

## Table of Contents

1. Introduction to the F-Secure app .....	1
2. System Requirements .....	1
3. Installing the Product .....	2
4. Protecting Your Children with Family Rules .....	3
5. Sharing Protection .....	11
6. Device Protection .....	14
7. Scam Protection .....	24
8. VPN .....	31
9. Password Vault .....	35
10. ID Monitoring .....	49
11. Technical Support .....	53

## 1. Introduction to the F-Secure app

The F-Secure app covers all your security and privacy protection needs.

The F-Secure app includes all the protection features you need in just one single app. It is built on the award-winning antivirus protection technology by F-Secure. It's up to you to decide what features you want to include in your subscription. Later, if the need arises, you can extend the range of protection features on the app without having to reinstall the app.

**F-Secure Total** gives you comprehensive protection both for the security of your devices and for your privacy. It also helps you avoid identity theft. As we share more and more of our personal lives online nowadays, we not only need to protect our devices, but our personal information as well.

The internet is an important part of our daily lives. We want to stay connected with our loved ones, do our banking and shopping online and search the internet for information by asking search engines questions.

With the amount of personal data we handle every day on our smartphones, tablets, and computers, it's important to keep all our devices protected, our information private, and our personal information safe.

With F-Secure Total, you can do the following:

- Protect yourself and your entire family and friends online
- Protect your browsing, online banking and shopping
- Secure your connection in wireless networks
- Stop tracking attempts online
- Protect yourself and your devices against malware and other online threats
- Access geo-blocked content
- Protect your own and your family's personal information against cyber crime

## 2. System requirements

This topic lists the operating system versions supported by the F-Secure app.

The F-Secure app supports the following operating systems:

**For Windows computers:**

- Windows 11
- Windows 10 with the latest updates installed (all 64-bit editions; 32-bit editions are not supported)

- Devices running the Windows on ARM64 operating system, although VPN functionality is currently not supported on ARM devices

#### For Mac computers:

- macOS 15 (Sequoia)
- macOS 14 (Sonoma)
- macOS 13 (Ventura)
- macOS 12 (Monterey)
- Intel and Apple Silicon processors are both supported

#### For smartphones and tablets:

- Android 10.0 or newer
- iOS 17.0 or newer

**Note:** Chromebook devices are currently not supported.

### 3. Installing the product on your device

- You will receive a welcome email from digisafe F-Secure with all the details, including credentials username and password and also the link to download the app. Click the link and you will be redirected to download page where you can download the app depending on the platform you are on (Windows, MacOS, IOS or Android).
- When the installation is complete, open the app.
- If you agree to the End User License Terms, select **Accept and continue**. You may be asked to log in to your account when you start the app for the first time.
- As you are setting up protection for yourself, select **Continue** to finalize the protection for the device.
- Login with the credentials provided on the email. After successfully logged in, you will be prompted to change the password.

**Important:** To be able to protect your device and connections, the app requires that you allow access to photos, media and files on your device.

### 4. Protecting your children with Family Rules

With Family Rules, you can limit your children's daily and nighttime device use as well as their access to inappropriate content to prevent them from being exposed to undesirable material on the internet.

The internet is full of interesting websites, but you might not consider all content desirable or appropriate, especially for children. With the content filtering, you can ensure your children view only appropriate content on their devices by restricting what web pages they can access.

With the device use limits, you can schedule the time that your children can spend online. You can specify the daily device use times for weekdays and weekends separately. You can also limit the device use during nighttime for school nights and weekend nights.

**Note:** Each device having the F-Secure app should have its own profile. When installing the app on a child's device, assign a child profile for the device. Only then can you use Family Rules to limit the child's device use.

**Note:** The Family Rules settings can be edited only on the parent's device or through the online management portal.

#### 4.1 Protecting your child's device

This topic describes how to start protecting your child's devices.

**Note:** Each device having the F-Secure app should have its own profile. When installing the app on a child's device, assign a child profile for the device. Only then can you use Family Rules to limit the child's device use.

To set up protection for your child:

1. Open the F-Secure app.
2. On the main view, select **People & Devices**.
3. On the **People & Devices** view, select + **Add device**.
4. Select **My child's device** > **Continue**.

**Note:** If you have previously already added child profiles, they are listed here. To add a new child profile, select **New child profile**.

5. Select how you want to deliver the installation link to the device you want to protect and then select **Send link**.
6. Open the message with your child's device and follow the installation instructions.
7. Select **Install from app store** to go to the app store and select **Install** to start the installation.
8. When the installation is complete, select **Open** to start the application.

The welcome page opens.

9. Agree to the End User License Terms by selecting **Accept and continue**.
10. When prompted, log in to your account.
11. As you are setting up protection for your child, select **Install for a child?**

**Note:** If you have previously already added child profiles, they are listed here. From the **Set up protection** for drop-down, select **New child profile** and then select **Continue**.

The **Create new child profile** view opens.

12. Enter the name of the child, select the age group the child belongs to, and then select **Next**.

The **Family Rules settings** view opens.

13. Select **Next**.

The **App Control** view opens.

14. Select **Turn on App Control** and do the following:
  1. Select the default setting for all new apps that will be installed on the device: **Time-limited** or **Blocked**.
  2. Select the setting for the apps that are already installed on the device: **Time-limited**, **Always allowed** or **Blocked**.
  3. Select **Next**.

The **Daily Time Limits** view opens.

15. Turn on **Daily Time Limits**, use the sliders to limit the daily use time of the apps that you have selected as Time-limited on weekdays and weekends, and select **Next**.

The **Bedtime** view opens.

16. Turn on **Bedtime** by using the sliders to limit the nighttime use of apps or device on school nights and weekend nights, and select **Next**.

The **Content Filtering** view opens.

17. Turn on **Content Filtering**, select the categories of web content you wish to block, and select **Next**.
18. To allow the app to access files, select **Allow > Allow**.
19. To allow the app to block apps and limit device use, and to prevent children from removing protection or uninstalling, you need to turn on accessibility:

**Note:** The following steps depend on the device model you use. Consult your device manual for more information.

1. Select **Allow**. The **Turn on accessibility** window opens.

2. Select **Continue**.
3. Select **Installed services**.
4. Select **F-Secure TOTAL > Off > Allow** to allow the app to have full control of your child's device.

Your child's device is now protected.

For ease of use, you can manage your child's online activity on your own device. This is a versatile way to make changes, add or remove restrictions on the fly without having your child's device physically with you.

#### 4.2 Making changes to existing child profile settings

At times you need to make changes to the family rule settings that you have set for a child.

As your children become older, you may need to change the age group they belong to. The time limits may also need some adjustments. Or you may not need the child profile any longer and want to remove it.

**Important:** For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

To edit the settings of a child profile:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

On the **Child profile** view, you can add new devices as well as make changes to the existing devices, family rule and profile settings of the child.

3. On the **Child profile** view, select the device you want to edit, and on the **Device** view you can do the following:
  - edit the device name
  - release the license allocated for the device.

**Note:** You need to log in to your account to confirm the license release.

4. On the **Child profile** view, you can immediately see which **FAMILY RULES** settings have been turned on and which are off. You can edit the following settings:
  - App Control (Android only)
  - Daily Time Limits (excluding devices running on iOS)

- Bedtime
- Content Filtering.

5. On the **Child profile** view, you can make the following changes to the **Profile settings**:

- edit the child's name
- move the child to another age group
- remove the child's profile.

**Note:** You need to log in to your account to confirm the profile removal.

### 4.3 Editing App Control settings

This topic describes how to make changes to current App Control settings (Android only).

With App Control, you can select which apps are always allowed, which are limited by daily time limits and bedtime settings, and which are always blocked on the child's devices.

If App Control is turned off, daily time limits and bedtime settings no longer apply to specific apps but restrict the use of the whole device. Calling and SMS messages are always allowed.

**Important:** For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the App Control settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **App Control**.

The **App Control** view opens. If **App Control** is turned off, use the switch to turn it on.

4. To see a list of current devices which use **App Control**, select **Which devices App Control works on**.

**Note:** App Control is supported only by devices running on Android.

5. Under **DEFAULT SETTING**, you can define how a newly-installed app is treated by App Control:

- **Time-limited** - This means that the app use is restricted by daily time limits and bedtime limits.
  - **Always blocked** - This means that the app cannot be used at all.
6. Under **ALL CURRENT APPS**, you can see the apps that have already been installed on the device. For each app, you can define separately how it is treated by App Control:
- **Time-limited** - This means that the app use is restricted by daily time limits and bedtime limits.
  - **Always allowed** - This means that the app use is not restricted by daily time limits nor bedtime limits.
  - **Always blocked** - This means that the app cannot be used at all.
7. To save the changes, select **Save**.

