PSB Computer Protection for Windows

18-07-25

Contents

Chapter

1

Getting started

Topics:

This section describes how you can access the product tools and features and how you can change the product settings.

👉 **Note:** In F-Secure Protection Service for Business, your administrator may enforce some security settings, which means that you may not be able to locally change some features.

1.1 Protection status icons

The protection status icon shows you the overall status of the product and its features.

The protection status icons:

Status icon	Status name	Description
✓	OK	Your device 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 device is not fully protected. The product requires your attention, for example, it has not received updates in a long time.
✖	Error	Your device is not protected. For example, a critical feature is turned off.
⊖	Off	A non-critical feature is turned off.

1.2 Viewing the tools

The **Tools** page shows the tools that you can use to protect your computer.

1.3 Checking for the latest updates

You can manually check for the latest updates.

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

To make sure that you have the latest updates:

1. On the main page, select **Tools**.
2. Select **Check for updates**.
   The product connects to the Internet and checks for the latest updates. If the protection is not up-to-date, it retrieves the latest updates.
3. Click **Close**.

1.4 Viewing recent events for the product

You can see what the product has done and how it has protected your computer on the **Event history** page.

The event history shows you various events for the installed products and details of the protective measures that the products have taken. For example, it shows you all the harmful items that have been detected and either cleaned or quarantined.

1. On the main page, select **Tools**.
2. Select **Recent events**.
   The **Event history** page opens.

The event history shows you the time and description of each event. Depending on the type of event, you can click the event to see more details for it. For example, for harmful files you can see 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.

1.5 What are flyers

Flyers are small notifications that are shown at the bottom right-hand corner of your computer screen.

The flyers inform you about the actions that the product has taken to protect your computer. The product informs you with flyers, for example, when it blocks a potentially harmful program from starting. These flyers are informational and do not require any action from you.

Chapter

2

Changing the product settings

Topics:

- *Edit settings*
- *Quick access to product settings*
- *View product messages*
- *Change notification settings*
- *View the latest updates*
- *Change connection settings*
- *Turning off all security features*

You can control how the product behaves by changing its settings.

Note that you need administrative rights to change the product settings. Some product settings can be accessed from the tray icon context menu.

Note: In F-Secure Protection Service for Business, your administrator may enforce some security settings, which means that you may not be able to locally change some features.

2.1 Edit settings

Edit settings to change the way that the product works.

To open the settings:

1. Open the **Malware Protection** page.
2. Select **Settings**.

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

3. Select the product component from the left pane. The right pane shows the settings related to selected component.

2.2 Quick access to product settings

Some product settings can be accessed from the tray icon context menu.

To open the tray icon context menu, follow these instructions:

1. Right-click the product icon on the Windows taskbar. If the product icon is hidden, click the **Show hidden icons** arrow in the taskbar first.
2. The context menu includes the following options.

Option	Description
Computer Protection feedback	Opens the product feedback form.
Check for updates	Checks and downloads the latest updates.
View messages	Shows important notifications that may require your attention.
View recent events	Shows the actions that the product has taken to protect your computer.
Open common settings	Shows the latest updates. Here you can also change your connection and privacy settings.
About	Shows the version information of the product.

2.3 View product messages

The product shows you any important messages automatically that require your attention.

If you have any pending messages, the product reminds you of them periodically.

To view messages:

1. Right-click the product icon in the system tray.
   A pop-up menu appears.
2. Select **View messages**.

   The number of messages currently available is shown in the pop-up menu next to **View messages**.

   The product message view opens, showing the first message that requires your attention.
3. If you do not want to do anything at the moment, click **Later**.
   If there are several messages, the next message is shown.

2.4 Change notification settings

Instructions on how to change which notifications are shown.

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

3. Under **My information**, select **Notifications**.
4. Select or clear **Show product notifications for useful tips and updates. Critical product notifications will always be shown**. When this setting is on, the product shows notifications about news, tips, and special offers.

