

# **F-Secure Anti-Virus 2013**



# Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Installation.....</b>                      | <b>5</b>  |
| Before you install for the first time.....               | 6         |
| Installing the product for the first time.....           | 6         |
| Installing and upgrading applications.....               | 6         |
| Help and Support.....                                    | 7         |
| <br>   |           |
| <b>Chapter 2: Getting started.....</b>                   | <b>9</b>  |
| How to use automatic updates.....                        | 10        |
| Check the update status.....                             | 10        |
| Change the Internet connection settings.....             | 10        |
| Check the status of Real-time Protection Network.....    | 11        |
| How to see what the product has done.....                | 11        |
| View notification history.....                           | 11        |
| Change the notification settings.....                    | 11        |
| Real-time Protection Network.....                        | 12        |
| What is Real-time Protection Network.....                | 12        |
| Real-time Protection Network benefits.....               | 12        |
| What data you contribute.....                            | 13        |
| How we protect your privacy.....                         | 14        |
| Becoming a Real-time Protection Network contributor..... | 14        |
| Questions about Real-time Protection Network.....        | 14        |
| How do I know that my subscription is valid.....         | 15        |
| Action center.....                                       | 15        |
| Activate a subscription.....                             | 15        |
| <br>   |           |
| <b>Chapter 3: Introduction.....</b>                      | <b>17</b> |
| View the overall status of my protection.....            | 18        |
| View the product statistics.....                         | 18        |
| Handle the product updates.....                          | 19        |
| View database versions .....                             | 19        |
| Change the mobile broadband settings.....                | 19        |
| What are viruses and other malware.....                  | 20        |
| Viruses.....   | 20        |
| Spyware.....   | 20        |
| Rootkits.....  | 21        |
| Riskware.....  | 21        |

|  |           |
|--|-----------|
| <b>Chapter 4: Protecting the computer against malware.....</b> | <b>23</b> |
| How to scan my computer.....                                   | 24        |
| Scan files automatically.....                                  | 24        |
| Scan files manually.....                                       | 26        |
| Scan e-mails.....  | 29        |
| View the scan results.....                                     | 29        |
| How to exclude files from the scan.....                        | 30        |
| Exclude file types.....  | 30        |
| Exclude files by location.....                                 | 30        |
| View excluded applications.....                                | 31        |
| How to use the quarantine.....                                 | 32        |
| View quarantined items.....                                    | 32        |
| Restore quarantined items.....                                 | 32        |
| What is DeepGuard.....   | 33        |
| Turn DeepGuard on or off.....                                  | 33        |
| Allow applications that DeepGuard has blocked.....             | 33        |
| Use DeepGuard in the compatibility mode.....                   | 34        |
| What to do with suspicious behavior warnings.....              | 34        |

## Installation

---

### Topics:

- *Before you install for the first time*
- *Installing the product for the first time*
- *Installing and upgrading applications*
- *Help and Support*

## Before you install for the first time

---

Thank you for choosing F-Secure.

To install the product, you need the following:

- The installation CD or an installation package. If you are using a netbook without a CD drive, you can download the installation package from [www.f-secure.com/netbook](http://www.f-secure.com/netbook).
- Your subscription key.
- An Internet connection.

If you have a security product from another vendor, the installer will attempt to remove it automatically. If this does not happen, please remove it manually.

 **Note:** If you have more than one account on the computer, log on with administrator privileges when installing.

## Installing the product for the first time

---

Instructions to install the product.

Follow these instructions to install the product:

1. Insert the CD or double-click the installer you downloaded.

If the CD does not start automatically, go to Windows Explorer, double-click on the CD-ROM icon and double-click the installation file to start the installation.

2. Follow the instructions on the screen.

- If you purchased the product on a CD from a shop, you can find the subscription key on the cover of the Quick Installation Guide.
- If you downloaded the product from the F-Secure eStore, the subscription key is included in the confirmation e-mail of the purchase order.

Your computer may need to restart before validating your subscription and downloading the latest updates from the Internet. If you are installing from the CD, please remember to remove the Installation CD before you restart your computer.

## Installing and upgrading applications

---

Instructions to activate your new subscription.

Follow these instructions to activate your new subscription or to install a new application using the launch pad:

 **Note:** You can find the launch pad icon on the Windows system tray.

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select **View my subscriptions**.
3. Under **My subscriptions**, go to the **Subscription status** page, and click **Activate subscription**.  
The **Activate subscription** window opens.

4. Enter your subscription key for the application, and click **OK**.
5. After your subscription is validated and activated, click **Close**.
6. Under **My subscriptions**, go to the **Installation status** page. If the installation does not start automatically, follow these instructions:
  - a) Click **Install**.  
The installation window opens.
  - b) Click **Next**.  
The application is downloaded, and the installation starts.
  - c) When the installation is complete, click **Close**.

The new subscription has been activated.

## Help and Support

---

You can access the product help online by clicking the Help icon or by pressing **F1** in any screen of the product.

After you register your license, you are entitled to additional services such as free product updates and product support. You can register at [www.f-secure.com/register](http://www.f-secure.com/register).



## Getting started

---

### Topics:

- [How to use automatic updates](#)
- [How to see what the product has done](#)
- [Real-time Protection Network](#)
- [How do I know that my subscription is valid](#)

Information about how to get started with the product.

