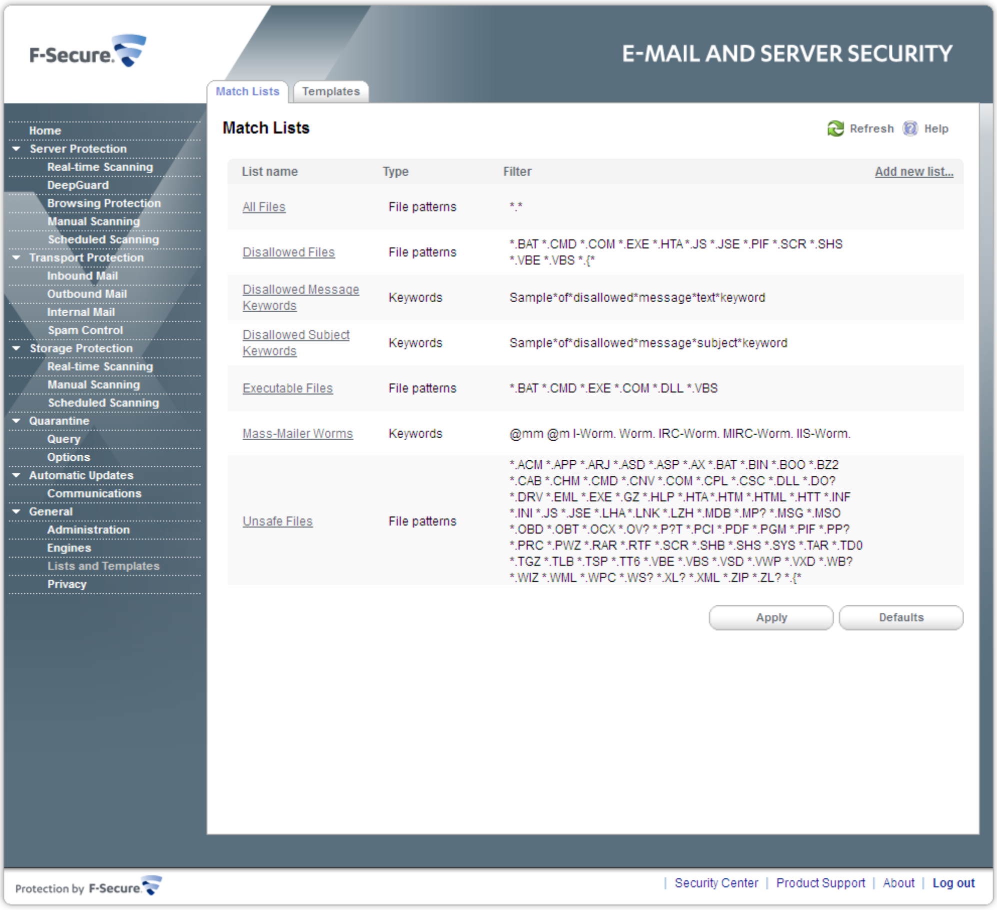
Specify how long a scan task can be carried out before it is automatically cancelled.

5.9.3 Lists and Templates

Note: These settings are used only if F-Secure Anti-Virus for Microsoft Exchange is installed with the product, otherwise these settings are not available.

5.9.3.1 Match Lists

Match lists are lists of file name patterns, keywords, or e-mail addresses that can be used with certain product settings.



Match Lists

List name	Type	Filter
All Files	File patterns	*.*
Disallowed Files	File patterns	*.BAT *.CMD *.COM *.EXE *.HTA *.JS *.JSE *.PIF *.SCR *.SHS *.VBE *.VBS *.{*
Disallowed Message Keywords	Keywords	Sample*of*disallowed*message*text*keyword
Disallowed Subject Keywords	Keywords	Sample*of*disallowed*message*subject*keyword
Executable Files	File patterns	*.BAT *.CMD *.EXE *.COM *.DLL *.VBS
Mass-Mailer Worms	Keywords	@mm @m I-Worm. Worm. IRC-Worm. MIRC-Worm. IIS-Worm.
Unsafe Files	File patterns	*.ACM *.APP *.ARJ *.ASD *.ASP *.AX *.BAT *.BIN *.BOO *.BZ2 *.CAB *.CHM *.CMD *.CNV *.COM *.CPL *.CSC *.DLL *.DO? *.DRV *.EML *.EXE *.GZ *.HLP *.HTA *.HTM *.HTML *.HTT *.INF *.INI *.JS *.JSE *.LHA *.LNK *.LZH *.MDB *.MP? *.MSG *.MSO *.OBD *.OBT *.OCX *.OV? *.P?T *.PCI *.PDF *.PGM *.PIF *.PP? *.PRC *.PWZ *.RAR *.RTF *.SCR *.SHB *.SHS *.SYS *.TAR *.TD0 *.TGZ *.TLB *.TSP *.TT6 *.VBE *.VBS *.VSD *.VWP *.VXD *.WB? *.WIZ *.WML *.WPC *.WS? *.XL? *.XML *.ZIP *.ZL? *.{*

Click the name of an existing match list to edit the list or **Add new list** to create a new match list.

List name

Select the match list you want to edit. If you are creating a new match list, specify the name for the new match list.

Type

Specify whether the list contains keywords, file patterns or e-mail addresses.