#### 4.4 Editing daily time limit settings

This topic describes how to make changes to current daily device use times.

You can control when and for how long a child can use the device.

**Important:** For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the daily time limit settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Daily Time Limits**.

The **Daily Time Limits** view opens. If **Daily Time Limits** is turned off, use the switch to turn it on.

4. On the **Daily Time Limits** view, set the maximum number of hours that your child is allowed to use the device on weekdays and at weekends:
  1. For **Weekdays**, use the slider to change the maximum time allowed per day.
  2. For **Weekends**, use the slider to change the maximum time allowed per day.

**Note:** If you do not want to limit the amount of time that the child uses the device each day, drag the slider as far to the left as possible to set the allowed number of hours to **Unlimited**.

5. To save the changes, select **Save**.



#### 4.5 Editing bedtime settings

This topic describes how to make changes to current bedtime settings.

Use the bedtime settings to prevent the use of the device during night time. Calling and SMS messages are always allowed. You can set a different bedtime for school nights—from Sunday night to Thursday night—and weekend nights—from Friday night to Saturday night.

With Android devices, turn on App Control to choose which individual apps are affected by the bedtime settings.

**Important:** For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the bedtime settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Bedtime**.

The **Bedtime** view opens.

4. On the **Bedtime** view, prevent the nighttime use of the device as follows:
  1. Turn on the **School nights** setup pane and drag the slider to set the time when bedtime starts and ends.
  2. Turn on the **Weekend nights** setup pane and drag the slider to set the time when bedtime starts and ends.
5. To save the changes, select **Save**.

#### 4.6 Editing content filtering settings

This topic describes how to make changes to current content filtering settings.

You can keep your children safe from the many threats on the internet by limiting the types of content they can view while browsing the web.

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

**Important:** For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

To select the types of web content to block on all browsers:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Content Filtering**.

The **Content Filtering** view opens. If **Content Filtering** is turned off, use the switch to turn it on to block the content you don't want children to have access to.

4. Enable Safe Search to hide undesired content from search results.

**Note:** Safe Search supports the following search engines on Windows and Mac computers: Google, Bing, DuckDuckGo, Yahoo and YouTube. On Android and iOS devices Safe Search supports the following search engines: Google, Bing, and DuckDuckGo when using Safe Browser.

5. Under **BLOCKED CONTENT CATEGORIES**, check that the content categories which you don't want your children to have access to are blocked.

**Note:** Click on the content category to see more detailed information about it.

6. To save the changes, select **Save**.

#### 4.7 Content categories

You can block access to several types of content.

##### Adult content

Websites that are aimed at an adult audience with content that is clearly sexual, or containing sexual innuendo. For example, sex shop sites or sexually-oriented nudity.

##### Disturbing

Websites that contain images, explanations, or video games that can be disturbing. This category contains information, images and videos that are disgusting, gruesome or scary, which can potentially disturb younger children.

### **Drugs**

Websites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.

### **Gambling**

Websites where people can bet online using real money or some form of credit. For example, online gambling and lottery websites, and blogs and forums that contain information about gambling online or in real life.

### **Alcohol and tobacco**

Websites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and websites of bars and night clubs.

### **Illegal**

Websites that contain imagery or information that is banned by law.

### **Illegal downloads**

Unauthorized file sharing or software piracy websites. For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.

### **Violence**

Websites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bomb, assault, murder, and suicide.

### **Hate**

Websites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals or institutions, or contain descriptions or images of physical assaults against any of them.

### **Weapons**

Websites that contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and bb guns.

### **Dating**

Websites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.

### **Shopping and auctions**

Websites where people can purchase any products or services, including sites that contain catalogs of items that facilitate online ordering and purchasing and sites that provide information on ordering and buying items online.

### **Streaming media**

Websites and services that let users stream various kind of videos, often without age restrictions.

### **Social networks**

Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.

### **Anonymizers**

Websites that allow or instruct people on how to bypass network filters, including web-based translation sites that allow people to do so. For example, sites that provide lists of public proxies that can be used to bypass possible network filters.

## Unknown

Websites that are new or unknown to our web filters. The content of these websites cannot be confirmed.

### 5. Sharing protection with a family member or friend

This topic describes how to share the protection with a family member or a friend.

When you invite family members or friends to your group, the invited persons get their own user account that allows them to protect their devices using your licenses.

**Note:** Note that if the person you want to invite to your group has already been added to your group or belongs to another My F-Secure group, you will see a message in the invitation dialog, saying that the person already belongs to your group or to another group. This means that the email address used in the invitation has already been activated for an F-Secure account. You can solve this either by using another email address, if any, to invite the user to your group or you can ask this user to delete the existing F-Secure account after which you can then use the email address in the invitation.

To share protection with someone else:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select + **Add device**.
3. Select **Someone else's device** > **Continue**.
4. To invite a user to your group:
  1. Enter the first name of the user.
  2. Enter the last name of the user.
  3. Enter the email address of the user.
  4. Select **Send Invitation**.

This person receives the invitation email and now has an account that allows them to protect their devices using your licenses. The users in your group won't see the devices or other details of other users or profiles in the group.

#### 5.1 Did you receive an invitation to protect your devices?

This topic describes how to start protecting your devices if you have received an invitation from your friend.

When your friend shares the protection with you, you'll receive an email in which you are invited to use their licenses to protect your PC, Mac, smartphone and tablet for free. We have already created an account for you, and you can find your account details in the message.

To start protecting your devices:

1. Open the invitation email and read it through carefully. Take note of your account details.
2. Select **Start now**.

Your account login page opens.

3. Enter your account login credentials sent to you in the invitation email and select **Log in**.

The **Change your password** window opens.

4. Create a new strong password for your account, select **Change**, and then select **Continue**.

Your online management portal opens. Start protecting your devices by selecting **Add device** to install the product to one of your devices.

You can now manage your own devices and their protection either through the online management portal or through the product's **People & Devices** view. As an invited user, you can manage your account as follows:

- Protect more of your own devices if the subscription allows.
- You can change the name of the device being protected.
- You can release the license in use. Note that the subscription owner, or the person who invited you to share the protection, can remove your licenses at any time.
- You can leave the group at any time.
- You can make changes to your account settings, such as changing the account password and taking 2-step verification into use.

## 5.2 Stop sharing protection with a family member or friend

This topic describes how to stop sharing protection with a family member or friend.

If you want to stop sharing protection with a family member or a friend, you can remove the sub-user from your My F-Secure group.

To remove a sub-user:

1. On the main view, select **People & Devices**.
2. Select the sub-user you want to stop sharing protection.
3. Select **Remove from group**.
4. To confirm the removal, you need to log in to your F-Secure account. Select **Log in**, enter your account credentials and then select **Log in**.

The **Remove from group** window opens.

#### 5. Select **Remove**.

The sub-user is removed from your My F-Secure group and is no longer protected by your subscription.

Alternatively, you can stop sharing protection and remove sub-users through the My F-Secure portal.

### 5.3 Releasing a license from a device

This topic describes how to release a license that is no longer needed for a device.

If you have a device that no longer needs a license, we recommend that you release the license. Only then can the license be used on another device. For example, if you buy a new computer, phone or tablet and the old one is no longer used, you need to release the license used by the old device before the license can be assigned to the new device.

To release a license from a device:

1. Open the F-Secure app.
2. On the main view, select **People & Devices**.
3. Select the user from whom you want to release the license.

A list of protected devices of the user is shown.

4. Select the device that you want to release a license from.

Basic details about the device are shown.

5. Select **Release license**.

**Note:** To confirm the license release, you may need to log in to your account. Select **Log in**, enter your account credentials and then select **Log in**.

The **Release license** window opens.

6. Select **Release license**.

This frees up the license that you can now use on another device.

Alternatively, you can release a license that is no longer needed through My F-Secure.

**Note:** Releasing a license from a device does not uninstall the security app from the device. To uninstall the app, you have to do it manually from the device.

## 6. Device Protection

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

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

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

DeepGuard provides an additional layer of security to help protect your personal data against being deleted, ransomed, or stolen by harmful applications.

## 6.1 Using automatic scanning

Automatic scanning protects your computer in real time by removing harmful files from your computer before they can damage it.

We recommend that you keep automatic scanning 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 automatic scan.

By default, automatic scanning is turned on when you install the security product on your computer.

To make sure that automatic scanning is on:

1. Open the F-Secure app.
2. If the product's main view shows a notification about automatic scanning being off, select **Turn ON**.

