Diagnostic Tools

Windows Operating System

Introduction

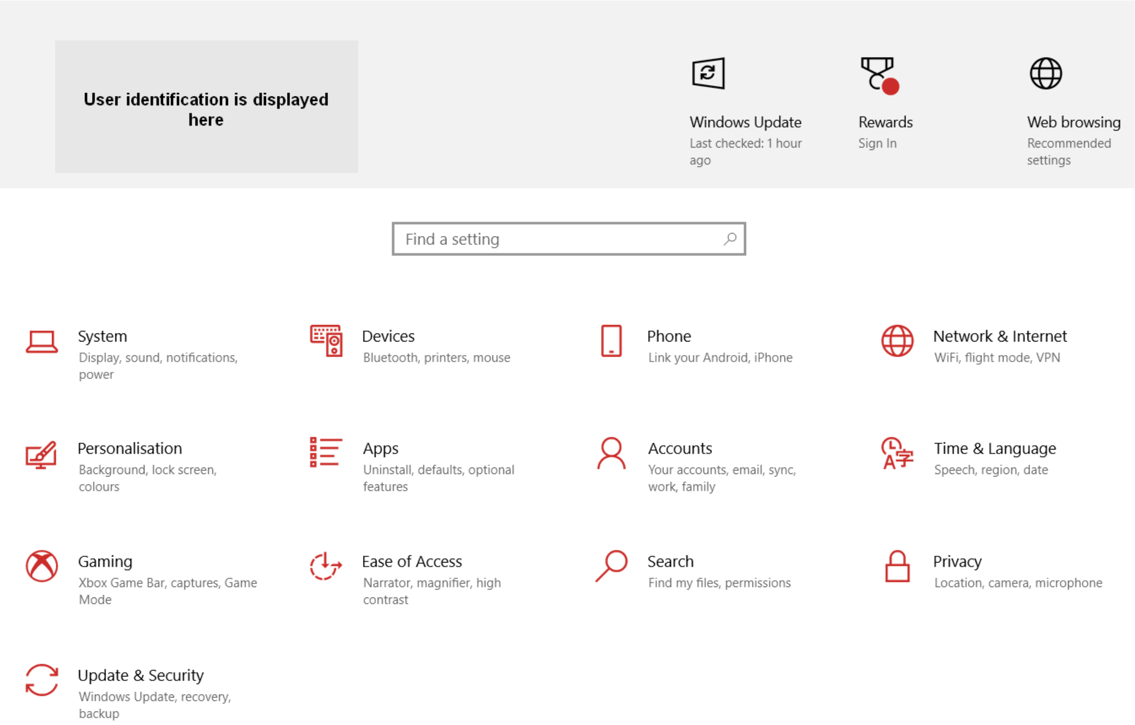
This booklet provides an overview of the diagnostic tools found in the Windows Operating System.

It is for use in learning how to access and apply these during efforts to identify and resolve faults and errors within a computer.

Contents

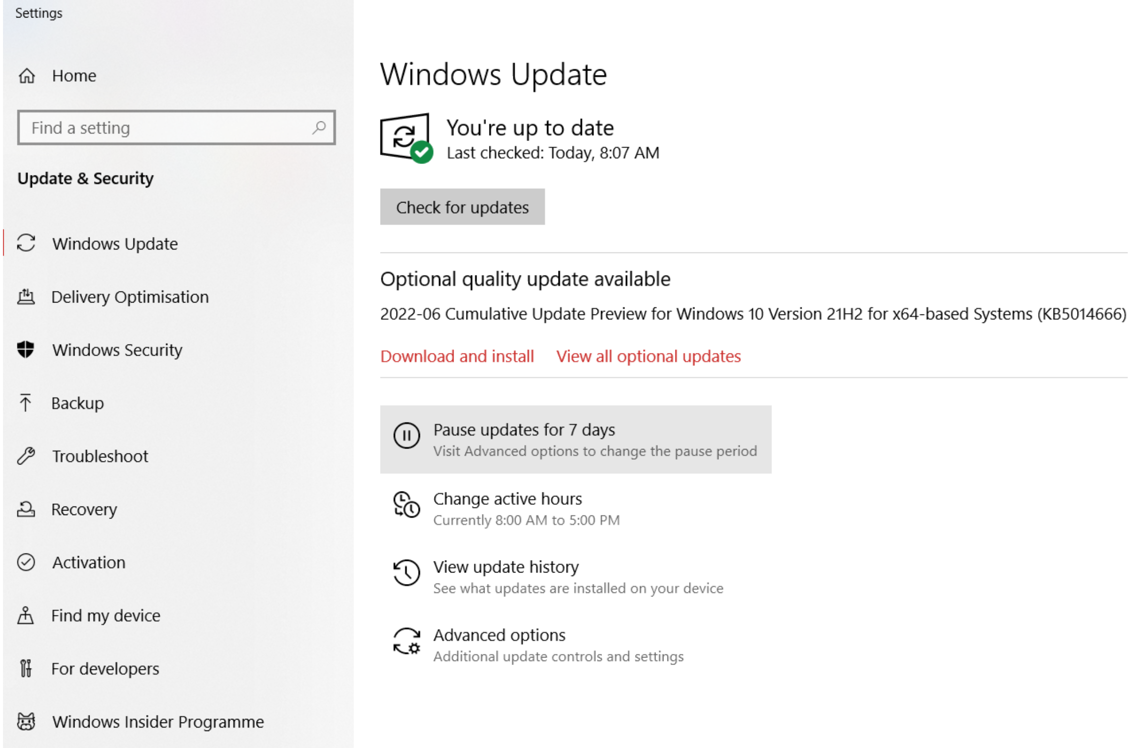
Checking Updates

To check if the Windows Operating System is the most current, open the Settings screen.



User identification is displayed here
Windows Update
Last checked: 1 hour ago
Rewards
Sign In
Web browsing
Recommended settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
WiFi, flight mode, VPN
Personalisation
Background, lock screen, colours
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

Checking of the O/S update status can occur by clicking the displayed Update details at the top banner leading to this menu screen:



You're up to date

Last checked: Today, 8:07 AM

Optional quality update available

2022-06 Cumulative Update Preview for Windows 10 Version 21H2 for x64-based Systems (KB5014666)

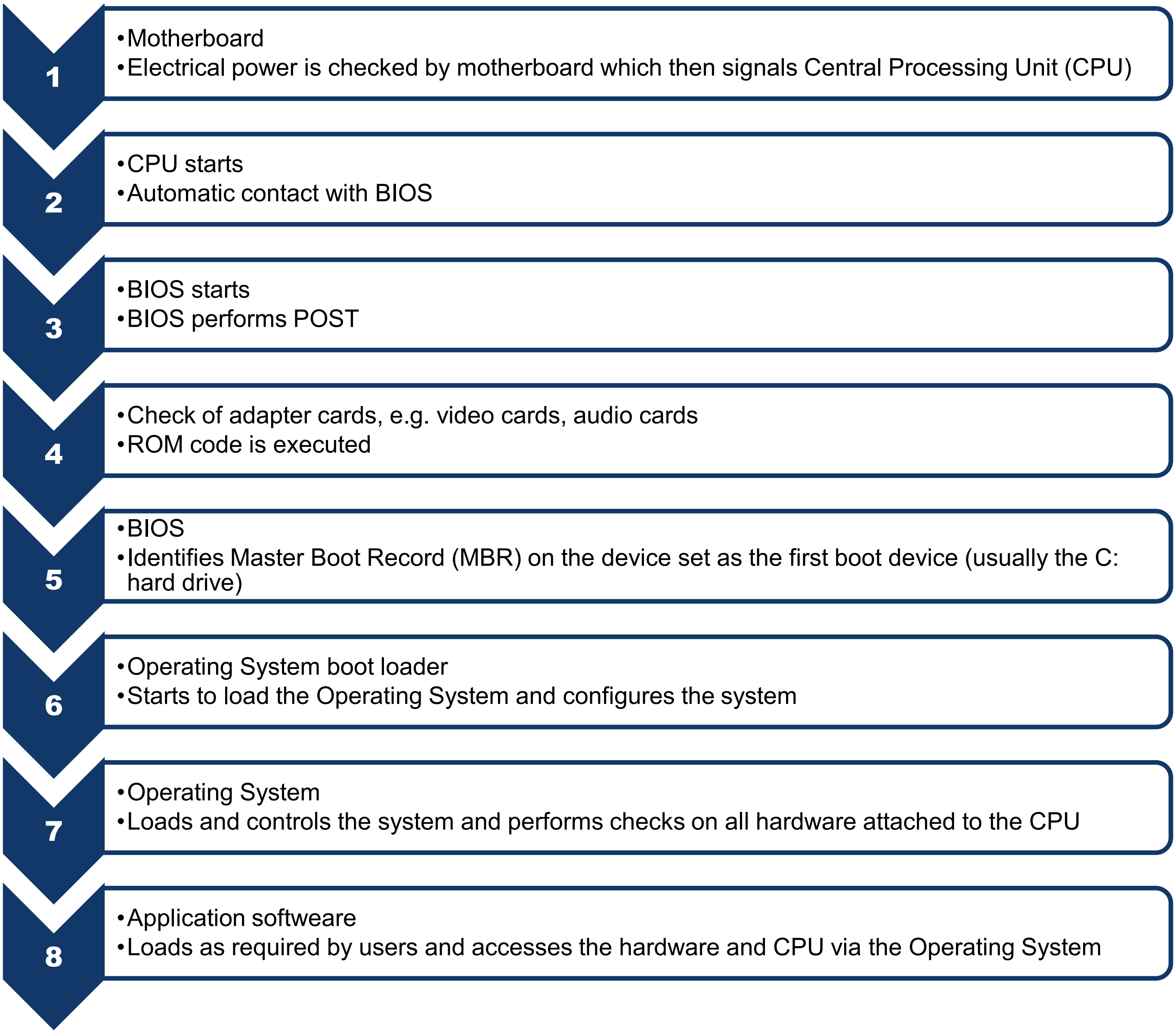
Currently 8:00 AM to 5:00 PM

System diagnostic

Because most of a computer’s work cannot be seen, a person must rely on the Operating System’s utility tools to investigate the machine’s activities and to identify and report its faults.

If the initial checks have occurred, the first ‘technical’ process to be tried is the Power On Self Test or more commonly known as a POST and system beep codes.

When a computer is turned on, the Basic Input / Output System (BIOS) performs a POST as part of the startup process. The startup process is called a ‘boot’ by may also be known as an initial program loading or bootstrapping. The sequencing of the ‘boot’ is where a computer searches non-volatile data storage devices containing program code to load the operating system (O/S). The sequencing of a computer ‘boot’ is shown below:



1
- Motherboard
- Electrical power is checked by motherboard which then signals Central Processing Unit (CPU)

2
- CPU starts
- Automatic contact with BIOS

3
- BIOS starts
- BIOS performs POST

4
- Check of adapter cards, e.g. video cards, audio cards
- ROM code is executed

5
- BIOS
- Identifies Master Boot Record (MBR) on the device set as the first boot device (usually the C: hard drive)

6
- Operating System boot loader
- Starts to load the Operating System and configures the system

7
- Operating System
- Loads and controls the system and performs checks on all hardware attached to the CPU

8
- Application softweare
- Loads as required by users and accesses the hardware and CPU via the Operating System

The POST conducts only basic hardware tests, e.g. it would only detect if a hard drive were present and appeared to be operational; it would not diagnose any problems that might occur with the hard drive.
At the end of the POST, the computer plays an audible beep. If the POST does not detect any problems with the system, it will generally play a single short beep to let the user know the test is complete. The computer will then continue to start up and load the operating system.

If however, the POST does detect any errors with any hardware devices, it reports the errors in various ways depending upon which stage of the boot process it is at. If it needs to report an error before the monitor is functioning, it uses what are called ‘beep codes’.

Beep codes are used by the vast majority of the major BIOS manufacturers though there may be some differences in the actual codes used. The beep codes for a specific BIOS may even vary between different versions of the same BIOS’s and between different manufacturers of the various BIOS’s. To make matters even more complicated, motherboards may influence the beep codes given by a BIOS.

Most motherboard manufacturers will list the specific beep codes in their product manuals. These codes should be cross referenced to the beep codes published by the various BIOS suppliers. This information is generally available from the product’s manual and the manufacturer’s website.

Website examples:

Understanding Beep Codes on a Dell Desktop Personal Computer

Beep Codes for a AMI BIOS

BIOS Beep Codes for Intel Desktop Motherboards

Using a POST card

There is a challenge with POST beep codes.

If a computer does not ‘boot’ then it is probable that the internal POST will not sound any of the beep codes. If this occurs a diagnostic hardware device called a POST card, or diagnostic board, may be used to help in diagnosing problems.

POST card for use with desktop computers

POST card for use with laptop computers

A POST card functions by detecting the POST codes generated by the operating system and displaying them in some other way other than using the system’s monitor or speakers. The codes are generally displayed using LED lights and/or hexadecimal numbers. (The hexadecimal number system is a type of number system, that has a base value equal to 16 – for more information on the number system used in computer software visit this site)

ICT technicians can use this reference documentation to interpret the meaning of the lights and/or hexadecimal numbers.

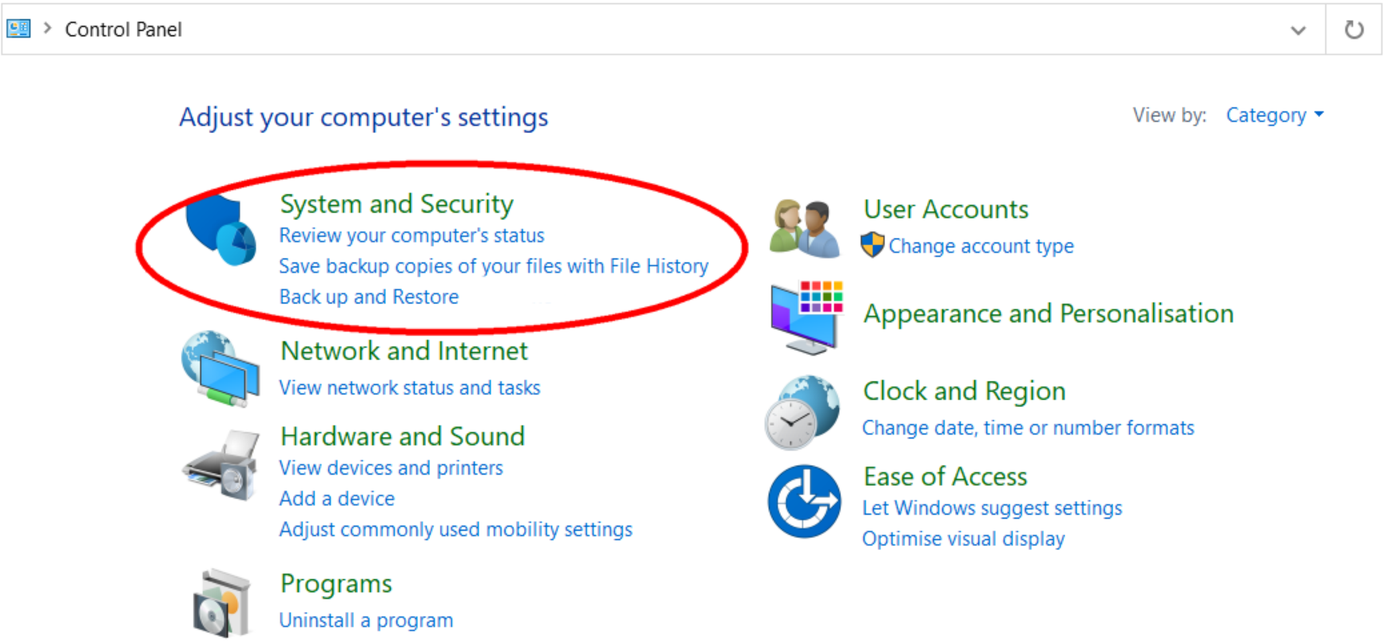
POST cards are usually designed to work with specific chip sets and therefore their messages are likely to be misleading when used with different chips and motherboards. There are however some manufactures which construct their POST cards to work on more than one type of motherboard slot.

It is not even necessary to have a monitor or hard disk to troubleshoot a system using this type of diagnostic device. The general procedures for using a POST card are as follows:

1. Before starting, make a note of the BIOS version by reading the stamp on the BIOS chip or by using Windows Setup.
2. Disconnect the power to the computer.
3. Install the card in an empty PCI or ISA slot depending on the type of card.
4. Record the POST codes shown by the LED lights and/or hexadecimal numbers.
5. Refer to the POST card manual to interpret the POST codes.

Windows 10 Diagnostic Tools

To locate and do basic diagnostic tasks in Windows 10 go to the ‘**Control Panel**’ and click on ‘**System and Security**’.