This section describes how to change common settings and manage your subscriptions through the launch pad.

The launch pad's common settings are settings that apply to all of the programs installed on the launch pad. Instead of changing the settings separately in each program, you can simply edit the common settings, which are then used by all of the installed programs.

The launch pad's common settings include:

- Downloads, where you can view information about what updates have been downloaded and manually check if new updates are available.
- Connection settings, where you can change how your computer connects to the Internet.
- Notifications, where you can view past notifications and set what kind of notifications you want to see.
- Privacy settings, where you can select whether or not your computer is allowed to connect to the Real-time Protection Network.

You can also manage your subscriptions for installed programs through the launch pad.

## How to use automatic updates

---

Automatic updates keeps the protection on your computer updated.

The product retrieves the latest updates to your computer when you are connected to the Internet. It detects the network traffic and does not disturb other Internet use even with a slow network connection.

### Check the update status

View the date and time of the latest update.

When automatic updates are turned on, the product receives the latest updates automatically when you are connected to the Internet.

To make sure that you have the latest updates:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.

2. Select **Open common settings**.

3. Select **Automatic updates > Downloads**.

4. Click **Check now**.

The product connects to the Internet and checks for the latest updates. If the protection is not up-to-date, it retrieves the latest updates.

 **Note:** If you are using a modem, or have an ISDN connection to the Internet, the connection must be active to check for updates.

### Change the Internet connection settings

Usually there is no need to change the default settings, but you can configure how the server is connected to the Internet so that you can receive updates automatically.

To change the Internet connection settings:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.

2. Select **Open common settings**.

3. Select **Automatic updates > Connection**.

4. On the **Internet connection** list, select how your computer is connected to the Internet.

- Select **Assume always connected** if you have a permanent network connection.

 **Note:** If your computer does not actually have the permanent network connection and is set up for dial-on-demand, selecting **Assume always connected** can result in multiple dial-ups.

- Select **Detect connection** to retrieve updates only when the product detects an active network connection.
- Select **Detect traffic** to retrieve updates only when the product detects other network traffic.

 **Tip:** If you have an uncommon hardware configuration that causes the **Detect connection** setting to detect an active network connection even when there is none, select **Detect traffic** instead.

5. On the **HTTP proxy** list, select whether or not your computer uses a *proxy server* to connect to the Internet.

- Select **No HTTP proxy** if your computer is connected to the Internet directly.

- Select **Manually configure HTTP proxy** to configure the *HTTP proxy* settings.
- Select **Use my browser's HTTP proxy** to use the same *HTTP proxy* settings that you have configured in your web browser.

## Check the status of Real-time Protection Network

To function properly, many product features depend on the Real-time Protection Network connectivity.

If there are network problems or if your firewall blocks Real-time Protection Network traffic, the status is 'disconnected'. If no product features are installed that require access to Real-time Protection Network, the status is 'not in use'.

To check the status:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Automatic updates > Connection**.

Under **Real-time Protection Network**, you can see the current status of Real-time Protection Network.

## How to see what the product has done

---

You can see what actions the product has taken to protect your computer on the **Notifications** page.

The product will show a notification when it takes an action, for example when it finds a virus that it blocks. Some notifications may also be sent by your service provider, for example to let you know about new services that are available.

## View notification history

You can see what notifications have been displayed in the notification history

To view the notification history:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Other > Notifications**.
4. Click **Show notification history**.  
The notification history list opens.

## Change the notification settings

You can select what type of notifications you want the product to display.

To change the notification settings:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Other > Notifications**.
4. Select or clear **Allow program messages** to turn program messages on or off.

When this setting is turned on, the product will show notifications from the installed programs.

5. Select or clear **Allow promotional messages** to turn promotional messages on or off.
6. Click **OK**.

## Real-time Protection Network

---

This document describes Real-time Protection Network, an online service from F-Secure Corporation that identifies clean applications and web sites while providing protection against malware and web site exploits.

### What is Real-time Protection Network

Real-time Protection Network is an online service which provides rapid response against the latest Internet-based threats.

As a contributor to Real-time Protection Network, you can help us to strengthen the protection against new and emerging threats. Real-time Protection Network collects statistics of certain unknown, malicious or suspicious applications and what they do on your device. This information is anonymous and sent to F-Secure Corporation for combined data analysis. We use the analyzed information to improve the security on your device against the latest threats and malicious files.

#### How Real-time Protection Network works

As a contributor to Real-time Protection Network, you can provide information on unknown applications and web sites and on malicious applications and exploits on web sites. Real-time Protection Network does not track your web activity or collect information on web sites that have been analyzed already, and it does not collect information on clean applications that are installed on your computer.

If you do not want to contribute this data, Real-time Protection Network does not collect information of installed applications or visited web sites. However, the product needs to query F-Secure servers for the reputation of applications, web sites, messages and other objects. The query is done using a cryptographic checksum where the queried object itself is not sent to F-Secure. We do not track data per user; only the hit counter of the file or web site is increased.

It is not possible to completely stop all network traffic to Real-time Protection Network, as it is integral part of the protection provided by the product.