For detailed information about this critical issue, select **More details...**

## 6.2 How automatic scanning works

Automatic 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, automatic scanning scans the file for malware before it allows your computer to access the file.

If automatic scanning finds any harmful content, it puts the file to Trash before it can cause any harm.

## Does automatic 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 automatic scanning takes depend on, for example, the contents, location and type of the file.



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

**Note:** Compressed files, such as .zip files, are not scanned by automatic scanning.

If you want to follow the scanning activity on your computer, you can choose to display the scan activity indicator in the menu bar in the following way:

1. Click the product icon in the menu bar and select **Settings**.
2. To be able to make changes to the settings, you need administrative rights: select the lock icon in the bottom-left corner.
3. In the **Device Protection** tab, select **Show automatic scan activity indicator in menu bar**.

Automatic 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 automatic scanning off temporarily

This topic describes how to temporarily turn off automatic scanning.

**Warning:** Disabling automatic scanning can make your computer vulnerable to storing harmful software on your hard drive and allowing it to run.

To turn automatic scanning off:

1. On the main view of the app, select **Device Protection**.
2. Select **Settings**.
3. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

4. In the **Device Protection** tab, select the time when to automatically turn scanning on again and then select **Disable**.

As soon as you turn off automatic scanning a notification of a critical task appears on the product's main view. You can turn automatic scanning on again at any time by selecting **Turn on** from the task and then by selecting **Re-enable** in the product settings.

### 6.3 Running a virus scan manually

You can scan your 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.

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

1. Open the F-Secure app.
2. On the main view of the app, select **Device Protection**.
3. Select **Antivirus scan**.
4. Select what you want to scan.

To scan your entire computer, select **Virus and spyware scan** > **Start scan**.

To scan specific files or folders:

1. Select **Choose what to scan** > **Choose**.

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

2. Select the files or folders that you want to scan and then select **Open**.

The scan starts. When the scan is completed, you can see the scan result in the scan window.

## 6.4 Excluding files or folders from scanning

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

To leave out files or folders from automatic and manual scanning:

1. Open the F-Secure app.
2. On the main view of the app, select **Device Protection**.
3. On the **Device Protection** view, select **Manage scanning exclusions**.

This opens the settings.

4. Select the lock icon to allow changes, then select **Set scanning exclusions**.

This opens the list of excluded files and folders.

5. Select + and then select the file or folder that you want to exclude from scanning.

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

## 6.5 What is DeepGuard?

DeepGuard provides an additional layer of security to help protect your personal data against being deleted, ransomed, or stolen by harmful applications.

DeepGuard makes sure that you use only safe applications. The safety of an application is verified from the trusted cloud service. If no information is available, DeepGuard displays a permission dialog that asks you to deny or allow the application.

By checking the file reputation, DeepGuard improves the detection of system compromises. It also makes sure that applications that do not respect privacy are prevented from using your webcam, installing new startup programs, taking control of other programs, eavesdropping on your internet connection, or other such activities that can affect your privacy.

To make sure that DeepGuard is active:

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **DeepGuard** tab.
3. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

4. You have the following options to choose from:
  - By default, **Monitor applications** is enabled. DeepGuard monitors applications for potentially harmful system changes.
  - Select **Let non-administrators save new rules** if you want to apply new DeepGuard rules without using an administrator account.
  - Select **Use advanced mode for prompts** if you want more options when DeepGuard asks you how to handle new applications. This allows you to create more detailed rules for handling specific applications or their access to certain files and folders on your computer. When DeepGuard detects a previously blocked or unknown application in advanced mode, select **Details** on the permission dialog to modify or adjust the rule for the application.

**Note:** All DeepGuard rules are visible to all users. The rules may include filenames and folder names with personal information. Therefore, be aware that other users of the same computer can see the paths and filenames included in the DeepGuard rules.

## 6.6 Selecting the DeepGuard security level

DeepGuard has three different security levels, or rulesets, that you can choose from, depending on how closely you want to monitor activity on your computer.

To change the ruleset:

1. Click the product icon in the menu bar and select **Settings**.

2. Select the **DeepGuard** tab.
3. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

4. Select **Configure DeepGuard**.

The **DeepGuard Configuration** app opens.

5. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

6. In the **DeepGuard Configuration** app, select the security level from the **Ruleset** drop-down menu.

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

- **Default:** This level allows most built-in macOS applications and processes to work normally. It does not monitor read operations on your computer, but does check attempts to write or run files.
- **Classic:** This level allows most built-in macOS applications and processes to work normally. It monitors attempts to read, write, or run files.
- **Strict:** This level only allows access to essential processes. It gives you more detailed control over system processes and built-in applications.

## 6.7 Optimizing DeepGuard for your system

You can use DeepGuard's learning mode to create rules that allow applications and operations that appear when you use your computer normally.

When you start the learning mode, use your computer as normal and start any applications that you want DeepGuard to allow. DeepGuard allows all file access attempts and creates customized rules for your computer that you can import when you stop the learning mode.

The learning mode is most useful for the **Classic** and **Strict** rulesets. If you are using the **Default** ruleset, you probably do not need the learning mode.

**Warning:** DeepGuard does not protect your computer while learning mode is in use.

To use the learning mode:

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **DeepGuard** tab.
3. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

4. Select **Configure DeepGuard**.

The **DeepGuard Configuration** app opens.

5. In the **DeepGuard Configuration** app, select **File > Learning Mode**, and when prompted, enter your admin credentials.
6. Select **OK** to start the learning mode.
7. Start the applications that you normally use on your computer.
8. Go back to the **DeepGuard Configuration** app and select **File > Learning Mode** again to stop the learning mode.

DeepGuard shows you a list of applications that you can import as rules, which allows the selected applications to access files on your computer.

9. Select the applications that you want to allow, then select **Import**.

You can later edit the imported rules in the **DeepGuard Configuration** app.

## 6.8 Allowing applications that DeepGuard has blocked

If DeepGuard has blocked an application that you trust and want to allow, you can edit the rule for that application in the **DeepGuard Configuration** app.

**Note:** The rules that DeepGuard creates are not user-specific, so they are visible to everyone who uses the same computer. For example, most macOS apps use the /Applications folder to install apps, which are then available to all users of the computer. This means that any rules that DeepGuard applies to such apps have a system-wide effect.

To allow an application that DeepGuard has blocked:

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **DeepGuard** tab.
3. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

4. Select **Configure DeepGuard**.

The **DeepGuard Configuration** app opens.

5. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

6. In the **DeepGuard Configuration** app, right-click the rule for the application that you want to allow and select **Edit**.
7. Select **Allow** as the **Policy** for the application.

8. Select the permissions that you want to allow for the application.
9. Select **Save**.

## 6.9 What harmful content does

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

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

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

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

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

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

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

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

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

## 6.10 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

## 6.11 Trojans

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

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

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

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

- **Trojan-downloader:** connects to a remote site to download and install other programs
- **Trojan-dropper:** contains one or more extra programs, which it installs
- **Trojan-pws:** Steals passwords stored on the device or entered into a web browser



- **Banking-trojan:** A specialized trojan-pws that specifically looks for usernames and passwords for online banking portals
- **Trojan-spy:** Monitors activity on the device and forwards the details to a remote site

## 6.12 Backdoors

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

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

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

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

## 6.13 Exploits

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

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

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

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

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

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



## 6.14 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.

## 6.15 Submitting a sample

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

When the product blocks an application, for example because it is a possible security risk for your computer or the application tried to do something potentially harmful, you can send us a sample of the application for security research purposes. You can do this if you know that the application that the product blocked incorrectly is safe or if you suspect that the application may be harmful.

Also, if you suspect that a website is unsafe, you can send us its URL for analysis.

To submit a sample for analysis:

1. Open the F-Secure app.
2. On the main view of the app, select **Device Protection**.
3. On the **Device Protection** view, select **Submit a sample**.

This opens the **Submit a sample** web page in your default web browser where you can submit either a file or a URL sample for analysis.

4. Fill in the form on the web page to submit your sample.

## 7. Scam Protection

This section explains how the app can ensure safe browsing on the internet, as well as safe online banking. The app also protects you against other common scams.

Browsing protection shows you safety ratings for websites listed on search engine results. By identifying websites 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 of websites are based on the analysis from our website reputation service.

Browsing protection works with the Safari, Microsoft Edge, Mozilla Firefox, and Google Chrome browsers.

### 7.1 Reputation rating icons in search results

Browsing Protection shows a website safety rating on the search results page when you use Google, Bing, Yahoo, or DuckDuckGo.

Color-coded icons show the safety rating of a current site. The safety rating for each link on the search results page appears with these same icons:



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



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



The site is harmful. We recommend that you avoid visiting this website. Alternatively, an administrator has blocked this site and you cannot visit it.