Control Panel

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

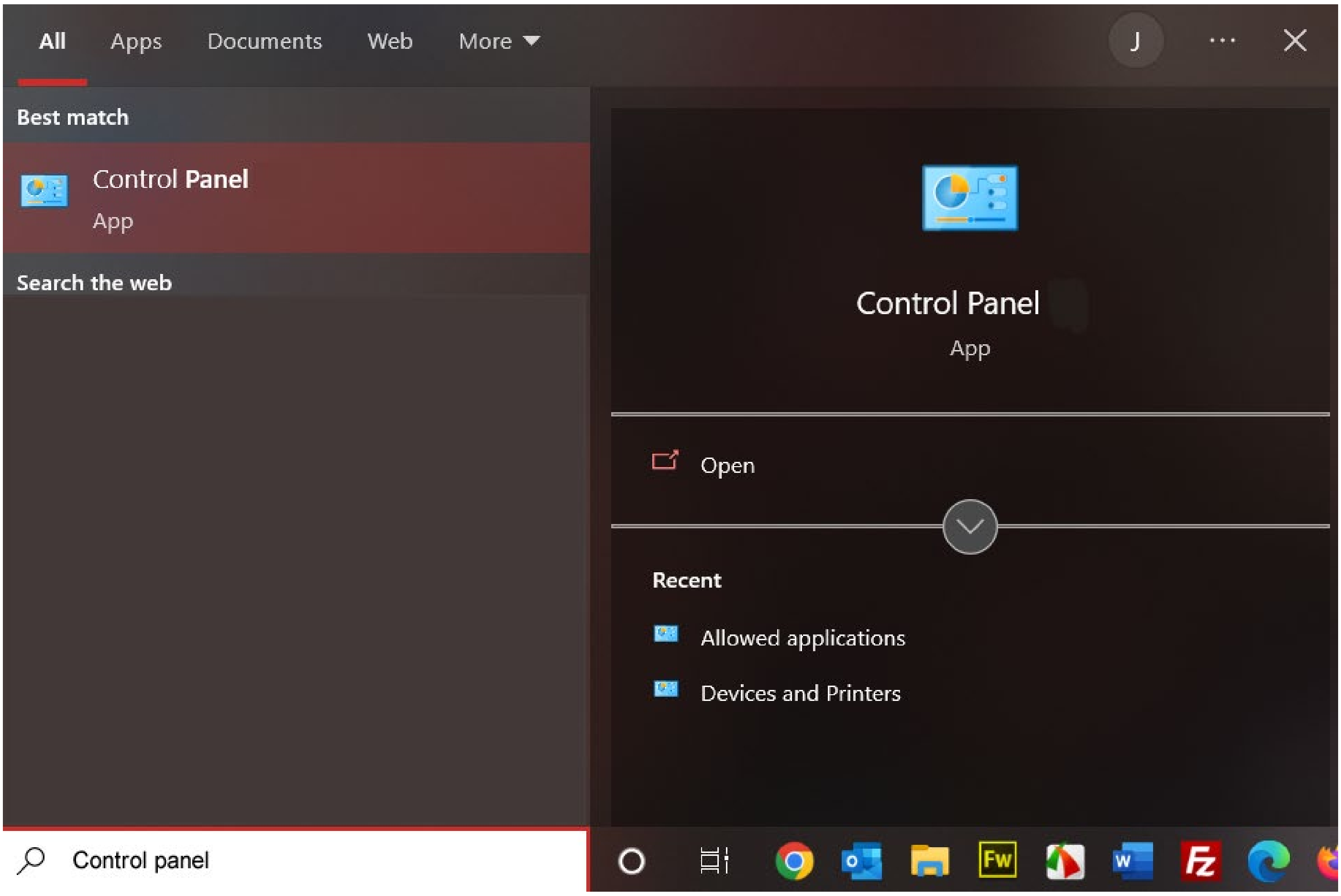
User Accounts
Change account type

Appearance and Personalisation

Clock and Region
Change date, time or number formats

Ease of Access
Let Windows suggest settings
Optimise visual display

The Control Panel may also be accessed by using the Search field at the bottom left of the desktop.



Best match

Control Panel
App

Search the web

Control Panel
App

Open

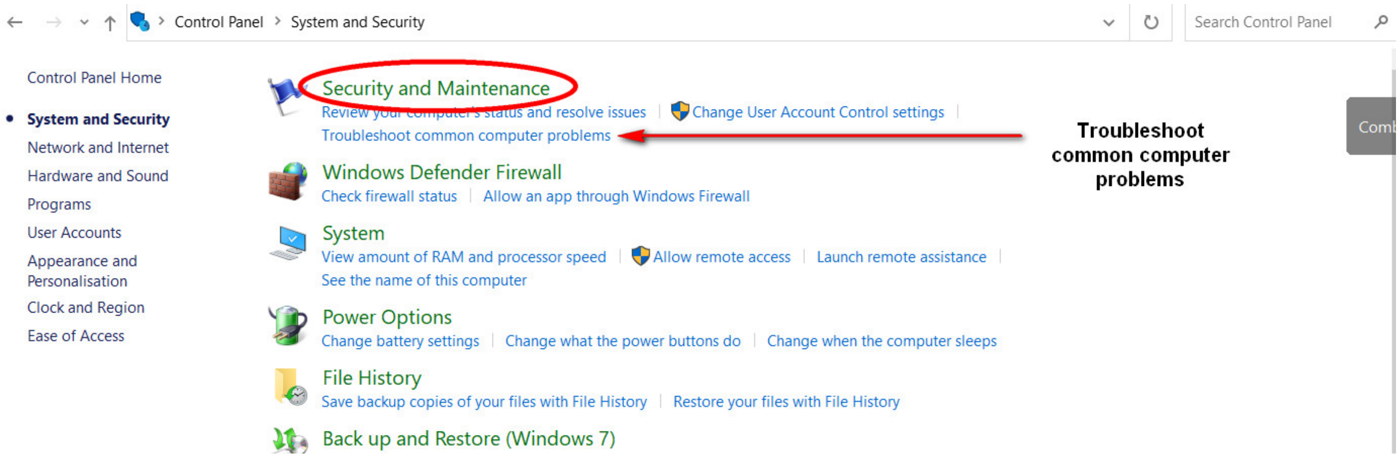
Recent

Allowed applications

Devices and Printers

Control panel

In the next window you click on ‘**Troubleshoot common computer problems**’ under ‘**Security and Maintenance**’.



Control Panel > System and Security

Search Control Panel

Control Panel Home

- **System and Security**

Network and Internet

Hardware and Sound

Programs

User Accounts

Appearance and Personalisation

Clock and Region

Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings |
Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance |
See the name of this computer

Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps

File History
Save backup copies of your files with File History | Restore your files with File History

Back up and Restore (Windows 7)

Troubleshoot common computer problems

Comb

Windows 10 above uses troubleshooters to help solve problems with a computer. To run a Troubleshooter:

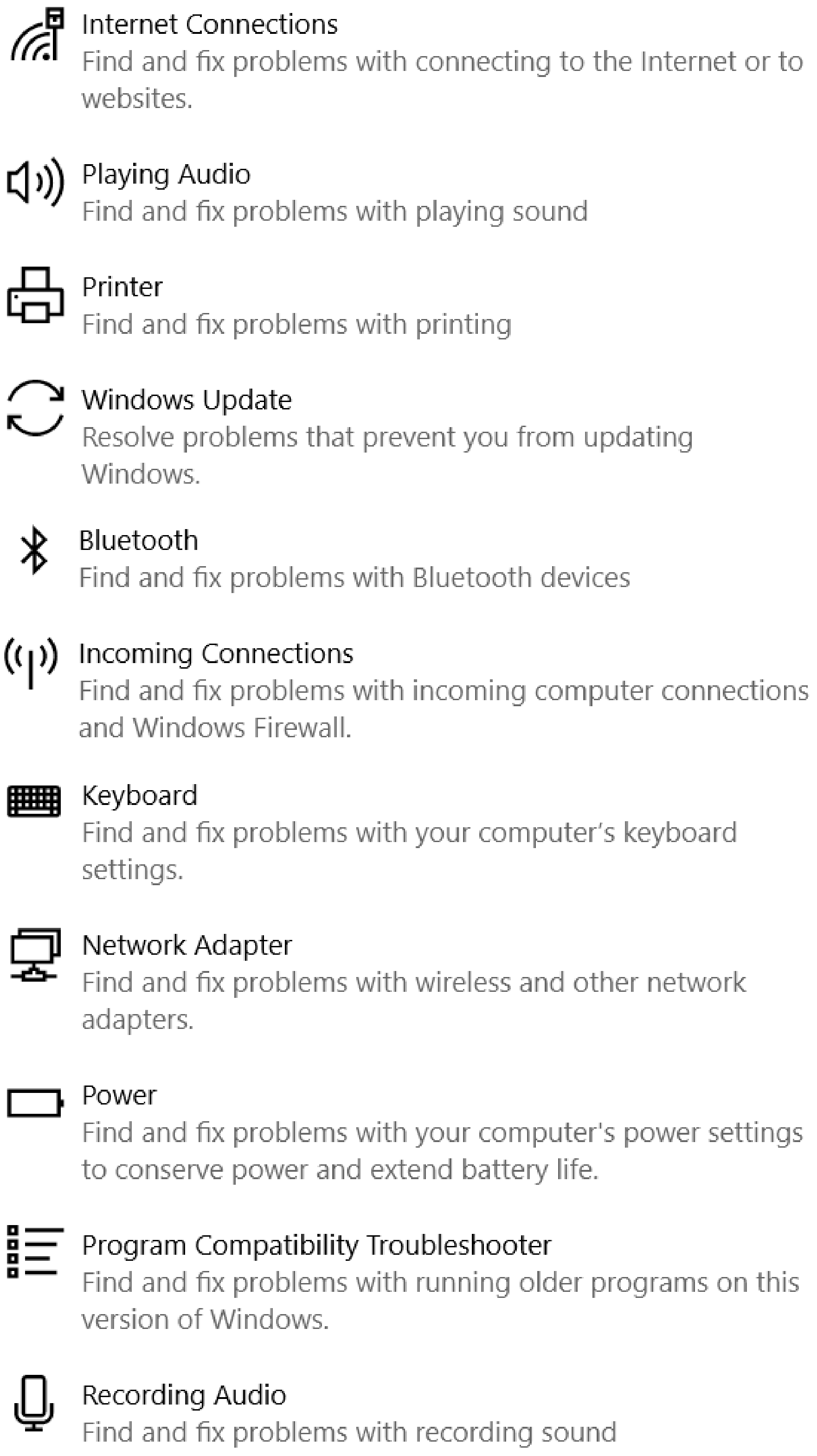
1. Select **Start > Settings > Update & Security > Troubleshoot**.

2. Select the type of troubleshooting required, then select **Run the selected Troubleshooter**.

3. Allow the Troubleshooter to run and then answer any questions on the screen. If a message displays that no changes or updates were necessary, the user can try recovery options, or find out more about error codes.

Use Windows 11/10 Troubleshooters to Fix Windows Errors

On the Troubleshoot page in Windows 11/10, user can access and run various Windows Troubleshooters to solve different Windows issues. Clicking the **Run** button next to the target troubleshooter to instantly run the troubleshooter with one click. Check the functions of the different troubleshooters in Windows 11/10 below.



Internet Connections
Find and fix problems with connecting to the Internet or to websites.

Playing Audio
Find and fix problems with playing sound

Printer
Find and fix problems with printing

Windows Update
Resolve problems that prevent you from updating Windows.

Bluetooth
Find and fix problems with Bluetooth devices

Incoming Connections
Find and fix problems with incoming computer connections and Windows Firewall.

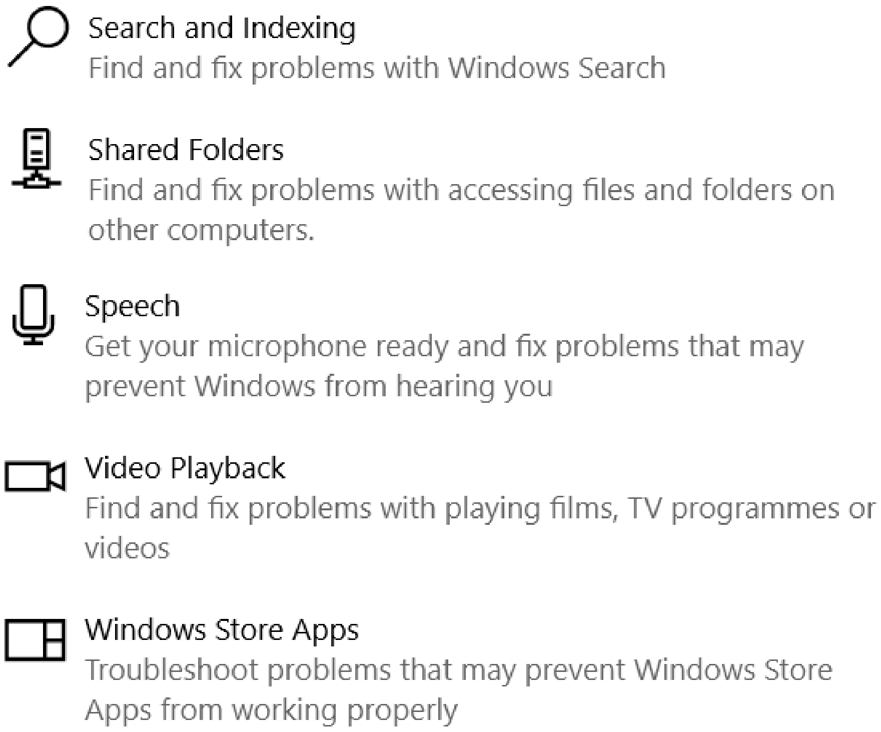
Keyboard
Find and fix problems with your computer's keyboard settings.

Network Adapter
Find and fix problems with wireless and other network adapters.

Power
Find and fix problems with your computer's power settings to conserve power and extend battery life.

Program Compatibility Troubleshooter
Find and fix problems with running older programs on this version of Windows.

Recording Audio
Find and fix problems with recording sound



Search and Indexing
Find and fix problems with Windows Search

Shared Folders
Find and fix problems with accessing files and folders on other computers.

Speech
Get your microphone ready and fix problems that may prevent Windows from hearing you

Video Playback
Find and fix problems with playing films, TV programmes or videos

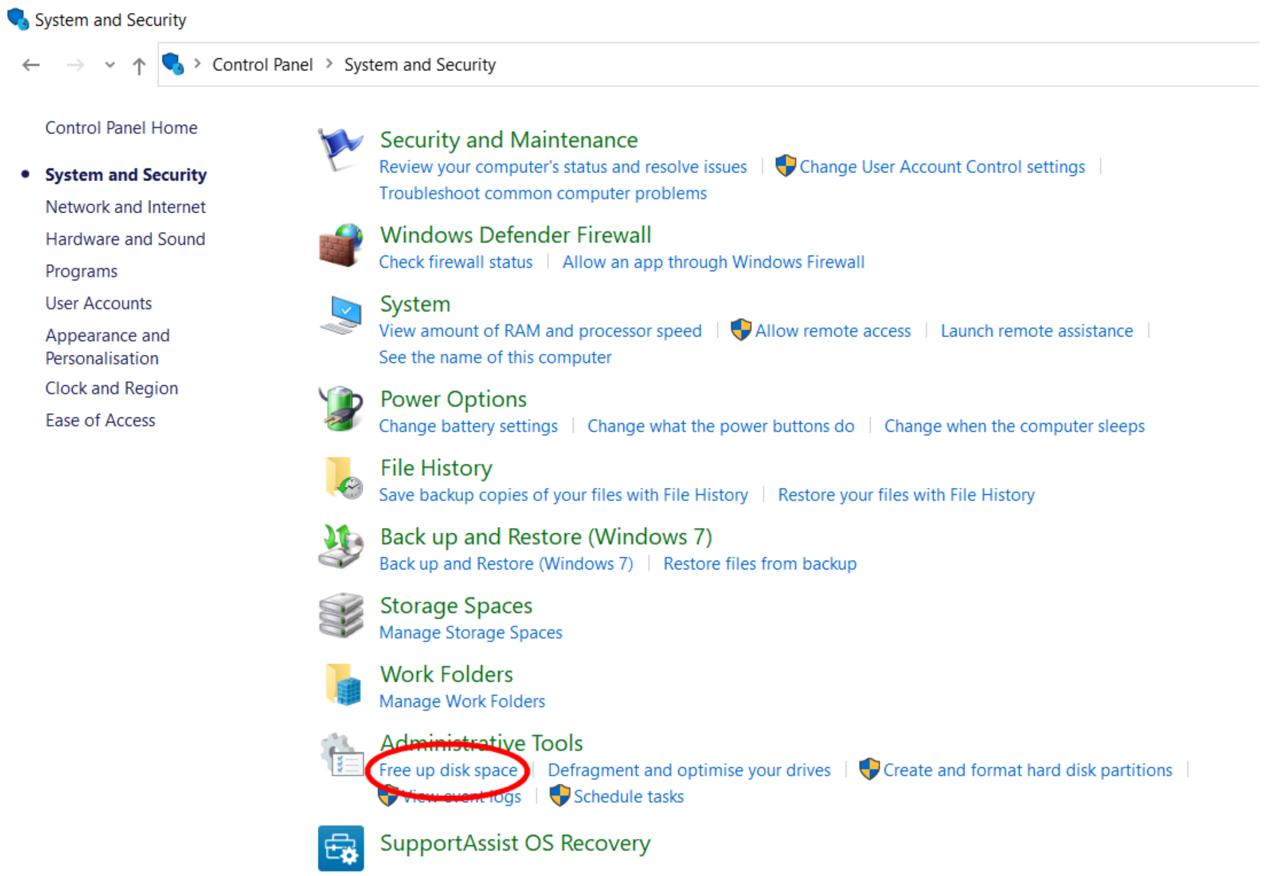
Windows Store Apps
Troubleshoot problems that may prevent Windows Store Apps from working properly

The built-in Windows 11/10 troubleshooters can conduct an effective diagnosis of the problems. They can fix the issues in a Windows computer to some extent. Besides, it is very easy to use for users to run the troubleshooter with one click.

