Exercise 1 - Scanning for Malware.

Windows Defender is an anti-malware program that comes preinstalled on Windows 11. In previous Windows editions, this antimalware was a distinct application that had to be downloaded and installed.

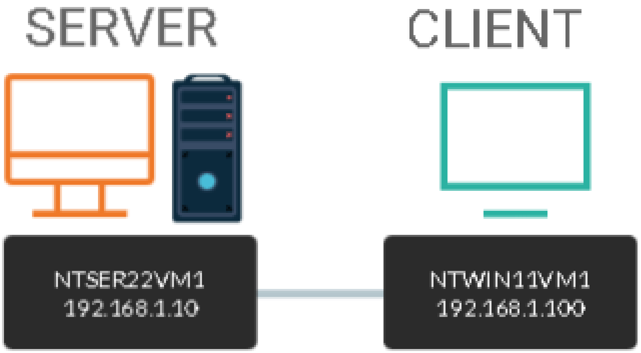
Windows Defender includes firewall protection, device performance monitoring, and a smart screen for Windows apps and Microsoft Edge browser protection

When necessary, the Windows Malicious Software Removal Tool (MSRT) can be downloaded. This program examines your computer for suspected malware, removes risks, and undoes any changes performed by the undesirable software. As part of Windows Update, MSRT is issued once a month.

In this exercise,

1. Install and run the MSRT from the intranet.

Topology



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTWIN11VM1 = Windows 11 – Domain Member

Prerequisite

- *VMware Workstation 16 Pro*
  - When making this tutorial, we used the "Windows Server 2019" VM Template and "Windows 10 & later" VM Template. Since VMware didn't have the updated templates.
- *Microsoft Windows Server 2022*
- *Microsoft Windows 11*

Task 1: Turn off Real-time Protection and Modify Scan Exclusion.

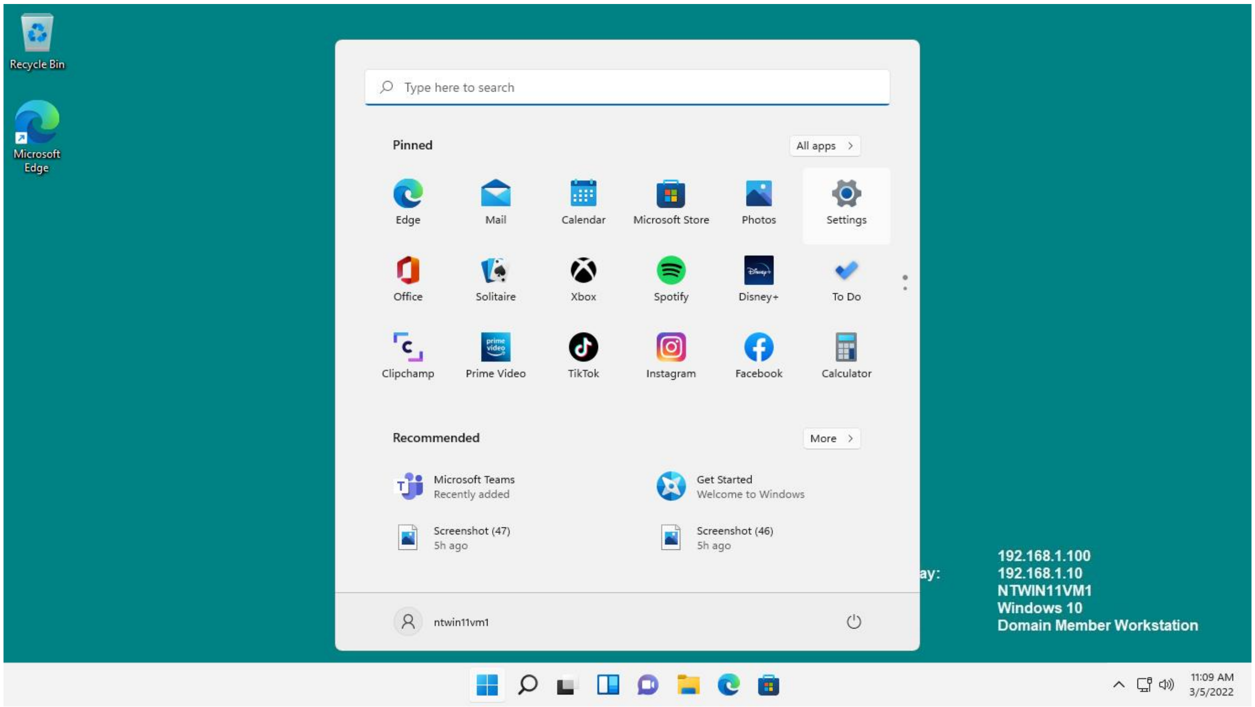
Windows Defender works in real time to prevent malware from reproducing infected files, which can cause system slowdown and performance issues. Windows Defender is a service that runs in the background.

Now let’s. facilitate the copying of sample malware to a Windows 11 device, briefly disable real-time protection. In a subsequent action, you'll change the scan exclusion settings to allow Windows Defender to scan particular directories.

Step 1:

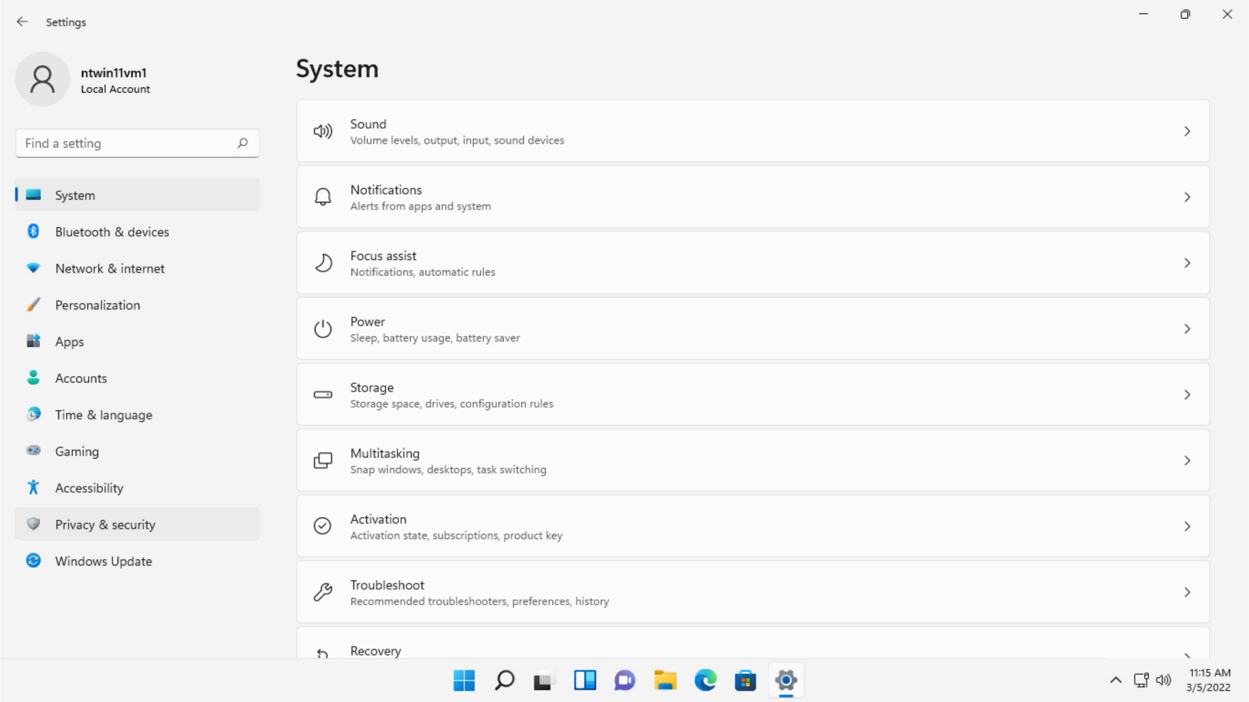
Ensure you have powered on the required devices defined in the introduction and connect to **NTWIN11VM1**.

Click **Start** and select **Settings**.



Step 2:

On **Windows Settings**, click **Privacy & Security.**



System

Sound
Volume levels, output, input, sound devices

Notifications
Alerts from apps and system

Focus assist
Notifications, automatic rules

Power
Sleep, battery usage, battery saver

Storage
Storage space, drives, configuration rules

Multitasking
Snap windows, desktops, task switching

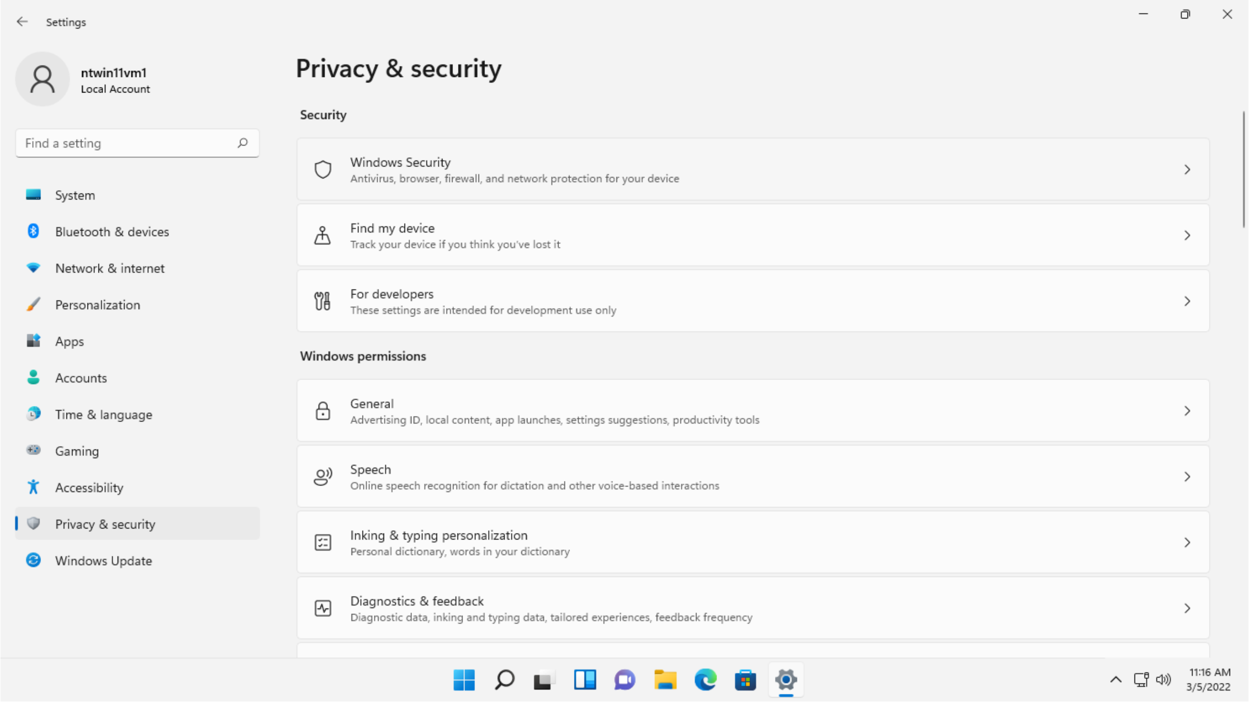
Activation
Activation state, subscriptions, product key

Troubleshoot
Recommended troubleshooters, preferences, history

Recovery

Step 3:

