# F-Secure Email and Server Security
# Administrator's Guide

# Contents

Chapter

1

# Introduction

**Topics:**



This guide describes how to use and manage F-Secure Email and Server Security. The solution can be licensed and deployed as standard or premium version.

Depending on the selected license and installed components, some product features may not be available. See the release notes for additional information about using this product.

**Note:** For more information on the licensing and the product deployment, see the F-Secure Email and Server Security Deployment Guide.

## 1.1 Product contents

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

The features that included with different product licenses:

| Feature | F-Secure Email and Server Security | F-Secure Email and Server Security Premium |
|---|---|---|
| Malware protection | X | X |
| DeepGuard | X | X |
| DataGuard | | X |
| Application control | | X |
| Firewall | X | X |
| Web traffic scanning | X | X |
| Browsing protection | X | X |
| Software Updater | | X |
| Offload Scanning Agent | X | X |
| Microsoft Exchange protection | X | X |
| Spam Control | X | X |
| Email Quarantine Manager | X | X |
| Microsoft SharePoint protection | X | X |

## 1.2 Administering the product

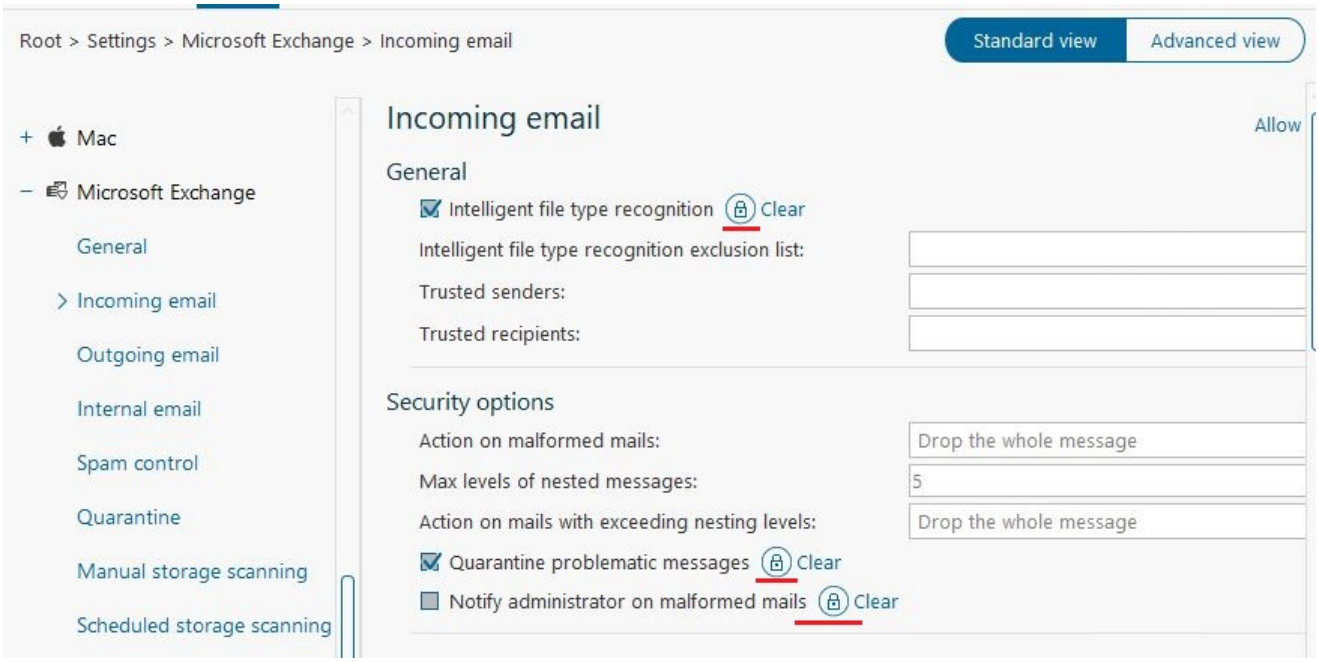
The product can be used either in the stand-alone mode or in the centrally managed administration mode, based on your selections during the installation and the initial setup.

### 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).

Here's an example of how the Final flag looks like in F-Secure Policy Manager:




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

#### 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.

## 1.3 Using Web Console

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

- Go to **Windows Start menu** > **Programs** > **F-Secure Email and Server Security** > **F-Secure Email 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.

### 1.3.1 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:** We recommend that you use your company's own security certificate for the Web Console.

**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.

### 1.3.2 Modifying settings and viewing statistics with Web Console

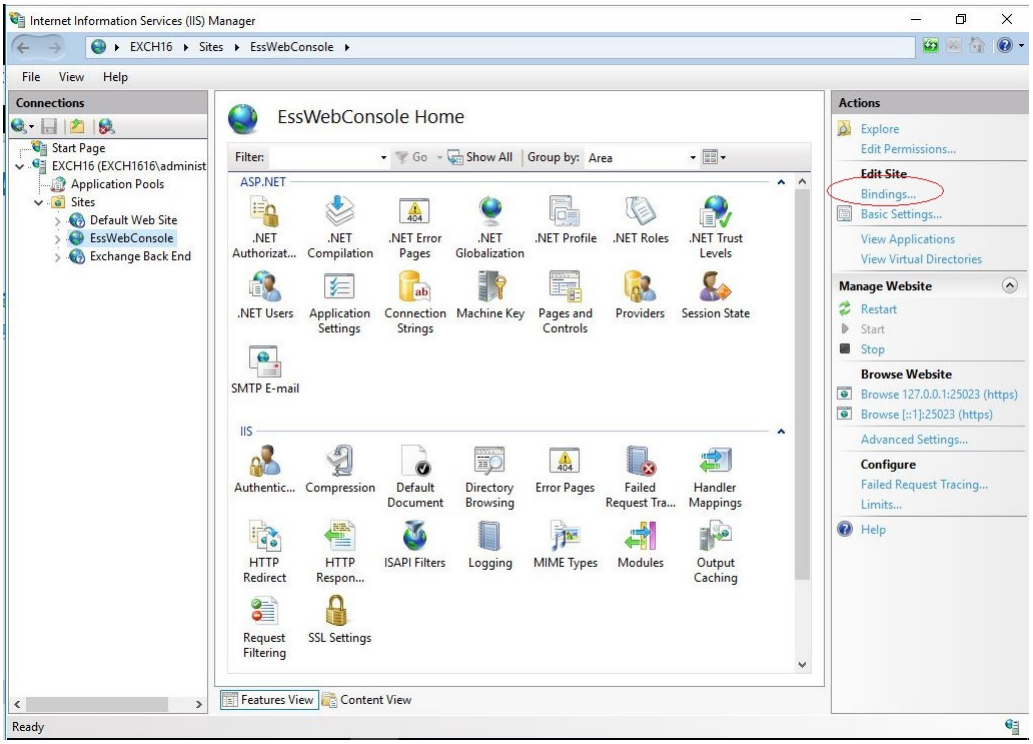
To change the product settings, open the Web Console and use the left pane to navigate the settings you want to change or statistics you want to view. For detailed explanations of all product settings, see Administration with Web Console on page 75.

## 1.3.3 Allowing hosts to access the web console

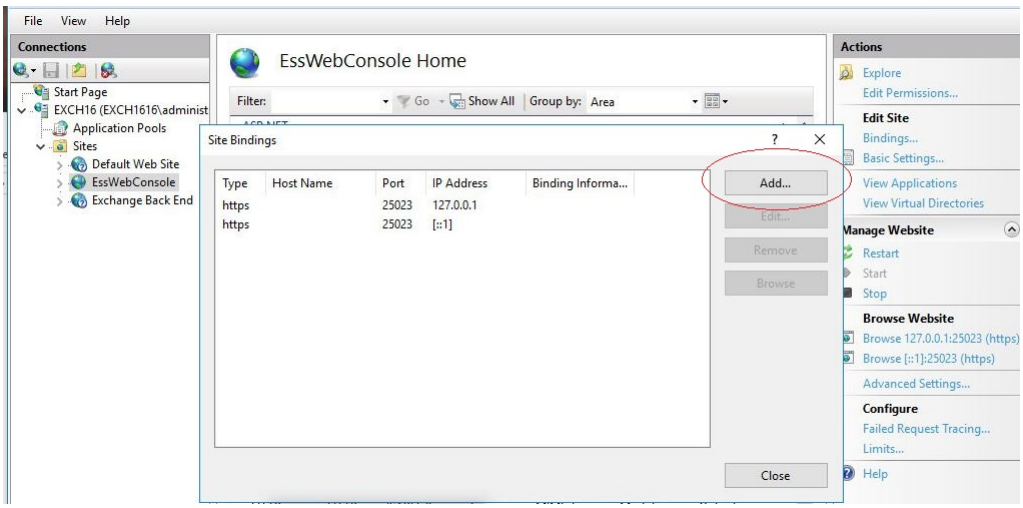
To access the web console from other hosts in the network, you need to allow them via Internet Information Services (IIS).

To allow access to the web console for all hosts:

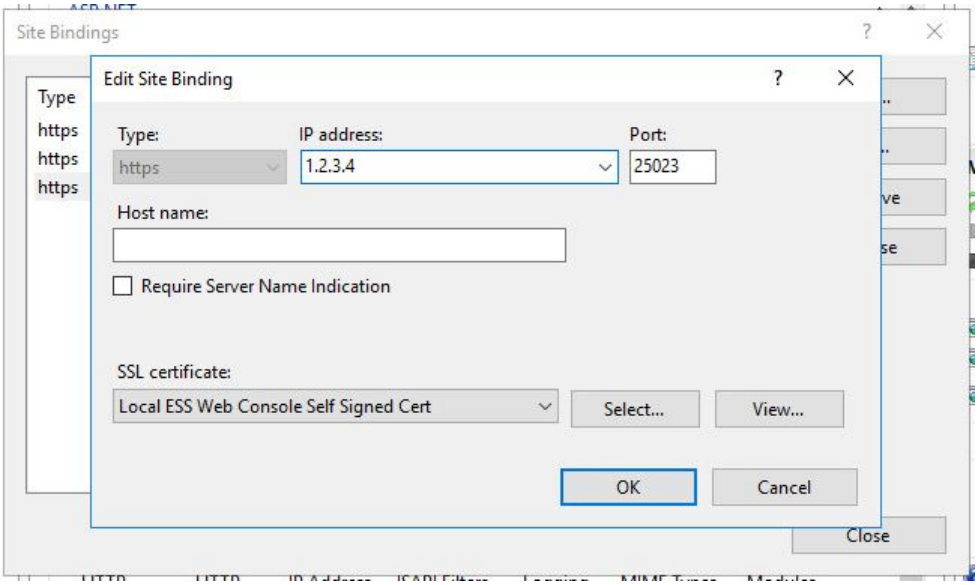
1. In **Administrative Tools**, start **Internet Information Services (IIS) Manager**.
2. Go to **Sites** > **EssWebConsole**.
3. Select **Bindings**.




4. Click **Add**.



5. Select **https** as the **Type**, enter the **IP address** for the server, and set the **Port** to 25023.




6. Select the **SSL certificate**, then click **OK**.

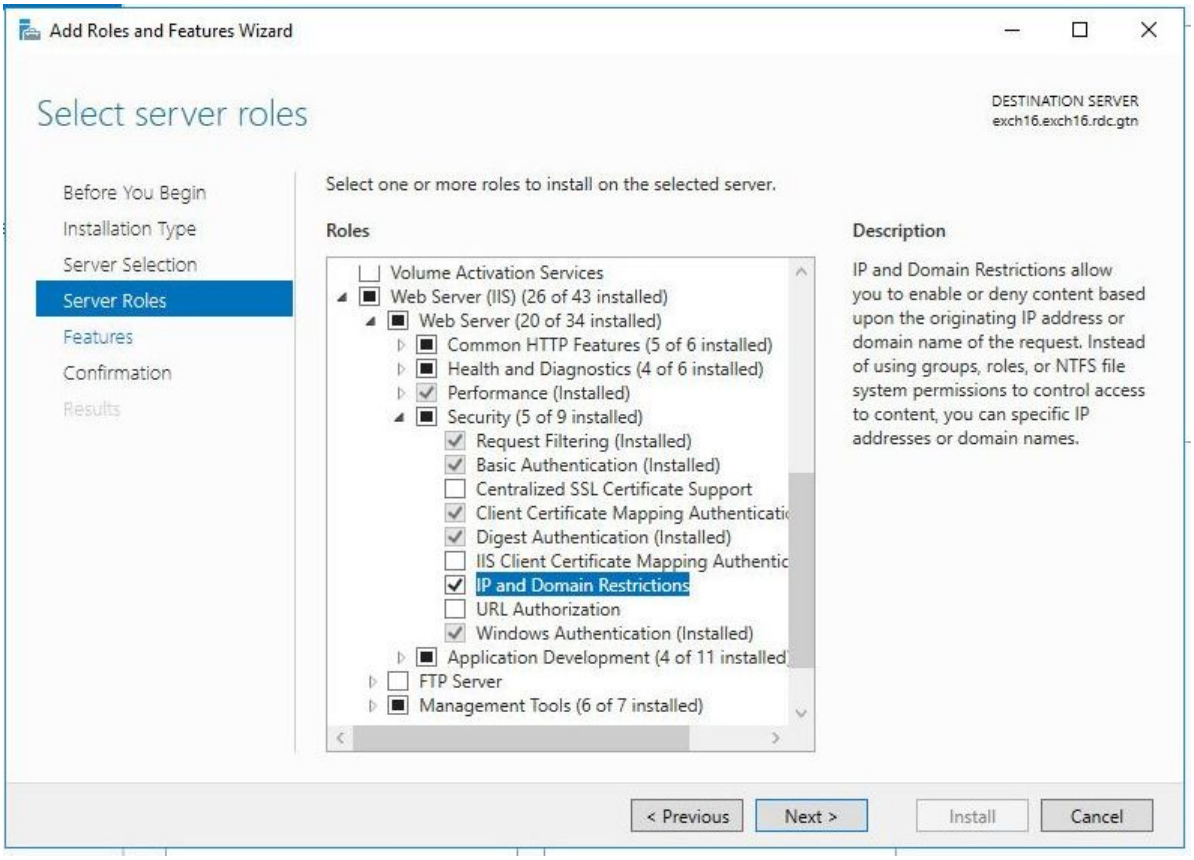
   **Note:** SSL 2.0 certificates are not supported due to vulnerabilities.

## 1.3.4 Restricting website access to specific IP addresses

After allowing access to the web console from other hosts in your network, you may want to restrict the access to a specific IP address or IP range.

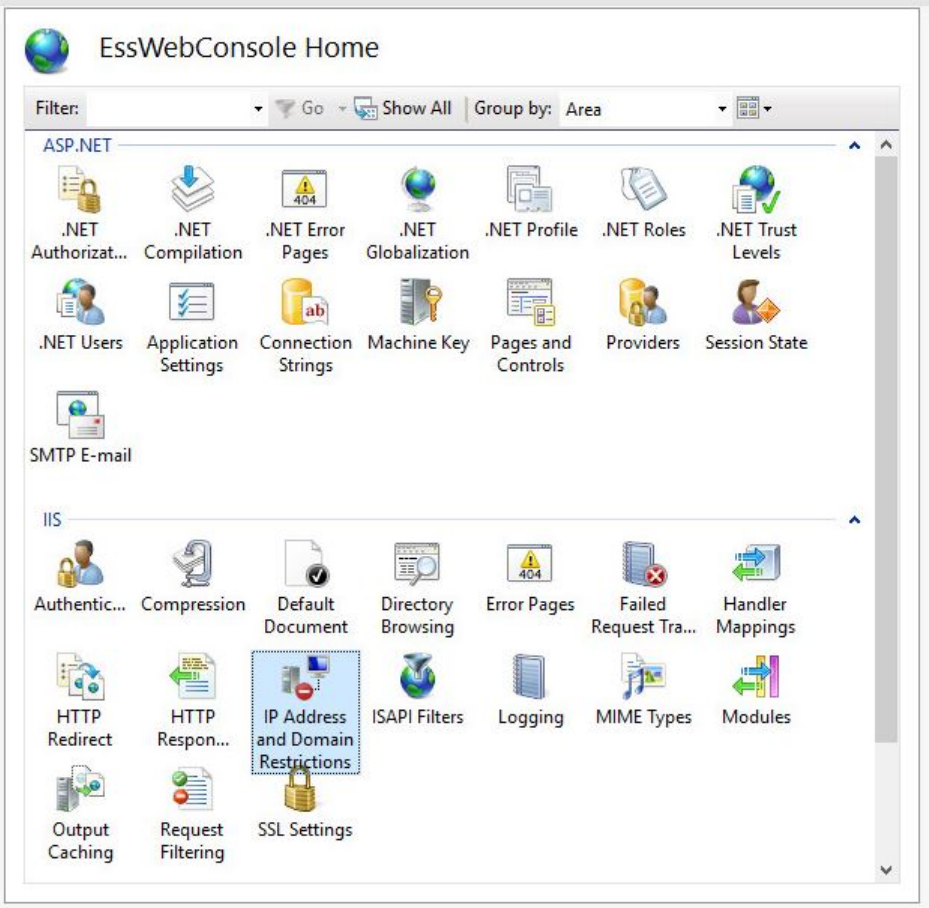
To allow only specific hosts to access the web console:

1. Make sure that the **IP and Domain Restrictions** feature is installed for Internet Information Services (IIS).



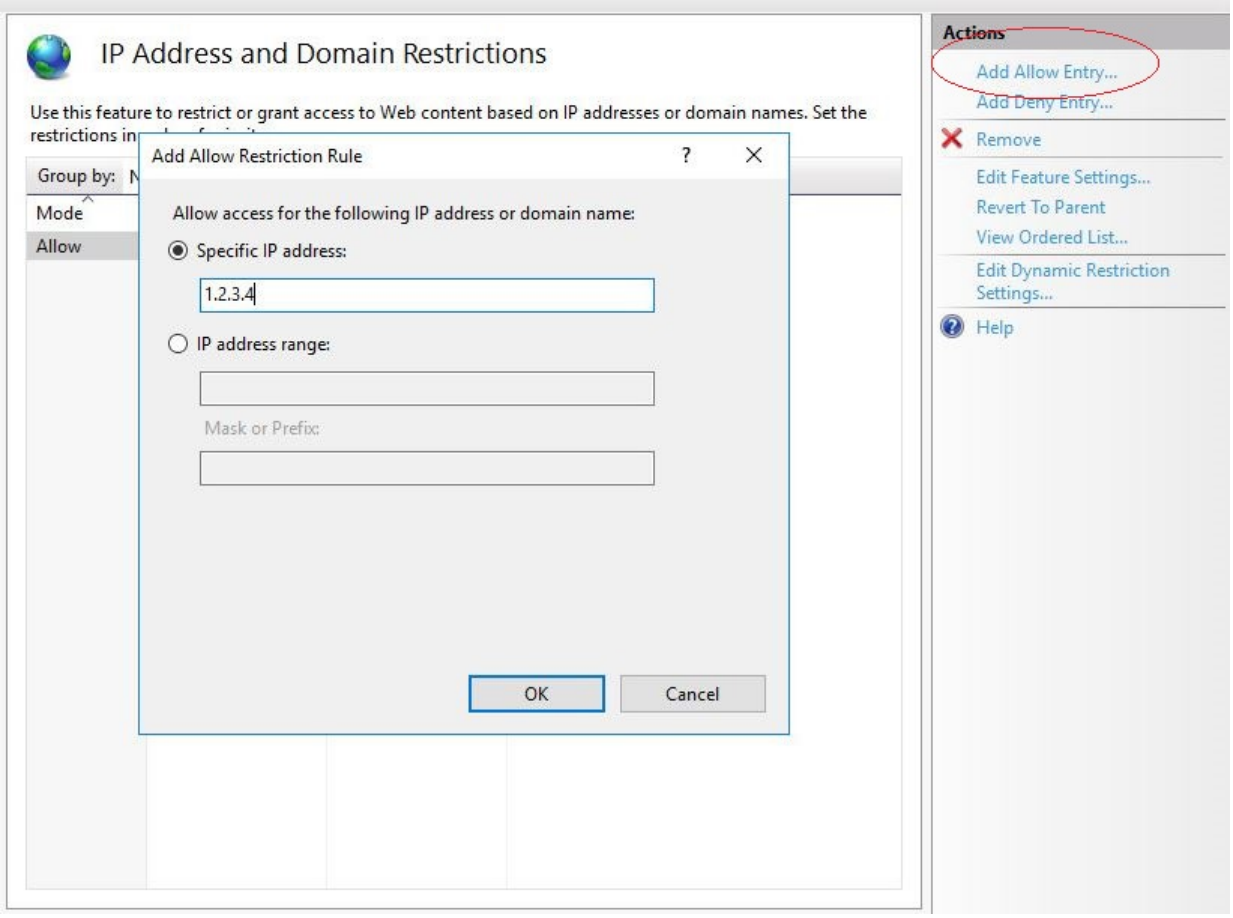

2. Go to **Sites** > **EssWebConsole**.

3. Open **IP and Domain Restrictions**.




4. Select **Add Allow Entry**.

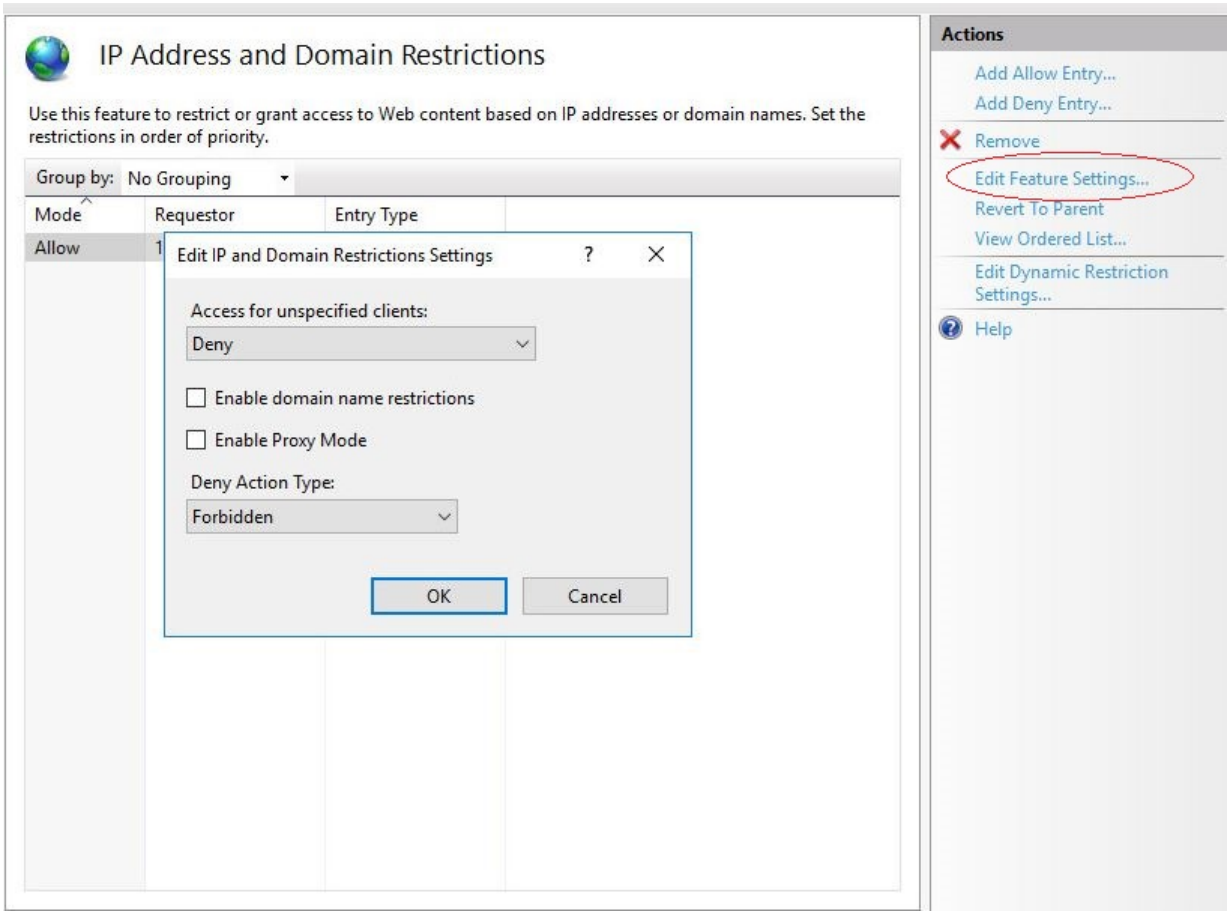
5. Enter the IP address or IP range.




**Note:** Make sure that you add the local IP address if you need to open the web console locally.

6. Click **OK**.
7. Select **Edit feature settings**.

8. Set **Access for unspecified clients** to **Deny**.




9. Click **OK**.
10. Restart the **EssWebConsole** site.

Chapter

2

# Protecting the computer against harmful content

**Topics:**



The product protects the computer from programs that may steal personal information, damage the computer, or use it for illegal purposes.

By default, the malware protection handles all harmful files as soon as it finds them so that they can cause no harm.

The product automatically scans your local hard drives, any removable media (such as portable drives or DVDs), and any content that you download.

The product also watches your computer for any changes that may suggest that you have harmful files on your computer. When the product detects any dangerous system changes, for example changes in system settings or attempts to change important system processes, its DeepGuard component stops the application from running as it can be harmful.

**Note:** Your administrator may enforce some security settings, which means that you may not be able to locally change some features.

## 2.1 What harmful content does

Harmful applications and files can try to damage your data or gain unauthorized access to your computer system to steal your private information.

### 2.1.1 Potentially unwanted applications (PUA) and unwanted applications (UA)

'Potentially unwanted applications' have behaviors or traits that you may consider undesirable or unwanted. 'Unwanted applications' can affect your device or data more severely.

An application may be identified as 'potentially unwanted' (PUA) if it can:

- **Affect your privacy or productivity** - for example, exposes personal information or performs unauthorized actions
- **Put undue stress on your device's resources** - for example, uses too much storage or memory
- **Compromise the security of your device or the information stored on it** - for example, exposes you to unexpected content or applications

These behaviors and traits can affect your device or data to a varying degree. They are not however harmful enough to warrant classifying the application as malware.

An application that shows more severe behaviors or traits is considered an 'unwanted application' (UA). The product will treat such applications with more caution.

The product will handle an application differently depending on whether it is a PUA or UA:

- **A potentially unwanted application** - The product will automatically block the application from running. If you are certain that you trust the application, you may instruct the F-Secure product to exclude it from scanning. You must have administrative rights to exclude a blocked file from scanning.
- **An unwanted application** - The product will automatically block the application from running.

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21
You can view and manage the applications and files that the product blocks in the **App and file control** view.

### 2.1.2 Worms

Worms are programs that send copies of themselves from one device to another over a network. Some worms also perform harmful actions on an affected device.

Many worms are designed to appear attractive to a user. They may look like images, videos, applications or any other kind of useful program or file. The aim of the deception is to lure the user into installing the worm. Other worms are designed to be completely stealthy, as they exploit flaws in the device (or in programs installed on it) to install themselves without ever being noticed by the user.

Once installed, the worm uses the device's physical resources to create copies of itself, and then send those copies to any other devices it can reach over a network. If a large quantity of worm copies is being sent out, the device's performance may suffer. If many devices on a network are affected and sending out worm copies, the network itself may be disrupted. Some worms can also do more direct damage to an affected device, such as modifying files stored on it, installing other harmful applications or stealing data.

Most worms only spread over one particular type of network. Some worms can spread over two or more types, though they are relatively rare. Usually, worms will try and spread over one of the following networks (though there are those that target less popular channels):

- Local networks
- Email networks
- Social media sites
- Peer-to-peer (P2P) connections
- SMS or MMS messages

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21
You can view and manage the applications and files that the product blocks in the **App and file control** view.

## 2.1.3 Trojans

Trojans are programs that offer, or appears to offer, an attractive function or feature, but then quietly perform harmful actions in the background.

Named after the Trojan Horse of Greek legend, trojans are designed to appear attractive to a user. They may look like games, screensavers, application updates or any other useful program or file. Some trojans will mimic or even copy popular or well-known programs to appear more trustworthy. The aim of the deception is to lure the user into installing the trojan.

Once installed, trojans can also use 'decoys' to maintain the illusion that they are legitimate. For example, a trojan disguised as a screensaver application or a document file will display an image or a document. While the user is distracted by these decoys, the trojan can quietly perform other actions in the background.

Trojans will usually either make harmful changes to the device (such as deleting or encrypting files, or changing program settings) or steal confidential data stored on it. Trojans can be grouped by the actions they perform:

- **Trojan-downloader**: connects to a remote site to download and install other programs
- **Trojan-dropper**: contains one or more extra programs, which it installs
- **Trojan-pws**: Steals passwords stored on the device or entered into a web browser
    - **Banking-trojan**: A specialized trojan-pws that specifically looks for usernames and passwords for online banking portals
- **Trojan-spy**: Monitors activity on the device and forwards the details to a remote site

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21
You can view and manage the applications and files that the product blocks in the **App and file control** view.

## 2.1.4 Backdoors

Backdoors are features or programs that can be used to evade the security features of a program, device, portal, or service.

A feature in a program, device, portal or service can be a backdoor if its design or implementation introduces a security risk. For example, hardcoded administrator access to an online portal can be used as a backdoor.

Backdoors usually take advantage of flaws in the code of a program, device, portal, or service. The flaws may be bugs, vulnerabilities or undocumented features.

Attackers use backdoors to gain unauthorized access or to perform harmful actions that allow them to evade security features such as access restrictions, authentication or encryption.

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21

You can view and manage the applications and files that the product blocks in the **App and file control** view.

## 2.1.5 Exploits

Exploits are objects or methods that take advantage of a flaw in a program to make it behave unexpectedly. Doing so creates conditions that an attacker can use to perform other harmful actions.

An exploit can be either an object or a method. For example, a specially crafted program, a piece of code or a string of characters are all objects; a specific sequence of commands is a method.

An exploit is used to take advantage of a flaw or loophole (also known as a vulnerability) in a program. Because every program is different, each exploit has to be carefully tailored to that specific program.

There are several ways for an attacker to deliver an exploit so that it can affect a computer or device:

- **Embedding it in a hacked or specially crafted program** - when you install and launch the program, the exploit is launched
- **Embedding it in a document attached to an email** - when you open the attachment, the exploit is launched
- **Hosting it on a hacked or harmful website** - when you visit the site, the exploit is launched

Launching the exploit causes the program to behave unexpectedly, such as forcing it to crash, or tampering with the system's storage or memory. This can create conditions that allow an attacker to perform other harmful actions, such as stealing data or gaining access to restricted sections of the operating system.

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21
You can view and manage the applications and files that the product blocks in the **App and file control** view.

## 2.1.6 Exploit kits

Exploit kits are toolkits used by attackers to manage exploits and deliver harmful programs to a vulnerable computer or device.

An exploit kit contains an inventory of exploits, each of which can take advantage of a flaw (vulnerability) in a program, computer or device. The kit itself is usually hosted on a harmful or a hacked site, so that any computer or device that visits the site is exposed to its effects.

When a new computer or device connects to the booby-trapped site, the exploit kit probes it for any flaws that can be affected by an exploit in the kit's inventory. If one is found, the kit launches the exploit to take advantage of that vulnerability.

After the computer or device is compromised, the exploit kit can deliver a payload to it. This is usually another harmful program that is installed and launched on the computer or device, which in turn performs other unauthorized actions.

Exploit kits are designed to be modular and easy to use, so that their controllers can simply add or remove exploits and payloads to the toolkit.

**Related Tasks**

Turning on real-time scanning on page 17
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 18
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using App and file control on page 21

You can view and manage the applications and files that the product blocks in the **App and file control** view.

## 2.2 How to scan my computer

When Malware protection is turned on, it scans your computer for harmful files automatically.