We have not analyzed the website yet or no information is currently available for it.



Access to this website is never blocked.

If you think that the blocked site is safe and should not be blocked at all, you can submit the website for analysis [here](#) or report it directly by using the browsing protection extension icon on the browser toolbar.

If you cannot see any reputation rating icons on the search results page, make sure the setting is turned on:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.

3. Select **Settings**.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Make sure that **Browsing Protection** is turned on.
6. Select **Show the reputation rating for websites in search results**.
7. If your browser is open, restart your browser to apply the changed settings.

**Note:** Browsing Protection requires that the Browsing Protection extension is turned on in the web browser that you use.

## 7.2 Blocking harmful websites

Browsing protection blocks access to harmful websites when it is turned on.

Browsing protection is automatically turned on when you take the product into use.

To make sure that Browsing protection is on:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Make sure that **Browsing protection** is selected.

**Note:** Browsing protection requires that you install and enable the extension for the web browser that you use. The product supports the Safari, Microsoft Edge, Mozilla Firefox, and Google Chrome browsers.

## 7.3 Allowing blocked websites

You can manually allow websites that the product has blocked if you are sure that they are safe.

To allow a blocked website:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Manage allowed and blocked websites**.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Under **Allowed websites**, select **Set allowed websites**.

The **Add the websites that you want to allow** window opens.

6. To add a website to the list of allowed websites, select + from the bottom-left corner of the window, enter the address of the website you want to allow, and press Enter.

The website is now listed as an allowed website.

7. To remove a website from allowed websites, select the address of the website and then select - from the bottom-left corner of the window.
8. To close the window, select **Done**.

#### 7.4 Allowing blocked websites manually

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

1. If you want to enter the website, select **Allow website on this computer > Allow**.
2. Enter your administrator password and select **OK**.

The blocked website opens. Also, the product adds the website to the allowed websites list.

If you think that the blocked site is safe and should not be blocked at all, you can submit the website for analysis [here](#).

#### 7.5 Turning on banking protection

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

Banking protection automatically detects secure connections to recognized online banking websites, and notifies you when you visit any such site.

Banking protection currently supports the following browsers:

- Safari
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

**Note:** Banking protection requires that browser extensions are in use.

By default, Banking protection is enabled. If it is not enabled, turn on Banking protection in the following way:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Select **Banking protection**.

As soon as your banking session is over, the clipboard will be cleared automatically. If you wish, you can change this setting in the Secure browsing settings.

## 7.6 Shopping safely online

Shopping Protection makes your online shopping sessions more secure by notifying you of fake and untrustworthy websites.

**Note:** Shopping Protection requires that the Browsing Protection extension is enabled in the web browser that you use.

By default, Shopping Protection is switched on to improve the safety of your online shopping. Upon entering a shopping website, a safety rating pop-up is displayed in the lower-right corner of the page to indicate how trustworthy the website is. If the shopping site is safe, the pop-up disappears after a few seconds and will not be shown again on the site during the shopping session. However, if the site is not safe, the pop-up warning will stay on the page until you leave the site.

You can adjust when the notifications are shown in the product settings, for example if you do not want to see notifications for safe shopping websites.

The safety rating pop-up is displayed also when you enter a shopping site by clicking a link, for example in an email or text message.

The safety ratings are also represented as informative icons on search results pages when you use popular search engines like Google, Bing, Yahoo, or DuckDuckGo. When you hover the mouse over the rating icon, you will see details about the safety of the website.

This information is also accessible via the browser extension icon in the browser toolbar.

To change the settings for Shopping Protection:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Switch **Shopping Protection** on or off.
6. Select or clear **Show notifications for safe shopping websites** and **Show notifications for suspicious shopping websites** according to what notifications you want to see.

## 7.7 Blocking advertisements on websites

Ad blocker blocks advertising content on the websites that you visit, making it harder to track you and improving your browsing experience.

By default, Ad blocker is switched on to prevent loading content from common advertising servers. The top right corner of the **Secure Browsing** view shows you the number of advertisements that the product has blocked.

If a page that you visit does not load correctly without advertisements, you can switch Ad blocker off temporarily:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Switch off **Block ads**.

When you reload the page in your browser, it will include advertisements.

## 7.8 Rejecting non-essential cookies

The Cookie Popup Blocker feature helps protect your privacy while browsing by avoiding unnecessary cookies.

Websites use cookies for various purposes, such as storing information related to your session, identifying your account, or tracking the pages that you browse. While some cookies are often necessary to make a website usable, some can be used to collect data on your online activity. This is why different regional authorities have implemented legislation that requires websites to ask for consent on the use of cookies from anyone visiting that site.

Cookie Popup Blocker identifies known cookie consent providers on websites that you visit and automatically rejects non-essential cookies. However, not all websites use such providers, so the feature does not work on those websites.

To change the settings for Cookie Popup Blocker:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Switch **Cookie Popup Blocker** on or off.

## 7.9 Checking that browser extensions are in use

Browsing protection **requires** browser extensions to be able to protect your web browsing, online banking and shopping, and to show you security information while you are browsing the internet.

Once you have installed the product on your computer, the product requires you to install and switch on the browser extension for the web browser that you use.

Also, the main view of the product shows you if the browser extension has not yet been set up. An easy way to set up the extension for your browser is to select **Set up** from the notification shown on the product's main view and follow the on-screen instructions.

To install and switch on the extensions for the browsers that you use, see the related instructions.

### 7.10 Installing and enabling browser extension for Safari

You need to install and enable the browser extension for Safari to be able to use the Safari browser safely.

To set up the browser extension:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select **Set up Safari extension**.
5. Select **Get > Install** to install the extension from App Store.
6. Once the installation is finished, select **Open > Quit and Open Safari Extensions Settings**.

The **Extensions** settings open. On the left, you can see which extensions are installed on your Mac.

7. Select the tickbox next to **Secure Browsing** to enable the extension.
8. Select **Turn on** to confirm that you want to enable the extension.
9. Under **Permissions**, select **Always Allow on Every Website**.

You can now use Safari to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: <https://unsafe.fstesting.net>. You should see the product block page.

### 7.11 Installing and enabling browser extension for Chrome

You need to install and enable the browser extension for Chrome to be able to use the Chrome browser safely.



To set up the browser extension:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select **Set up Chrome extension**.

The **Browsing protection from F-Secure** page opens.

5. Select **Add to Chrome > Add extension**.

You can now use Chrome to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: <https://unsafe.fstesting.net>. You should see the product block page.

## 7.12 Installing and enabling browser extension for Firefox

You need to install and enable the browser extension for Firefox to be able to use the Firefox browser safely.

To set up the browser extension:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select **Set up Firefox extension**.

The **Browsing protection by F-Secure** page opens.

5. Select **Add to Firefox > Add**.

Once the extension is installed, a user consent dialog opens. The browser extension requires your permission to access information about the websites you visit.

6. Select **Allow**.

If you decline to grant the permission, you will not be able to use the extension and Browsing protection cannot block harmful websites nor show search result ratings. Also, the extension will be removed from the browser.

7. To complete setting up the extension, select **OK**.

You can now use Firefox to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: <https://unsafe.fstesting.net>. You should see the product block page.



### 7.13 Installing and enabling browser extension for Edge

You need to install and enable the browser extension for Microsoft Edge to be able to use the Edge browser safely.

To set up the browser extension:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Select **Set up Microsoft Edge extension**.

The **Browsing protection by F-Secure** page opens.

5. Select **Get > Add extension**.

You can now use Edge to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: <https://unsafe.fstesting.net>. You should see the product block page.

## 8. VPN

The app's virtual private network (VPN) creates a secure, encrypted connection from your device to the internet.

VPN protects your connection in a WiFi network by making your data unreadable for outsiders. It even prevents anyone from changing your data or hijacking your network traffic.

When you browse the internet, data collection companies track your online activities and sell your data to advertisers. VPN blocks these tracking attempts from HTTP traffic so you can browse anonymously and undisturbed.

**Note:** This feature is not available in all versions of the app.

You can easily see how your privacy has been protected on the **VPN** view. It shows you the volume of your internet traffic that has been protected.

When you take the product into use, the app asks your permission to set up a VPN connection. You need to allow this so that VPN can monitor network traffic. Later, you can turn VPN on or off on the main view of the app.

**Important:** If you have any other VPN software, such as F-Secure FREEDOME VPN, installed on your device, make sure that you don't have both VPNs turned on at the same time. If you have FREEDOME VPN turned on and then turn Total's VPN on, the network stops working until you turn off one of the VPN connections.

