Internet Security 2015

Contents

Installation

Topics:

1.1 Before you install for the first time

Thank you for choosing our product.

To install the product, you need the following:

- The installation CD or an installation package.
- 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.

1.2 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.

1.3 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. Right-click the product icon in the system tray.
   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.

1.4 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.

Getting started

Topics:

Information about how to get started with the product.

This section describes how to change common settings and manage your subscriptions for the product.

The 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.
- Subscriptions for the programs that are installed.

2.1 Where can I find my account ID?

Our customer support may ask for your account ID if you need to contact us.

To view your account and device identity codes:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **View my subscriptions**.
3. Select **Identity codes**.

The page shows your account and the current device identity codes that you can use to manage your subscriptions.

2.2 How to use the action center

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

If the action center has any pending actions, it reminds you of them periodically.

2.2.1 Open the action center

Open the action center to view all notifications that require your attention.

To open the action center:

1. Right-click the product icon in the system tray.
   The **Open action center** item in the pop-up menu shows how many pending actions you have.
2. Select **Open action center**.
   The action center shows a list of all items that need to be solved.
3. Click the item in the list to see more information about it.
4. If you do not want to do anything to any unsolved item at the moment, click **Postpone** to solve it later.

> **Note:** If you have multiple items in the action center, click **Postpone all** to close the action center and solve all items later.

2.2.2 Install a product upgrade

When a free upgrade to a product that you have installed is available, you need to install it to take the new version into use.

To upgrade the product:

1. Open the action center.
   The action center shows **Product upgrade available** item. If you have multiple items in the action center, click the item to open it.
2. Click **Upgrade**.

> **Note:** You need to accept new license terms to upgrade the product if they have changed.

When the upgrade is complete, you may need to restart your computer.

2.2.3 Install a new product

If a new product is added to your subscription, you can install it to take it into use.

New products can be added to your subscription while it is still valid.

To install a new product:

1. Open the action center.
   The action center shows **Install new product** item. If you have multiple items in the action center, click the item to open it.

2. Click **Install**.

   Note: If you do not want to install the product, you can click the trashcan icon in the top-right corner to close the reminder and to remove it from the action center.

3. Follow the instructions in the setup wizard to install the product.

When the installation is complete, you may need to restart your computer.

2.2.4 Replace an expiring product

If your subscription is expiring and your currently installed product is no longer available, you cannot continue your subscription, but you can upgrade to the new product for free.

To upgrade the product:

1. Open the action center.
   The action center shows **Upgrade product** item. If you have multiple items in the action center, click the item to open it.
2. Click **Upgrade**.

When the upgrade is complete, you may need to restart your computer.

2.3 How do I know that my subscription is valid

Your subscription type and status are shown on the **Subscriptions** page.

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

To check your subscription validity:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **View my subscriptions**.
3. Select one of the following options:
   - Select **Subscriptions** to view information about your subscriptions for installed programs.
   - Select **Installation** 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.

2.3.1 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. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **View my subscriptions**.
3. Click **Add new subscription**.
4. In the dialog box that opens, enter your new subscription key or campaign code and click **Validate**.

   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 **Subscriptions** page.

2.3.2 Renew your subscription

When the product subscription is about to expire, you need to renew it to keep using the product.

To renew your subscription:

1. Open the action center.
   The action center shows **Renew subscription** item. If you have multiple items in the action center, click the item to open it.
2. You need a new subscription key to renew your subscription.
   - If you already have an available subscription that you can use for this computer, click **Activate** to take the new subscription into use.
   - If you have purchased a new subscription key already, click **Enter key**.

     In the dialog box that opens, enter your new subscription key and click **OK**.
   - Otherwise, click **Renew now**.

     You can renew your subscription in our online store. When you renew your subscription, you receive a new subscription key.

If you do not want to renew your subscription, uninstall the product with the expired subscription.

2.4 How to use automatic updates

Automatic updates keep your computer protected from the latest threats.

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

2.4.1 Check the update status

View the date and time of the latest update.

Usually, you do not need to check the updates by yourself as the product receives the latest updates automatically when you are connected to the Internet and automatic updates are turned on.

To make sure that you have the latest updates:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Downloads**.
4. Click **Check now**.
   The product retrieves the latest updates if there are any.

Note: Your Internet connection must be active when you want to check for the latest updates.

2.4.2 Change the Internet connection settings

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

To change the Internet connection settings:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **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.

2.4.3 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 and later versions of Windows.

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. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Connection**.
4. Select the preferred update option for mobile connections:

   - **Never**

     Updates are not downloaded when you use mobile broadband.
   - **Only in my operator 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.
   - **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.

     Note: If you want to decide separately every time you exit your home operator's network, select **Ask before roaming in a new 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 and later versions of Windows.

2.5 How to see what the product has done

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

The product shows a notification when it takes an action, for example to protect files that are stored on your computer. Some notifications may also be sent by your service provider, for example to let you know about new services that are available.

To view the product timeline:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Click **Open product timeline**.
   The product timeline's list of notifications opens.

2.6 Gaming mode

Turn on the *gaming mode* when you want to free up system resources while playing computer games.

Computer games often require a lot of system resources to run smoothly. When you have other applications running in the background while you play a game, they degrade the performance of the game as they consume system resources and use your network.

The *gaming mode* reduces the product's impact on your computer and reduces its network use. This way, it frees up more system resources for computer games while still maintaining the essential functionality of the product. For example, it suspends automatic updates, scheduled scans and other operations that may need a lot of system resources and network traffic.

When you use any full-screen application, for example when you are viewing a presentation, slideshow or video, or play a game in full-screen mode, we show only critical notifications if they require your immediate attention. Other notifications are only shown when you exit the full-screen or *gaming mode*.