We recommend that you keep Malware protection turned on all the time. You can also scan files manually and set up scheduled scans if you want to make sure that there are no harmful files on your computer or to scan files that you have excluded from the real-time scan. Set up a scheduled scan if you want to scan your computer regularly every day or week.

### 2.2.1 How real-time scanning works

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

When your computer tries to access a file, Real-time scanning scans the file for malware before it allows your computer to access the file.

If Real-time scanning finds any harmful content, it puts the file to quarantine before it can cause any harm.

#### 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 depend on, for example, the contents, location and type of the file.

Files on removable drives such as CDs, DVDs, and portable USB drives take a longer time to scan.

**Note:** Compressed files, such as .zip files, are not scanned by real-time scanning.

Real-time scanning may slow down your computer if:

- you have a computer that does not meet the system requirements, or
- you access a lot of files at the same time. For example, when you open a directory that contains many files that need to be scanned.

#### Turning on real-time scanning

Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

To make sure that real-time scanning is on:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select  .
3. Select **Malware Protection** > **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.
4. Turn on **Real-time Scanning**.

### 2.2.2 Scan files manually

You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

The full computer scan scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete. You can also scan only the parts of your system where harmful applications are commonly found to remove unwanted applications and harmful items on your computer more efficiently.

### Scanning files and folders

If you are suspicious of a certain files on your computer, you can scan only those files or folders. These scans will finish a lot quicker than a scan of your whole computer. For example, when you connect an external hard drive or USB flash drive to your computer, you can scan it to make sure that they do not contain any harmful files.

## Running a malware scan

You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

To scan your computer, follow these instructions:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. If you want to optimize how the manual scanning scans your computer, on the main page, select and then select **Scanning settings**.
   a) Select **Scan only file types that commonly contain harmful code (faster)** if you do not want to scan all files.
   The files with the following extensions are examples of file types that are scanned when you select this option: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.
   b) Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Scanning inside compressed files makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.
3. On the main page, select .
4. Select either **Malware scan** or **Full computer scan**.
   - **Malware scan** starts by scanning the active memory of the computer and then locations where malware is commonly found, including the document folders. It can find and remove unwanted applications and harmful items on the computer in a shorter time.
   - **Full computer scan** scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete.

   The virus scan starts.
5. If the virus scan finds any harmful items, it shows you the list of harmful items that it detected.
6. Click the detected item to choose how you want to handle the harmful content.

| Option | Description |
|---|---|
| **Clean up** | Clean the files automatically. Files that cannot be cleaned are quarantined. |
| **Quarantine** | Store the files in a safe place where they cannot spread or harm your computer. |
| **Delete** | Permanently remove the files from your computer. |
| **Skip** | Do nothing for now and leave the files on your computer. |
| **Exclude** | Allow the application to run and exclude it from future scans. |

**Note:** Some options are not available for all harmful item types.

7. Select **Handle all** to start the cleaning process.
8. The malware scan shows the final results and the number of harmful items that were cleaned.

**Note:** The malware scan may require that you restart your computer to complete the cleaning process. If the cleaning requires a computer restart, select **Restart** to finish cleaning harmful items and restart your computer.

You can see the final results of the latest virus scan by selecting **Open last scanning report**.

### Scan in Windows Explorer

You can scan disks, folders, and files for harmful files and unwanted applications in Windows Explorer.

If you are suspicious of certain files on your computer, you can scan only those files or folders. These scans will finish a lot quicker than a scan of your whole computer. For example, when you connect an external hard drive or USB flash drive to your computer, you can scan it to make sure that they do not contain any harmful files.

To scan a disk, folder, or file:

1. Right-click the disk, folder, or file you want to scan.
2. From the right-click menu, select **Malware scan**.
   The virus scan starts and scans the disk, folder, or file that you selected.

The virus scan guides you through the cleaning stages if it finds harmful files or unwanted applications during the scan.

## 2.2.3 Scheduling scans

Set your computer to scan and remove malware and other harmful applications automatically when you do not use it, or set the scan to run periodically to make sure that your computer is clean.

To schedule a scan:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select  .
3. Select **Scanning settings**.
4. Turn on **Scheduled scanning**.
5. In **Perform scan**, select how often you want to scan your computer automatically.

| Option | Description |
|---|---|
| **Daily** | Scan your computer every day. |
| **Every week** | Scan your computer on selected days of the week. Select the weekday from the list. |
| **Every four weeks** | Scan your computer on a selected weekday at four-week intervals. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday. |

6. In **Start time**, select when the scheduled scan starts.
7. Select **Run scanning on low priority** to make the scheduled scan interfere less with other activities on the computer. Running the scan on low priority takes longer to complete.
8. Select **Scan only file types that commonly contain harmful code (faster)** if you do not want to scan all files.

   The files with the following extensions are examples of file types that are scanned when you select this option: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.
9. Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Scanning inside compressed files makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.

**Note:** Scheduled scans are canceled when the presentation mode is on. When you turn the presentation mode off, they run according to the schedule again.

## 2.3 What is DeepGuard

DeepGuard monitors applications to detect potentially harmful changes to the system.

DeepGuard makes sure that you use only safe applications. The safety of an application is verified from the trusted cloud service. If the safety of an application cannot be verified, DeepGuard starts to monitor the application behavior.

**Tip:** If you want F-Secure to add your application to the allowed applications list, submit your application for analysis here. Once we have analyzed the program, we will notify you of the analysis results if you have provided us with your contact details.

DeepGuard blocks new and undiscovered Trojans, worms, exploits, and other harmful applications that try to make changes to your computer, and prevents suspicious applications from accessing the internet.

Potentially harmful system changes that DeepGuard detects 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.

To make sure that DeepGuard is active:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select .
3. Select **Malware Protection** > **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.

4. Select **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.

5. Turn on **DeepGuard**.

When DeepGuard is on, it automatically blocks applications that try to make potentially harmful changes to the system.

**Related Tasks**

Security Data

## 2.3.1 Using DataGuard

DataGuard monitors a set of folders for potentially harmful changes made by ransomware or other, similar harmful software.

Ransomware is harmful software that encrypts important files on your computer, preventing you from accessing them. Criminals demand a ransom to restore your files, but there are no guarantees you would ever get your personal data back even if you choose to pay.

DataGuard only allows safe applications to access the protected folders. The product notifies you if any unsafe application tries to access a protected folder. If you know and trust the application, you can allow it to access the folder. DataGuard also lets DeepGuard use its list of protected folders for an additional layer of protection.

You can choose which folders require an additional layer of protection against destructive software, such as ransomware.

**Note:** You must turn on DeepGuard to use DataGuard. DataGuard is available only in the Premium version.

To manage your protected folders:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select .
3. Select **Malware Protection** > **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.

4. Turn on **DataGuard**.
5. Select **View protected folders**.
6. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
7. Add or remove folders as needed.

   To add a new protected folder:

   a) Click **Add new**.
   b) Select the folder that you want to protect.

c) Click **Select folder**.

To remove a folder:

a) Select the folder on the list.

b) Click **Remove**.

**Tip:** Click **Restore defaults** if you want to undo any changes that you have made to the list of protected folders since installing the product.

**Related Tasks**

Adding and removing protected folders on page 23

You can choose which folders require an additional layer of protection against destructive software, such as ransomware.

## 2.4 Using App and file control

You can view and manage the applications and files that the product blocks in the **App and file control** view.

To access the **App and file control** view:

1. Open the product from the Windows **Start** menu.
2. Select **Viruses and Threats**.
3. Select **App and file control**.

The **App and file control** view opens, including four separate tabs:

| | |
|---|---|
| **Quarantined** | Quarantine is a safe repository for files that may be harmful. The product can place both harmful items and potentially unwanted applications in quarantine to make them harmless. You can restore applications or files from the quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in the quarantine removes it permanently from your computer. |
| **Blocked** | This tab shows you the applications that DeepGuard has blocked. DeepGuard blocks the applications that it monitors when they behave suspiciously or try to connect to the internet. |
| **Excluded** | This tab shows you the applications, files, and folders that are excluded from scanning. DeepGuard does not block any excluded applications from running, and the product does not scan any excluded locations for harmful items. You can exclude both folders and individual files. |
| **Protected** | This tab shows you the folders that are protected against destructive software, such as ransomware. The product blocks any unsafe applications from making changes to the files stored in these folders.<br>**Note:** This tab is available only in the Premium version. |

### 2.4.1 View quarantined items

You can view more information on items placed in quarantine.

Quarantine is a safe repository for files that may be harmful. The product can place both harmful items and potentially unwanted applications in quarantine to make them harmless. You can restore applications or files from quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in quarantine removes it permanently from your computer.

To view information on items placed in quarantine:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Quarantined** tab.
   This list shows you the name, date of detection, and infection type for each quarantined item.

5. Double-click a quarantined item to see more information.
   For single items, this shows you the original location of the quarantined item.

## 2.4.2 Restore quarantined items

You can restore the quarantined items that you need.

You can restore applications or files from quarantine if you need them. Do not restore any items from quarantine unless you are sure that items pose no threat. Restored items move back to the original location on your computer.

To restore quarantined items:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Quarantined** tab.
5. Select the quarantined item that you want to restore.
6. Click **Allow**.
7. Click **Yes** to confirm that you want to restore the quarantined item.

The selected item is automatically restored to its original location. Depending on the type of infection, the item may be excluded from future scans.

**Note:** To view all the currently excluded files and applications, select the **Excluded** tab in the **App and file control** view.

## 2.4.3 Exclude files or folders from scanning

When you exclude files or folders from scanning, they are not scanned for harmful content.

To leave out files or folders from scanning:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Excluded** tab.
   This view shows you a list of excluded files and folders.
5. Select **Add new**.
6. Select the file or folder that you do not want to include in scans.
7. Select **OK**.

The selected files or folders are left out from the future scans.

## 2.4.4 View excluded applications

You can view applications that you have excluded from scanning, and remove them from the excluded items list if you want to scan them in the future.

If the product detects a potentially unwanted application that you know to be safe or spyware that you need to keep on your computer to use some other application, you can exclude it from scanning so that the product does not warn you about it anymore.

**Note:** If the application behaves like a virus or other harmful application, it cannot be excluded.

To view the applications that are excluded from scanning:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Excluded** tab.
   This view shows you a list of excluded files and folders.
5. If you want to scan the excluded application again:
   a) Select the application that you want to include in the scan.
   b) Click **Remove**.

New applications appear on the exclusion list only after you exclude them during scanning and cannot be added to the exclusion list directly.

## 2.4.5 Allow applications that DeepGuard has blocked

You can control which applications DeepGuard allows and blocks.

Sometimes DeepGuard may block a safe application from running, even if you want to use the application and know it to be safe. This happens because the application tries to make system changes that might be potentially harmful. You may also have unintentionally blocked the application when a DeepGuard pop-up has been shown.

To allow the application that DeepGuard has blocked:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Blocked** tab.
   This shows you a list of the applications that DeepGuard has blocked.
5. Find the application that you want to allow and select **Allow**.
6. Select **Yes** to confirm that you want to allow the application.

The selected application is added to the **Excluded** list, and DeepGuard allows the application to make system changes again.

## 2.4.6 Adding and removing protected folders

You can choose which folders require an additional layer of protection against destructive software, such as ransomware.

DataGuard blocks any unsafe access to your protected folders.

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

   **Note:** You need administrative rights to change the settings.

   The **App and file control view** opens.
4. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
5. Add or remove folders as needed.

   To add a new protected folder:

a) Click **Add new**.
b) Select the folder that you want to protect.
c) Click **Select folder**.

**Tip:** As you must separately allow all applications that need to access the protected folder, we recommend that you do not add folders that contain your installed games or applications (for example, Steam Library Folders). Otherwise, these applications may stop working correctly.

To remove a folder:

a) Select the folder on the list.
b) Click **Remove**.

**Tip:** Click **Restore defaults** if you want to undo any changes that you have made to the list of protected folders since installing the product.

## 2.5 Prevent applications from downloading harmful files

You can prevent applications on your computer from downloading harmful files from the internet.

Some websites contain exploits and other harmful files that may harm your computer. With advanced network protection, you can prevent any application from downloading harmful files before they reach your computer.

To block any application from downloading harmful files:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. Select **Edit settings**.

   **Note:** You need administrative rights to change the settings.

3. On the main page, select .
4. Select **Malware Protection** > **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.

5. Turn on **Advanced Network Protection**.

   **Note:** This setting is effective even if you turn off the firewall.

## 2.6 Using AMSI integration to identify script-based attacks

Antimalware Scan Interface (AMSI) is a Microsoft Windows component that allows the deeper inspection of built-in scripting services.

**Note:** AMSI integration is only available on Windows Server 2016, 2019 and 2022.

Advanced malware uses scripts that are disguised or encrypted to avoid traditional methods of scanning. Such malware is often loaded directly into memory, so it does not use any files on the device.

AMSI is an interface that applications and services that are running on Windows can use to send scanning requests to the antimalware product installed on the computer. This provides additional protection against harmful software that uses scripts or macros on core Windows components, such as PowerShell and Office365, or other applications to evade detection.

To turn on AMSI integration in the product:

1. Open F-Secure Server Security from the Windows **Start** menu.
2. On the main page, select .
3. Select **Malware Protection** > **Edit settings**.

**Note:** You need administrative rights to change some of the settings.

4. Turn on **Antimalware Scan Interface (AMSI)**.
   The product now notifies you of any harmful content that AMSI detects, and logs those detections in the event history.

Chapter

3

# Centrally managed administration

**Topics:**

## 3.1 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 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 F-Secure Policy Manager Console (settings marked as **Final** are greyed out in Web Console).

## 3.2 Settings for Microsoft Exchange

The F-Secure Email and Server Security settings related to Microsoft Exchange are located under **Microsoft Exchange** on the **Settings** tab in Policy Manager Console.

### 3.2.1 General settings

#### Network

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

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

**Note:** If email messages come from internal SMTP sender hosts and contain both internal and external recipients, messages are split and processed as internal and outgoing respectively.

| | |
|---|---|
| **Internal domains** | Specify internal domains. Messages coming to internal domains are considered to be inbound mail unless they come from internal SMTP sender hosts.<br><br>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 email client to send and receive email, 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.

---

## Notifications

Specify the **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.

## Lists and templates

The product uses lists and templates for several settings, for example to define folder paths, as well as notification message content. You can edit the lists and templates in Policy Manager Console by clicking **Edit lists** or **Edit templates** respectively next to the applicable setting.

### 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 file patterns or email addresses.

| | |
|---|---|
| **Filter** | Specify file names, extensions, or email addresses that the match list contains. You can use wildcards.<br>  **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** | Specify the subject line of the notification message. |
| **Body** | Specify the notification message text.<br>For more information about the variables you can use in notification messages, see Variables in warning messages on page 134 . |
| **Description** | Specify a short description for the template. |

## 3.2.2 Transport protection

You can configure incoming, outgoing, and internal message protection separately. For more information about the mail direction and configuration options, see General settings on page 27 .

**General**

| | |
|---|---|
| **Intelligent file type recognition** | Select whether you want to use **Intelligent file type recognition** or not.<br>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.<br>  **Note:** Using Intelligent file type recognition strengthens the security, but can degrade the system performance. |

| | |
|---|---|
| **FTR exclusions** | Enter any file extensions that you do not want intelligent file type recognition to process. |
| **Trusted senders** | Specify senders who are excluded from the mail scanning and processing. For more information, see General settings on page 27 . |
| **Trusted recipients** | Specify recipients who are excluded from the mail scanning and processing. For more information, see General settings on page 27 . |

### Security options

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

| | |
|---|---|
| **Add disclaimer** | Specify whether you want to add a disclaimer to all outgoing messages.<br><br>When the disclaimer is enabled, a disclaimer text is added to all outbound messages.<br><br>  **Note:** You can configure disclaimer settings for outbound messages only.<br><br>  **Important:**<br>Some malware add disclaimers to infected messages, so disclaimers should not be used for stating that the message is clean of malware. |
| Disclaimer | Specify the text of disclaimer that is added at the end of outbound messages. |

**Action on malformed mails**

Specify the action for non-RFC compliant emails. 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 email messages. A nested email message is a message that includes one or more email 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.<br>**Drop the whole message** - Messages with exceeding nesting levels are not delivered to the recipient.<br>**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 email message. |

### Attachment filtering

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

| | |
|---|---|
| **Strip attachments** | Enable or disable the attachment stripping. |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see General settings on page 27 . |
| **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 on disallowed attachments** | Specify how disallowed attachments are handled.<br>**Drop attachment** - Remove the attachment from the message and deliver the message to the recipient without the disallowed attachment.<br>**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 which files are not quarantined even when they are stripped. For more information, see General settings on page 27 . |
| **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. |
| **Notification about stripped attachment to the recipient** | Specify the template for the notification message that is sent to the intended recipient when disallowed or suspicious attachment is found.<br>  **Note:** Note that the notification message is not sent if the whole message is dropped. |
| **Notification about stripped attachment to the 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 General settings on page 27 .<br>Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent. |

### Malware scanning

Specify incoming, outgoing 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. |
| **Scan these attachments** | Specify attachments that are scanned for viruses. For more information, see General settings on page 27 . |
| **Exclude these attachments** | Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scan. |

**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 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 General settings on page 27 .

**Notification about virus to the 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.

**Notification about virus to the 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 General settings on page 27 .

**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 General settings on page 27 .

**Notify administrator**

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

### Grayware scanning

Specify how the product processes grayware items in incoming, outgoing, and internal messages.

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

**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.<br>**Pass through** - Leave grayware items in the message.<br>**Drop attachment** - Remove grayware items from the message.<br>**Drop the whole message** - Do not deliver the message to the recipient. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **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 General settings on page 27 . |
| **Notification about grayware to the recipient** | Specify the template for the notification message that is sent to the intended recipient when a grayware item is found in a message.<br>  **Note:** Note that the notification message is not sent if the whole message is dropped. |
| **Notification about grayware to the 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.<br>Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.<br>For more information, see General settings on page 27 . |
| **Do not notify on these grayware** | Specify the list of grayware types that are not notified about. |
| **Notify administrator** | Specify whether the administrator is notified when the product finds a grayware item in a message. |

### Archive scanning

Specify how the product processes incoming, outgoing, 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 General settings on page 27 . |
| **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 scan. |
| **Limit max levels of nested archives to** | Specify how many levels of archives inside other archives the product scans when **Scan archives** is turned on. |
| **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 to** setting.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - Remove the archive from the message and deliver the message to the recipient without it.<br>**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.<br>**Note:** Disallowed content is not processed when the archive scanning is disabled. |
| **Disallowed files** | Specify files which are not allowed inside archives. For more information, see General settings on page 27 . |
| **Action on archives with disallowed files** | Specify the action to take on archives which contain disallowed files.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - Remove the archive from the message and deliver the message to the recipient without it.<br>**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 Email quarantine on page 111 . |

| | |
|---|---|
| **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.<br><br>**Pass through** - Deliver the message with the password protected archive to the recipient.<br><br>**Drop attachment** - Remove the password protected archive from the message and deliver the message to the recipient without it.<br><br>**Drop the whole message** - Do not deliver the message to the recipient. |
| **Notify administrator** | Specify whether the administrator is notified when the product blocks a malformed, password protected, or nested archive file.<br><br>**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. |

### Unsafe URLs

Specify how the product handles unsafe URLs that are detected in the message body.

| | |
|---|---|
| **Scan messages for unsafe URLs** | Switch on to check all URLs found in the message body. |
| **Action on unsafe URLs** | Select how you want to handle messages that contain unsafe URLs:<br><br>**Drop the whole message** - Do not deliver the message to the recipient.<br><br>**Pass through** - The product allows the message to pass through. |
| **Quarantine dropped messages** | Select this if you have selected **Drop the whole message** as the action for handling unsafe URLs and you want to move those messages to the quarantine instead of deleting them. |
| **Notification about unsafe URLs to the recipient** | Specify the template for the notification message that is sent to the recipient of the message when an unsafe URL is found in a message. |
| **Notification about unsafe URLs to the sender** | Specify the template for the notification message that is sent to the original sender of the message when an unsafe URL is found in a message.<br><br>Leave notification message fields empty if you do not want to send any notification messages. By default, notification messages are not sent.<br><br>For more information, see General settings on page 27 . |

| | |
|---|---|
| **Notify administrator** | Specify whether the administrator is notified when the product blocks a message that contains an unsafe URL. |

## 3.2.3 Spam control

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

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.

### General

| | |
|---|---|
| **Check incoming email messages for spam** | Specify whether incoming 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.<br><br>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 email messages are falsely identified as spam.<br><br>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. |
| **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.<br><br>**Note:** Since all spam messages are relatively small in size, it is recommended to use the default value. |
| **Forward spam messages to email address** | Specify the email address where messages considered as spam are forwarded when the **Action on spam** setting is set to **Forward**. |
| **Action on spam** | Specify actions to take with messages considered as spam, based on the spam filtering level.<br><br>**Quarantine** - Place the message into the quarantine folder.<br><br>**Forward** - Forward the message to the email address specified in the **Forward spam messages to email address** setting.<br><br>**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.

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 *****.

## Safe senders and recipients

**Safe senders**

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

**Safe recipients**

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

## Blocked senders and recipients

**Blocked senders**

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

## 3.2.4 Quarantine

When the product places content to the email quarantine, it saves the content as separate files into the email quarantine storage and inserts an entry to the quarantine database with information about the quarantined content.

### General

**Quarantine storage**

Specify the path to the email quarantine storage where all quarantined mails and attachments are placed.

**Note:** If you change this setting, lock the setting (if it is unlocked, click the lock icon) to override initial settings.

**Note:** During 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 email quarantine storage on page 132.

### Quarantine thresholds

**Quarantine size threshold**

Specify the critical size (in megabytes) of the email quarantine. If the quarantine size reaches the specified value, the product sends an alert to the administrator.

If the threshold is set to zero (0), the size of the quarantine is not checked.

**Quarantined items threshold**

Specify the critical number of items in the email quarantine. When the quarantine holds the critical number of items, the product sends an alert to the administrator.

If the threshold is set to 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 email content is released from the quarantine.

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.

### Quarantine retention

| | |
|---|---|
| **Retain items in quarantine** | Specify how long quarantined emails are stored in the email quarantine before they are deleted automatically.<br><br>The setting defines the default retention period for all quarantine categories. To change the retention period for different categories, configure **Cleanup exceptions** settings. |
| **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. |

## 3.2.5 Manual storage 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. Go to the **Operations** tab in F-Secure Policy Manager Console.
2. Click **Scan** under **Exchange storage scan**.
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 include in the manual scan.

| | |
|---|---|
| **Scan mailboxes** | Specify mailboxes that are scanned for viruses.<br><br>**Do not scan mailboxes** - Do not scan any mailboxes.<br><br>**Scan all mailboxes** - Scan all mailboxes.<br><br>**Scan only included mailboxes** - Scan mailboxes specified in the **Included mailboxes** list.<br><br>**Scan all except excluded mailboxes** - Scan all mailboxes except those specified in the **Excluded mailboxes** list. |
| **Configure included and excluded mailboxes** | Specify the mailboxes to include or exclude in scanning when **Scan mailboxes** is set to either **Scan only included mailboxes** or **Scan all except excluded mailboxes**. |
| **Scan public folders** | Specify public folders that are scanned for viruses.<br><br>**Disabled** - Do not scan any public folders.<br><br>**Scan all public folders** - Scan all public folders.<br><br>**Scan only included public folders** - Scan public folders specified in the **Included folders** list.<br><br>**Scan all except excluded public folders** - Scan all public folders except those specified in the **Excluded folders** list. |

**Configure included and excluded public folders**

Specify the public folders to include or exclude in scanning when **Scan public folders** is set to either **Scan only included public folders** or **Scan all except excluded public folders**.

Specify public folders that are scanned for viruses when the **Scan public folders** setting is set to **Scan only included public folders**.

**Incremental scanning**

When selected, the operation only scans messages that have not been scanned since the previous manual or scheduled scan.

**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.

**FTR exclusions**

Enter any file extensions that you do not want intelligent file type recognition to process.

**Scan in test mode**

Select this to run the manual scan without making any modifications to scanned messages. This allows you to check the scanning report to see how messages and attachments would be processed based on your current settings. After testing your settings, clear this setting and run the manual scan again to apply changes.

**Limit max levels of nested messages to**

Specify how many levels deep to scan in nested email messages.

A nested email message is a message that includes one or more email 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.

**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 in the public folders.

---

### Attachment filtering

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

| | |
|---|---|
| **Strip attachments** | Enable or disable the attachment stripping. |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see General settings on page 27 . |
| **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. |
| **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 General settings on page 27 . |
| **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 General settings on page 27 . |

### Malware 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. |
| **Scan these attachments** | Specify attachments that are scanned for viruses. For more information, see General settings on page 27 . |
| **Exclude these attachments** | Specify attachments that are not scanned. Leave the list empty if you do not want to exclude any attachments from the scan. |
| **Ignore these viruses** | Specify the virus names that you want to ignore during scanning. You can use this, for example, to skip test files. |
| **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.<br><br>**Note:** Disinfection may affect the product performance.<br><br>**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 General settings on page 27 . |
| **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 General settings on page 27 . |

### 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.<br>**Pass through** - Leave grayware items in the message and notify the administrator.<br>**Drop attachment** - Remove grayware items from the message. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **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 General settings on page 27 . |
| **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 General settings on page 27 . |

### Archive scanning

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. |

| | |
|---|---|
| **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 scan. |
| **Limit max levels of nested archives to** | Specify how many levels deep to scan in nested archives, if **Scan archives** is enabled.<br><br>A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.<br><br>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 **Limit max levels of nested archives to** setting.<br><br>**Pass through** - Nested archives are scanned up to level specified in the **Limit max levels of nested archives to** setting. Exceeding nesting levels are not scanned, but the archive is not removed.<br><br>**Drop attachment** - Archives with exceeding nesting levels are removed. |
| **Detect disallowed files inside archives** | Specify whether files inside compressed archive files are processed for disallowed content. |
| **Disallowed files** | Specify files which are not allowed inside archives. For more information, see General settings on page 27 . |
| **Action on archives with disallowed files** | Specify the action to take on archives which contain disallowed files.<br><br>**Pass through** - Leave the archive in the message.<br><br>**Drop attachment** - 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 Email quarantine on page 111 . |
| **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.<br><br>**Pass through** - Leave the password protected archive in the message.<br><br>**Drop attachment** - Remove the password protected archive from the message. |

## 3.2.6 Scheduled storage 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. Select the checkbox to make it active again.
- Click **Add** to add a new scheduled task to the list.
- 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.

### Creating scheduled tasks

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

#### General Properties

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.<br>  **Note:** Do not use any special characters in the task name. |
| **Perform this task** | Specify how frequently you want the operation to be performed.<br>**Once** - Only once at the specified time.<br>**Daily** - Every day at the specified time, starting from the specified date.<br>**Weekly** - Every week at the specified time on the same day when the first operation is scheduled to start.<br>**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

Choose which mailboxes are processed during the scheduled operation.

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

### Public Folders

Choose which public folders are processed during the scheduled operation.

| | |
|---|---|
| **Public folders** | Specify public folders that are processed during the scheduled scan.<br>**Do not scan public folders** - Disable the public folder scanning.<br>**Scan all public folders** - Scan all public folders.<br>**Scan only included public folders** - Scan all specified public folders. Click **Add** or **Remove** to edit public folders that are scanned.<br>**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.<br>The format to enter the included or excluded mailbox is the name of the public folder. |

### Attachment Filtering

Choose settings for stripping attachments during the scheduled operation.

| | |
|---|---|
| **Strip attachments from email messages** | Enable or disable the attachment stripping. |
| Targets | |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see General settings on page 27 . |
| **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 General settings on page 27 . |
| 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 General settings on page 27 . |

### Virus Scanning

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. |
| Targets | |
| **Scan these attachments** | Specify attachments that are scanned for viruses. For more information, see General settings on page 27 . |
| **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.<br>  **Note:** Disinfection may affect the product performance.<br>  **Note:** Infected files inside archives are not disinfected even when the setting is enabled. |
| **Virus exclusion list** | Specify the virus names that you want to ignore during scanning. You can use this, for example, to skip test files. |
| **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 General settings on page 27 . |
| 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 General settings on page 27 . |

### Grayware Scanning

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.<br>**Report only** - Leave grayware items in the message and notify the administrator.<br>**Drop attachment** - Remove grayware items from the message. |
| Grayware exclusion list | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **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 General settings on page 27 . |
| 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 General settings on page 27 . |

### Archive Processing

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 General settings on page 27 .

**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 archives** is turned on.

**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 inside archives**

Select a list of disallowed files inside archives on which you want to take action.

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 attachment** - 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 nesting archives** setting.

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

**Drop attachment** - 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 attachment** - 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 Email quarantine on page 111 . |

### Advanced Options

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

**Processing options**

| | |
|---|---|
| **Use test mode** | Select this to run the scan without making any modifications to scanned messages. This allows you to check the scanning report to see how messages and attachments would be processed based on your current settings. |
| **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 email messages. A nested email message is a message that includes one or more email messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.<br>  **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.<br>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.<br>  **Note:** Using Intelligent File Type Recognition strengthens the security, but can degrade the system performance. |
| **FTR exclusions** | Enter any file extensions that you do not want intelligent file type recognition to process. |

### Summary

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

## 3.3 Settings for Microsoft SharePoint

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

### 3.3.1 General

Choose whether or not to use intelligent file type recognition for SharePoint, and how to handle the downloading of infected files.

| | |
|---|---|
| **Intelligent file type recognition** | Select whether you want to use **Intelligent file type recognition** or not.<br><br>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.<br><br>**Note:** Using Intelligent file type recognition strengthens the security, but can degrade the system performance. |
| **FTR exclusions** | Enter any file extensions that you do not want intelligent file type recognition to process. |
| **Download infected file action** | Select **Show warning** to display a warning about the infected file, but allow users to download them. Select **Block** to prevent users from downloading infected files. |

### 3.3.2 Malware scanning

Specify how the product processes malware.

| | |
|---|---|
| **Scan documents for viruses** | 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. |
| **Scan these documents** | Specify documents that are scanned for viruses. |
| **Exclude these documents** | Specify the list of documents that should not be scanned for viruses. |
| **Ignore these viruses** | Specify the virus names that you want to ignore during scanning. You can use this, for example, to skip test files. |
| **Notify administrator** | Specify whether the administrator is notified when the product finds a virus and the alert level of the notification. |

### 3.3.3 Grayware scanning

Specify how the product processes grayware items.

| | |
|---|---|
| **Scan documents for grayware** | When grayware scanning is enabled, the product scans for grayware (adware, spyware, riskware and similar).<br>**Note:** Grayware scanning is disabled if virus scanning is disabled. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **Action on grayware** | Specify the action to take on items which contain grayware.<br>**Pass through** - Let users access grayware items.<br>**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. |

### 3.3.4 Archive scanning

Specify how the product processes viruses inside archives.

| | |
|---|---|
| **Scan archives** | 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. |
| **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 scan. |
| **Limit max levels of nested archives to** | Specify how many levels deep to scan in nested archives, if archive processing is enabled.<br>A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.<br>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 **Limit max levels of nested archives to** setting.<br><br>**Pass through** - Nested archives are scanned up to level specified in the **Limit max levels of nested archives to** setting. Exceeding nesting levels are not scanned, but the archive is not removed.<br><br>**Block document** - 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.<br><br>**Pass through** - Leave the password protected archive in the message.<br><br>**Block document** - 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. |

### 3.3.5 Advanced configuration

The settings on the **Advanced configuration** page are intended for managing the product services that affect the performance of the server.

| | |
|---|---|
| **Notify SharePoint service of virus definition updates and scanning configuration changes** | Select this to send product update and configuration change notifications to the SharePoint service. |
| **Maximum number of concurrent scanning transactions** | Specify the maximum number of scanning processes that can be running at any given time. The default is 5. |
| **Maximum file size for scanning** | Specify the maximum size for individual files stored on SharePoint in megabytes. Any files larger than this are not scanned. |

## 3.4 Managing endpoint security

This section contains information on how to configure the endpoint security for managed Email and Server Security hosts in your network.

