Computer Protection for Mac

Contents

Chapter

1

Getting started

Topics:

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

1.1 How to make sure that my computer is protected

The **Status** page shows the current protection status and other important information about the product.

To open the **Status** page:

1. Click on the product icon in the menu bar.
2. Select **Open** from the menu.
3. The **Status** page opens when you open the product.

   In the **Status** page, you can:

   - check the current protection status,
   - make sure that all features are up-to-date and the date of the last update, and
   - check how long your subscription is still valid.

1.1.1 Protection status icons

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

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

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

1.2 Uninstallation

The product cannot be uninstalled by moving the application to the Trash. You need to use the product uninstaller to remove it from your computer.

You need rights to administer the computer to uninstall the product.

Follow these instructions:

1. Open the folder where you installed the product. By default, the product is in the `Applications` folder.
2. Double-click the `Uninstall <Product_Name>` icon.
   The uninstallation program opens.
3. Click **Uninstall**.
   You need to enter your administrator password to uninstall the product.
4. Enter your administrator user name and password and click **OK**.

The product is removed from your computer.

Chapter

2

Protecting the computer against harmful content

Topics:

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

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

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

2.1 What are viruses and other malware

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

Malware can:

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

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

2.1.1 Viruses

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

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

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

2.1.2 Spyware

Spyware are programs that collect your personal information.

Spyware may collect personal information including:

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

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

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

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

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

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

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

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

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

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

2.2 How to scan my computer

You can scan your computer for malware in real time or manually whenever you want.

2.2.1 Scan files automatically

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

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

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

Does real-time scanning affect the performance of my computer?

Normally, you do not notice the scanning process because it takes a small amount of time and system resources. The amount of time and system resources that real-time scanning takes depend on, for example, the contents, location and type of the file.

Files that take a longer time to scan:

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

Real-time scanning may slow down your computer if:

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

View the infection report

The infection report shows viruses and spyware that the real-time protection has found and moved to the Trash.

To view the infection report:

1. Click on the product icon in the menu bar.
2. Select **Infection report** from the menu.

Note: The infection report does not list malware that have been found and removed during the manual scan.

2.2.2 Scan files manually

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

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

Scanning files and folders

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

How to select the type of manual scan

You can scan your Home folder or any location that you specify.

You can manually scan files or folders if suspect that they may contain some malware.

To start the manual scan:

1. Click on the product icon in the menu bar.
2. Select **Choose what to scan**.

   Tip: Select **Scan Home folder** to scan all files in your Home folder.

   A window opens in which you can select which location to scan.
3. If the product finds any *malware* during the scan, it shows the name and location of the detected malware, and moves the infected file to the *Trash* automatically.

   Tip: Empty the *Trash* to remove infected files permanently.

2.3 Submitting a sample

You can help us to improve the protection by contributing suspicious applications 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 possibly harmful, you can send a sample of the application for security research purposes.

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

To submit a sample for analysis:

1. On the main page, select **Tools**.
2. Select **Submit a sample**.
   This opens a new web page in your default web browser.
3. Fill in the form on the web page to submit your sample for analysis.

2.4 How to use automatic updates

Automatic updates keep your computer protected from the latest threats.

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

2.4.1 Check the update status

View the date and time of the latest update.

Usually, you do not need to check the updates as the product receives the latest updates automatically when you are connected to the Internet.

To make sure that you have the latest updates:

1. Click on the product icon in the menu bar.
2. Select **Check for updates** from the menu.
   The product menu shows the date of the latest installed database.

Chapter

3

What is a firewall

Topics:

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

The firewall controls connections between your computer and other computers in the Internet. You can use the product to temporarily allow all connections.

3.1 Allow all connections to your computer

In some cases, you may need to turn off your firewall completely.

To allow all connections between your computer and other computers in the Internet, follow these instructions:

1. Click on the product icon in the menu bar.
2. Select **Open** from the menu.
3. On the main page, select **Tools**.
4. Click **Disable firewall**.