2.6.1 Turn gaming mode on

Turn the *gaming mode* on to improve the performance of games on your computer.

To turn the *gaming mode* on:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Gaming mode**.
   The product's use of system resources is now optimized so that games can run smoothly on your computer.

Remember to turn off the *gaming mode* after you stop playing the game. The *gaming mode* turns off automatically when you restart your computer or when it returns from sleep mode.

Security Cloud

Topics:

This document describes *Security Cloud*, an online service from F-Secure Corporation that identifies clean applications and web sites while providing protection against malware and web site exploits.

3.1 What is *Security Cloud*

Security Cloud is an online service which provides rapid response against the latest Internet-based threats.

As a contributor, you allow *Security Cloud* to collect data that helps us to strengthen your protection against new and emerging threats. *Security Cloud* collects information on certain unknown, malicious or suspicious applications and unclassified web sites. This information is anonymous and sent to F-Secure Corporation for combined data analysis. We use the analyzed information to improve your protection against the latest threats and malicious files.

How *Security Cloud* works

Security Cloud collects information on unknown applications and web sites and on malicious applications and exploits on web sites. *Security Cloud* 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, *Security Cloud* 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 *Security Cloud*, as it is integral part of the protection provided by the product.

3.1.1 Check the status of *Security Cloud*

To function properly, many product features depend on the *Security Cloud* connectivity.

If there are network problems or if your firewall blocks *Security Cloud* traffic, the status is 'disconnected'. If no product features are installed that require access to *Security Cloud*, the status is 'not in use'.

To check the status:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Connection**.

Under **Security Cloud** , you can see the current status of *Security Cloud*.

3.2 *Security Cloud* benefits

With *Security Cloud*, 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 *Security Cloud*, you can help us to find new and undetected malware and remove possible false positive ratings.

All participants in *Security Cloud* help each other. When *Security Cloud* finds a suspicious application, you benefit from the analysis results if the same application has already been found by someone else. *Security Cloud* improves overall performance, as the installed security product does not need to scan any applications that *Security Cloud* has already analyzed and found clean. Similarly, information about malicious websites and unsolicited bulk messages is shared through *Security Cloud*, and we are able to provide you with more accurate protection against web site exploits and spam messages.

The more people that contribute to *Security Cloud*, the better individual participants are protected.

3.3 What data you contribute

As a contributor, you allow *Security Cloud* to collect information on applications that you have installed and the web sites that you visit so that *Security Cloud* can provide better protection against the latest malicious applications and suspicious web sites.

Analyzing the file reputation

Security Cloud collects information only on applications that do not have a known reputation and on files that are suspicious or known to be malware.

Only information on application (executable) files is collected, not on any other file types.

Depending on the product, the collected information can include:

- the file path of the application (excluding any personally identifiable information),
- 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 (excluding any personally identifiable information),
- F-Secure DeepGuard and anti-virus analysis results of scanned files, and
- other similar information.

Security Cloud 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.

Submitting files for analysis

In some products, you can also submit suspicious applications to *Security Cloud* for analysis.

You can submit individual suspicious applications manually when the product prompts you to do so, or you can turn on the automatic upload of suspicious applications in the product settings. *Security Cloud* never uploads your personal documents.

Analyzing the web site reputation

Security Cloud does not track your web activity. It makes sure that visited web sites are safe as you browse the web. When you visit a web site, *Security Cloud* checks its safety and notifies you if the site is rated as suspicious or harmful.

In order to improve the service and maintain a high rating accuracy, *Security Cloud* may collect information about visited web sites. Information is collected if the site that you visit contains malicious or suspicious content or a known exploit, or if the content on the site has not yet been rated or categorized. Collected information includes the URL and meta data related to the visit and the web site.

Security Cloud has strict controls to ensure that no private data is sent. The number of collected URLs is limited. Any submitted data is filtered for privacy-related information before it is sent, and all fields that are likely to contain information that may be linked to you in a personally identifiable format are removed. *Security Cloud* does not rate or analyze web pages in private networks, and it never collects any information on private network addresses or aliases.

Analyzing the system information

Security Cloud collects the name and version of your operating system, information about the Internet connection and the *Security Cloud* 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.

3.4 How we protect your privacy

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

The collected information is not processed individually; it is grouped with information from other *Security Cloud* 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. *Security Cloud* 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.

3.5 Becoming a *Security Cloud* contributor

You help us to improve the *Security Cloud* protection by contributing information of malicious programs and web sites.

You can choose to be participate in *Security Cloud* during the installation. With the default installation settings, you contribute data to *Security Cloud*. You can change this setting later in the product.

Follow these instructions to change *Security Cloud* settings:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Other** > **Privacy**.
4. Check the participation check box to become a *Security Cloud* contributor.

3.6 Questions about *Security Cloud*

Contact information for any questions about *Security Cloud*.

If you have any further questions about *Security Cloud*, please contact:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

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

Scanning the computer for harmful files

Topics:

- *Protecting the computer against harmful applications*
- *How to scan my computer*
- *How to exclude files from the scan*
- *How to use the quarantine*

Virus protection protects the computer from programs that may steal personal information, damage the computer, 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, the product scans your local hard drives, any removable media (such as portable drives or compact disks) and downloaded content automatically.

You can set the product to scan your e-mails automatically as well.

Virus protection 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*.

4.1 Protecting the computer against harmful applications

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

The product protects your computer from applications that may steal your personal information, damage your files, or use your computer for illegal purposes.

Virus protection scans your computer for harmful files automatically.

DeepGuard monitors applications to detect and prevent potentially harmful changes to your system, and prevents intruders and harmful applications from getting into your computer from the Internet.

The product keeps the protection up to date. It downloads databases that contain information on how to find and remove harmful content automatically.

Note: The product downloads the latest databases after the installation is complete. During this time, Virus protection may not detect all threats but other product features, such as DeepGuard, keep your computer protected.