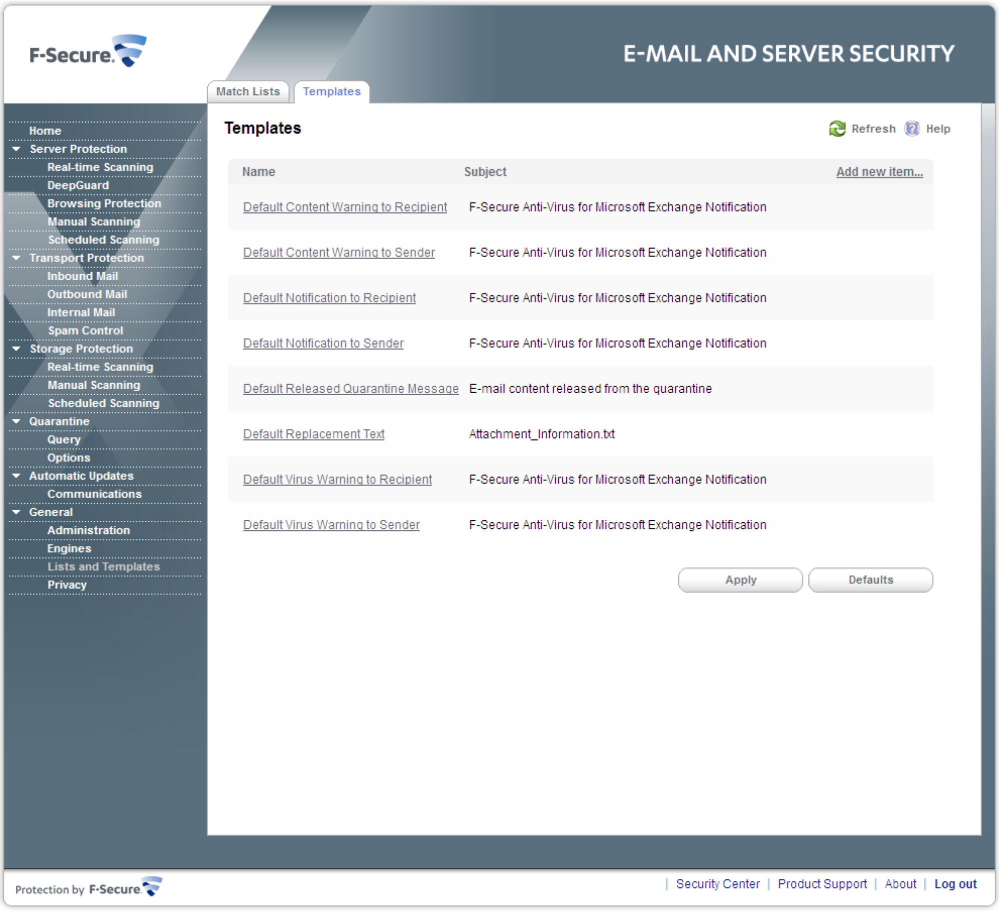
Filter

Specify file names, extensions, keywords or e-mail addresses that the match list contains. You can use wildcards.

Note: To add multiple patterns to the filter, start each item from a new line.

5.9.3.2 Message Templates

Message templates can be used for notification messages.



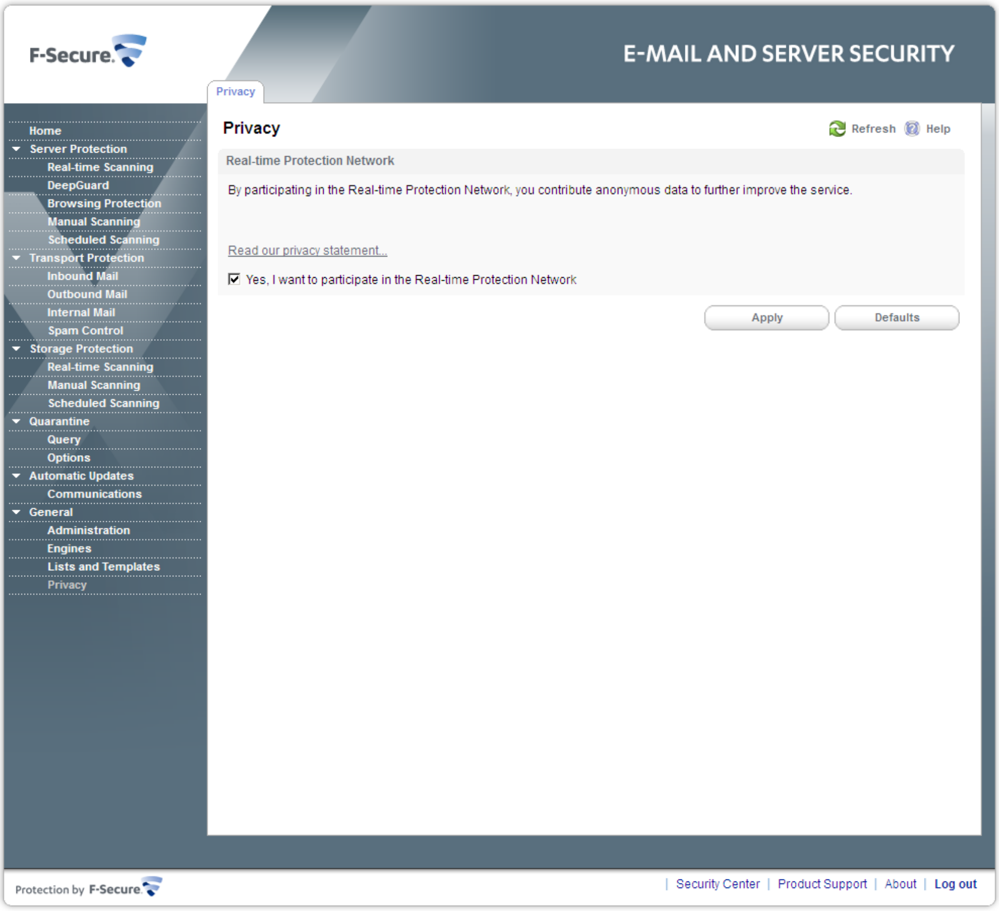
Templates

Name	Subject	Add new item...
Default Content Warning to Recipient	F-Secure Anti-Virus for Microsoft Exchange Notification	
Default Content Warning to Sender	F-Secure Anti-Virus for Microsoft Exchange Notification	
Default Notification to Recipient	F-Secure Anti-Virus for Microsoft Exchange Notification	
Default Notification to Sender	F-Secure Anti-Virus for Microsoft Exchange Notification	
Default Released Quarantine Message	E-mail content released from the quarantine	
Default Replacement Text	Attachment_Information.txt	
Default Virus Warning to Recipient	F-Secure Anti-Virus for Microsoft Exchange Notification	
Default Virus Warning to Sender	F-Secure Anti-Virus for Microsoft Exchange Notification	

Click the name of an existing template to edit it or **Add new item** to create a new template.

