# WithSecure Server Security

# Contents

Chapter
1

# Getting started

**Topics:**



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

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

## 1.1 Disclaimer

F-Secure Business is now WithSecure™ which is reflected in the form of new logos and names.

We are in the process of rebranding our products, and during this period, you may see a mix of F-Secure and WithSecure™ in the products and portals, until all the changes have been made.

## 1.2 System requirements

This section contains important information about WithSecure Server Security.

We strongly recommend that you read the entire document before you start using the product.

### Supported operating systems

**Note:** WithSecure supports only those operating systems that are supported by their vendor. If you are interested in long-term support for a platform that vendors no longer support, contact your sales representative.

The product can be installed on a computer running one of the following operating systems:

- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 Essentials
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2012 R2 Essentials
- Microsoft® Windows Server 2012 R2 Foundation
- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core

**Note:** Windows Server 2016 Nano is not supported.

**Note:** ARM is not supported.

All Microsoft Windows Server editions are supported except:

- Windows Server for Itanium processor
- Windows HPC editions for specific hardware
- Windows MultiPoint Server
- Windows Home Server

**Note:** All operating systems are required to have the latest Service Pack installed. Also, the operating systems must support Microsoft Azure Code Signing certificates. You can find more information here.

**Note:** For performance and security reasons, you can install the product only on an NTFS partition.

### Supported terminal servers

WIthSecure Server Security supports the following terminal server platforms:

- Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms)
- Citrix® XenApp 5.0
- Citrix® XenApp 6.0
- Citrix® XenApp 6.5
- Citrix® XenApp 7.5, 7.6, 7.14, 7.15
- Citrix® Virtual Apps and Desktops 2009

### Hardware and system requirements

Before you install the product, we recommend that you review this section to ensure that your network, hardware, software, and other system components meet the requirements.

**Note:** The minimum hardware requirements may not be sufficient if you run multiple services on the same system.

To install WithSecure Server Security, the following minimum hardware and system requirements are recommended:

- Any computer that meets the requirements for the supported operating system.
- 10 GB or more disk space is recommended.
- An internet connection is required to receive updates and to use cloud-based detection.
- This Server Security version requires Windows Universal C Runtime (https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows) for installation.

### Setup and configuration

Installation instructions:

Import the product installation JAR package to Policy Manager Console and deploy the product remotely to selected hosts. With Policy Manager Console, you can also export an MSI package that you can deploy via other central management systems to install the product.

To run the installation locally, you need to create the MSI package with the export tool in the WithSecure Policy Manager Console.

**Note:** The local installation requires local administrator rights.

### Supported languages

The supported languages are: English, Chinese (P.R.C, Taiwan, Hong Kong), Czech, Danish, Dutch, Estonian, Finnish, French, Canadian French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Brazilian Portuguese, Romanian, Russian, Slovenian, Spanish, Latin American Spanish, Swedish, and Turkish.

## 1.3 Changing the product settings

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

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

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

**Related Tasks**

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18

DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

Changing Windows Firewall settings on page 37
When the firewall is turned on, it restricts access to and from your computer. Some applications may require that you allow them through the firewall to work properly.

Viewing recent events for the product on page 8
You can see what the product has done and how it has protected your computer on the **Event history** page.

Turning off all security features on page 7
You can turn off all of the security features if you need to free up more system resources.

## 1.3.1 Quick access to product settings

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

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

**Note:** If the product icon is hidden, click the **Show hidden icons** arrow in the taskbar first.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. The context menu includes the following options:

| Option | Description |
|---|---|
| **View current status** | Shows the current protection status of your computer. |
| **Check for updates** | Checks and downloads the latest updates. |
| **View recent events** | Shows the actions that the product has taken to protect your computer. |
| **Open settings** | Opens the product settings. |
| **About** | Shows the version information of the product. |

## 1.3.2 Turning off all security features

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

**Note:** Your administrator may have set a policy that prevents you from turning the security features off.

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

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Turn off all security features**.

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

## 1.4 How to see what the product has done

The protection status icon shows that the product is running and the protection statistics show information how it has protected your computer.