Under the **Privacy & Security** section, click **Windows Security** on the left navigation pane



Privacy & security

Security

Windows Security
Antivirus, browser, firewall, and network protection for your device

Find my device
Track your device if you think you've lost it

For developers
These settings are intended for development use only

Windows permissions

General
Advertising ID, local content, app launches, settings suggestions, productivity tools

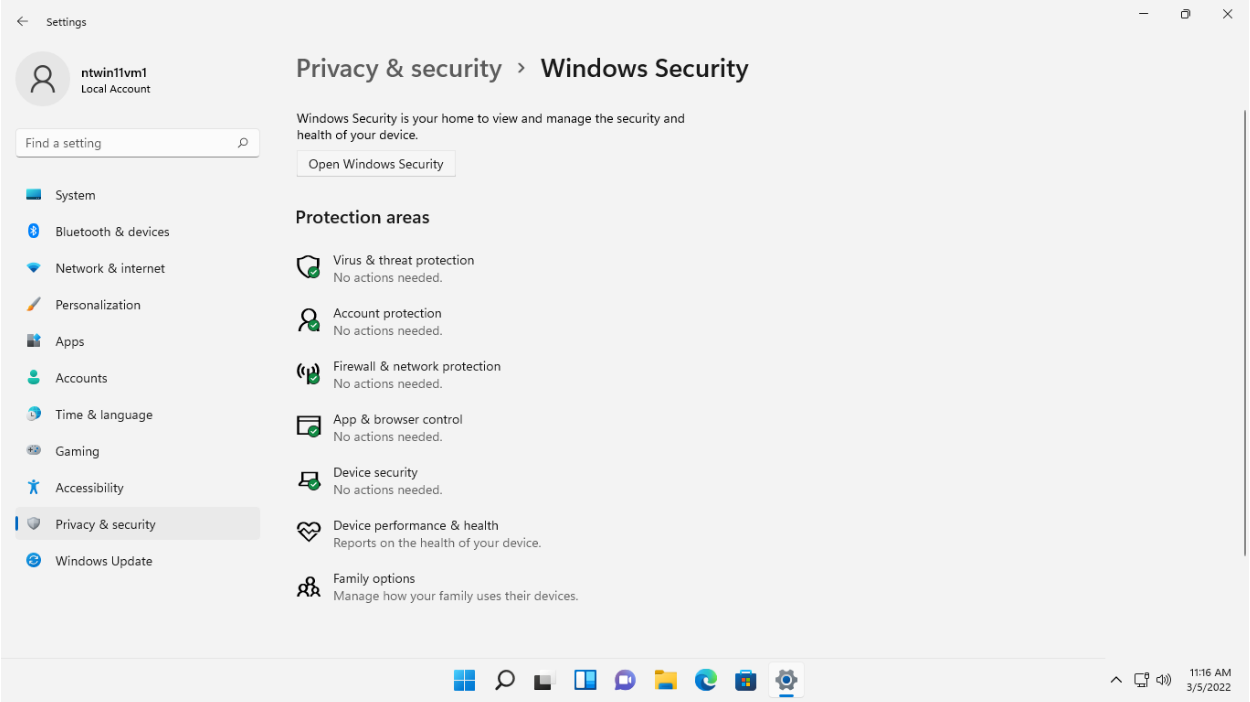
Speech
Online speech recognition for dictation and other voice-based interactions

Inking & typing personalization
Personal dictionary, words in your dictionary

Diagnostics & feedback
Diagnostic data, inking and typing data, tailored experiences, feedback frequency

Step 4:

On the **Windows Security** page, click the **Open Windows Security** button.



Settings

ntwin11vm1
Local Account

Find a setting

- System
- Bluetooth & devices
- Network & internet
- Personalization
- Apps
- Accounts
- Time & language
- Gaming
- Accessibility
- Privacy & security
- Windows Update

Privacy & security > 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.

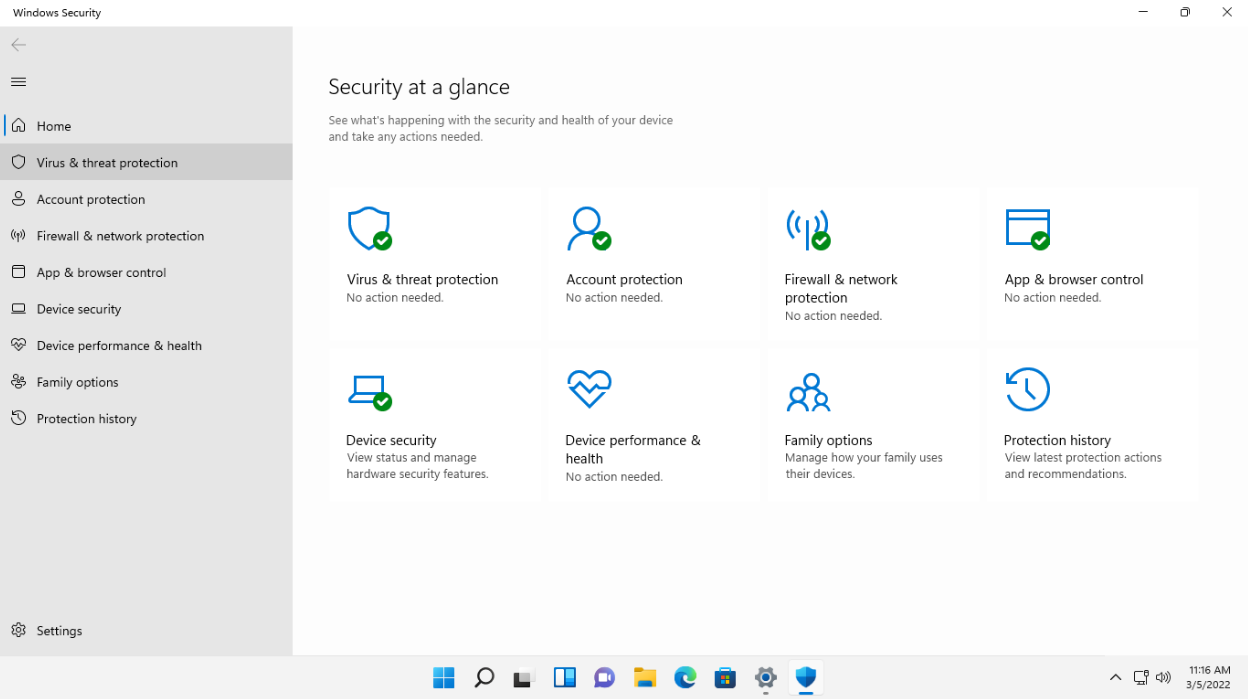
Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

11:16 AM
3/5/2022

Step 5:

On the **Security at a glance** window, click **Virus & threat protection.**



Windows Security

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options
- Protection history
- Settings

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.

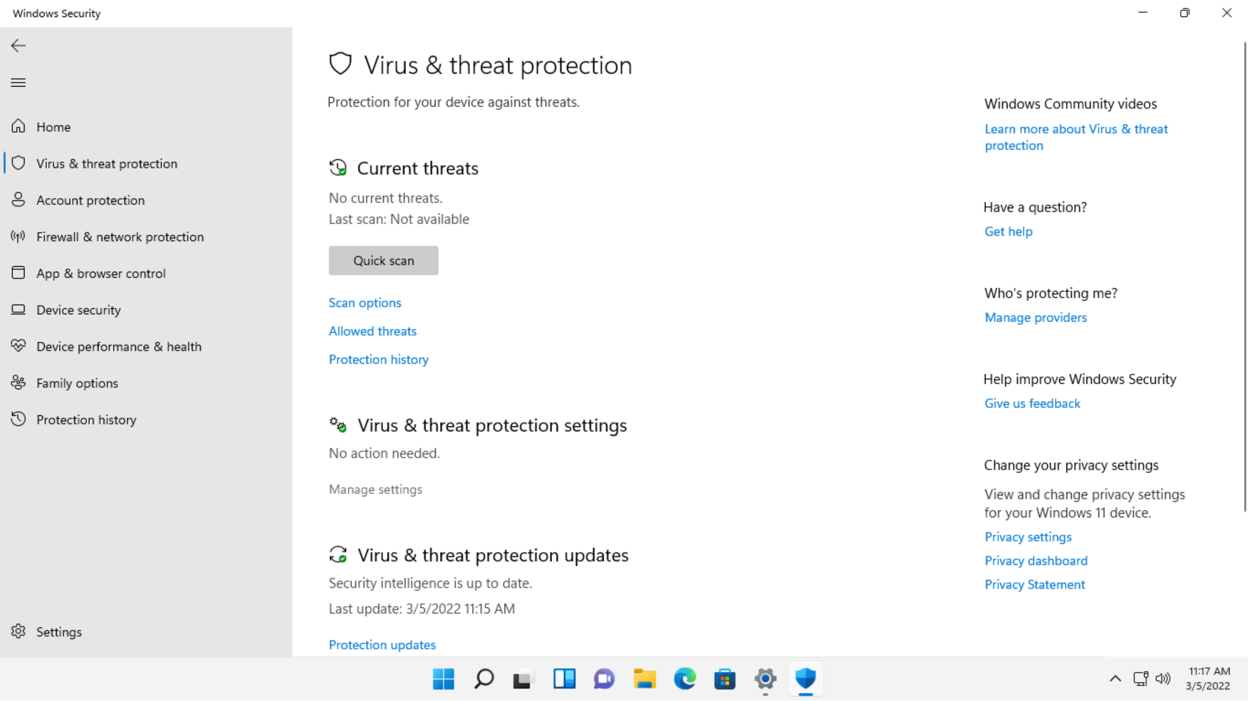
Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

11:16 AM
3/5/2022

Step 6:

On the **Virus & threat protection** page, under the **Virus & threat protection settings** section, click **Manage settings.**



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: Not available

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

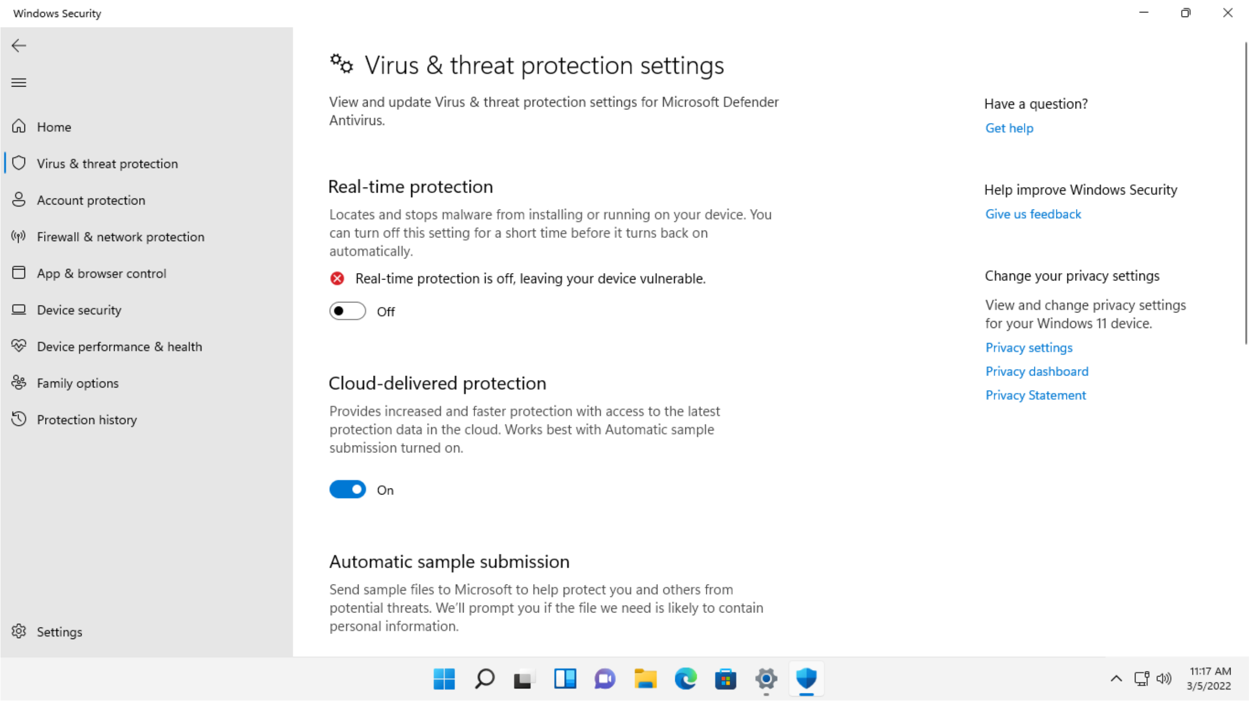
Last update: 3/5/2022 11:15 AM

View and change privacy settings for your Windows 11 device.