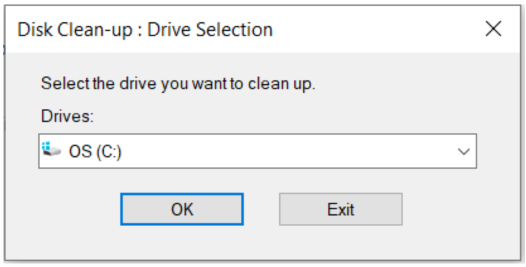
If the troubleshooter in Windows Settings is not available, a user can use the general **Hardware and Devices troubleshooter** in Windows to fix some Windows issues. To open and run the built-in **Hardware and Devices troubleshooter**, press **Windows + R**, type **msdt.exe -id DeviceDiagnostic**, and press Enter to open the tool. It can also help diagnose and fix the hardware and devices issues in Windows.

Cleaning Up Hard Drives

To clean up hard drives and gain more storage space, use the Control Panel to access the System and Security panel again. This time, the area to access is in **Administrative Tools> Free up disk space**.

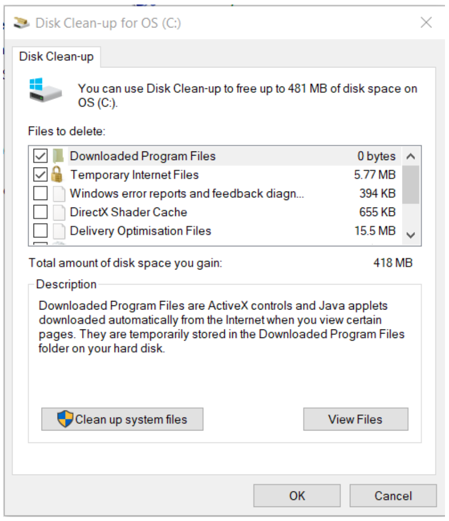

System and Security
Control Panel > System and Security
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalisation
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall
System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer
Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps
File History
Save backup copies of your files with File History | Restore your files with File History
Back up and Restore (Windows 7)
Back up and Restore (Windows 7) | Restore files from backup
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space | Defragment and optimise your drives | Create and format hard disk partitions | View event logs | Schedule tasks
SupportAssist OS Recovery

Select the hard drive to clean and organise.



Select the drive you want to clean up.

Drives: OS (C:)



You can use Disk Clean-up to free up to 481 MB of disk space on OS (C:).

Files to delete:

☑	Downloaded Program Files	0 bytes
☑	Temporary Internet Files	5.77 MB
☐	Windows error reports and feedback diagn...	394 KB
☐	DirectX Shader Cache	655 KB
☐	Delivery Optimisation Files	15.5 MB

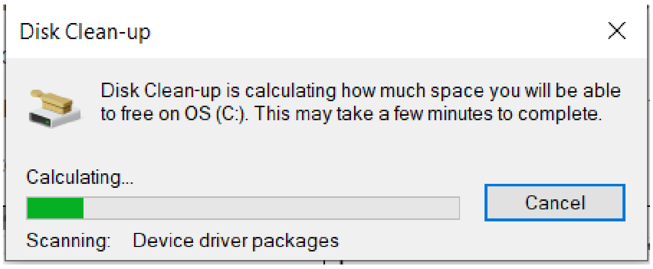
Total amount of disk space you gain: 418 MB

Description

Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

Selecting OK starts an analysis what needs to be cleared. This is then shown in the screen:

Clicking the Clean-up system files starts the cleaning process.



Disk Clean-up is calculating how much space you will be able to free on OS (C:). This may take a few minutes to complete.

Calculating...

Scanning: Device driver packages

In the next popup window, a report is shown on the amount of fragmentation on the disks. In the example below the disks are OK – note that in Windows 10/11, the defragmentation process is an automatically scheduled procedure. You are still able to manual ‘defrag’ a disk.

However, it is suggested that you ‘**Analyse Disk**’. If it does not require a defragmentation, a window will appear suggesting defragmenting is not required.

Defragmenting a disk can take some time. It is suggested a user does not use the computer until the defragmenting is completed.

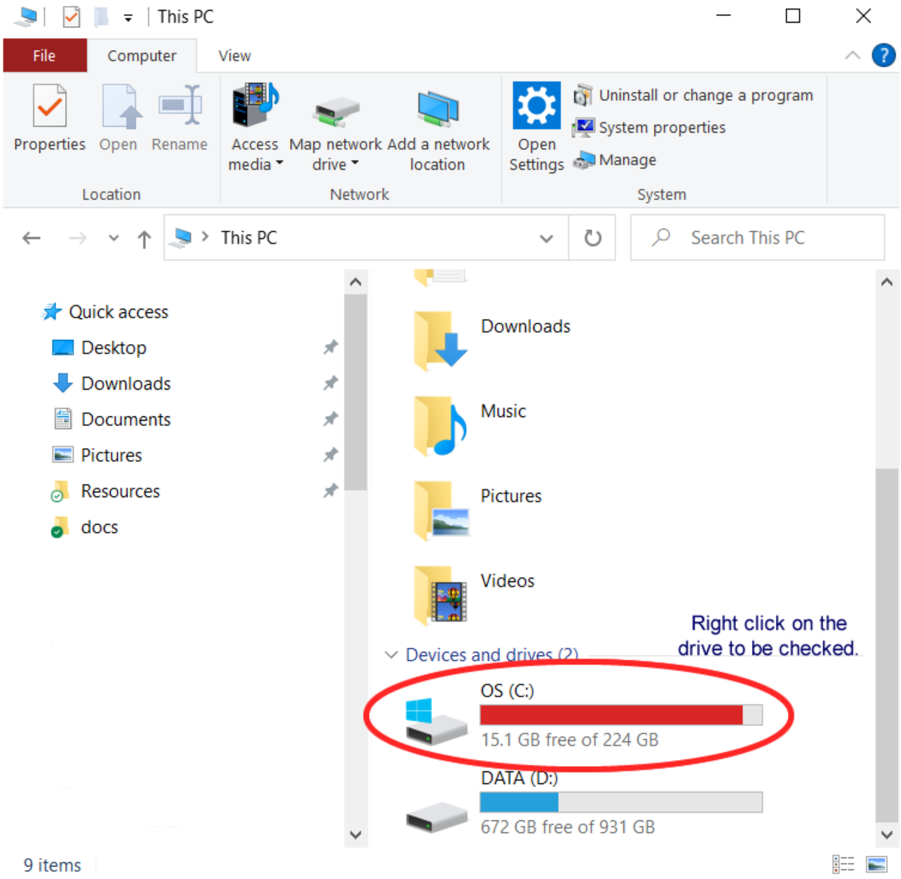
To defragment the disks, select the disk and click ‘**Optimise**’.

CHKDSK Utility

Like the defragmentation tool, the **Check Disk (CHKDSK)** utility tool in Windows 10/11 operates automatically conducting disk error checking. This means that it is not as important as it once was, for a user to check for disk errors. The tool remains available to users and can be used manually.

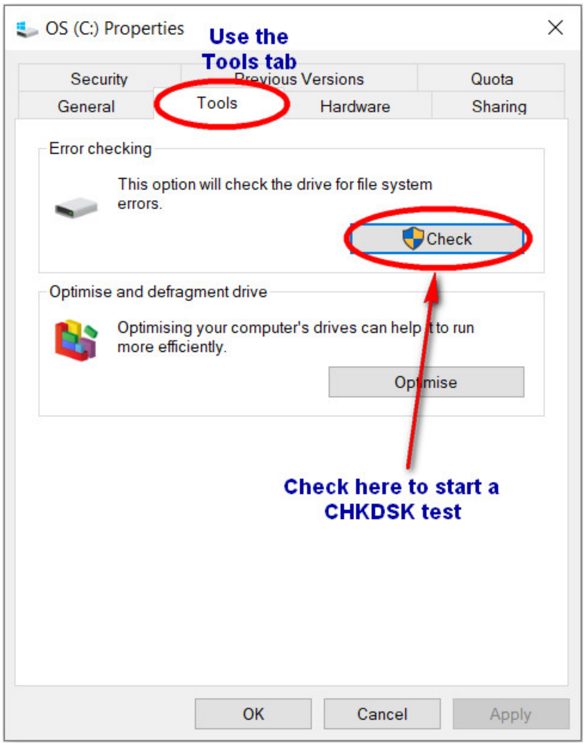
The Check Disk (CHKDSK) utility tool is a **Settings window** serves as a central hub for most of your computer's basic settings.

To run CHKDSK in Windows 10/11, go to the '**Start Menu**' and click on '**File Explorer**'.
On the next window, click on 'This PC' and then you right click on the to be tested drive's icon.

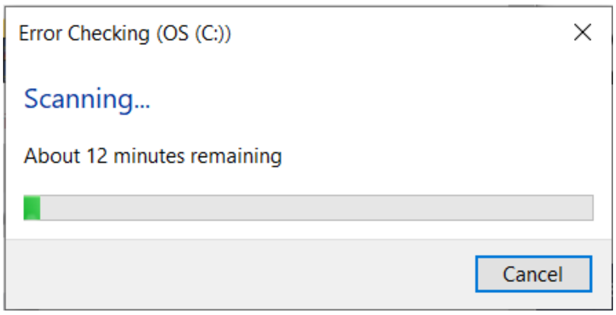


Right click on the drive to be checked.

This will take you to the popup menu:

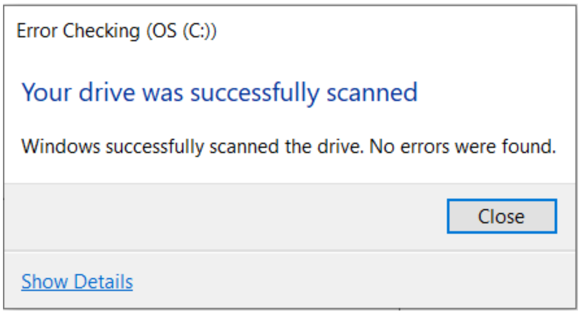

OS (C:) Properties
Use the Tools tab
Security
Previous Versions
Quota
General
Tools
Hardware
Sharing
Error checking
This option will check the drive for file system errors.
Check
Optimise and defragment drive
Optimising your computer's drives can help it to run more efficiently.
Optimise
Check here to start a CHKDSK test
OK
Cancel
Apply

In the next window click on ‘**Tools**’, then ‘**Check**’ under ‘**Error Checking**’. As stated earlier, Windows 10/11 automatically carries out disk error checking, so a popup window may appear that states a disk check is not required. If a disk check is still required, then clicking on ‘**Scan drive**’ will start the utility and display a progress window.


Error Checking (OS (C:))

Scanning...

About 12 minutes remaining


Error Checking (OS (C:))

Your drive was successfully scanned

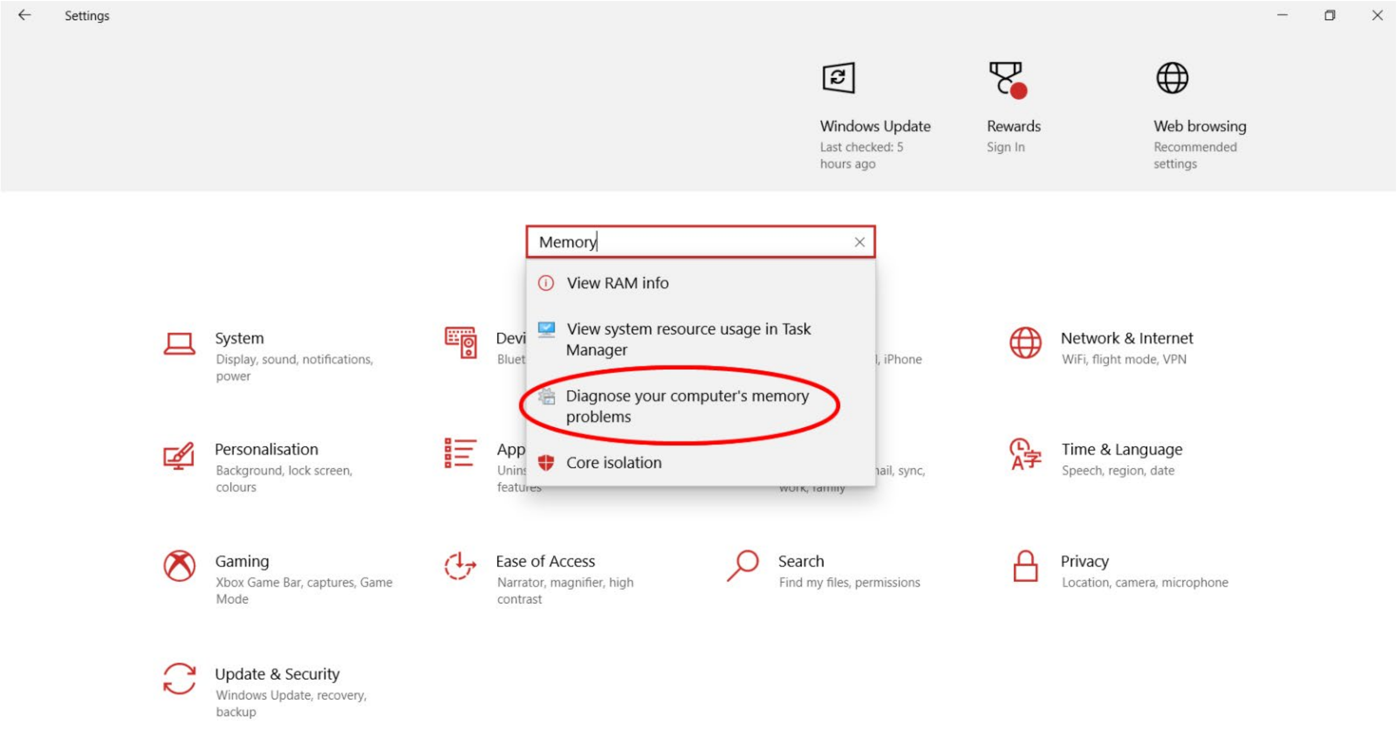
Windows successfully scanned the drive. No errors were found.

Windows Memory Test

Windows 10/11 includes built-in features to help a user identify and diagnose problems with the computer’s memory. If it is suspected that a computer has a memory problem that isn’t being automatically detected, a user can run the **Windows Memory Diagnostics** utility.

To start this application, go to the ’**Start Menu**’ and open the ’**Settings**’ panel and then in the search field type in ’**Memory**’.

In the new window, click on ‘’**Diagnose your computers memory problems**’.


Settings
Windows Update
Last checked: 5 hours ago
Rewards
Sign In
Web browsing
Recommended settings
Memory
View RAM info
View system resource usage in Task Manager
Diagnose your computer's memory problems
Core isolation
System
Display, sound, notifications, power
Devi
Bluet
, iPhone
Network & Internet
WiFi, flight mode, VPN
Personalisation
Background, lock screen, colours
App
Unins
features
ail, sync,
work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

A window will appear to start the memory diagnostic check. It is important that all programs and applications are closed prior to starting the diagnostic check. The check may can take some time. If the ‘**Restart now and check for problems**’ option is selected, make certain that work is saved and programs are exited, as this option starts the check tool immediately.

.

The Memory Diagnostics Tool will run automatically when you click on ‘Restart now…’.

It might take several minutes for the tool to finish checking your computer's memory. When the check test is completed, Windows automatically restarts. If there are no errors, the tool will inform the user.

If the check tool detects errors, contacting the computer manufacturer for information about fixing these will need to occur as memory errors usually indicate a problem with the memory chips in the computer or other significant hardware problem. It is possible that the memory modules (RAM chips) may simply not be correctly installed in the appropriate motherboard memory socket. This would cause memory errors, even though the RAM chips are not faulty.

Manually identify error RAM chips

When there is a need to manually identify a failing memory component, work must be carried out on the internal hardware, i.e. within the computer's case.