### 8.1 Turning on the VPN connection

You can turn the VPN connection on or off from the main view of the app.

To turn on VPN:

1. Open the F-Secure app.
2. Under **VPN**, select the toggle switch to turn VPN on.

**Note:** When you first install the app, it shows you a **Get started** button instead of the switch.

VPN is turned on, connecting the app to the location offering the best possible connection.

3. To turn VPN off again, go to the **VPN** view and select the toggle switch above the map.

If you want that the VPN connection is automatically turned on whenever your device is turned on:

1. Open the F-Secure app.
2. On the main view, select **VPN**.
3. Select **Settings** to open the settings for VPN.
4. Turn on **Automatic VPN protection**.

From now on, the VPN connection will be automatically turned on whenever your device is turned on.

## 8.2 Marking a local WiFi network as trusted

You can mark your current network as trusted to allow connections to other devices within the same network while VPN is on.

This feature works only when the Killswitch feature is switched on. If Killswitch is switched off, you can access your local network without marking the network as trusted.

To mark a network as trusted:

1. Open the F-Secure app.
2. On the main view, select **VPN**.
3. Select **Trusted networks**.

The **Trusted networks** view opens.

4. Under **Current networks**, select **Trust network** for the network that you want to trust.

Your current network is now marked as trusted.

**Important:** Never mark networks that don't require a password as trusted.

## 8.3 Changing your virtual location

Using a virtual location protects your privacy and lets you access your favorite streaming services when abroad.

By default, the app uses the location that gives you the best possible connection. This is usually the location closest to you, but this may vary, for example, depending on the amount of network traffic.

Companies use IP geolocation to block access to their content in certain countries. With VPN, you may be able to access some of these services by changing your virtual location.

To change your virtual location:

1. Open the F-Secure app.
2. On the main view, select **VPN**.
3. Select the virtual location that you want.

The new location is immediately in use.

Your device will still know its real location, even without GPS, and apps may have permission to use it.

## 8.4 Using tracking protection

Tracking protection ensures your privacy while you browse the web, although you may have to switch it off for some apps or websites to work properly.

**Note:** This feature is not available in all versions of the app.

When you go to a website or use an app that tries to track you, VPN hides your IP address, blocks tracking cookies, and prevents apps from sending information about you to data collection sites.

Tracking protection removes all cookies set by known advertising networks, preventing the ad networks from tracking individual visitors from site to site. It also prevents communication with any tracking domains identified by F-Secure's reputation analysis.

However, many websites and services use encrypted communications (HTTPS/TLS/SSL) to transfer content, and in those cases VPN cannot decrypt the full address of linked content to reliably determine whether it is a tracking cookie or legitimate content. This means that some pages might load slowly or have missing content.

In addition, some apps may stop working due to an incorrectly blocked connection. This issue may appear if you are buying something online and the purchase flow is cut off during the transition between the online shop and your banking app, for example.

By default, tracking protection is turned on. If an app that you trust is not working or websites take a long time to load, you can try turning tracking protection off:

1. Open the F-Secure app.
2. On the main view, select **VPN**.
3. Select **Settings**.
4. Switch off **Tracking protection**.

The app does not aim to block anything going from your browser to the site you are visiting. because blocking cookies from the site you visit easily breaks login sessions, stored preferences, and other valuable features.

The anti-tracking statistics in the app only show the total amount of data that was blocked and the number of cookies that were filtered to prevent tracking. We are not able to provide more accurate data about what was blocked to our users since we do not log any traffic for privacy reasons.

### 8.5 Blocking internet access when VPN is disrupted or is being established

Killswitch cuts off the internet access and blocks connections to other devices within the same network if the VPN connection drops for some reason.

By default, the Killswitch feature is turned off when you set up the VPN connection.

To turn Killswitch on:

1. Open the F-Secure app.
2. On the main view, select **VPN**.
3. Select **Settings**.
4. Switch on **Killswitch** if you don't want to allow data traffic to bypass VPN.

### 8.6 Changing the VPN protocol used

A VPN protocol is a set of rules that your device and the VPN server use to set up the connection.

Depending on the version of the app that you have, it supports one of the following sets of VPN protocols:

- OpenVPN, OpenVPN (TCP), IKEv2
- Hydra, Wireguard, OpenVPN, OpenVPN (TCP)

By default, the app uses either the OpenVPN or Hydra protocol, depending on your version of the app.

To change the VPN protocol:

1. Open the F-Secure app.

2. On the main view, select **VPN**.
3. Select **Settings**.
4. Under **VPN protocol**, select the protocol you want to use.

## 9. Password Vault

With Password Vault, you can improve your security by creating strong and unique passwords. It also allows you to sync your passwords across all your devices which means that you have your passwords available to you no matter which one of your devices you are using. This makes signing in to your online accounts easier and safer.

### 9.1 Getting started with Password Vault

This topic describes how to get started with Password Vault.

Before you can start using your passwords and personal information in Password Vault, you have to

- create your master password – the only password that you have to remember once you have taken Password Vault into use;
- create a recovery QR code – a unique and personal code which is the only way to regain access to Password Vault if you forget your master password;
- set up autofill to automatically fill in stored usernames and passwords on websites.

**Note:** If you are an existing user of Password Vault, simply connect your devices and sync your passwords and personal information.

To get started with Password Vault:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select **Get started**.
4. Do one of the following:
  - **If you are a new user:**
    1. Select **Create Master Password**.
    2. Choose a password or passphrase that is easy to remember but only makes sense to you.
    3. Repeat the master password.
    4. Select **Create Master Password**.

5. If you forget your master password, the only way to recover it is to use a recovery QR code which you must create beforehand. Select **Save Recovery QR Code**.
  6. Select the location where you want to save the recovery QR code image and then select **Save**.
  7. Start adding your passwords and credit card details in to Password Vault.
- If you are already using Password Vault on another device or app, simply connect the devices and sync your passwords and personal information:
    1. Select **Connect devices**.
    2. Open Password Vault on your other device that already has Password Vault installed.
    3. Depending on whether the other device is a mobile device or a desktop device, do one of the following:

- On a mobile device, select



> **Connect Devices** > **Generate sync code**.

- On a desktop device, select



**Connect Devices**.

A sync code is automatically generated.

4. Enter the generated sync code to the **Sync code** field and select **Connect devices**.
5. When prompted, enter your master password that you use on the device in which you generated the sync code and select **Confirm**.

Your passwords and data are now synced across these two devices.

5. Set up autofill to access your online services without having to enter your username and password manually:

- In Password Vault, select



**Autofill**.

The **Autofill** view opens.

- Select the button to install the browser extension or add-on for the browser that you use.
- After installing the extension, go back to the **Autofill** view and select **Copy code** to copy the authorization code.

- Back in the browser, click the password manager extension icon in the top-right corner of the browser and paste the code in the field.

From now on, when you place the mouse in the username and password fields on the login page of the online service you want to access, the Password Vault icon appears in the field. Click on the icon and select the service to access it.

## 9.2 Using Password Vault

With Password Vault, you can create and edit password and payment card entries, let the app generate strong passwords for your online services, and access your password history.

Logging in to an online service with Password Vault

There are various ways you can log in to an online service whose credentials and login page web address you have stored in Password Vault.

To be able to log in to an online service:

- You must have the required details – the **username, password, and the web address** of the online service or website – stored in Password Vault.
- The password manager browser extension has to be installed for the browser that you use to access the service. This is required for the autofill to work.

Use any of the following ways to log in to an online service or website:

1. To access an online service directly from your web browser through the password manager extension icon:
  1. Make sure that your Password Vault is unlocked.
  2. On the browser toolbar, click on the puzzle piece icon to open the **Extensions** menu and select the **Password Manager by F-Secure** extension.

**Note:** If the **Password Manager by F-Secure** extension is not listed on the menu, you must set up the required extension for the browser that you are using. See **Related topics** below.

2. The **Password Vault** pop-up dialog opens.
  1. Search for the desired online service and select it when found.
  2. Select **Go to web address** and once the log-in page opens, click the Password Vault icon in the username field, and select the desired online service.

The app fills in your username and password. Note that on some login pages you have to select the password for the online service separately.

3. Select the login button.
3. To access the online service directly from your web browser:
  1. Make sure that your Password Vault is unlocked.



2. Open your browser and go the login page of the online service (website) you want to access.

If you have set up the password manager browser extension for the browser you are using, you should see the Password Vault icon in the username field.

3. Click the icon and select the online service from the drop-down list that opens.

The app fills in your username and password. Note that on some login pages you have to select the password for the online service separately.

4. Select the login button.

4. To access the online service from Password Vault:

1. Open the Total app.
2. On the main view, select **Password Vault**.
3. Select the entry of the online service you want to access.

