WithSecure Elements Endpoint Protection for Computers (Mac)

2026-10-06

Contents

Chapter 1: Getting started....3

1.1 Disclaimer....4
1.2 System requirements....4
1.3 Viewing information about your subscription....5
1.4 Changing the product settings....5
1.5 How to make sure that my computer is protected....6

Chapter 2: Protecting the computer against harmful content....7

2.1 What harmful content does....8
2.2 Scanning your computer....10
2.3 Submitting a sample....13
2.4 How to use automatic updates....13
2.5 What is WithSecure XFENCE?....14

Chapter 3: Protecting your web browsing....15

3.1 Blocking harmful websites....16
3.2 Banking safely online....17
3.3 Checking that browser extensions are in use....18

Chapter 4: What is a firewall....21

4.1 Allow all connections to your computer....22

Chapter 5: Technical support....23

5.1 Where can I find version information of the product?....24
5.2 Where can I find my account ID?....24
5.3 Using the support tool....24
5.4 Phone scams and what to do if you think you are targeted....25

Glossary....27

Chapter 1
Getting started

Topics:

- Disclaimer
- System requirements
- Viewing information about your subscription
- Changing the product settings
- How to make sure that my computer is protected

Getting started

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

NOTE: For instructions on how to deploy the product, see Deployment methods for Mac devices.

1.1 Disclaimer

WithSecure™ is the new name for F-Secure Business.

Some product interfaces and portals may still display the former F-Secure name.

1.2 System requirements

Review the system requirements for WithSecure Elements Agent for Mac, formerly F-Secure PSB Computer Protection & RDR for Mac.

Supported operating systems

NOTE: WithSecure supports only operating systems that are currently supported by their vendor. Learn more about WithSecure's operating system support policies at Product updates and supported versions. If you are interested in long-term support for a platform that vendors no longer support, contact your sales representative.

Elements Agent for Mac supports the following operating system versions:

macOS 27 "Golden Gate"
macOS 26 "Tahoe"
macOS 15 "Sequoia"

System requirements

The recommended system requirements are:

- Intel or Apple Silicon Mac
- 1 GB of free disk space
- 1 GB or more of memory
- Internet connection: An internet connection is required to validate your subscription and receive updates

Supported browsers

Safari
Chrome
Firefox

Supported languages

The supported languages are: English, Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, French (Canadian), German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Brazilian Portuguese, Romanian, Russian, Slovenian, Spanish, Spanish (Mexican), Swedish, Turkish, Vietnamese, Traditional Chinese (Hong Kong), Traditional Chinese (Taiwan) and Simplified Chinese.

1.3 Viewing information about your subscription

This section provides information related to your subscription.

To view information about your subscription:

1. Open the product from the product icon in the menu bar.
2. From the product menu, select **Settings...**.
3. In the window that opens, select the **Subscription** tab.

On the view, you can see information about your current subscription and its status.

1.4 Changing the product settings

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

You need administrative rights to change the product settings. You can access the product settings from the product icon in the menu bar.

> **NOTE:** Your administrator may have enforced some security settings, which means that you may not be able to locally change some features.

1.4.1 Quick access to product settings

The product settings, or preferences, can be accessed from the app menu and from the product icon in the menu bar.

To change the product settings, select the product icon in the menu bar, then select

☰

and then **Settings...** from the drop-down menu.

Apart from **Settings...**, the menu includes the following options:

Table 1: Menu options

Option	Description
Settings...	Opens the **WithSecure Elements Agent** window where you can make changes to the product settings.
Malware Scan	Scans every accessible file in the system for a complete malware check.
Choose what to scan...	Allows you to scan a specific folder in the system.
Check for updates	Checks and downloads the latest updates.
Infections report...	Opens a window listing all the infections found in the system.
About	Opens a window that shows the product, database and sensor versions. It also has links to the third-party licenses, license terms, and privacy policy.

When you select the product icon in the menu bar, the page shows the protection status of your computer, a link to status details, and the product version.

1.4.2 Viewing the tools

You can access the tools that you can use to protect your computer via the **Malware Protection**, **Secure Browsing** , and **XFENCE** tabs.

The product menu provides options for malware scans, updates, infection reports, and product information. The **Malware Protection**, **Secure Browsing**, and **XFENCE** tabs provide access to related protection features.