4.1.1 Protection status icons

The icons of the **Status** page show you the overall status of the product and its features.

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

Status icon	Status name	Description
✓	OK	Your computer is protected. Features are turned on and working properly.
ℹ	Information	The product informs you about a special status. All features are working properly, but for example, the product is downloading updates.
!	Warning	Your computer is not fully protected. The product requires your attention, for example, it has not received updates in a long time.
✖	Error	Your computer is not protected. For example, your subscription has expired or a critical feature is turned off.
⊖	Off	A non-critical feature is turned off.

4.1.2 View the product statistics

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

To open the **Statistics** page:

Click **Statistics**.

The **Statistics** page shows you the following:

- **Virus protection** 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.

4.1.3 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 versions** page.

To open the **Database versions** page:

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

   Note: You need administrative rights to change the settings.

2. Select **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 and later versions of Windows.

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. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
3. Select **Connection**.
4. Select the preferred update option for mobile connections:
   - **Never**

     Updates are not downloaded when you use mobile broadband.
   - **Only in my operator 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.
   - **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.

     Note: If you want to decide separately every time you exit your home operator's network, select **Ask before roaming in a new 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 and later versions of Windows.

4.1.4 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.

4.2 How to scan my computer

When Virus protection 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 protection 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 protection removes harmful files from your computer at the specified times.

4.2.1 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 Status page, click **Settings**.

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

2. Turn **Virus protection** on or off.
3. Click **OK**.

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 Status page, click **Settings**.

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

2. Select **Virus protection**.
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 protection 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 protection 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.

Action to take	What happens to the riskware
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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Virus protection**.
3. Select **Remove tracking cookies**.
4. Click **OK**.

4.2.2 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:

Note: If you want to quickly scan the system, click **Scan** on the Status page.

1. On the Tools page, click the arrow next to **Advanced 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

Scan type	What is scanned	When to use this type
		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 folder or drive for viruses, spyware and riskware	When you suspect that a specific location on your computer may have malware, for example, the location contains downloads from potentially dangerous sources, such as peer-to-peer file sharing networks. Time the scan will take depends of the size of the target that you scan. The scan completes quickly if, for example, you scan a folder that contains only a few small files.

Scan 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **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`, `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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

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

Option	Description
Always ask me (default)	You can select the action to take for every item that is found during manual scanning.
Clean the files	The product tries to automatically disinfect infected files that are found during manual scanning. **Note:** 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.
Quarantine the files	The product moves any harmful files that are found during manual scanning to the quarantine where they cannot harm the computer.
Delete the files	The product deletes any harmful files that are found during manual scanning.
Report only	The product leaves any harmful files that are found during during manual scanning as they are and records the detection in the scan report. **Note:** 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Scheduled scanning**.
3. Turn **Scheduled scanning** on.
4. Select when you would like the scan to start.

Option	Description
Daily	Scan your computer every day.
Weekly	Scan your computer on selected days of the week. Select the days from the list.
Monthly	Scan your computer on selected days of the month. To select the days: **1.** Select one of the **Day** options. **2.** Select the day of the month from the list next to the selected day.

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

Option	Description
Start time	Start the scan at the specified time.
After computer is not used for	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.

Note: Scheduled scans are paused when the *gaming mode* is on. When you turn it off, a suspended scan continues automatically.

4.2.3 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Virus protection**.
3. Select **Remove harmful e-mail attachments**.
4. Click **OK**.

When are e-mail messages and attachments scanned

Virus protection can remove harmful content from e-mails that you receive.

Virus protection 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 protection 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.

4.2.4 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Virus protection**.
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.

4.3 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.

4.3.1 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 Status 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 **Virus protection** to exclude the file type from real-time scanning.
   - Select **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.

4.3.2 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 Status 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 **Virus protection** to exclude the location from real-time scanning.
   - Select **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.

4.3.3 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 Status 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 **Virus protection** to view applications that have been excluded from real-time scanning.
   - Select **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.

4.4 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.

4.4.1 View quarantined items

You can view more information on items in the quarantine.

To view information on items in the quarantine:

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

   Note: You need administrative rights to change the settings.

2. Select **Virus protection**.
3. Click **View quarantine**.
   The **Quarantine** page shows the total number of items stored in quarantine.
4. To view detailed information on a selected item in the quarantine, click **Details**.
5. To view more information on why an item was quarantined, click the ⓘ icon next to the item.

4.4.2 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Virus protection**.
3. Click **View quarantine**.
4. Select the quarantined items that you want to restore.
5. Click **Restore**.

What is DeepGuard

Topics:

- *Choose what DeepGuard monitors*
- *What to do with suspicious behavior warnings*
- *Submitting suspicious applications for analysis*

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.

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.

5.1 Choose what DeepGuard monitors

DeepGuard monitors important system settings and files, and any attempts to turn off important applications, including this security product.

To choose what DeepGuard monitors:

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

   Note: You need administrative rights to change the settings.

2. Select **DeepGuard**.
3. Make sure that **DeepGuard** is turned on.
4. Select the settings for DeepGuard:

   Warn me about suspicious behavior Keep this setting turned on to get warnings about suspicious application behavior. If you turn this off, DeepGuard stops monitoring suspicious behavior, which lowers security.

   Warn me about application exploits Keep this setting turned on to get warnings about potential exploit attempts. If you turn this off, harmful web pages and documents can exploit your applications, which lowers security. We recommend that you do not turn this off.

   Ask my permission to make an Internet connection Keep this setting turned on if you want DeepGuard to notify you when an unknown application tries to connect to the Internet.

   Use the compatibility mode (lowers security) 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.