### 3.4.1 Configuring virus and spyware protection

Virus and spyware protection consists of automatic updates, manual scanning, scheduled scanning, real-time scanning, spyware scanning, DeepGuard, email scanning and browsing protection.

Virus and spyware protection keeps computers protected against file viruses, spyware, riskware, and viruses that are spreading by email attachments and in web traffic.

Automatic updates guarantee that virus and spyware protection is always up-to-date. Once you have set up virus and spyware protection and the automatic updates by distributing the settings in a security policy, you can be sure that the managed network is protected. You can also monitor the scanning results and other information the managed hosts send back to Policy Manager Console.

When a virus is found on a computer, one of the following actions will be taken:

- the infected file is disinfected,
- the infected file is renamed,
- the infected file is deleted,
- the infected file is quarantined,
- the user is prompted to decide what action to take with the infected file,
- the infected file or attachment (in email scanning) is reported only, or
- the infected attachment (in email scanning) is either disinfected, removed or blocked.

## Configuring automatic updates

This section explains the different configuration settings available for automatic updates in Policy Manager, and gives some practical configuration examples for hosts with different protection needs.

By following these instructions you can always keep the virus and spyware definitions on hosts up-to-date, and choose the best update source based on user needs.

### Configuring automatic updates from Policy Manager Server

When centralized management is used, all hosts can fetch their virus and spyware definition updates from Policy Manager Server.

In **Standard view**, this is configured as follows:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Make sure that the polling interval defined in **Interval for polling updates from F-Secure Policy Manager Server** is suitable for your environment.
4. If your network includes hosts with Client Security version 13.x installed, make sure that **Enable automatic updates** is selected.
5. If you want to restrict users from changing these settings, click the lock symbol beside the settings.
6. Click the following icon to distribute the policy:

### Configuring Policy Manager Proxy

If the different offices of a company have their own Policy Manager Proxy in use, it is often a good idea to configure the laptops that the user takes from one office to another to use a Policy Manager Proxy as the updates source.

In this configuration example, it is assumed that the laptops have been imported to one subdomain on the **Policy domains** tab, and that the different offices of the company have their own Policy Manager Proxy , and all of them will be included on the list of Policy Manager Proxy servers.

In **Standard view**:

1. Select the subdomain where you want to use the Policy Manager Proxy on the **Policy domains** tab.
2. Go to the **Settings** tab and select **Windows** > **Centralized management**.
3. Click **Add** next to the **Policy Manager Proxies** table to add new servers to the list of available proxy servers. This opens the **Policy Manager Proxy server properties** window.
4. Enter a priority number for the Policy Manager Proxy in the **Priority** text box.

   The priority numbers are used to define the order in which the hosts try to connect to the Policy Manager Proxy. Use, for example, `10` for the Policy Manager Proxy in the office where the host is normally located, and `20`, `30` and so on for the other proxies.
5. Enter the URL of the Policy Manager Proxy server in the **Address** text box, then click **OK**.
6. Repeat the above steps to add the other servers to the list.

7. When you have added all proxies to the list, check that they are in the correct order.
   If necessary, you can modify their order by altering the priority numbers.
8. If the policy domain includes hosts with Client Security 13.x installed, make sure that **Enable automatic updates** is selected.
9. If you want to restrict users from changing these settings, click the lock symbols beside the settings.
10. Click the following icon to distribute the policy:

**Note:** End users can also add a Policy Manager Proxy to the list in the local user interface, and the host uses a combination of these two lists when downloading virus and spyware definitions updates. A Policy Manager Proxy added by an end user is tried before those added by the administrator.

## Configuring real-time scanning

Real-time scanning protects the computer all the time, as it is scanning files when they are accessed, opened or closed.

It runs in the background, which means that once it has been set up, it is mostly transparent to the user.

### Enabling real-time scanning for the whole domain

In this example, real-time scanning is enabled for the whole domain.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
3. Select **Enable real-time scanning**.
4. Select **Files with these extensions** from the **Files to scan:** drop-down list.
5. Select how to handle infected files from the settings under the **Actions on malware detection** sections.
   The settings are divided into two groups so that you can choose different settings for workstations and servers.
6. Check that the other settings on this page are suitable for your system, and modify them if necessary.
7. Click the following icon to distribute the policy:

### Excluding files from real-time scanning

You may want real-time scanning to skip certain files, either based on the file extension or the file path.

For example, you might not want to scan Microsoft Outlook's `.PST` file to avoid slowing down the system unnecessarily, as PST files are typically very large and take a long time to scan.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
   To select files based on their file extension:
   a) Select **Do not scan files with the following extensions**.
   b) Enter the extension in **Excluded extensions**.

   **Note:** The extensions should be added without the preceding `.` (dot). Separate multiple extensions with spaces.

   To select files based on their location or checksum (hash):
   a) Select **Do not scan the following files and applications**.
   b) Click **Add**.
   c) Select the scope.
   Select **All** if you want the exclusion to apply to both real-time and manual scanning.

d) Select the identification method.

Select **File path** if the file always uses the same path.

Select **Folder path** if you want scanning to skip all files in a specific folder.

Select **Application SHA-1** if the path for the file may vary across different hosts. Note that this option is only available for the real-time scanning scope.

e) Enter the path or hash that you want to exclude from scanning.
For example:

- File name: `text.txt` (all files named `text.txt` are not scanned).
- Full file path: `C:\test\text.txt` (the `text.txt` file in the `C:\test` folder is not scanned).
- Folder path: `C:\test` (all contents in the `C:\test` folder are not scanned).

For more information on using wildcards, see https://community.f-secure.com/t5/Business/Using-wildcards-in-exclusions/ta-p/20428.

**Note:** DeepGuard does not support exclusions that are configured using wildcards or device names.

You can also add a comment if you want to keep a record of why the file or application was excluded.

f) Click **OK**.

3. If you do not want to allow users to exclude files or applications from scanning, select **Prevent users from adding scanning exclusions**.
4. Click the following icon to distribute the policy:

## Excluding processes from real-time scanning

To optimize disk performance on managed hosts, you may want to exclude some processes from scanning.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** › **Real-time scanning**.
3. Select **Do not scan the following processes**.
4. Enter each process to exclude on its own line in **Excluded processes**.

   Enter the full path for each process, for example `C:\Program Files\Application\app1.exe`. You can also use system environment variables in the path, for example `%ProgramFiles%\Application\app1.exe`.

   **Note:** Any files that the excluded processes access are also excluded from scanning.

5. Click the following icon to distribute the policy:

## Configuring scheduled scanning

You can add a scheduled scanning task in **Advanced view**.

In this example, a scheduled scanning task is added in a policy for the whole policy domain. The scan is to be run weekly, every Monday at 8 p.m, starting from August 24, 2020.

In **Advanced view**:

1. Select **Root** on the **Domain tree**.
2. On the **Settings** tab, select **F-Secure** › **F-Secure Anti-Virus** › **Settings** › **Scheduler** › **Scheduled tasks**.
   The currently set scheduled tasks are displayed on the **Scheduled tasks** table. Now you can add scheduled scanning as a new task.
3. Click **Add**.
   This adds a new row to the **Scheduled tasks** table.

4. Click the **Name** cell on the row you just created and then click **Edit**.
5. The **Name** cell is now activated and you can enter a name for the new task.

   For example, `Scheduled scanning for all hosts`.
6. Next click the **Scheduling parameters** cell, and then click **Edit**.
7. Now you can enter the parameters for the scheduled scan.

   A scheduled scan that is to be run weekly, every Monday starting at 8 p.m, from August 24, 2020 onwards, is configured as follows: `/t20:00 /b2020-08-24 /rweekly`

   **Note:** When the **Scheduling parameters** cell is selected, the parameters that you can use and their formats are displayed as a help text in the **Messages** pane (below the **Scheduled tasks** table).
8. Select the task type by clicking the **Task type** cell and then clicking **Edit**.
9. From the drop-down list that opens select **Scan local drives**.
   The scanning task is now ready for distribution.
10. Click the following icon to distribute the policy:

Running scheduled scans on specific weekdays and days of the month:

When you are configuring a weekly scheduled scan, you can also define specific weekdays when the scan is to be run. Similarly, when you are configuring a monthly scheduled scan, you can define specific days of the month when the scan is to be run. For both of these, you can use the `/Snn` parameter:

- For weekly scheduled scans you can use `/rweekly` together with parameters `/s1` - `/s7`. `/s1` means Monday and `/s7` means Sunday.

  For example, `/t18:00 /rweekly /s2 /s5` means that the scan is run every Tuesday and Friday at 6 p.m.
- For monthly scheduled scans you can use `/rmonthly` together with parameters `/s1` - `/s31`.

  For example, `/t18:00 /rmonthly /s5 /s20` means that the scan is run on the 5th and 20th of each month at 6 p.m.

**Note:** If you do not define a weekday, weekly scheduled scans are run on each Monday by default. Monthly scheduled scans are run on the first day of each month by default, if you have not defined a specific day.

## Configuring DeepGuard

DeepGuard is a host-based intrusion prevention system that analyzes the behavior of files and programs.

DeepGuard can be used to block intrusive ad pop-ups and to protect important system settings, as well as Internet Explorer settings against unwanted changes.

If an application tries to perform a potentially dangerous action, it will be checked for trust. Safe applications are allowed to operate, while actions by unsafe applications are blocked.

To turn on DeepGuard:

1. Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
2. Select **Enable DeepGuard**.
3. Select **Block rare and suspicious files** if you want to use DeepGuard's prevalence-based rules to block files that may not be commonly recognized.

   **Note:** This feature is only available for version 15 and newer clients.
4. Click the following icon to distribute the policy:

## DataGuard

DataGuard is a feature that strengthens DeepGuard by monitoring specific folders to prevent untrusted applications from modifying files on managed hosts.

DataGuard is especially useful against any new ransomware that is able to get past other security layers.

In Policy Manager, you can set the folders that DataGuard monitors and protects. There are predefined options for the default folders for user content, such as Documents, Music, Pictures, etc. You can also set the trusted applications that are allowed to access the protected folders and modify the files there. Applications that are not considered trusted are stopped if they try to modify any protected files.

## SETTING UP DATAGUARD

You can define the folders that DataGuard protects on managed computers, and add trusted applications that you do not want DataGuard to block

When DataGuard is turned on, untrusted applications and malware (including ransomware) cannot modify files in folders that you define as protected.

**Note:** Be careful in selecting the protected folders and trusted applications for DataGuard. Adding a wide range of data (either lots of folders or, for example, `C:\`) can cause a lot of unnecessary interruptions. Also, adding a very wide scope of locations to the trusted applications list may allow malware to modify protected files.

To use DataGuard:

1. Go to the **Settings** tab and select **Windows** > **DataGuard**.
2. Select **Turn on DataGuard protection**.
3. In the **Protected data folders** table, select the folders that you want to protect.

   To add more protected folders:

   a) Enter the folder path in the **Folder** field.

   You can use environment variables in the path. User environment variables apply to the corresponding paths for each Windows user account on the computer. The supported variables are: `%UserProfile%`, `%HomeDrive%`, `%HomePath%`, `%ProgramData%`, `%WinDir%`, `%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%`, and `%ProgramFiles(x86)%`.

   b) Add a description for the new folder in the **Comments** field.

**Note:** Universal Naming Convention (UNC) paths are also supported for the protected folders.

4. Select the applications that are allowed to modify files that are in protected folders.
5. Select **Discover trusted applications automatically** if you want to allow known, trusted system applications to modify the protected folders.
6. Add more trusted applications to the table if necessary.

   - To add a single application, enter the full path to the executable including file name and extension.
   - To add a folder that may contain several applications, enter the path to the folder.

**Note:** Some applications and standard Windows features may require adding more than one application file to the list of trusted applications. For example, the print-to-PDF functionality in Windows uses the following executable files: `<Windows folder>\System32\spoolsv.exe` and `<Windows folder>\System32\printfilterpipelinesvc.exe`.

7. Click the following icon to distribute the policy:

We recommend that you apply the common practices and tools for your organization when considering the protected folders and trusted applications for DataGuard. It is also a good idea to apply specific rules for separate policy domains where possible. For example, if your domain tree is structured according to teams or departments, you can apply separate rules for developers and salespeople.

## Managing quarantined objects

Quarantine management gives you the possibility to process objects that have been quarantined on host machines in a centralized manner.

All infected files and spyware or riskware that have been quarantined on host machines are displayed on the **Settings** > **Windows** > **Quarantine management** page. From there, you can either release the objects from quarantine, or delete them.

**Note:** Quarantine management should be used primarily for troubleshooting purposes. For example, if a business-critical application is considered riskware and it has not yet been included in the virus definition database, you can use quarantine management to allow it to be used. Such cases are relatively rare, and once new virus definition updates that treat the application as normal are available, the problem should be fixed automatically.

## Deleting quarantined objects

Infected files, spyware or riskware that have been quarantined on hosts can be removed from quarantine, in which case they are deleted from the host machine.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Quarantine management**.
3. Select the quarantined object you want to delete on the **Quarantined objects** table, and click **Delete**.
   The object is moved to the **Actions to perform on quarantined objects** table, with **Delete** given as the **Action** for the object.
4. Click the following icon to distribute the policy:

## Releasing quarantined objects

Infected files, spyware or riskware that have been quarantined on hosts can be released from quarantine, in which case they are allowed on the host machines and can be accessed and run normally.

In **Standard view**:

1. Select the target domain.
2. Create an exclusion rule for the object.

   Exclusion rules are required to make sure that the object will not be quarantined again in future. If the object is listed as a virus or infected file:

   a) Go to the **Settings** > **Windows** > **Quarantine management** page and copy the object's file path.
   b) Go to the **Settings** tab and select **Windows** > **Real-time scanning**.
   c) Check that **Do not scan the following files and applications** is selected.
   d) Click **Add** next to the exclusion table.
   e) Select **All scans** as the scope, select **File path**, and paste the object's file path to the path field.
   f) Click **OK**.
3. Go to the **Settings** tab and select **Windows** > **Quarantine management**.
4. Select the quarantined object you want to allow on the **Quarantined objects** table, and click **Release**.
   The object is moved to the **Actions to perform on quarantined objects** table, with **Release** given as the **Action** for the object.
5. Click the following icon to distribute the policy:

## Hiding notifications on managed hosts

You can hide the security notifications and computer restart prompts from end users.

Policy Manager includes separate settings for the visibility of notifications on workstations and servers.

In **Standard view**:

1. Select the target domain.

   To hide security notifications and computer restart prompts from end users:

   a) Go to the **Settings** tab and select **Windows** › **Centralized management**.

   b) Under **User notifications**, select **Administrators only** from drop-down lists for workstations and servers.

2. Click the following icon to distribute the policy:

## Preventing users from changing settings

If you want to make sure that the users cannot change some or any of the virus protection settings, you can make these settings final.

There are different possibilities for doing this:

- If you want to prevent users from changing a certain setting, click on the lock symbol beside it.
- When you are on one of the pages on the **Settings** tab in **Standard view**, you can set all the settings on the page final at once by clicking **Disallow user changes**. This page-specific shortcut affects only the settings that have an attached lock symbol and it operates all lock symbols on the page at once.
- If you want to make all settings for both virus protection and firewall final, go to the **Settings** tab and **Centralized management** page in **Standard view**, and click **Do not allow users to change any settings...**.

## Setting all virus protection settings as final

In this example, all the virus protection settings are set as final.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** › **Centralized management**.
3. Select **Do not allow users to change any settings**.
4. Click **Yes**.
5. Click the following icon to distribute the policy:

## Configuring alert sending

This section describes how to configure the product to send virus alerts to an email address and how to disable the alert pop-ups.

It is a good idea to have all virus alerts sent to administrators by email to ensure that they are informed of any potential outbreaks as quickly as possible.

## Sending virus alerts to an email address

In this example, all the security alerts that the managed hosts generate are forwarded to an email address.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** › **Alert sending**.
3. Click **13.x clients**.
4. Set up **Email alert sending**:

   If email alert sending has not been set up before, you can do it now, as follows:

   a) Enter the address of the SMTP server in the **Email server address (SMTP)** field.

   Use the following format:

   `<host>[:<port>]` where `host` is the DNS name or IP address of the SMTP server, and `port` is the SMTP server port number.

   b) Enter the sender's address for email alert messages in the **Email sender address (From):** field.

c) Enter the email alert message subject in the **Email subject:** field.

Refer to the MIB help text for a list of possible parameters to use in the message subject.

5. Set up **Alert forwarding**:

The **Alert forwarding** table is used to configure where different types of alerts are forwarded.

a) Select the **Email** check box on the **Security alert** row.
This opens the **Email recipient addresses (To)** dialog box.

b) Select **Use the same address for all products**, and enter the email address in the field that is activated.

If you want the alerts to be sent to several email addresses, separate them by commas.

c) When finished, click **OK**.

6. Click the following icon to distribute the policy:

## Disabling alert pop-ups

In this example, alerting is configured so that no alert pop-ups are displayed to users.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Alert sending**.
3. Clear the check boxes for all products in the **Local user interface** column.
4. Click the following icon to distribute the policy:

## Monitoring viruses on the network

Policy Manager offers different ways and levels of detail for monitoring infections on your network.

The best way to monitor whether there are viruses on the network is to check the **Virus protection for endpoints** section of the **Summary** view on the **Dashboard** tab. If it displays new infections, you can access more detailed information by clicking **View hosts' infection status**. It takes you to the **Status** tab and **Virus protection** page, where you can see details of each host's infection status.

You can also check the **Alerts** and **Scanning reports** tabs to see the scanning reports from different hosts.

## Testing your antivirus protection

To test that the managed security products operate correctly, you can use a special test file that is detected as though it were a virus.

This file, known as the EICAR Standard Anti-Virus Test File, is also detected by several other antivirus programs. You can also use the EICAR test file to test your email scanning. EICAR is the European Institute of Computer Anti-virus Research. The Eicar info page can be found at http://www.f-secure.com/v-descs/eicar.shtml.

You can test your antivirus protection as follows:

1. You can download the `EICAR` test file from http://www.f-secure.com/v-descs/eicar.shtml.

Alternatively, use any text editor to create the file with the following single line in it:

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

2. Save this file to any name with a `.com` extension, for example `EICAR.COM`.

Make sure that you save the file in the standard MS-DOS ASCII format. Note also that the third character of the extension is an upper-case O, not numeral 0.

3. Now you can use this file to see what it looks like when the product detects a virus.

Naturally, the file is not a virus. When executed without any virus protection, `EICAR.COM` displays the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!` and exits.

## 3.4.2 Configuring firewall settings

This section provides an overview of the firewall settings and how you can configure them to suit your network.

The firewall protects computers against unauthorized access from the internet as well as against attacks originating from inside the LAN.

F-Secure product versions 14.00 and newer use the Windows Firewall component. F-Secure's firewall profiles provide an additional security layer on top of the Windows Firewall user rules and other domain rules. The F-Secure firewall profiles or rules are not applied if Windows Firewall is off. Therefore, we recommend that you always keep the firewall on.

Older product versions use F-Secure's own firewall component. This contains predefined security levels, each of which has a set of pre-configured firewall rules associated with them. Different security levels can be assigned to different users based on, for example, company security policy, user mobility, location, and user experience.

**Note:** If you use a GPO or third-party firewall, in most cases you need to turn off F-Secure firewall profiles to avoid conflicts. If this is the case, make sure that the **Enable firewall configuration through Policy Manager** setting on the **Settings** > **Windows** > **Firewall** page is not selected.

### Turning on the firewall

Keep the firewall turned on to block intruders from accessing computers in your managed network.

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. Select **Enable firewall configuration through Policy Manager**.

   **Note:** If you use a GPO or third-party firewall, in most cases you need to make sure that this setting is not selected to avoid conflicts.

5. Select **Enable firewall**.
6. Click the following icon to distribute the policy:

### Configuring network quarantine

Network quarantine is a firewall feature that makes it possible to restrict the network access of hosts that have very old virus definitions and/or that have real-time scanning turned off.

The normal access rights of such hosts are automatically restored once the virus definitions are updated and/or real-time scanning is turned on again.

This section describes the network quarantine settings and contains an example of how to enable the network quarantine feature in the managed domain. There is also a short description of how to configure the network quarantine security level by adding new firewall rules.

### Turning network quarantine on in the whole domain

You can enable network quarantine for the whole domain by following the steps given here.

In **Standard view**:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Select **Enable network quarantine**.
4. Specify the **Virus definitions age to activate network quarantine**.
5. If you want to restrict the host from accessing the network when real-time scanning is turned off, select **Activate network quarantine on host if real-time scanning is disabled**.
6. Click **Configure network isolation rules** to modify the firewall rules for quarantined hosts.
7. Click the following icon to distribute the policy:

## Fine-tuning network quarantine

Network quarantine is implemented by forcing hosts to use a restricted set of firewall rules.

You can add new **Allow** rules to the network isolation rules to allow additional network access to hosts in network quarantine. You should not restrict access further as this may cause hosts to lose network connectivity.

**Note:** For product versions 13 and older, quarantined hosts are forced to the **Network quarantine** firewall security level. This security level has a restricted set of firewall rules. Similarly to the network isolation rules for newer product versions, you can add new **Allow** rules to the security level, but should not restrict access further.

## Firewall settings for version 14 clients and newer

This section describes the settings that you can configure for F-Secure's firewall profiles, which provide an additional layer of security for Windows Firewall.

**Note:** You must have Windows Firewall turned on for your network via Group Policy Object (GPO) to manage the firewall settings through Policy Manager. If Windows Firewall is turned off via GPO, Policy Manager cannot override those settings and the firewall policies will not be applied.

## Selecting the active firewall profile for a domain

You can set a specific firewall profile for any domain within your managed network.

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. Select the firewall profile for the domain from the **Workstation host profile** and **Server host profile** drop-down lists.

   **Note:** The default profile for F-Secure Server Security clients is set to **Server**.

5. Click the following icon to distribute the policy:

## Creating a new firewall profile for a domain

You can create a new firewall profile by cloning an existing one.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. In the **Profile being edited** drop-down, select the profile that you want to clone.
5. Click **Clone**.
6. Enter a name for the new profile, then click **OK**.
7. Configure the settings and rules for the new profile.
8. Click the following icon to distribute the policy:

## Adding firewall rules

You can add new rules to firewall profiles that have been added within the scope of your domain access.

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Firewall**.
3. Click **14.x clients**.
4. In the **Profile being edited** drop-down, select the profile that you want to edit.
5. Click **Add rule**.

6. Enter a name for the rule and select the type (either **Allow** or **Block**), then click **Next**.

   **Note:** For **Block** rules, select **Send an alert when the rule blocks a connection** if you want to receive alerts when the rule is triggered.

7. For each network service that you want the rule to include:
   a) Click **Add**.
   b) Select the service from the **Service** drop-down list.
   c) Select the traffic direction from the **Direction** drop-down list.

| Direction | Explanation |
|---|---|
| **Both** | The service will be allowed/denied to/from your computer in both directions. |
| **Inbound** | The service will be allowed/denied if coming from the defined remote hosts or networks to your computer. |
| **Outbound** | The service will be allowed/denied if going from your computer to the defined remote hosts or networks. |

8. Click **Next**.
9. Specify the remote addresses that apply for the rule, then click **Next**.
10. Specify the scope for the rule, then click **Finish**.
    The new rule is added to the **Firewall rules** table for the selected profile.
11. Click the following icon to distribute the policy:

**Note:** Added firewall rules only apply to the profile that you are editing. If several profiles require the same rule, you have to add it for each profile separately.

**Related tasks**

Creating a new network service for firewall rules on page 65
If you need a network service that is missing from the set of default services, you can add it separately for use in custom firewall rules.

### Creating a new network service for firewall rules

If you need a network service that is missing from the set of default services, you can add it separately for use in custom firewall rules.

1. Go to the **Settings** tab and select **Windows** › **Firewall**.
2. Click **14.x clients**.
3. Click **Configure network services** below the **Firewall rules** list.
4. Click **Add**.
5. Enter a name for the service.
6. Select the IP protocol number, then click **Next**.
7. Enter the initiator ports, then click **Next**.
8. Enter the responder ports, then click **Finish**.

You can now select the new network service when you add or edit your custom firewall rules.

## 3.4.3 Configuring application control

Application control prevents execution and installation of applications, and prevents them from running scripts.

**Note:** Application control is only available for F-Secure product versions 14 and newer.

Application control reduces the risks that malicious, illegal, and unauthorized software pose in the corporate environment. It provides the following features:

- Security: Pre-configured security rules designed by F-Secure penetration testers cover attack vectors that are used to breach into corporate environments.
- Policy enforcement: Based on a simple rule editor, policy enforcement helps the administrator define which applications are blocked, allowed, or monitored.

## Configuring application control

Application control prevents execution and installation of applications, and prevents them from running scripts.

**Note:** Application control is only available for F-Secure product versions 14 and newer.

Application control reduces the risks that malicious, illegal, and unauthorized software pose in the corporate environment. It provides the following features:

- Security: Pre-configured security rules designed by F-Secure penetration testers cover attack vectors that are used to breach into corporate environments.
- Policy enforcement: Based on a simple rule editor, policy enforcement helps the administrator define which applications are blocked, allowed, or monitored.

Turn on application control to prevent the execution and installation of applications, and to prevent them from running scripts:

1. Select **Root** on the **Domain tree**.
2. Go to the **Settings** tab and select **Windows** > **Application control**.
3. Select **Enable Application control**.
4. Select the profile to use in the **Host profile** drop-down list.
5. Click the following icon to distribute the policy:

## Creating a new application control profile

You can create a new application control profile by cloning an existing one.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Application control**.
3. Select the profile that you want to clone from the **Profile being edited** drop-down list.
4. Click **Clone**.
5. Enter a name for the new profile, then click **OK**.
6. Select how you want to handle applications in the **Default rule applied to all applications** drop-down list.
   The selected action is applied to any applications that are not covered by the exclusion rules for the profile.
7. Configure the exclusion rules for the new profile.
8. Click the following icon to distribute the policy:

## Adding exclusion rules

Application control's exclusion rules give you a way to define the applications that you want to explicitly allow or block.

Any applications that match the conditions that you set within the rules are excluded from the default rule for the profile. For example, if the default rule is **Allow**, you can create rules to specify the applications or locations that you want to block. Another example could be that you want to receive a report of any applications that match the triggering conditions, even though they are still allowed or blocked based on the default rule for the profile.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Application control**.

3. Select the profile that you want to edit from the **Profile being edited** drop-down list.

   **Note:** You cannot edit the exclusion rules for any profiles that are marked as **Predefined**.

4. Click **Add rule**.
   This opens the exclusion rule wizard.
5. Enter a name and description for the rule.
6. Select the **Event** and **Action** for the rule.

   The following table lists the available event types and when they are triggered.

| Event | Description |
|---|---|
| Run application | A combination of Start process and Load dynamic library. Triggers when an executable file or script is launched and when a DLL is about to get loaded into a process. |
| Run installation | Triggers when `msiexec.exe` is launched with some MSI package as a command line parameter. |
| Start process | Triggers when an executable file or script is launched. |
| Load dynamic library | Triggers when a DLL is about to get loaded into a process. |
| File access | Triggers when a file matching the target conditions is opened or accessed by an application. |

   For example, if you select **Run application** as the event and **Block** as the action, the rule prevents applications from running if they match the conditions for the rule.
7. Click **Add condition**.

   You can add multiple conditions to the same rule to get the scope that you want.

   Note the following when adding conditions to an exclusion rule:

   - If you use attribute `Target SHA1` or `Parent SHA1` in the exclusion rule condition, you have to use **Start process** as the event type.
   - If a dynamic link library (.dll) is blocked and you want it to be allowed by Application Control, you have to use the **Load dynamic library** event type in the exclusion rule. In a case like this, you cannot therefore use attribute `Target SHA1` nor `Parent SHA1` in the exclusion rule.
   - Attributes `Target file names mismatch` and `Parent file names mismatch` kick in when the binary filename is different from the "Original filename" found under file Properties > Details.

8. Select the attribute, operator, and value for each condition.

   The following table explains the attributes that you can select to match the condition values.

| Selected attribute | Description |
|---|---|
| Target | Values of the actual application. For example, **Target file name** is the actual file that you want to block. |
| Parent | Values of the process that launches the application. For example, **Parent file name** is the file that launches the application that you want to block. |

   For example, if you want to block Internet Explorer, `iexplore.exe` is the target and `explorer.exe` (Windows Explorer) is the parent.

   The following table explains how different operators work with the values that you enter.

| Selected condition | Description |
|---|---|
| Equals | The value must be exactly the same as the target, for example, `iexplore.exe`. |
| Not equals | The value may be anything except the target. |
| Less, Greater, Less or equals, Greater or equals | These apply to numeric values, for example if you select **Target product version** as the attribute. |
| Contains | The selected attribute must contain the value, for example, `explore`. |
| Starts with | The selected attribute must start with the value, for example, `ie`. |
| Ends with | The selected attribute must end with the value, for example, `explore.exe`. |

9. Click **OK**.
10. Change the order of the rules if necessary.

    The rules listed for the profile are applied in priority order from the top down.
11. Click the following icon to distribute the policy:

**Note:** If there are any issues with the rule, for example if some information is missing or invalid, the host sends an alert to Policy Manager.

## Example: Preventing a vulnerable version from running

To use Application control to prevent vulnerable applications from running, for example, to block an unpatched version, use a Target file version attribute.

For example, a program had a vulnerability that was patched in version 1.2.4. To block any version older than 1.2.4 from running, do the following.

1. Create the following exclusion rule:
   a) Give the rule a name: `Block an unpatched program`.
   b) From the **Event** drop-down menu, select **Run application**.
   c) From the **Action** drop-down menu, select **Block**.
2. Then, add the first condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target file description**.

      **Note:** To find the file description, right-click the file in the File Explorer and select Properties.

   b) From the operator drop-down menu, select **Contains**.
   c) In the value field, enter the name of the unpatched program as it appears in the file description. For example, "Internet Explorer".

      **Note:** As "Internet Explorer" is in the target file description, the program is blocked regardless of the file name or its location.
3. Then, add the second condition to the exclusion rule:
   a) From the attribute drop-down menu, select **Target file version**.
   b) From the operator drop-down menu, select **Less or equals**.
   c) In the value field, enter `1.2.3.*.*`.

**Note:** The condition for the target file version is "less or equal to 1.2.3.*.*" The asterisk indicates that only major and minor fields are used in the comparison.

## 3.4.4 Using Device Control

Device Control blocks certain hardware devices to protect the network.

Device Control prevents malware from spreading to the network from external devices such as USB storage devices and DVD/CD-ROM drives. When a blocked device is plugged in to the client computer, Device Control turns it off to prevent access to it.

### Configuring Device control

Device control can be configured with F-Secure Policy Manager.

Follow these instructions to configure Device control.

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. To turn on Device control, select **Device control enabled**.
3. Set the type of alert that is sent to the administrator when a device is blocked.
4. The **Device access rules** table contains rules for blocking devices.
   A device that has **Access Level** set to **Blocked** cannot be accessed, when the rule is set as active.

### Limiting access permissions for removable drives

Device Control allows you to specify the access permissions for removable drives, such as USB sticks and portable hard drives.

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. Select the access permissions under **Removable storage devices**:
   - Select **Allow write access** if you want to allow users to copy files to removable drives. If this is not selected, users will have read-only access to any allowed removable drives.
   - Select **Allow executables to run** if you want to allow users to run executable files, such as `.exe` or `.msi` files, that are located on a removable drive.
3. To add devices where executable files are allowed to run as exceptions, click **Configure removable storage devices where execute and write permissions are allowed**.

   **Note:** Exceptions are only applicable on version 15.00 and newer client applications.

   a) Click **Add** to include a new exception.
   b) Enter the hardware ID for the removable storage device that you want to add.
   c) Click **OK**.
   The new device is added to the table.

   On the devices listed in this table, end users can always run executable files and always have write access to files on the devices, regardless of the other settings for removable storage devices.