### Real-time Protection Network benefits

With Real-time Protection Network, you will have faster and more accurate protection against the latest threats and you will not receive unnecessary alerts for suspicious applications which are not malicious.

As a contributor to Real-time Protection Network, you can help us to find new and undetected malware and remove possible false positives from our virus definition database.

All participants in Real-time Protection Network help each other. When Real-time Protection Network finds a suspicious application on your device, you benefit from the analysis results when the same application has been found on other devices already. Real-time Protection Network improves the overall performance of your device, as the installed security product does not need to scan any applications that Real-time Protection Network has already analyzed and found clean. Similarly, information about malicious websites and unsolicited bulk messages is shared through Real-time Protection Network, and we are able to provide you with more accurate protection against web site exploits and spam messages.

The more people that contribute to Real-time Protection Network, the better individual participants are protected.

## What data you contribute

As a contributor to Real-time Protection Network, you provide information on applications stored on your device and the web sites that you visit so that Real-time Protection Network can provide the protection against the latest malicious applications and suspicious web sites.

### Analyzing the file reputation

Real-time Protection Network collects information only on applications that do not have a known reputation and on files that are suspicious or known to be malware.

Real-time Protection Network collects anonymous information of clean and suspicious applications on your device. Real-time Protection Network collects information of executable files only (such as Portable Executable files on the Windows platform, which have .cpl, .exe, .dll, .ocx, .sys, .scr, and .drv file extensions).

Collected information includes:

- the file path where the application is in your device,
- the size of the file and when it was created or modified,
- file attributes and privileges,
- file signature information,
- the current version of the file and the company that created it,
- the file origin or its download URL,
- F-Secure DeepGuard and anti-virus analysis results of scanned files, and
- other similar information.

Real-time Protection Network never collects any information of your personal documents, unless they have found to be infected. For any type of malicious file, it collects the name of the infection and the disinfection status of the file.

With Real-time Protection Network, you can also submit suspicious applications for analysis. Applications that you submit include Portable Executable files only. Real-time Protection Network never collects any information of your personal documents and they are never automatically uploaded for analysis.

### Submitting files for analysis

With Real-time Protection Network, you can also submit suspicious applications for analysis.

You can submit individual suspicious applications manually when the product prompts you to do so. You can only submit Portable Executable files. Real-time Protection Network never uploads your personal documents.

### Analyzing the web site reputation

Real-time Protection Network does not track your web activity or collect information on web sites that have been analyzed already. It makes sure that visited web sites are safe as you browse the web. When you visit a web site, Real-time Protection Network checks its safety and notifies you if the site is rated as suspicious or harmful.

If the web site that you visit contains malicious or suspicious content or a known exploit, Real-time Protection Network collects the whole URL of the site so that the web page content can be analyzed.

If you visit a site that has not been rated yet, Real-time Protection Network collects domain and subdomain names, and in some cases the path to the visited page, so that the site can be analyzed and rated. All the URL parameters that are likely to contain information that can be linked to you in a personally identifiable format are removed to protect your privacy.

- 👉 **Note:** Real-time Protection Network does not rate or analyze web pages in private networks, so it never collects any information on private IP network addresses (for example, corporate intranets).

### Analyzing the system information

Real-time Protection Network collects the name and version of your operating system, information about the Internet connection and the Real-time Protection Network usage statistics (for example, the number of times web site reputation has been queried and the average time for the query to return a result) so that we can monitor and improve the service.

## How we protect your privacy

We transfer the information securely and automatically remove any personal information that the data may contain.

Real-time Protection Network removes identifying data before sending it to F-Secure and it encrypts all collected information during the transfer to protect it from unauthorized access. The collected information is not processed individually; it is grouped with information from other Real-time Protection Network contributors. All data is analyzed statistically and anonymously, which means that no data will be connected to you in any way.

Any information that might identify you personally is not included in the collected data. Real-time Protection Network does not collect IP addresses or other private information, such as e-mail addresses, user names and passwords. While we make every effort to remove all personally identifiable data, it is possible that some identifying data remains in the collected information. In such cases, we will not seek to use such unintentionally collected data to identify you.

We apply strict security measures and physical, administrative and technical safeguards to protect the collected information when it is transferred, stored and processed. Information is stored in secured locations and on servers that are controlled by us, located either at our offices or at the offices of our subcontractors. Only authorized personnel can access the collected information.

F-Secure may share the collected data with its affiliates, sub-contractors, distributors and partners, but always in a non-identifiable, anonymous format.

## Becoming a Real-time Protection Network contributor

You help us to improve the Real-time Protection Network protection by contributing information of malicious programs and web sites.

You can choose to participate in Real-time Protection Network during the installation. With the default installation settings, you contribute data to Real-time Protection Network. You can change this setting later in the product.

Follow these instructions to change Real-time Protection Network settings:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Other > Privacy**.
4. Check the participation check box to become a Real-time Protection Network contributor.

## Questions about Real-time Protection Network

Contact information for any questions about Real-time Protection Network.

If you have any further questions about Real-time Protection Network, please contact:

---

F-Secure Corporation

Tammasaarekatu 7

PL 24

00181 Helsinki

Finland

[http://www.f-secure.com/en/web/home\\_global/support/contact](http://www.f-secure.com/en/web/home_global/support/contact)

---

The latest version of this policy is always available on our web site.