5. Click **OK**.

5.1.1 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 Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **DeepGuard**.
3. Click **Change application permissions**.
   The **Monitored applications** list is shown.
4. Find the application that you want to allow and click **Details**.

   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.

5. Select **Allow**.
6. Click **OK**.
7. Click **Close**.

DeepGuard allows the application to make system changes again.

5.2 What to do with suspicious behavior warnings

DeepGuard blocks the applications that it monitors when they behave suspiciously or try to connect to the Internet.

You can decide whether you want to allow the application to continue or not based on what happened.

5.2.1 DeepGuard blocks a harmful application

DeepGuard notifies you when it detects and blocks a harmful application.

When the notification opens:

Click **Details** to view more information about the application.
The details show you:

- the location of the application,
- the reputation of the application in Security Cloud,
- how common the application is, and
- the name of the detected malware.

You can submit a sample of the application for analysis.

5.2.2 DeepGuard blocks a suspicious application

When **Warn me about suspicious behavior** is turned on in DeepGuard settings, DeepGuard notifies you when it detects an application that is behaving suspiciously. If you trust the application, you can allow it to continue.

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

1. Click **Details** to view more information about the application.
   The details section shows you:
   - the location of the application,
   - the reputation of the application in Security Cloud,
   - how common the application is, and
   - the name of the malware.
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.

You can submit a sample of the suspicious application for analysis.

5.2.3 Unknown application tries to connect to the Internet

When you turn on **Ask my permission to make an Internet connection** in DeepGuard settings, it notifies you when an unknown application tries to connect to the Internet. If you trust the application, you can allow it to continue.

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

1. Click **Details** to view more information about the application.
   The details section shows you:
   - the location of the application,
   - the reputation of the application in Security Cloud,
   - how common the application is,
   - what the application tried to do, and
   - where the application tried to connect.
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. Block it permanently.** 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.

When the *gaming mode* is on, DeepGuard allows any unknown application to connect to the Internet. Note that it still blocks all harmful applications that try to connect to the Internet when the *gaming mode* is on.

You can submit a sample of the suspicious application for analysis.

5.2.4 DeepGuard detects a possible exploit

When **Warn me about application exploits** is turned on in DeepGuard settings, DeepGuard notifies if it detects suspicious behavior from an application after you open a harmful web page or a document.

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

1. Click **Details** to view more information about the application.
   The details section shows you:
   - the name of the malware, and
   - the source of the exploit (a harmful web page or document), if known.
2. Decide whether you trust the application that DeepGuard has blocked:
   - Choose **Keep the application open (may put your device at risk)** if you do not want to close the application.

     You may want to keep the application open if closing the application without saving your data is unacceptable at the moment.
   - Choose **Close the application to prevent the exploit** if you want to close the application and make sure that you do not put your device at risk.

     We recommend that you close the application so that you do not put your device at risk.

You can submit a sample for analysis if the source of the exploit was identified.

5.3 Submitting suspicious applications for analysis

You can help us to improve the protection by contributing suspicious applications for analysis.

When DeepGuard blocks an application, for example because it is a possible security risk for your computer or the application tried to do something possibly harmful, you can send a sample of the application for security research purposes.

You can do this if you know that the application that DeepGuard blocked is safe or if you suspect that that application may be harmful.

To submit a sample for analysis:

1. When DeepGuard blocks an application, select whether you want to block the application or let it continue.
2. DeepGuard may ask whether you want to submit the application for analysis. Click **Submit** to submit the sample.

   Note: DeepGuard does not always ask you to submit a sample, for example when we have information about the blocked application already.

What is a firewall

Topics:

- *Turn firewall on or off*
- *Change firewall settings*
- *Prevent applications from downloading harmful files*
- *Using personal firewalls*

The *firewall* prevents intruders and harmful applications getting into your computer from the Internet.

Firewall allows only safe Internet connections from your computer and blocks intrusions from the Internet.

6.1 Turn firewall on or off

Keep firewall turned on to block intruders from accessing your computer.

To turn firewall on or off:

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

   Note: You need administrative rights to change the settings.

2. Turn **Firewall** on or off.

   Note: Your computer is not fully protected when you turn off security features.

3. Click **OK**.

We recommend that you do not keep the *firewall* turned off. If you do, your computer is vulnerable to network attacks. If an application stops working because it cannot connect to the Internet, change the *firewall settings* instead of turning the *firewall* off.

6.2 Change firewall settings

When the firewall is turned on, it restricts access to and from your computer. Some applications may require that you allow them through the firewall to work properly.

The product uses Windows Firewall to protect your computer.

To change Windows Firewall settings:

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

   Note: You need administrative rights to change the settings.

2. Select **Firewall**.
3. Click **Change Windows Firewall settings**.

   Note: You need administrative rights to edit the settings.

For more information on Windows Firewall, refer to Microsoft Windows documentation.

6.3 Prevent applications from downloading harmful files

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

Some web sites 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. On the Status page, click **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Firewall**.
3. Select **Do not allow applications to download harmful files**.

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

6.4 Using personal firewalls

The product is designed to work with Windows Firewall. Other personal firewalls require additional setup to work with the product.

The product uses Windows Firewall for basic firewall functions, such as controlling incoming network traffic and keeping your internal network separate from the public Internet. In addition, DeepGuard monitors installed applications and prevents suspicious applications from accessing the Internet without your permission.

If you replace Windows Firewall with a personal firewall, make sure that it allows incoming and outgoing network traffic for all F-Secure processes and that you allow all F-Secure processes when the personal firewall prompts you to do so.

Tip: If your personal firewall has a manual filtering mode, use it to allow all F-Secure processes.

Block spam

Topics:

- *Turn spam filtering on or off*
- *Label spam messages*
- *Set up my e-mail programs to filter spam*

Use spam filtering to catch spam and phishing messages and to keep them away from your inbox.