### 1.4.1 Viewing recent events for the product

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

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

To see your product's entire event history:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Recent events**.
   The **Event history** page opens.

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

- Date and time when the harmful file was found
- The name of the malware and its location on your computer
- The performed action

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 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.

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

**Note:** Your administrator may enforce some security settings, which means that you may not be able to locally change some features.

## 2.1 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.

### 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' 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 WithSecure 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.

**Related Tasks**

Turning on real-time scanning on page 13
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

### 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

**Related Tasks**

Turning on real-time scanning on page 13
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

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

**Related Tasks**

Turning on real-time scanning on page 13
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

## 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.

**Related Tasks**

Turning on real-time scanning on page 13
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

## 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.

**Related Tasks**

Turning on real-time scanning on page 13
Keep real-time scanning turned on to remove harmful files from your computer before they can harm it.

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

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

**Related Tasks**

Turning on real-time scanning on page 13

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

Running a malware scan on page 14
You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications.

Using DataGuard Access Control on page 18
DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

## 2.2 How to scan my computer

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

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

### 2.2.1 How real-time scanning works

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

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

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

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

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

Files 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 real-time scanning.

Real-time scanning may slow down your computer if:

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

#### Turning on real-time scanning

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

To make sure that real-time scanning is on:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Malware Protection** > **Edit settings**.

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

4. Turn on **Real-time Scanning**.

### 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 where harmful applications are commonly found to remove unwanted applications and harmful items on your computer more efficiently.

### Scanning files and folders

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

## Running a malware scan

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

To scan your computer, follow these instructions:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. If you want to optimize how the manual scanning scans your computer, on the main page, select and then select **Scanning settings**.
   a) Select **Scan only file types that commonly contain harmful code (faster)** if you do not want to scan all files.

      The files with the following extensions are examples of file types that are scanned when you select this option: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.

   b) Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Scanning inside compressed files makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.
3. On the main page, select .
4. Select either **Malware scan** or **Full computer scan**.

   - **Malware scan** starts by scanning the active memory of the computer and then locations where malware is commonly found, including the document folders. It can find and remove unwanted applications and harmful items on the computer in a shorter time.
   - **Full computer scan** scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete.

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

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

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

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

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

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

### Scan in Windows Explorer

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

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.

To scan a disk, folder, or file:

1. Right-click the disk, folder, or file you want to scan.
2. From the right-click menu, select **Scan for malware**.

   **Note:** On Windows 11, select **Show more options** and then select **Malware scan**.

   The virus scan starts and scans the disk, folder, or file that you selected.

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

## 2.2.3 Scheduling scans

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

To schedule a scan:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Scanning settings**.
4. Turn on **Scheduled scanning**.
5. In **Perform scan**, select how often you want to scan your computer automatically.

| Option | Description |
|---|---|
| **Daily** | Scan your computer every day. |
| **Every week** | Scan your computer on selected days of the week. Select the weekday from the list. |
| **Every four weeks** | Scan your computer on a selected weekday at four-week intervals. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday. |

6. In **Start time**, select when the scheduled scan starts.
7. Select **Run scanning on low priority** to make the scheduled scan interfere less with other activities on the computer. Running the scan on low priority takes longer to complete.
8. Select **Scan only file types that commonly contain harmful code (faster)** if you do not want to scan all files.

   The files with the following extensions are examples of file types that are scanned when you select this option: `com`, `doc`, `dot`, `exe`, `htm` , `ini`, `jar`, `pdf`, `scr`, `wma`, `xml`, `zip`.
9. Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Scanning inside compressed files makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.

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

## 2.3 What is DeepGuard

DeepGuard offers proactive, instant protection against unknown threats.

DeepGuard monitors applications to detect and stop potentially harmful changes to the system in real-time. It makes sure that you use only safe applications. The safety of an application is verified from the trusted cloud service. If the safety of an application cannot be verified, DeepGuard starts to monitor the application behavior.

**Tip:** If you want WithSecure to add your application to the allowed applications list, submit your application for analysis here. Once we have analyzed the program, we will notify you of the analysis results if you have provided us with your contact details.