Step 7:

On the **Virus & threat protection settings** page, under the **Real-time protection** section, switch the slider to **Off**.

You will get a warning that **Windows Defender Anti-Virus** has been turned off. You can dismiss the message.



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

☒ Real-time protection is off, leaving your device vulnerable.

○ Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

● On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Have a question?
Get help

Help improve Windows Security
Give us feedback

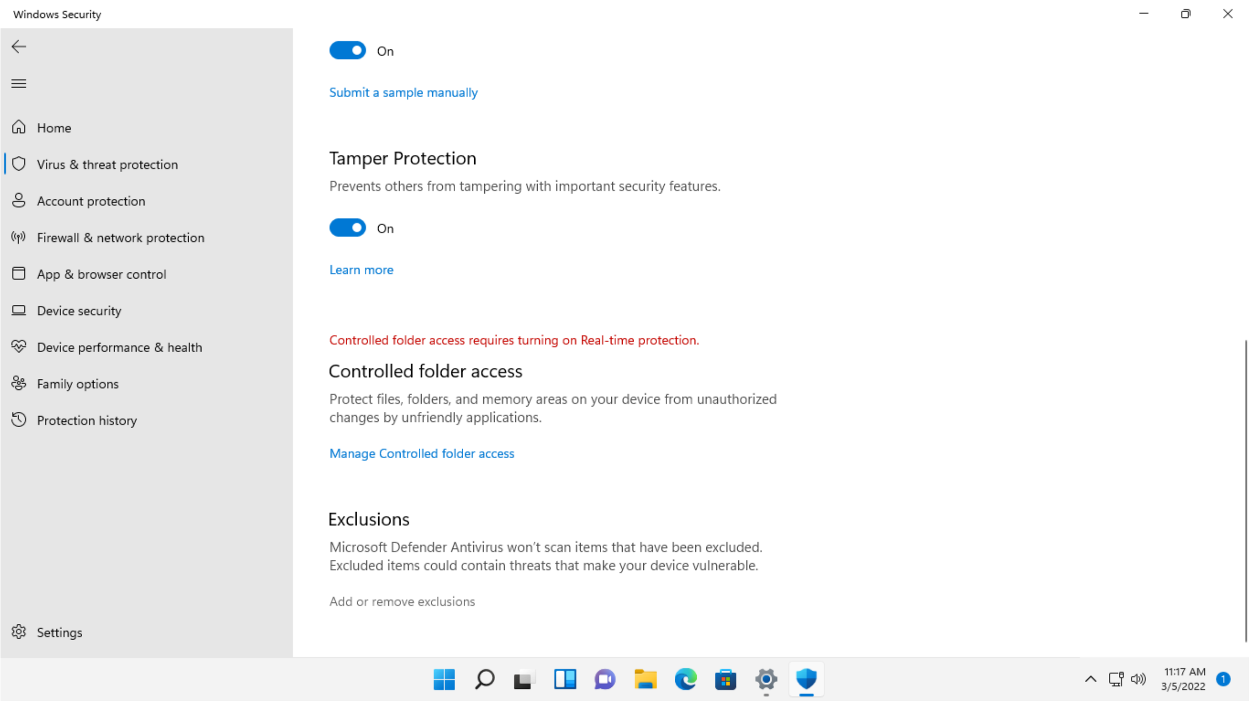
Change your privacy settings

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

Step 8:

Scroll down the page to the **Exclusions** section.

Under the **Exclusions** section, click the **Add or remove exclusions** web link.



● On

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

● On

Learn more

Controlled folder access requires turning on Real-time protection.

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Manage Controlled folder access

Exclusions

Microsoft Defender Antivirus won't scan items that have been excluded. Excluded items could contain threats that make your device vulnerable.

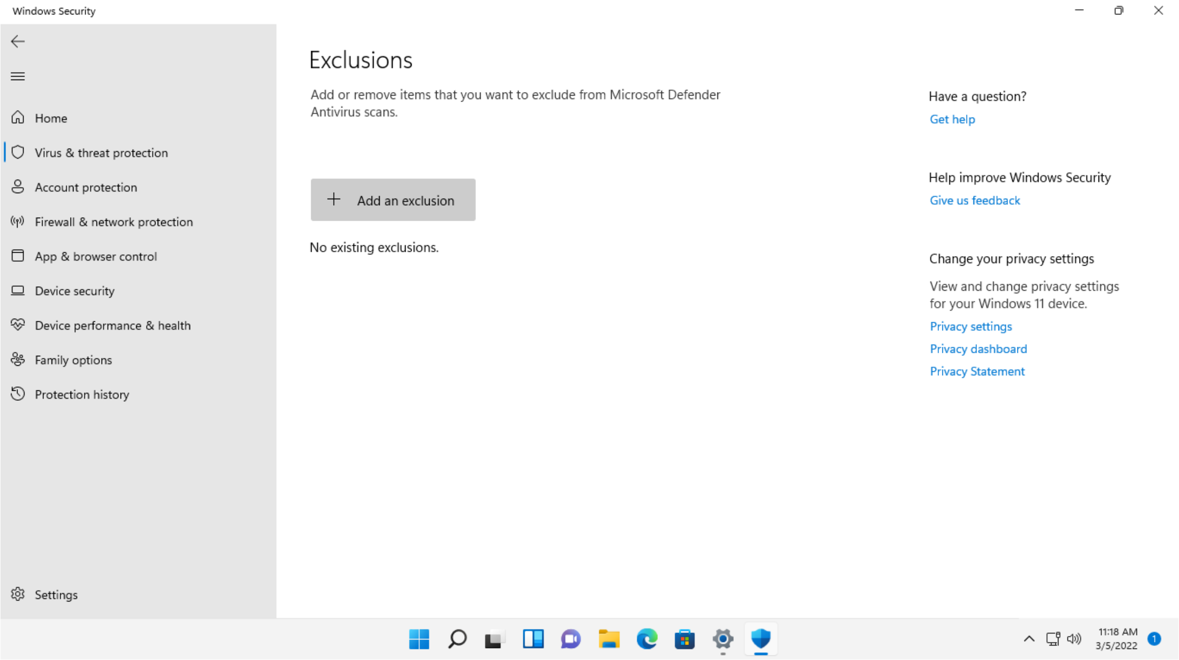
Add or remove exclusions

Step 9:

In my case there is no folder in the Exclusion. If you have please do the below step.

- Click the down arrow next to **C:\ Folder** and select **Remove.**

Note: This is required so you can select a specific folder later to perform a custom scan.



Exclusions

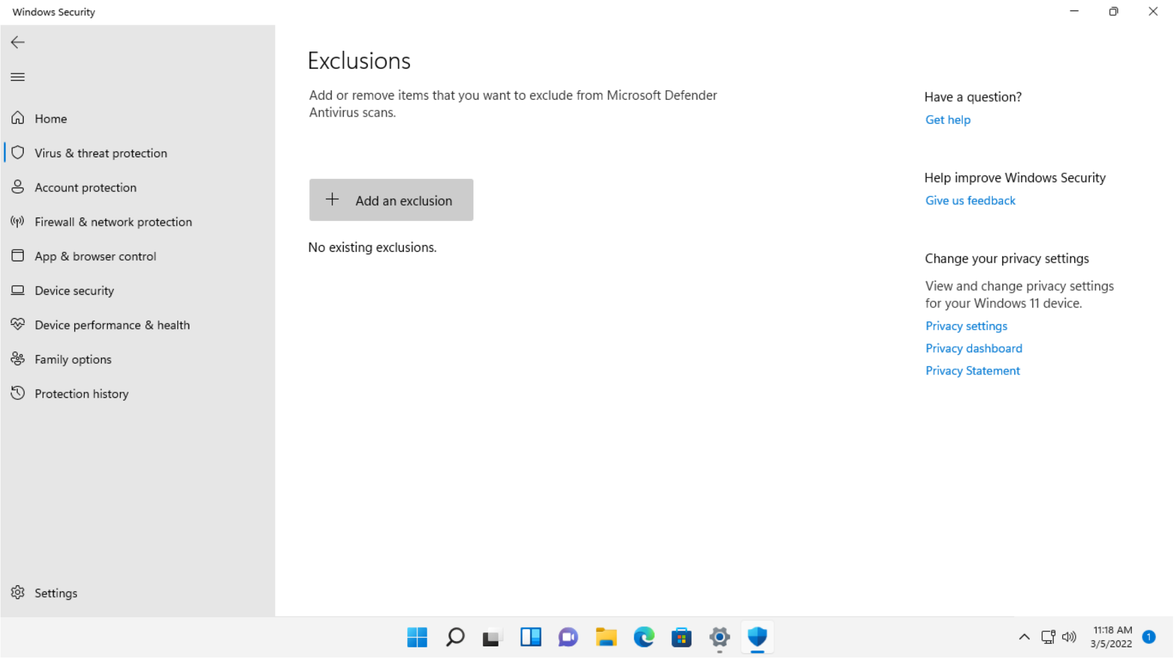
Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

No existing exclusions.

View and change privacy settings for your Windows 11 device.

Step 10:

After removing the exclusions, click the back arrow at the top left corner.