Spam and *phishing* messages often tend to swamp desirable e-mail messages.

An e-mail message is considered *spam* if it is sent as a part of a larger collection of messages that all have mostly identical content and you have not granted permission for the message to be sent to you.

Phishing messages attempt to to steal your personal information. These authentic-looking messages appear to come from legitimate businesses and are designed to try to fool you into giving away your personal data, such as bank account numbers, passwords, and credit card and social security numbers. Do not trust the content of any e-mail message that spam and phishing filtering detects.

7.1 Turn spam filtering on or off

Keep spam filtering turned on to remove spam and phishing messages from your inbox.

To turn spam filtering on or off:

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

   Note: You need administrative rights to change the settings.

2. Turn **Spam filtering** on or off.
3. Click **OK**.

Tip: Create a spam filtering rule in your e-mail program to move mass advertisements and deceitful e-mails to a spam folder automatically.

7.2 Label spam messages

Spam filtering can label the subject field of spam messages.

To add the [SPAM] text to spam and phishing messages:

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

   Note: You need administrative rights to change the settings.

2. Select **Spam filtering**.
3. Select **Mark spam with [SPAM] in the e-mail subject field**.
4. Click **OK**.

When you receive a spam or phishing e-mails, spam filtering adds a `[SPAM]` text in the e-mail message subject field.

7.3 Set up my e-mail programs to filter spam

You can create a *spam* and a *phishing* filtering rules in your e-mail program to move unwanted messages to a separate folder automatically.

Spam filtering marks all spam and phishing e-mails that it detects with a [SPAM] prefix in the e-mail message subject field. If you want to move these messages away from your inbox automatically, you need to create a spam folder and filtering rules in your e-mail program. If you have multiple e-mail accounts, you have to create the filtering rules for each e-mail account separately.

This section contains instructions on how you can create the spam folder and the filtering rule for Windows Mail, Microsoft Outlook, Mozilla Thunderbird, Eudora, and Opera. You can also follow these instructions to create similar filtering rules in other e-mail programs.

Note: *Spam* filtering supports only the POP3 protocol. Web-based e-mail programs or other protocols are not supported.

7.3.1 Blocking spam in Windows Mail

To filter *spam* and phishing e-mail messages, you need to create a spam folder and the filtering rule.

To use spam and phishing filtering with Windows Mail, make sure that **Mark spam with [SPAM] in the e-mail subject field** is turned on in **Spam filtering** settings.

To create a *spam* filtering rule:

1. Select **Folders** > **Message rules** from the **Windows Mail** menu.

   Note: If the **New Mail Rule** window does not appear automatically, click **New** on the **Email rules** tab.

2. In the **New Mail Rule** window, create a rule for moving an e-mail message to the *spam* folder:
   a) In the conditions field, select **Where the Subject line contains specific words**.
   b) In the actions field, select **Move it to the specified folder**.
3. In the rule description field, click the **contains specific words** link.
   a) In the **Type Specific Words** window, enter `[SPAM]` and click **Add**.
   b) Click **OK** to close the **Type Specific Words** window.
4. In the rule description field, click the **specified** folder link.
   a) In the **Move** window, click **New Folder**.
   b) Enter `spam` as the new folder name and click **OK**.
   c) Click **OK** to close the **Move** window.
5. In the rule name field, enter `Spam`.
6. Click **Save rule** to close the **New Mail Rule** window.
   The **Rules** window opens.
7. Click OK to close the **Rules** window.

   If you want to apply the new rule to e-mail messages that are already in your inbox, select the **spam** rule and click **Apply now**.

You have now created the *spam* filtering rule. From now on, *spam* e-mail messages are filtered to the *spam* folder.

7.3.2 Block spam in Microsoft Outlook

To filter *spam* and phishing e-mail messages, you need to create a spam folder and the filtering rule.

To use spam and phishing filtering with Microsoft Outlook, make sure that **Mark spam with [SPAM] in the e-mail subject field** is turned on in **Spam filtering** settings.

Note: The steps given here apply to Microsoft Outlook 2007. The steps for other versions may vary slightly.

To create a *spam* filtering rule:

1. In **Tools** menu, select **Rules and Alerts**.
2. In **E-mail Rules** tab, click **New Rule**.
3. Select **Move messages with specific words in the subject to a folder** template under **Stay Organized** list.
4. Click **Next**.
5. In **Step 2: Edit the rule description** pane, click the **specific words** link.
   a) In the **Specify words or phrases to search for in the subject** field, enter `[SPAM]` and click **Add**.
   b) Click **OK** to close the **Type Specific Words** window.
6. In **Step 2: Edit the rule description** pane, click the **specified** folder link.
   a) In the **Rules and Alerts** window, click **New**.
   b) Enter `spam` as the new folder name and click **OK**.
   c) Click **OK** to close the **Rules and Alerts** window.
7. Click **Finish**.
8. Click **OK**.

   If you want to apply the new rule to e-mail messages that are already in your inbox, click **Run Rules Now** before exiting Rules and Alerts.

You have now created the *spam* filtering rule. From now on, *spam* e-mail messages are filtered to the *spam* folder.

7.3.3 Blocking spam in Mozilla Thunderbird and Eudora OSE

To filter *spam* and phishing e-mail messages, you need to create a spam folder and the filtering rule.