### Blocking hardware devices

You can block the access to devices with predefined rules.

By default, rules do not block any devices. To block devices, follow these instructions.

1. Go to the **Settings** tab and select **Windows** > **Device control**.
2. On the **Device access rules** table, select the row for the device that you want to block, and click **Edit**.
3. Set **Access Level** to **Blocked** to block the selected device.

**Note:** Some USB Wi-Fi adapters do not use the `USB\Class_E0 hardware` ID and need a custom rule to work with Device control.

### Granting access to specific devices

You can set rules to allow a specific device while all other devices of same class are blocked.

You need to know the hardware ID of the device that you want to allow before you can create a rule that grants full access to the device.

To add an exception to a rule, follow these instructions.

1. Get the hardware ID for the device that you want to allow.
   The hardware ID has to be more specific than the ID which is used to block the device.
2. Go to the **Settings** tab and select **Windows** > **Device control**.
3. On the **Device access rules** table, click **Add**.
4. Enter the hardware ID for the device as the **Hardware ID** in the new rule.
5. Set **Access Level** to **Full access** to allow the use of the device.
6. Set **Active** to **Yes** for the new rule.

### Finding hardware ID for a device

You can find the hardware ID of the device in multiple ways. You can use this ID with blocking rules.

Follow these instructions to find the hardware ID either with F-Secure Policy Manager or Windows Device Manager.

1. Select the target host.
2. Select the **Status** tab and select **Advanced view**.
3. Go to **F-Secure Device Control** > **Statistics** > **Devices** > **Devices**.
   Use **Hardware IDs**, **Compatible IDs** and **Device Class** columns to find the ID of the device that has been blocked.
   If you are not sure which ID is sufficiently unique to define a specific device:
   a) Go to **F-Secure Device Control** > **Settings** > **Report installed devices**.
   b) Set **Report installed devices** to **Yes**.
   c) Go to the **F-Secure Device Control** > **Statistics** > **Devices** > **Devices** table.
   d) Find the device that you want and compare the reported IDs.

   
   **Note:** You can right-click the table and select **Export table as text** to make it easier to compare them.
4. If you cannot find the ID using the statistics or the device has not been blocked yet, open Windows **Device Manager** in the client computer.
5. Find the device which ID you want to know in the list of devices.
6. Right-click the device and select **Properties**.
7. Go to **Details** tab.
8. Select one of the following IDs from the drop-down menu and write down its value:
   - Hardware IDs
   - Compatible IDs
   - Device class guid
   - Parent ID

   
   **Note:** For external storage devices, this is the only ID that includes the unique serial number of the device.

## 3.4.5 Managing software updates

You can manage and install software updates for the computers in your network.

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

You can configure Policy Manager to automatically install security updates to computers. You can also check the status of software updates and install missing software updates manually when needed.

**Note:** This feature does not support all managed products or versions. Check the release notes for your product to see if your current version is supported.

**Note:** Policy Manager only downloads and updates the Software Updater databases if you have hosts that have Software Updater installed.

## Installing software updates automatically

You can configure Policy Manager to automatically install security updates for software to computers in your network.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** › **Software Updater**.
3. Select **Enable Software Updater**.
4. Select how you want managed hosts to fetch the software updates next to **Download software updates from Policy Manager**.
   - **Always**: The managed hosts fetch the updates from Policy Manager Server or Proxy when they are available.
   - **If possible**: The managed hosts fetch the updates from Policy Manager Server or Proxy if they are available, otherwise they download the updates from the internet.
   - **Never**: The managed hosts always fetch the updates from the internet.
5. Under **Automatic installation**, select the security update categories and schedule that you want to use.

   You can exclude any software that you do not want Software Updater to update automatically. Under **Exclude software from automatic installation**, click **View** to see a list of the excluded programs.
6. Select **Run the task even if a scheduled start is missed** if you want the updates to be installed as soon as possible on hosts that are not available when the scheduled installation is run.
7. Select **Allow further installation of software updates before restarting** if you want to minimize the amount of restarts needed on managed hosts.
8. Click the following icon to distribute the policy:

## Excluding software updates from automatic installation

You can enter the name and bulletin ID for any software that you do not want Software Updater to update automatically.

Exclusion is based on the update installation status reported by managed hosts. When a host starts installing missing updates, it checks for any excluded updates and reports that they were not installed due to exclusion by the administrator. This also means that excluded updates do not immediately disappear from the list on the **Software updates** tab, because the hosts only report the installation status once they attempt to install the missing update.

In **Standard view**:

1. Select the target domain.
2. To manually enter the details for the software updates that you want to exclude:
   a) Go to the **Settings** tab and select **Windows** › **Software Updater**.
   b) Under **Exclude software from automatic installation**, click **Add**.
   c) Enter the details for the update that you want to exclude.

      You can enter both the name of the software and the bulletin ID for the specific update. The software name can include a product name and a service pack name. For example "windows sp3" will match all windows updates related to SP3. If you use the bulletin ID for excluding updates, only updates matching the exact bulletin ID will be excluded.

      You can also select a software vendor to exclude. If you select a vendor and do not enter any other details, all updates for that vendor's software are excluded.
3. To exclude a software update from the current list of available updates:
   a) On the **Software updates** page, right-click the update that you want to exclude.

b) Select **Exclude by Software** to use the update name given in the **Software** column or **Exclude by Bulletin ID** to use the bulletin ID.

**Note:** If you exclude an update by its software name, any other updates that use the same name are also excluded.

4. Click the following icon to distribute the policy:

Any updates for software matching the entered text, selected software name, or bulletin ID is now excluded from automatic installation. You can click **View** in the **Matching updates** column under **Exclude software from automatic installation** to see a list of the updates currently found for the entered software.

## Checking the status of software updates in your network

On the **Software updates** page, you can check the status of software updates in your network.

The **Software updates** page provides a list of updates for the software in use within your network. Each entry on the list includes the software in question, category, ID and description for the update, corresponding knowledge base (KB) number, as well as the update status if a single host is selected. If you select a domain or multiple hosts, you can click **View hosts** to see the update status. From this page, you can check which computers are missing selected updates, and also install the missing updates to those computers.

The **Status** column in the **Missing software update** view also shows you if you need to download the update package manually, or if the package has already been downloaded manually. These status links open the **Manual downloads** view.

**Tip:** You can also use the **Search missing updates** field on the **Software updates** page to find hosts that are missing an update. You can use any of the visible criteria for the update as a keyword for your search.

**Tip:** In **Advanced view**, you can turn off checking for missing service packs and updates that are not security-related.

## Installing missing software updates

You can install missing software updates manually.

To install the missing software updates:

1. Select the target domain.
2. On the **Software updates** page, select the updates that you want to install.
3. Click **Install**.
4. In the confirmation dialog, click **Yes**.
   The workstations will install the updates the next time they connect to Policy Manager Server.

You can also see the update status in Policy Manager Console.

## Configuring a third-party HTTP proxy for Software Updater

You can set up Software Updater to receive its updates through an external HTTP proxy.

As of version 12.20, Policy Manager works as a proxy for the software update packages by default, and the default cache size is set to 10 GB (you can configure this setting in Policy Manager Console). However, some organizations or network setups may require the use of a dedicated third-party proxy.

To configure the proxy and caching for Software Updater updates:

1. Install and configure the proxy of your choice.
   For example, with Squid, make the following configurations in `squid.conf`:
   a) Set the disk cache to 100 GB:
      ```
      cache_dir ufs /var/spool/squid 100000 16 256
      ```
   b) Set the maximum caching file size:
      ```
      maximum_object_size 2048 MB
      ```
   c) Configure the proxy to be used for software updates only (Software Updater is identified by its User-Agent name):

```
acl FSecSwUp browser F-SecureSoftwareUpdater
http_access allow FSecSwUp
http_access deny all
```

Once the caching proxy is up and running, it needs to be added to the Software Updater policy.

2. Configure the Software Updater policy in **Advanced view**:
   a) Set **F-Secure Software Updater** > **Settings** > **Communications** > **Use HTTP Proxy** to **User-defined**
   b) In **F-Secure Software Updater** > **Settings** > **Communications** > **User-defined proxy**, enter the address and port for the proxy (`http://<proxy_address>:<port_number>`).

## 3.4.6 Rapid Detection & Response

You can manage the distribution and basic operations of F-Secure Rapid Detection and Response sensors with Policy Manager.

**Note:** More advanced incident-related information and operations are available in the F-Secure Rapid Detection and Response portal. Click here to see the documentation for the portal.

F-Secure Rapid Detection and Response is a leading context-level endpoint detection and response (EDR) solution for companies.

Organizations can be breached in many ways. Increasingly, the attacks are fileless and do not require attackers to install malware on desktops or laptops. Advanced Persistent Threats (APT) and cyber threats are an extremely costly problem for companies. They are difficult to recognize just using traditional protection methods. Also, these attacks can be difficult to analyze and respond to. Defending against these attacks requires both the latest technological solutions and the expertise to analyze and understand the available data.

With its deep bi-directional intelligence and high level of automation, F-Secure Rapid Detection and Response protects against advanced threats even before breaches happen. It detects incidents with lightweight sensors, which are installed on monitored hosts in the organization. Sensors collect data on behavioral events, such as files being accessed, processes or network connections being created, or something being written into the registry or system log. These events are then further analyzed in the backend. The solution does not just to do real-time detections, but also makes detections based on applying new rules to old data.

Often targeted attacks could go unnoticed for months or even years. With F-Secure Rapid Detection and Response, you can prevent the attack from breaching critical servers through the targeted hosts.

### Activating endpoint sensors

Endpoint sensors are lightweight, discreet sensors, which are included in Client Security 14.10 and Server Security 14.00 and newer. These sensors collect behavioral data from endpoint devices and are specifically designed to withstand a wide range of attacks.

You need an activation keycode for registering the Rapid Detection and Response (RDR) sensors. Contact your F-Secure partner to get your RDR for Business Suite keycode.

In **Standard view**:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Rapid Detection & Response**.
3. Enter your sensor activation keycode for the corresponding host type (workstations or servers).
4. Select **Enable Rapid Detection & Response**.
5. Click the following icon to distribute the policy:

### Checking the status of endpoint sensors

You can see the status of deployed Rapid Detection and Response endpoint sensors on the **Status** tab.

Policy Manager shows you the connection status of the sensors as well as any errors related to activation, for example if the subscription is not valid or has expired.

To check the status of endpoint senors:

Select the **Status** tab and go to the **Rapid Detection & Response** page.
This page shows you basic information on the endpoint sensors in your managed network.

More details and operations are available in the Rapid Detection & Response portal. The **Status** > **Rapid Detection & Response** page in Policy Manager has a link that opens the portal in your web browser. You will receive access credentials for the portal in connection with your sensor activation keycodes.

## Isolating hosts from the network

You can isolate one or more hosts from the network.

**Note:** Use network isolation with caution and only in case of a network attack.

To isolate a host from the network:

1. Select the target host in the policy domain tree.
2. Go to the **Operations** tab.
3. Click **Isolate** under **Network isolation**.
   This isolates the selected host from the network.
4. To reconnect an isolated host to the network, click **Release** on the **Operations** tab.

Isolated hosts are shown on the **Host issues** section of the dashboard.

## Unregistering endpoint sensors

You can unregister endpoint sensors if needed.

To unregister an endpoint sensor:

1. Select the target domain.
2. Go to the **Settings** tab and select **Windows** > **Rapid Detection & Response**.
3. Delete the keycode for the corresponding host.
4. Uncheck **Enable Rapid Detection & Response**.
5. Click the following icon to distribute the policy:

Chapter

4

# Administration with Web Console

**Topics:**



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

The product uses Windows-based authorization for the Web Console to increase the security of the process. For this reason, you need to start the browser with administrator rights.

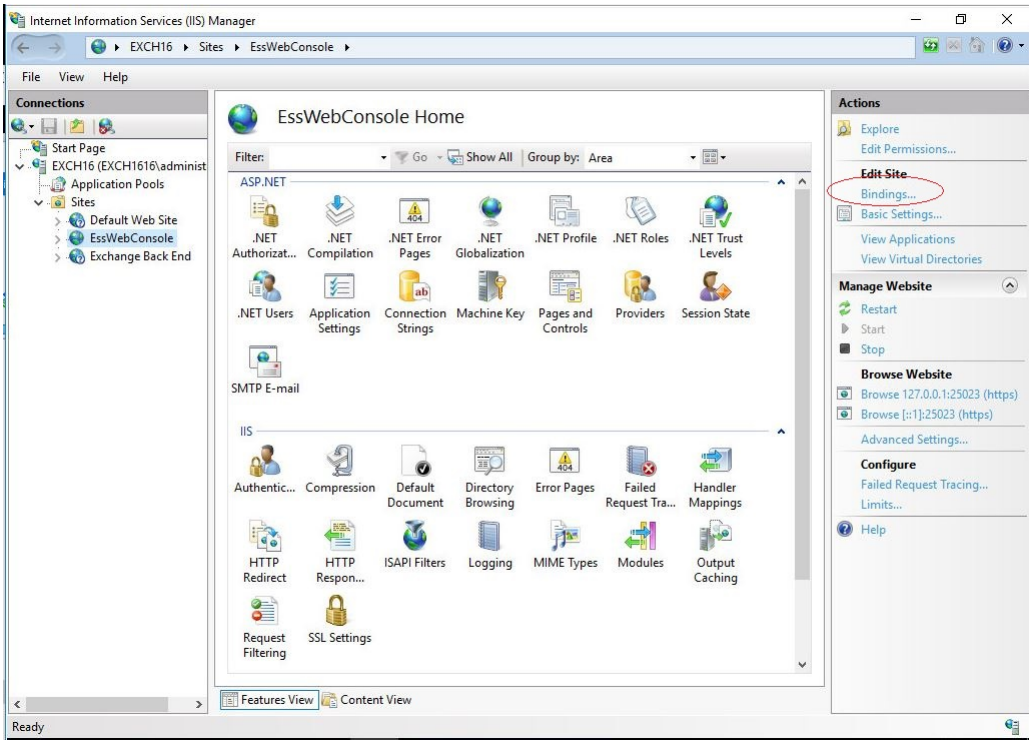
**Note:** After you edit the product settings, Web Console shows an **Unsaved changes** popup at the bottom of the page. Click **Save and apply** before you close Web Console to apply the changes that you have made.

## 4.1 Allowing hosts to access the web console

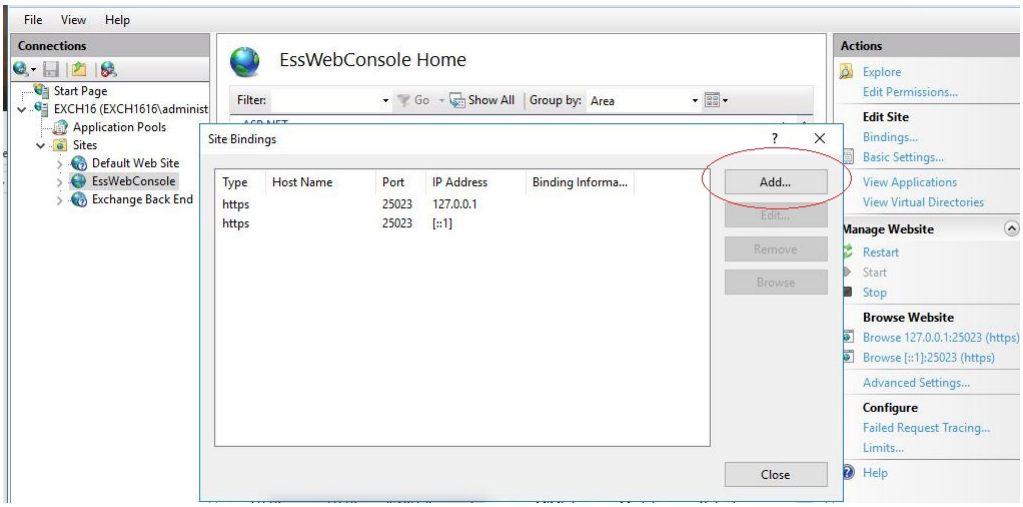
To access the web console from other hosts in the network, you need to allow them via Internet Information Services (IIS).

To allow access to the web console for all hosts:

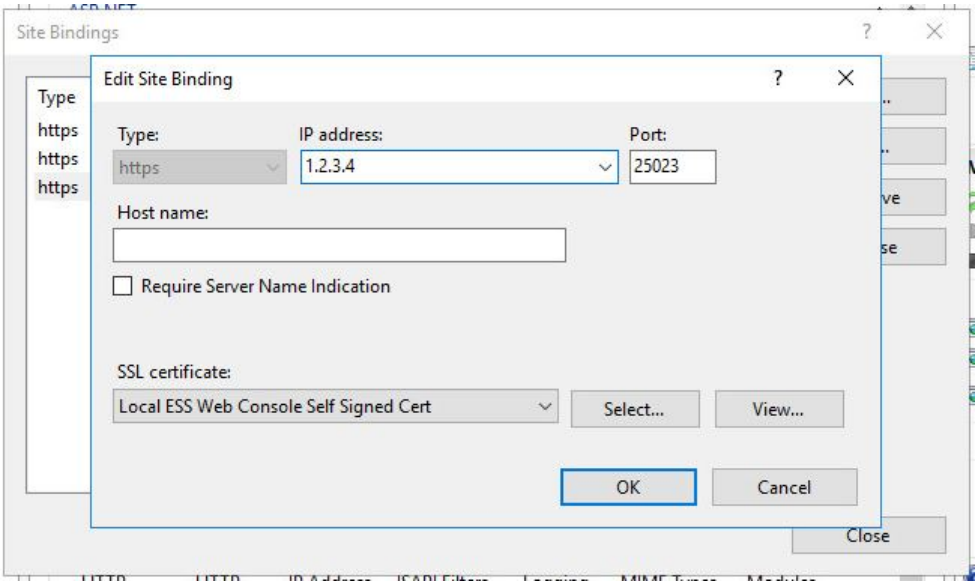
1. In **Administrative Tools**, start **Internet Information Services (IIS) Manager**.
2. Go to **Sites** > **EssWebConsole**.
3. Select **Bindings**.




4. Click **Add**.



5. Select **https** as the **Type**, enter the **IP address** for the server, and set the **Port** to 25023.




6. Select the **SSL certificate**, then click **OK**.

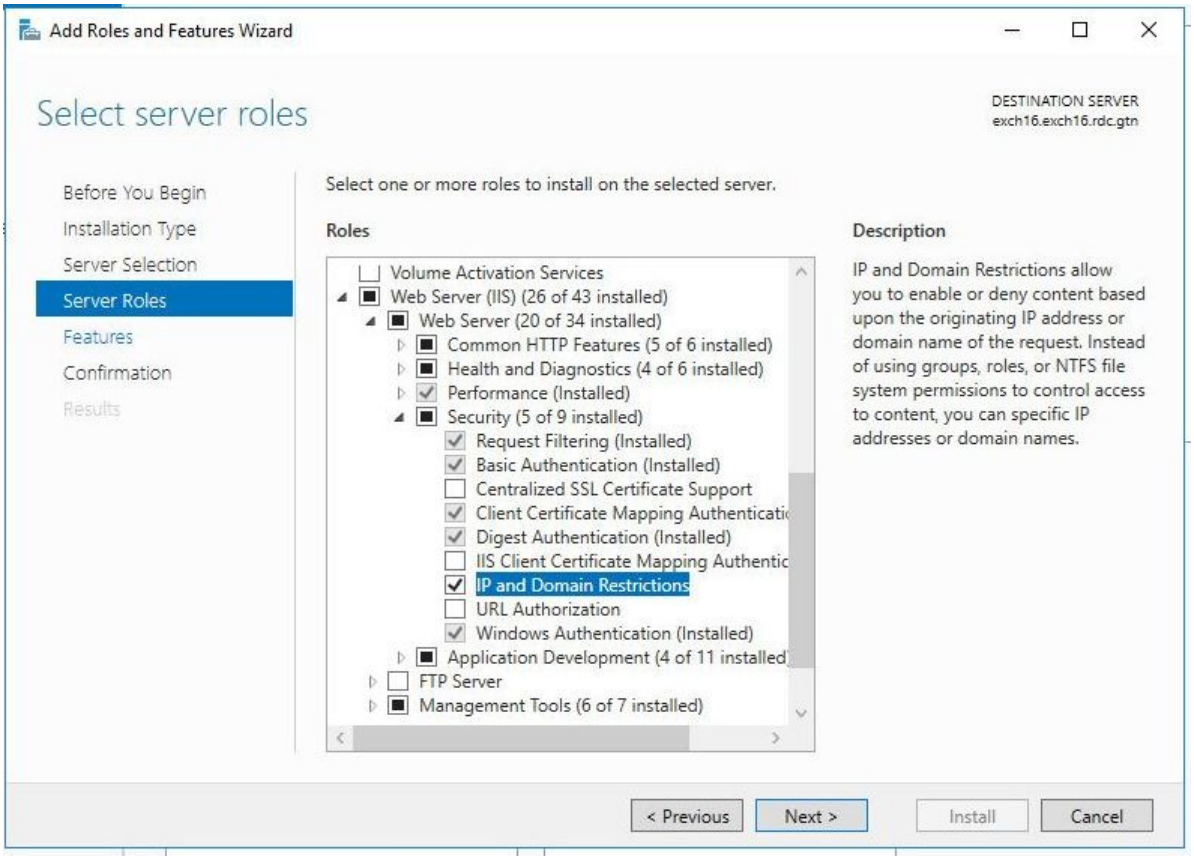
   **Note:** SSL 2.0 certificates are not supported due to vulnerabilities.

## 4.2 Restricting website access to specific IP addresses

After allowing access to the web console from other hosts in your network, you may want to restrict the access to a specific IP address or IP range.

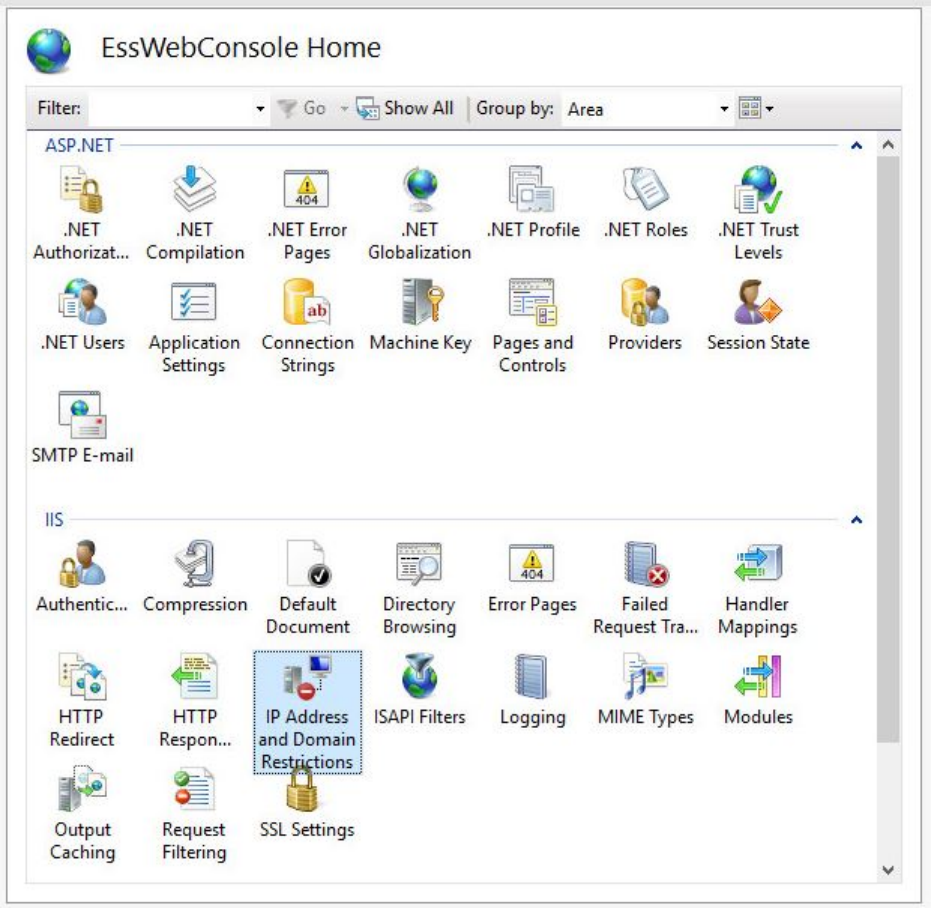
To allow only specific hosts to access the web console:

1. Make sure that the **IP and Domain Restrictions** feature is installed for Internet Information Services (IIS).



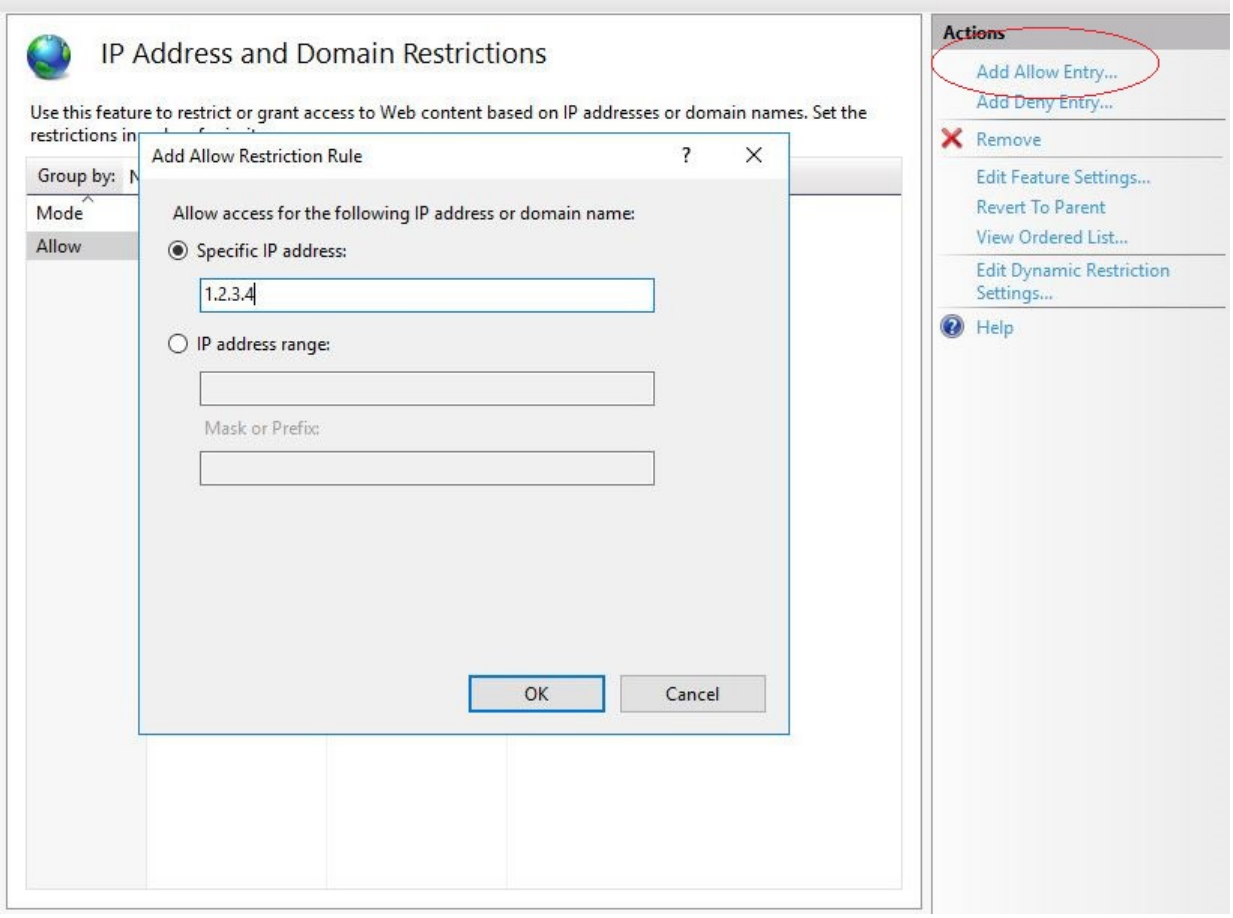

2. Go to **Sites** > **EssWebConsole**.

3. Open **IP and Domain Restrictions**.




4. Select **Add Allow Entry**.

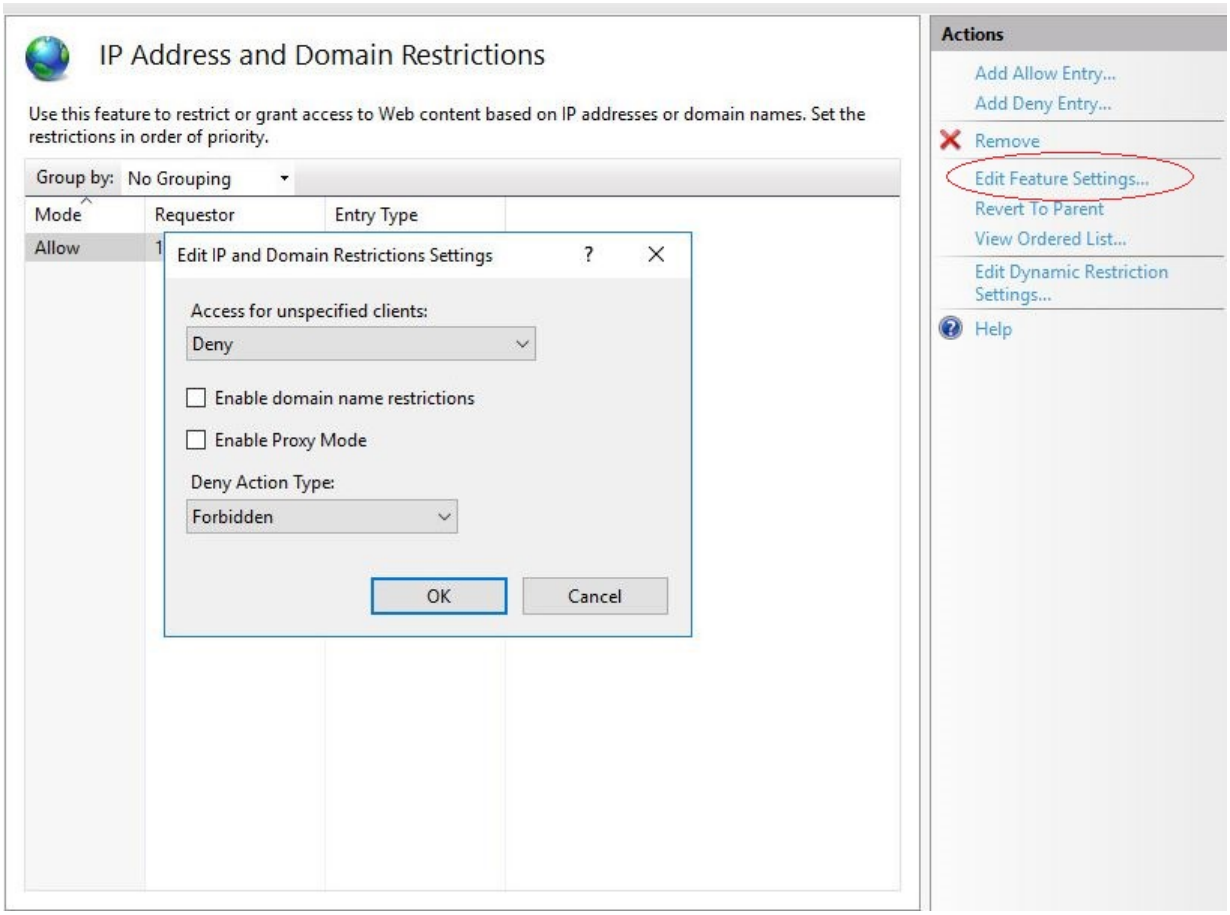
5. Enter the IP address or IP range.