Name	Select the template you want to edit. If you are creating a new template, specify the name for the new template.
Subject/Filename	Specify the subject line of the notification message.
Message body	Specify the notification message text.
	For more information about the variables you can use in notification messages, see *Variables in Warning Messages*.
Description	Specify a short description for the template.

5.9.4 Privacy



Privacy

Real-time Protection Network

By participating in the Real-time Protection Network, you contribute anonymous data to further improve the service.

Read our privacy statement...

☑ Yes, I want to participate in the Real-time Protection Network

Real-time Protection Network is an online service which provides rapid response against the latest Internet-based threats.

As a contributor to Real-time Protection Network, you can help us to strengthen the protection against new and emerging threats. Real-time Protection Network collects statistics of certain unknown, malicious or suspicious applications and what they do on your device. This information is anonymous and sent to F-Secure Corporation for combined data analysis. We use the analyzed information to improve the security on your device against the latest threats and malicious files.

For the full Real-time Protection Network policy, consult our web site: *http://www.f-secure.com/en/web/home_global/rtpn-privacy*

E-mail Quarantine Management

Topics:

6.1 Introduction

You can manage and search quarantined mails with the Web Console. You can search for quarantined content by using different search criteria, including the quarantine ID, recipient and sender address, the time period during which the message was quarantined, and so on. You can reprocess and delete messages, and specify storage and automatic deletion times based on the reason for quarantining the message.

If you have multiple product installations, you can manage the quarantined content on all of them from one single Web Console.

The E-mail Quarantine consists of:

- Quarantine Database, and
- Quarantine Storage.

Quarantine Database

The E-mail Quarantine database contains information about the quarantined messages and attachments. If there are several product installations in the network, they can either have their own quarantine databases, or they can use a common quarantine database. An SQL database server is required for the quarantine database.

👉 **Note:** For more information on the SQL database servers that can be used for deploying the quarantine database, consult the product Deployment Guide.

Quarantine Storage

The E-mail Quarantine storage where the quarantined messages and attachments are stored is located on the server where the product is installed. If there are several installations of the product in the network, they all have their own storages. The storages are accessible from a single Web Console.

6.1.1 Quarantine Reasons

The E-mail Quarantine storage can store:

- Messages and attachments that are infected and cannot be automatically disinfected.**(Infected)**
- Suspicious content, for example password-protected archives, nested archives and malformed messages.**(Suspicious)**
- Messages and attachments that have been blocked by their filename or filename extension.**(Disallowed attachment)**
- Messages that contain disallowed words in the subject line or message body. **(Disallowed content)**
- Messages that are considered as spam.**(Spam)**
- Messages that contain grayware.**(Grayware)**
- Files that could not be scanned, for example severely corrupted files.**(Scan failure)**
- Messages that contain patterns that can be assumed to be a part of a spam or virus outbreak.**(Unsafe)**

6.2 Configuring E-mail Quarantine Options

In stand-alone installations, all the quarantine settings can be configured on the `Quarantine` page in the Web Console. For more information on the settings, see *Quarantine*.

In centrally managed installations, the quarantine settings are configured with F-Secure Policy Manager in the `F-Secure Anti-Virus for Microsoft Exchange / Settings / Quarantine` branch. For more information, see *Quarantine*.

The actual quarantine management is done through the Web Console.

6.3 Quarantine Status

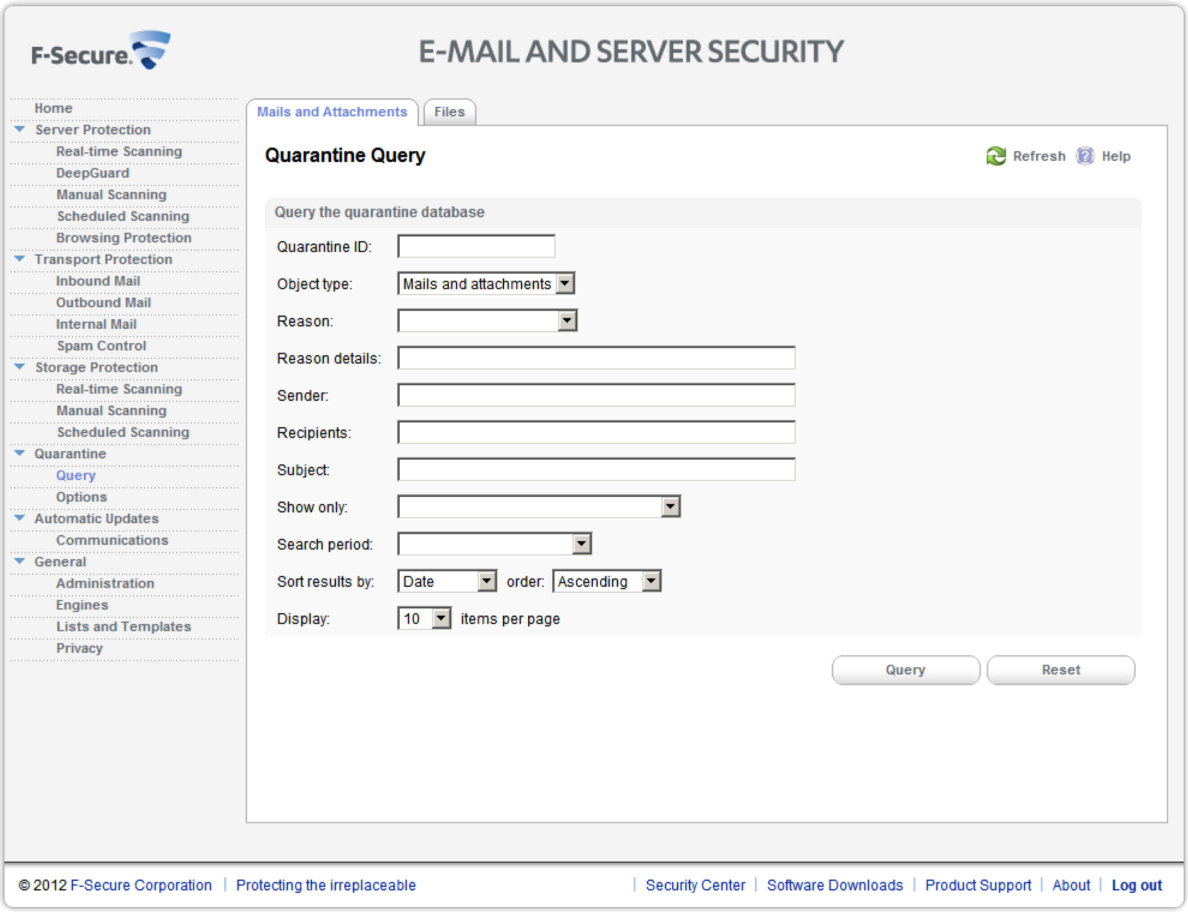
The Quarantine status page displays the number of quarantined items in each quarantine category, and the total size of the quarantine.