To create the *spam* filtering rule:

1. Create a new folder for spam and phishing messages:
   a) Right-click your e-mail account name and select **New Folder**.
   b) Enter `spam` as the new folder name.
   c) Click **Create Folder**.
2. Make sure that your account name is selected and click **Manage message filters** in the **Advanced Features** list.
3. Click **New**.
4. Enter `spam` as the **Filter name**.
5. Create a customized e-mail header:
   a) In the **Match all of the following** list, open the first drop-down menu that has **Subject** selected by default.
   b) Select **Customize** from the drop-down menu .
   c) In the **Customize Headers** dialog box, enter `X-Spam-Flag` as the new message header and click **Add**.
   d) Click **OK** to close the **Customize Headers** dialog box.
6. Create a rule to filter spam messages:
   a) In the **Match all of the following** list, open the first drop-down menu and select **X-Spam-Flag** that you created in the previous step.
   b) Select **contains** from the second drop-down menu.
   c) Enter `Yes` as the text you want to match to the last text box on the row.
7. Create an action that moves the spam to the spam folder:
   a) In the **Perform these actions** list, select **Move Message to**.
   b) Select the `spam` folder in the second drop-down list.
8. Click **OK** to save the changes.
9. Close the **Message Filters** dialog.

You have now created the *spam* filtering rule. From now on, *spam* e-mail messages are filtered to the *spam* folder.

7.3.4 Blocking spam in Opera

To filter *spam* and phishing e-mail messages, you need to create a spam folder and the filtering rule.

Note: The steps given here apply to Opera version 12. The steps for other versions may vary slightly.

To create a *spam* filtering rule:

1. Open the **Opera Mail** view.
2. Right-click your default *Spam* folder and select **Properties**.
3. Click **Add Rule**.
4. Create a rule for moving an e-mail message to the *spam* filter:
   a) From the first list, select **Any header**.
   b) From the second list, select **contains**.
   c) In the text box, enter `X-Spam-Flag: Yes` as the text you want to match.

   Make sure that you leave a space between the colon and `Yes`.
5. Click **Close** to confirm your new *spam* filtering rule.

You have now created the *spam* filtering rule. From now on, *spam* e-mail messages are filtered to the *spam* folder.

Using the Internet safely

Topics:

Information about how to get started with the product.

This product helps you to browse the web safely. In addition to protecting you against malicious software and web sites, you can also restrict the type of content that can be viewed by different user accounts.

The product uses Windows user accounts to control the settings for each person who uses your computer. Only someone with administrative access rights is allowed to change the product settings for the various Windows user accounts. We recommend that you set up a separate Windows user account for each person who uses your computer. For example, any guest users should not have administrative access rights for their Windows user accounts.

Note: The version of the product that you have installed may not include all of the features described here.

8.1 How to protect different user accounts

To provide the best protection against online threats, you should use separate Windows user accounts for each person who uses your computer.

The product allows you to use different settings for each Windows user account that you have set up on your computer. Only users who have administrator access can change the product settings for other user accounts. Anyone else except administrators should only have normal access rights, so that they cannot change the settings that you have defined for them.

8.1.1 Creating Windows user accounts

You can create new Windows user accounts through the product.

To create Windows user accounts:

1. On the main page, click **Create new**.
   This opens the user account settings in Windows.
2. Complete the necessary details to create or edit the user account.

The main page of the product shows both the user name and user account type.

8.1.2 Viewing statistics

You can see what web pages have been viewed and blocked on the **Settings** > **Other** > **Statistics** page.

The product collects information on visited and blocked web sites. This information is user-specific for each Windows user account.

The information shows you whether a blocked site has content that you have intentionally blocked or if the product has identified it as a potentially harmful site.

8.2 Browsing secure web sites

The product installs an extension on all your browsers to provide full support for browsing protection on secure (HTTPS) web sites.

Your browsers should automatically detect the extension and turn it on, but in some cases you may need to turn it on manually.

To turn on the browser extension, edit your browser settings:

- On Firefox, select **Tools** > **Add-ons** from the menu and click **Enable** next to the extension.
- On Chrome, select **Settings** from the menu, then click **Extensions** and select **Enable** next to the extension.
- On Internet Explorer, select **Tools** > **Manage Add-ons**, select the browser extension and click **Enable**.

Note: If you have to turn on the extension manually, you should turn it on separately for each user account on your computer.

8.3 What are safety ratings

Safety ratings in search results help you avoid the Internet threats.

The safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

✓ The site is safe to the best of our knowledge. We did not find anything suspicious in the web site.

! The site is suspicious and we recommend that you are careful when you visit this web site. Avoid downloading any files or providing any personal information.

✖	The site is harmful. We recommend that you avoid visiting this web site.
?	We have not analyzed the web site yet or no information is currently available for it.
✓	Administrator has allowed you to visit this web site.
⛔	Administrator has blocked this site and you cannot visit it.

8.4 What is browsing protection

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

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

The safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

8.4.1 How to turn browsing protection on or off

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

To turn browsing protection on or off:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Browsing protection**.
3. Click the switch in the top-right corner.
4. If your browser is open, restart your browser to apply the changed settings.

Show ratings for web links

When you set browsing protection to show ratings, it shows the safety rating for web sites on search engine results (Google, Yahoo, and Bing).

To show ratings for web sites:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Browsing protection**.
3. Select **Show the reputation rating for web sites in search results**.
4. Click **OK**.

When you search the web with a search engine, browsing protection shows safety ratings for web sites that are found.

8.4.2 What to do when a web site is blocked

A browsing protection block page appears when you try to access a site that has been rated harmful.

When a browsing protection block page appears:

If you want to enter the web site anyway, click **Allow web site**.

8.5 Using online banks safely

Banking protection protects you against harmful activity when you access your online bank or make transactions online.

Banking protection automatically detects secure connections to online banking web sites, and blocks any connections that do not go to the intended site. When you open an online banking web site, only connections to online banking web sites, or to web sites that are considered safe for online banking, are allowed.

Banking protection currently supports the following browsers:

- Internet Explorer 9 or newer
- Firefox 13 or newer
- Google Chrome

8.5.1 Turning banking protection on

When Banking protection is turned on, your online banking sessions and transactions are protected.