Doing this incorrectly or without care may result in damage to hardware and the added expense to repair or replace components. Persons should not attempt to do this if they:

- Have no experience working with computer hardware
- Are unwilling to take the chance of damaging the hardware
- Have a computer that is still under warranty.

If work with the internal hardware is to go ahead, then the following must occur:

- The computer is turned off and the power cord is disconnected from the power socket.
- Remove personal static by touching an unpainted metal part of the computer case with a part of the body to discharge any static electricity from worker's body.
- Avoid walking walk around while working on a computer (walking can produce static electrical build-up). If breaking from the computer work, the person needs to re-ground themself before working on the computer again.
- Wear an antistatic wrist strap.

The process for checking RAM chips for errors is described below:

1. Remove all memory modules except for one.
2. Rerun Windows Memory Diagnostic and then do one of the following:
    - If no errors are reported, remove the current memory module and add one from the
    - set of memory modules that you previously removed.
    - Rerun Windows Memory Diagnostic.
    - If errors are reported, remove the current memory module, making sure to separate it from the other memory modules.
    - Add a new memory module from the set of memory modules that have not yet been
    - tested.
    - Rerun Windows Memory Diagnostic.
    - Repeat this procedure until all the memory modules have been tested.

System Configuration

Modifying a computer’s system configuration is a way of fixing some of the error issues that may be identified.

If errors have been found in during boot up via the standard POST start test or through POST Card use, it is likely that the error is a hardware issue. If this is the case, the hardware component should be replaced and the tests run again to see if the error has reappeared.

If a diagnostic tool identifies a software error and provides a list of recommended actions, note these and then process each recommendation until the error is repaired.

If the diagnostic tool identifies an error, but has no recommended repair process, or if the recommended repair does not resolve the issue, further research will be needed to find a solution.

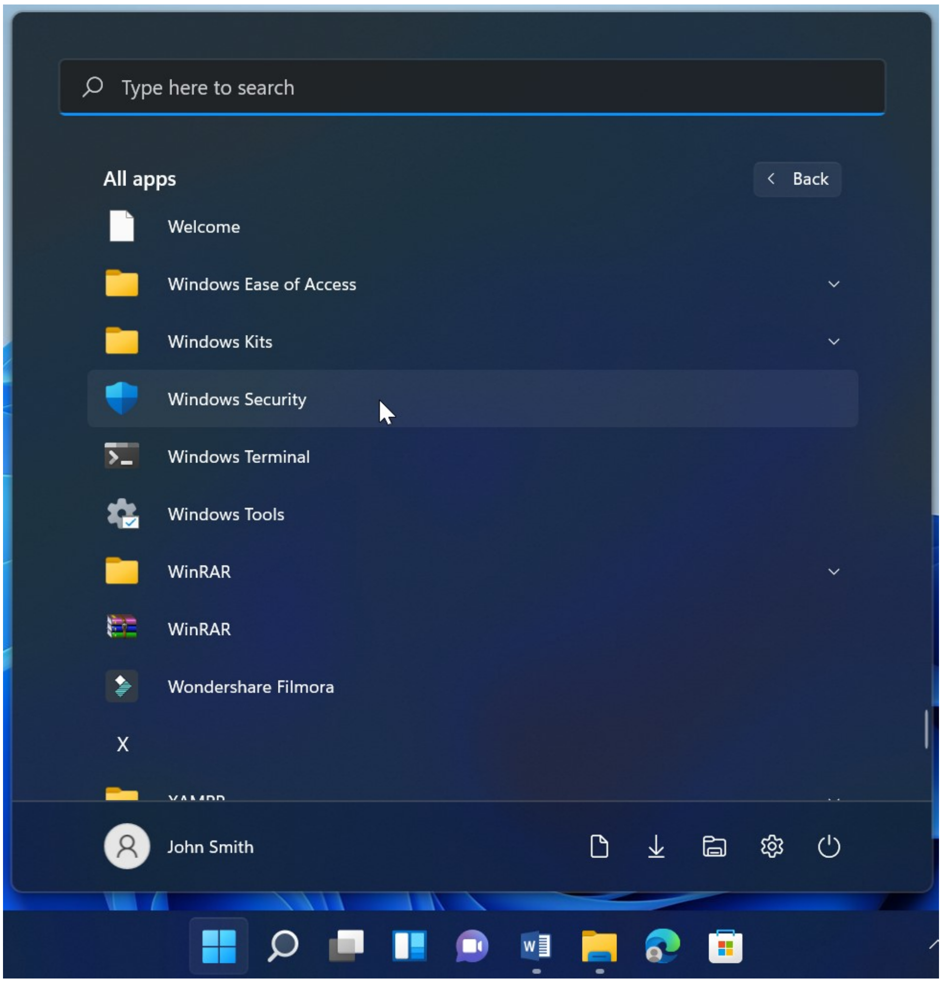
When errors have been resolved, always run the diagnostics tests again as a check that the repair is working and that the initial error was not hiding other faults. It is possible for some issues to hide others, e.g. a video card may not be seated correctly but this is also hiding the fact that the driver software is incorrect. Until the hardware issue is fixed, the software issue cannot be identified.

Computer security

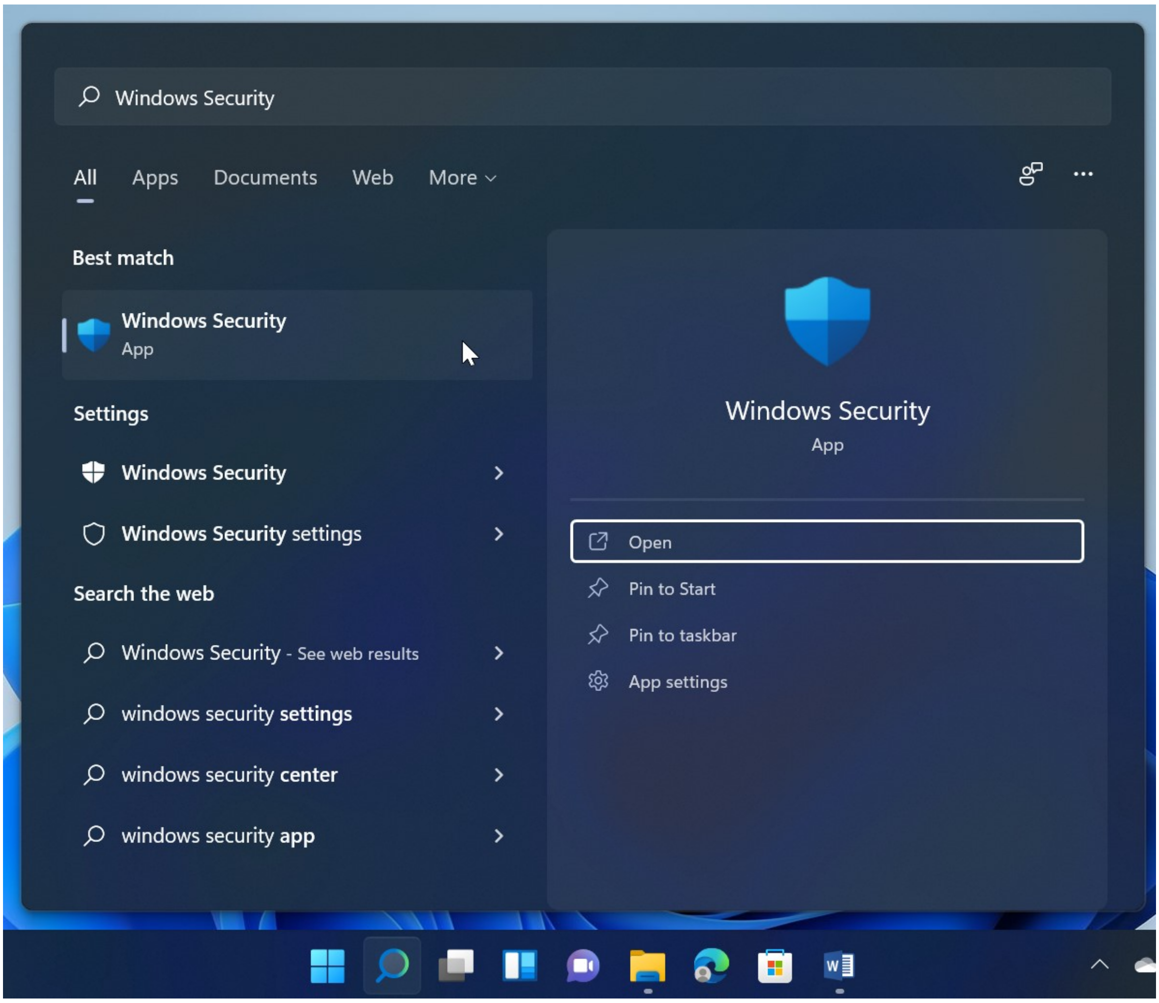
It is worthwhile spending some time on the most recent release of Windows – Windows 11. This Operating System includes a built-in antivirus package called **Windows Security** that is active as soon as the computer is turned on. Windows Security is designed to protect the computer from a variety of threats found on the Internet.

It will scan any files that are downloaded to a computer, looking for malicious code. As this application is automated to ensure that it scans for threats on a regular basis and will update itself, typically there is little need to interact with it often. However, it is important to know how to work with it, should the need arise.

Windows Security, unlike other third-party security products, is integrated directly into the Windows 11 operating system. It does have an interface that can be used to interact with it and its settings. In Windows 11, to open the Security use the Start menu, display the **All apps** list and click the **Windows Security** listing:

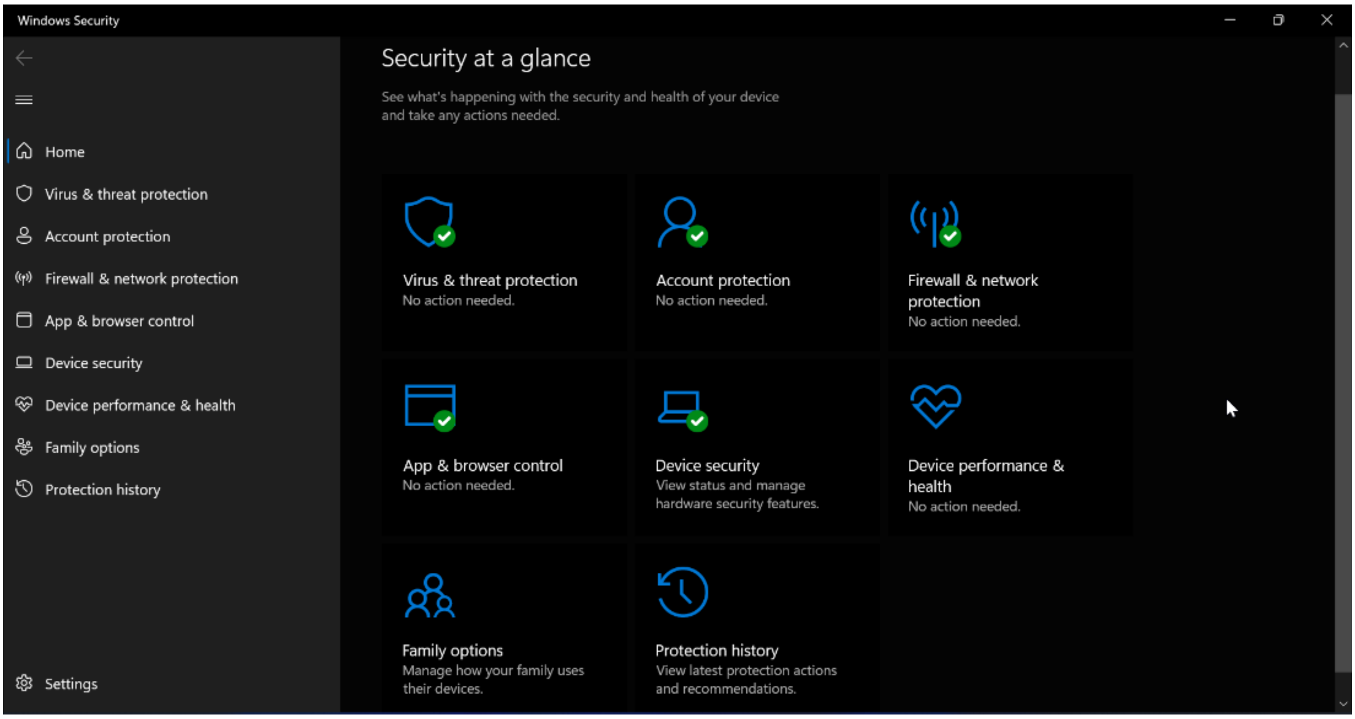


Alternatively, typing “**Windows Security”** into the search field and clicking on the **Windows Security** app will also work.



Overview of Windows Security

When Windows Security is opened, the following interface will be displayed:



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

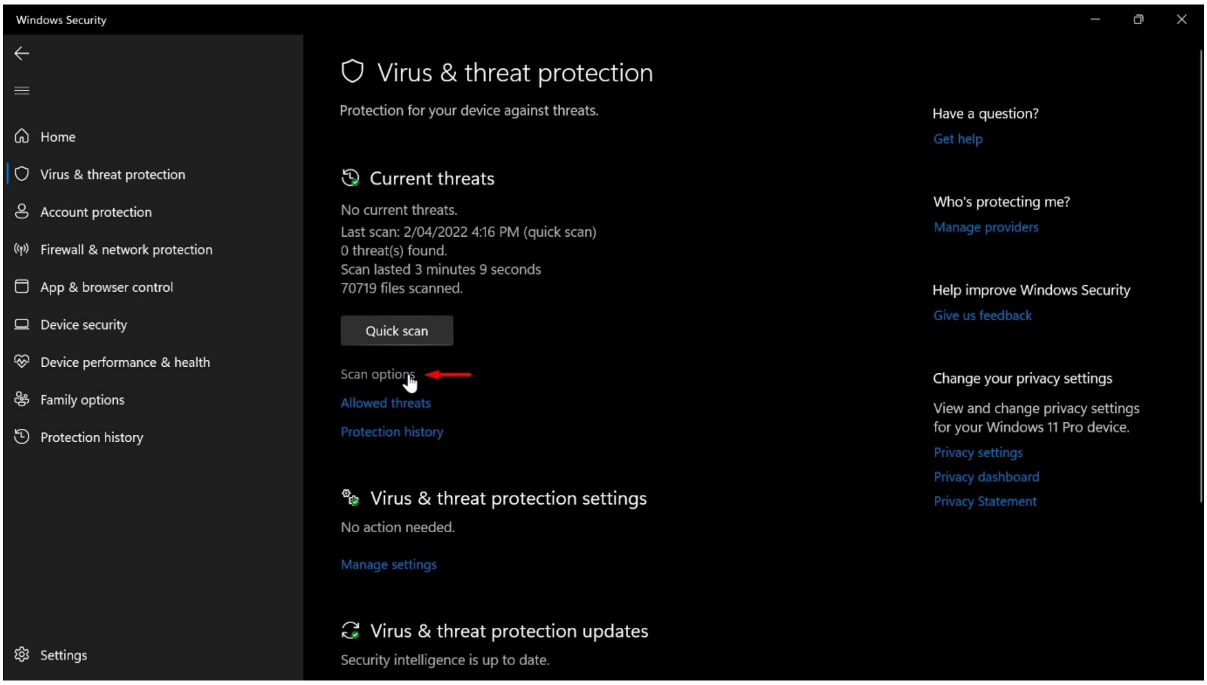
Protection history
View latest protection actions and recommendations.

The main portion of the interface is divided into several tabs, including Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, Family options, and Protection history.

Virus and Threat Protection

This option in Windows Security provides several options to scan for any possible threats on the device. It also displays the status, along with any current threats found. Lastly, it tells the user the last time the system was scanned, along with the number of files it scanned.

To view the various options to scan, click on **Scan options**:



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 2/04/2022 4:16 PM (quick scan)
0 threat(s) found.
Scan lasted 3 minutes 9 seconds
70719 files scanned.

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Have a question?

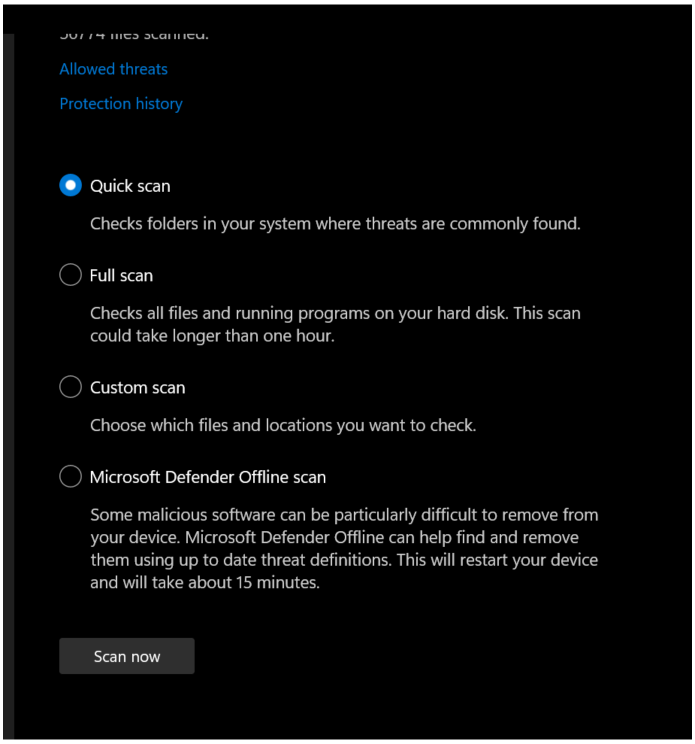
Who's protecting me?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 Pro device.