1.5 How to make sure that my computer is protected

The product main view shows the current protection status and other important information about the product.

In the top-right corner of the main view, you can see the status of your subscription.

When you place your mouse on the product icon in the menu bar, a notification is shown which indicates that your security is centrally managed; whether Malware protection and Browsing protection are active, and whether the Safari browser extension is in use.

To make sure that the product has the latest updates:

1. Select the product icon in the menu bar.
2. Select

   ☰

   and from the drop-down menu, select **Check for updates**.
   The product fetches the latest updates immediately.

Chapter 2

Protecting the computer against harmful content

Topics:

- What harmful content does
- Scanning your computer
- Submitting a sample
- How to use automatic updates
- What is WithSecure XFENCE?

Protecting the computer against harmful content

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 as soon as 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.

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

2.1 What harmful content does

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 do the following:

- 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
- 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 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 a considerable amount of storage or memory
- Puts the security of your device or the information stored on it at risk - 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 treated as an 'unwanted application' (UA). The product deals with 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 before the application is allowed to run. If you trust the application, you can allow the product to run it. 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 set the product to ignore it in the future scans.

2.1.2 Worms

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

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

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

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

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

2.1.3 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 searches for usernames and passwords for online banking portals
- Trojan-spy: Monitors activity on the device and forwards the details to a remote site

2.1.4 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.

2.1.5 Exploits

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

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

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

There are 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.

2.1.6 Exploit kits

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

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

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

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

Exploit kits are modular. Their controllers can add or remove exploits and payloads from the toolkit.

2.2 Scanning your computer

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

Real-time scanning checks files when you access them. Manual scanning checks your whole computer or selected files and folders.

2.2.1 Scanning 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 moves the file to quarantine before it can cause any harm.

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

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

Files that take a longer time to scan:

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

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.

Viewing the infection report

The infection report shows malware that the real-time protection has found and moved to quarantine.

To view the infection report:

1. Select the product icon in the menu bar.
2. Select

   ☰

   and from the drop-down menu, **Infections report...**.
   *The **Infections** report opens.*

Quarantine

Quarantine keeps infected files in a safe location where they cannot harm the computer.

When real-time scanning or a manual scan finds an infected file, the product moves the file to quarantine. The file stays in quarantine until you restore or delete it.

The product does not quarantine archives that contain infected files. It lists the archive as harmful in the infections report. The product quarantines the infected files only after they are extracted from the archive. You can delete the archive from the infections report.

When a file is quarantined or restored, the product sends a security event to WithSecure Elements Security Center.

Administrators can set the product to delete old quarantined files automatically after a number of days, and decide whether users can restore quarantined files. They make these settings in the profile in WithSecure Elements Security Center.

Restore quarantined files

You can restore a file from quarantine if you are sure that it is safe.

Restoring a quarantined file returns potentially harmful content to your computer. Restore a file only if you are sure that it is safe.

> **NOTE:** Your administrator can prevent users from restoring quarantined files. In that case, you cannot restore files from the infections report.

To restore a quarantined file:

1. Select the product icon in the menu bar.
2. Select
   ☰
   and from the drop-down menu, **Infections report...**.
   *The **Infections** report opens and shows the quarantined files.*
3. Select the file that you want to restore.
4. Select **Restore selected files**.
   A warning asks you to confirm that you want to restore a potentially harmful file.
5. Select **Yes, Restore**.

The file is restored to its original location. The product sends a security event about the restored file to WithSecure Elements Security Center.

Delete quarantined files

You can delete quarantined files that you do not need.

You can delete quarantined files and archives that the product has listed as harmful. To delete quarantined files:

1. Select the product icon in the menu bar.
2. Select
   ☰
   and from the drop-down menu, **Infections report...**.
   *The **Infections** report opens and shows the quarantined files.*
3. Select the files that you want to delete.
4. Select **Delete selected files**.
   The product deletes the files immediately and does not ask for confirmation.
5. Optional: To remove the deleted entries from the report, select **Clear history**.

2.2.2 Scanning 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 malware 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 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.

Selecting what to scan manually

You can scan a specific file or folder in the system.

You can manually scan files and folders if you suspect that they may contain malware.

To scan a file or folder manually:

1. Select the product icon in the menu bar.
2. Select

   ☰

   Choose what to scan....
   A window opens in which you can select what to scan.
3. 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.