2.5 View the latest updates

View the date and time of the latest update.

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

To see details of the latest updates for the installed products:

1. Right-click on the product icon in the system tray.
   A pop-up menu appears.
2. Select **Open common settings**.
   The **Common settings** page is displayed.
3. Select **Downloads**.
   Details of the latest updates download by the product are displayed.
4. To manually check for newer updates, select **Check now**.
   The product checks to see if an newer update is available.

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

2.6 Change connection settings

Instructions on how to change how your computer connects to the Internet and how you want to handle updates while using mobile networks.

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 HTTP proxy list, select whether or not your computer uses a proxy server to connect to the Internet.
   - Select **Do not use** if your computer is connected to the Internet directly
   - Select **Use the browser's settings** to use the same HTTP proxy settings that you have configured in your web browser
   - Select **Custom address** to manually configure the HTTP proxy settings

2.7 Turning off all security features

You can turn off all security features if you need to free up more system resources.

The features are automatically turned back on the next time you restart your computer. You can also turn them on manually on the main view of the product.

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

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

1. On the main page, select **Tools**.
2. Select **Turn off all security features**.

Chapter

3

Protecting the computer against harmful content

Topics:

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

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

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

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

Note: In F-Secure Protection Service for Business, your administrator may enforce some security settings, which means that you may not be able to locally change some features.

3.1 What is harmful content

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

3.1.1 Potentially unwanted applications (PUA) and unwanted applications (UA)

'Potentially unwanted applications' have behaviors or traits that you may consider undesirable or unwanted. 'Unwanted applications' have behaviors or traits with more severe impact on your device or data.

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

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

The impact of these behaviors and traits on your device or data can range from mild to severe. They are not however harmful enough to warrant classifying the application as malware.

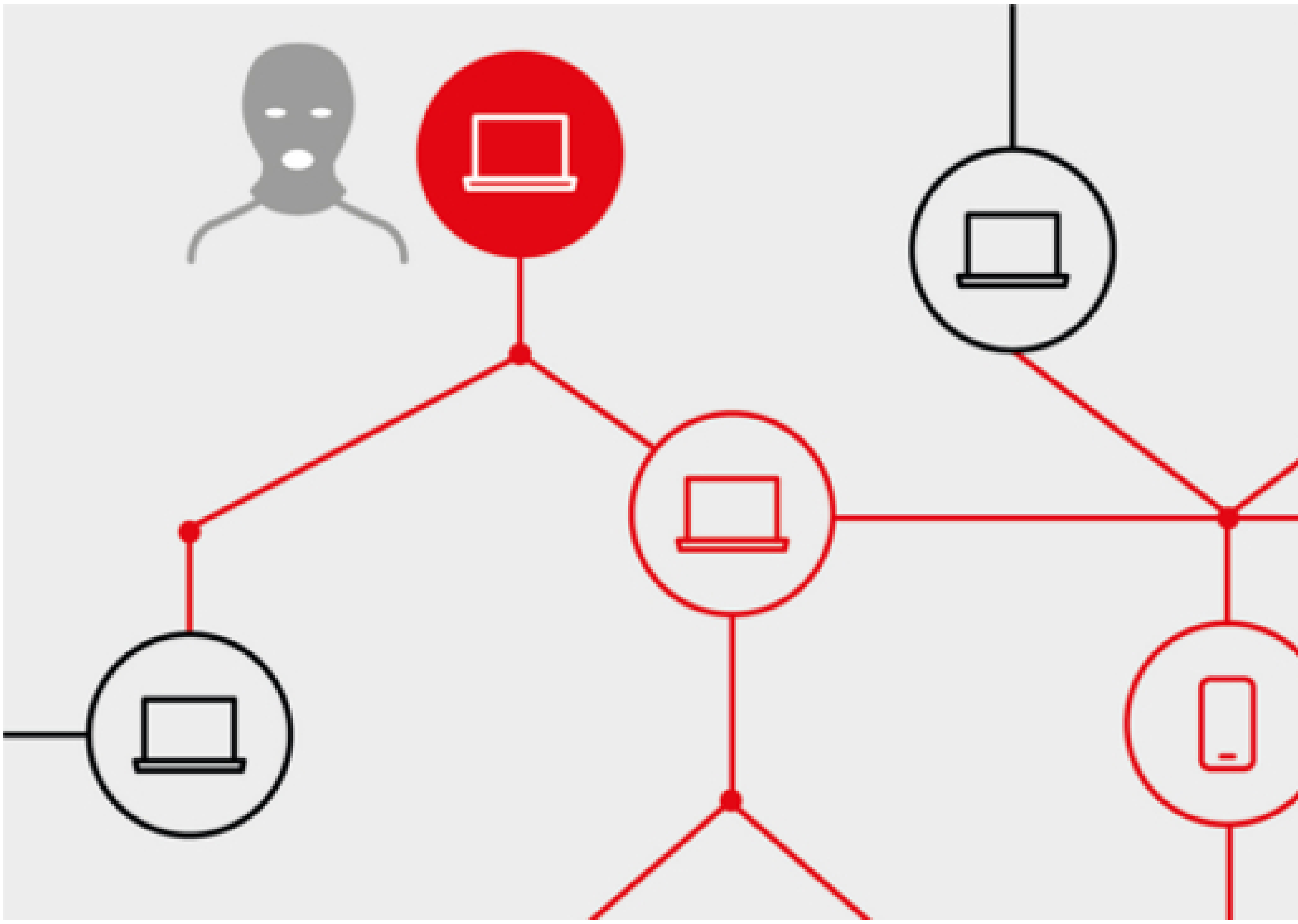
If an application has behaviors or traits that have a severe impact, it is considered an 'unwanted application' (UA). The product will treat such applications with more caution.