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

Potentially harmful system changes that DeepGuard detects include:

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

To make sure that DeepGuard is active:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Malware Protection** > **Edit settings**.

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

4. Select **Edit settings**.

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

5. Turn on **DeepGuard**.

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

**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.

**Related Tasks**

Security Data on page 44
The service sends queries on potential malicious activities or on protected devices to the WithSecure ***Security Cloud***.

### 2.3.1 Allow applications that DeepGuard has blocked

You can control which applications DeepGuard allows and blocks.

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

To allow the application that DeepGuard has blocked:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

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

The **App and file control** view opens.

4. Select the **Blocked** tab.
   This shows you a list of the applications that DeepGuard has blocked.
5. Find the application that you want to allow and select **Allow**.
6. Select **Yes** to confirm that you want to allow the application.

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

## 2.3.2 Using DataGuard

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

Ransomware is harmful software that encrypts important files on your computer, preventing you from accessing them. Criminals demand a ransom to restore your files, but there are no guarantees you would ever get your personal data back even if you choose to pay.

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

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

**Note:** You must turn on DeepGuard to use DataGuard. DataGuard is available only in the Premium version.

To manage your protected folders:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Malware Protection** > **Edit settings**.

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

4. Turn on **DataGuard**.
5. Select **View protected folders**.
6. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
7. Add or remove folders as needed.

   To add a new protected folder:

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

   To remove a folder:

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

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

**Related Tasks**

Adding and removing protected folders on page 18

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

## 2.3.3 Adding and removing protected folders

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

DataGuard blocks any unsafe access to your protected folders.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⋯.
3. Select **Quarantine and exclusions**.

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

   The **App and file control** view opens.
4. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
5. Add or remove folders as needed.

   To add a new protected folder:

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

   **Tip:** As you must separately allow all applications that need to access the protected folder, we recommend that you do not add folders that contain your installed games or applications (for example, Steam Library Folders). Otherwise, these applications may stop working correctly.

   To remove a folder:

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

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

# 2.4 Using DataGuard Access Control

DataGuard Access Control protects folders from ransomware (encryption blackmail) by preventing unknown application from accessing them.

**Note:** DataGuard is available only in the Premium version.

To turn on **DataGuard Access Control**:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Malware Protection** > **Edit settings**.

   **Note:** You need administrative rights to change some of the settings.
4. Turn on **DataGuard Access Control**.

## 2.4.1 View quarantined items

You can view more information on items placed in quarantine.

Quarantine is a safe repository for files that may be harmful. The product can place both harmful items and potentially unwanted applications in quarantine to make them harmless. You can restore applications or

files from quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in quarantine removes it permanently from your computer.

To view information on items placed in quarantine:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ···.
3. Select **Quarantine and exclusions**.

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

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

## 2.4.2 Restore quarantined items

You can restore the quarantined items that you need.

You can restore applications or files from quarantine if you need them. Do not restore any items from quarantine unless you are sure that items pose no threat. Restored items move back to the original location on your computer.

To restore quarantined items:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ···.
3. Select **Quarantine and exclusions**.

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

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

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

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

## 2.4.3 Exclude 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 scanning:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ···.
3. Select **Quarantine and exclusions**.

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

   The **App and file control** view opens.
4. Select the **Excluded** tab.
   This view shows you a list of excluded files and folders.
5. Select **Add new**.

6. Select the file or folder that you do not want to include in scans.
7. Select **OK**.

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

## 2.4.4 View excluded applications

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

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

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

Also, DeepGuard does not block certain Steam games. Therefore, you don't have to exclude Steam games from scanning or turn off DeepGuard to run them.

To view the applications that are excluded from scanning:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ···.
3. Select **Quarantine and exclusions**.

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

   The **App and file control** view opens.
4. Select the **Excluded** tab.
   This view shows you a list of excluded files and folders.
5. If you want to scan the excluded application again:
   a) Select the application that you want to include in the scan.
   b) Click **Remove**.

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

## 2.4.5 Adding and removing protected folders

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

DataGuard blocks any unsafe access to your protected folders.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ···.
3. Select **Quarantine and exclusions**.