Quarantine Logging

To view the E-mail Quarantine Log, open the `Quarantine` page. Then click the **View Quarantine Log** link.

6.4 Searching the Quarantined Content

You can search the quarantined e-mail messages and attachments on the `Quarantine Query` page in the Web Console.



Quarantine Query

Query the quarantine database

Quarantine ID:

Object type: Mails and attachments

Reason:

Reason details:

Sender:

Recipients:

Subject:

Show only:

Search period:

Sort results by: Date order: Ascending

Display: 10 items per page

You can use any of the following search criteria. Leave all fields empty to see all quarantined content.

Quarantine ID	Enter the quarantine ID of the quarantined message. The quarantine ID is displayed in the notification sent to the user about the quarantined message and in the alert message.
Object type	Select the type of the quarantined content. **Mails and attachments** - Search for both quarantined mails and attachments.

Attachment - Search for quarantined attachments.

Mail - Search for quarantined mails.

Reason

Select the quarantining reason from the drop-down menu. For more information, see *Quarantine Reasons*.

Reason details

Specify details about the scanning or processing results that caused the message to be quarantined. For example:

The message is infected - specify the name of the infection that was found in an infected message.

Sender

Enter the e-mail address of the message sender. You can only search for one address at a time, but you can widen the search by using the wildcards.

Recipients

Enter the e-mail address of the message recipient.

Subject

Enter the message subject to be used as a search criteria.

Message ID

Enter the Message ID of the quarantined mail.

Sender Host

Enter the address of the sender mail server or client.

Note: You can specify Message ID and Sender Host only when you search for quarantined mails.

Name

Enter the file name of the quarantined attachment.

Location

Enter the location of the mailbox or public folder where the quarantined attachment was found.

Note: You can specify Name and Location only when you search for quarantined attachments.

Show only

You can use this option to view the current status of messages that you have set to be reprocessed, released or deleted. Because processing a large number of e-mails may take time, you can use this option to monitor how the operation is progressing.

The options available are:

`Unprocessed e-mails` - Displays only e-mails that the administrator has not set to be released, reprocessed or deleted.

	`E-mails to be released` - Displays only e-mails that are currently set to be released, but have not been released yet. `E-mails to be reprocessed` - Displays only e-mails that are currently set to be reprocessed, but have not been reprocessed yet. **E-mails to be released or reprocessed** - Displays e-mails that are currently set to be reprocessed or released, but have not been reprocessed or released yet.
Search period	Select the time period when the data has been quarantined. Select **Exact start and end dates** to specify the date and time (year, month, day, hour, minute) when the data has been quarantined.
Sort Results	Specify how the search results are sorted by selecting one of the options in the `Sort Results` drop-down listbox: based on `Date`. `Sender`. `Recipients`. `Subject` or `Reason`.
Display	Select how many items you want to view per page.

1. Click **Query** to start the search. The `Quarantine Query Results` page is displayed once the query is completed.
2. If you want to clear all the fields on the `Query` page, click **Reset**.

Using Wildcards

You can use the following SQL wildcards in the quarantine queries:

Wildcard	Explanation
%	Any string of zero or more characters.
_ (underscore)	Any single character.
[ ]	Any single character within the specified range ([a-f]) or set ([abcdef]).
[^]	Any single character not within the specified range ([^a-f]) or set ([^abcdef]).

Note: If you want to search for '%', '_' and '[' as regular symbols in one of the fields, you must enclose them into square brackets: '[%]', '[_]', '[[]'

6.5 Query Results Page

The Quarantine Query Results page displays a list of mails and attachments that were found in the query. To view detailed information about a quarantined content, click the Quarantine ID (QID) number link in the QID column. For more information, see *Viewing Details of the Quarantined Message*.

The Query Results page displays status icons of the content that was found in the search:

Icon	E-mail status
✉	Quarantined e-mail. The administrator has not specified any actions to be taken on this e-mail.
✉	Quarantined e-mail with attachments. The administrator has not specified any actions to be taken on this e-mail.
✉	Quarantined e-mail that the administrator has set to be released. The release operation has not been completed yet.
✉	Quarantined e-mail that the administrator has set to be reprocessed. The reprocessing operation has not been completed yet.
✉	Quarantined e-mail that the administrator has set to be deleted. The deletion operation has not been completed yet.
✉	Quarantined e-mail that the administrator has submitted to F-Secure for analysis.
✉	Quarantined e-mail set to be released, which failed.
✉	Quarantined e-mail set to be reprocessed, which failed.
✉	Quarantined e-mail set to be submitted to F-Secure, which failed.

For information how to process quarantined content, see *Quarantine Operations*.

6.5.1 Viewing Details of the Quarantined Message

To view the details of a quarantined message or attachment, do the following:

1. On the **Query Search Results** page, click the Quarantine ID (QID) number link in the QID column.
2. The **Quarantined Content Details** page opens.

The Quarantined Content Details page displays the following information about the quarantined mails and attachments:

QID	Quarantine ID.
Submit time	The date and time when the item was placed in the quarantine.
Processing server	The server that processed the message. **Quarantined messages only.**
Sender	The address of the message sender
Recipients	The addresses of all the message recipients.
Sender host	The address of the sender mail server or client. **Quarantined messages only.**
Location	The location of the mailbox or public folder where the quarantined attachment was found. **Quarantined attachments only.**
Subject	The message subject
Message size	The size of the quarantined message. **Quarantined messages only.**
Attachment name	The name of the attachment. **Quarantined attachments only.**
Attachment size	The size of the attachment file. **Quarantined attachments only.**
Quarantine reason	The reason why the content was quarantined.