As you are the best judge of whether you want to trust and use a 'potentially unwanted' or 'unwanted' application, you can choose how you want the product to handle it:

- **A potentially unwanted application** - The product will display a warning notification message before the application is allowed to run normally. If you trust the application, you can allow the product to do so. You can also opt to have the product block the application.
- **An unwanted application** - The product will block and quarantine the application. If you trust the application, you can exclude it from further scanning.

3.1.2 Worms

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



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

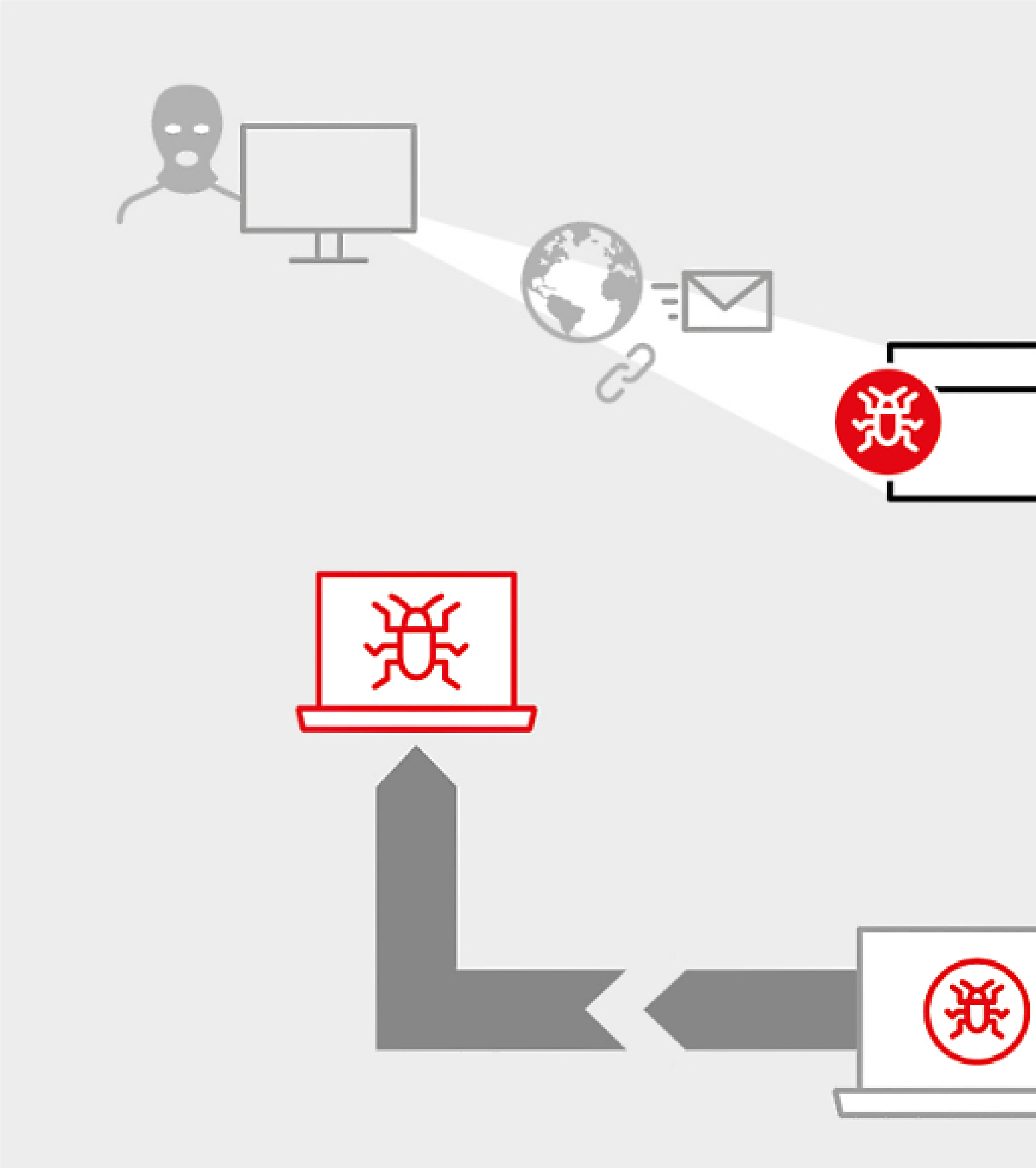
Once installed, the worm uses the device's physical resources to create copies of itself, and then send those copies to any other devices it can reach over a network. If a large quantity of worm copies is being sent out, the device's performance may suffer. If many devices on a network are affected and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

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

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

3.1.3 Trojans

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



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

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

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

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

3.1.4 Backdoors

Backdoors are features or specially crafted programs that can be used to evade the security features of a targeted program, device, portal or service. They are typically used by attackers to gain unauthorized access or to perform harmful actions.

A feature in a program, device, portal or service can be considered a backdoor if its design or implementation introduces a security risk. For example, a secret administrator's access point for an online portal with a hardcoded password can be considered a backdoor.

A program that is specially crafted as a backdoor usually takes advantage of flaws in the code of a targeted program, device, portal or service. The flaws may be bugs, vulnerabilities or undocumented features.

A backdoor is typically used by attackers to gain unauthorized access or to perform harmful actions that allow them to evade security features such as access restrictions, authentication or encryption.

3.1.5 Exploits

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

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

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

There are a number of ways an attacker can deliver an exploit so that it is in a position to affect a computer or device:

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

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

3.1.6 Exploit kits

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

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

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

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

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

3.2 How to scan my computer

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

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

3.2.1 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.

Turning on real-time scanning

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

To make sure that real-time scanning is on:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Malware protection**.
3. Turn on **Malware protection**.

3.2.2 Scan files manually

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

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

Scanning files and folders

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

Running a malware scan

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

To scan your computer, follow these instructions:

1. On the main page, select **Tools**.
2. Select **Scan options**.
3. If you want to optimize how the manual scanning scans your computer, select **Change scanning settings**.