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

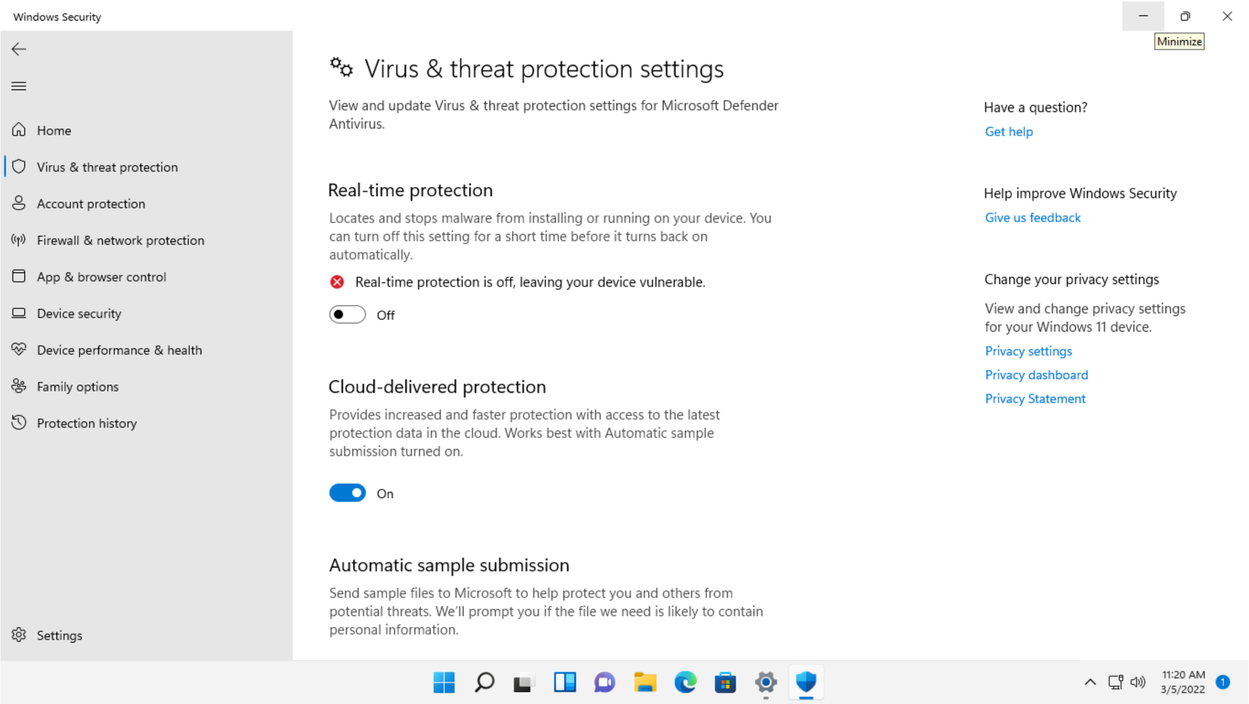
No existing exclusions.

View and change privacy settings for your Windows 11 device.

Step 11:

This will redirect you back to **Virus & threat protection settings** page.

Minimize both the **Virus & threat protection settings** and **Windows Security** windows.



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

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

Task 2: Download Sample Virus and Windows 11 MSRT.

To make it seem like malware has infected Windows 11, you'll need to obtain a sample virus file from the European Institute for Computer Antivirus Research (EICAR).

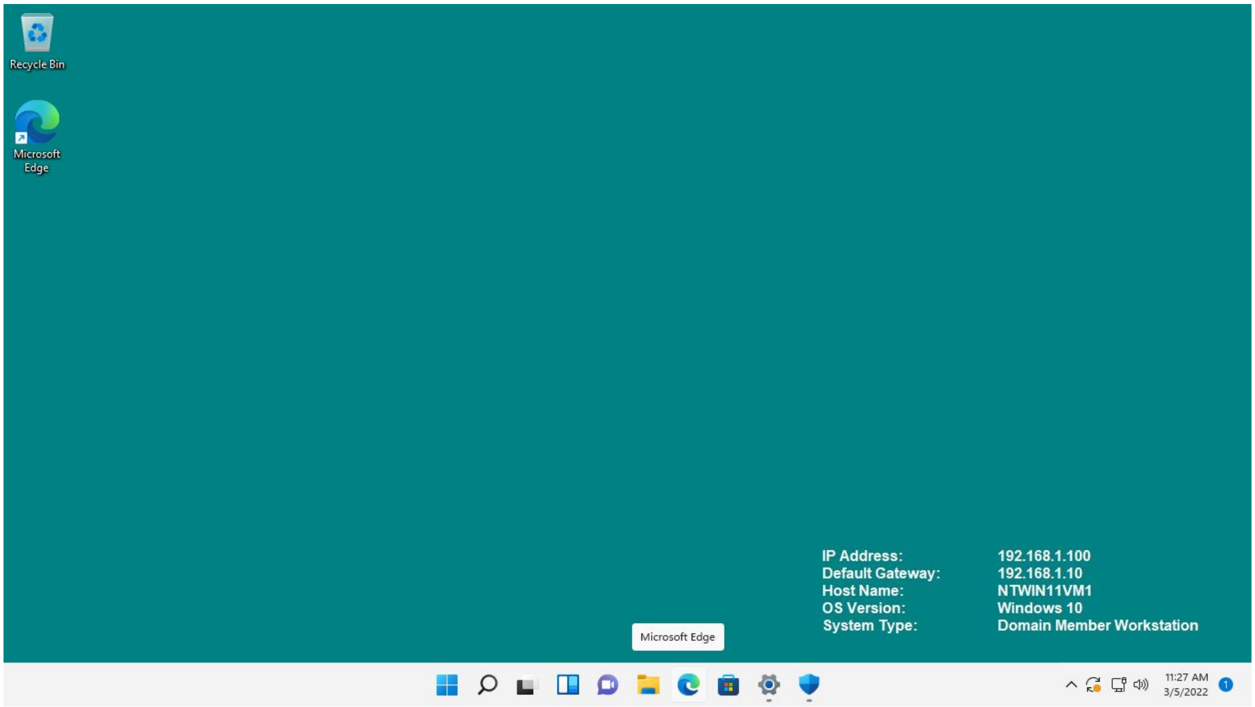
You'll test Windows Defender's capacity to prevent malware from spreading in the system using this sample virus file.

Now let's, download a sample virus file and Windows 11 Malicious Software Removal Tool (MSRT).

Step 1:

Ensure you are still connected to **NTWIN11VM1**.

Click **Microsoft Edge** on the **Taskbar.**

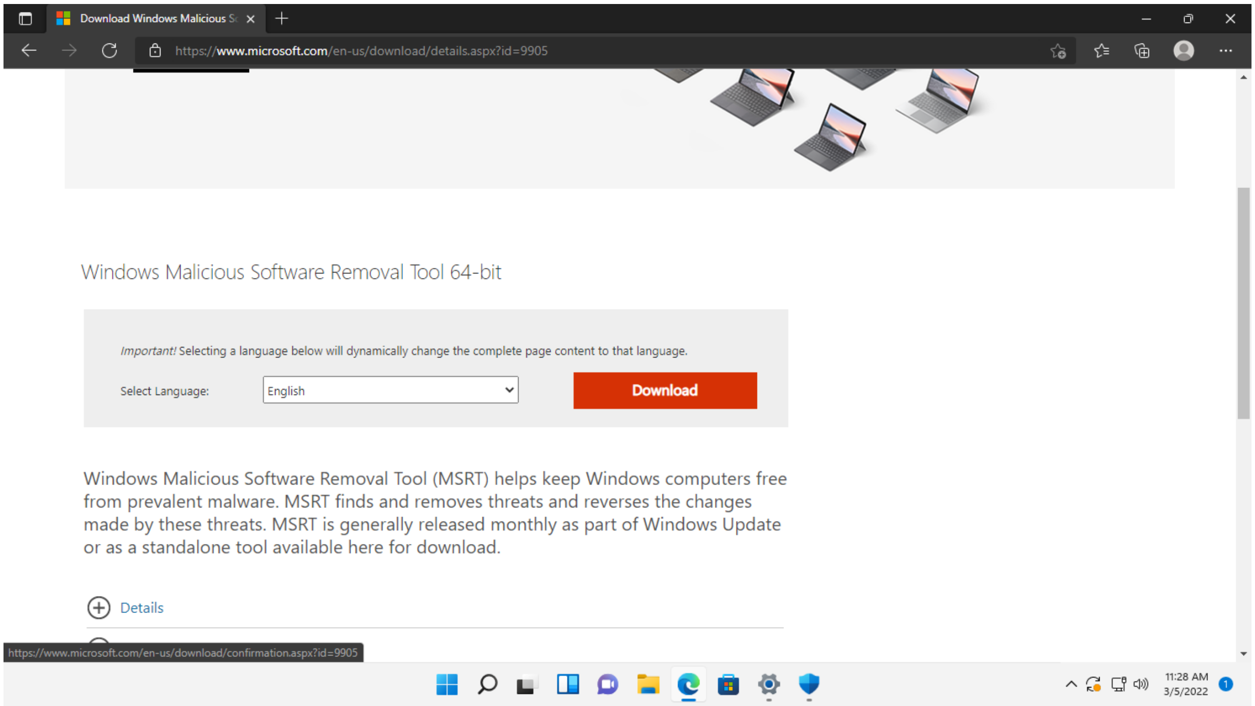


IP Address: 192.168.1.100
Default Gateway: 192.168.1.10
Host Name: NTWIN11VM1
OS Version: Windows 10
System Type: Domain Member Workstation

Step 2:

Go for the above links and download the MSRT

Wait a moment while the file downloads.



https://www.microsoft.com/en-us/download/details.aspx?id=9905

Windows Malicious Software Removal Tool 64-bit

Important! Selecting a language below will dynamically change the complete page content to that language.

Select Language: English

Windows Malicious Software Removal Tool (MSRT) helps keep Windows computers free from prevalent malware. MSRT finds and removes threats and reverses the changes made by these threats. MSRT is generally released monthly as part of Windows Update or as a standalone tool available here for download.

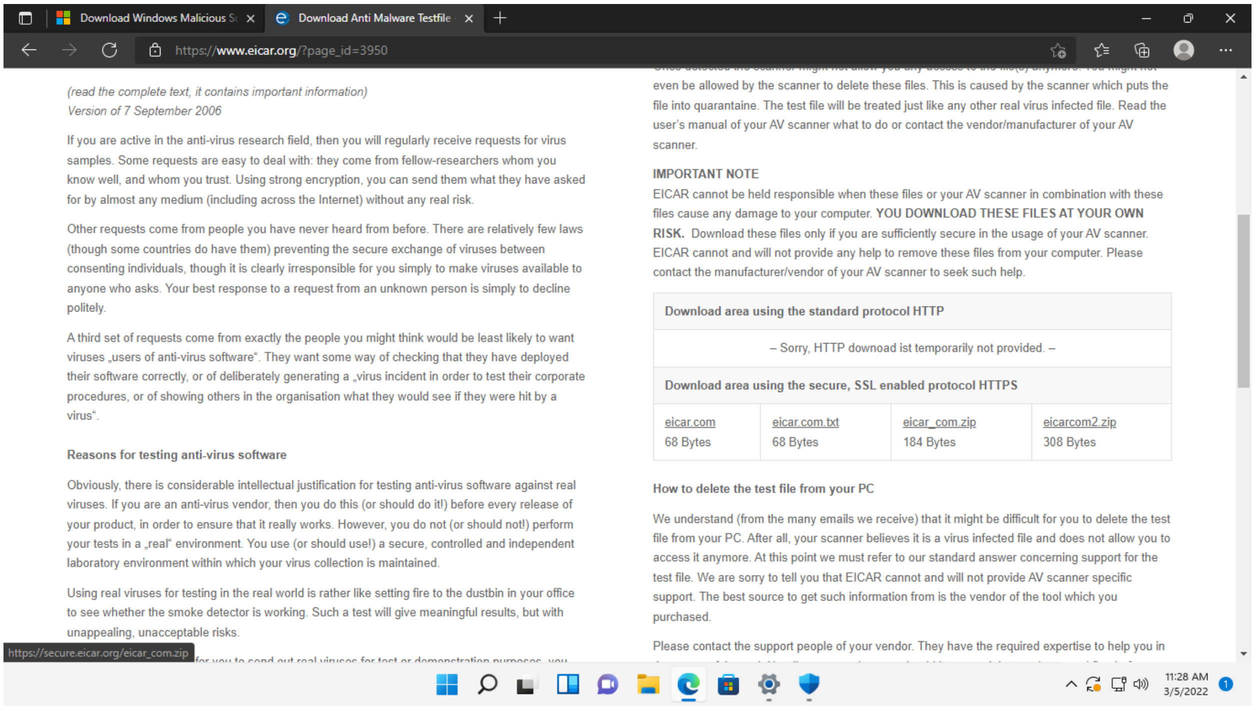
https://www.microsoft.com/en-us/download/confirmation.aspx?id=9905

Step 3:

Also, download the **eicar.com.zip** file.