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 quarantine automatically.

> **TIP:** Delete the quarantined files from the infections report to remove them 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 send a file to us anonymously for analysis if you think that it has been incorrectly marked as a threat or suspect that it is malicious.

To submit a sample for analysis:

1. Open the product from the product icon in the menu bar.
2. Select

   ☰

   and from the drop-down menu, **Settings...**.
3. Select the **Support** tab, and then select **Submit a sample**.
   This opens a new web page in your default web browser.
4. Complete 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 Checking 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. Select the product icon in the menu bar.
2. Select **Check for updates**.
   The product installs the latest updates automatically if there are new updates available.
3. To check the date of the latest database installed, select the product icon.
   Information about the latest database can be seen at the bottom of the menu.

2.5 What is WithSecure XFENCE?

WithSecure XFENCE provides an additional layer of security to help protect your personal data against being deleted, ransomed, or stolen by malware.

When an application attempts to write to or delete a file, XFENCE checks the reputation of the application from WithSecure's Security Cloud. If the application is trusted, the operation is allowed, and if the application is suspicious or known to be harmful, it is blocked. If no information is available, XFENCE displays a permission dialog that asks you to deny or allow the application.

By checking the file reputation, XFENCE 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.

Chapter 3

Protecting your web browsing

Topics:

- Blocking harmful websites
- Banking safely online
- Checking that browser extensions are in use

Protecting your web browsing

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 WithSecure malware analysts and WithSecure partners.

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

3.1 Blocking harmful websites

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

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

To turn on browsing protection:

1. Select the product icon in the menu bar.
2. Select **Settings...**.

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

> **NOTE:** Browsing protection requires that a browser extension is installed and turned on in the web browser that you use. The product normally installs the extension for Safari automatically, but you need to enable the extension before it works. The product supports also Firefox and Chrome, but you need to install and enable them manually.

3.1.1 Allowing specific websites

Browsing Protection automatically blocks access to websites that are rated harmful and may try to steal personal information.

You can manually allow automatically-blocked websites if you are sure they are safe.

To allow a website:

1. Open the product from the product icon in the menu bar.
2. On the Settings view, select **Secure Browsing**.
3. Select the lock icon in the bottom-left corner to unlock it.

   You need administrative rights to change these settings.
4. Select **+**, enter the address of the website you want to allow and press **Enter**.

   The website is added to the list of website exceptions.

3.1.2 What to do when a website 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 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 find instructions on how to submit the website for analysis sample submission instructions.

3.1.3 Browsing protection safety ratings

Browsing protection shows safety ratings for websites 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:

Table 2: Safety rating 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.
	Administrator has blocked this site and you cannot visit it.

Safety ratings are available on the following search sites:

Google
Bing
Yahoo
DuckDuckGo

TIP: If you think that a file or a URL has been falsely detected, you can find instructions on how to submit the website for analysis sample submission instructions. You can submit multiple URLs or IP addresses by combining them into a text file and submitting them as a file.

3.2 Banking safely online

Banking protection adds another layer of security to prevent attackers from interfering with your confidential transactions and protects you against harmful activity when you access your online bank or make transactions online.

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

Banking protection currently supports the following browsers:

Safari
Firefox
Google Chrome

3.2.1 Turning on banking protection

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

You need administrative rights to change these settings.

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

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

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.
3. Select the **Secure Browsing** tab.
4. Select the lock icon in the bottom-left corner.
5. Select **Turn on Banking protection**.

NOTE: Banking protection requires that browser extensions are in use.

3.3 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 activate the browser extension for the web browser that you use.

The product installs the browser extension for Safari automatically, and the only thing you need to do is to make sure that the extension is turned on.

For Chrome and Firefox, you need to install and enable the browser extension to be able to browse the internet safely. Also, the installation of the extension requires your permission to access information about the web addresses you visit. For more detailed information, see the related information.

3.3.1 Enabling browser extension for Safari

You must enable the browser extension for Safari to be able to use the browser safely.

The product installs the browser extension automatically, and the only thing you need to do is to make sure that the extension is turned on.