**Note:** Make sure that you add the local IP address if you need to open the web console locally.

6. Click **OK**.
7. Select **Edit feature settings**.

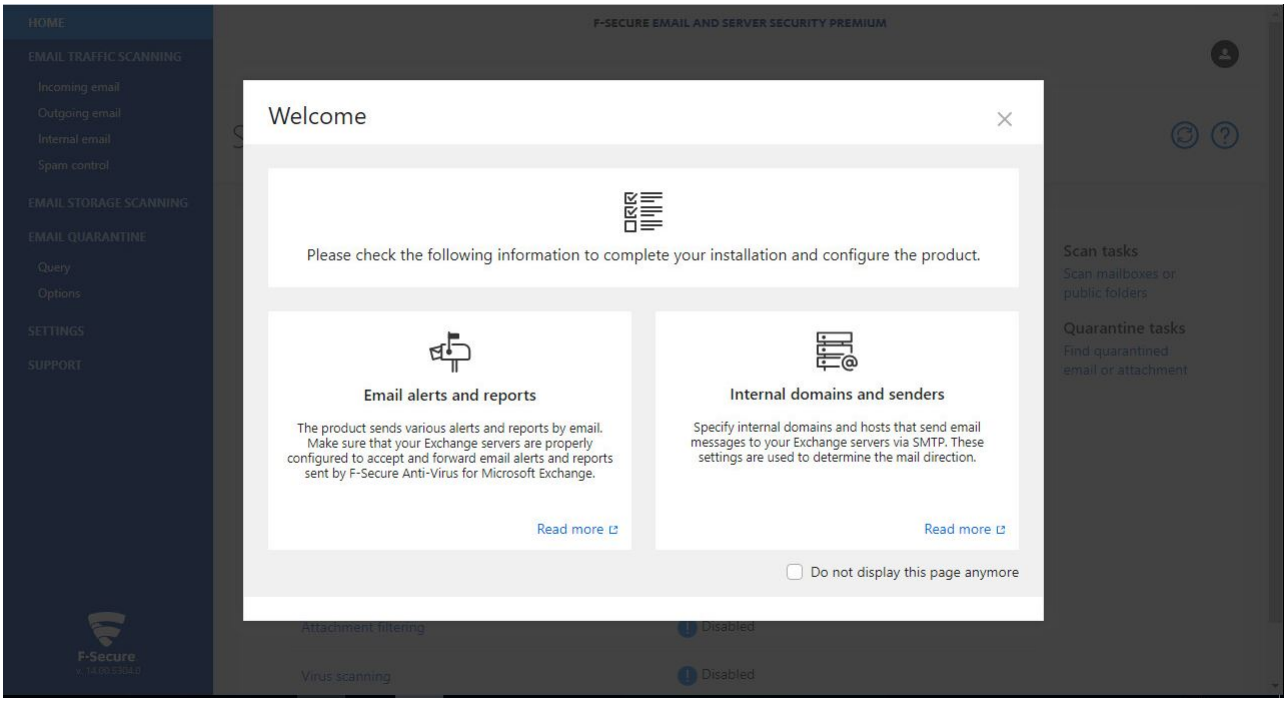
8. Set **Access for unspecified clients** to **Deny**.




9. Click **OK**.
10. Restart the **EssWebConsole** site.

## 4.3 Home

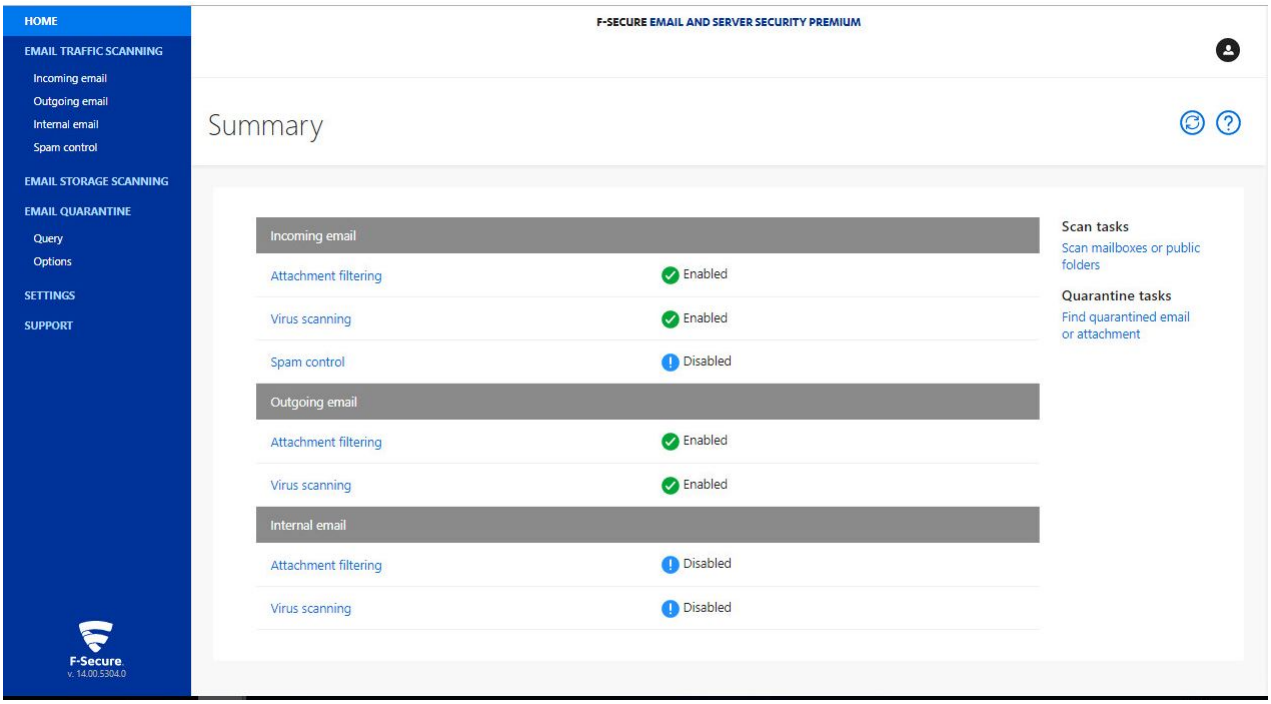
When you log in for the first time, the Web Console displays **Welcome** page.



The **Welcome** page lists items that you should check and configure to complete your installation.

## 4.3.1 Summary

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




| | |
|---|---|
| | **Normal**; the feature is enabled and everything is working as it should. |
| | **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. |

### Scan tasks

Click **Scan mailboxes or public folders** to manually scan mailboxes and public folders for viruses and strip attachments in them. For instructions, see Email storage scanning on page 96 .

### Quarantine tasks

Click **Find quarantined email or attachment** to search for the quarantined messages and attachments.

## 4.4 Email traffic scanning

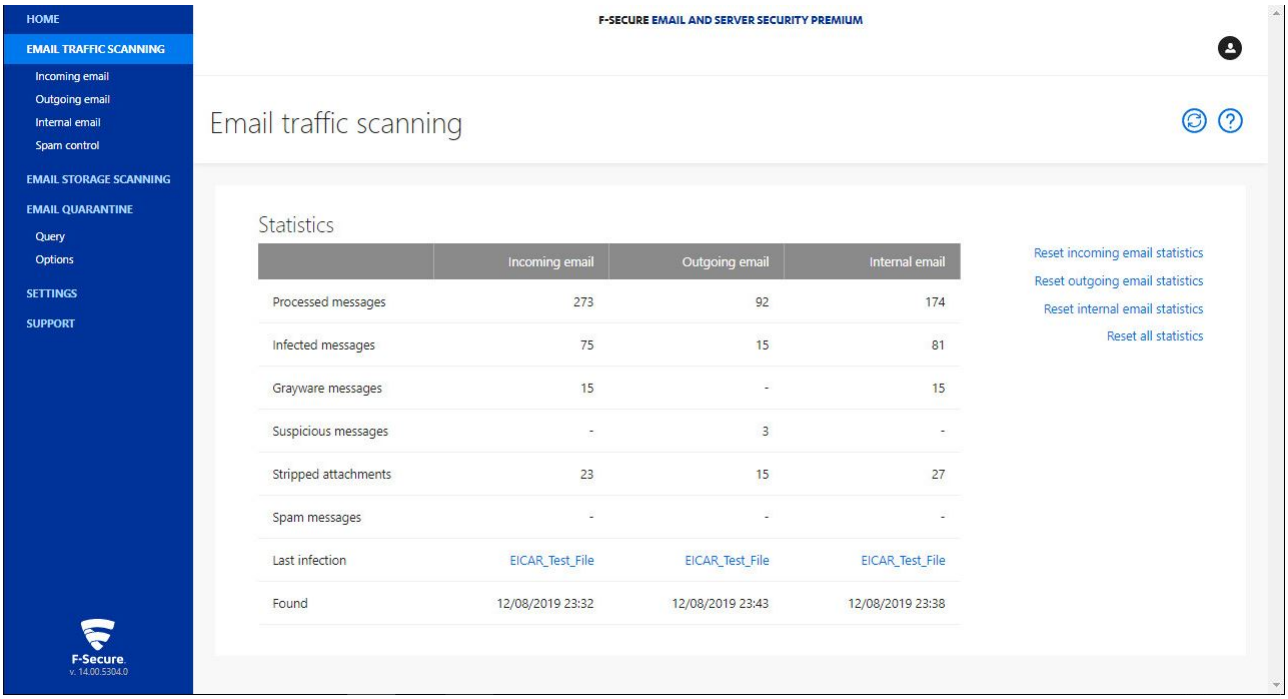
With Email traffic scanning, you can protect the email traffic from malicious code on the transport level.

You can configure incoming, outgoing, and internal message protection separately. For more information about the mail direction and configuration options, see General settings on page 27 .

**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.

### Statistics




The **Email traffic scanning** page displays a summary of the processed incoming, outgoing and internal mail messages:

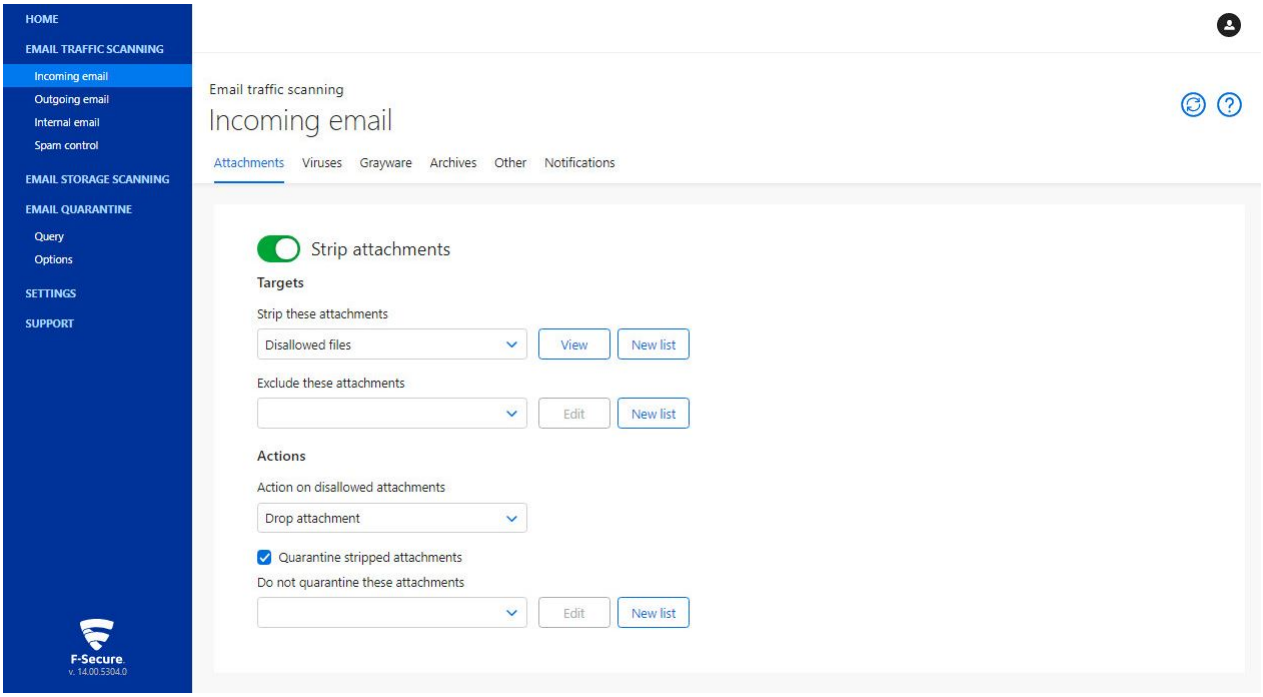
| | |
|---|---|
| **Processed messages** | Displays the total number of processed messages since the last reset of statistics. |
| **Infected messages** | Displays the number of messages with attachments that are infected and cannot be automatically disinfected. |
| **Grayware messages** | Displays the number of messages that have grayware items, including spyware, adware, dialers, joke applications, 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. |

| | |
|---|---|
| **Spam messages** | Displays the number of messages that are classified as spam. |
| **Last Infection** | Displays the name of the last infection found in incoming, outgoing, or internal messages |
| **Found** | Displays the date when the last infection was detected. |

**Note:** You can use Reset statistics links to reset either incoming, outgoing, internal, or all email statistics.

## 4.4.1 Attachments

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

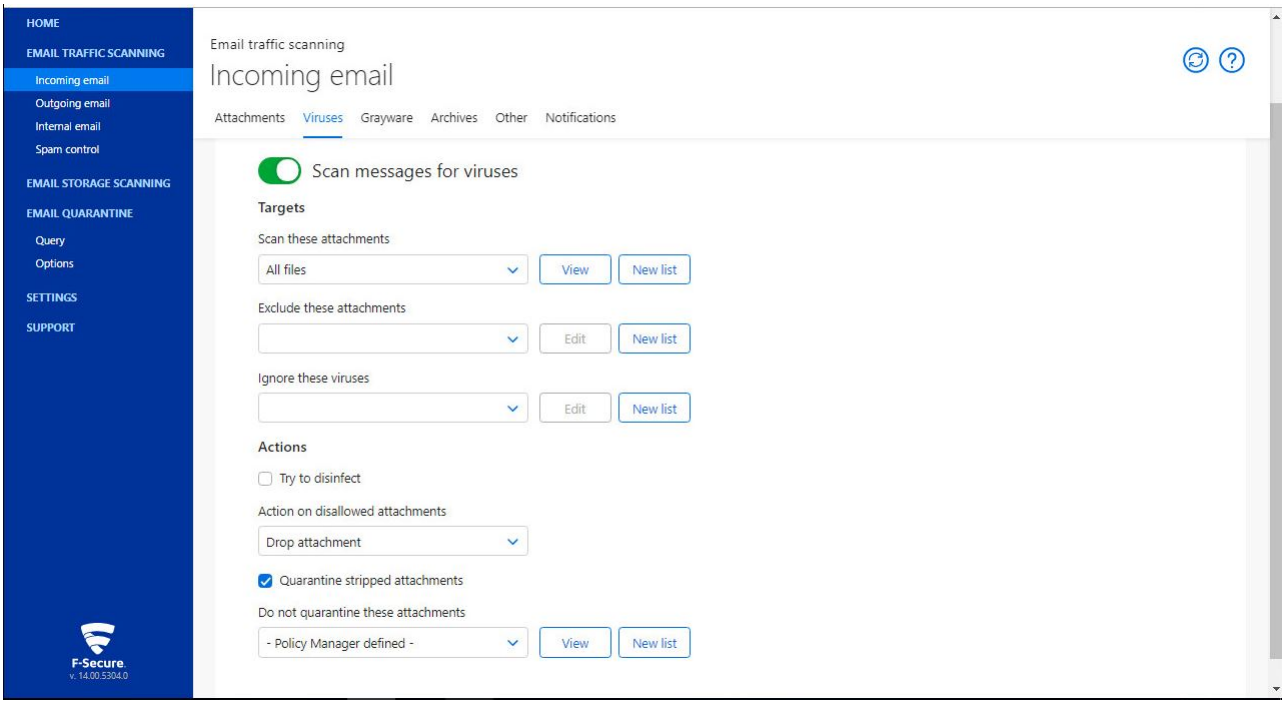



| | |
|---|---|
| **Strip attachments** | Enable or disable the attachment stripping. |
| Targets | |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see Lists on page 121 . |
| **Exclude these attachments** | Specify attachments that are not 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.<br>**Drop Attachment** - Remove the attachment from the message and deliver the message to the recipient without the disallowed attachment.<br>**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 Lists on page 121 . |

## 4.4.2 Viruses

Specify incoming, outgoing and internal email messages and attachments that should be scanned for malicious code.




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

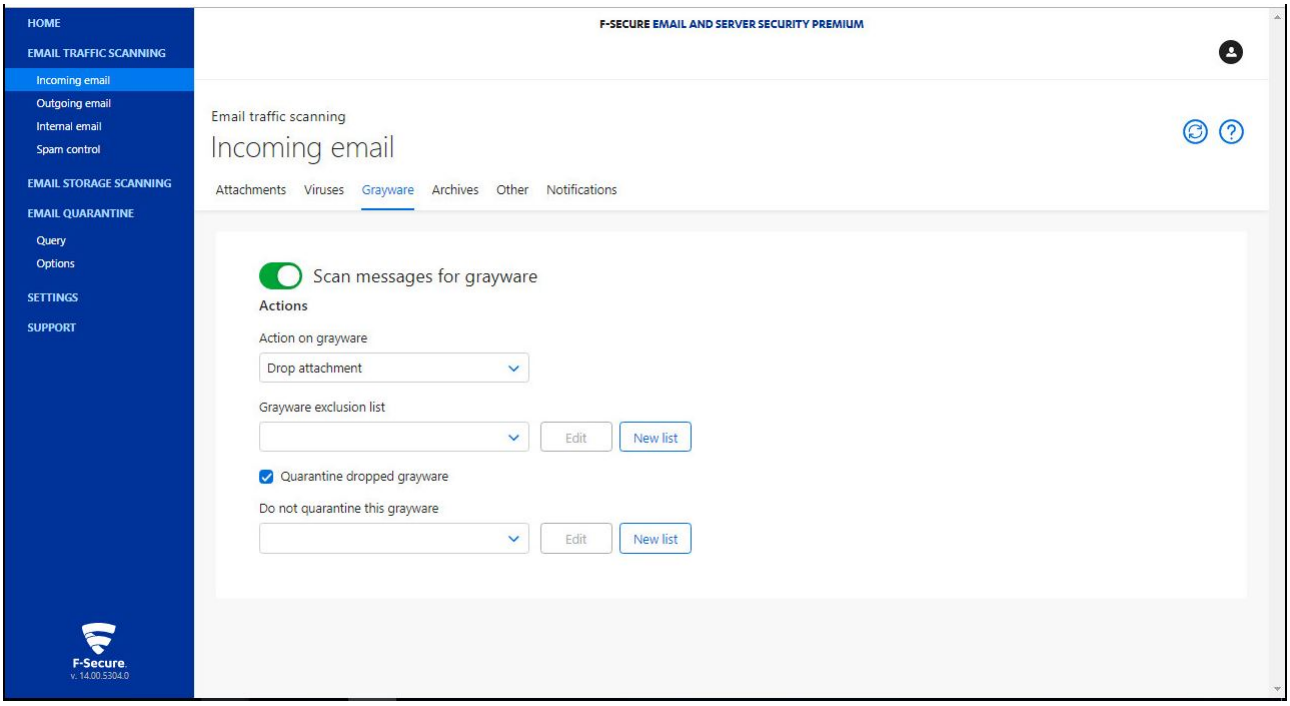
| | |
|---|---|
| **Scan messages for viruses** | Enable or disable the virus scan. The virus scan scans messages for viruses and other malicious code. |
| Targets | |
| **Scan these attachments** | Specify attachments that are scanned for viruses. For more information, see Lists on page 121 . |
| **Exclude 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.<br><br>**Note:** Disinfection may affect the product performance.<br><br>**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.<br><br>**Drop attachment** - Remove the infected attachment from the message and deliver the message to the recipient without the attachment.<br><br>**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 Lists on page 121 . |

## 4.4.3 Grayware

Specify how the product processes grayware items in incoming, outgoing and internal messages.



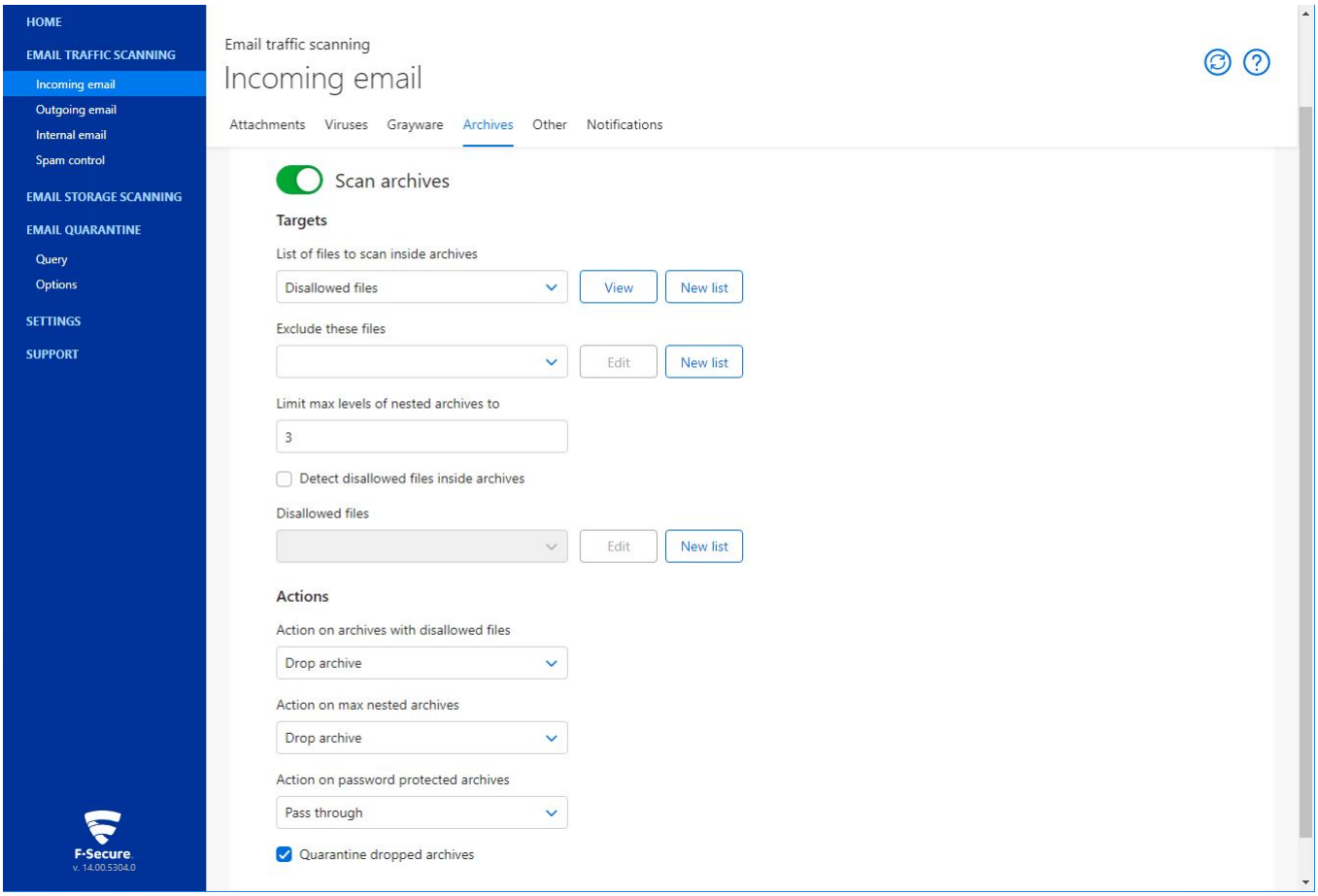
Note that grayware scanning increases the scanning overhead. By default, grayware scanning is enabled for incoming messages only.

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

| | |
|---|---|
| **Scan messages for grayware** | Enable or disable the grayware scan. |
| Actions | |
| **Action on grayware** | Specify the action to take on items which contain grayware.<br>**Pass through** - Leave grayware items in the message.<br>**Drop attachment** - Remove grayware items from the message.<br>**Drop the whole message** - Do not deliver the message to the recipient. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **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 Lists on page 121 . |

## 4.4.4 Archives

Specify how F-Secure Anti-Virus processes the product processes archived attachments in incoming, outgoing, and internal messages.




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 Lists on page 121 . |
| **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 turned on. |
| **Detect disallowed files inside archives** | Specify files which are not allowed inside archives. For more information, see Lists on page 121 . |

Actions

| | |
|---|---|
| **Action on archives with disallowed files** | Specify the action to take on archives which contain disallowed files.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - Remove the archive from the message and deliver the message to the recipient without it.<br>**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.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - Remove the archive from the message and deliver the message to the recipient without it.<br>**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.<br>**Pass through** - Deliver the message with the password protected archive to the recipient.<br>**Drop attachment** - Remove the password protected archive from the message and deliver the message to the recipient without it.<br>**Drop the whole message** - Do not deliver the message to the recipient.<br>The default values are **Drop archive** for incoming mail, **Drop the whole message** for outgoing mail, and **Pass through** for internal mail. |
| **Quarantine dropped archives** | Specify whether archives that are not delivered to recipients are quarantined. |

## 4.4.5 Unsafe URLs

Specify how the product handles unsafe URLs that are detected in the message body.

| | |
|---|---|
| **Scan messages for unsafe URLs** | Switch on to check all URLs found in the message body. |

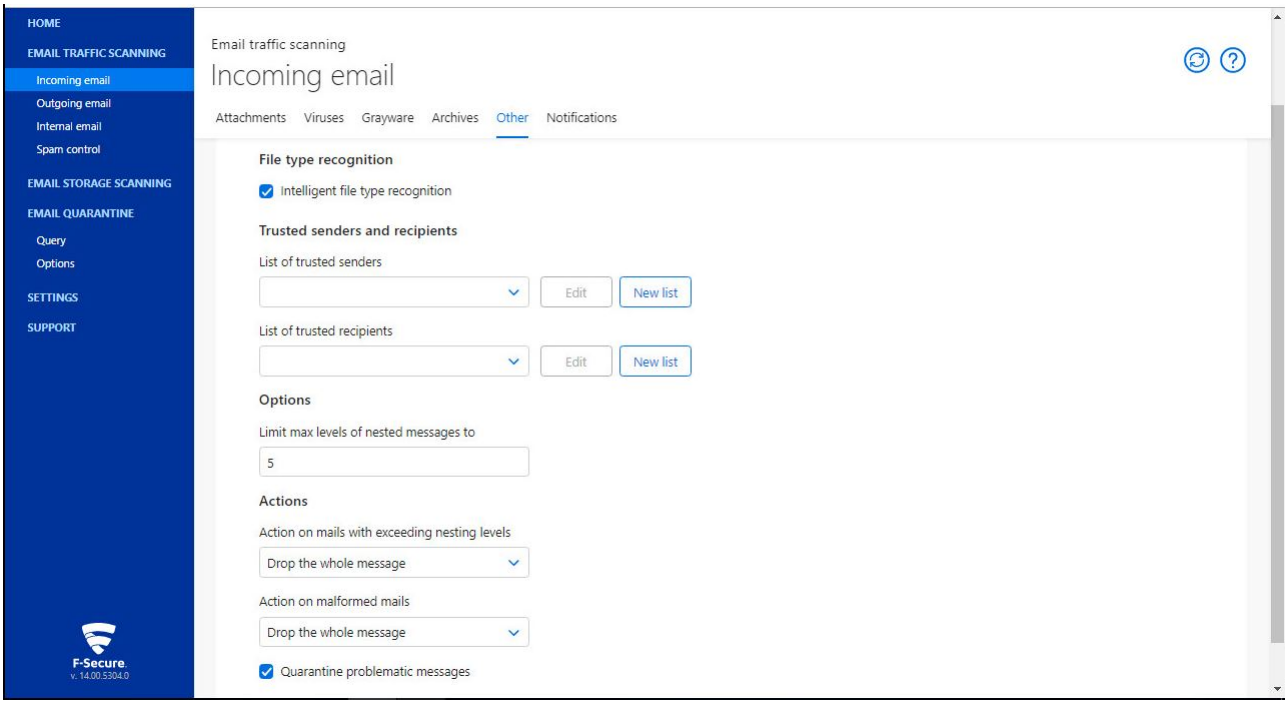
| | |
|---|---|
| **Action on unsafe URLs** | Select how you want to handle messages that contain unsafe URLs:<br>**Drop the whole message** - Do not deliver the message to the recipient.<br>**Pass through** - The product allows the message to pass through. |
| **Quarantine dropped messages** | Select this if you have selected **Drop the whole message** as the action for handling unsafe URLs and you want to move those messages to the quarantine instead of deleting them. |

You can also specify allowed and denied URLs. You can allow false positives, that is, you can allow web sites that are incorrectly detected as having vulnerabilities. Alternatively, you can deny web sites that are considered safe.

| | |
|---|---|
| **Allowed URLs** | Select an existing list from the drop-down menu, select **Edit** to edit a current list or select **Add list** to create a new list of URLs that are allowed in the body of an email message. The email is allowed to pass through. |
| **Denied URLs** | Select an existing list from the drop-down menu, select **Edit** to edit a current list, or select **Add list** to create a new list of URLs that are not allowed in the body of an email message. The email is either dropped or quarantined. |

## 4.4.6 Other

Configure other options to limit actions on malformed and problematic messages.




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.

**FTR exclusions**

Enter any file extensions that you do not want intelligent file type recognition to process.

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 Lists on page 121 .

Options

**Limit max levels of nested messages to**

Specify how many levels deep to scan in nested email messages. A nested email message is a message that includes one or more email 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 emails. 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.

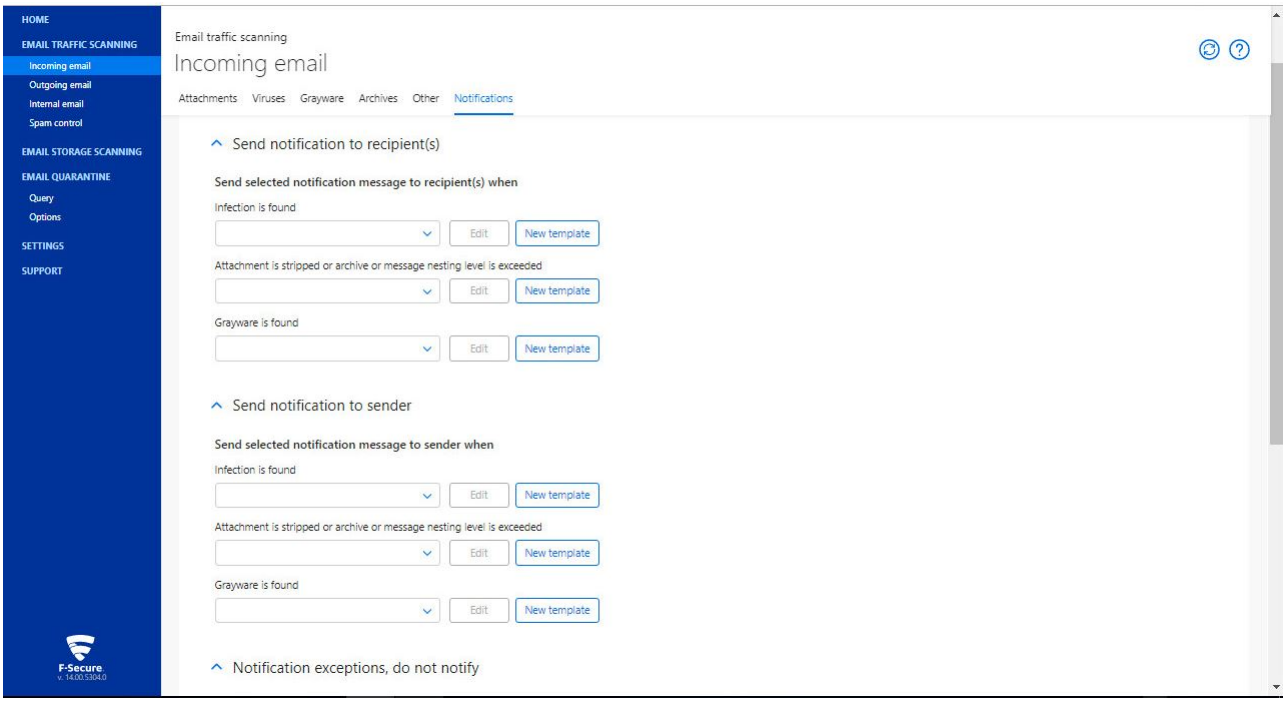
**Pass through and report** - The product allows the message to pass through, but sends a report to the administrator.