## How do I know that my subscription is valid

---

Your subscription type and status are shown on the [Subscription status](#) page.

When the subscription is about to expire or if your subscription has expired, the overall protection status of the program on the corresponding launchpad icon changes.

To check your subscription validity:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select [View my subscriptions](#).
3. Select [Subscription status](#) to view information about your subscriptions for installed programs.
4. Select [Installation status](#) to see what programs are available to be installed.

If your subscription has expired, you need to renew your subscription to continue receiving updates and using the product.

## Action center

The action center shows you any important notifications that require your attention.

If your subscription has expired or is about to expire, the action center notifies you of this. The background color and content of the action center message depends on your subscription type and status:

- If your subscription is about to expire, and there are free subscriptions available, the message has a white background and an [Activate](#) button.
- If your subscription is about to expire and there are no free subscriptions available, the message has a yellow background and [Buy](#) and [Enter key](#) buttons. If you have already bought a new subscription, you can click [Enter key](#) to provide the subscription key and activate your new subscription.
- If your subscription has expired, and there are free subscriptions available, the message has a red background and an [Activate](#) button.
- If your subscription has expired and there are no free subscriptions available, the message has a red background and [Buy](#) and [Enter key](#) buttons. If you have already bought a new subscription, you can click [Enter key](#) to provide the subscription key and activate your new subscription.

 **Note:** The [Show notification history](#) link on the action center shows a list of product notification messages, not earlier action center messages.

## Activate a subscription

When you have a new subscription key or campaign code for a product, you need to activate it.

To activate a subscription:

1. On the launch pad, right-click the right-most icon.  
A pop-up menu appears.
2. Select [View my subscriptions](#).

3. Choose one of the following:

- Click [Activate subscription](#).
- Click [Activate campaign code](#).

4. In the dialog box that opens, enter your new subscription key or campaign code and click **OK**.

-  **Tip:** If you received your subscription key by e-mail, you can copy the key from the e-mail message and paste it into the field.

After you have entered the new subscription key, the new subscription validity date is shown on the [Subscription status](#) page.

## Introduction

---

### Topics:

- [View the overall status of my protection](#)
- [View the product statistics](#)
- [Handle the product updates](#)
- [What are viruses and other malware](#)

This product protects your computer against viruses and other harmful applications.

The product scans files, analyzes applications and updates automatically. It does not require any actions from you.

## View the overall status of my protection

---

The **Status** page shows you a quick overview of installed product features and their current status.

To open the **Status** page:

On the main page, click **Status**.

The **Status** page opens.

The icons show you the status of the program and its security features.

| Status icon   | Status name | Description   |
|---|-------------|---|
|    | OK          | Your computer is protected. The feature is turned on, and working properly.   |
|    | Information | The product informs you about a special status of a feature.<br>For example, the feature is being updated.  |
|    | Warning     | Your computer is not fully protected.<br>For example, the product has not received updates in a long time, or the status of a feature requires attention. |
|  | Error       | Your computer is not protected.<br>For example, your subscription has expired or a critical feature is turned off.  |
|  | Off         | A non-critical feature is turned off.   |

---

## View the product statistics

---

You can see what the product has done since its installation in the **Statistics** page.

To open the **Statistics** page:

On the main page, click **Statistics**.

The **Statistics** page opens.

- **Last successful update check** shows the time of the latest update.
- **Virus and spyware scanning** shows how many files the product has scanned and cleaned since the installation.

- **Applications** shows how many programs DeepGuard has allowed or blocked since the installation.
- **Firewall connections** shows the number of allowed and blocked connections since the installation.
- **Spam and phishing filtering** shows how many e-mail messages the product has detected as valid e-mail messages and as spam messages.

## Handle the product updates

---

The product keeps the protection updated automatically.

### View database versions

You can see the latest update times and version numbers in the **Database updates** page.

To open the **Database updates** page:

1. On the main page, click **Settings**.

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

2. Select **Other settings > Database versions**.

The **Database versions** page displays the latest date when the virus and spyware definitions, DeepGuard, and spam and phishing filtering were updated and their version numbers.

### Change the mobile broadband settings

Select whether you want to download security updates when you use mobile broadband.

 **Note:** This feature is available only in Microsoft Windows 7.

By default, security updates are always downloaded when you are in your home operator's network. However, the updates are suspended when you visit another operator's network. This is because the prices of connections may vary between operators, for example, in different countries. You might consider keeping this setting unchanged, if you want to save bandwidth and possibly, also costs, during your visit.

 **Note:** This setting applies only to mobile broadband connections. When the computer is connected to a fixed or wireless network, the product is automatically updated.

To change the setting:

1. On the main page, click **Settings**.

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

2. Select **Other settings > Mobile broadband > Download security updates**.

3. Select the preferred update option for mobile connections:

- **Only in my home operator's network**

Updates are always downloaded in your home operator's network. When you visit another operator's network, the updates are suspended. We recommend that you select this option to keep your security product up to date at expected costs.

- **Never**

Updates are not downloaded when you use mobile broadband.

- **Always**

Updates are always downloaded, no matter what network you use. Select this option if you want to make sure that the security of your computer is always up to date regardless of the costs.