To turn Banking protection on:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Banking protection**.
3. Click the switch in the top-right corner.
4. If you want to keep your current connections open, select **Do not interrupt my active Internet connections**.

   When you access your bank's web site or make online payments, Banking protection activates and blocks all connections that are not necessary for online banking. This means that it closes all your current Internet connections as well unless you select this setting.

8.5.2 Using banking protection

When Banking protection is turned on, it automatically detects when you access an online banking web site.

When you open an online banking web site in your browser, the **Banking protection** notification appears at the top of your screen. All other connections are blocked while Banking protection is active.

Tip: If you do not want to interrupt your other active connections when Banking protection activates, click **Change settings** on the notification to change the product settings for your user account.

To end your banking protection session and restore your other connections:

Click **End** on the **Banking protection** notification.

8.6 Making browsing safe

You can stay safe from the many threats of the Internet by monitoring the browsing of all Windows user accounts on your computer.

The Internet is full of interesting web sites, but there are also many risks for anyone who uses the Internet. Many web sites contain material that you might consider inappropriate. People can get exposed to inappropriate material, or they may receive harassing messages via e-mail or chat. They can accidentally download files that contain *viruses* that could damage the computer.

Note: Restricting access to online content protects your user accounts from chat and e-mail programs that run in your web browser.

You can restrict what web pages can be viewed, and schedule the time that can be spent online. You can also block links to adult content from being shown in search engine results. These restrictions are applied to Windows user accounts, so whenever someone logs in with their own user account, the restrictions are in place.

8.6.1 Limit access to web content

You can select the type of filtering that you want to use for different Windows user accounts.

Web page filtering blocks access either to any web pages that you have not allowed, or to any web pages that contain content that you have decided to block.

Allow web pages

You can allow access to only those web sites and pages that you trust by adding them to the list of allowed web sites.

To allow access to specific web pages:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Content blocker**.
3. Click the switch in the top-right corner.
4. Select **Allow only selected web sites**.
5. Click **Add** to add web sites to the **Allowed web sites** list.
6. When you have added all the web sites you want to allow, click **OK**.

When they are logged in on your computer, anyone using the Windows user account that you edited can now only access the web sites that you added to the list of allowed web sites.

Block web pages by their content type

You can block access to web sites and pages that contain unsuitable content.

To select the types of web content to block:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Content blocker**.
3. Click the switch in the top-right corner.
4. Select **Block web content**.
5. Select the types of content that you want to block.
6. When you have selected all of the content types that you want to block, click **OK**.

When they are logged in on your computer, anyone using the Windows user account that you edited will not be able to access web sites that contain a type of content that you have blocked.

Editing allowed and blocked web sites

You can choose to allow specific web sites that are blocked, and also block individual web sites that are not included in any content type.

Note: Depending on the version of the product that you are using, you may only be able to either allow or block web sites, but not both.

For example, you may consider a web site safe, even though you want to block other web sites of that content type. You may also want to block a specific web site, even though other web sites of that content type are allowed.

To allow or block a web site:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Content blocker**.
3. Click **View web site exceptions**.

If the web site you want to edit is already listed as allowed or denied, and you want to move it from one list to the other:

a) Depending on which web site list you want to edit, click the **Allowed** or **Denied** tab.
b) Right-click the web site on the list and select **Allow** or **Deny**.

If the web site is not included in either list:

a) Click the **Allowed** tab if you want to allow a web site, or the **Denied** tab if you want to block a web site.
b) Click **Add** to add the new web site to the list.
c) Enter the address of the web site you want to add, then click **OK**.
d) In the **Web site exceptions** dialog, click **Close**.

4. Click **OK** to return to the main page.

To change the address of an allowed or blocked web site, right-click the web site on the list and select **Edit**.

To remove an allowed or blocked web site from the list, select the web site and click **Remove**.

8.6.2 Using the search result filter

You can turn on the search result filter to block explicit content from search results.

Search result filter hides adult content by making sure that Google, Yahoo and Bing use the SafeSearch "strict" level. While this cannot block all inappropriate and explicit content from appearing in your search results, it helps you avoid most such material.

To turn on search result filter:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Online Safety** > **Search result filter**.
3. Click the switch in the top-right corner.

When search result filter is turned on, it will override the SafeSearch settings on web sites for anyone logged in to that Windows user account.

8.7 How to schedule browsing time

You can control the time that can be spent browsing the Internet on your computer.

You can set different restrictions for each Windows user account on your computer. You can control:

- When someone is allowed to browse the Internet. For example, you can allow Internet browsing only before 8 o'clock in the evening.
- For how long someone is allowed to browse the Internet. For example, you can allow Internet browsing for only one hour per day.

Note: If you remove the time restrictions, your Internet browsing is allowed without any time limits.

8.7.1 Allow Internet browsing only during specific hours

You can limit when someone is allowed to browse the Internet by setting the browsing hours for their Windows user account.

To set the allowed browsing hours:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Browsing time limits**.
3. Click the switch in the top-right corner.
4. On the *Browsing hours* table, select the times when web browsing is allowed on each day of the week.
5. Select how many hours of browsing is allowed on weekdays and weekends.

If you do not want to limit the amount of time allowed spent browsing the Internet, make sure that the browsing time for both weekdays and weekends is set to **Max**.

6. Click **OK**.

When they are logged in on your computer, anyone using the Windows user account that you edited can now only browse the Internet during the allowed times.

8.7.2 Restrict daily Internet browsing time

You can use daily time limits to restrict Internet access.

You can set different daily time limits for each Windows user account on your computer.

To set the time limits:

1. On the main page, select the Windows user account that you want to edit and click **Settings**.
   The **Settings** dialog box opens.
2. Select **Browsing time limits**.
3. Click the switch in the top-right corner.
4. On the *Browsing hours* table, select the times when web browsing is allowed on each day of the week.