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

   The **App and file control** view opens.
4. Select the **Protected** tab.
   This shows you a list of all currently protected folders.
5. Add or remove folders as needed.

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

**Tip:** As you must separately allow all applications that need to access the protected folder, we recommend that you do not add folders that contain your installed games or applications (for example, Steam Library Folders). Otherwise, these applications may stop working correctly.

To remove a folder:

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

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

## 2.5 Prevent applications from downloading harmful files

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

Some websites contain exploits and other harmful files that may harm your computer. With advanced network protection, you can prevent any application from downloading harmful files before they reach your computer.

To block any application from downloading harmful files:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. Select **Edit settings**.

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

3. On the main page, select ⚙.
4. Select **Malware Protection** > **Edit settings**.

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

5. Turn on **Advanced Network Protection**.

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

## 2.6 Using AMSI integration to identify script-based attacks

Antimalware Scan Interface (AMSI) is a Microsoft Windows component that allows the deeper inspection of built-in scripting services.

**Note:** AMSI integration is only available on Windows Server 2016, 2019 and 2022.

Advanced malware uses scripts that are disguised or encrypted to avoid traditional methods of scanning. Such malware is often loaded directly into memory, so it does not use any files on the device.

AMSI is an interface that applications and services that are running on Windows can use to send scanning requests to the antimalware product installed on the computer. This provides additional protection against harmful software that uses scripts or macros on core Windows components, such as PowerShell and Office365, or other applications to evade detection.

To turn on AMSI integration in the product:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Malware Protection** > **Edit settings**.

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

4. Turn on **Antimalware Scan Interface (AMSI)**.

The product now notifies you of any harmful content that AMSI detects, and logs those detections in the event history.

Chapter
3

# Protecting your web browsing

**Topics:**



Browsing Protection helps you browse the internet safely by providing safety ratings for websites on your browser and blocking access to websites that have been rated harmful.

## 3.1 Blocking harmful websites

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

To make sure that Browsing Protection is on:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Secure Browsing**.
4. Select **Edit settings**.

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

5. Turn on **Browsing Protection**.
6. 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.

### 3.1.1 Blocking suspicious and prohibited websites

Browsing Protection can prevent you from unintentionally accessing websites that are not trustworthy or have prohibited content.

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

You can use Browsing Protection to avoid unintentionally accessing these websites.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Secure Browsing**.
4. Select **Edit settings**.

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

5. Make sure that **Browsing Protection** is turned on.
6. If you want to block websites that are rated as suspicious in addition to ones that are considered harmful, select **Block suspicious websites**.
7. If you want to block websites that contain prohibited content, select **Block prohibited websites**.
8. 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.

### 3.1.2 Using reputation rating icons

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. |

To see the reputation rating icons on the search results page:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Secure Browsing**.
4. Select **Edit settings**.

   **Note:** You need administrative rights to change the settings.
5. Make sure that **Browsing Protection** is turned on.
6. Select **Show the reputation rating for web sites 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.

## 3.1.3 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**. You need administrator rights to allow blocked websites.
   The **Add allowed website** window opens, showing the address which you are about to allow.
2. 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.

**Note:** If the block page does not appear, make sure that the Browsing Protection extension is turned on in the web browser that you use.

## 3.1.4 Web site exceptions

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

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

To view and edit web site exceptions:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Secure Browsing** > **Edit settings**.
4. Select **View web site exceptions**.

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

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

   If the web site is not included in either list:

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

5. Select **OK** to return to the main page.

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

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

## 3.2 Checking that browser extensions are in use

Reputation-based browsing **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 tries to install the browser extensions automatically. When you open your browser, it displays a notification about the newly installed extension and you may need to enable it.

If the WithSecure Browsing Protection extension is not listed in your browser, you need to reinstall the extension manually.

If you miss the notification, the main view of the product shows you if the browser extension has not yet been set up. The easiest 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.

However, if you don't see the notification on the product's main view or you have missed it, you can check if the browser extension has been installed and enabled in the following way:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Edit settings** in the pop-up screen at the bottom left corner.