4. If you want to decide separately every time you exit your home operator's network, select [Ask me each time I leave my home operator's network](#).

### Suspended security updates

The security updates may be suspended when you use mobile broadband outside your home operator's network.

In this case, you can see the [Suspended](#) notification flyer in the lower right corner of your screen. The updates are suspended because the prices of connections may vary between operators, for example, in different countries. You might consider keeping this setting unchanged, if you want to save bandwidth and possibly, also costs, during your visit. However, if you still want to change the settings, click the [Change](#) link.

 **Note:**

This feature is available only in Microsoft Windows 7.

## What are viruses and other malware

---

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

Malware can:

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

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

### Viruses

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

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

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

### Spyware

Spyware are programs that collect your personal information.

Spyware may collect personal information including:

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

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

## Rootkits

Rootkits are programs that make other *malware* difficult to find.

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

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

## Riskware

Riskware is not designed specifically to harm your computer, but it may harm your computer if it is misused.

Riskware is not strictly speaking malware. Riskware programs perform some useful but potentially dangerous functions.

Examples of riskware programs are:

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

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

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



## Protecting the computer against malware

---

### Topics:

- [How to scan my computer](#)
- [How to exclude files from the scan](#)
- [How to use the quarantine](#)
- [What is DeepGuard](#)

Virus and spyware scanning protects the computer from programs that may steal personal information, damage the server, or use it for illegal purposes.

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

By default, Virus and spyware scanning scans your local hard drives, any removable media (such as portable drives or compact disks) and downloaded content automatically. You can set it to scan your e-mails automatically as well.

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

## How to scan my computer

---

When Virus and spyware scanning is turned on, it scans your computer for harmful files automatically. You can also scan files manually and set up scheduled scans.

We recommend that you keep Virus and spyware scanning is turned on all the time. Scan your files manually when you want to make sure that there are no harmful files on your computer or if want to scan files that you have excluded from the real-time scan.

By setting up a scheduled scan, Virus and spyware scanning removes harmful files from your computer at the specified times.

### Scan files automatically

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 that take a longer time to scan:

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

 **Note:** Compressed files are not scanned by default.

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.

### Turn real-time scanning on or off

Keep real-time scanning turned on to stop *malware* before it can harm your computer.

To turn real-time scanning on or off:

1. On the main page, click **Status**.
2. Click **Change settings on this page**.

 **Note:** You need administrative rights to turn off security features.

3. Turn **Virus and spyware scanning** on or off.
4. Click **Close**.

### Handle harmful files automatically

Real-time scanning can handle harmful files automatically without asking you any questions.

To let real-time scanning handle harmful files automatically:

1. On the main page, click **Settings**.

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

2. Select **Computer Security > Virus and spyware scanning**.
3. Select **Handle harmful files automatically**.

If you choose not to handle harmful files automatically, real-time scanning asks you what you want to do to a harmful file when it is found.

### Handle spyware

Virus and spyware scanning blocks spyware immediately when it tries to start.

Before a spyware application can start, the product blocks it and lets you decide what you want to do with it.

Choose one of the following actions when a spyware is found:

| Action to take                | What happens to the spyware   |
|-------------------------------|---|
| Handle automatically          | Let the product decide the best action to take based on the spyware that was found. |
| Quarantine the spyware        | Move the spyware to the quarantine where it cannot harm your computer.              |
| Delete the spyware            | Remove all spyware related files from your computer.                                |
| Only block the spyware        | Block the access to the spyware but leave it on your computer.                      |
| Exclude the spyware from scan | Allow spyware to run and exclude it from the scanning in the future.                |

### Handle riskware

Virus and spyware scanning blocks riskware immediately when it tries to start.

Before a riskware application can start, the product blocks it and lets you decide what you want to do with it.

Choose one of the following actions when a riskware is found:

| Action to take                 | What happens to the riskware  |
|--------------------------------|---|
| Only block the riskware        | Block the access to the riskware but leave it on your computer.         |
| Quarantine the riskware        | Move the riskware to the quarantine where it cannot harm your computer. |
| Delete the riskware            | Remove all riskware related files from your computer.                   |
| Exclude the riskware from scan | Allow riskware to run and exclude it from the scanning in the future.   |

### Remove tracking cookies automatically

By removing tracking cookies, you stop web sites from being able to track the sites you visit on the Internet.

Tracking cookies are small files that allow web sites to record what web sites you visit. Follow these instructions to keep tracking cookies off your computer.

1. On the main page, click **Settings**.

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

2. Select **Computer Security > Virus and spyware scanning**.
3. Select **Remove tracking cookies**.
4. Click **OK**.

## Scan files manually

You can scan your files manually, for example when you connect an external device to your computer, to make sure they do not contain any malware.

### Starting the manual scan

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

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

To start manually scanning your computer:

1. On the main page, click the arrow under **Scan**.  
The scanning options are shown.
2. Select the type of scan.  
Select **Change scanning settings** to optimize how the manual scanning scans your computer for viruses and other harmful applications.
3. If you selected **Choose what to scan**, a window opens in which you can select which location to scan.  
The **Scan Wizard** opens.