To ensure that the browser extension for Safari is turned on:

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
5. In the pop-up window, select **Safari** and then **Enable**.
6. In the **Extensions** dialog, do the following:

a) Make sure that **Browsing protection** is selected.
b) Under **Private Browsing**, select **Allow in Private browsing**.
c) Under **Permissions**, select **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: WithSecure test URL. You should see the product block page.

3.3.2 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 for Chrome:

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
   *The **Browsing protection installation** window opens.*
5. From the drop-down, select **Chrome** and then **Install now**.
6. Select **Add to Chrome** > **Add extension**.

   Once the extension is installed, a user consent dialog opens. The browser extension requires your permission to access information about the web addresses you visit.
7. Select **Accept**.

   NOTE: 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.
8. To complete setting up the extension, select **OK**.

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: WithSecure test URL. You should see the product block page.

3.3.3 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 for Firefox:

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
   *The **Browsing protection installation** window opens.*
5. From the drop-down, select **Firefox** and then **Install now**.
6. Select **Add**.

   Once the extension is installed, a user consent dialog opens. The browser extension requires your permission to access information about the web addresses you visit.
7. Select **Accept**.

> **NOTE:** 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.

8. 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: WithSecure test URL. You should see the product block page.

Chapter 4
What is a firewall

Topics:

- Allow all connections to your computer

What is a firewall

The *firewall* prevents intruders and harmful applications from 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. When installed, the product turns on the system firewall by default, unless the remote management settings prevent it.

You can view the Firewall settings in the **Firewall** tab by opening the product from the product icon in the menu bar and selecting **Settings**. WithSecure firewall is managed remotely from Elements Security Center and Apple Firewall can be managed from both macOS settings or remotely from Elements Security Center.

4.1 Allow all connections to your computer

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

You need administrative rights to change System Preferences.

To allow all connections between your computer and other computers in the internet:

1. Open the product from the product icon in the menu bar.
2. On the main view, select **Viruses & Threats**.
3. On the **Viruses & Threats** view, select **macOS Firewall preferences**.
4. On the **Firewall** tab of the **Security & Privacy** preferences, select first the lock icon in the bottom-left corner, enter your admin password, and then select **Unlock**.
5. Select **Turn Off Firewall**.

The computer's firewall is now turned off. All incoming connections to this computer are allowed.

> **NOTE:** If you want to make other changes to the Firewall preferences on your computer, select **Firewall Options...**.

Chapter 5
Technical support

Topics:

- Where can I find version information of the product?
- Where can I find my account ID?
- Using the support tool
- Phone scams and what to do if you think you are targeted

Technical support

Technical support resources help you resolve product issues.

This section covers finding product and account details, collecting diagnostics with the support tool, and recognizing support phone scams.

5.1 Where can I find version information of the product?

Our customer support may ask information of your product version if you need to contact us.

To view the current version information:

1. Open the product from the product icon in the menu bar.
2. Select **About**.
   *Apart from the product version information, the **About** window contains information about the latest database and sensor versions of the product.*

5.2 Where can I find my account ID?

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

To find your account ID:

1. Open the product from the product icon in the menu bar.
2. On the main view, select

   in the top-right corner.
3. Select **About**.
   You can find the account ID with the product version information.

5.3 Using the support tool

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

You need administrative rights to run the tool.

To run the support tool:

1. Go to the product folder under **Applications** and run the **Support Tool** application.
2. Select **Run Diagnostics** on the **Support Tool** window.
3. Enter the administrator password for your computer.

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

4. 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.*
5. Send the file to customer support when you are asked for it.

NOTE: Your administrator may request the support tool diagnostics remotely. The product shows you a notification of this and prompts you to **Allow** or **Deny** the request.

5.4 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 urge you to call the advertised tech support number.

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 enter your credit card details in a form. 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 recognize the phone scam scenario, 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 **Viruses & Threats** > **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 effectively gives them 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 give anyone your 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 and Banking 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.

Glossary

Adware

Adware is software that automatically displays or downloads advertising material, often bundled with other programs and sometimes tracking user activity without clear consent.

Agent

An agent is the client software installed on a managed device that enforces protection, reports device status, and communicates with the management service; more broadly, a program that acts on behalf of a user or another system.

Antivirus

Software that prevents, detects, and removes viruses and other malware.

Backdoor

An undocumented way of gaining access to a computer system.

Banking Protection

Protects users against harmful activities when they access online banks or make transactions online.