Wait a moment while the file downloads.

When the two files have been successfully downloaded, close **Microsoft Edge**.


Download Windows Malicious S
Download Anti Malware Testfile
https://www.eicar.org/?page_id=3950
https://secure.eicar.org/eicar_com.zip
11:28 AM
3/5/2022

(read the complete text, it contains important information)
Version of 7 September 2006

If you are active in the anti-virus research field, then you will regularly receive requests for virus samples. Some requests are easy to deal with: they come from fellow-researchers whom you know well, and whom you trust. Using strong encryption, you can send them what they have asked for by almost any medium (including across the Internet) without any real risk.

Other requests come from people you have never heard from before. There are relatively few laws (though some countries do have them) preventing the secure exchange of viruses between consenting individuals, though it is clearly irresponsible for you simply to make viruses available to anyone who asks. Your best response to a request from an unknown person is simply to decline politely.

A third set of requests come from exactly the people you might think would be least likely to want viruses „users of anti-virus software". They want some way of checking that they have deployed their software correctly, or of deliberately generating a „virus incident in order to test their corporate procedures, or of showing others in the organisation what they would see if they were hit by a virus".

Reasons for testing anti-virus software

Obviously, there is considerable intellectual justification for testing anti-virus software against real viruses. If you are an anti-virus vendor, then you do this (or should do it!) before every release of your product, in order to ensure that it really works. However, you do not (or should not!) perform your tests in a „real" environment. You use (or should use!) a secure, controlled and independent laboratory environment within which your virus collection is maintained.

Using real viruses for testing in the real world is rather like setting fire to the dustbin in your office to see whether the smoke detector is working. Such a test will give meaningful results, but with unappealing, unacceptable risks.

even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

IMPORTANT NOTE
EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol HTTP			
– Sorry, HTTP downoad ist temporarily not provided. –			
Download area using the secure, SSL enabled protocol HTTPS			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

How to delete the test file from your PC

We understand (from the many emails we receive) that it might be difficult for you to delete the test file from your PC. After all, your scanner believes it is a virus infected file and does not allow you to access it anymore. At this point we must refer to our standard answer concerning support for the test file. We are sorry to tell you that EICAR cannot and will not provide AV scanner specific support. The best source to get such information from is the vendor of the tool which you purchased.

Please contact the support people of your vendor. They have the required expertise to help you in

Task 3: Install and Run MSRT

In Windows 11, the Microsoft Software Removal Tool (MSRT) is usually distributed once a month as part of the regular Windows Update.

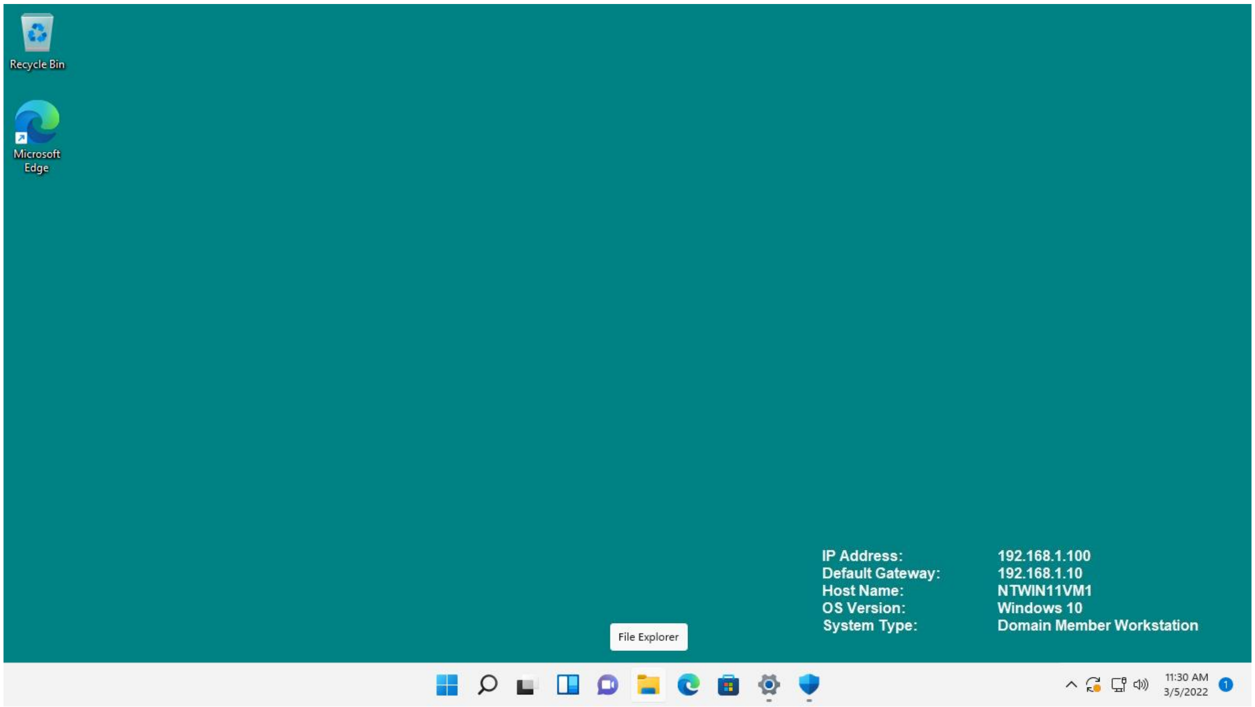
A newer version has superseded the version presented in this lab. Nonetheless, you will install the earlier version downloaded from the site address for the sake of experience.

Now let's, install MSRT and perform a quick scan on Windows 11 to check for malware.

Step 1:

Ensure you are still connected to **NTWIN11VM1**.

Click **File Explorer** on the **Taskbar**.

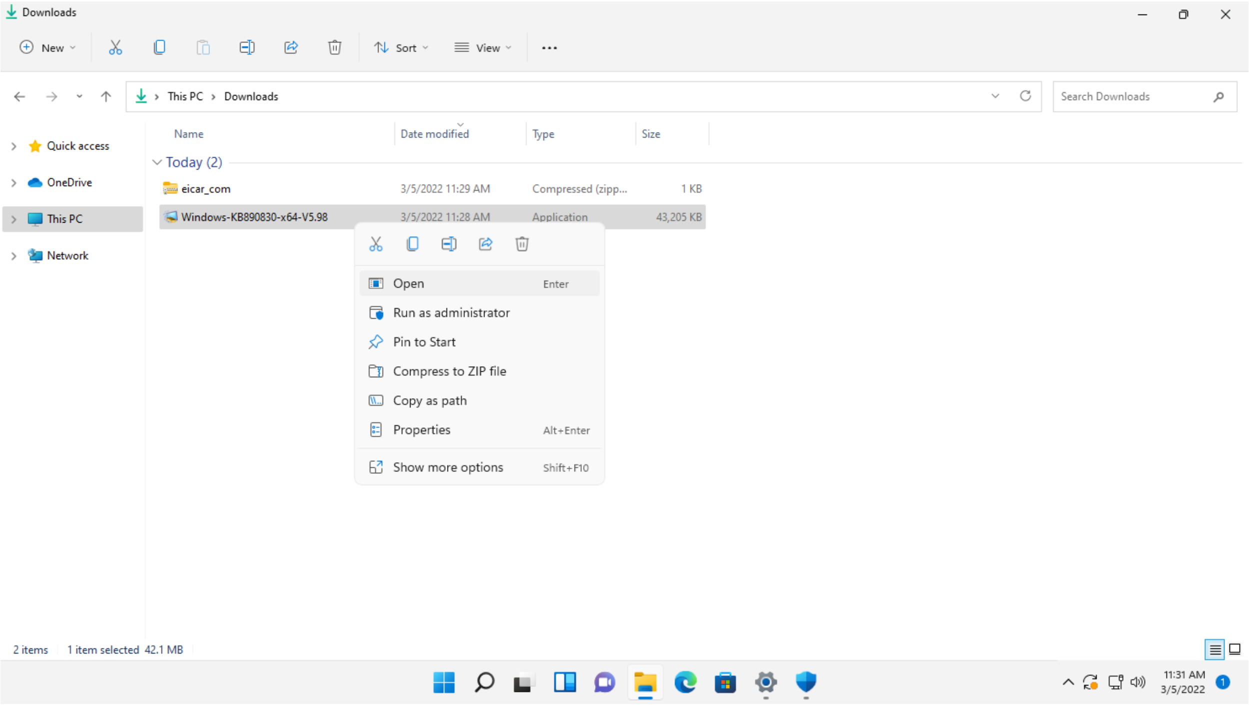


IP Address: 192.168.1.100
Default Gateway: 192.168.1.10
Host Name: NTWIN11VM1
OS Version: Windows 10
System Type: Domain Member Workstation

Step 2:

Under the **Quick Access** section in the left-hand pane, click the **Downloads** folder.

Right-click **Windows-KB890830-x64-V5.98** and select **Open**.



Name	Date modified	Type	Size
Today (2)			
eicar_com	3/5/2022 11:29 AM	Compressed (zipp...	1 KB
Windows-KB890830-x64-V5.98	3/5/2022 11:28 AM	Application	43,205 KB

2 items 1 item selected 42.1 MB

Step 3:

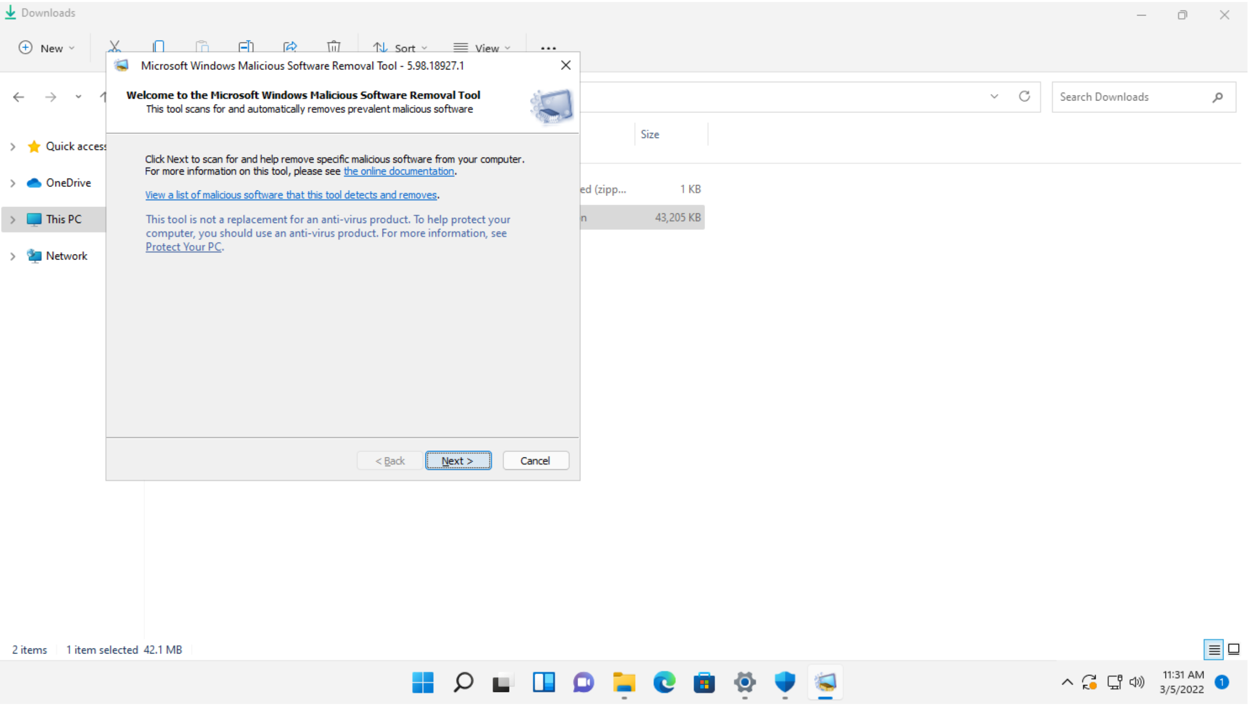
If a message box appears in the **Taskbar** indicating a more recent version of the tool may be available.