### Types of scan

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

The following lists the different types of scan:

| Scan type              | What is scanned  | When to use this type  |
|------------------------|--|--|
| Virus and spyware scan | Parts of your computer for viruses, spyware and riskware   | This type of scan is much quicker than a full scan. It searches only the parts of your system that contain installed program files. This scan type is recommended if you want to quickly check whether your computer is clean, because it is able to efficiently find and remove any active malware on your computer.  |
| Full computer scan     | Your entire computer (internal and external hard drives) for viruses, spyware and riskware   | When you want to be completely sure that there is no malware or riskware on your computer. This type of scan takes the longest time to complete. It combines the quick malware scan and the hard drive scan. It also checks for items that are possible hidden by a rootkit.   |
| Choose what to scan    | A specific file, folder or drive for viruses, spyware and riskware   | When you suspect that a specific location on your computer may have malware, for example, the location contains downloads from potentially dangerous sources, such as peer-to-peer file sharing networks. Time the scan will take depends of the size of the target that you scan. The scan completes quickly if, for example, you scan a folder that contains only a few small files. |
| Rootkit scan           | Important system locations where a suspicious item may mean a security problem. Scans for hidden files, folders, drives or processes | When you suspect that a rootkit may be installed on your computer. For example, if malware was recently detected in your computer and you want to make sure that it did not install a rootkit.   |

## Scan in Windows Explorer

You can scan disks, folders and files for *viruses*, *spyware* and *riskware* in Windows Explorer.

To scan a disk, folder or file:

1. Place your mouse pointer on and right-click the disk, folder or file you want to scan.
2. From the right-click menu, select **Scan Folders for Viruses** (the option name depends on whether you are scanning a disk, folder or file).  
The **Scan Wizard** window opens and the scan starts.

If a *virus* or *spyware* is found, the **Scan Wizard** guides you through the cleaning stages.

## Select files to scan

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

1. On the main page, click **Settings**.

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

2. Select **Other settings > Manual scanning**.

3. Under **Scanning options**, select from the following settings:

**Scan only known file types** To scan only those file types that are most likely to have infections, for example, executable files. Selecting this option also makes the scanning faster. The files with the following extensions are scanned: .ani, .asp, .ax, .bat, .bin, .boo, .chm, .cmd, .com, .cpl, .dll, .doc, .dot, .drv, .eml, .exe, .hlp, .hta, .htm, .html, .htt, .inf, .ini, .job, .js, .jse, .lnk, .lsp, .mdb, .mht, .mpp, .mpt, .msg, .ocx, .pdf, .php, .pif, .pot, .ppt, .rtf, .scr, .shs, .swf, .sys, .td0, .vbe, .vbs, .vxd, .wbk, .wma, .wmv, .wmf, .wsc, .wsf, .wsh, .wri, .xls, .xlt, .xml, .zip, .jar, .arj, .lzh, .tar, .tgz, .gz, .cab, .rar, .bz2, and .hqx.

**Scan inside compressed files** To scan archive files and folders.

**Use advanced heuristics** To use all available heuristics during the scan to better find new or unknown malware.

 **Note:** If you select this option, the scanning takes longer, and can result in more false positives (harmless files reported as suspicious).

4. Click **OK**.

 **Note:** Excluded files on the excluded items list are not scanned even if you select them to be scanned here.

## What to do when harmful files are found

Select how you want to handle harmful files when they are found.

To select the action to take when harmful content is found during the manual scanning:

1. On the main page, click **Settings**.

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

2. Select **Other settings > Manual scanning**.

3. In **When virus or spyware is found**, choose of of the following options:

| Option                      | Description  |
|-----------------------------|--|
| <b>Ask me (default)</b>     | You can select the action to take for every item that is found during manual scanning.   |
| <b>Clean the files</b>      | The product tries to automatically disinfect infected files that are found during manual scanning.<br><br> <b>Note:</b> If the product cannot clean the infected file, it is quarantined (except when found on network or removable drives), so it cannot harm the computer.    |
| <b>Quarantine the files</b> | The product moves any harmful files that are found during manual scanning to the quarantine where they cannot harm the computer.   |
| <b>Delete the files</b>     | The product deletes any harmful files that are found during manual scanning.   |
| <b>Report only</b>          | The product leaves any harmful files that are found during during manual scanning as they are and records the detection in the scan report.<br><br> <b>Note:</b> If real-time scanning is turned off, any malware is still able to harm the computer if you select this option. |

 **Note:** When harmful files are found during scheduled scanning, they are cleaned automatically.

## Schedule a scan

Set your computer to scan and remove viruses 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. On the main page, click **Settings**.

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

2. Select **Other settings > Scheduled scanning**.

3. Turn **Scheduled scanning** on.

4. Select when you would like the scan to start.

| Option         | Description  |
|----------------|--|
| <b>Daily</b>   | Scan your computer every day.  |
| <b>Weekly</b>  | Scan your computer on selected days of the week. Select the days from the list.  |
| <b>Monthly</b> | Scan your computer on selected days of the month. To select the days: <ol style="list-style-type: none"> <li>1. Select one of the <b>Day</b> options.</li> <li>2. Select the day of the month from the list next to the selected day.</li> </ol> |

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

| Option                                | Description  |
|---------------------------------------|--|
| <b>Start time</b>                     | Start the scan at the specified time.  |
| <b>After computer is not used for</b> | Start the scan after you have not used your computer for the specified period of time. |

Scheduled scanning uses the manual scanning settings when it scans your computer, except that it scans archives every time and cleans harmful files automatically.