Browsing Protection

A feature that evaluates the safety of visited websites and prevents users from unintentionally accessing harmful websites.

Company

A customer organization, either managed by a partner or standalone, that is the lowest level in the organizational hierarchy and has no child organizations.

DeepGuard

A feature that protects the computer against unknown threats by monitoring program behavior in real-time and stopping dangerous activities.

Detection

A detection is an identified suspicious, malicious, or policy-relevant event, activity, or finding recognized by a security control or analysis system.

Encryption

Encryption is the process of converting data into a secure format using cryptographic algorithms, ensuring confidentiality and protection against unauthorized access.

Endpoint Protection

Endpoint protection is the set of security capabilities used to prevent, detect, and handle threats on endpoint devices such as workstations, servers, and mobile devices.

Exploit

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.

Exploit Kit

Toolkits used by attackers to manage exploits and deliver harmful programs to a vulnerable computer or device.

Family Rules

A feature that limits the amount of time that children can spend online and blocks websites that contain inappropriate content.

Harmful Content

Harmful content is files, applications, or web content that can damage data or compromise a device, such as malware or malicious websites.

Infection

An infection is the state in which a file, object, system, or workload contains or has been affected by malicious code or other harmful content.

Malware

A program or a file that is developed for the purpose of doing harm. This includes computer viruses, worms and Trojan horses.

Malware Protection

Malware Protection is the feature that detects, blocks, and removes viruses and potentially unwanted applications on a device.

Malware Scan

A malware scan is a scan that checks a device, file set, or workload for malicious software or other harmful content.

Manual Scanning

Manual scanning is a user-started security scan that runs on demand instead of running automatically on a schedule or in real time.

Phishing

In a phishing attack, an attacker sends a fraudulent message posing as a trusted sender to trick the recipient into revealing sensitive data such as credentials or financial information.

Potentially Unwanted Application (PUA)

A software program that may not be malicious but could introduce security risks, intrusive behavior, or unwanted advertisements.

Privacy

Privacy is the protection of a person's or organization's information from unauthorized collection, access, use, or disclosure.

Privacy Policy

A privacy policy is a published statement that describes how an organization collects, uses, discloses, and manages personal data.

Quarantine

Quarantine is an isolated storage location or state where potentially harmful files, messages, or other items are held to prevent them from affecting systems or users while allowing later review, release, or deletion.

Ransomware

A malicious program that prevents the user from accessing their data and/or device and demands a ransom to 'restore normal access'. The program may not actually restore normal access even if the ransom is paid.

Rapid Detection & Response (RDR)

Rapid Detection & Response (RDR) is a WithSecure managed service that quickly identifies, analyzes, and responds to threats to minimize damage.

Real-Time Protection

Real-time protection continuously scans files as they are accessed and blocks those that contain malware, providing always-on protection through real-time scanning.

Real-Time Scanning

Real-time scanning is continuous scanning that checks content or activity as it is accessed, saved, or processed.

Rootkit

Programs that make other malware difficult to find by concealing running processes, files, or system data from the operating system.

Sample Submission

A sample submission is a request that sends a suspicious file, URL, or email for analysis and follow-up handling.

Scan

A scan is a security check that examines a device, system, application, account, or other target for threats, vulnerabilities, suspicious activity, or policy-relevant findings.

Security Cloud

Security Cloud is WithSecure's cloud-based threat analysis and reputation service that helps classify files, websites, and other security-relevant observations and deliver up-to-date protection against emerging threats.

Sensor

Software that runs on monitored devices (hosts). The sensor monitors the device status and communicates with Elements Endpoint Detection and Response backend.

Spam

Spam messages are unsolicited email messages that are usually sent in bulk to a large list of recipients.

Spyware

Software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

Support Tool

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

Trojan

A Trojan is malicious software that disguises itself as a legitimate program to trick users into running it, then performs harmful actions such as stealing data or opening a backdoor.

Unwanted Application

An application that can compromise privacy or has a severe impact on a device's security.

Virus

A virus is usually a program that can attach itself to files and replicate itself repeatedly; they can alter and replace the contents of other files in a way that may damage the computer.

Vulnerability

A flaw, loophole or unexpected behavior in a program or operating system that can be exploited by an attacker in order to perform unauthorized actions on the affected system / device.