**Quarantine problematic messages**

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

## 4.4.7 Notifications

Specify whether and when the product sends notifications and alerts.




### Send notifications to recipients and senders

**Send notification to recipient(s) when**

Specify whether recipients are notified when an infection is found; an attachment is stripped or archive or message nesting level is exceeded; when a grayware item is found; when an unsafe URL is detected; or when a password-protected archive is found.

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

| | |
|---|---|
| **Send notification to sender when** | Specify whether senders are notified when an infection is found; an attachment is stripped or archive or message nesting level is exceeded; when a grayware item is found; when an unsafe URL is detected; or when a password-protected archive is found.<br><br>To enable the notification, select a template for the notification message. To disable the notification, leave the notification field empty.<br><br>**Note:** For more information, see "Message Templates". |
| **Notification exceptions, do not notify** | Specify infections, attachments, archive or message nesting levels, or a grayware item that do not generate notifications. When the product finds specified file or file extension, no notification is sent. |
| **These infections:**<br><br>**These attachments or archive/message nesting levels:**<br><br>**This grayware:** | Specify infections, attachments, or grayware types that do not generate notifications.<br><br>When the product finds the specified infection, file or file extension, or grayware item, no notification is sent. |

Select **Edit** to edit an existing notification template. To create a new notification template, select **New template**, then specify its name, the subject line and the text of the notification message.

### Send alerts to administrators

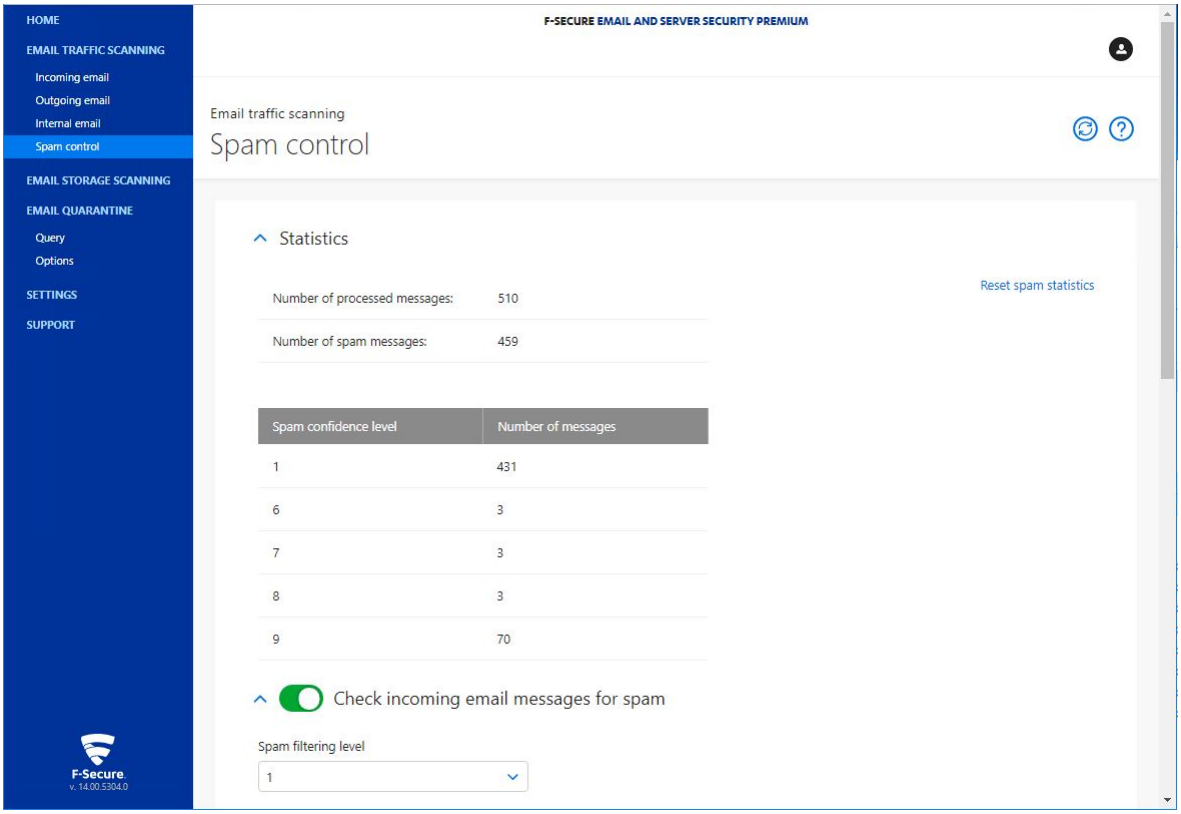
| | |
|---|---|
| **Send alert to administrator when** | Specify whether the administrator is notified when an infection or grayware item is found, when an attachment is stripped, when an archive or message nesting level is exceeded, or when an unsafe URL is detected. |

## 4.4.8 Spam control

Spam control identifies spam and phishing patterns from the message envelope, headers, and message body during the first minutes of the new spam or phishing outbreak.

**Note:** You can configure Spam Control settings for incoming messages only if you have F-Secure Spam Control installed.

## Statistics

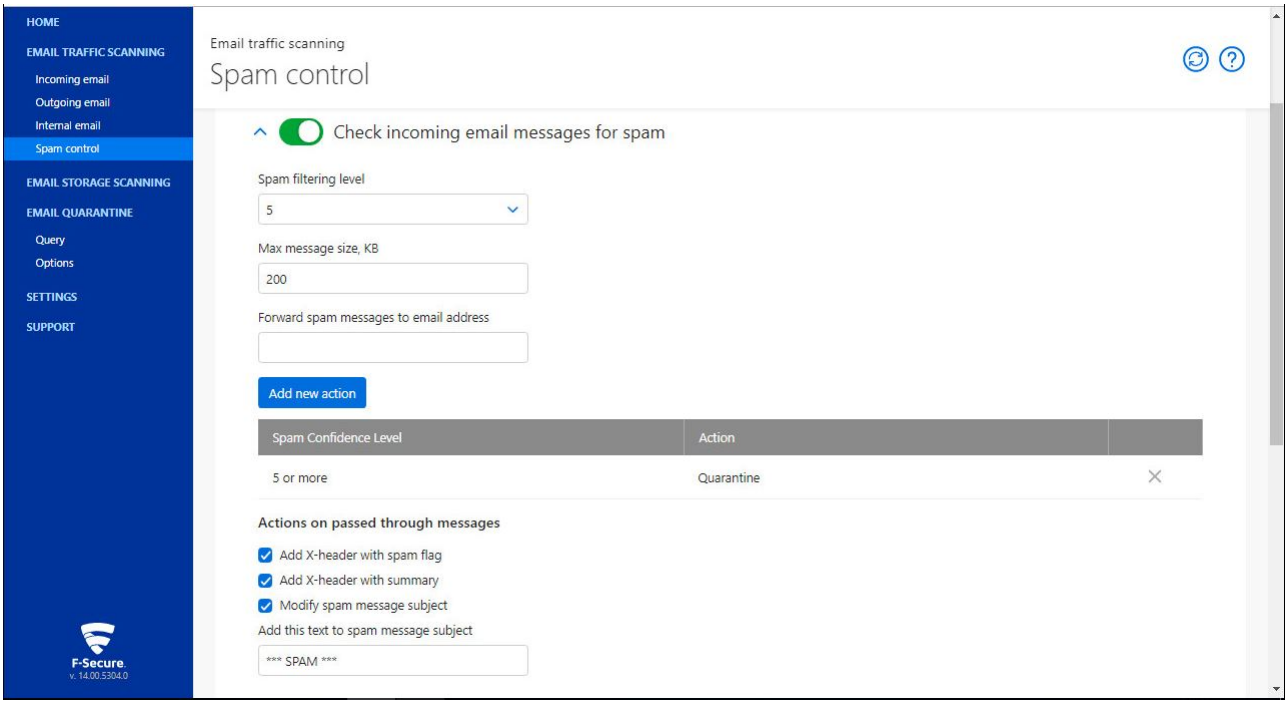



The **Statistics** page displays the statistics of the spam scanner:

| | |
|---|---|
| **Number of processed messages** | Displays the total number of processed messages since the last reset of statistics. |
| **Number of spam messages** | Displays the total number of spam messages found since the last reset of statistics. |
| **Spam confidence level / number of messages** | Displays the number of messages found with specified spam confidence levels. |

**Note:** You can use the **Reset spam statistics** link to reset all spam statistics.

## Check incoming email messages for spam




Specify how the product processes inbound spam messages.

| | |
|---|---|
| **Check incoming email messages for spam** | Turn spam checking on or off. |
| **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 email messages are falsely identified as spam.<br><br>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.<br><br>The allowed values are from 0 to 9. |
| **Max message size, KB** | 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 email address** | Specify the email 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 email 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.<br><br>**Note:** The product checks the sender address from the SMTP message envelope, not from the message headers. |
| **List of blocked recipients** | Specify blocked recipients. Messages sent to the specified addresses are always treated as spam. |

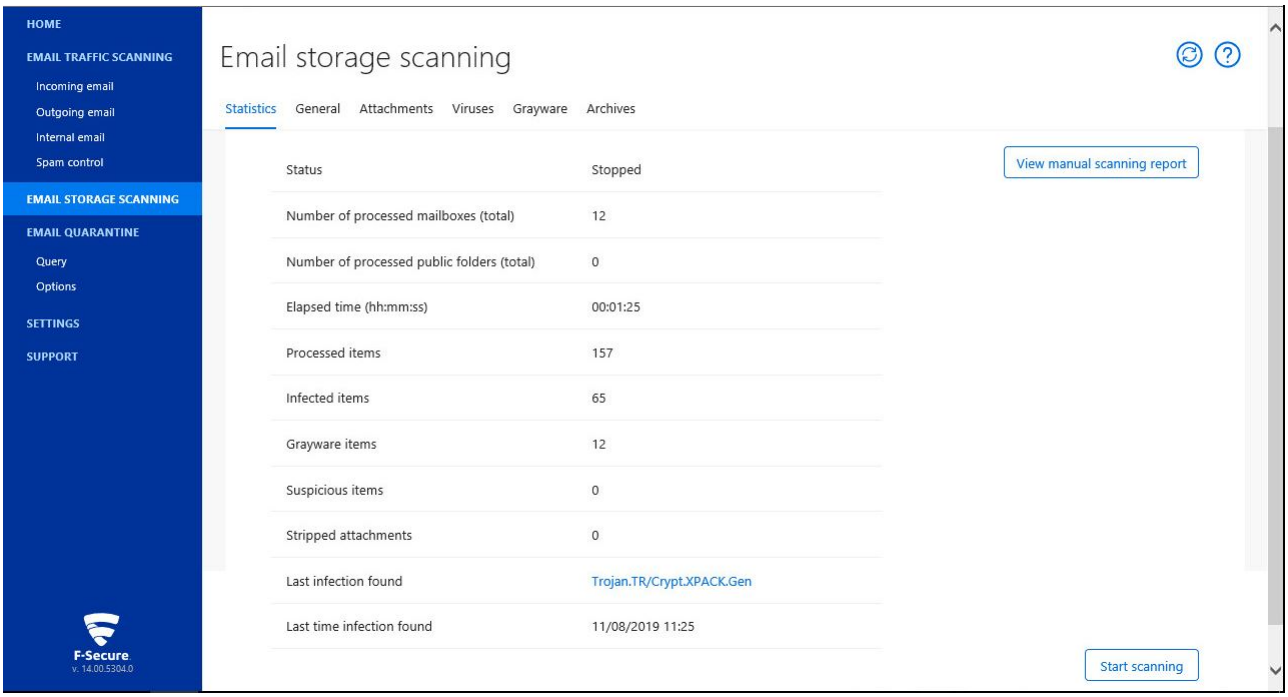
## 4.5 Email storage scanning

Configure Email storage scanning settings to specify how email 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.

You can scan mailboxes and public folders for viruses and strip attachments manually at any time.

### Statistics




The **Statistics** page displays a summary of the messages processed during the latest manual email storage scan:

| | |
|---|---|
| **Status** | Displays whether the manual scan is running or stopped. |
| **Number of processed mailboxes (total)** | 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 (total)** | Displays the number of public folders that have been scanned and the total number that will be scanned when the manual scan is complete. |

| | |
|---|---|
| **Elapsed time (hh:mm)** | 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 applications, 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. |

### Tasks

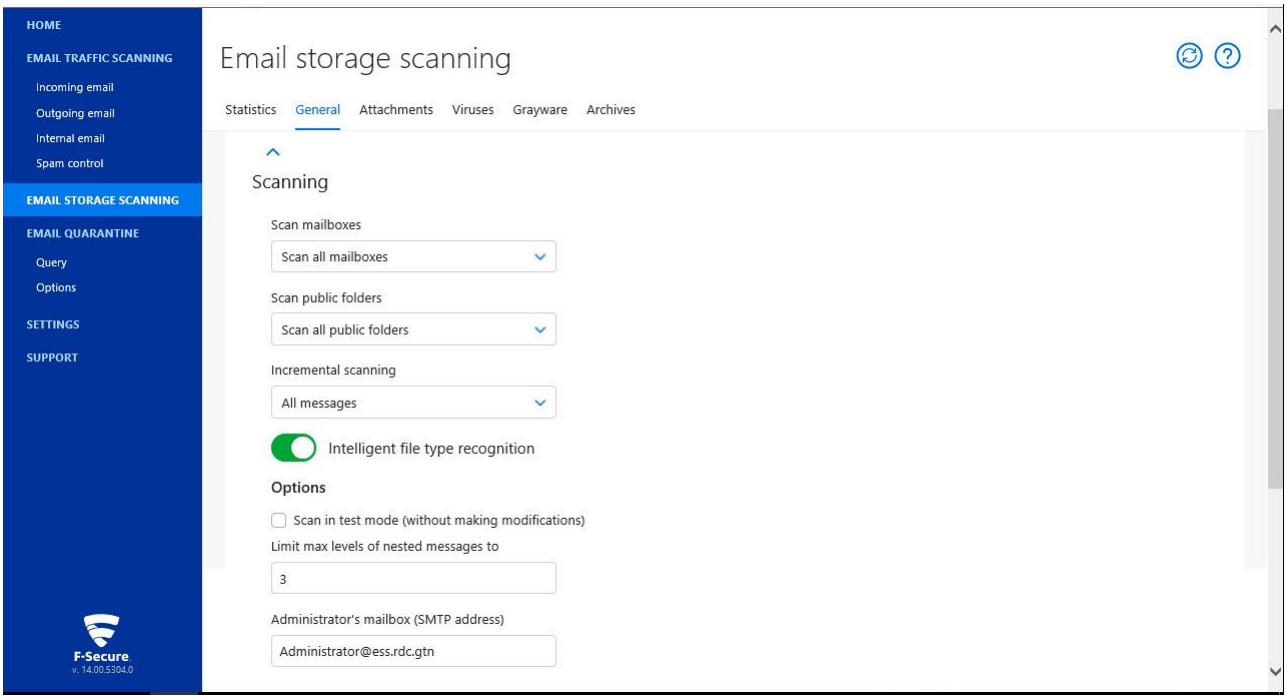
Click **Start scanning** to start the manual scan.

Click **Stop scanning** to stop the manual scan.

Click **View manual scanning report** to view the latest manual scan report.

## 4.5.1 General

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



Scanning

**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 public 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.

**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.

**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.

**FTR exclusions**

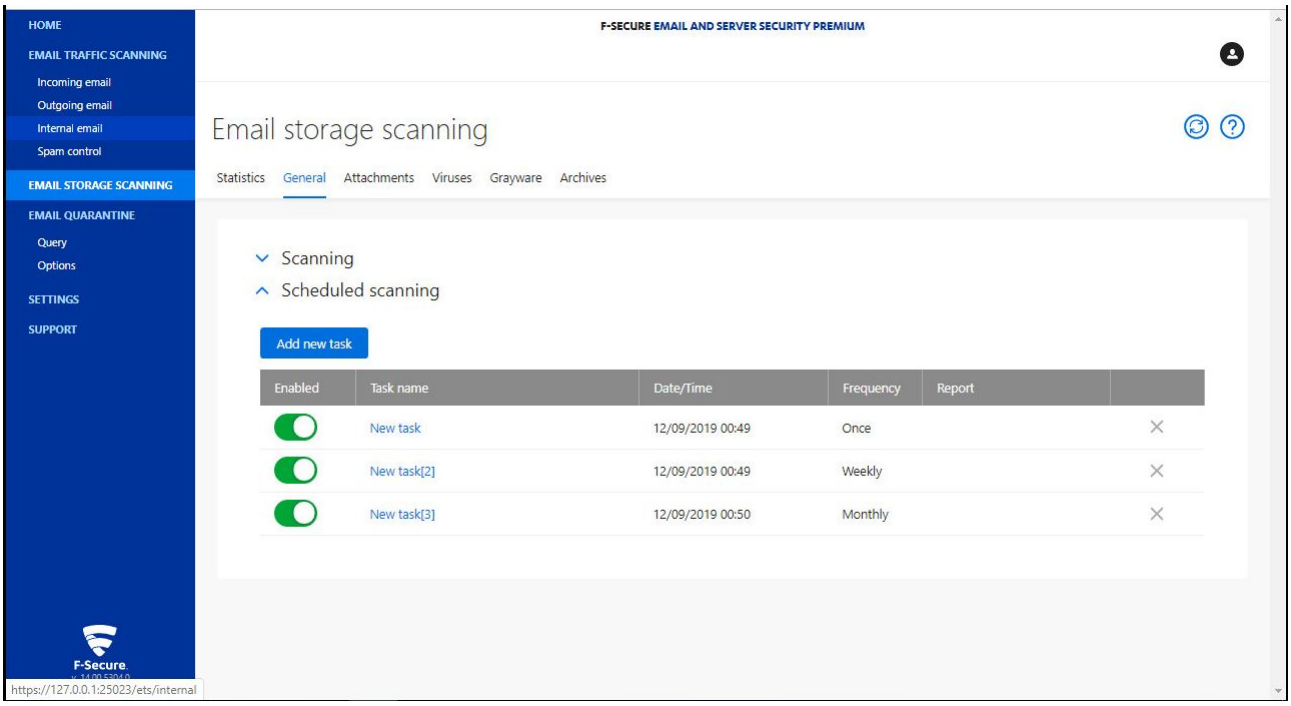
Enter any file extensions that you do not want intelligent file type recognition to process.

Options

| | |
|---|---|
| **Scan in test mode (without making modifications)** | Select whether you want to scan in test mode.<br><br>**Tip:** Run the manual scan in the test mode and check the scanning report to see how messages and attachments would be processed based on your current settings. |
| **Limit max levels of nested messages to** | Specify how many levels deep to scan in nested email messages. A nested email message is a message that includes one or more email messages as attachments. If zero (0) is specified, the maximum nesting level is not limited. |
| **Administrator's mailbox (SMTP address)** | 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. |

## Scheduled scanning

Under **Scheduled scanning**, the **Task name** list displays the scheduled tasks that scan email storage and date and time when they occur for the next time.



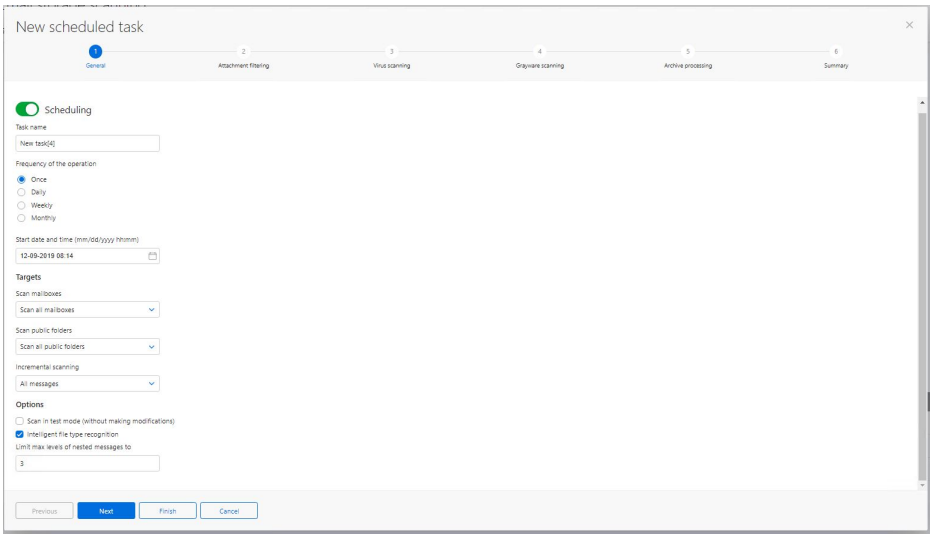

Click **Add new task** to create a new scheduled operation.

Click the scheduled task name to edit it or the **X** icon to completely remove it.

Click **View report** in the scheduled tasks table to see the latest scheduled task results.

## Specify scanning task name and schedule

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




**Scheduling** switch

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 date and time**

Enter the date and time for starting the task in `mm/dd/yyyy hh:mm` format.

You can also click the field to select the date and time from a calendar widget.

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 public 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.

**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

**Scan in test mode (without making modifications)**

Select whether you want to scan in test mode.

**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.

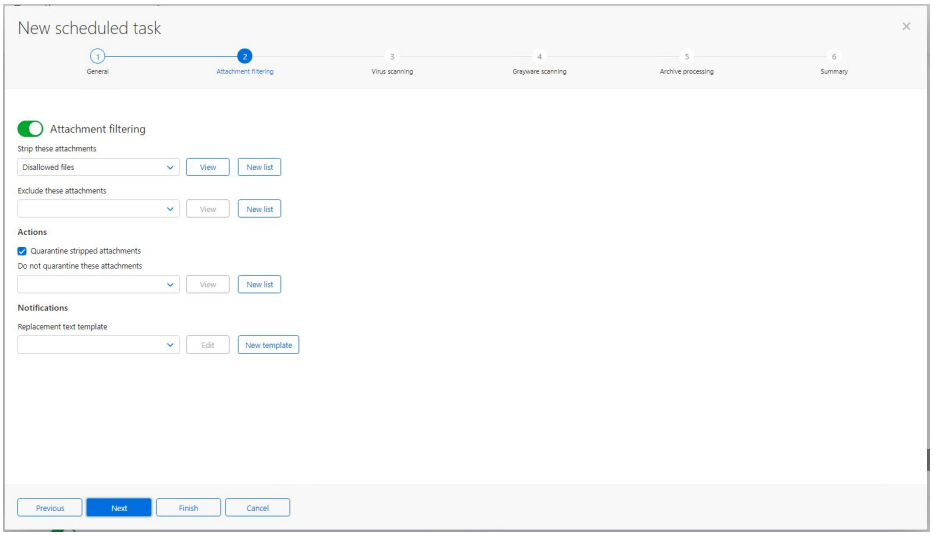
**FTR exclusions**

Enter any file extensions that you do not want intelligent file type recognition to process.

| | |
|---|---|
| **Limit max levels of nested messages to** | Specify how many levels deep to scan in nested email messages. A nested email message is a message that includes one or more email messages as attachments. If zero (0) is specified, the maximum nesting level is not limited.<br><br>**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. |

## Specify attachment filtering options

Choose settings for stripping attachments during the scheduled operation.



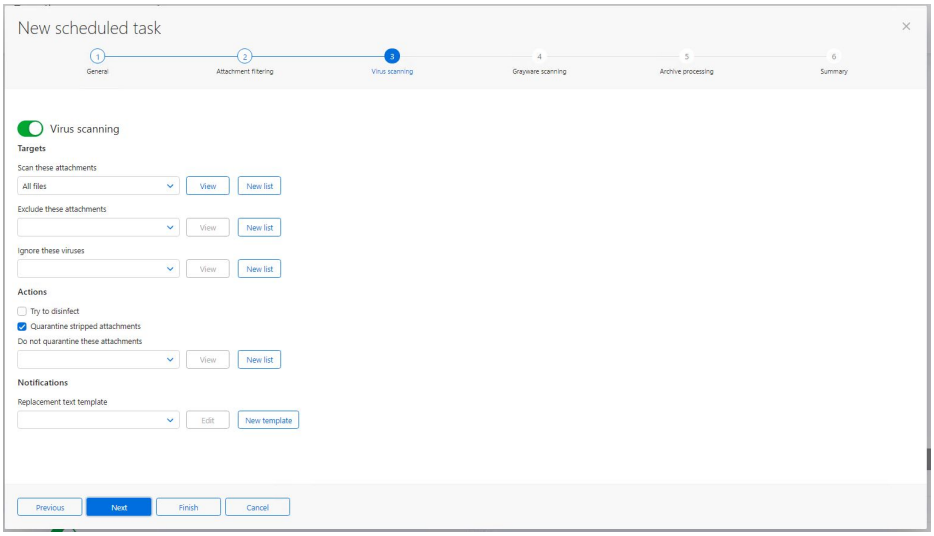

| | |
|---|---|
| **Attachment filtering** switch | Enable or disable the attachment stripping. |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see Lists on page 121 . |
| **Exclude these attachments** | Specify attachments that are not filtered. 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 Lists on page 121 . |
| 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 Templates on page 122 .

## Specify virus scanning options

Choose how mailboxes and public folders are scanned for viruses during the scheduled operation.




**Virus scanning** switch

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.

Targets

**Scan these attachments**

Specify attachments that are scanned for viruses. For more information, see Lists on page 121 .

**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.

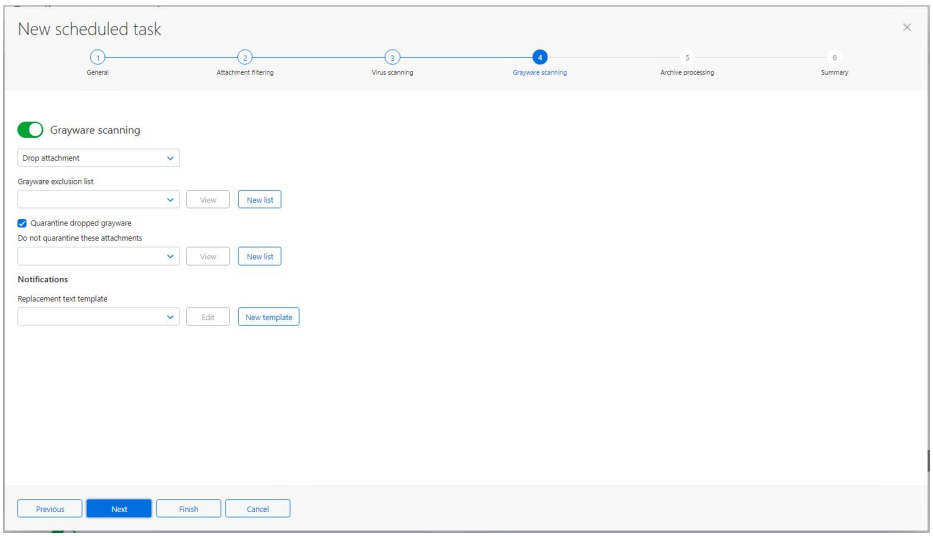
**Note:** Disinfection may affect the product performance.

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

| | |
|---|---|
| **Quarantine stripped attachments** | Specify whether infected or suspicious attachments are quarantined. |
| **Do not quarantine these attachments** | Specify infections that are never placed in the quarantine. For more information, see Lists on page 121 . |
| 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 Templates on page 122 . |

## Specify grayware scanning options

Choose settings for grayware scanning during the scheduled operation.



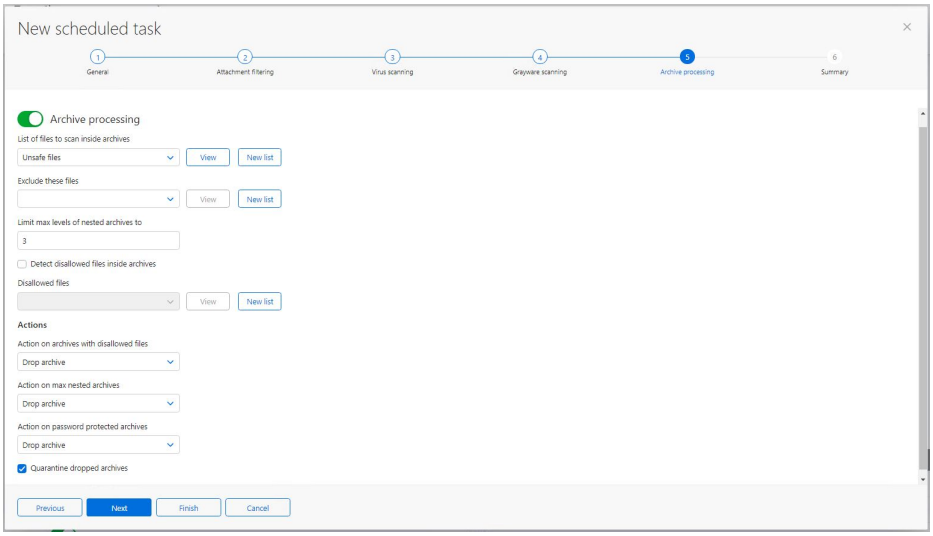

| | |
|---|---|
| **Grayware Scanning** switch | Enable or disable the grayware scan. |
| Actions | Specify the action to take on items which contain grayware.<br>**Report only** - Leave grayware items in the message and notify the administrator.<br>**Drop attachment** - Remove grayware items from the message. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |
| **Quarantine dropped grayware** | Specify whether grayware attachments are quarantined when dropped. |
| **Do not quarantine these attachments** | Specify grayware that are never placed in the quarantine. For more information, see Lists on page 121 . |

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 Templates on page 122 . |

## Specify archive processing options

Choose settings for archive processing during the scheduled operation.




| | |
|---|---|
| **Archive Processing** switch | Specify if files inside archives 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 on page 121 . |
| **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 Lists on page 121 . |

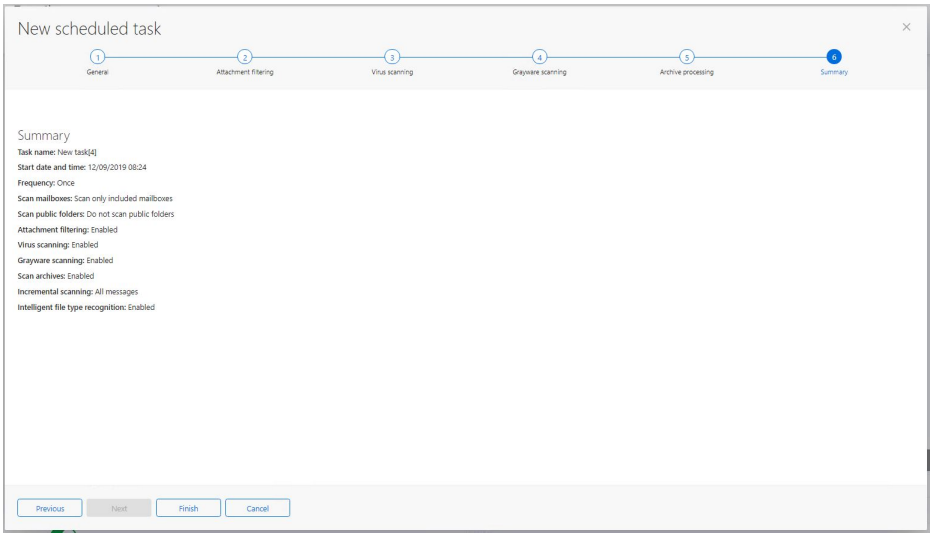
Actions

| | |
|---|---|
| **Action on archives with disallowed files** | Specify the action to take on archives which contain disallowed files.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - 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.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - 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.<br>**Pass through** - Deliver the message with the password protected archive to the recipient.<br>**Drop attachment** - 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. |

## Finish

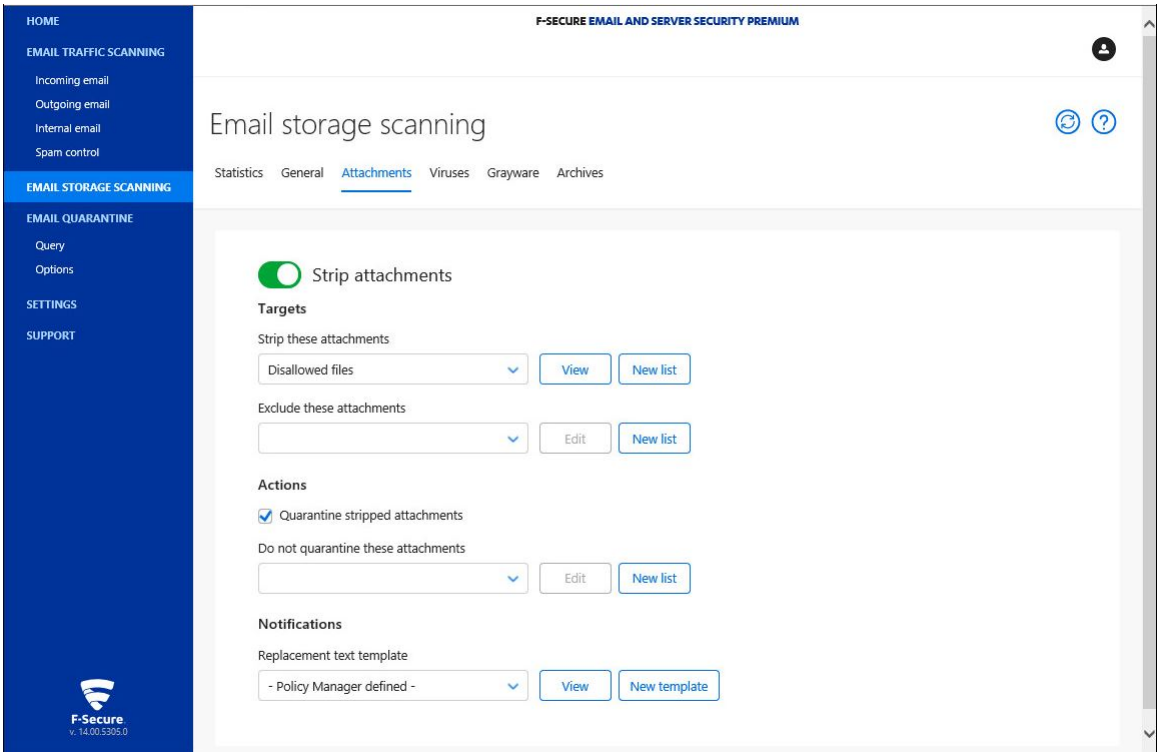
The **Summary** page displays an overview of the scheduled task.