Click **OK** to continue.

Step 4:

The **Welcome to the Microsoft Windows Malicious Software Removal Tool** window will appear

Click **Next.**



Microsoft Windows Malicious Software Removal Tool - 5.98.18927.1

Welcome to the Microsoft Windows Malicious Software Removal Tool
This tool scans for and automatically removes prevalent malicious software

Click Next to scan for and help remove specific malicious software from your computer.
For more information on this tool, please see the online documentation.

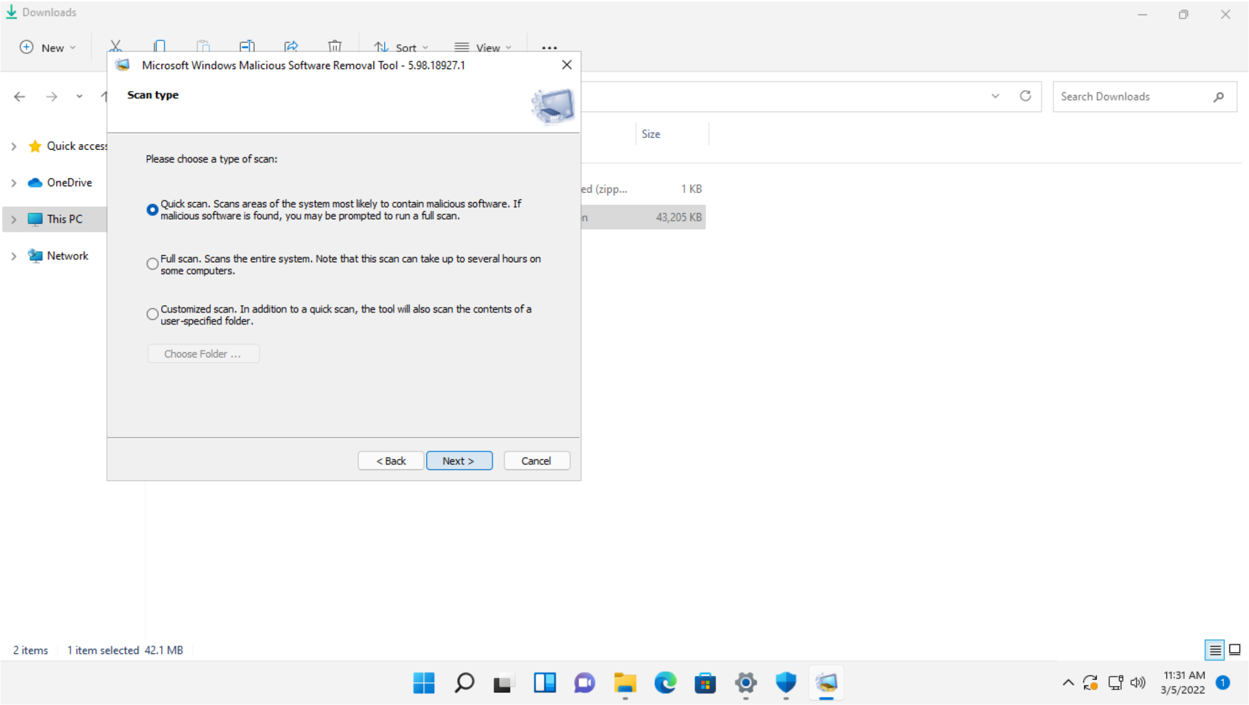
View a list of malicious software that this tool detects and removes.

This tool is not a replacement for an anti-virus product. To help protect your computer, you should use an anti-virus product. For more information, see Protect Your PC.

Step 5:

On the **Scan type** page, **Quick scan** is the default selection.

Click **Next.**



Microsoft Windows Malicious Software Removal Tool - 5.98.18927.1

Scan type

Please choose a type of scan:

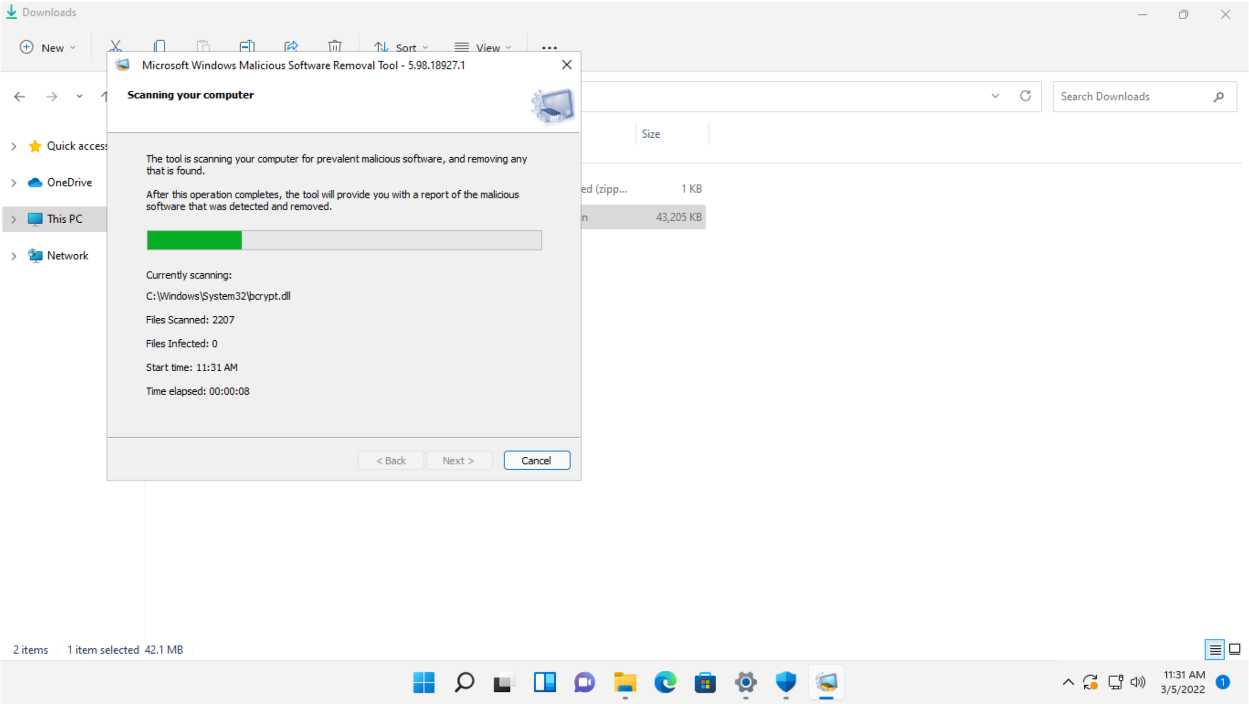
● Quick scan. Scans areas of the system most likely to contain malicious software. If malicious software is found, you may be prompted to run a full scan.

○ Full scan. Scans the entire system. Note that this scan can take up to several hours on some computers.

○ Customized scan. In addition to a quick scan, the tool will also scan the contents of a user-specified folder.

Step 6:

Please wait while the **Scanning your computer** process runs.



Microsoft Windows Malicious Software Removal Tool - 5.98.18927.1

Scanning your computer

The tool is scanning your computer for prevalent malicious software, and removing any that is found.

After this operation completes, the tool will provide you with a report of the malicious software that was detected and removed.

Currently scanning:

C:\Windows\System32\bcrypt.dll

Files Scanned: 2207

Files Infected: 0

Start time: 11:31 AM

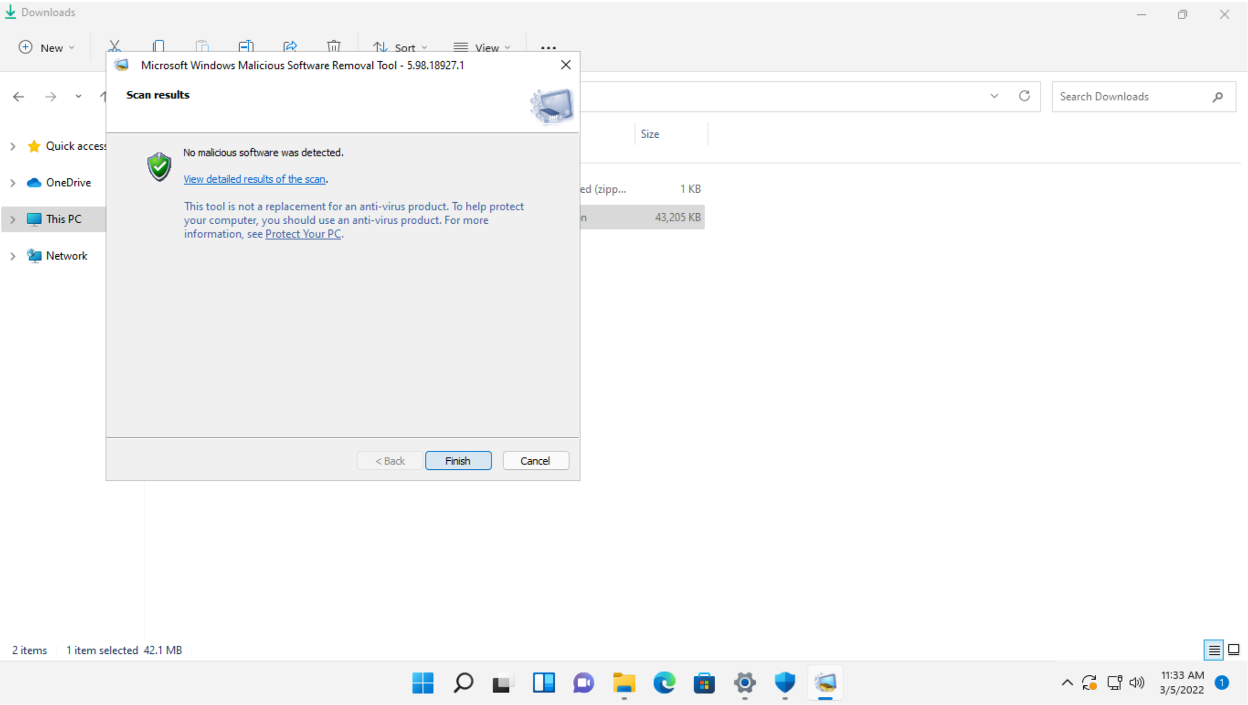
Time elapsed: 00:00:08

Step 7:

The **Scan results** page should indicate that no malicious software was detected.