The entry details open.

4. Select the web address of the service.

The login page of the service opens in your browser. If you have set up the password manager browser extension for the browser you are using, you should see the Password Vault icon in the username field.

5. Click the icon and select the online service from the drop-down list that opens.

The app fills in your username and password. Note that on some login pages you have to select the password for the online service separately.

6. Select the login button.

**Note:** On some login pages, the username and password are automatically filled in, and the only thing you need to do is to select the login button.

### 9.3 Storing a new password in Vault

This topic describes how to add new passwords in Vault.

To store a new password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.


3. Select  next to the **Title** field and choose a color and a symbol for the entry, then select **Update**.




Depending on the symbol you choose, the app may automatically fill in the title and web address of the website or online service.

4. In the **Title** field, enter the name of the website or online service if the app hasn't already done it.
5. In the **Username** field, enter the user name that you use for the website or service.
6. In the **Password** field, do one of the following:
  - Create a strong password or passphrase.



- Select  to let the app generate a strong, random password for you. When you are satisfied with the password, select **Update**.



**Note:** Select  if you want to view the password.

7. In the **Web address** field, enter the web address (URL) of the login page of the online service if the app hasn't already done it.

**Note:** The format of the web address must be `https://example.com`.

8. In the **Notes** field, enter any additional information you may have.
9. Select **Save**.

The entry details have now been stored in Vault.

**Important:** If you change or generate a password in Password Vault, remember also to change the password in the web service or application and vice versa.

#### 9.4 Storing your payment card information in Vault

This topic describes how to store your payment card details in Vault.

To store payment card details:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select + **Add new**.

The entry details open, showing "Password" as the default entry type.

4. From the **Type** drop-down, select **Credit card**.
5. To change the entry icon on the left, tap on it, choose a color and one of the available payment card symbols, then select **Update**.

Based on the symbol you select, the app may fill in the name and web address of the payment card company for you.

6. In the **Title** field, enter the name of the payment card company if the app hasn't already done it.
7. In the **Cardholder name** field, enter your name as it is on the payment card.
8. In the **Credit card number** field, enter your card number.
9. In the **PIN** field, enter your personal ID number linked to the card.
10. In the **Expiration date** field, enter the date (in format MM/YY) until which the card is valid.
11. In the **Verification code** field, enter your card's 3- or 4-digit security code that helps protect you from credit card fraud.
12. If desired, you can enter the web address of the card issuer in the **Web address** field.
13. In the **Notes** field, enter any other information you want to add.
14. Select **Save**.

Your payment card details have now been stored in Password Vault.

## 9.5 Editing existing data

You may need to edit a Password Vault entry at some point.

To edit an entry:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry that you want to edit.

The entry details open.

4. Select **Edit**.
5. Make the required changes.
6. Select **Save** to save the changes.

### Deleting entries

You can delete Password Vault entries that you don't need any longer.

To delete an entry:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry that you want to delete.

The entry details open.

4. Select **Edit**.
5. To delete the entry , select **Remove** > **OK**.

To delete multiple entries in one go:

1. On the entry view, select the entries that you want to delete: hold down the **Command** key and select the entries. On the right, you can see the number of entries selected.
2. To delete the selected entries, select **Delete** > **Delete**.

## 9.6 Letting the app generate a new password for an existing entry

When you need to change a password, Password Vault can generate a strong password for you.

You can choose the length and complexity of the password.


To generate a password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry whose password you want to change.

The entry details open.

4. Select **Edit** to edit the entry details.



5. In the **Password** field, select .
6. In the **Generate password** view, you can do the following:
  - Drag the slider from side to side to select the number of characters you want in your password.
  - Select the type of characters (lower and upper case letters, numbers and special characters) you want in your password.
  - Select  **Generate** to generate a new password.

7. To take the generated password into use, select **Update** > **Save**.

Accessing your old passwords

The password history log contains your previous passwords, if any, for the online service in question.

After you have changed a password in Password Vault, you may still need to log in to the online service with the old password. Also, quite often, before being able to change a password for a service, you need to enter the old password.

To access the previous passwords:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry whose previous passwords you want to view.

The entry details open.

4. In the entry details, select **Password history**.

**Note:** If you cannot see **Password history** in the entry details, there are no previous passwords available for that particular online service.

The **Password history** view opens.

5. To view a hidden password, select  next to the password.

**Note:** You can copy the desired password to clipboard by selecting  .

6. To close the **Password history** view, select **Close**.

If you want, you can delete the password history by selecting **Clear**.

## 9.7 Making sure your passwords are strong

Weak passwords make you vulnerable to identity theft.

Password Vault helps you improve your passwords.

To find out how good your passwords are:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.

3. Select  **Password Analysis**.

The **Password Analysis** view opens, showing the quality of your passwords.

4. If you have a weak password, select **Edit** next to the password.

The entry details open.

5. Edit the password to make it stronger and safer, and then select **Save** to save the changes.

**Important:** If you change or generate a password in Password Vault, remember also to change the password in the web service or application and vice versa.

6. Repeat the above until all your passwords are strong.

Connecting devices to sync your Password Vault data across all your devices

If you use Password Vault on another device or app, you can connect your devices and sync your data to have it readily available and always up to date on both devices.

Make sure that you have the devices you want to connect at hand and that you have the app already installed on both devices.

To sync your data across both devices:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.

3. Select  **Connect Devices**.

The **Connect devices** view opens, and a synchronization code is automatically generated. It is valid for 60 seconds at a time. A new code is generated immediately after the current code expires.

4. Open the app on the device with which you want to connect and sync your data, and select **Password Vault**.
5. Depending on whether the other device is a mobile device or a desktop device, do one of the following:
  - **On a mobile device:**
    1. Select **I am an existing user**. The **Connect devices** view opens.
    2. Enter the sync code generated in the first device and select **Connect**.
  - **On a desktop device:**
    1. Select **Connect Devices**.
    2. Enter the sync code generated in the first device and select **Connect devices**.
6. When prompted, enter your master password that you use on the device in which you generated the sync code and select **Confirm**.

Your data has now been synchronized between these two devices. If you have more devices to be connected, repeat the above steps with each device. Note that you can generate the sync code on any of your connected devices.

Setting up autofill to access your online services faster

You can quickly access your online services without having to enter your login credentials manually.

To automatically fill in your usernames and passwords for your online services, you first need to install the browser extension or add-on for the browsers that you use. Password Vault supports the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

**Note:** Autofill is currently not supported on Safari.

To install and authorize the browser extension:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.

3. Select  **Autofill**.

The **Autofill** view opens.

4. Do the following for all the browsers that you use:
  - For Google Chrome:
    1. Select **Install Chrome Extension**.
    2. On the Chrome Web Store, select **Add to Chrome** > **Add extension** .  
The **Password Manager by F-Secure** extension has now been added to your browser extensions.
    3. Click the extensions icon in the top-right corner of your browser and select the **Pin** icon next to **Password Manager by F-Secure**. This makes it easier to access the extension when you need to authorize it.
    4. To complete the installation of the browser extension, you still need to authorize the extension as follows:
      1. Go back to Password Vault, and at the bottom of the **Autofill** view, select **Copy code** to copy the authorization code needed to complete the setup.

2. Back in the browser, click on the extensions icon in the top-right corner of your browser, select **Password Manager by F-Secure** and paste the copied authorization code in the window that opens.
  3. Select **Authorize > Close**. The browser extension is now enabled.
- For Mozilla Firefox:
    1. Select **Install Firefox Add-on**.
    2. On the Firefox ADD-ONS page, select **Add to Firefox > Add**. The extension has now been added to your browser and the Password Manager by F-Secure icon appears in the top-right corner of the browser.
    3. To complete the installation of the browser extension, you still need to authorize the extension as follows:
      1. Go back to Password Vault, and at the bottom of the **Autofill** view, select **Copy code** to copy the authorization code needed to complete the setup.
      2. Back in the browser, click the **Password Manager by F-Secure** extension icon in the top-right corner of the browser and paste in the copied authorization code in the window that opens.
      3. Select **Authorize > Close**. The browser extension is now enabled.
  - For Microsoft Edge:
    1. Select **Install Edge Add-on**.
    2. On the Edge Add-ons page, select **Get > Add extension**. The **Password Manager by F-Secure** extension has now been added to your browser extensions.
    3. To complete the installation of the browser extension, you still need to authorize the extension as follows:
      1. Go back to Password Vault, and at the bottom of the **Autofill** view, select **Copy code** to copy the authorization code needed to complete the setup.
      2. Back in the browser, click on the extensions icon in the top-right corner of your browser, select **Password Manager by F-Secure** and paste the copied authorization code in the window that opens.
      3. Select **Authorize > Close**. The browser extension is now enabled.