Click **Finish** to accept the new scheduled task and exit the wizard.

## 4.5.2 Attachments

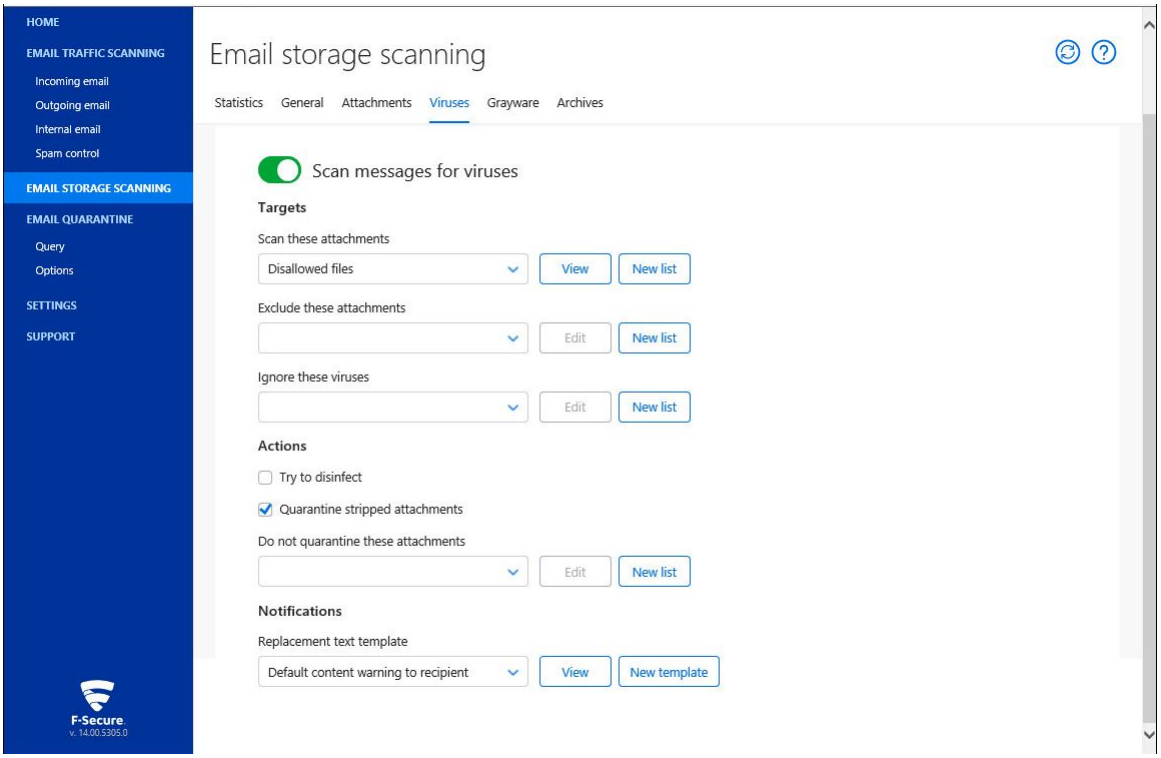
Specify attachments that are removed from messages during the manual scan.




| | |
|---|---|
| **Strip attachments** | Enable or disable the attachment stripping. |
| Targets | |
| **Strip these attachments** | Specify which attachments are stripped from messages. For more information, see Lists on page 121 . |
| **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 Lists on page 121 . |
| 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 Templates on page 122 . |

## 4.5.3 Viruses

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.

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

Targets

**Scan these attachments**

Specify attachments that are scanned for viruses. For more information, see Lists on page 121 .

**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 Lists on page 121 .

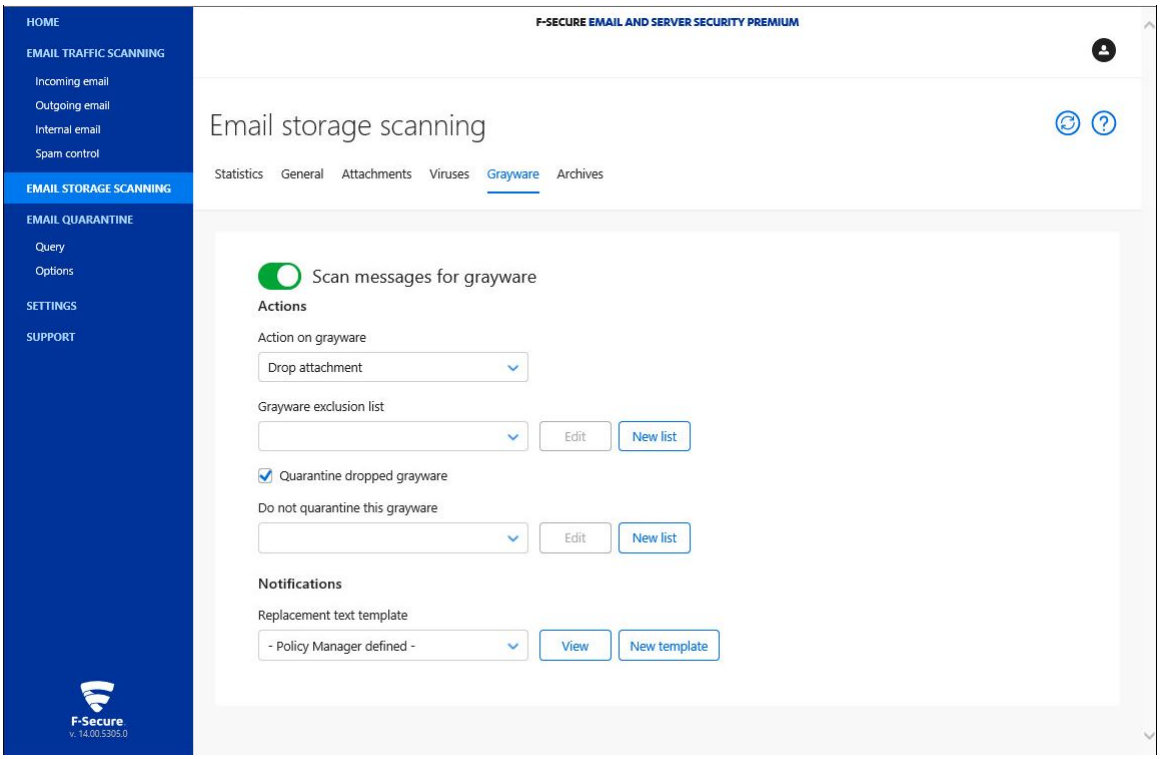
Notifications

**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 Templates on page 122 .

## 4.5.4 Grayware

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




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

**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 Lists on page 121 .

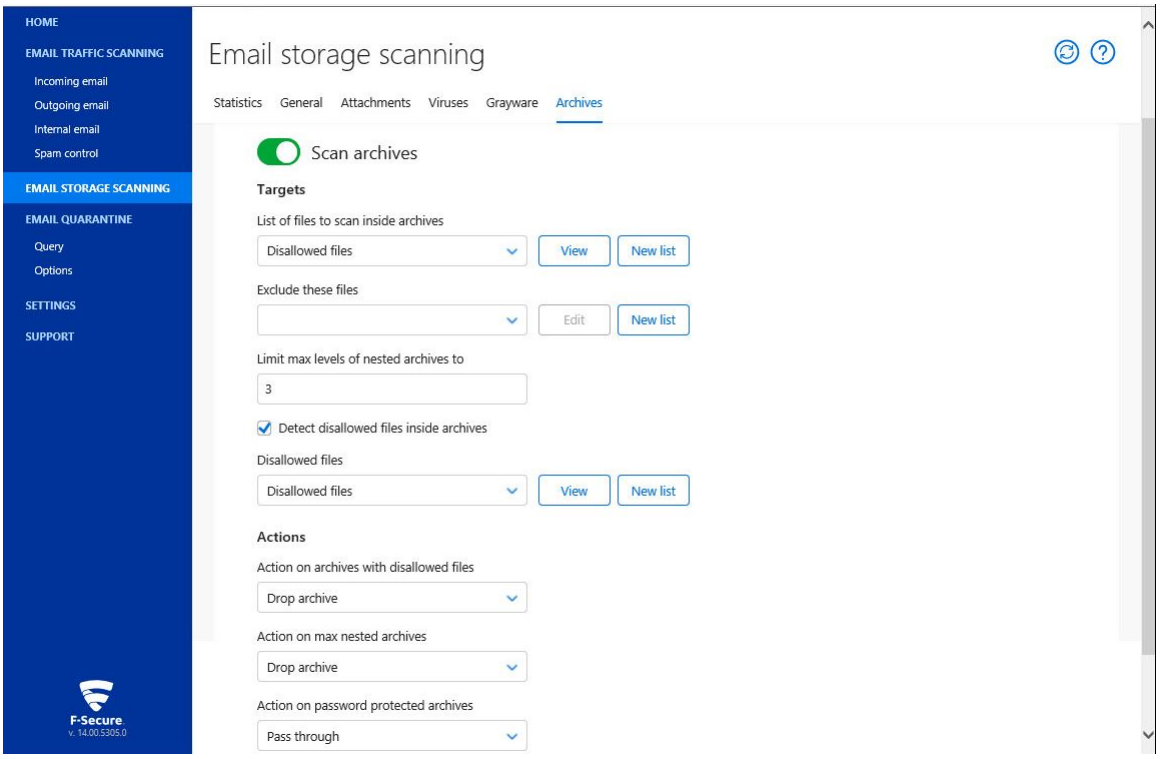
Notifications

**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 Templates on page 122 .

## 4.5.5 Archives

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.

Targets

**List of files to scan inside archives**

Specify files inside archives that are scanned for viruses. For more information, see Lists on page 121 .

| | |
|---|---|
| **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.<br>If you want to detect disallowed content, specify files that are not allowed. |
| Actions | |
| **Action on archives with disallowed files** | Specify the action to take on archives that contain disallowed content.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - 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.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - 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.<br>**Pass through** - Deliver the message with the archive to the recipient.<br>**Drop attachment** - 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. |

## 4.6 Email 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 emails to make them harmless. You can restore files and email messages from the quarantine later if you need them.

Email Quarantine quarantines email 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

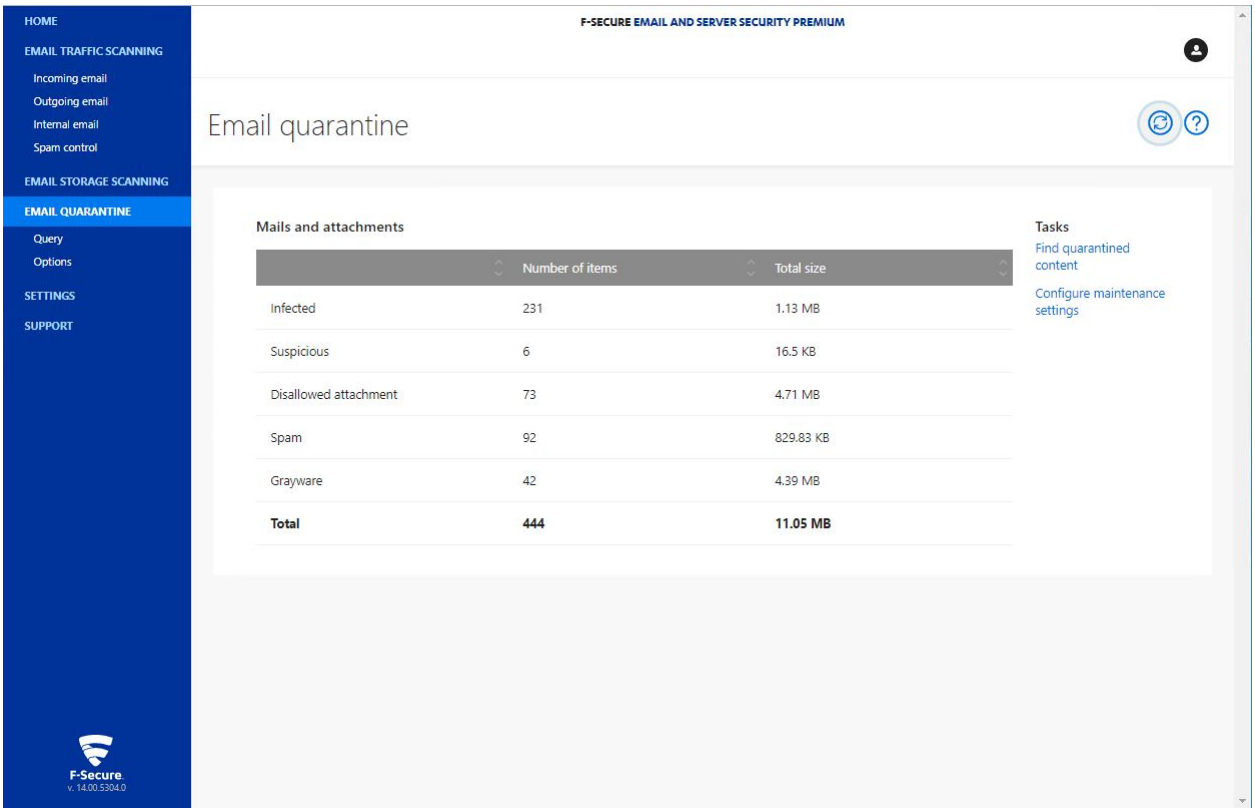
installed on different Microsoft Windows Servers running Microsoft Exchange Server, the Email Quarantine is handled through an SQL database and may be installed on a dedicated server.

**Note:** For additional information on different deployment scenarios for the product and how to install the Email Quarantine, consult F-Secure Email 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




The **Email quarantine** 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 applications, remote access tools and other unwanted applications. |
| **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. |
| **Scan failure** | Displays the number of files that could not be scanned, for example severely corrupted files. |
| **Total** | Displays the total number of messages and attachments that have been quarantined. |

#### Email quarantine tasks

Click **Find quarantined content** to search for the quarantined emails and attachments.

Click **Configure maintenance settings** to configure settings for automatic reprocessing and cleanup items in Email Quarantine.

## 4.6.1 Query

You can use Query pages to search and manually handle the quarantined content.

#### Quarantined mails and attachments

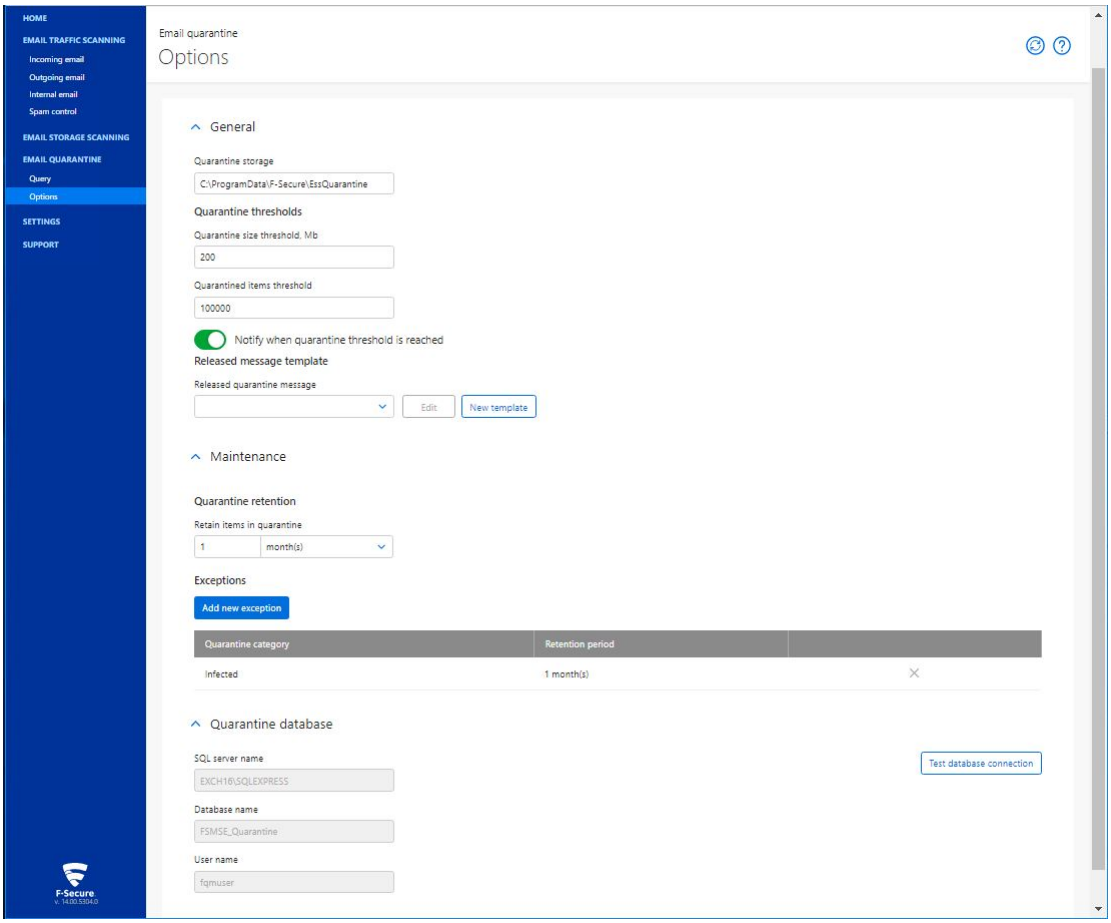
With the Quarantine Query page, you can create different queries to search quarantined emails and file attachments from the email quarantine database.

## 4.6.2 Options

You can configure the email quarantine storage location and threshold, how quarantined email messages and attachments are processed and quarantine logging options.

**Note:** All the described options affect the email quarantine only.

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**

Specify the location of the Email Quarantine storage.

Before you change the location, see Moving the email quarantine storage on page 132 .

**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 Email 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** switch | Specify if the administrator should be notified when the size or items thresholds are reached. No alert is sent if both thresholds are set to zero (0). |
| Released message template | |
| **Released quarantine message** | Specify the template for the message that is sent to the intended recipients when email content is released from the quarantine. For more information, see Templates on page 122 . |

### Maintenance

When removing quarantined messages from the quarantine, the product uses the currently configured quarantine retention and cleanup settings.

| | |
|---|---|
| Quarantine retention | |
| **Retain items in quarantine** | Specify how long quarantined items should be retained in the Email Quarantine before they are deleted.<br>Use the **Exceptions** table to change the retention period for a particular Quarantine category. |
| **Exceptions** | Specify separate quarantine retention period and cleanup interval for any Quarantine category. If the retention period for a category is not defined in this table, the default one (specified above) is used.<br>Click **Add new exception** to specify a separate retention period for a quarantine category.<br>**Active** - Enable or disable the selected entry.<br>**Quarantine category** - Select a category the retention period or cleanup interval of which you want to modify. The categories are:<br>• Unknown<br>• Infected<br>• Suspicious<br>• Disallowed attachment<br>• Spam<br>• Scan failure<br>• Grayware<br>**Retention period** - Specify an exception to the default retention period for the selected Quarantine category.<br>Click the **X** icon to remove the entry from the table. |

**Remove deleted items from the quarantine database**

Click **Start** to remove any entries from the quarantine database that have been manually deleted from file storage. You can choose to remove either only those entries that have been marked for deletion or all entries that no longer have an associated file available.

**Important:** This action cannot be undone. Before you remove all deleted items from the database, make sure that the current **Quarantine storage** folder is correct, or that the network share is accessible if you are using a centralized quarantine. We recommend that you create a backup of the quarantine database before you start this operation.

### Quarantine database

You can see the database where information about quarantined emails is stored and from which it is retrieved.

| 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`. |

## 4.7 SharePoint protection

SharePoint protection scans the content that is uploaded and downloaded from the SharePoint server.

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 **SharePoint protection** page displays a summary of the scanned and detected documents categorized by direction (download and upload) and detected threat (infection, grayware, suspicious documents, and failed scans).

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

### 4.7.1 General settings for SharePoint

Choose whether or not to use intelligent file type recognition for SharePoint, and how to handle the downloading of infected files.

| | |
|---|---|
| **Intelligent file type recognition** | Select whether you want to use the intelligent file type recognition or not.<br><br>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.<br><br>**Note:** Using Intelligent file type recognition strengthens the security, but can degrade the system performance. |
| **FTR exclusions** | Enter any file extensions that you do not want intelligent file type recognition to process. |
| **Download infected file action** | Select **Warn** to display a warning about the infected file, but allow users to download them. Select **Block** to prevent users from downloading infected files. |

## 4.7.2 Virus scanning settings for SharePoint

Specify how the product processes malware.

| | |
|---|---|
| **Scan documents for viruses** | 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. |
| **Scan these documents** | Specify documents that are scanned for viruses. |
| **Exclude these documents** | Specify the list of documents that should not be scanned for viruses. |
| **Ignore these viruses** | Specify the virus names that you want to ignore during scanning. You can use this, for example, to skip test files. |

## 4.7.3 Grayware scanning settings for SharePoint

Specify how the product processes grayware items.

| | |
|---|---|
| **Scan documents for grayware** | When grayware scanning is enabled, the product scans for grayware (adware, spyware, riskware and similar).<br>**Note:** Grayware scanning is disabled if virus scanning is disabled. |
| **Action on grayware** | Specify the action to take on items which contain grayware.<br>**Pass through** - Let users access grayware items.<br>**Block document** - Prevent users from accessing grayware items. |
| **Grayware exclusion list** | Specify attachments that are not filtered. Leave the list empty if you do not want to exclude any attachments from the filtering. |

## 4.7.4 Archive scanning settings for SharePoint

Specify how the product processes viruses inside archives.

| | |
|---|---|
| **Scan archives** | 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. |
| **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 to** | Specify how many levels deep to scan in nested archives, if archive processing is enabled.<br><br>A nested archive is an archive that contains another archive inside. If zero (0) is specified, the maximum nesting level is not limited.<br><br>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 archives with nesting levels exceeding the upper level specified in the **Limit max levels of nested archives** setting.<br><br>**Pass through** - Nested archives are scanned up to level specified in the **Limit max levels of nested archives to** setting. Exceeding nesting levels are not scanned, but the archive is not removed.<br><br>**Block document** - 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.<br><br>**Pass through** - Leave the password protected archive in the message.<br><br>**Block document** - Remove the password protected archive from the message. |

### 4.7.5 SharePoint notifications

Specify whether and when the product sends alerts to the administrator.

In centrally managed installations, the notifications are sent to Policy Manager Console.

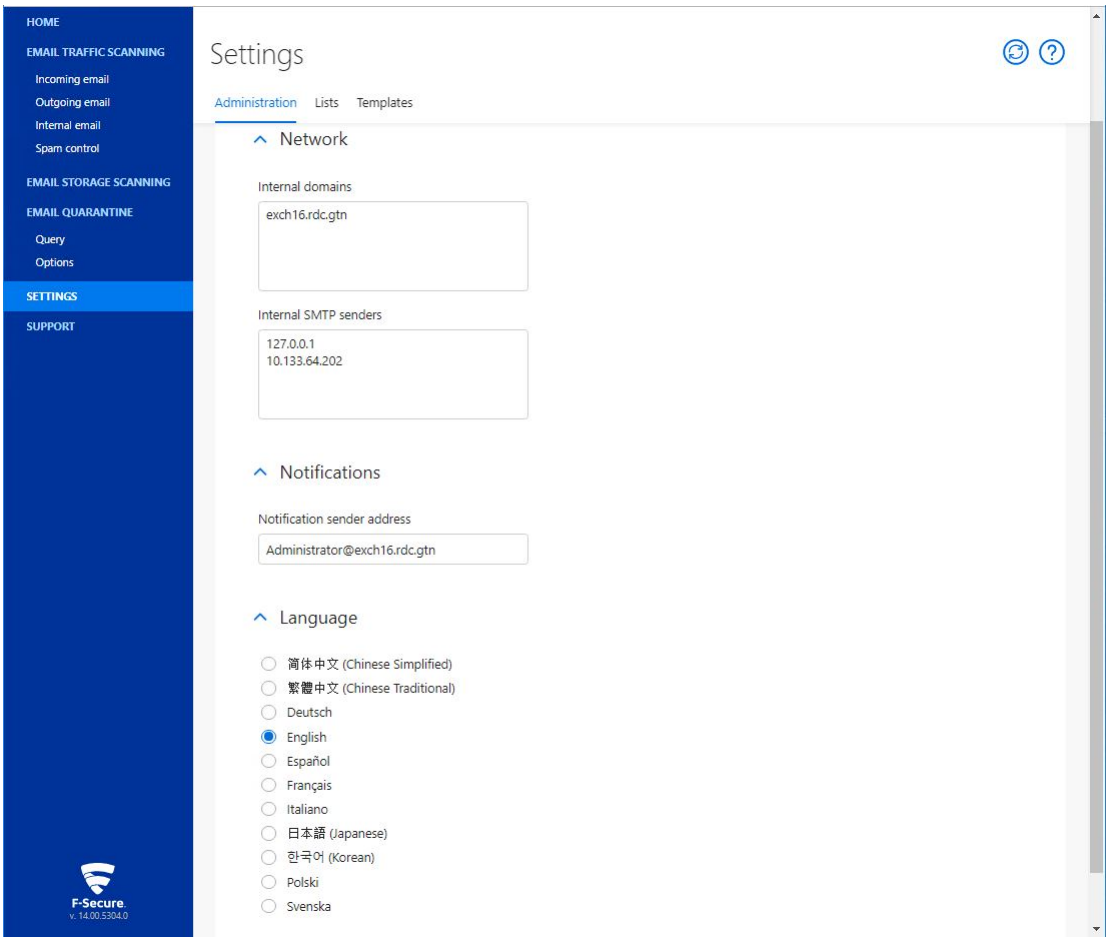
| | |
|---|---|
| **Send alert to administrator when** | Specify if the administrator is notified when an infection or grayware item is found or when an archive or message nesting level is exceeded. |

## 4.7.6 Advanced settings for SharePoint

The settings on the **SharePoint protection** > **Advanced configuration** page are intended for managing the product services that affect the performance of the server.

| | |
|---|---|
| **Use this host to notify SharePoint service of virus definition updates and scanning configuration changes** | Select this to send product update and configuration change notifications to the SharePoint service.<br><br>This setting is related to the use of SharePoint farms. When Email and Server Security is installed on a SharePoint farm, each installation sends product update and configuration change notifications to the same SharePoint service by default. As this can have an impact on performance, you can select one of the installations to handle the notifications on behalf of all Email and Server Security installations within the same SharePoint farm. |
| **Maximum number of concurrent scanning transactions** | Specify the maximum number of scanning processes that can be running at any given time. The default is 5. |
| **Maximum file size for scanning** | Specify the maximum size for individual files stored on SharePoint in megabytes. Any files larger than this are not scanned. |

## 4.8 Settings



The **Settings** allow you to configure the internal network addresses, language for the Web Console, and the lists and templates that are used by the various product features.

### Administration

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

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

**Note:** If email messages come from internal SMTP sender hosts and contain both internal and external recipients, messages are split and processed as internal and outgoing respectively.

---

Network

**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:

- IPv4 address (for example, 172.16.4.4 172.16.4.0-16 172.16.250-255),
- 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

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 email client to send and receive email, 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:**

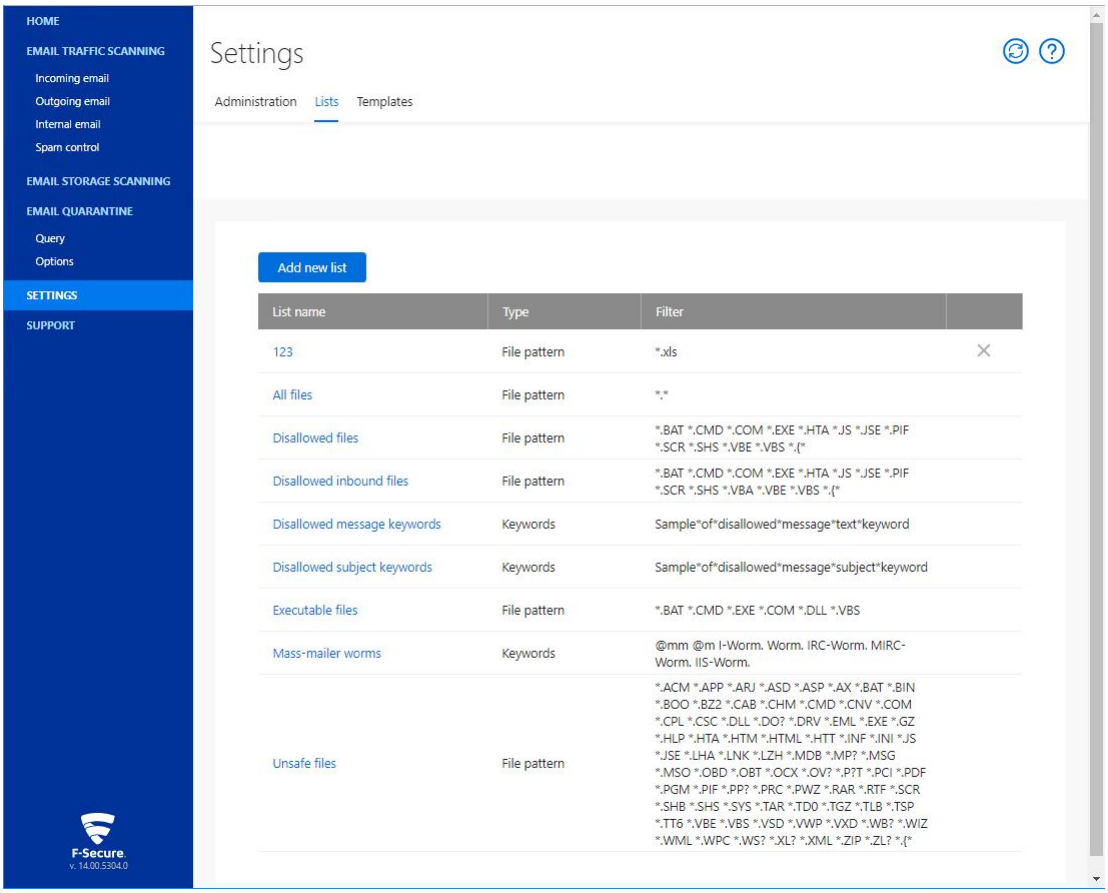
Do not specify the server where the Edge role is installed as Internal SMTP Sender.