Chapter

4

What is browsing protection

Topics:

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

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

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

Browsing protection works with the Safari, Firefox, and Chrome web browsers.

4.1 How to turn browsing protection on or off

The product protects you against harmful websites when browsing protection is turned on.

To turn on browsing protection:

1. Click on the product icon in the menu bar.
2. Click **Preferences**.

   Make sure that the **Browsing protection** tab is open.
3. Select **Turn on Browsing protection**.
4. Browsing protection requires that a browser extension is installed. Click **Install browser extension** if it is not installed yet for the web browser that you use.
   - For Safari, you need to download the browser extension and install it separately. Clicking **Install browser extension** opens a web page that automatically downloads the extension and provides further instructions.
   - For other browsers, you do not need to download the extension. No further action is needed after you click **Install browser extension**.

When browsing protection is on, it shows you safety ratings for web sites listed on search engine results and blocks harmful websites.

4.1.1 Using browsing protection with Chrome

Instructions how to make sure that the browsing protection works with your Google Chrome web browser.

1. Make sure that you have turned on the browsing protection in the product and installed the browser extension for Google Chrome.
2. In Google Chrome, open the **Chrome** menu and select **Preferences**.
3. Select **Extensions** from the list on the left pane.
4. Check that **Browsing protection by F-Secure** is listed and enabled.

Reinstalling the browser extension to Google Chrome

If you have uninstalled the browsing protection extension from the Google Chrome, you need to edit Chrome settings manually to take it into use again.

Follow these instructions to use the browsing protection with Google Chrome again:

1. In Google Chrome, open the **Chrome** menu and select **Settings**.
2. Select **Extensions** from the list on the left pane and leave the Chrome open in the background.
3. Click **Finder** in **Dock**.
4. Open the **Go** menu and select **Go to Folder**.
5. Enter the folder name: `/usr/local/f-secure/browsingprotection/chrome/`
6. Click **Go**.
7. Drag the file `browsing-protection.chromeextension.crx` to the **Extensions** window in Chrome.
8. Check that **Browsing protection by F-Secure** is listed and enabled.

4.1.2 Using browsing protection with Firefox

Instructions how to make sure that the browsing protection works with your Firefox web browser.

1. Make sure that you have turned on the browsing protection in the product and installed the browser extension for Firefox.
2. In Firefox, open the **Tools** menu and select **Add-ons**.
3. Select **Extensions** from the list on the left pane.
4. Check that **Browsing protection** is listed enabled.

   If the extension is greyed out and disabled, click **Enable**.

4.1.3 Using browsing protection with Safari

Instructions how to make sure that the browsing protection works with your Safari web browser.

1. Make sure that you have turned on the browsing protection in the product and installed the browser extension for Safari.
2. In Safari, open Safari menu and select **Preferences**.
3. Open the **Extensions** tab.
4. Select **Browsing protection** from the extensions list.
5. Check that **Browsing protection** is enabled.

4.2 Browsing protection safety ratings

Browsing protection shows safety ratings for web sites on search engine results.

Color-coded icons show the safety rating of the current site. The safety rating of each link on search results is also shown with the same icons:

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

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

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

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

The access to this web site is never blocked.

Safety ratings are available on the following search sites:

- Google
- Bing
- Yahoo

4.3 What to do when a web site is blocked

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

When a browsing protection block page appears:

1. If you want to enter the web site anyway, click **Allow web site**.
   The product adds the web site to the allowed web sites list.
2. To view web sites that you have allowed:
   a) Click on the product icon in the menu bar.
   b) Click **Preferences**.
      Make sure that the **Browsing Protection** tab is open.

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

Chapter

5

Using online banks safely

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

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

To turn on Banking protection:

1. Click on the product icon in the menu bar.
2. Click **Preferences**.

   Make sure that the **Browsing protection** tab is open.
3. Select **Turn on Banking protection**.