To look for threats, you can choose from **Quick scan**, **Full scan**, **Custom scan** or **Microsoft Defender Offline scan**.



● Quick scan

Checks folders in your system where threats are commonly found.

○ Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

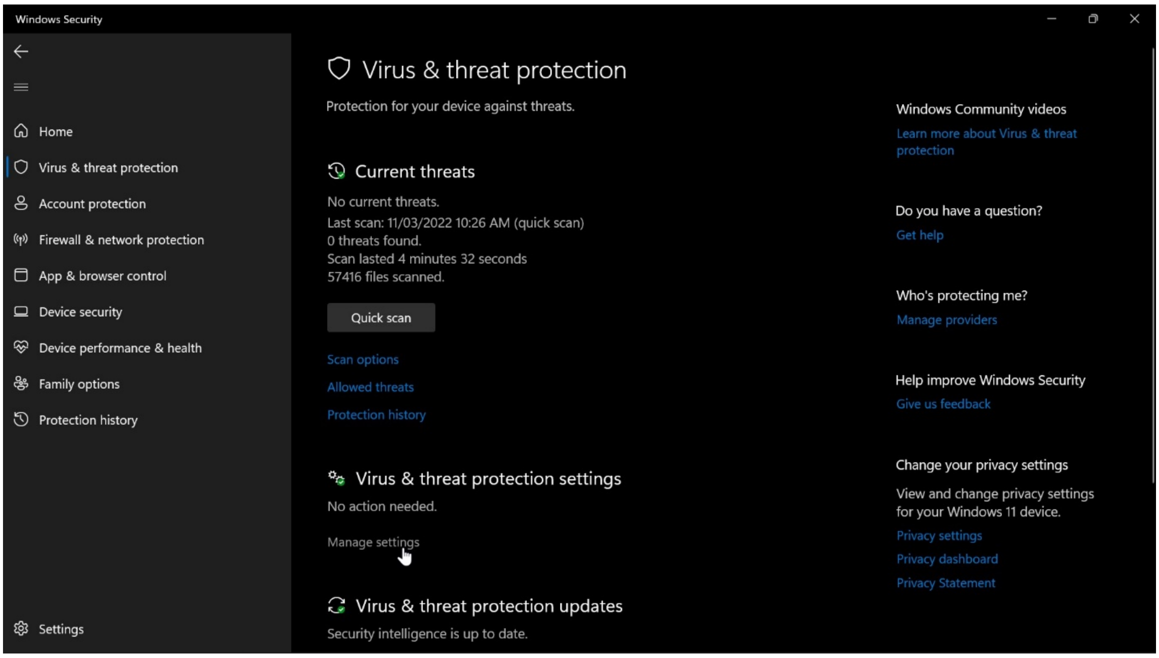
○ Custom scan

Choose which files and locations you want to check.

○ Microsoft Defender Offline scan

Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Offline can help find and remove them using up to date threat definitions. This will restart your device and will take about 15 minutes.

Virus & threat protection is turned on by default, however if a user wishes to turn off the protection, clicking on **Manage settings** link in the section **Virus & threat protection settings** aopens up an option selection.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 11/03/2022 10:26 AM (quick scan)
0 threats found.
Scan lasted 4 minutes 32 seconds
57416 files scanned.

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Windows Community videos

Do you have a question?

Who's protecting me?

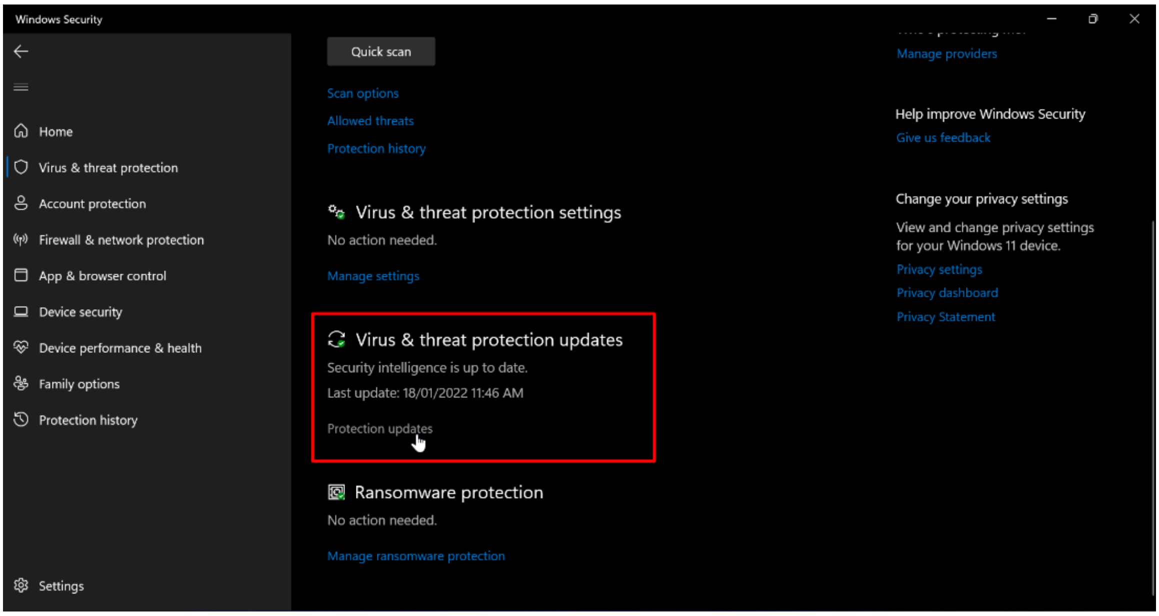
Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 device.

The **Virus & threat protection updates tab** displays detailed information about the computer's virus and spyware definitions.

Definitions are used to identify threats, so they need to be updated constantly to keep the computer protected. This process is automatic by default, but a user can start a manual update by clicking the **Protection Updates** button.



Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Last update: 18/01/2022 11:46 AM

Ransomware protection

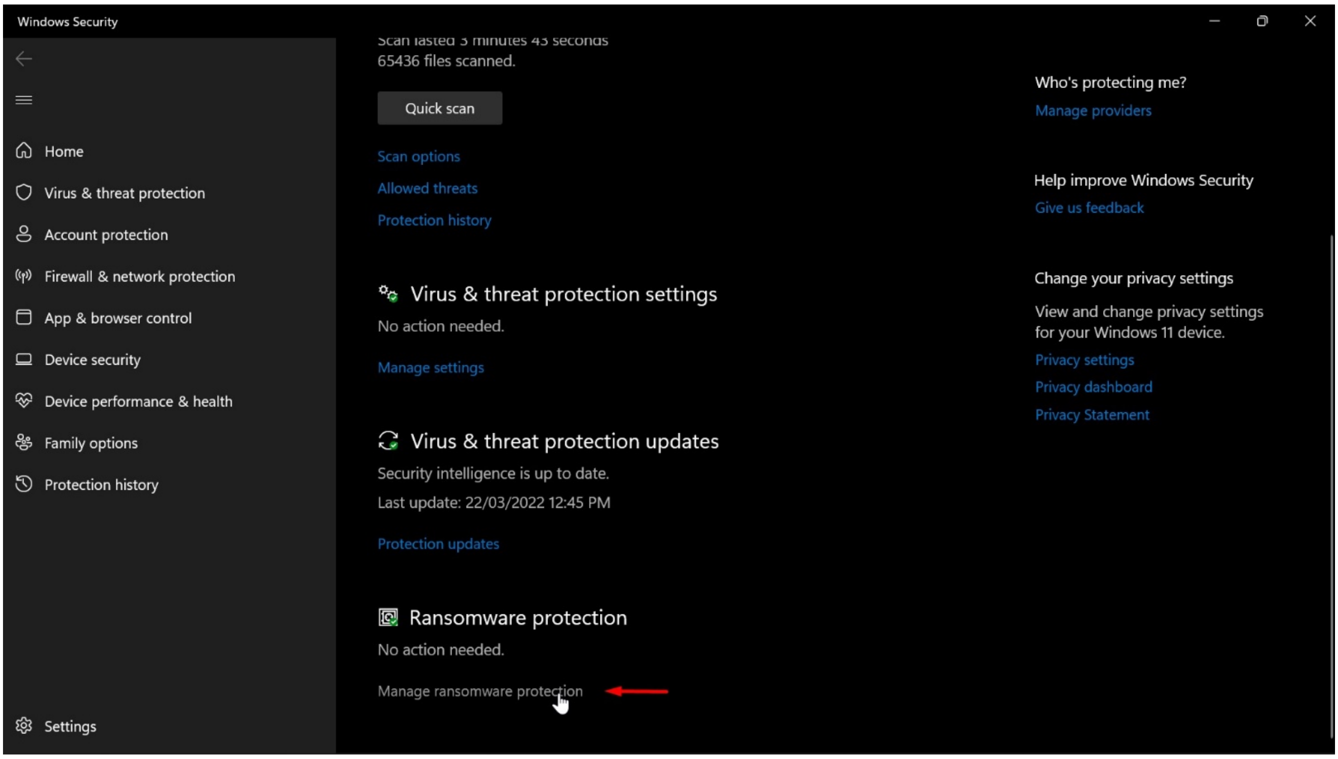
No action needed.

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 device.

The lower portion of this window will display **Ransomware protection**. To access settings, click on **Manage ransomware protection**:



Scan lasted 3 minutes 43 seconds
65436 files scanned.

Virus & threat protection settings
No action needed.

Virus & threat protection updates
Security intelligence is up to date.
Last update: 22/03/2022 12:45 PM

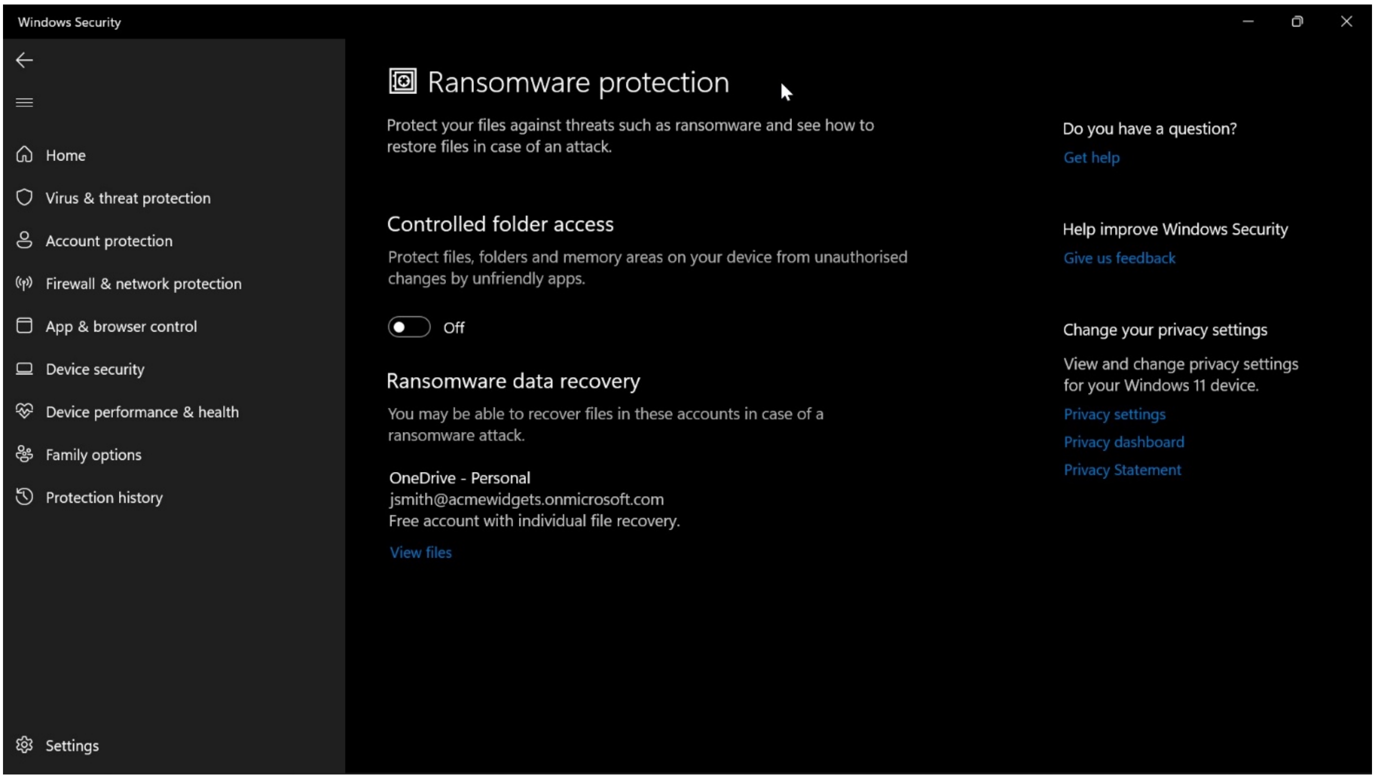
Ransomware protection
No action needed.

Who's protecting me?

Help improve Windows Security

Change your privacy settings
View and change privacy settings for your Windows 11 device.

Ransomware protection gives the user information about controlled folder access, ransomware data recovery and details about OneDrive.



Ransomware protection
Protect your files against threats such as ransomware and see how to restore files in case of an attack.

Controlled folder access
Protect files, folders and memory areas on your device from unauthorised changes by unfriendly apps.

○ Off

Ransomware data recovery
You may be able to recover files in these accounts in case of a ransomware attack.

OneDrive - Personal
jsmith@acmewidgets.onmicrosoft.com
Free account with individual file recovery.

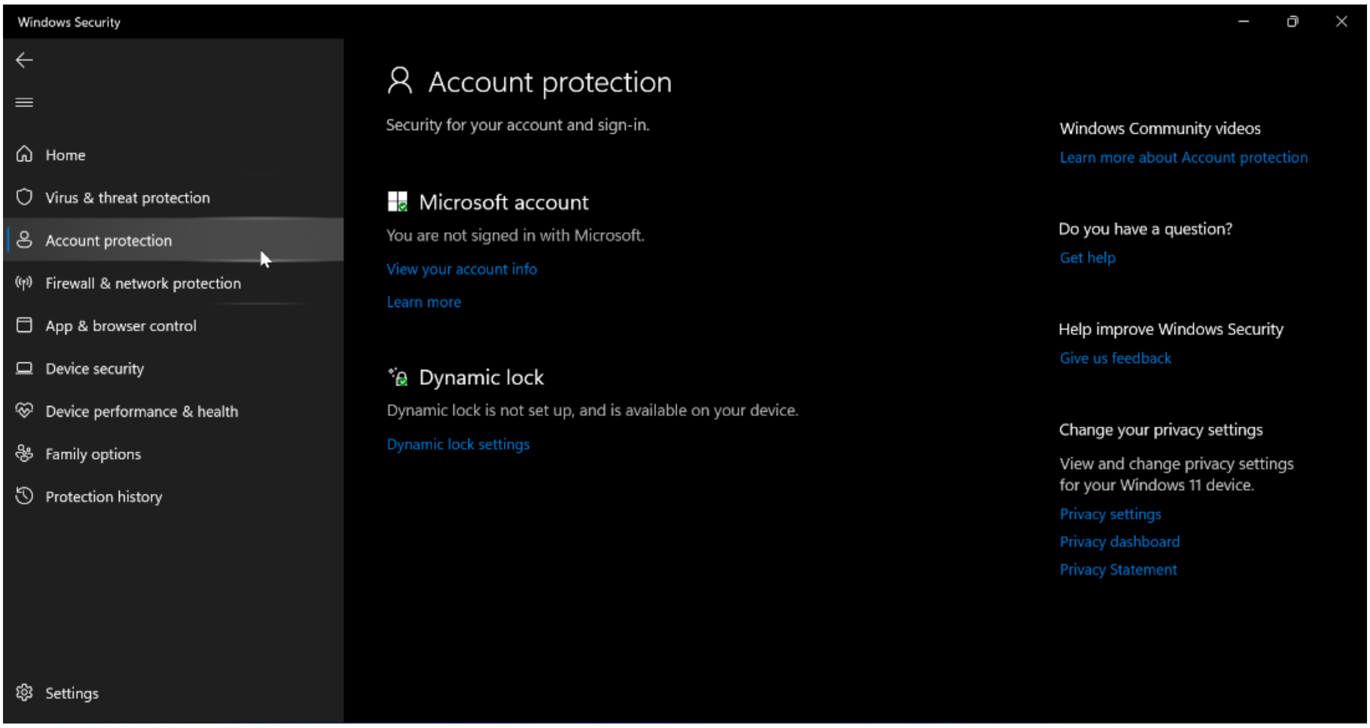
Do you have a question?