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

   a) Select **Scan only known file types** to scan only files that are most likely to be harmful, for example, executable files. Selecting this option makes the scanning faster. Leave the option unchecked to scan all files.

   The files with the following extensions are examples of known file types: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.

   b) Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Selecting this option makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.

   c) Select **OK** to return to **Tools** page.
4. Select either **Virus scan** or **Full computer scan**.
   - **Virus scan** scans only the parts of your system that contain installed applications. It can find and remove unwanted applications and harmful items on your computer in a shorter time.
   - **Full computer scan** scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete.

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

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

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

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

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

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

Scan in Windows Explorer

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

To scan a disk, folder, or file:

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

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

Scheduling scans

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

To schedule a scan:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Other settings** > **Scheduled scanning**.
3. Turn on **Scheduled scanning**.
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.

6. You can optimize how the scheduled scanning scans your computer.
   a) Select **Run scanning on low priority** to make the scheduled scan interfere less with other activities on the computer. Running the scan on low priority takes longer to complete.
   b) Select **Scan only known file types** to scan only files that are most likely to be harmful, for example, executable files. Selecting this option makes the scanning faster. Leave the option unchecked to scan all files.

   The files with the following extensions are examples of known file types: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.

   c) Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Selecting this option makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.
7. Click **OK**.

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

3.3 What is DeepGuard

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

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

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

Potentially harmful system changes that DeepGuard detects include:

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

To make sure that DeepGuard is active:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **DeepGuard**.
3. Turn on **DeepGuard**.

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

3.4 What is DataGuard

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

Ransomware is a type of harmful software that takes control of your computer to encrypt any important data. The encrypted data usually cannot be recovered except by paying the requested ransom.

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

To turn on DataGuard:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **DataGuard**.
3. Turn on DataGuard.
   When it is turned on, DataGuard automatically blocks applications that try to make potentially harmful changes to its list of protected folders.

3.4.1 Adding and removing protected folders

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

DataGuard blocks any unsafe access to your protected folders.

1. On the **Tools** page, click **Quarantine and exclusions**.

   Note: You need administrative rights to access these settings.

2. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
3. Add or remove folders as needed.

   To add a new protected folder:

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

   To remove a folder:

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

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

3.5 Handling blocked applications

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

The **App and file control** view includes three separate tabs:

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

Blocked This tab shows you the applications that DeepGuard has blocked. DeepGuard blocks the applications that it monitors when they behave suspiciously or try to connect to the Internet.

Excluded This tab shows you the applications, files, and folders that are excluded from scanning. DeepGuard does not block any excluded applications from running, and the product does not scan any excluded locations for harmful items. You can exclude both folders and individual files.

Protected This tab shows you the folders that are protected against destructive software, such as ransomware. The product blocks any unsafe applications from making changes to the files stored in these folders.

3.5.1 View quarantined items

You can view more information on items in the quarantine.

To view information on items in the quarantine:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Click **View quarantine**.
   The **App and file control** view opens.
3. Select the **Quarantined** tab.
   This list shows you the name, date of detection, and infection type for each quarantined item.
4. Double-click a quarantined item to see more information.
   For single items, this shows you the original location of the quarantined item.

3.5.2 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 on your computer.

To restore quarantined items:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

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

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

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

3.5.3 Exclude files by location

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

To add files or folders that you want to exclude:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Click **View quarantine**.
   The **App and file control** view opens.
3. Select the **Excluded** tab.
   This view shows you a list of currently excluded locations and applications.
4. Click **Add new**.
5. Select the file or folder that you want to exclude.
6. Click **OK**.

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

3.5.4 View excluded applications

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

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

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

To view the applications that are excluded from scanning:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Click **View quarantine**.
   The **App and file control** view opens.
3. Select the **Excluded** tab.
   This view shows you a list of currently excluded locations and applications.
4. If you want to scan the excluded application again:
   a) Select the application that you want to include in the scan.
   b) Click **Clear**.