Click **Finish**.

Minimize **File Explorer** window.



Microsoft Windows Malicious Software Removal Tool - 5.98.18927.1

Scan results

No malicious software was detected.

View detailed results of the scan.

This tool is not a replacement for an anti-virus product. To help protect your computer, you should use an anti-virus product. For more information, see Protect Your PC.

Task 4: Turn on Real-Time Protection

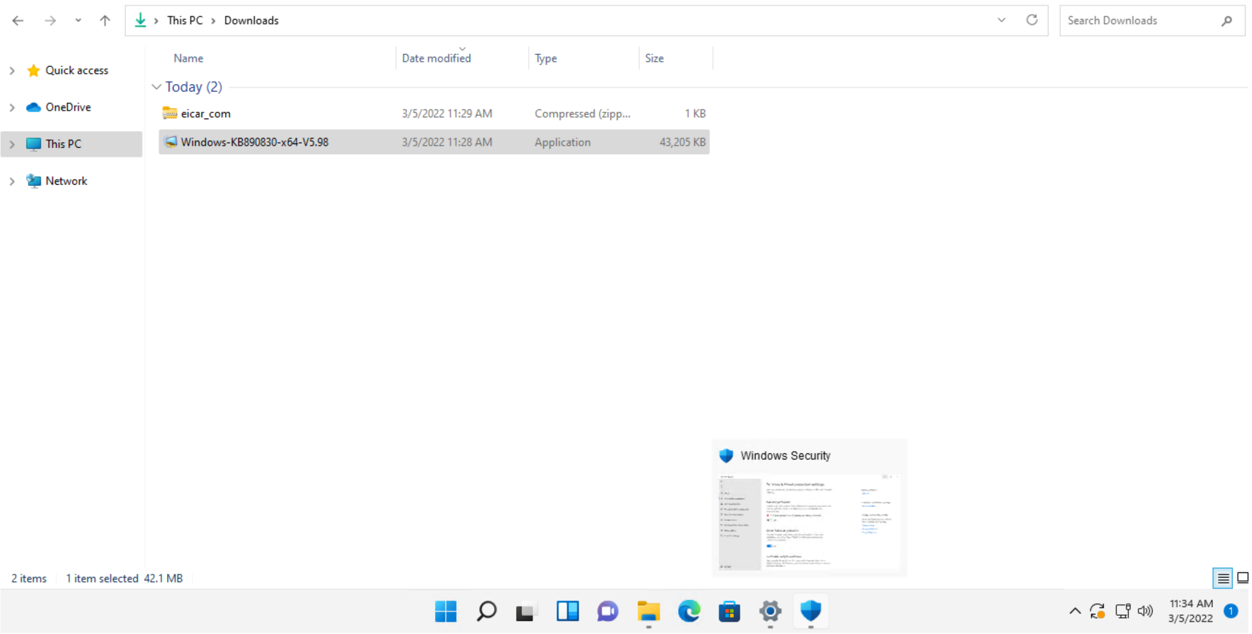
After scanning the machine for malware using the MSRT program, turn on real-time protection and let Windows Defender check the system for malware.

Now let’s, re-enable real-time protection and let Windows Defender search the computer for malware.

Step 1:

Ensure you are still connected to **NTWIN11VM1**.

On **NTWIN11VM1**, reopen the **Windows Security** window (shield icon) from the Taskbar.



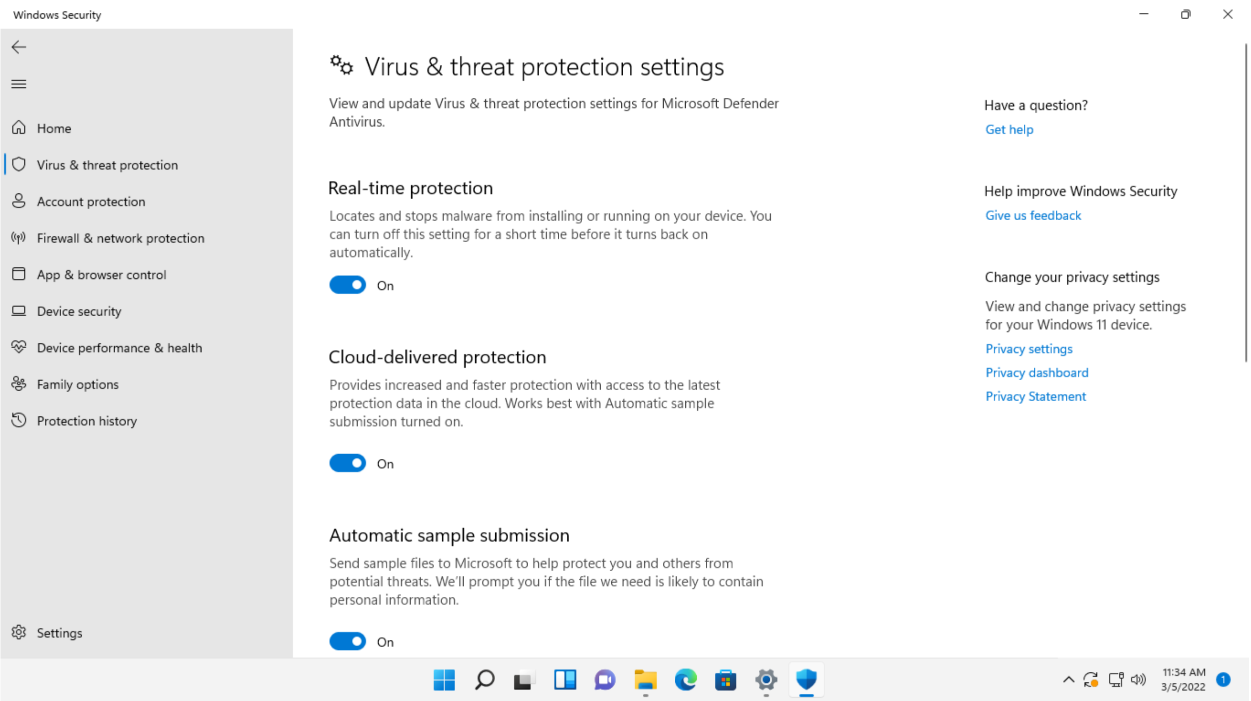
This PC › Downloads

Name	Date modified	Type	Size
Today (2)			
eicar_com	3/5/2022 11:29 AM	Compressed (zipp...	1 KB
Windows-KB890830-x64-V5.98	3/5/2022 11:28 AM	Application	43,205 KB

2 items 1 item selected 42.1 MB

Step 2:

Under the **Real-time protection** section, click the slider button to **On**.



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

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.

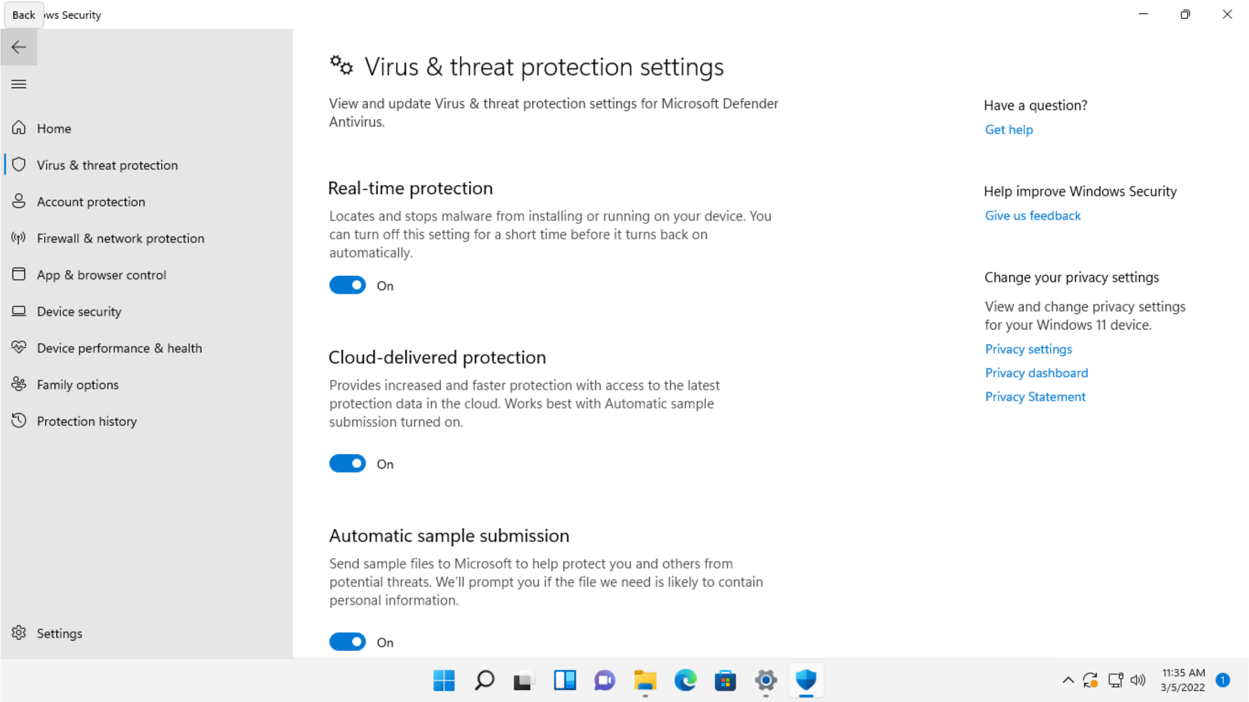
Privacy settings

Privacy dashboard

Privacy Statement

Step 3:

After turning on the **Real-time protection,** click the back button at the top left of the window



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

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.