1. Click the **Show** link to access the content of the quarantined message.
2. Click **Download** to download the quarantined message or attachment to your computer to check it.

⚠ **Caution:**

In many countries, it is illegal to read other people's messages.

For information how to process quarantined content, see *Quarantine Operations*.

6.6 Quarantine Operations

Quarantined mails and attachments can be reprocessed, released and removed from the E-mail Quarantine storage after you have searched the quarantined content you want to process.

Quarantined Mail Operations

You can select an operation to perform on the messages that were found in the query:

- Click **Reprocess** to scan the currently selected e-mail again, or click **Reprocess All** to scan all e-mail messages that were found. For more information, see *Reprocessing the Quarantined Content*.
- Click **Release** to deliver the currently selected e-mail without further processing, or click **Release All** to deliver all e-mail messages that were found. For more information, see *Releasing the Quarantined Content*.

  Caution:

  Releasing quarantined content entails a security risk, because the content is delivered to the recipient without being scanned.
- Click **Delete** to delete the currently selected e-mail from the quarantine, or click **Delete All** to delete all e-mail messages that were found. For more information, see *Removing the Quarantined Content*.
- Click **Send to F-Secure** to submit a sample of quarantined content to F-Secure for analysis.

Quarantined Attachment Operations

You can select an operation to perform on the attachments that were found in the query:

- Click **Send** to deliver the currently selected attachment, or click **Send All** to deliver all attachments that were found.

  Attachments sent from the quarantine go through the transport and storage protection and are scanned again. For more information, see *Releasing the Quarantined Content*.
- Click **Delete** to delete the currently selected e-mail from the quarantine, or click **Delete All** to delete all e-mail messages that were found. For more information, see *Removing the Quarantined Content*.

6.6.1 Reprocessing the Quarantined Content

When quarantined content is reprocessed, it is scanned again, and if it is found clean, it is sent to the intended recipients.

Note: if you reprocess a quarantined spam e-mail, the reprocessed content may receive a lower spam score than it did originally and it may reach the recipient.

For example, if some content was placed in the E-mail Quarantine because of an error situation, you can use the time period when the error occurred as search criteria, and then reprocess the content. This is done as follows:

1. Open the `Quarantine > Query` page in the Web Console.
2. Select the start and end dates and times of the quarantining period from the `Start time` and `End Time` drop-down menus.
3. If you want to specify how the search results are sorted, select the sorting criteria and order from the `Sort results` and `order` drop-down menus.
4. Select the number of items to be displayed on a results page from the `Display` drop-down menu.
5. Click the **Query** button.
6. When the query is finished, the query results page is displayed. Click the **Reprocess All** button to reprocess the displayed quarantined content.
7. The progress of the reprocessing operation is displayed in the Web Console.
   - The e-mails that have been reprocessed and found clean are delivered to the intended recipients. They are also automatically deleted from the quarantine.
   - E-mails that have been reprocessed and found infected, suspicious or broken return to the quarantine.

6.6.2 Releasing the Quarantined Content

When you release quarantined content, the product sends the content to intended recipients without any further processing on the protection level that blocked the content previously. For example, if you have a password-protected archive in the quarantine that you want to deliver to the recipient, you can release it.

Caution:

Releasing quarantined content is a security risk, as the content is delivered to the recipient without being scanned.

If you release a message that was quarantined on the transport protection level, the released message is not checked on the transport level again, but the real-time scanning on the storage protection level processes the message before it is delivered to the mailbox of the recipient. If the storage level check catches the message, it is not released and remains in the Quarantine.

If you need to release a quarantined message, follow these instructions:

1. Open the `Quarantine > Query` page in the Web Console.
2. Enter the Quarantine ID of the message in the `Quarantine ID` field. The Quarantine ID is included in the notification message delivered to the user.
3. Click **Query** to find the quarantined content.
4. Quarantine may contain either the original e-mail message or just the attachment that was quarantined.
   a. When the quarantined content is an e-mail message, click the **Release** to release the displayed quarantined content. The `Release Quarantined Content` dialog opens.
   b. When the quarantine contains an attachment, click **Send**. The quarantined attachment is attached to the template specified in **General Quarantine Options** that is sent to the recipient.
5. Specify whether you want to release the content to the original recipient or specify an address where the content is to be forwarded.

   Note: It may not be legal to forward the e-mail to anybody else than the original recipient.
6. Specify what happens to the quarantined content after it has been released by selecting one of the `Action after release` options:
   - Leave in the quarantine
   - Delete from the quarantine
7. Click **Release** or **Send**. The content is now delivered to the recipient.

6.6.3 Removing the Quarantined Content

Quarantined messages are removed from the quarantine based on the currently configured quarantine retention and cleanup settings. For an example on how to configure those settings, see *Deleting Old Quarantined Content Automatically*.

If you want to remove a large amount of quarantined messages at once, for example all the messages that have been categorized as spam, do the following:

1. Open the `Quarantine > Query` page in the Web Console.
2. Select the quarantining reason, `Spam`, from the `Reason` drop-down listbox.
3. Click **Query**.
4. When the query is finished, the query results page is displays all quarantined messages that have been classified as spam. Click the **Delete All** button to delete all the displayed quarantined content.
5. You are prompted to confirm the deletion. Click **OK**. The content is now removed from the quarantine.

6.6.4 Deleting Old Quarantined Content Automatically

Quarantined messages and attachments are deleted automatically, based on the **Quarantine Retention and Cleanup** settings in the **Maintenance** tab on the **Quarantine > Options** page. By default, all types of quarantined content are stored in quarantine for one month, and quarantine clean-up task is executed once an hour.

You can specify exceptions to the default retention and clean-up times in the `Exceptions` table. These exceptions are based on the quarantine category. If you want, for example, to have infected messages deleted sooner, you can specify an exception rule for them as follows:

1. Go to the `Quarantine` > `Options` page.
2. Open the **Maintenance** tab.

3. Click **Add new exception** at the **Exceptions** table. A **New Quarantine Cleanup Exception** dialog opens.
4. Select the Quarantine category for which you want to specify the exception. Specify a **Retention period** and a **Cleanup interval** for the selected category.
5. To turn on the exception, make sure that the **Active** check box is selected. Click **Ok**.
6. Click **Apply** to apply the new changes.