Notifications

| | |
|---|---|
| **Notification sender address** | Specify the email address that is used to send warning and informational messages to the end-users (for example, recipients, senders, and mailbox owners). |
| Language | Specify the language that you want to use.<br><br>**Note:** Reload the Web Console after you change the language to take the new language into use. |

## 4.8.1 Lists

Match lists are lists of file name patterns or email addresses that can be used with certain product settings.



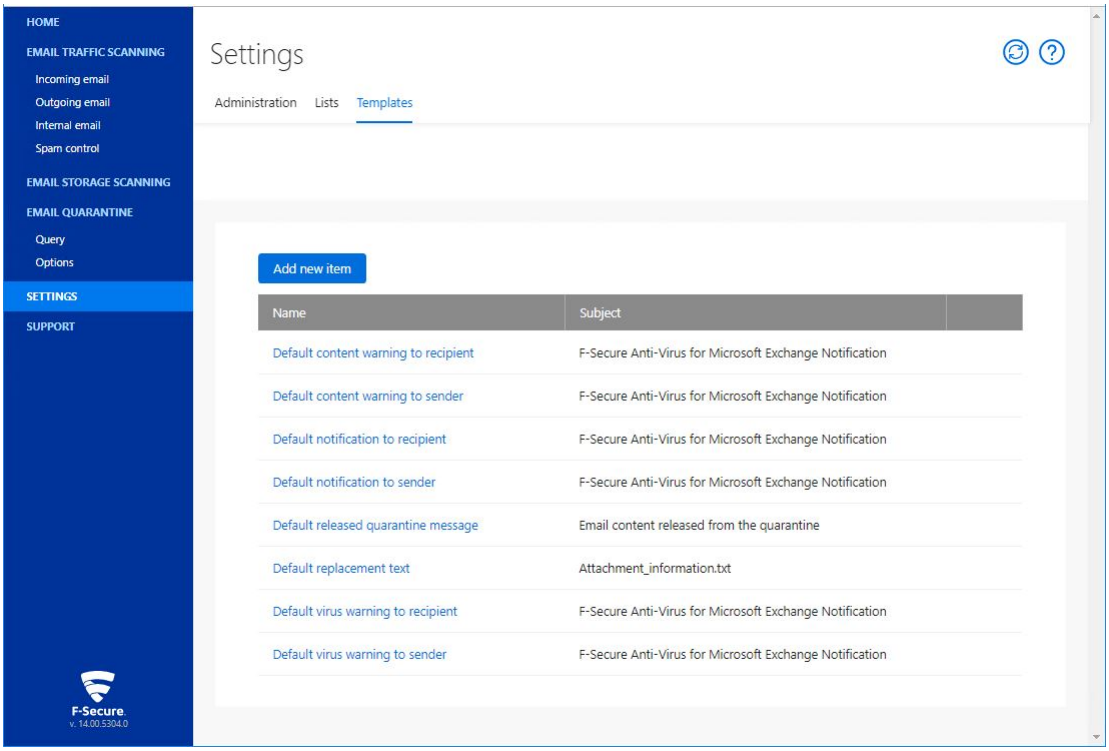

Click the name of an existing match list to edit the list or **Add new list** to create a new match list.

| | |
|---|---|
| **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 file patterns or email addresses. |
| **Filter** | Specify file names, extensions, or email 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.

## 4.8.2 Templates

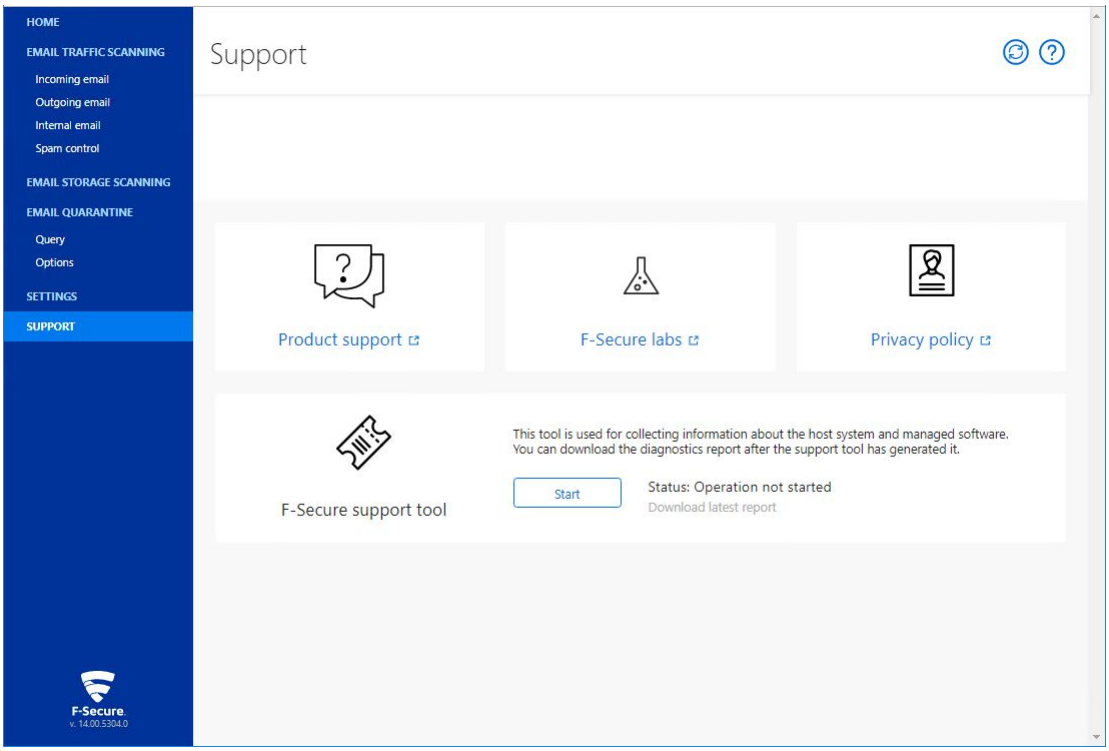
Message templates can be used for notification messages.




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.<br><br>For more information about the variables you can use in notification messages, see Variables in warning messages on page 134 . |
| **Description** | Specify a short description for the template. |

## 4.9 Support




**Product support**

F-Secure Technical Support is available through F-Secure support web pages, email 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 https://www.f-secure.com/en/web/business_global/support. 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.

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. Select **F-Secure support tool** on the **Support** 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 `diagnostics` directory under the product installation directory, or run **F-Secure Email and Server Security > Support Tool** in the Windows Start menu. The tool generates a file called `fsdiag.zip`.

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.
- 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.

**F-Secure labs** F-Secure Corporation maintains a comprehensive collection of virus-related information on its website. To view the Virus Information Database, connect to: https://www.f-secure.com/en/web/labs_global/threat-descriptions.

**Privacy policy** Click **Support** > **Privacy policy** to read more information about what information F-Secure collects and how it is used.

Chapter

5

# Email quarantine management

**Topics:**



You can manage and search quarantined mails with the Web Console or the Email Quarantine Manager (EQM).

**Note:** EQM requires a separate installation. See the F-Secure Email and Server Security Deployment guide for the installation instructions.

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 Email quarantine consists of:

- Quarantine database, and
- Quarantine storage.

### Quarantine database

The Email 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 Email 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.

## 5.1 Quarantine reasons

The Email 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 are considered as spam. **(Spam)**
- Messages that contain grayware. **(Grayware)**
- Files that could not be scanned, for example severely corrupted files. **(Scan failure)**

## 5.2 Configuring email 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 Email quarantine on page 111 .

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.

The actual quarantine management is done through either the Web Console or Email Quarantine Manager (EQM).

**Note:** To start using the EQM app, enter the following address in your browser: `https://<host>/eqm/`. <host> is the host name or IP address of your server.

## 5.3 Quarantine status

The Email quarantine page displays the number of quarantined items in each quarantine category, and the total size of the quarantine.

## 5.4 Searching the quarantined content

You can search the quarantined email messages and attachments on the **Email quarantine** > **Query** page in the Web Console.

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.<br>**Mails and attachments** - Search for both quarantined mails and attachments.<br>**Attachment** - Search for quarantined attachments.<br>**Mail** - Search for quarantined mails. |
| **Reason** | Select the quarantining reason from the drop-down menu. |
| **Reason details** | Specify details about the scanning or processing results that caused the message to be quarantined. For example:<br>**The message is infected** - specify the name of the infection that was found in an infected message. |

| | |
|---|---|
| **Sender** | Enter the email 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 email address of the message recipient. |
| **Subject** | Enter the message subject to be used as a search criteria. |
| **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 emails may take time, you can use this option to monitor how the operation is progressing.<br>The options available are:<br>**Unprocessed emails** - Displays only emails that the administrator has not set to be released, reprocessed or deleted.<br>**Emails to be released** - Displays only emails that are currently set to be released, but have not been released yet.<br>**Emails to be reprocessed** - Displays only emails that are currently set to be reprocessed, but have not been reprocessed yet.<br>**Emails to be released or reprocessed** - Displays emails 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 by** | 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. |

| Wildcard | Explanation |
|---|---|
| _ (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: '[%]', '[_]', '[[]'

## 5.5 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.

The Query Results page displays status icons of the content that was found in the search:

| Icon | Email status |
|---|---|
|  | Quarantined email. The administrator has not specified any actions to be taken on this email. |
|  | Quarantined email with attachments. The administrator has not specified any actions to be taken on this email. |
|  | Quarantined email that the administrator has set to be released. The release operation has not been completed yet. |
|  | Quarantined email that the administrator has set to be reprocessed. The reprocessing operation has not been completed yet. |
|  | Quarantined email that the administrator has set to be deleted. The deletion operation has not been completed yet. |
|  | Quarantined email that the administrator has submitted to F-Secure for analysis. |
|  | Quarantined email set to be released, which failed. |
|  | Quarantined email set to be reprocessed, which failed. |
|  | Quarantined email set to be submitted to F-Secure, which failed. |

## 5.5.1 Viewing details of the quarantined message

To view the details of a quarantined message or attachment, do the following:

**Note:** You cannot view the details in the Email Quarantine Manager.

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. |
| **Reason details** | More details on why the content was quarantined. |

1. Click the **Show message source** switch to access the content of the quarantined message. **Quarantined messages only.**
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.

## 5.6 Quarantine operations

Quarantined mails and attachments can be reprocessed, released and removed from the Email 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 email again, or click **Reprocess All** to scan all email messages that were found.
- Click **Release** to deliver the currently selected email without further processing, or click **Release All** to deliver all email messages that were found.

**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 email from the quarantine, or click **Delete All** to delete all email messages that were found. For more information, see Removing the quarantined content on page 132 .
- 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.
- Click **Delete** to delete the currently selected email from the quarantine, or click **Delete All** to delete all email messages that were found. For more information, see Removing the quarantined content on page 132 .
- Click **Send to F-Secure** to submit a sample of the quarantined content to F-Secure for analysis.

### 5.6.1 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 email, 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 Email 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 or the main page of the EQM app.
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 emails that have been reprocessed and found clean are delivered to the intended recipients. They are also automatically deleted from the quarantine.
   - Emails that have been reprocessed and found infected, suspicious or broken return to the quarantine.

### 5.6.2 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 or the main page of the EQM app.

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 email message or just the attachment that was quarantined.
   a. When the quarantined content is an email 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 email 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.

### 5.6.3 Removing the quarantined content

Quarantined messages are removed from the quarantine based on the currently configured quarantine retention and cleanup settings.

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 or the main page of the EQM app.
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 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.

### 5.6.4 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 **Maintenance**.
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 **Save and apply**.

## 5.7 Moving the email quarantine storage

When you want to change the Email 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 Email 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 Email Quarantine storage directory by copying the existing directory with the current ownership and ACL information. In the following example, the Email 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 Email Quarantine storage from the F-Secure Policy Manager Console (`F-Secure Anti-Virus for Exchange/Settings/Quarantine/Quarantine Storage`) or the Web Console (Quarantine Storage field on the **Quarantine** > **Options** > **General**).
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.

Chapter

6

# Variables in warning messages

The following tables list the variables that can be included in the warning and informational messages that the product sends when it finds a harmful file or blocks content.

If the product is set to both scan files and strip attachments and it finds both types of disallowed content (infected file that should be stripped) in an email message, the product sends a warning message instead of an informational one.

These variables are dynamically replaced by their actual names. If the actual name does not exist, the variable is replaced with [Unknown].

| Variable | Description |
|---|---|
| $ANTI-VIRUS-SERVER | The DNS/WINS name or IP address of F-Secure Email and Server Security. |
| $NAME-OF-SENDER | The email address where the original content comes from. |
| $NAME-OF-RECIPIENT | The email addresses where the original content is sent. |
| $SUBJECT | The original email message subject. |
| $DIRECTION | The direction of email message (incoming, outgoing, 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 do not apply to replacement texts that are used on real-time scanning the Exchange storage.

The following table lists variables that can be included in the scan report, which is the warning message between $REPORT-BEGIN and $REPORT-END variables.

| 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. |

Chapter

7

# Troubleshooting

**Topics:**

## 7.1 Registering F-Secure Transport Agent

F-Secure Transport Agent should be registered in the Microsoft Exchange Transport Service automatically during the installation.

To check whether F-Secure Transport Agent is installed and working correctly:

1. Open Exchange Management Shell.
2. Run the following command: `Get-TransportAgent "F-Secure Transport Agent"`

If F-Secure Transport Agent is successfully installed and running, you will receive the following output:`Enabled=true` and `Priority=1`

If you have issues with automatic installation of F-Secure Transport Agent, 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\Email and Server Security\Anti-Virus for Microsoft Services"` to go to the product installation directory.
4. Type `PowerShell.exe -command ".\fstragnt.ps1 install"` to install F-Secure Transport Agent.

## 7.2 Checking the web console

Follow these steps if you have issues accessing or logging in to the web console.

**Issue**: The web console is not accessible (not displayed).

**Possible solutions:**

1. Check that the state of the application pools (EssWebUiPool, EssWebAPIPool) is 'Started' in IIS.
2. If you cannot log in with your `user` and `password` combination, try using `domain\user` and `password`.
3. Open a browser on a remote machine and go to `https:<ess_server_ip>:25023` and log in with your user name.
4. Verify that TLS 1.0, 1.1 and 1.2 are enabled. Our advice is to use TLS 1.2. To check that TLS is enabled:
   a. Launch Internet Explorer.
   b. Enter the URL you wish to check in the browser.
   c. Right-click the page or select the Page drop-down menu and select **Properties**.
   d. In the new window, look for the "Connection" section. From there, you will find the version of TLS or SSL used.

   You need to complete the following three tasks to enable TLS 1.2 on clients:

   a. Update Windows and WinHTTP.
   b. Ensure that TLS 1.2 is enabled as a protocol for SChannel at the operating system level.
   c. Update and configure the .NET Framework to support TLS 1.2.

   To check that TLS 1.2 is enabled in the registry, ensure that `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client\DisabledByDefault` registry key is present and that the value is `0`.
5. Try to disable HTTP 2.0:
   a. Open the Windows **Start** menu and enter `regedit`.
   b. Enter the following path: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters`.
   c. Right-click the `Parameters` folder and select **New** > **DWORD (32-bit) Value** to add the following values:
      - `EnableHttp2Tls`
      - `EnableHttp2Cleartext`
   d. Right-click the values and select **Modify** to check that both values are set to `0` (disabled).

e. Restart the computer.

6. Use the self-signed certificate:

   a. In Administrative Tools, start **Internet Information Services (IIS) Manager**.
   b. Go to **Sites** > **EssWebConsole**.
   c. Select **Bindings**.
   d. Select the HTTPS entry that has Port 25023 and IP address.
   e. Click **Edit** and make sure "Local ESS Web Console Self Signed Cert" is selected.

   If the Email and Server Security WebUI is not displayed and the certificate is missing from IIS, you can run the setup `F-Secure.Ess.Config.exe` to create a new certificate. The tool can be found in `C:\Program Files (x86)\F-Secure\Email and Server Security\ui\F-Secure.Ess.Config.exe`:

   a. Go to your Exchange Server locally `C:\Program Files (x86)\F-Secure\Email and Server Security\ui`.
   b. Run `F-Secure.Ess.Config` as administrator.
   c. Make sure you select 'Use self-signed certificate (NOT SECURE!)' at the corresponding step.
   d. Complete the setup.

   Once completed, you should now be able to select the certificate in **IIS** > **EssWebConsole** > **Bindings**.

   **Note:** While using a self-signed certificate could help in testing issues, we still recommend that you use your company's own security certificate for the Web Console.

7. Check that the **Static Content** Windows feature is enabled in the following way: **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off** > **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features** > **Static Content**.
8. In rare cases, there may be installation errors preventing the WebUI display (MSI errors can be found in Windows event log).

   Resolution:

   a. Use the uninstallation tool, restart the machine, and then install again.
   b. Check that the state of the application pools (EssWebUiPool, EssWebAPIPool) is 'Started' in IIS.

**Issue**: I am unable to log in to the F-Secure Email and Server Security Web Console after product installation.

**Possible solutions:**

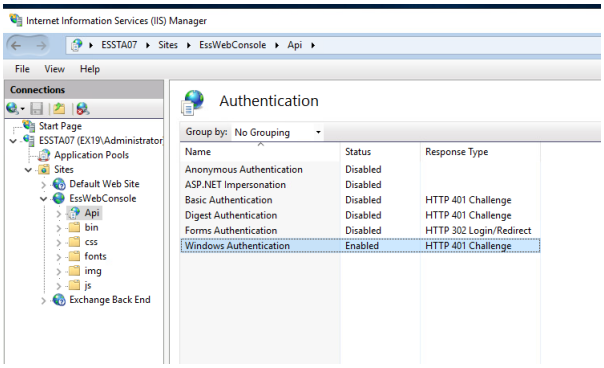
1. Check that the AD account can log in to Windows.
2. Check that the server supports Windows Authentication: **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off** > **Internet Information Services** > **World Wide Web Services** > **Security** > **Windows Authentication**.

   a. On the taskbar, click **Server Manager**.
   b. In Server Manager, click the **Manage** menu, and then click **Add Roles and Features**.
   c. In the Add Roles and Features wizard, click **Next**. Select the installation type and click **Next**. Select the destination server and click **Next**.
   d. On the Server Roles page, expand Web Server (IIS), expand Web Server, expand Security, and then select **Windows Authentication**. Click **Next**.
   e. On the Select features page, click **Next**.
   f. On the Confirm installation selections page, click **Install**.
   g. On the Results page, click **Close**.

   Check that Windows Authentication enabled in IIS:

   a. On the Start screen, click **Control Panel**.
   b. Click **System and Security** > **Administrative Tools**.
   c. In the Administrative Tools window, double-click **Internet Information Services (IIS) Manager**.
   d. Expand the node and go to **Sites**, expand **EssWebConsole** and click on **API**.

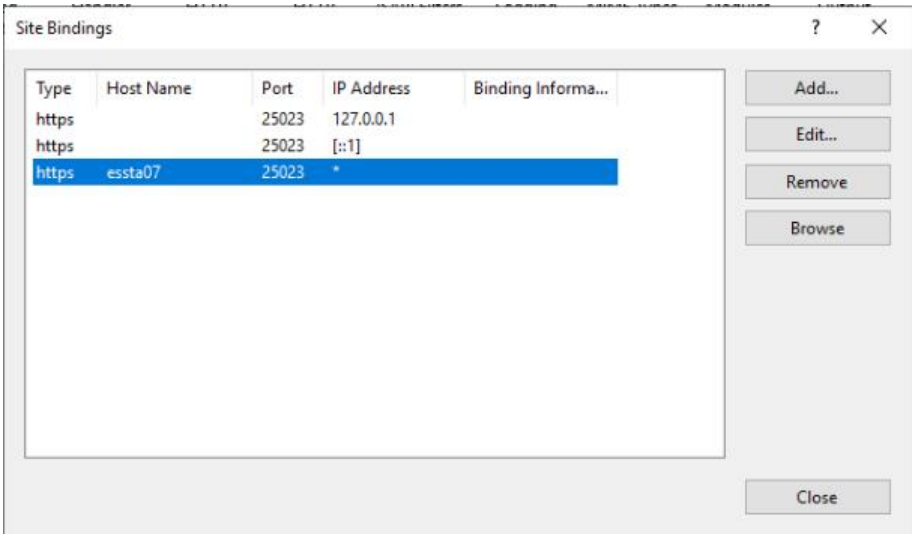
**e.** Click on Authentication and make sure it's enabled:




**3.** The account you are using to enter the WebUI is a member of the "Protected Users" group.

To resolve this issue you need to either remove a user from this group or tune IIS in the following way:

**a.** Add an additional site binding with the name of the target server where the web console is installed; for example:




The name should be a part of service principal names (you can check it by using the following command in PowerShell: `setspn -L [domain]\[server name]`

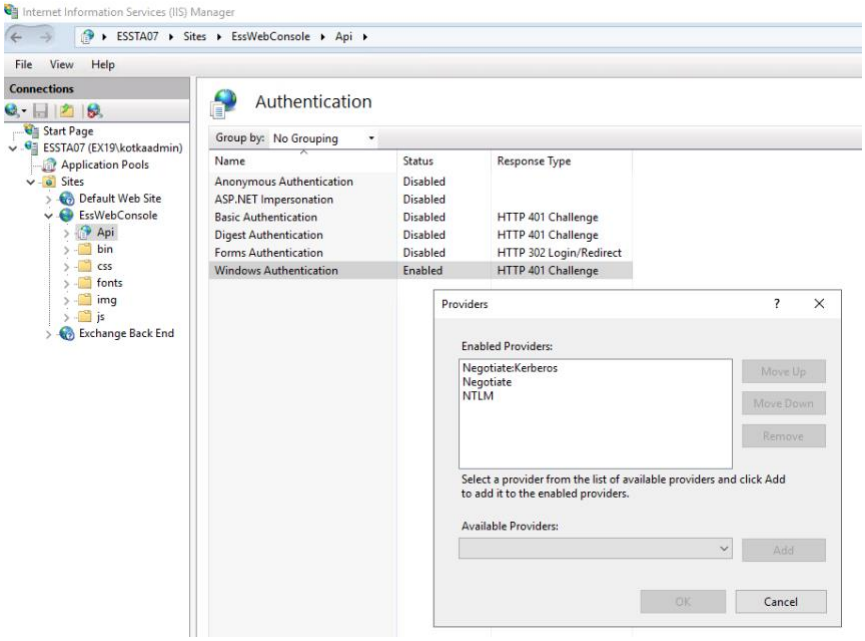
**b.** Rearrange providers priority inside **IIS** > **EssWebConsole** > **Api** > **Authentication**:

Negotiate: Kerberos

Negotiate

NTLM

An example:




**c.** Try to log in using a link such as the following: https://servername:25023 (not https://127.0.0.1:25023) .

**4.** The Firefox browser persistently asks for credentials despite opening the web console successfully. Try the following workaround: create a new empty Firefox profile, disable all add-ons, clear cache, update Firefox, and try again.

## 7.3 Securing the email quarantine

**Problem:**

I have installed the product and I'm worried about security of the local Email Quarantine storage where stripped attachments are quarantined. What do you recommend me?

**Solution:**

The product creates and adjusts access rights to the local Email Quarantine storage during the installation. Keep in mind the following when setting up the local Email Quarantine storage:

- Do not place the Email 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 Email Quarantine storage manually if you use one on a network drive.
- Create and adjust access rights to the Email Quarantine storage manually when you change its path from F-Secure Policy Manager Console or the Web Console.

## 7.4 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, select **Final** check box to enforce the change.

## 7.5 Resolving issues with spam scanning

Follow these steps if you experience issues with the anti-spam module.

If Email and Server Security incorrectly classifies an email message as spam, see the following article for more information: Email messages are incorrectly classified by the F-Secure spam scanner.

1. Open the following page in the server's browser to check that Email and Server Security is able to connect to the internet: https://aspam.sp.f-secure.com/bdnc/config.

   The page should open and show the following JSON content:

   ```
   {"benchmarkInterval":3600,"benchmark":1,"servers":["aspam.sp.f-secure.com"],
   "statsInterval":1800,"enforceSSL":true,"benchmarkThreshold":5,"disableThreshold":10}
   ```

   The anti-spam scanner needs to connect to the detection center for each message that it scans. The product includes a small local database that is used for internal optimization, but that does not cover enough data to complete a scan.

   If the page does not open:

   a) Check if you need a proxy to access the page in your browser.

      If so, you need to configure the anti-spam scanner to use the same proxy in Policy Manager.

   b) Check that your firewall allows access to the following domains:

      - `*.f-secure.com`
      - `*.fsapi.com`

2. Check that Anti-Spam updates are downloaded.

   a) Open the product's local user interface.

   b) Select **Settings** > **Updates** and check the list of updates under **Update history**.

3. If spam messages are not being quarantined, check the maximum email size under **Email traffic scanning** > **Spam control** in the web console and increase it if it is set too low.

4. Check the quarantine rules.

   For example, if you have set the quarantine rules as follows:

   - If the spam detection level is between 1 and 5, the message is only marked as spam
   - If the spam detection level is between 6 and 8, the message is quarantined
   - If the spam detection level is 9, the message is dropped

   On receiving 10 messages rated at level 4, 10 messages rated at level 6, and 10 messages rated at level 9, this means that a total of 30 messages are scanned, but only 10 are quarantined.

5. There could be wrong settings in `internal_senders` which results in wrong email direction handling (spam filter works only for incoming direction); for example:

   ```
   windows.microsoft.exchange.general.internal_domains: "domain.com domain2.com"
   windows.microsoft.exchange.general.internal_senders: "administrator@domain.com <IP of one
   server>"
   ```

   It is supposed to put a list of all IPs of computers that send/receive emails to `internal_senders`. An example: 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0 192.168.3.0/255.255.255.0

   **Note:** The IP of Frontend/Edge servers should not be listed in `internal_senders`, and neither the server's name in `internal_domains`. If they are listed, all incoming emails will be considered internal, and hence there will be no spam scanning.

   For example, you can exclude one IP in `internal_senders` in the following way: `192.168.*.1-125 192.168.*.127-255`

   For more information, see General settings on page 27

## 7.6 Checking quarantine access

You can check the quarantine access either in the web console or on the server where the product is installed.

1. In the web console, go to **Email quarantine** > **Options** and select **Test database connection**.
2. Check the local permissions on the Windows server where the product is installed.

   The FQM service should be run under the `LocalSystem` account. As the `Microsoft Exchange Transport` service uses the `NETWORK SERVICE` account, so does the product's transport agent.

   a) Check that the following accounts have access to the `...Anti-Virus For Microsoft Services\` folder:

- NETWORK SERVICE: read, execute

b) Check that the following accounts have access to the C:\ProgramData\F-Secure\EssTemp\ folder:

- LocalSystem: FULL
- administrators: FULL
- NETWORK SERVICE: read, write, delete

c) Check that the following accounts have access to the C:\ProgramData\F-Secure\EssLimited\ folder:

- LocalSystem: FULL
- administrators: FULL
- NETWORK SERVICE: read, delete

d) Check that the following accounts have access to the C:\ProgramData\F-Secure\EssQuarantine\ folder:

- LocalSystem: FULL
- administrators: FULL

3. If you are using centralized mode for the quarantine, check the permissions for the network share:
   a) Check that the FQM account (SYSTEM by default) has read, write, and change access rights to the remote centralized quarantine (**Share** and **Folder Security** tabs).
   b) Check that the Exchange Servers group or specific Exchange computers have read, write, and delete access rights on the **Security** and **Share** pages.
4. Check SQL Management Studio.
   a) Check that the instance is running.
   b) Check that mixed authentication mode is enabled.
   c) Check that the database exists.
   d) Check that the FQM user account has write access to the database (database owner).

**Important:** Once all permissions have been set properly, you need to restart F-Secure Quarantine Manager.

**Issue:** During the setup, the SQL path can't be found.

**Resolution:** The setup will find the path if the SQL server is installed on the same server as ESS. If it fails for some reason, you can enter .\sqlexpress to locate it. If SQL is not installed on the same server, enter the network path and the SQL instance name. Then the setup will find it.

**Issue:** No quarantine database path in the WebUI after an upgrade

**Resolution:**

1. Run F-Secure.Ess.Config.exe as administrator from the target server. F-Secure.Ess.Config.exe is located at C:\Program Files (x86)\F-Secure\Email and Server Security\ui.
2. Configure the setup for an existing database or create a new database. Make sure that the permissions are set correctly.

**Issue:** Released emails from the F-Secure Email and Server Security quarantine are not reaching the recipient's mailbox.

**Note:** There can also be a delay based on the number of items selected, SQL connection speed, and system performance.

**Resolution:**

1. Restart the F-Secure Quarantine Manager (FQM) service and see if the items are released from the mailboxes.
2. Check permissions for your quarantine as described above.

## 7.7 Resolving issues with unsafe URLs

Follow these steps if you experience issues with unsafe URLs.

**Issue:** Scan messages for unsafe URLs for an internal policy route is deactivated but nevertheless the messages are dropped.

**Resolution:**

Make sure that the network settings for your F-Secure Email and Server Security are set correctly.

For more information, see General settings on page 27

## 7.8 Checking connectivity issues

The connection checker tool allows you to verify the connection to our servers, and is especially useful when dealing with environments where a proxy is being used and if it is unclear if our components are able to connect or not to the required cloud services.

This tool can be found at `C:\Program Files (x86)\F-Secure\Email and Server Security\ui\fsconnectionchecker.exe`.

To verify the connection:

1. Once the UI starts, select the product.
2. Manually add proxies and servers to check the connectivity through.

   The necessary backend servers for each product are already pre-defined. The UI tool tries to verify a connection and returns a result: success or failed with description.
3. When everything is ready, you can save the report as an HTML file.

Chapter

8

# Technical support

**Topics:**

## 8.1 F-Secure online support resources

F-Secure Technical Support is available through F-Secure support web pages, email 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 https://www.f-secure.com/en/business/support-and-downloads or by selecting **Product support** on the Support page in the Web Console. 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.

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. Select **F-Secure support tool** on the **Support** 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 `diagnostics` directory under the product installation directory, or run **F-Secure Email and Server Security > Support Tool** in the Windows Start menu. The tool generates a file called `fsdiag.zip`.

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.
- 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.

## 8.2 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/.

## 8.3 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, either connect to: https://www.f-secure.com/en/web/labs_global/threat-descriptions or on the Web Console **Support** page, select **F-Secure labs**, and then select **Knowledge Base** > **Threat Descriptions**.