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

4. Select **Yes** to allow the app to make changes to your device.
5. Select **Secure Browsing**.
6. Depending on the web browser you use, do as follows:

   - If you use **Firefox**, under **Add-ons and themes** > **Extensions**, select **Add to Firefox**. The extension will be added and enabled for Firefox.
   - If you use **Chrome**, select first the **Open Chrome Web Store** link under **Browser extensions**. The Browsing Protection by WithSecure page opens in Chrome Web Store. If the extension has already been installed on Chrome but turned off, go to **Extensions** and turn it on. If the extension has not yet been installed, select **Add to Chrome** > **Add extension**. The extension will be added and enabled for Chrome.
   - If you use **Microsoft Edge**, select first the **Open Edge Add-ons** link under **Browser extensions**. The Browsing Protection by WithSecure page opens in Edge Add-ons. If the extension has already been installed on Microsoft Edge but disabled, select **Turn on** to enable it. If the extension has not yet been installed, then select **Get** > **Add extension**. The extension will be added and enabled for Microsoft Edge.

     **Note:** You may need to reinstall the extensions after upgrading the product or installing a new browser.

You can check that the browser extension is turned on by opening the following test page in your browser: https://unsafe.fstestdomain.com. If the product block page opens, the browser extension is in use. If you do not see the product block page, you need to turn on the browser extension manually.

Chapter
4

# Protecting your sensitive data

**Topics:**



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

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

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

***Connection control*** currently supports the following browsers:

- Microsoft Edge (Chromium)
- Firefox
- Google Chrome

## 4.1 Turning on Connection control

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

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

To turn on ***Connection control***:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Secure Browsing** > **Edit settings**.

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

4. Turn on **Connection Control**.
5. To adjust the ***Connection Control*** settings:
   - Clear **Disconnect untrusted apps** if you do not want ***Connection control*** to close your already open connections. If you leave the setting unselected, ***Connection control*** closes all your current Internet connections as well when it activates.
   - If you have to use an external tool that is being blocked by ***Connection Control***, clear **Disconnect command-line and scripting tools**.

     **Note:** We recommend that you keep this setting selected unless it is absolutely necessary, as some malware attacks can use built-in Windows components, such as PowerShell, to gain access to your banking credentials and personal information.

   - Choose how you want ***Connection control*** to handle data that has been copied to your clipboard. By default, ***Connection control*** clears all data from the clipboard to protect your privacy when your ***Connection control*** session ends.

     Clear this settings if you do not want ***Connection control*** to clear your clipboard.

   - By default, remote access to your device is blocked during your banking session. Banking transactions are always private and confidential, and you should never log in to your online bank if someone has remote access to your device.

     **Important:** Do not clear the **Block remote access during banking session** setting on anyone's request unless you know both the person requesting the access and the exact purpose of the request.

## 4.2 Using Connection control

When ***Connection control*** is turned on, it automatically detects when you access an online banking web site.

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

**Tip:** If you do not want to interrupt your other active connections when ***Connection control*** activates, to change the settings, select the **Connection control** indicator, and then select ⚙ at the top right corner of the Connection control notification.

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

1. Click the **Connection control** indicator at the top of your screen.
2. Click **End** on the notification.

Chapter
5

# Setting up content control

**Topics:**



You can limit access to inappropriate content to avoid viewing undesirable material on the internet.

The internet is full of interesting websites, but not all contain content you might consider desirable or appropriate.

With the content blocker, you can ensure no one views inappropriate content on computers by restricting what web pages can be viewed, and scheduling the time that can be spent online. You can also block links to adult content from being shown in search engine results.

## 5.1 Blocking web content

You can limit the types of content that can be viewed while browsing the web.

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

To select the types of web content to block:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Web Content Control**.
4. Select who the settings apply to from the drop-down menu.
5. Turn on **Content filtering** to limit the content you choose on all browsers.
   - To block web pages by content type, select **Block web content**. Then, select checkboxes next to the content types that you want to block.
   - To allow access only to certain web pages, select **Allow only selected web sites**. Then, select **View allowed sites** and enter web addresses that you want to allow.
6. To hide the adult content from search results, turn on **Search Result Filter**.