6.7 Moving the E-mail Quarantine Storage

When you want to change the E-mail Quarantine storage location either using the F-Secure Policy Manager Console or the Web Console, note that the product does not create the new directory automatically. Before you change the E-mail Quarantine storage directory, make sure that the directory exists and it has proper security permissions.

You can use the `xcopy` command to create and change the E-mail Quarantine storage directory by copying the existing directory with the current ownership and ACL information. In the following example, the E-mail Quarantine storage is moved from `C:\Program Files\F-Secure\Quarantine Manager\quarantine` to `D:\Quarantine`:

1. Stop F-Secure Quarantine Manager service to prevent any quarantine operations while you move the location of the Quarantine storage. Run the following command from the command prompt:`net stop "F-Secure Quarantine Manager"`
2. Run the following command from the command prompt to copy the current content to the new location:
   ```
   xcopy "C:\Program Files\F-Secure\Quarantine Manager\quarantine"
   D:\Quarantine\ /O /X /E
   ```

   Note the use of backslashes in the source and destination directory paths.
3. Change the path for `FSMSEQS$` shared folder. If the product is installed in the local quarantine management mode, you can skip this step.

   To change the `FSMSEQS$` path, follow these steps:

   a. Open **Windows Control Panel** > **Administrative Tools** > **Computer Management**.
   b. Open **System Tools** > **Shared Folders** > **Shares** and find `FSMSEQS$` there.
   c. Right-click `FSMSEQS$` and select **Stop Sharing**. Confirm that you want to stop sharing `FSMSEQS$`.
   d. Right-click `FSMSEQS$` again and select **New Share**.
   e. Follow **Share a Folder Wizard** instructions to create `FSMSEQS$` shared folder.

      - Specify the new directory (in this example, `D:\Quarantine`) as the folder path, `FSMSEQS$` as the share name and F-Secure Quarantine Storage as the description.
      - On the **Permissions** page, select Administrators have full access; other users have read-only access. Note that the Quarantine storage has file/directory security permissions set only for the SYSTEM and Administrators group.

   f. Click **Finish**.
4. Change the location of the E-mail Quarantine storage from the F-Secure Policy Manager Console (`F-Secure Anti-Virus for Exchange/Settings/Quarantine/Quarantine Storage`) or the Web Console (**Anti-Virus for Microsoft Exchange** > **Quarantine** > **Options** > **Quarantine Storage**).
5. Make sure that the product has received new settings.
6. Restart F-Secure Quarantine Manager service. Run the following command from the command prompt: `net start "F-Secure Quarantine Manager"`

👉 **Note:** For more information about the xcopy command and options, refer to MS Windows Help and Support.

Updating Virus and Spam Definition Databases

Topics:

- *Overview*
- *Automatic Updates*
- *Configuring Automatic Updates*

7.1 Overview

It is of the utmost importance that virus definition databases are kept up-to-date. The product takes care of this task automatically.

Information about the latest virus database update can be found at: *http://www.f-secure.com/download-purchase/updates.shtml*

7.2 Automatic Updates

Using F-Secure Automatic Update Agent is the most convenient way to keep the databases updated. It connects to F-Secure Policy Manager Server or the F-Secure Update Server automatically. F-Secure Automatic Update Agent uses incremental technology and network traffic detection to make sure that it works without disturbing other Internet traffic even over a slow line.

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

7.3 Configuring Automatic Updates

F-Secure Automatic Update Agent user interface provides information about downloaded virus and spam definition updates. To access the F-Secure Automatic Update Agent user interface, open the Web Console, and go to the **Automatic Updates** page. For more information, see *Automatic Updates*.

In centrally managed installations, you can use the Web Console only for monitoring the F-Secure Automatic Update Agent settings. To change these settings, you need to use F-Secure Policy Manager Console. For more information, see *F-Secure Automatic Update Agent Settings*.

If necessary, reconfigure the firewall and other devices that may block the database downloads.

Note: In common deployment scenarios, make sure that the following ports are open:

- DNS (53, UDP and TCP)
- HTTP (80)
- Port used to connect to F-Secure Policy Manager Server

Variables in Warning Messages

The following table lists the variables that can be included in the warning and informational messages sent by the product if an infection is found or content is blocked.

If both stripping and scanning are allowed and the Agent found both types of disallowed content (infected and to be stripped) in an e-mail message, a warning message will be sent to the end-user instead of an informational one, if it is required.

These variables will be dynamically replaced by their actual names. If an actual name is not present, the corresponding variable will be replaced with [Unknown].

Variable	Description
`$ANTI-VIRUS-SERVER`	The DNS/WINS name or IP address of F-Secure E-mail and Server Security.
`$NAME-OF-SENDER`	The e-mail address where the original content comes from.
`$NAME-OF-RECIPIENT`	The e-mail addresses where the original content is sent.
`$SUBJECT`	The original e-mail message subject.
`$DIRECTION`	The direction of e-mail message (inbound, outbound or internal).
`$REPORT-BEGIN`	Marks the beginning of the scan report. This variable does not appear in the warning message.
`$REPORT-END`	Marks the end of the scan report. This variable does not appear in the warning message.

Note: `$REPORT-BEGIN`, `$REPORT-END`, `$DIRECTION` macros are not applicable in the replacement text used on real-time scanning in the Exchange storage.

The following table lists variables that can be included in the scan report, in other words the variables that can be used in the warning message between `$REPORT-BEGIN` and `$REPORT-END`.

Variable	Description
`$AFFECTED-FILENAME`	The name of the original file or attachment.
`$AFFECTED-FILESIZE`	The size of the original file or attachment.
`$THREAT`	The name of the threat that was found in the content. For example, it can contain the name of the found infection, etc.
`$TAKEN-ACTION`	The action that was taken to remove the threat. These include the following: dropped, disinfected, etc.
`$QUARANTINE-ID`	The identification number of the quarantined attachment or file.

Sending E-mail Alerts And Reports

Topics:

9.1 Overview

You can configure the product to send alerts to the administrator by e-mail. F-Secure Management Agent that handles the alerting uses a simple SMTP protocol (without authentication and encryption) to send alerts to the specified e-mail address.