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

3.5.5 Allow applications that DeepGuard has blocked

You can control which applications DeepGuard allows and blocks.

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

To allow the application that DeepGuard has blocked:

1. On the **Malware Protection** page, select **Settings**.

Note: You need administrative rights to change the settings.

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

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

Chapter

4

Protecting your web browsing

Topics:

Browsing protection helps you browse the Internet safely by providing safety ratings for web sites on your browser and blocking access to web sites that have been rated harmful.

4.1 Turning on the browsing protection

The browsing protection blocks the access to harmful web sites when it is turned on.

To make sure that the browsing protection is on:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Browsing protection**.
3. Turn on **Browsing protection**.
4. If your browser is open, restart your browser to apply the changed settings.

4.2 Blocking suspicious and prohibited web sites

The browsing protection can prevent you from unintentionally accessing web sites that are not trustworthy or have prohibited content.

Sometimes you may browse to a web site that contains suspicious, infringing, or prohibited content. For example, the web site may be a fake, known spam site, contain potentially unwanted programs, or illegal no matter where you are located.

You can use the browsing protection to avoid unintentionally accessing these web sites.

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Browsing protection**.
3. Make sure that the browsing protection is turned on.
4. If you want to block web sites that are rated as suspicious in addition to ones that are considered harmful, select **Block suspicious web sites**.
5. If you want to block web sites that contain prohibited content, select **Block prohibited web sites**.
6. If your browser is open, restart your browser to apply the changed settings.

4.3 Blocked web content

Your administrator may block access to web sites and pages that contain unsuitable content.

Note: This feature may not be included in your version of the product.

If you go to a web site that contains content that your administrator has blocked, a block page appears to prevent you from accessing the site. If you think that the site does not contain any unsuitable content, or for more information on why the web site has been blocked, contact your administrator.

Note: Restricted access to online content can also apply to chat and email programs that run in your web browser.

4.4 Web site exceptions

The web site exceptions list shows specific web sites are either allowed or blocked.

Note: If your administrator has explicitly blocked a web site or if it contains content that has been blocked, you cannot access the site even if you add it to the **Allowed** list.

To view and edit web site exceptions:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Browsing protection**.
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**.

4.5 Using reputation rating icons

The browsing protection can show you the reputation rating for web sites on search results when you use either Google, Yahoo, or Bing.

To see reputation rating icons in search results:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.
2. Select **Security settings** > **Browsing protection**.
3. Make sure that the browsing protection is turned on.
4. Select **Show the reputation rating for web sites in search results**.
5. If your browser is open, restart your browser to apply the changed settings.

4.6 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:

1. If you want to enter the web site, select **Allow web site**.
   Windows User Access Control asks you to confirm this action.
2. If necessary, enter your administrator account information, then confirm the change.

If you think that a blocked site is safe, click **Report this web site**. This opens a new page where you can fill in the necessary details to submit the web site for analysis.

4.7 Checking that browser extensions are in use

The browsing protection uses browser extensions to give you security information while you are browsing.

For example, if the extension is not installed for your browser, you will see a browser error page instead of a block page if you visit a harmful website. Also, search results may not show you the safety rating icons.

Note: Some browsers, for example Microsoft Edge, do not support extensions.

The **Antivirus** page of the product shows you if the extension for your default browser is not turned on.

Note: Even if the extension is not installed for your default browser, the product still protects you while browsing, but you do not see the security information.

If the product shows you a warning that the browser extension is not installed or is turned off:

1. Open your browser to check if the browser extension is turned on.

   If you use Firefox:

   a) Select **Add-ons** from the menu, then click **Extensions**.

   b) Click **Enable** next to the browsing protection extension.

   If you use Chrome:

   a) Select **More tools** > **Extensions** from the menu.

   b) Select **Enable** next to the browsing protection extension.