## Scan e-mails

E-mail scanning protects you against getting harmful files in e-mails that are sent to you.

Virus and spyware scanning must be turned on to scan e-mails for viruses.

To turn e-mail scanning on:

1. On the main page, click **Settings**.

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

2. Select **Computer Security > Virus and spyware scanning**.
3. Select **Remove harmful e-mail attachments**.
4. Click **OK**.

## When are e-mail messages and attachments scanned

Virus and spyware scanning can remove harmful content from e-mails that you receive.

Virus and spyware scanning removes harmful e-mail messages that are received by e-mail programs, such as Microsoft Outlook and Outlook Express, Microsoft Mail, or Mozilla Thunderbird. It scans unencrypted e-mail messages and attachments every time your e-mail program receives them from the mail server using POP3 protocol.

Virus and spyware scanning cannot scan e-mail messages in webmail, which include e-mail applications that run in your web browser, such as Hotmail, Yahoo! mail, or Gmail. You are still protected against *viruses* even if you do not remove harmful attachments or you are using webmail. When you open e-mail attachments, real-time scanning removes any harmful attachments before they can cause harm.

 **Note:** Real-time scanning protects only your computer, but not your friends. Real-time scanning does not scan attached files unless you open the attachment. This means that if you are using webmail and you forward a message before opening its attachment, you may forward an infected e-mail to your friends.

## View the scan results

Virus and spyware history displays all harmful files that the product has found.

Sometimes, the product cannot perform the action you have selected when something harmful is found. For example, if you select to clean files and a file cannot be cleaned, the product moves it to quarantine. You can view this information in the virus and spyware history.

To view the history:

1. On the main page, click **Settings**.

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

2. Select **Computer Security > Virus and spyware scanning**.
3. Click **View removal history**.

The virus and spyware history displays the following information:

- date and time when the harmful file was found,
- the name of the malware and its location on your computer, and
- the performed action.

## How to exclude files from the scan

Sometimes you may want to exclude some files or applications from the scan. Excluded items are not scanned unless you remove them from the excluded items list.

-  **Note:** Exclusion lists are separate for real-time and manual scanning. For example, if you exclude a file from the real-time scan, it is scanned during the manual scan unless you exclude it from the manual scan as well.

### Exclude file types

When you exclude files by their type, files with specified extensions are not scanned for harmful content.

To add or remove file type that you want to exclude:

1. On the main page, click **Settings**.
  -  **Note:** You need administrative rights to change the settings.
2. Choose whether you want to exclude the file type from real-time or manual scanning:
  - Select **Computer Security > Virus and spyware scanning** to exclude the file type from real-time scanning.
  - Select **Other settings > Manual scanning** to exclude the file type from manual scanning.
3. Click **Exclude files from the scan**.
4. To exclude a file type:
  - a) Select the **File Types** tab.
  - b) Select **Exclude files with these extensions**.
  - c) Type a file extension that identifies the type of files that you want to exclude, in the field next to the **Add** button.
 

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

For example, to exclude executable files, type `exe` in the field.
  - d) Click **Add**.
5. Repeat the previous step for any other extension you want to be excluded from being scanned for viruses.
6. Click **OK** to close the **Exclude from scanning** dialog box.
7. Click **OK** to apply the new settings.

The selected file types are excluded from the future scans.

### Exclude files by location

When you exclude files by location, files in specified drives or folders are not scanned for harmful content.

To add or remove file locations that you want to exclude:

1. On the main page, click **Settings**.
  -  **Note:** You need administrative rights to change the settings.
2. Choose whether you want to exclude the location from real-time or manual scanning:
  - Select **Computer > Virus and spyware scanning** to exclude the location from real-time scanning.
  - Select **Computer > Manual scanning** to exclude the location from manual scanning.

3. Click **Exclude files from the scan**.
4. To exclude a file, drive, or folder:
  - a) Select the **Objects** tab.
  - b) Select **Exclude objects (files, folders, ...)**.
  - c) Click **Add**.
  - d) Select the file, drive, or folder that you want to exclude from virus scanning.
 

 **Note:** Some drives may be removable drives, such as CD, DVD or network drives. Network drives and empty removable drives cannot be excluded.
  - e) Click **OK**.
5. Repeat the previous step to exclude other files, drives, or folders from being scanned for viruses.
6. Click **OK** to close the **Exclude from scanning** dialog box.
7. Click **OK** to apply the new settings.

The selected files, drives or folders are excluded from the future scans.

## 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 real-time or manual scanning detects an application that behaves like spyware or riskware but you know it to be safe, 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 malicious software, it cannot be excluded.

You cannot exclude applications directly. New applications appear on the exclusion list only if you exclude them during scanning.

To view the applications that are excluded from scanning:

1. On the main page, click **Settings**.
 

 **Note:** You need administrative rights to change the settings.
2. Choose whether you want to view applications that have been excluded from real-time or manual scanning:
  - Select **Computer > Virus and spyware scanning** to view applications that have been excluded from real-time scanning.
  - Select **Computer > Manual scanning** to view applications that have been excluded from manual scanning.
3. Click **Exclude files from the scan**.
4. Select the **Applications** tab.
 