   If you do not want to limit web browsing to specific hours, make sure that all of the cells in the *Browsing hours* table are selected.
5. Select how many hours of browsing is allowed on weekdays and weekends, then click **OK**.

When they are logged in on your computer, anyone using the Windows user account that you edited can now only browse the Internet for the allowed amount of time.

What is Safe Search

Topics:

- *What are safety ratings*
- *Set up Safe Search to your web browser*
- *Removing Safe Search*

Safe Search shows the safety of web sites on search results and prevents you from unintentionally accessing harmful web sites.

Safe Search detects web sites that contain security threats, such as malware (viruses, worms, trojans) or try to steal your sensitive information, like user names and passwords.

9.1 What are safety ratings

Safety ratings in search results help you avoid the Internet threats.

The safety ratings are based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

✅ The site is safe to the best of our knowledge. We did not find anything suspicious in the web site.

⚠ The site is suspicious and we recommend that you are careful when you visit this web site. Avoid downloading any files or providing any personal information.

❌ The site is harmful. We recommend that you avoid visiting this web site.

❓ We have not analyzed the web site yet or no information is currently available for it.

☑ Administrator has allowed you to visit this web site.

⛔ Administrator has blocked this site and you cannot visit it.

9.2 Set up Safe Search to your web browser

You can set up Safe Search as your default search tool in your web browser during when you install the product.

Safe Search supports the following web browsers:

- Internet Explorer 8 for Windows XP SP3
- Internet Explorer, two latest released versions for Windows Vista, Windows 7, and Windows 8
- Firefox, two latest released versions
- Google Chrome, two latest released versions

9.2.1 Using Safe Search with Internet Explorer

You can make Safe Search as your default home page and search provider, and install the search toolbar when you use Internet Explorer.

Follow these instructions to use Safe Search with Internet Explorer:

1. Open Internet Explorer.
2. Click **Change** when Internet Explorer shows you a message that a program would like to change your search provider.

   Note: You do not see this message if you did not choose Safe Search as your default search provider during the installation.

3. When Internet Explorer shows you a message that the toolbar add-on is ready for use, click **Enable**. If you see a **Several add-ons are ready for use** dialog instead, click **Choose add-ons** first.

   Note: In Internet Explorer 8, the toolbar is ready for use automatically.

   Note: You do not see this message if you did not choose to install the search toolbar during the installation.

9.2.2 Using Safe Search with Firefox

You can make Safe Search as your default home page, search provider, and install the search toolbar when you use Firefox.

Note: If your Firefox configuration prevents changing the home page or default search provider, the Safe Search cannot modify these settings.

Follow these instructions to use Safe Search toolbar with Firefox after you have installed the product:

1. Open Firefox.
2. Open **Install Add-on** tab.
3. Make sure that the add-on to be installed is *Safe Search.*
4. Select **Allow this installation** check box.
5. Click **Continue**.
6. Click **Restart Firefox**.

9.2.3 Using Safe Search with Chrome

You can make Safe Search as your default search provider and install the search toolbar when you use Chrome.

If you use Chrome as your default browser, the product installation can install the search toolbar and change your search provider automatically.

9.3 Removing Safe Search

9.3.1 Removing Safe Search from Internet Explorer

Follow these instructions if you want to stop using Safe Search in Internet Explorer.

1. Open Windows Control Panel.
2. Open **Network and Internet** > **Internet Options**.
   The **Internet Properties** window opens.
3. To remove Safe Search as your default home page, follow these instructions:
   a) In **Internet Properties**, open the **General** tab.
   b) Under **Home page**, click **Use default**.
4. In **Internet Properties**, open the **Programs** tab.
5. Click **Manage add-ons**.
   The **Manage Add-ons** window opens.
6. To stop using Safe Search as your search provider, follow these instructions:
   a) In **Manage Add-ons**, select **Search Providers**.
   b) Select *Safe Search*.
   c) Click **Remove**.
7. To remove the Safe Search toolbar, follow these instructions:
   a) In **Manage Add-ons**, select **Toolbars and Extensions**.
   b) Select *Safe Search*.
   c) Click **Disable**.

Note: Uninstall Safe Search to remove the Safe Search search engine and the toolbar completely.

9.3.2 Removing Safe Search from Firefox

Follow these instructions if you want to stop using Safe Search in Firefox.

1. To remove Safe Search as your default home page, follow these instructions:
   a) Go to the **Tools** > **Options**.

   a) In the **Options** window, open the **General** tab.
   b) Click **Restore to Default** under the **Home Page** field.

2. To stop using Safe Search as your search provider, follow these instructions:
   a) Click the search provider icon in the search field to open the search engine menu.
   b) Click **Manage Search Engines**.
   c) Select *Safe Search* from the list and click **Remove.**
   d) Click **OK.**

3. To remove the Safe Search toolbar, follow these instructions:
   a) Go to the **Tools** > **Add-ons**.
   b) In the **Add-ons Manager** window, open the **Extensions** tab.
   c) Click **Disable** in the Safe Search extension row.
   d) Restart your browser to remove the toolbar.

Note: Uninstall Safe Search to remove the Safe Search search engine and the toolbar completely.

9.3.3 Removing Safe Search from Chrome

Follow these instructions if you want to stop using Safe Search in Chrome.

1. To stop using Safe Search as your search provider, follow these instructions:
   a) Open **Settings** from the Chrome menu.
   b) Find the **Search** settings.
   c) Click **Manage search engines**.
   d) Click the **X** at the end of the Safe Search row.

2. To remove the Safe Search toolbar, follow these instructions:
   a) Right click the Safe Search toolbar icon.
   b) Select **Remove from Chrome browser**.

Note: Uninstall Safe Search to remove the Safe Search search engine and the toolbar completely.