   If you use Internet Explorer:

   a) Select **Tools** > **Manage Add-ons**.

   b) Select the browser extension and click **Enable**.

2. If the browsing protection extension is not listed in your browser, you need to reinstall the extension manually.

   a) On the **Antivirus** page of the product, click **Settings**.

   b) Select **Other settings** > **Browser extensions**

   - If you use Firefox or Internet Explorer, click **Reinstall extensions**.
   - If you use Chrome, click **Open Chrome Web Store** to go the browsing protection extension's page, and then click **Add to Chrome**.

3. Open the following test page in your browser to check that the extensions are turned on: *https://unsafe.fstestdomain.com*.

   If you do not see the product block page, you need to turn on the browser extension manually.

4.8 Protecting your sensitive data

Connection control adds another layer of security to prevent attackers from interfering with your confidential transactions and protects you against harmful activity, for example when you access online banks or make transactions online.

Connection control 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.

If you need to access a blocked web site to complete an ongoing transaction, you can temporarily allow access to the blocked page or end the *Connection control* session.

Connection control currently supports the following browsers:

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

4.8.1 Turning on Connection control

When *Connection control* is turned on, it provides additional protection to your secure connections.

Connection control blocks unsafe connections when it is active. For example, when you access a bank's web site or make online payments, *Connection control* activates and blocks all connections that are not necessary for online banking so that they cannot interfere with your confidential transactions.

To turn on *Connection control*:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Connection control**.
3. Select **Do not interrupt my active Internet connections** if you do not want *Connection control* to close your already open connections.

If you leave the setting unselected, *Connection control* closes all your current Internet connections as well when it activates.

4.8.2 Using Connection control

When *Connection control* 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 *Connection control* notification appears at the top of your screen. All other connections are blocked while the banking protection is active.

Tip: If you do not want to interrupt your other active connections when *Connection control* activates, click **Change settings** on the notification.

To end your *Connection control* session and restore your other connections:

Click **End** on the *Connection control* notification.

Chapter

5

What is a firewall

Topics:

- *Turning on firewall*
- *Changing Windows 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.

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

5.1 Turning on firewall

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

We recommend that you keep the *firewall* turned on. When the firewall is turned off, 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.

To make sure that the firewall is on:

1. On the **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

2. Select **Security settings** > **Firewall**.
3. Turn on **Firewall**.

5.2 Changing Windows 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 main page, select **Tools**.
2. Select **Windows Firewall settings**.

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

5.3 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 **Malware Protection** page, select **Settings**.

   Note: You need administrative rights to change the settings.

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

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

5.4 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.

Chapter

6

Privacy

Topics:

This section explains what is Security Cloud and how you can contribute anonymous data and help us improve the product.

6.1 Security Cloud

Security Cloud (formerly known as Real-time protection network) collects security data on unknown applications and web sites and on malicious applications and exploits on web sites.

We collect this information to provide you security services to which you have subscribed and to enhance the security of our other services. We need to collect security data on unknown files, suspicious device behavior, or visited URLs. This data is essential for our services to work. Objects collected in this way are only kept for a limited amount of time, and are deleted after that period.

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. Security data is not used for personalized marketing purposes.

Contributing data

As a contributor, you allow Security Cloud to keep the security data that helps us to strengthen your protection against new and emerging threats. Data collected this way is only kept for a limited time and is deleted after that period.

1. Open the **Common settings** page.
2. Under **My information** > **Privacy**, select **Contribute anonymous data to security cloud**.

> **Note:** You can read our privacy policy here: *http://download.sp.f-secure.com/eula/latest/security_cloud_enu.html*

6.2 Improving the product

You can help us improve the product by sending usage data.

To send usage data:

1. Open the **Common settings** page.
2. Under **My information** > **Privacy**, select **Send usage data**.

> **Note:** You can read our privacy policy here: *http://download.sp.f-secure.com/eula/latest/privacy_enu.html*