 **Note:** Only spyware and riskware applications can be excluded, not viruses.
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**.
6. Click **OK** to close the **Exclude from scanning** dialog box.
7. Click **OK** to exit.

## How to use the quarantine

---

Quarantine is a safe repository for files that may be harmful.

Quarantined files cannot spread or cause harm to your computer.

The product can quarantine *malware*, *spyware*, and *riskware* 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.

- In general, you can delete quarantined *malware*.
- In most cases, you can delete quarantined *spyware*. It is possible that the quarantined *spyware* is part of a legitimate software program and removing it stops the actual program from working correctly. If you want to keep the program on your computer, you can restore the quarantined *spyware*.
- Quarantined *riskware* can be a legitimate software program. If you have installed and set up the program by yourself, you can restore it from the quarantine. If the *riskware* is installed without your knowledge, it is most likely installed with malicious intent and should be deleted.

### View quarantined items

You can view more information on items in the quarantine.

To view information on items in the quarantine:

1. On the main page, click [Settings](#).

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

2. Select [Computer Security](#) > [Virus and spyware scanning](#).

3. Click [View quarantine](#).

The [Quarantine](#) page shows the total number of items stored in quarantine.

4. To view detailed information on items in the quarantine, click [Details](#).

You can sort the content either by malware name or file path.

A list of the first 100 items is shown with the type of the quarantined items, their name, and the path where the files were installed.

5. To view more information on a quarantined item, click the  icon next to the item on the [State](#) column.

### Restore quarantined items

You can restore the quarantined items that you need.

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

To restore quarantined items:

1. On the main page, click [Settings](#).

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

2. Select [Computer Security](#) > [Virus and spyware scanning](#).

3. Click [View quarantine](#).

4. Select the quarantined items that you want to restore.

5. Click [Restore](#).

## What is DeepGuard

---

DeepGuard analyzes the content of files and behavior of applications, and monitors applications that are not trusted.

DeepGuard blocks new and undiscovered *viruses*, *worms*, and other harmful applications that try to make changes to your computer, and prevents suspicious applications from accessing the Internet.

When DeepGuard detects a new application that tries to make potentially harmful changes to the system, it allows the application to run in a safe-zone. In the safe-zone, the application cannot harm your computer. DeepGuard analyzes what changes the application tried to make, and based on this, it decides how likely the application is to be *malware*. If the application is likely to be *malware*, DeepGuard blocks it.

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.

## Turn DeepGuard on or off

Keep DeepGuard turned on to prevent suspicious applications from making potentially harmful system changes in your computer.

If you have Windows XP, make sure you have Service Pack 2 installed before you turn DeepGuard on.

To turn DeepGuard on or off:

1. On the main page, click [Status](#).
2. Click [Change settings on this page](#).

 **Note:** You need administrative rights to turn off security features.

3. Turn [DeepGuard](#) on or off.
4. Click [Close](#).

## 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. On the main page, click [Tools](#).
2. Click [Applications](#).  
The [Monitored applications](#) list is shown.
3. Find the application that you want to allow.

 **Note:** You can click column headings to sort the list. For example, click the [Permission](#) column to sort the list into groups of allowed and denied programs.

4. Select **Allow** in the **Permission** column.
5. Click **Close**.

DeepGuard allows the application to make system changes again.

## Use DeepGuard in the compatibility mode

For maximum protection, DeepGuard temporarily modifies running programs. Some programs check that they are not corrupted or modified and may not be compatible with this feature. For example, online games with anti-cheating tools check that they have not been modified in any way when they are run. In these cases, you can turn on the compatibility mode.

To turn on the compatibility mode:

1. On the main page, click **Settings**.

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

2. Select **Computer Security** > **DeepGuard**.
3. Select **Use the compatibility mode**.
4. Click **OK**.

## What to do with suspicious behavior warnings

DeepGuard monitors applications that are not trusted. If a monitored application tries to access the Internet, tries to make changes to your system, or behaves suspiciously, DeepGuard blocks it.

When you have selected **Warn me about suspicious behavior** in DeepGuard settings, DeepGuard notifies you when it detects a potentially harmful application or when you start an application that has an unknown reputation.

To decide what you want to do with the application that DeepGuard has blocked:

1. Click **Details** to view more information about the program.

The details section shows you:

- the location of the application,
- the reputation of the application in Real-time Protection Network, and
- how common the application is.

2. Decide whether you trust the application that DeepGuard has blocked:

- Choose **I trust the application. Let it continue**, if you do not want to block the application.

The application is more likely to be safe if:

- DeepGuard blocked the application as a result of something you did,
- you recognize the application, or
- you got the application from a trusted source.

- Choose **I do not trust the application. Keep it blocked**, if you want to keep the application blocked.

The application is more likely to be unsafe if:

- the application is uncommon,
- the application has unknown reputation, or
- you do not know the application.

3. If you want to submit a suspicious application for analysis:

- a) Click **Report the application to F-Secure**.  
The product displays the submission conditions.
- b) Click **Accept** if you agree with the conditions and want to submit the sample.

We recommend that you send a sample when:

- DeepGuard blocks an application that you know to be safe, or
- you suspect that the application may be *malware* .