From now on, once you place the mouse on the username and password fields on the login page of the online service you want to access, the Password Vault icon appears on the field. Click on the icon and select the service to access it.



## Importing passwords from other password managers

Instructions on how to import passwords from other compatible password managers to Password Vault.

You can import passwords from other password managers that support export to open text format. Importing is possible only with the Windows and Mac versions of the product.

Password Vault supports importing passwords from the following password managers:

- Dashlane
- F-Secure ID PROTECTION
- Google Chrome
- KeePassX V2
- LastPass
- Microsoft Edge
- Mozilla Firefox
- True Key

In addition, you can import passwords from any other instance of Password Vault, for example a previously installed F-Secure app or a service provider version that includes Password Vault.

To import passwords into Password Vault:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.



3. Select **Settings > Import passwords**.

4. From the drop-down list, select the password manager from where you want to import the passwords.

**Note:** Instructions on how to export your passwords from the chosen password manager in to a file are shown. To find out detailed instructions on how to export passwords from your old password manager product, consult the product documentation of the password manager in question.

5. Once you have exported and saved the file locally, either drag and drop it to Password Vault, or select **Choose file to import**, locate the file, and finally select **Open**.

After a successful import, you will be shown the number of imported passwords.

## 9.8 Exporting Password Vault data

Instructions on how to export your Password Vault data.

You can export your data from Password Vault to a decrypted file. Exporting is possible only with the Windows and Mac versions of the product.

To export your Password Vault data:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.



3. Select **Settings > Export passwords**.
4. Select **Export my vault**.

The **Confirm with Master Password** window opens.

5. Enter your master password and select **Confirm**.
6. Select the location where you want to save the file and select **Export**.

By default, your password data will be saved in the ExportedPasswords.fsk file.

7. Select the location where you want to save the file and then select **Save**.

The number of exported passwords and the file path are shown.

**Note:** When you export your Password Vault data, the file is exported as plain text and can, therefore, be read easily by others. If you need to store this file, store it where it cannot be easily accessed or damaged. Also, remember to delete the file once you have transferred the data.

## 9.9 Changing your master password

This topic describes how you can change your Password Vault master password.

To change your master password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.



3. Select **Settings > Change Master Password**.
4. Enter your current master password.
5. Enter your new master password.
6. Repeat the new master password and select **Change Master Password**.

Your master password has now been changed. Once you have changed your master password on one device, you must use the new password on all your connected devices.


**Note:** When you change the master password for any reason, you need to create a new recovery QR code. Any old code will no longer be valid. Therefore, make sure that the recovery QR code is always up to date and valid for your current master password.

#### Creating a recovery QR code for the master password

This topic explains how to create a recovery QR code for your Password Vault master password.

**Important:** We strongly recommend that you create a recovery QR code for your master password when you take Password Vault into use. It is the only way for you to regain your master password if you forget it.

To create your master password recovery code:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select  **Settings > Create Recovery QR Code**.

The recovery code image is automatically created.

4. Select **Save** to save the image.
5. Enter your master password and select **Confirm**.
6. Select the location where you want to save the file, and select **Save**.
7. Go to the folder, and print out the recovery code image.

**Note:** We recommend that you save the code as an image and print out the file for safekeeping, rather than store it in a cloud storage service.

#### Using the recovery QR code to recover your forgotten master password

This topic explains how to recover your Password Vault master password by using the recovery QR code.

**Important:** You can recover your master password only if you have previously created a recovery QR code for it.

To recover your master password with the recovery QR code:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.

3. On the login screen, select **Forgot Master Password?**.

The **Forgot Master Password?** view opens.

4. Select **Import**.
5. Find and open the recovery QR code image file which you have created earlier.

Your master password appears on the screen.

6. Enter your master password and select **Unlock**.

Password Vault opens.

## 8.10 Unlocking and locking Password Vault


This topic shows you how to unlock Password Vault.


**Important:** To keep your passwords and personal information safe, we recommend that you lock Password Vault whenever you are not using it.

To unlock Password Vault, do the following:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Enter your master password and select **Unlock**.

**Note:** By default, Password Vault locks itself automatically after five minutes. To set the time

after which Password Vault locks itself, go to  **Settings > Automatic Lock**, and select the time. The options are 5 minutes, 15 minutes, 30 minutes, 60 minutes, 10 hours, and 1 week.

4. To lock Password Vault manually, select  **Lock** from the left navigation.

## 10. ID Monitoring

With **ID Monitoring**, you can add email addresses and other items for monitoring and receive guidance on what to do if your personal information has been leaked in a data breach.

The notification email includes information on what personally identifiable information (PII) has been associated with the breach; what the breach was; what company or entity was breached; when the breach took place; and what other pieces of PII has been associated with the monitored email address, such as passwords, credit card numbers, street address, and so on.

You can add up to 10 items of each type for monitoring; that is, 10 email addresses, 10 payment cards, 10 phone numbers, etc.

## 10.1 Adding items for monitoring

This topic describes how to add items for monitoring.

The first item you add for monitoring must be your email address. Only after having added the email address for monitoring can you add other items, such as usernames and credit card numbers for monitoring. This address will also be the email address to which F-Secure sends notifications if your information appears in a data breach.

To add more items for monitoring:

1. Open the F-Secure app.
2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Monitored Items**.

The **Monitored Items** view opens.

4. Select **+ Add item**.

The **Add new** dialog opens, listing all the available item types to choose. Note that if you have not yet added any email address for monitoring, the product asks you first to add an email address for monitoring. Only after that can you add other types of items for monitoring.

5. Select the type of item you want to add for monitoring.

The **New Monitored Item** view opens.

6. Enter the requested information and select **Add**.

Monitoring immediately starts looking for breaches with your personal data and shows you the result of the search. Note that to be able to see more detailed information about your leaked data, if any, and the recommended actions, make sure that you have confirmed your contact email address.

7. If you have not yet confirmed your email address, open the confirmation email, and select the link to confirm that this is your email address.
8. To see the details of your exposed personal information and what you should do, select the specific breach listed in the **ID Monitoring** view.

**Important:** If your information has been exposed in a data breach, we urge you to execute the recommended actions as soon as possible to eliminate the risk of your information being misused.

## 10.2 Editing and deleting monitored items

This topic describes how to edit and delete a monitored item.

**Note:** You cannot directly edit an item that is added for monitoring. If you need to edit an existing monitored item, first delete the item and then add it again for monitoring.

To delete a monitored item:

1. Open the F-Secure app.
2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Monitored Items**.

The **Monitored Items** view opens, listing all your currently monitored items.

4. To delete an item from the list, first select  next to the item you want to remove and then select **Delete**.

The **Delete Monitored Item?** dialog opens.

5. To confirm that you want to stop monitoring the item, select **Delete**.

The item disappears from the monitored items.

**Note:** To edit your contact email address or to delete it from monitoring, you need to delete all other monitored items, if any, before you can edit or delete the contact email address.

### 10.3 Changing your contact email address

You will receive notifications to your contact email address as soon as any of your monitored items appears in a data breach.

The first email address that you add as a monitored item becomes automatically your contact email address.

To change your contact email address:

1. Open the F-Secure app.
2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Monitored Items**.


The list of your monitored items opens.

4. If you haven't yet added the email address that you want to use as the new contact email address to the monitored items, do as follows:
  1. Select **+ Add item > Email** and then enter the email address and select **Add**.

An email with a confirmation link is sent to the address you entered.

2. Open the email and confirm your email address.

Once confirmed, the email address can be used as your contact email address.

5. In the **Monitored Items** view, select first  next to the email address and then select **Assign as contact information > Assign**.

Your new contact email address is now in use.

**Note:** To edit your contact email address or to delete it from monitoring, you need to delete all other monitored items, if any, before you can edit or delete the contact email address.

## 10.4 Security Data

The service sends queries on potential malicious activities or on protected devices to the F-Secure Security Cloud.

The F-Secure Security Cloud is a cloud-based system for cyber threat analysis that is operated by F-Secure. We collect the minimum amount of data to provide you with the security services to which you have subscribed and to provide high quality protection for our users.

With the F-Secure Security Cloud, F-Secure can maintain an up-to-date overview of the global threat landscape and protect our customers against new threats the moment they are first found.

The Security Cloud only collects data that may contain information about files or websites that have been blocked by F-Secure for security reasons. Security data is not used for personalized marketing purposes.