Help improve Windows Security

Change your privacy settings
View and change privacy settings for your Windows 11 device.

Account Protection

Clicking on **Account protection** will provide two main sub-categories – **Microsoft account** and **Dynamic lock**. Microsoft account allows a user to view their account information. Dynamic lock enables the devices to lock automatically if a user forgets to lock them. Whenever the signal strength of the Bluetooth paired with the device drops low, the Dynamic lock will spring into action.



Account protection

Security for your account and sign-in.

Microsoft account

You are not signed in with Microsoft.

View your account info

Learn more

Dynamic lock

Dynamic lock is not set up, and is available on your device.

Dynamic lock settings

Windows Community videos

Learn more about Account protection

Do you have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

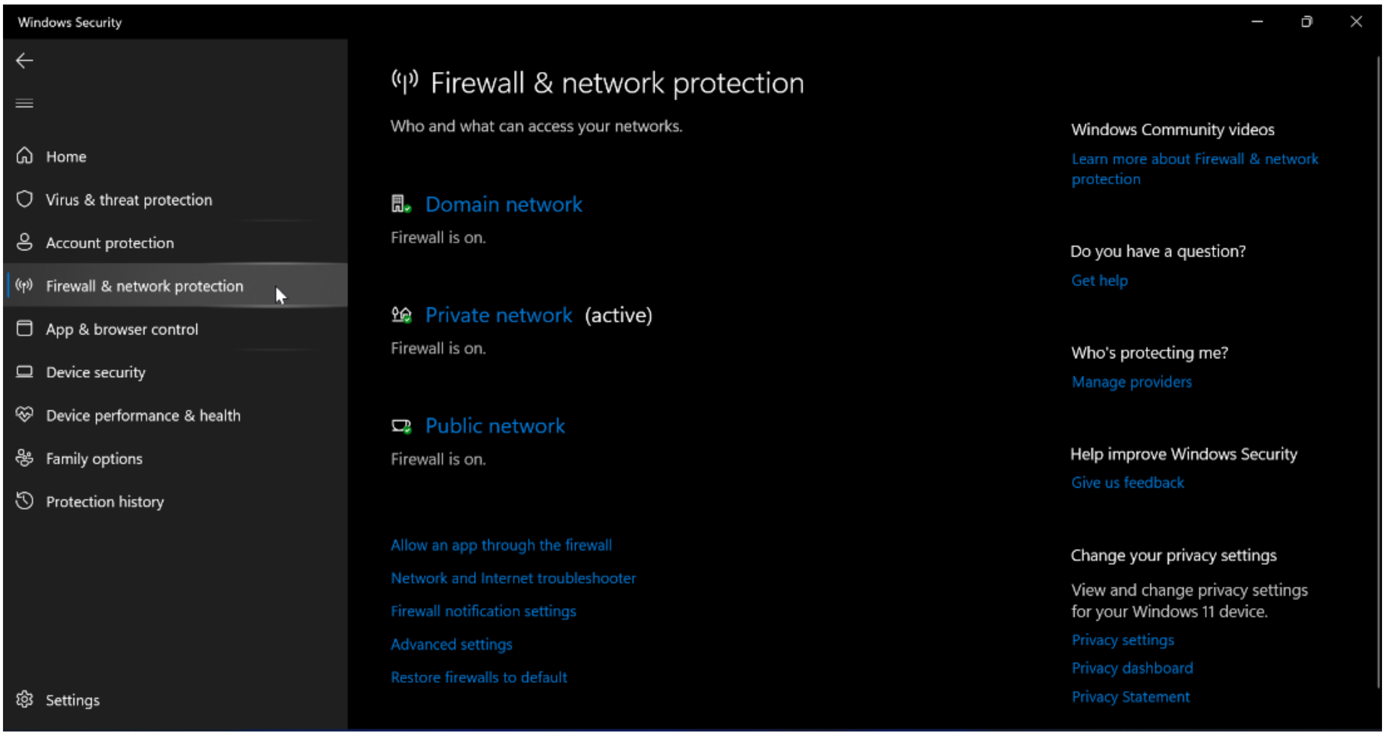
View and change privacy settings for your Windows 11 device.

Privacy settings

Privacy dashboard

Privacy Statement

Firewall & **network protection** has several options including Domain network, Private network and Public network. These options have access to — and give the user more information about — the firewall settings that includes the Windows Defender firewall.



Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network (active)

Firewall is on.

Public network

Firewall is on.

Allow an app through the firewall

Network and Internet troubleshooter

Firewall notification settings

Advanced settings

Restore firewalls to default

Windows Community videos

Learn more about Firewall & network protection

Do you have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 device.

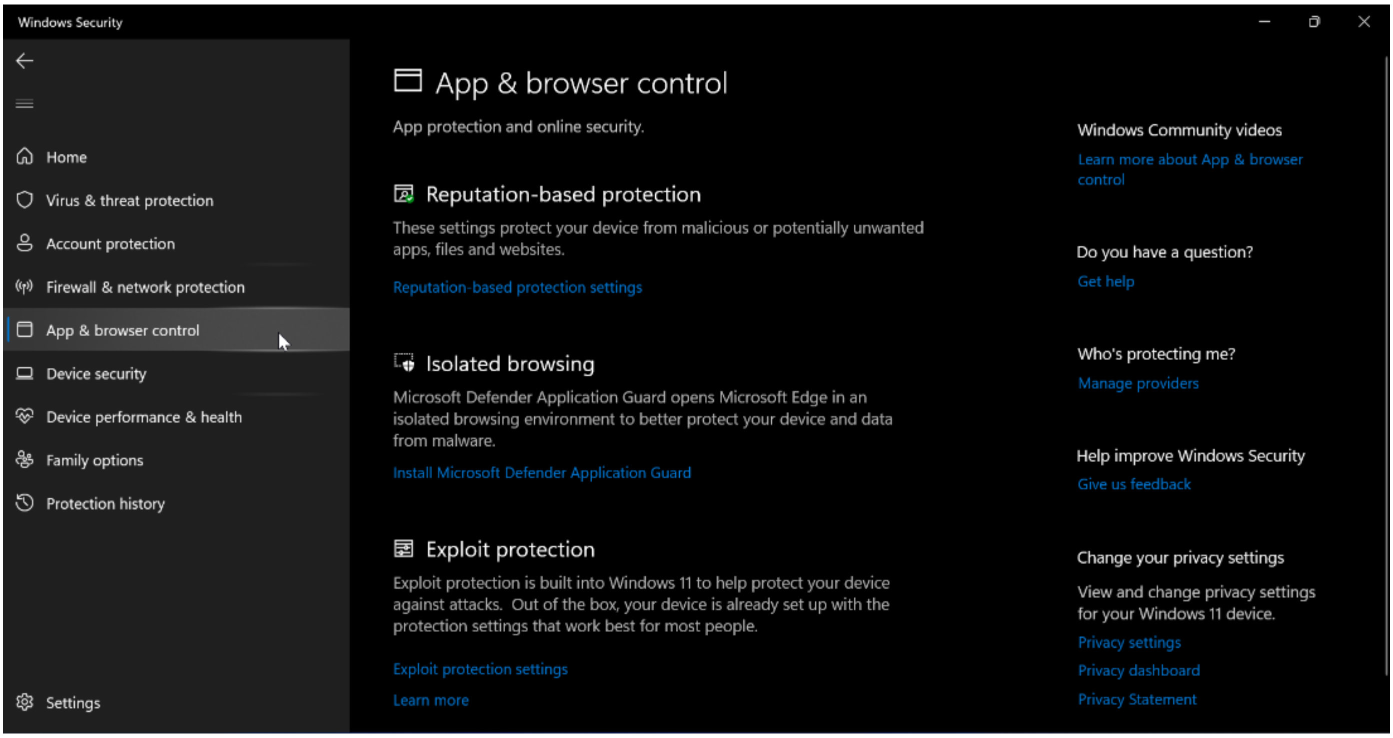
Privacy settings

Privacy dashboard

Privacy Statement

App and Browser Control

The **App and browser control** is another setting that protects the computer. Here, there are three options, including **Reputation-based protection**, **Isolated browsing**, and **Exploit protection**. While the Reputation-based protection shields a device from harmful apps, websites and files, the Isolated browsing setting will open the browser in an isolated environment to protect devices. Exploit protection is a built-in function that protects devices from malicious attacks.



App & browser control

App protection and online security.

Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files and websites.

Reputation-based protection settings

Isolated browsing

Microsoft Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.

Install Microsoft Defender Application Guard

Exploit protection

Exploit protection is built into Windows 11 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

Exploit protection settings

Learn more

Windows Community videos

Learn more about App & browser control

Do you have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 device.

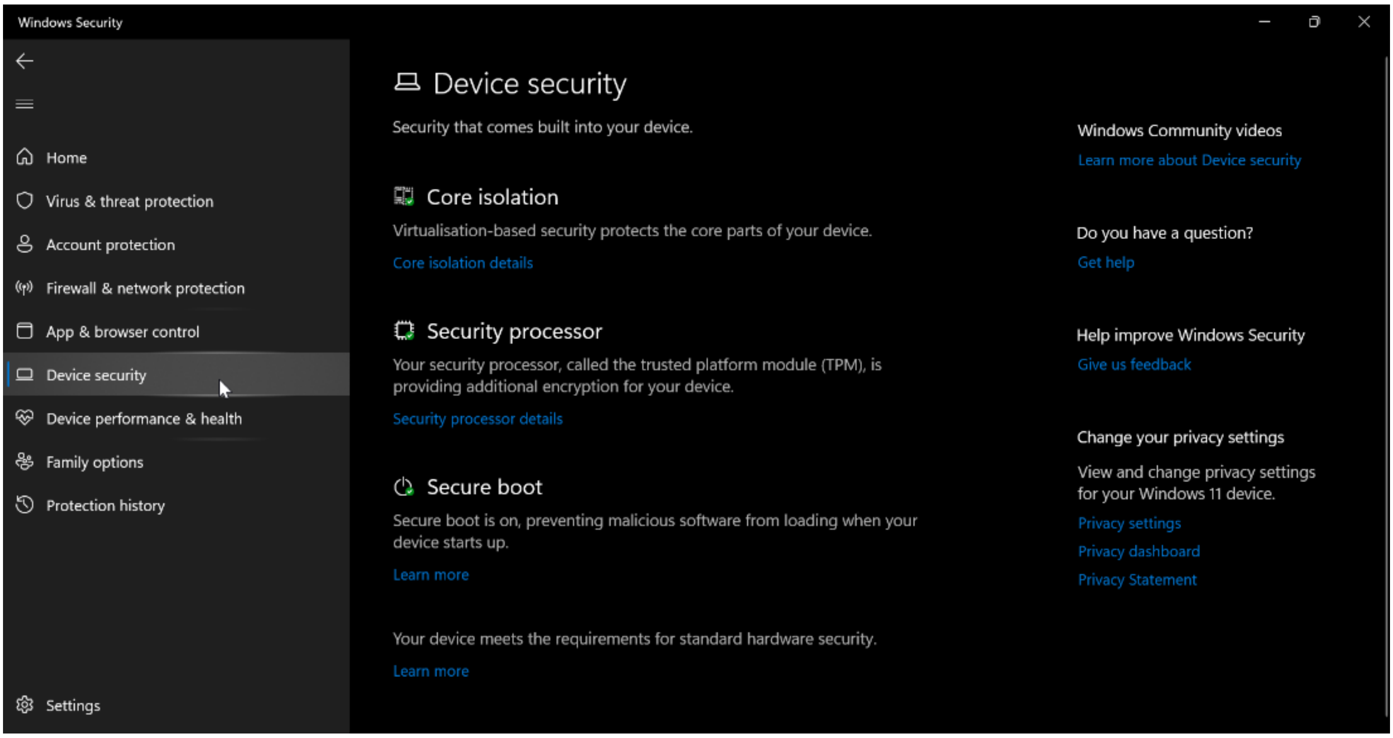
Privacy settings

Privacy dashboard

Privacy Statement

Device Security

Device security is a built-in setting that gives the user access to the device's security settings. It provides three options, including **Core isolation**, **Security processor**, and **Secure boot**. Core isolation is meant to protect the device's core parts and Security processor provides additional encryption. The Secure boot prevents harmful software from loading automatically when the computer is turned on.



Device security

Security that comes built into your device.

Core isolation

Virtualisation-based security protects the core parts of your device.

Core isolation details

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

Security processor details

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

Learn more

Your device meets the requirements for standard hardware security.

Learn more

Windows Community videos

Learn more about Device security

Do you have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 device.

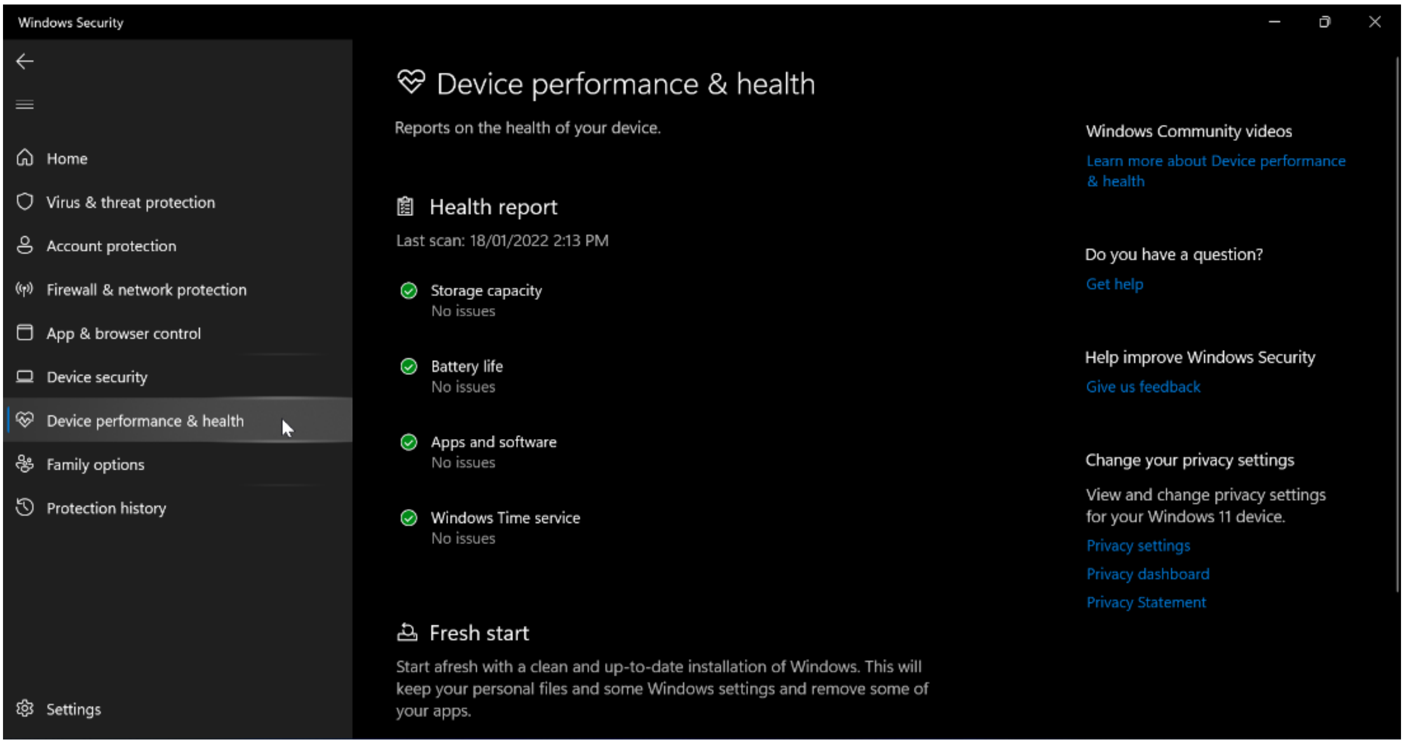
Privacy settings

Privacy dashboard

Privacy Statement

Device Performance & Health

Device performance & health provides more information about the storage space, drivers and general issues related to updates. It offers two options, including **Health report** and **Fresh start**. Health report displays several categories that deliver reports on Storage capacity, Battery life, Apps and software, and Windows Time service. If everything is functioning normally, a user will see a green check mark next to all these categories. Fresh start, located at the bottom, gives the user the opportunity to re-install Windows and start afresh.



Device performance & health

Reports on the health of your device.

Health report

Last scan: 18/01/2022 2:13 PM

✓ Storage capacity
No issues

✓ Battery life
No issues

✓ Apps and software
No issues

✓ Windows Time service
No issues

Fresh start

Start afresh with a clean and up-to-date installation of Windows. This will keep your personal files and some Windows settings and remove some of your apps.

Windows Community videos

Learn more about Device performance & health

Do you have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 device.