In Microsoft Exchange Server 2007 and 2010, the message relaying is tightly restricted, even on servers that are not connected to the Internet. By default, only e-mail messages that come from authenticated or allowed sources can be relayed.

This means that the product cannot send SMTP alerts and reports unless some changes are done in the Microsoft Exchange Server 2007 and 2010 configurations. These changes can be done before or after the product has been deployed.

9.2 Solution

In order to make F-Secure alerts and reports relayed through Microsoft Exchange Server 2007 or 2010, you need to create a special receive connector configure it to allow anonymous, non-authenticated submissions. This connector has to be created on Exchange Edge and/or Hub server(s) that are specified as the SMTP server where the product sends alerts and reports to.

9.2.1 Creating a Scoped Receive Connector

The connector can be created from the Exchange management shell. Run the following command to create a scoped receive connector on the local server:

```
New-ReceiveConnector -Name
<connector_name> -Bindings <listen_ip_port> -RemoteIPRanges <accepted_hosts>
-AuthMechanism Tls -PermissionGroups "AnonymousUsers" -RequireEHLODomain $false
-RequireTLS $false
```

where:

- `<connector_name>` is the name for the connector,
- `<listen_ip_port>` is the IP address and port number (separated by a colon) that the receive connector listens for inbound messages, and
- `<accepted_hosts>` is the IP address or IP address range from which inbound connections are accepted.

  The IP address or IP address range can be entered in one of the following formats:

  - IP address: 192.168.1.1
  - IP address range: 192.168.1.10-192.168.1.20
  - IP address with subnet 192.168.1.0 (255.255.255.0)
  - IP address by using Classless Interdomain Routing (CIDR) notation: 192.168.1.0/24

For example, to create a new connector that listens on all configured local IP addresses and accepts connections from the local host only, run the following command in the Exchange management shell:

```
New-ReceiveConnector -Name "F-Secure alerts and reports" -Bindings
0.0.0.0:25 -RemoteIPRanges 127.0.0.1 -AuthMechanism Tls -PermissionGroups
"AnonymousUsers" -RequireEHLODomain $false -RequireTLS $false
```

To create a new connector that is bound to a single IP addresses and accepts connections from the specified remote servers, run the following command:

```
New-ReceiveConnector -Name "F-Secure
alerts and reports" -Bindings 192.168.58.128:25 -RemoteIPRanges 192.168.58.129,
192.168.58.131 -AuthMechanism Tls -PermissionGroups "AnonymousUsers"
-RequireEHLODomain $false -RequireTLS $false
```

9.2.2 Grant the Relay Permission on the New Scoped Connector

The receive connector accepts anonymous SMTP submissions but messages are not relayed. To relay messages, grant ms-Exch-SMTP-Accept-Any-Recipient the permission to the anonymous account. To do this, run the following command:

```
Get-ReceiveConnector <connector_name> |
Add-ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights
"ms-Exch-SMTP-Accept-Any-Recipient"
```

where:

- `<connector_name>` is the name of the connector you created.

For example:`Get-ReceiveConnector "F-Secure alerts and reports" | Add-ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "ms-Exch-SMTP-Accept-Any-Recipient"`

9.2.3 Specify SMTP Server for Alerts and Reports

Check that the product is properly configured and the address and port of the SMTP server corresponds to the address and port on which the receive connector listens for inbound messages. Remember to specify the return address for e-mail alerts.

Troubleshooting

Topics:

- *Overview*
- *Viewing the Log File*
- *Common Problems and Solutions*
- *Frequently Asked Questions*

10.1 Overview

If you have a problem that is not covered in here, see *Technical Support*.

10.2 Viewing the Log File

The product uses the log file `Logfile.log` that is maintained by F-Secure Management Agent service and contains all alerts generated by F-Secure components installed on the host. `Logfile.log` can be found on all hosts running F-Secure Management Agent. You can view the `Logfile.log` with any text editor, for example Windows Notepad. Open the `Logfile.log` from the `common` directory under the product installation directory or from the `Summary` page of the Web Console by clicking **View F-Secure Log**.

`Logfile.log` contains all the alerts generated by the host, regardless of the severity. To configure the Logfile.log file size in F-Secure Policy Manager, go to `F-Secure Management Agent / Settings / Alerting / Alert Agents / Logfile / Maximum File Size`.

E-mail Quarantine Logs

E-mail Quarantine logs are not stored in `Logfile.log`. By default, they are stored in the quarantine log directory. You can view E-mail Quarantine logs with any text editor.

To specify the path to the directory where E-mail Quarantine logfiles are placed, change the **Quarantine > Quarantine Log Directory** setting in F-Secure Policy Manager or **Quarantine > Options > Logging > Quarantine log directory** setting in the Web Console. For more information, see *Quarantine Logging*.

10.3 Common Problems and Solutions

If you think that you have an issue that is not listed here, check that both the product and its components are up and running.

10.3.1 Registering F-Secure Transport Agent

F-Secure Transport Agent should be registered in the Microsoft Exchange Transport Service automatically during the installation. If Web Console notifies that it is not, follow these instructions:

1. Open Exchange Management Shell.
2. Call the `Get-TransportAgent` command from the command line in Shell.
3. If **F-Secure Transport Agent** is not listed as a transport agent, you need to install it manually:
   a. Enter `cmd` in the **Start menu > Run** to open the command prompt.
   b. Type `cd “C:\Program Files (x86)\F-Secure\Anti-Virus for Microsoft Exchange”` to go to the product installation directory.
4. Type `PowerShell.exe -command ".\fstragnt.ps1 install"` to install F-Secure Transport Agent.

10.3.2 Checking the Web Console

Problem:

I cannot open or access the Web Console.

Solution:

1. Make sure that F-Secure WebUI Daemon has started and is running. Check the Services in Windows Control Panel. The following service should be started:
   - F-Secure WebUI Daemon

   Check the Task Manager. The following process should be running:
   - fswebuid.exe

2. If you try to connect to the product Web Console from a remote host, make sure that the connection is not blocked by a firewall or proxy server.

10.3.3 Checking F-Secure Content Scanner Server

Problem:

When the F-Secure E-mail and Server Security tries to send an attachment to F-Secure Content Scanner Server, the attachment is not scanned and the e-mail does not reach the recipient.