### 5.1.1 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 web sites. 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. |
|  **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 not categorized. You can use this category to block content that is unknown. |

Chapter
6

# Using the search result filter

**Topics:**



Search result filter hides adult content by making sure that Google, Yahoo, Bing, and YouTube use the SafeSearch "strict" level.

While this cannot block all inappropriate and explicit content from appearing in your search results, it helps you avoid most such material.

## 6.1 Turning on the search result filter

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

To turn on search result filter:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Web Content Control**.
4. Turn on **Search Result Filter**.

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

Chapter
7

# Central management

**Topics:**



This product is run in centrally managed mode, where the product settings are controlled remotely by a trusted expert.

In centrally managed mode:

- some or all of the product settings may be set remotely.
- some of these settings may be locked, so that you cannot change them yourself.

The **Settings** > **Central Management** page shows you information about your computer. You may need to provide this information to your IT administrator if there are issues with your product settings.

Use Windows Event Viewer to check for recorded errors.

## 7.1 Open Windows Event Viewer

If you suspect there was a problem with this product you can use Windows Event Viewer to check if an error was recorded.

Windows Event Viewer stores details of import system events. This includes details of actions and errors of this product.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Central Management**.
4. Click **Open Event Viewer** .
   Windows Event Viewer opens.
5. To find messages from this product, click **Windows Logs** and select either **Application** or **System** .

**Note:** You can click **Source** to order the messages by their source. This makes it easier to find messages from this product.

Chapter
8

# What is a firewall

**Topics:**



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

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

## 8.1 Changing Windows Firewall settings

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

The product uses Windows Firewall to protect your computer.

To change Windows Firewall settings:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main view, select **Viruses & Threats**.
3. Select **Windows Firewall settings**.

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

## 8.2 Using personal firewalls

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

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

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

**Tip:** If your personal firewall has a manual filtering mode, use it to allow all WithSecure processes.

Chapter 9

# Keeping your software up to date

You can use the product to check the software installed on your computer and install any missing updates.

**Note:** Your administrator may restrict the installation of software updates on managed computers.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select  .
   The **Software updates** view shows the updates that are not yet installed.
3. Select **Click here to manage your updates**.

   **Note:** You need administrative rights to install missing updates.
4. Select **Check now** if you want to see if there are new updates available.
5. Select the updates that you want to install.
6. Select **Install selected updates**.
   The **Installations** tab shows you the status and progress for each selected update.

Chapter
10

# How to use updates

**Topics:**



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.

## 10.1 View the latest updates

View the date and time of the latest update.

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

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

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Updates**.
4. You see details of the latest updates under **Connection**.
5. To manually check for the latest updates, select **Check now**.
   The product installs the latest updates automatically if they are available.

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

## 10.2 Updating malware definitions on isolated Server Security hosts

If you have installed Server Security on hosts that do not have a network connection, you can update the malware definitions using the tool provided with Policy Manager.

The tool for downloading updates is bundled with Policy Manager and can be extracted with the provided scripts. When you run it on any machine with internet access, the tool downloads the latest updates and required diffs to generate an all-in-one archive.

By default, the tool uses the `data\updates` folder to store the downloaded update binaries. It also stores the update history to use as a reference for downloading the relevant diffs to the latest version.

In addition to the update binaries, you also need the `fsaua-update_32` tool to import the prepared updates. This tool is included in the Server Security installation package: `C:\Program Files (x86)\F-Secure\Server Security\fsaua-update_32.exe`.