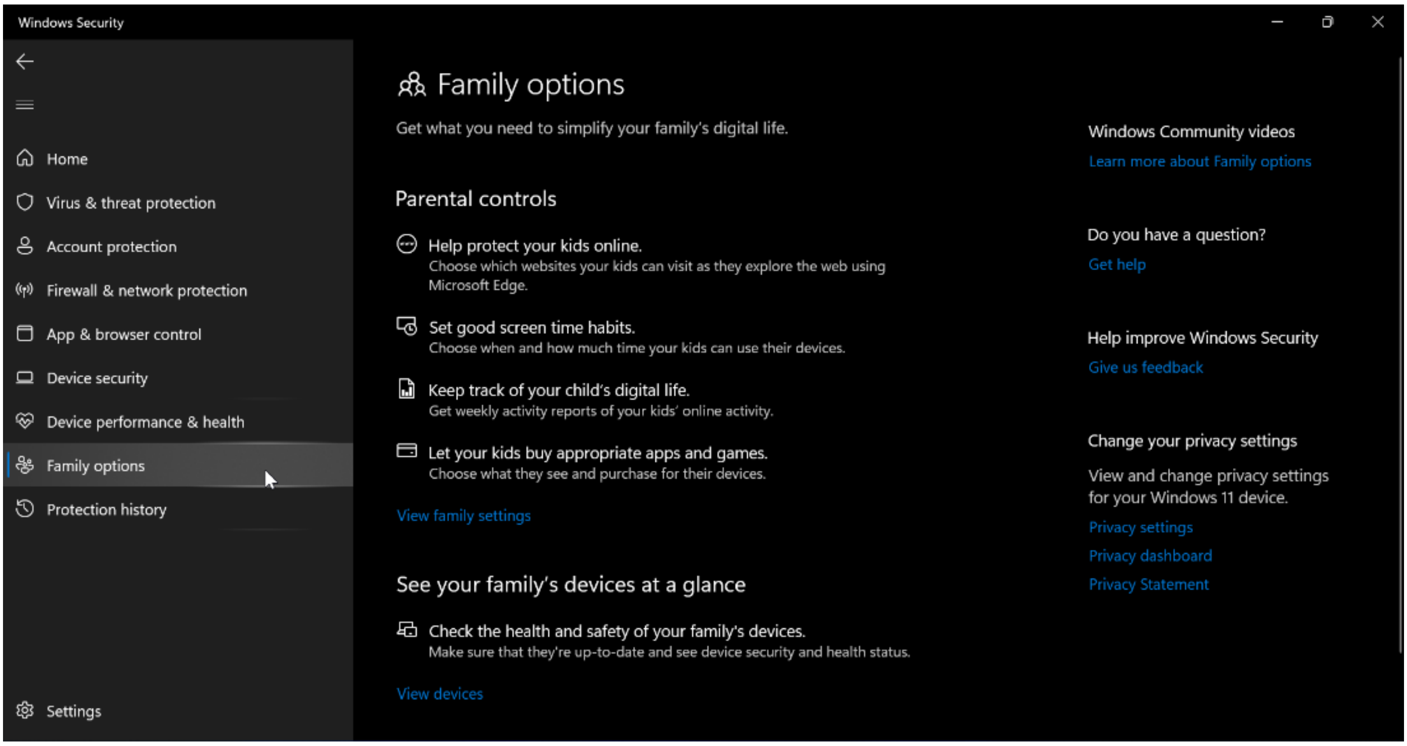
Privacy settings

Privacy dashboard

Privacy Statement

Family Options

Finally, **Family options** offers options for parents to control the browsing habits of their children and keep them safe. It provides two options, including **Parental controls** and **See your family's devices at a glance**. Here, parents can choose what websites their children may potentially visit. In addition, a specific screen time can be set for children, and their digital activity — including their games and apps purchases — can be tracked.



Family options

Get what you need to simplify your family's digital life.

Parental controls

Help protect your kids online.
Choose which websites your kids can visit as they explore the web using Microsoft Edge.

Set good screen time habits.
Choose when and how much time your kids can use their devices.

Keep track of your child's digital life.
Get weekly activity reports of your kids' online activity.

Let your kids buy appropriate apps and games.
Choose what they see and purchase for their devices.

View family settings

See your family's devices at a glance

Check the health and safety of your family's devices.
Make sure that they're up-to-date and see device security and health status.

View devices

Windows Community videos
Learn more about Family options

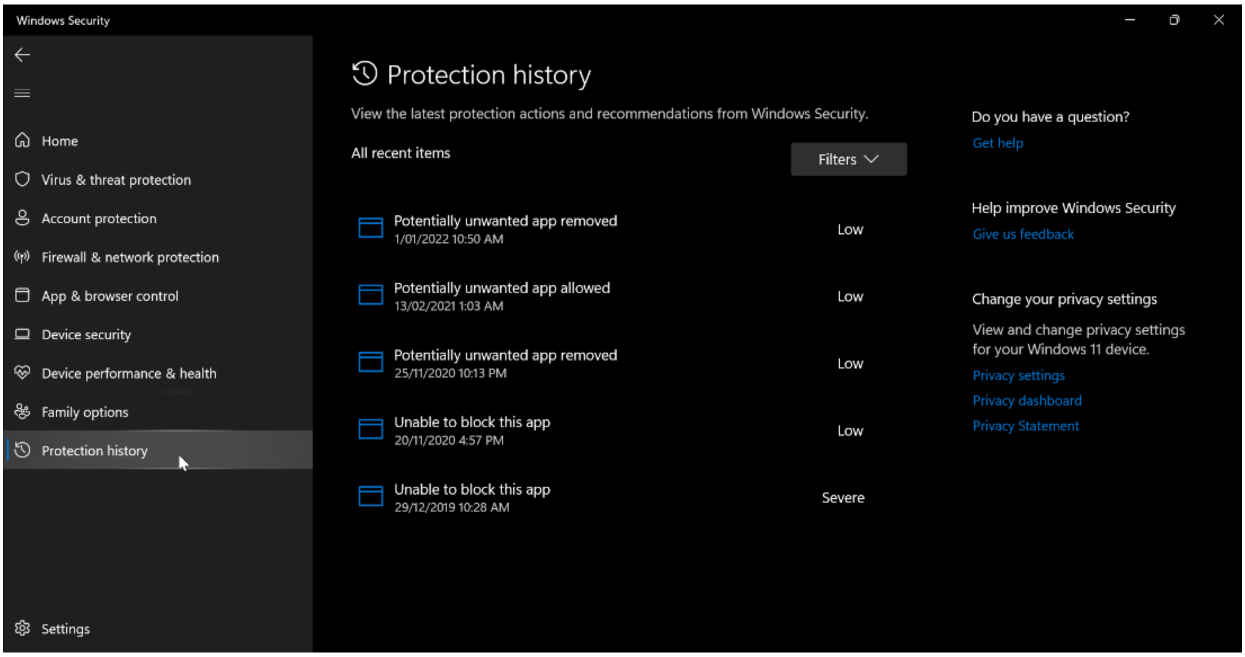
Do you have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 11 device.
Privacy settings
Privacy dashboard
Privacy Statement

Protection History

The **Protection history** tab shows the latest protection actions and recommendations from Windows Security. It shows potentially harmful threats to a computer, as well as the severity of the threats:



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Potentially unwanted app removed
1/01/2022 10:50 AM
Low

Potentially unwanted app allowed
13/02/2021 1:03 AM
Low

Potentially unwanted app removed
25/11/2020 10:13 PM
Low

Unable to block this app
20/11/2020 4:57 PM
Low

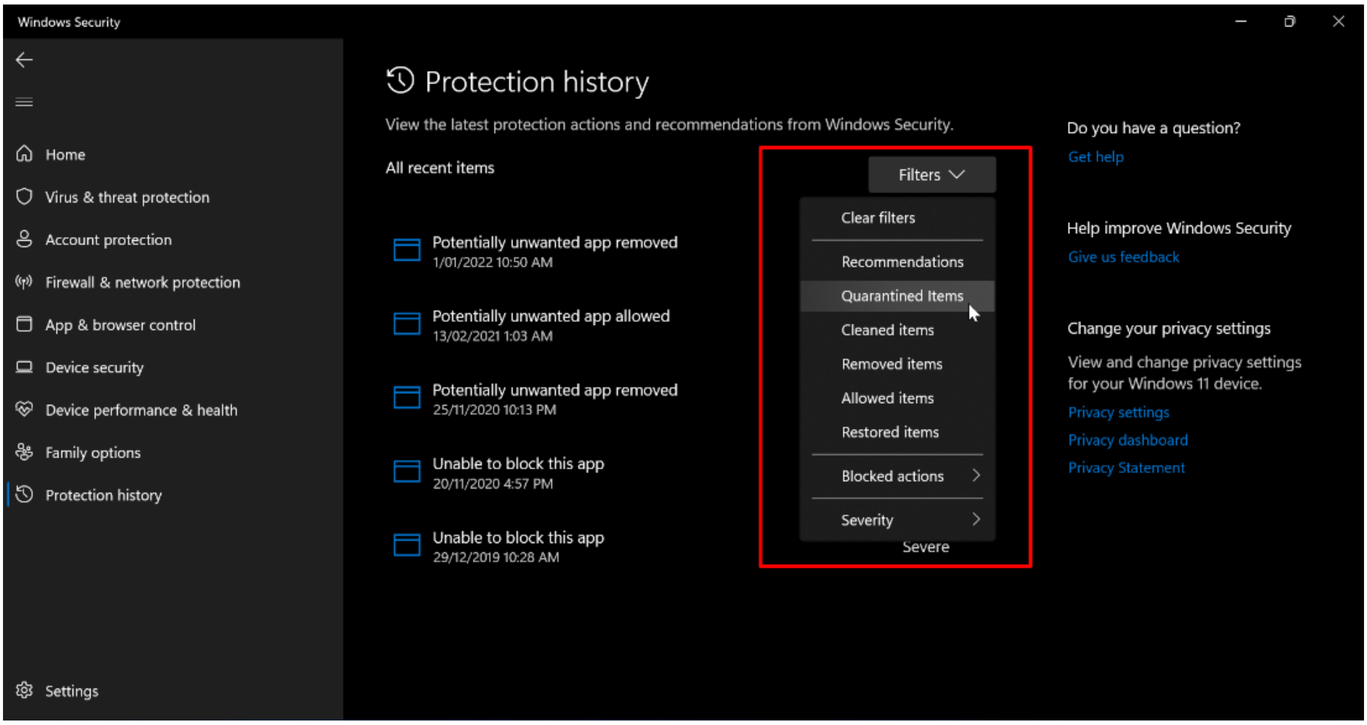
Unable to block this app
29/12/2019 10:28 AM
Severe

Do you have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 11 device.
Privacy settings
Privacy dashboard
Privacy Statement

Clicking the **Filters** button allows the user to select the items they want to show:



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Potentially unwanted app removed
1/01/2022 10:50 AM

Potentially unwanted app allowed
13/02/2021 1:03 AM

Potentially unwanted app removed
25/11/2020 10:13 PM

Unable to block this app
20/11/2020 4:57 PM

Unable to block this app
29/12/2019 10:28 AM

Severe

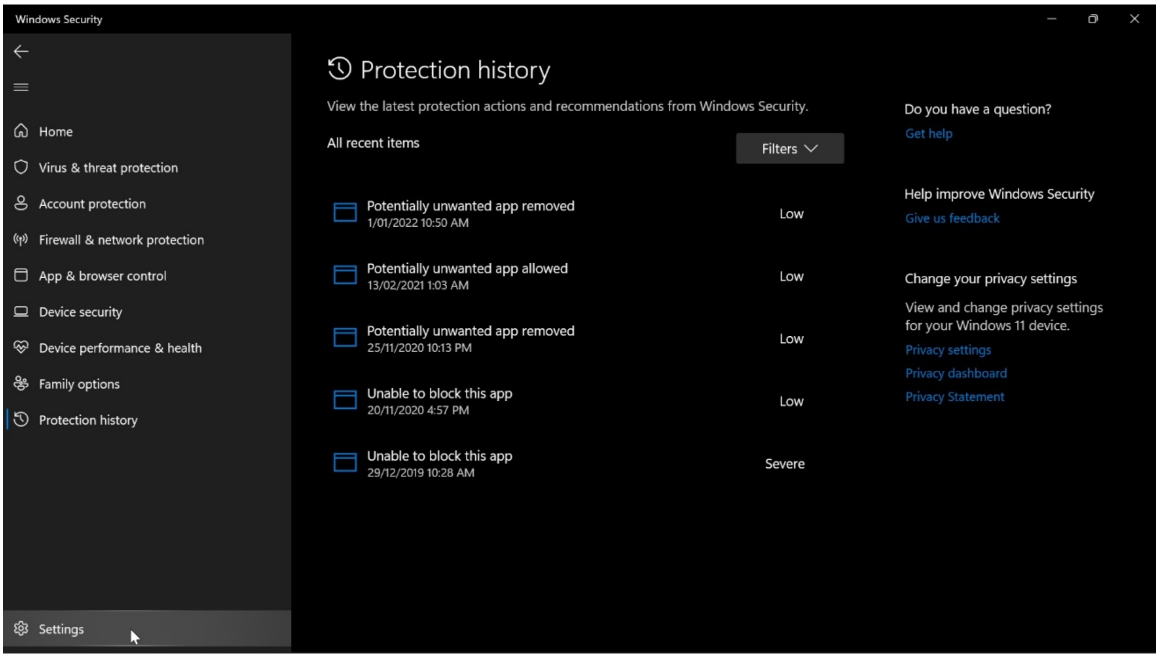
Do you have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 device.

Clear filters lets a user clear all filters and start afresh.
Recommendations provides suggestions that may work for a user.
Quarantined items will display any actions that were prevented from being executed but are stored in a secure location.
Cleaned items will display items that have been cleaned to protect the device.
Removed items will display items that were deleted.
Allowed items will list any items that a user have chosen to run despite being flagged as a possible issue.
Restored items will list any items a user previously deleted and restored.
Near the lower left-hand corner of the Windows Security window, a user will also see the **Settings** button:



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Potentially unwanted app removed
1/01/2022 10:50 AM
Low

Potentially unwanted app allowed
13/02/2021 1:03 AM
Low

Potentially unwanted app removed
25/11/2020 10:13 PM
Low

Unable to block this app
20/11/2020 4:57 PM
Low

Unable to block this app
29/12/2019 10:28 AM
Severe

Do you have a question?

Help improve Windows Security

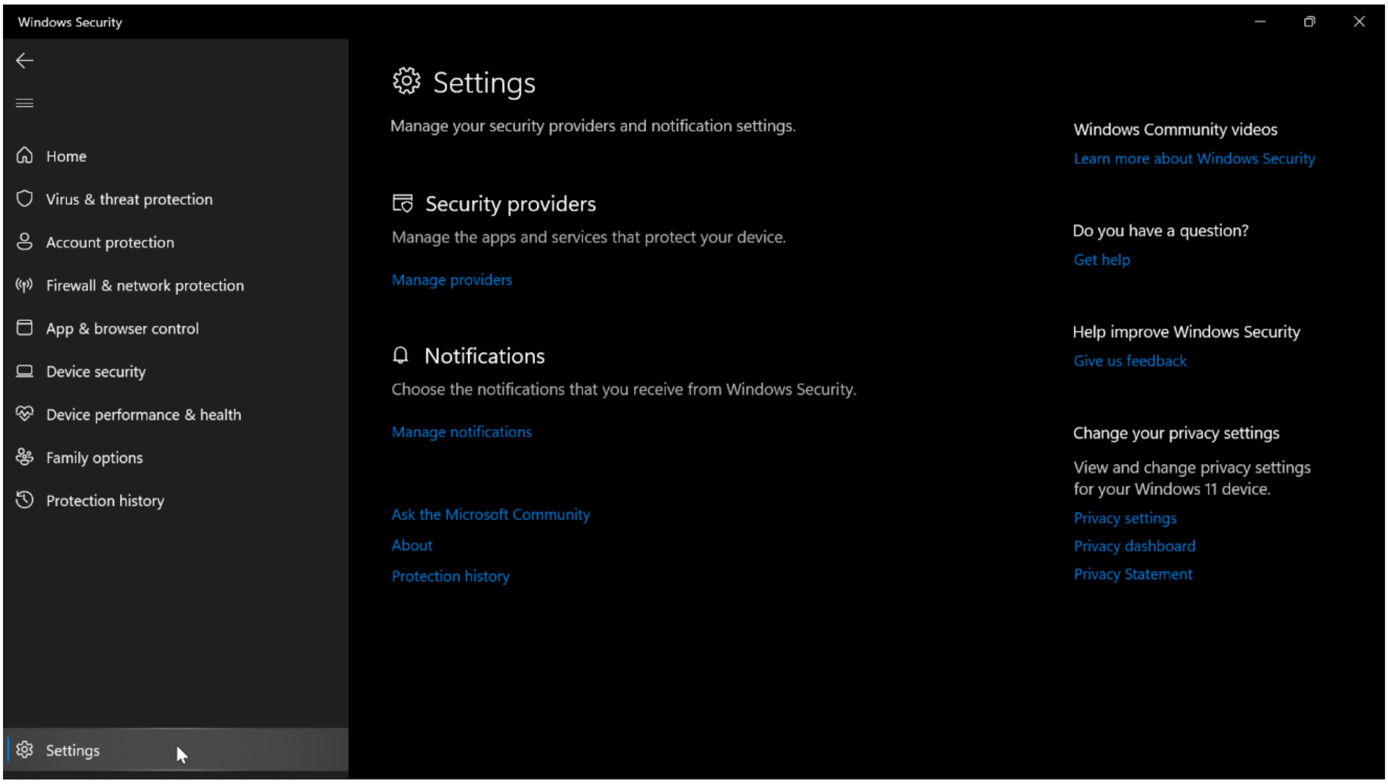
Change your privacy settings

View and change privacy settings for your Windows 11 device.