Solution:

F-Secure E-mail and Server Security cannot contact F-Secure Content Scanner Server.

A service or process may not be running on F-Secure Content Scanner Server. Make sure that all processes and services of F-Secure Content Scanner Server have started. Check the Services in Windows Control Panel. The following services should be started:

- F-Secure Content Scanner Server
- F-Secure Management Agent
- F-Secure Network Request Broker

To make sure that F-Secure Content Scanner Server accepts connections, run the following command from the command line on the Microsoft Exchange Server: telnet 127.0.0.1 18971

If you get the cursor blinking in the upper left corner, it means that the connection has been established and F-Secure Content Scanner Server can accept incoming connections.

If you get "Connection to the host lost" or other error message or if the cursor does not go to the upper left corner, it means that the connection attempt was unsuccessful. If the telnet connection attempt was unsuccessful, make sure that F-Secure Content Scanner Server is up and running and that there is no local firewall on the server blocking the access.

10.3.4 Securing the E-mail Quarantine

Problem:

I have installed the product and I'm worried about security of the local E-mail Quarantine storage where stripped attachments are quarantined. What do you recommend me?

Solution:

The product creates and adjusts access rights to the local E-mail Quarantine storage during the installation. Keep in mind the following when setting up the local E-mail Quarantine storage:

- Do not place the E-mail Quarantine storage on a FAT drive. FAT file system does not support access rights on directories and files for different users. If you place the Quarantine storage on a FAT drive everyone who has access to that drive will be able to get access to the quarantined content.
- Create and adjust access rights to the E-mail Quarantine storage manually if you use one on a network drive.
- Create and adjust access rights to the E-mail Quarantine storage manually when you change its path from F-Secure Policy Manager Console or the Web Console.

10.3.5 Administration Issues

Some settings are initially configured during the product installation. They can be viewed on the Status tab of F-Secure Policy Manager Console.

When changing such settings in F-Secure Policy Manager Console for the first time, you must enforce the change by selecting the **Final** check box.

10.3.6 Turning on EMC CAVA support

If you install the product with EMC CAVA support, it should be on after the installation is complete.

If Web Console notifies that EMC CAVA support has improper policies, follow these instructions:

1. Open F-Secure Policy Manager.

2. Go to the **F-Secure Anti-Virus** > **Settings** > **Settings for Real-Time Protection** > **Scanning options** > **File Scanning** branch.
3. Set **Scan Network Drives** to **Enabled**.
4. Go to the **F-Secure Anti-Virus** > **Settings** > **Security Levels** > **Server** > **Settings for Real-Time Protection** > **Scanning options** > **File Scanning** branch.
5. Set **Decide action automatically** to **Enabled**.
6. Distribute the policy.

10.4 Frequently Asked Questions

All support issues, frequently asked questions and hotfixes can be found under the support pages at *http://support.f-secure.com/*.

For more information, see *Technical Support*.

Technical Support

Topics:

- *F-Secure Online Support Resources*
- *Software Downloads*
- *Virus Descriptions on the Web*

11.1 F-Secure Online Support Resources

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 support web pages for any F-Secure product can be accessed at *http://support.f-secure.com/*. All support issues, frequently asked questions and hotfixes can be found under the support pages.

If you have questions about the product 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, please contact your local F-Secure Business Partner. Send your e-mail to:

Anti-Virus-<country>@f-secure.com

Example: 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 "Request Support form" accessible through F-Secure support web pages under the "Contact Support" page. Fill in all the fields and describe the problem as accurately as possible. Please include the FSDiag report taken from the problematic server with the support request.

F-Secure Support Tool

Before contacting support, please run the F-Secure Support Tool `FSDiag.exe` on each of the hosts running the product. This utility gathers basic information about hardware, operating system, network configuration and installed F-Secure and third-party software. You can run the F-Secure Support Tool from the Web Console as follows:

1. Log in to the Web Console.
2. Type *https://127.0.0.1:25023/fsdiag/* in the browser’s address field or or click **F-Secure support tool** on **General Server Properties** page.
3. The F-Secure Support Tool starts and the dialog window displays the progress of the data collection.

   Note: Note that in some web browsers, the window may appear behind the main browser window.

4. When the tool has finished collecting the data, click **Report** to download and save the collected data.

You can also find and run the FSDiag.exe utility in the `Common` directory under the product installation directory, or run **F-Secure E-mail and Server Security > Support Tool** in the Windows Start menu. The tool generates a file called `FSDiag.tar.gz`.

Please include the following information with your support request:

- Product and component version numbers. Include the build number if available.
- 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. For Windows, include the build number and Service Pack number.
- The version number and the configuration of your Microsoft Exchange Server, if you use F-Secure Anti-Virus for Microsoft Exchange component. 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.
- If the whole product or a component crashed, include the `drwtsn32.log` file from the Windows NT directory and the latest records from the Windows Application Log.

11.2 Software Downloads

The F-Secure web site provides assistance and updated versions of the F-Secure products.

In order to maximize your security level we strongly encourage you to always use the latest versions of our products. You can find the latest product version, hotfixes and all related downloadable materials in: *http://www.f-secure.com/en_EMEA/downloads/product-updates/*.

11.3 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/security_center/*.

About F-Secure Corporation

F-Secure Corporation protects consumers and businesses against computer viruses and other online threats from the Internet and mobile networks. We want to be the most reliable provider of internet security services in the market. One way to demonstrate this is the speed of our response.

F-Secure's award-winning solutions for real-time virus protection are available as a service subscription through more than 170 Internet service providers and mobile operator partners around the world, making F-Secure the global leader in the market of internet and computer security. The solutions are also available as licensed products through thousands of resellers globally.

F-Secure aspires to be the most reliable mobile and computer security provider, helping make computer and smartphone users' networked lives safe and easy. This is substantiated by the company's independently proven ability to respond faster to new threats than its main competitors. Founded in 1988 and headquartered in Finland, F-Secure has been listed on the OMX Nordic Exchange Helsinki since 1999. The company has consistently been one of the fastest growing publicly listed companies in the industry.

The latest news on real-time virus threat scenarios is available at the http://www.f-secure.com/weblog/