To update the malware definitions:

1. Run the following command on the Policy Manager machine to prepare the tool:
   - Windows: `<F-Secure installation folder>\Management Server 5\bin\prepare-fspm-definitions-update-tool.bat <destination folder>`
   - Linux: `/opt/f-secure/fspms/bin/prepare-fspm-definitions-update-tool <destination folder>`
2. Transfer the prepared binaries to a machine that has internet access, if necessary.
3. Modify the tool configuration, if necessary:
   - `conf\channels.json`: this contains a list of the channels to be updated. By default, it includes updates for all the supported clients managed by Policy Manager, so we recommend that you leave only the Server Security versions necessary for your environment.
4. Run the tool:
   - Windows: `fspm-definitions-update-tool.bat`
   - Linux: `fspm-definitions-update-tool`

   The resulting archive contains the full set of the latest definitions and diffs to this version. If all data is up to date, no archive is generated.
5. Transfer the prepared archive (`data\f-secure-updates.zip` by default) to the isolated host directory on the isolated Server Security host: `C:\Program Files (x86)\F-Secure\Server Security`

6. Launch the update on the isolated host: Run `C:\Program Files (x86)\F-Secure\Server Security\fsaua-update_32.exe` with administrator privileges.

## 10.3 Change connection settings

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

Your Internet service provider (ISP) may offer or require you to use a proxy. A proxy acts as an intermediary between your computer and the internet. It intercepts all requests to the internet to see if it can fulfill the request using its cache. Proxies are used to improve performance, filter requests, and hide your computer from the internet to improve security.

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Updates** > **Edit settings**.

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

4. Under **Manual proxy setup**, select whether or not your computer uses a proxy server to connect to the internet.
   - Select **Do not use** if your computer is connected to the internet directly.
   - Select **Use the browser's settings** to use the same HTTP proxy settings that you have configured in your web browser.
   - Select **Custom address** and then add the proxy address and the **Port** number to configure your HTTP proxy settings manually.

Chapter
11

# Privacy

**Topics:**



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

## 11.1 Security Data

The service sends queries on potential malicious activities or on protected devices to the WithSecure ***Security Cloud***.

The WithSecure Security Cloud is a cloud-based system for cyber threat analysis that is operated by WithSecure. 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 Security Cloud, WithSecure 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 WithSecure for security reasons. Security data is not used for personalized marketing purposes.

Contributing data

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. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select .
3. Go to the **Privacy** settings page.
4. Select **Edit settings**.

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

5. Under **Security Cloud**, select **Allow deeper analysis**.

## 11.2 Improving the product

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

To send usage data:

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select .
3. Go to the **Privacy** settings page.
4. Select **Edit settings**.

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

5. Under **Product improvement**, select **Send non-personalized usage data**.

**Note:** You can read our Privacy Statement here.

Chapter
12

# Technical support

**Topics:**



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 WithSecure Community and see if you can find an answer to your question there.

## 12.1 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 WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Support**.
4. Find information of the currently installed product under **Version information**.

## 12.2 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. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Support**.
4. Select **Edit settings**.

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

5. Select **Run support tool**.
6. Select **Run diagnostics** on the **Support Tool** window.
   The support tool starts and displays the progress of the data collection.

When the tool has finished running, it saves the collected data to an archive on your desktop. You can submit the collected data (the diagnostics file) here:
https://www.withsecure.com/en/support/contact-support/email-support.

**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 Windows**, select **Download** and save the `fsdiag_standalone.exe` file, for example in your Downloads folder. Double-click the file to run the tool.

## 12.3 Debugging product issues

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

You can temporarily give our customer support specific permission to analyze issues in the product. Note that the information collected by debug logging may be regarded as sensitive.

WebView2 is a technology used for embedding web content in native applications. For example, our account log-in page uses the WebView2 technology.

If you are having difficulties with the embedded web views, the WebView2 console debugger can help our customer support analyze the web view issues for you.

To give our support temporary permission to debug product issues:

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

1. Open WithSecure Server Security from the Windows **Start** menu.
2. On the main page, select ⚙.
3. Select **Edit settings**.

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

4. Under **Tools**, select the toggle switch to turn on **Debug logging**.
   Once the debug logging is enabled, the **WebView2 console debugger** option becomes visible.
5. If you want to turn on **WebView2 console debugger**, select the toggle switch.
   Once you enter an embedded web view, the console window opens.
6. As soon as our customer support has completed analyzing the issue, turn off **Debug logging** by selecting the toggle switch.

## 12.4 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 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 **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 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.