Changing Windows Security Settings

In the **Windows Security** settings category, a user will find all sorts of settings to control how the program works.

Each section in this sub-category are listed below:



Settings

Manage your security providers and notification settings.

Security providers

Manage the apps and services that protect your device.

Manage providers

Notifications

Choose the notifications that you receive from Windows Security.

Manage notifications

Ask the Microsoft Community

About

Protection history

Windows Community videos

Learn more about Windows Security

Do you have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

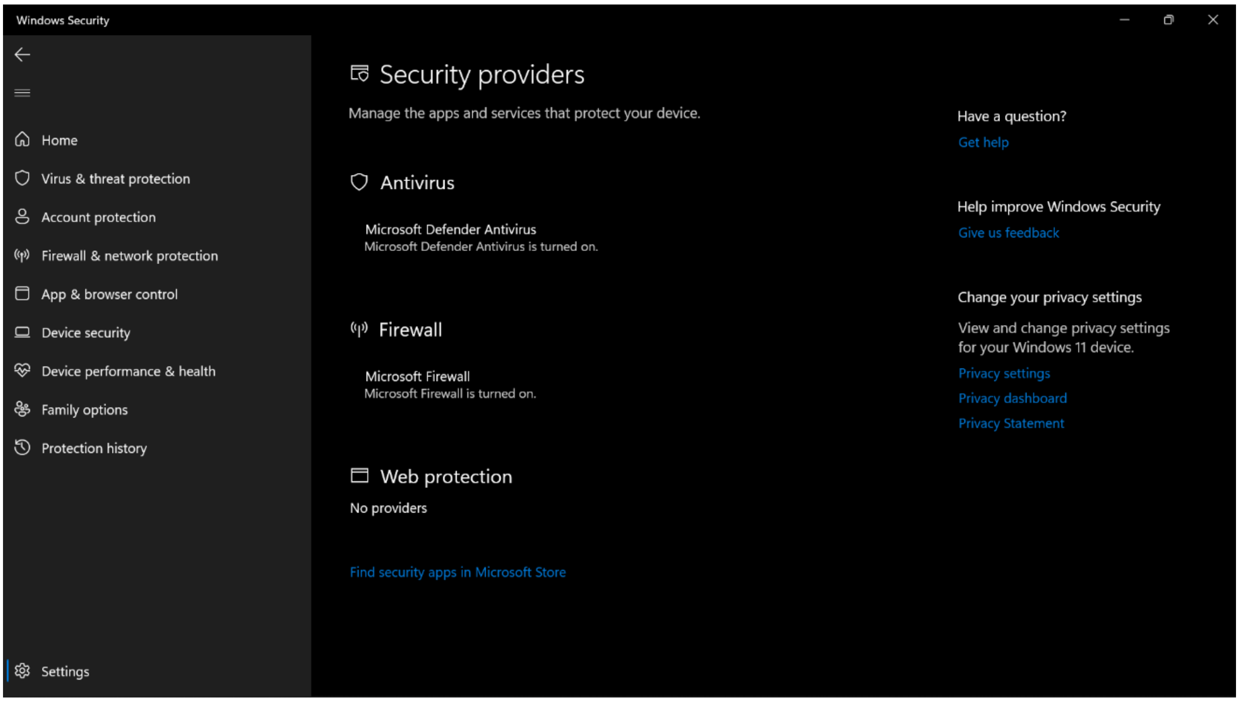
View and change privacy settings for your Windows 11 device.

Privacy settings

Privacy dashboard

Privacy Statement

In the centre, are two options — **Security providers** and **Notifications**. Security providers will give a user information on services and apps tasked with protecting their device. For example, clicking on **Security providers** will show a user providers offering antivirus, firewall, and web protection.



Security providers

Manage the apps and services that protect your device.

Antivirus

Microsoft Defender Antivirus
Microsoft Defender Antivirus is turned on.

Firewall

Microsoft Firewall
Microsoft Firewall is turned on.

Web protection

No providers

Find security apps in Microsoft Store

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

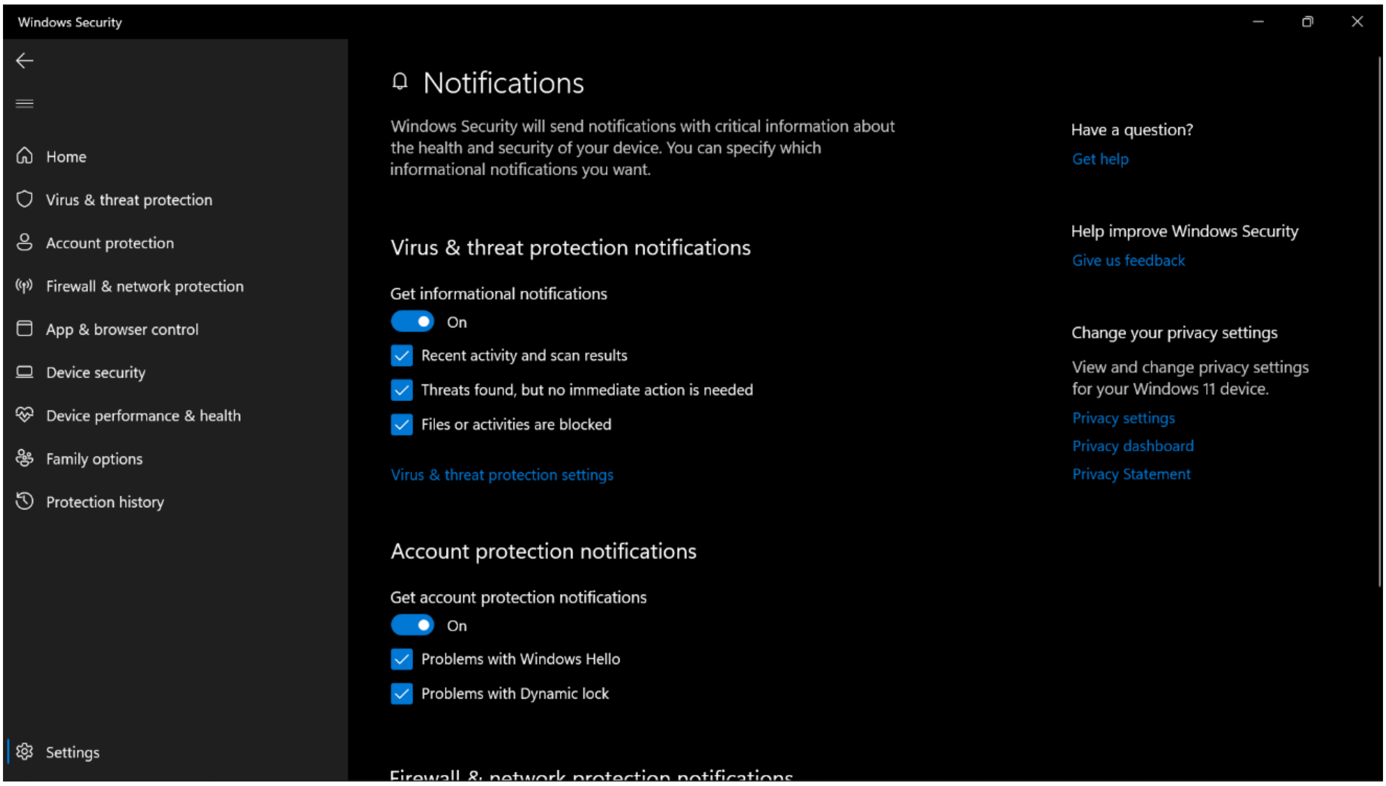
View and change privacy settings for your Windows 11 device.

Privacy settings

Privacy dashboard

Privacy Statement

Notifications settings allow a user to customise the type of notifications that **Windows Security** sends.



Windows Security

Notifications

Windows Security will send notifications with critical information about the health and security of your device. You can specify which informational notifications you want.

Virus & threat protection notifications

Get informational notifications

On

☑ Recent activity and scan results

☑ Threats found, but no immediate action is needed

☑ Files or activities are blocked

Virus & threat protection settings

Account protection notifications

Get account protection notifications

On

☑ Problems with Windows Hello

☑ Problems with Dynamic lock

Firewall & network protection notifications

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 device.

Privacy settings

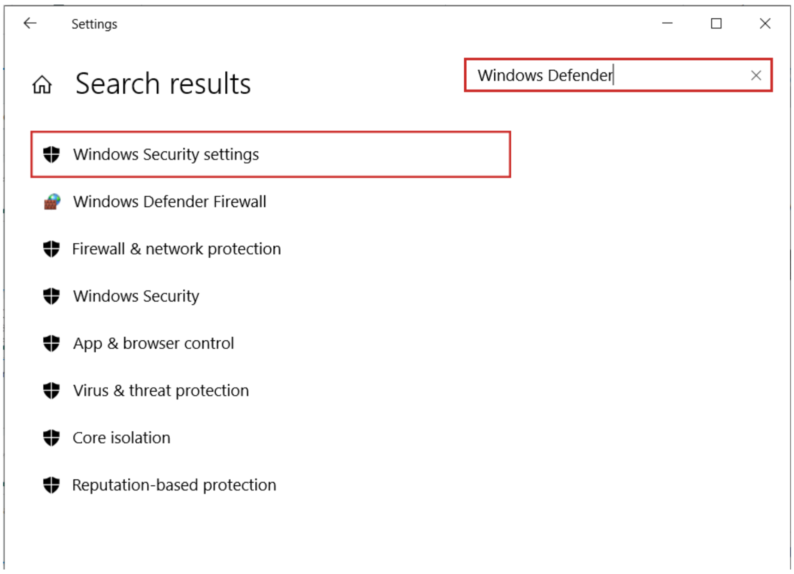
Privacy dashboard

Privacy Statement

Windows 10 – Windows Defender

To use Windows Defender in Windows 10 you go to the ‘**Start**’ menu and click on ‘**Settings**’.

On the next window you type in ‘**Windows Defender**’ in the ‘**Search Field**’.



Settings

Search results

Windows Defender

Windows Security settings

Windows Defender Firewall

Firewall & network protection

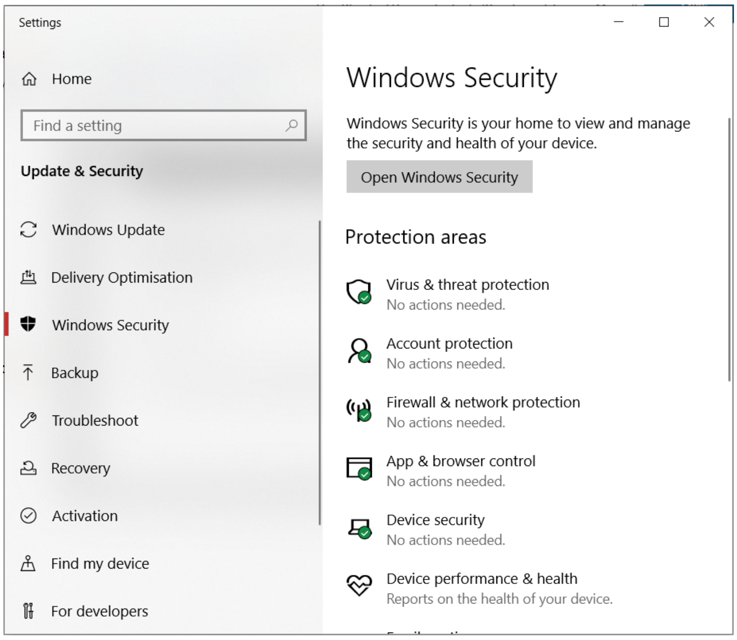
Windows Security

App & browser control

Virus & threat protection

Core isolation

Reputation-based protection



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

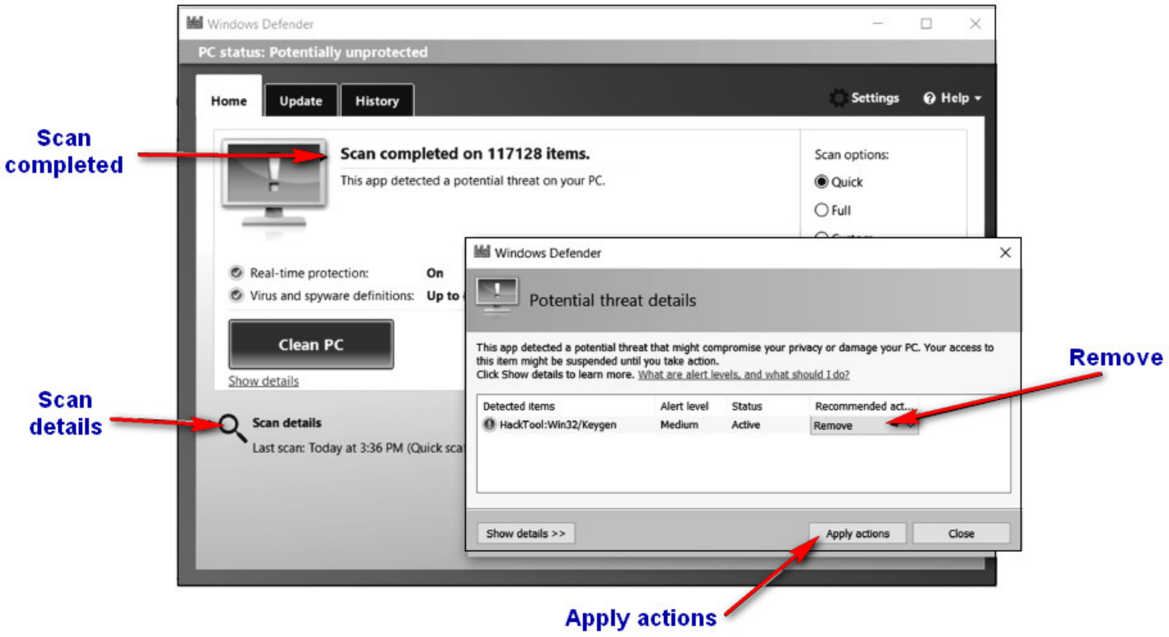
This opens the window above in which Windows Defender provides an overview of the status of several functions or tasks that it is doing.

If during one of its scheduled scans of the computer identifies a virus or malware it provides a report and isolates the suspected file or files.

If there are no viruses detected the user will get a message letting them know their computer is secure.

A user can remove the identified virus by following the prompts:

1. Wait until the scan is complete.
2. Click on ‘**Scan Details**’ and the next window would show the user what virus was found and how to remove it.
3. Clicking ’**Remove**’ and then click on ‘**Apply Actions**’.



PC status: Potentially unprotected

Scan completed on 117128 items.

This app detected a potential threat on your PC.

Scan options:
● Quick
○ Full

Real-time protection: On
Virus and spyware definitions: Up to

Scan details
Last scan: Today at 3:36 PM (Quick sca

Potential threat details

This app detected a potential threat that might compromise your privacy or damage your PC. Your access to this item might be suspended until you take action.
Click Show details to learn more. What are alert levels, and what should I do?

Detected items	Alert level	Status	Recommended act...
HackTool:Win32/Keygen	Medium	Active	Remove

Scan completed

Scan details

Remove

Apply actions

Recovery Plan

If it is not possible to clean the virus from the computer's system, tit is possible to revert to the backup files.

The reason an organisation does backups is if in the event of a system failure, where data is lost the data can be restored to the system from the backup store.

If backup files were to be used to restore data, then these must be scanned for viruses prior to reinstalling.

The amount of permanent data loss will be related to the timing of the last virus clean backup. Explanation: If the very last backup was a full backup then the data permanently lost will be those files that changed after the full back up was done. If the last backup was an incremental backup, again the data permanently lost would be those files that were changed since the last backup. However, to perform a proper recovery with incremental backups, you must go back to the last full backup that was performed and restore all the files on it first. Then restore the first incremental backup made since that full backup, then the next one and so on, until the most recently made incremental backup has been restored.

Organisations should have a data recovery plan. This plan would include the necessary steps involved to restore a computer system. Any person working in IT should be aware of their role and responsibilities in any recovery procedures.