As a contributor, you allow the Security Cloud to keep the security data that helps us 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. Select the product icon in the menu bar.
2. Select **Settings**.
3. Select the **Privacy** tab.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Select **Allow deeper analysis**.

## 10.5 Improving the product

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

To send usage data:



1. Select the product icon in the menu bar.
2. Select **Settings**.
3. Select the **Privacy** tab.
4. Select the lock icon in the bottom-left corner.

You need administrative rights to change these settings.

5. Select **Send non-personalized usage data**.

**Note:** You can read our Privacy Statement [here](#).

## 11. Technical support


Here you can find information that can help you solve your technical issues.

If you have a question about the product or an issue with it, before contacting our customer support, go to [F-Secure Community](#) and see if you can find an answer to your question there.

### 11.1 Where can I find my account ID?

When you contact our customer support, they may ask for your account ID.

To find out your account ID:


1. Open the F-Secure app.
2. On the main view, select  in the top-right corner.
3. Select **About**.

You can find the account ID below the product version information.

### 11.2 Where can I find version information about the product?

If you need to contact us, our customer support may ask information about your product version.

To view the current version information:

1. Open the F-Secure app.
2. On the main view, select  in the top-right corner.
3. Select **About**.

Apart from the product version information, the **About** window contains information about your account ID and the latest database version of the product.

### 11.3 Using the support tool

Before contacting support, run the support tool to collect basic information about hardware, operating system, network configuration and installed software.

If you have technical problems with your security product, our customer support may ask you to create and send an FSDIAG file to our technical support. The file contains information that can be used for troubleshooting and solving problems specific to your computer.

You can create the file by using the Support Tool. The tool gathers information about your system and its configuration. The information includes product details, operating system logs and system settings. Note that part of the information may be confidential. The gathered information is stored in a file which is saved on your computer desktop.

To run the support tool:

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **Support** tab and then select **Open Support Tool**.
3. Select **Run Diagnostics** on the **Support Tool** window.

**Note:** You need administrative rights to run the tool.

4. Enter the administrator password for your computer.

The support tool starts and displays the progress of the data collection.

5. When the data collection is complete, select where you want to save the resulting tar.gz archive and then select **Save**.

The support tool opens a **Finder** window showing the saved file.

6. Send the file to customer support when you are asked for it.

**Tip:** If you cannot access the Support Tool through the product itself, go to the [Support Tools](#) web page and under **Support tool (FSDIAG) for Mac**, select **Download** and save the Support Tool.zip file, for example in your Downloads folder. Double-click the file, then click **Support Tool**, and select **Run diagnostics**.

#### 11.4 How to submit a large FSDIAG file to customer support

This guide outlines the steps involved in uploading a large file to F-Secure through a secure link provided by our customer support.

When F-Secure's customer support asks for an FSDIAG file larger than 50MB, you will receive a dedicated, secure link from the customer support team, either through email or in a chat. As soon as you have received the link from F-Secure, complete the following steps:

1. Click on the link to open it in your preferred browser (Chrome, Edge, Firefox or Safari).

The **Upload a diag file** page opens.

2. Select **Choose File** and select the FSDIAG from your device.

**Note:** You can select only a file that has "fsdiag" in the filename and the file format must be either \*.zip or \*.tar.gz.

3. Select **I'm not a robot** and fill in the reCAPTCHA.
4. Select **Submit**.

As soon as the file is submitted successfully, "Upload finished" is displayed.

5. Inform the customer care agent who requested the file about the successful upload, either through email or chat.

### 11.5 Debugging product issues

Debug logging helps our customer support to analyze and solve issues, if any, in the product.

**Note:** Switch debug logging on only when our customer support agent asks you to do so.

While the support tool collects a lot of valuable information, it also omits various information by default for privacy and performance reasons. To enable full debug logging, you have to install a special configuration profile before reproducing the issue and running the support tool. The configuration profile expires automatically after 14 days.

Debug logging may have some impact on performance because the product stores more logging data on your computer.

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **Support** tab.
3. Select **Enable debug logging**.

**Note:** You need administrative rights to run the tool.

You are asked to review and install the profile.

4. Confirm and install the new profile.

For macOS 15 (Sequoia) and newer:

1. Open the **System Settings** app.
2. Select **General > Device Management**
3. Double-click the **F-Secure debug logging** entry, then follow the on-screen instructions.

For macOS 13 (Ventura) and 14 (Sonoma):

4. Open the **System Settings** app.
5. Select **Privacy & Security > Profiles**.

6. Double-click the **F-Secure debug logging** entry, then click **Install**.

For macOS 12 (Monterey):

7. Open the **System Preferences** app.
8. Click the **Profiles** icon.
9. Select the **F-Secure debug logging** entry, then click **Install** to show the profile details.
10. Click **Install** to confirm.

Debug logging remains active for 14 days.

If you want to switch debug logging off before the 14-day expiration, go to **System Settings > Privacy & Security > Profiles** and remove the profile manually.

On older macOS versions (previous to 13), go to **System Preferences > Profiles** to remove the profile manually.

#### Resetting reputation cache

This topic describes how to ensure that you have the latest data from the F-Secure Security Cloud.

If you want to make sure that you have the latest file and website reputation information from our Security Cloud, reset the reputation cache:

1. Click the product icon in the menu bar and select **Settings**.
2. Select the **Support** tab.
3. Select **Reset reputation cache**.

**Note:** You need administrative rights to reset the cache.

## 11.6 Phone scams and what to do if you think you are targeted

Phone scams are unfortunately on the rise with scammers using social engineering to target their victims.

This topic is to help you identify these calls, and in the worst case—if you have been targeted—give you some information on what to do next.

### What are phone scams?

Phone calls can start either as a cold call or via an advert or link that triggers a pop-up on your computer. These pop-ups then urge you to call the tech support number advertised; the pop-ups may appear suddenly and are not that easy to get rid of.

### How can I recognize a phone scam?

These types of calls normally follow a certain pattern: The scammers usually claim that your computer has a problem, say a virus—when it actually doesn't—and then they trick you into paying for a service that doesn't exist either. They catch you off-guard and play on your emotions. Here's the basic scenario:

- Phone scammers claim to be from a well-known company, such as Microsoft, your bank, or even your network operator. As they use a reputable name, this puts you more at ease. They also seem knowledgeable and use technical terms, which make them seem legitimate and believable.
- As the risk seems real and you feel worried about possible computer viruses, you give the scammers access to your computer. They convince you to let them install an application that gives them access to your computer using remote access tools.
- Once the scammers have access to your computer, they pretend to fix the virus, and may also ask for your personal credentials. When the scammers have "fixed" the issue, they ask you to log into your online bank or ask you to fill in a form with your credit card details. The scammers charge you for the bogus service, which ends up being much more than you thought. In fact, it's difficult to know how much they really charge you.

### What to do if you think you have been scammed

If you think you are being scammed and you recognize the scenario that we described above, do the following:

- Act without delay.
- Immediately contact your credit card company or bank, report the scam and cancel any bank or credit cards. If you act promptly, they even may be able to stop the transaction and reverse the charges.
- Report the scam to the appropriate authority.
- Change all your passwords on every website or service that you think might have been affected.
- Uninstall any unknown, third-party software.
- Run a full scan on your computer: Open your security product, then select **Device Protection > Full computer scan**.

### Things to remember about unsolicited phone calls

- If you receive this type of a call, think: have I requested this?

**Note:** Normally, customer support calls you if you have already contacted them and created a support ticket.

- Remote sessions are commonly used in tech support as a way to assist you in solving issues.

**Remember:** Only allow remote sessions with people or companies you know and trust. Only ever allow remote sessions if you have contacted your service provider beforehand and have a valid support case with them. Also, guard your remote access data as you would guard any other password.

- Never give access to your device to people you don't know. Granting scammers remote access means that, in effect, you hand over the admin rights to your computer. Even if you have antivirus software installed, this can no longer protect you, as the scammers take control of your computer.
- Microsoft has informed its users that they never include phone numbers in their software's error messages or warning messages.
- Never freely hand over any personal credentials or credit card details.
- End the call immediately.
- These types of phone calls are illegal, and when in doubt, turn to the relevant authority that deals with fraud and report it.

#### **How can the security product help?**

With the security product installed, your computer is protected from viruses, trojans and ransomware. The Browsing protection, Banking protection, and Remote access tool protection features also add another layer of protection and make sure that you can browse and do your online banking safely.

If you have been targeted and you already have a security product installed, you can immediately run a full computer scan to help detect any applications that may have been installed by the scammers; these are called Potentially Unwanted Applications (PUAs). The product is not able to protect you from these types of phone scams, however.

Be vigilant and stay safe.



**DIGICOM**  
përtej shpejtësisë