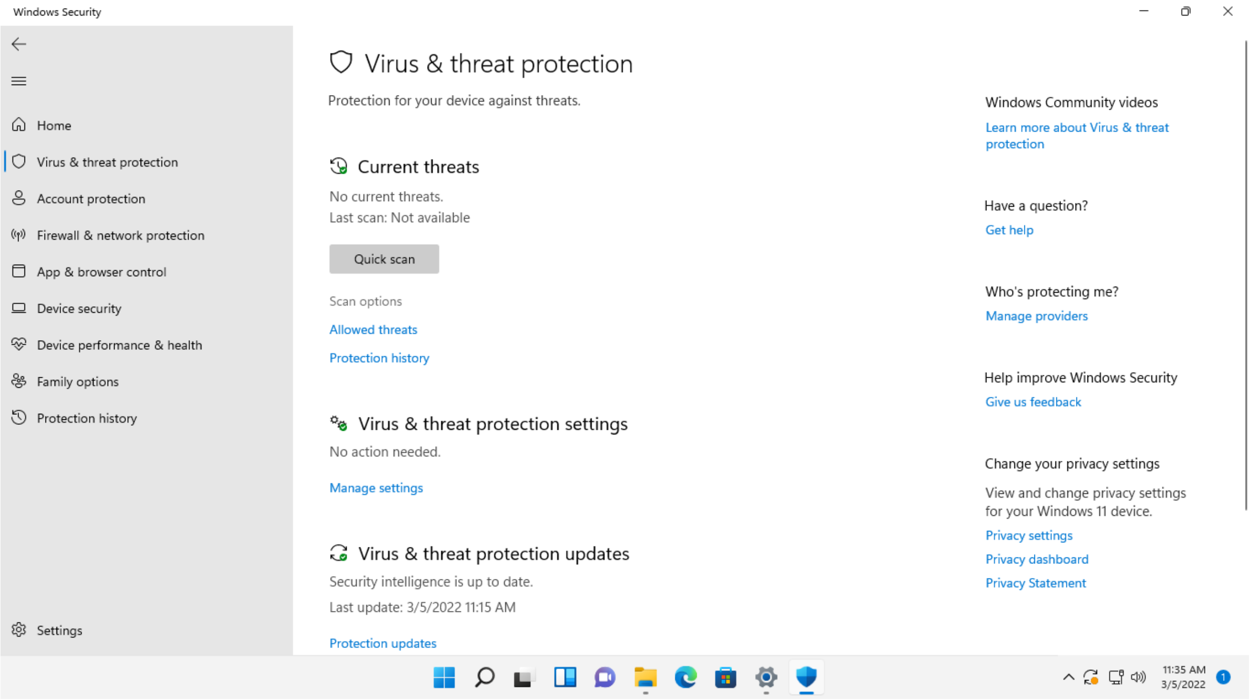
Privacy settings

Privacy dashboard

Privacy Statement

Step 4:

On the **Virus & threat protection** page, under the **Current threats** section, click the **Scan options** web link.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.

Last scan: Not available

Quick scan

Scan options

Allowed threats

Protection history

Virus & threat protection settings

No action needed.

Manage settings

Virus & threat protection updates

Security intelligence is up to date.

Last update: 3/5/2022 11:15 AM

Protection updates

Windows Community videos

Learn more about Virus & threat protection

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.

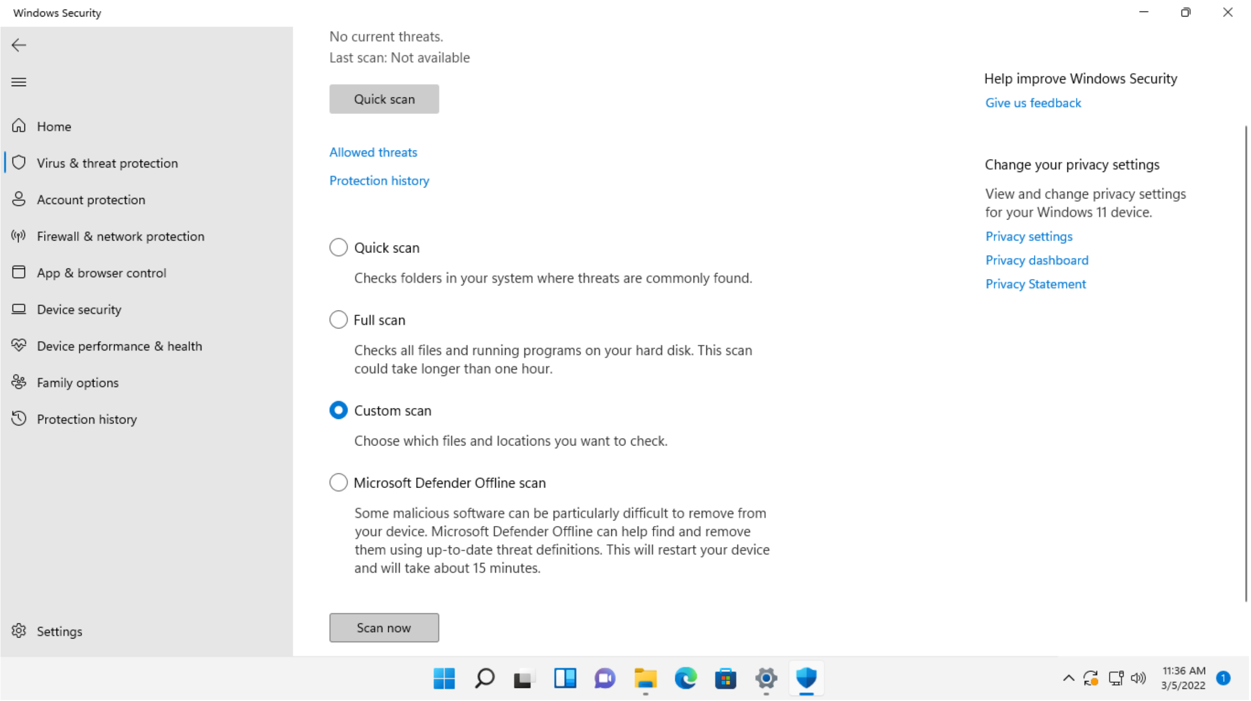
Privacy settings

Privacy dashboard

Privacy Statement

Step 5:

Choose **Custom scan**, then click **Scan now**.



No current threats.
Last scan: Not available

○ 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.

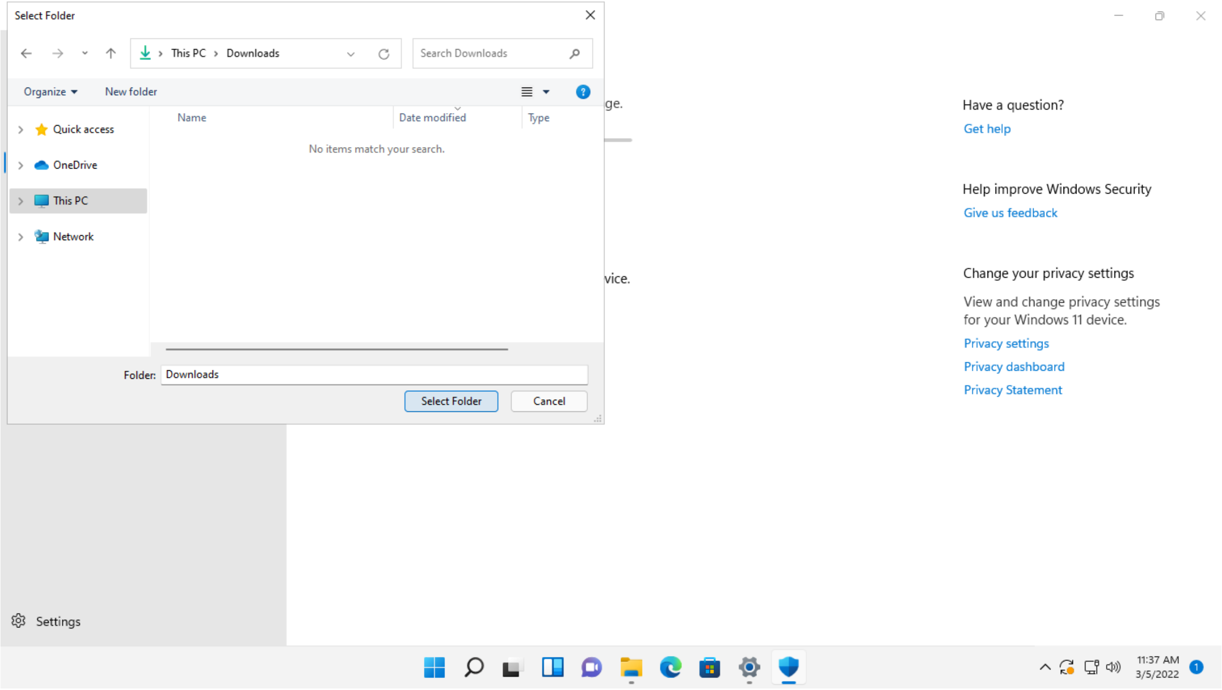
Change your privacy settings

View and change privacy settings for your Windows 11 device.

Step 6:

On the **Select Folder** dialog box, under **Quick access**, click **Downloads** folder.

Click **Select Folder**.



No items match your search.

Folder: Downloads

Change your privacy settings

View and change privacy settings for your Windows 11 device.

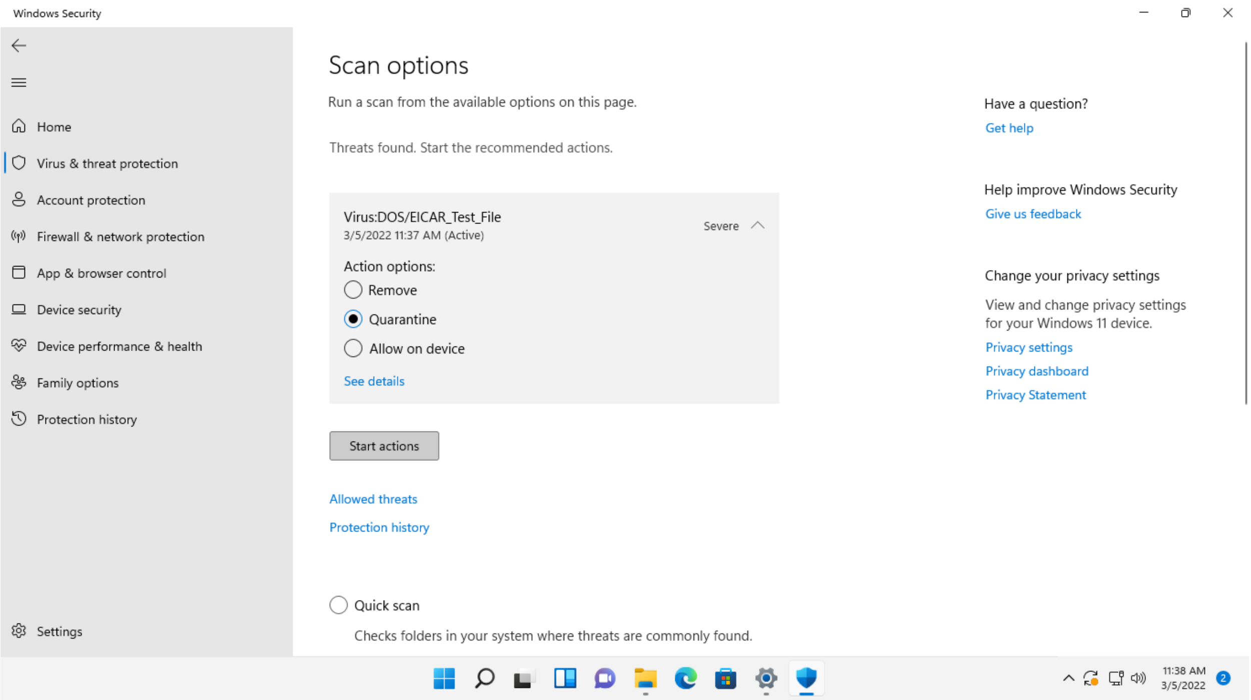
Step 7:

Please wait while the scan is in progress.

The **Virus & threat protection** page will now show that a threat has been found named "Virus:DOS/EICAR_Test_File."

Under **Current threats**, click the up arrow next to the title "**Severe**" to expand.

Then select **Quarantine** and click **Start actions.**



Windows Security

Scan options

Run a scan from the available options on this page.

Threats found. Start the recommended actions.

Virus:DOS/EICAR_Test_File
3/5/2022 11:37 AM (Active)

Severe

Action options:

○ Remove

● Quarantine

○ Allow on device

See details

Start actions

Allowed threats

Protection history

○ Quick scan

Checks folders in your system where threats are commonly found.

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

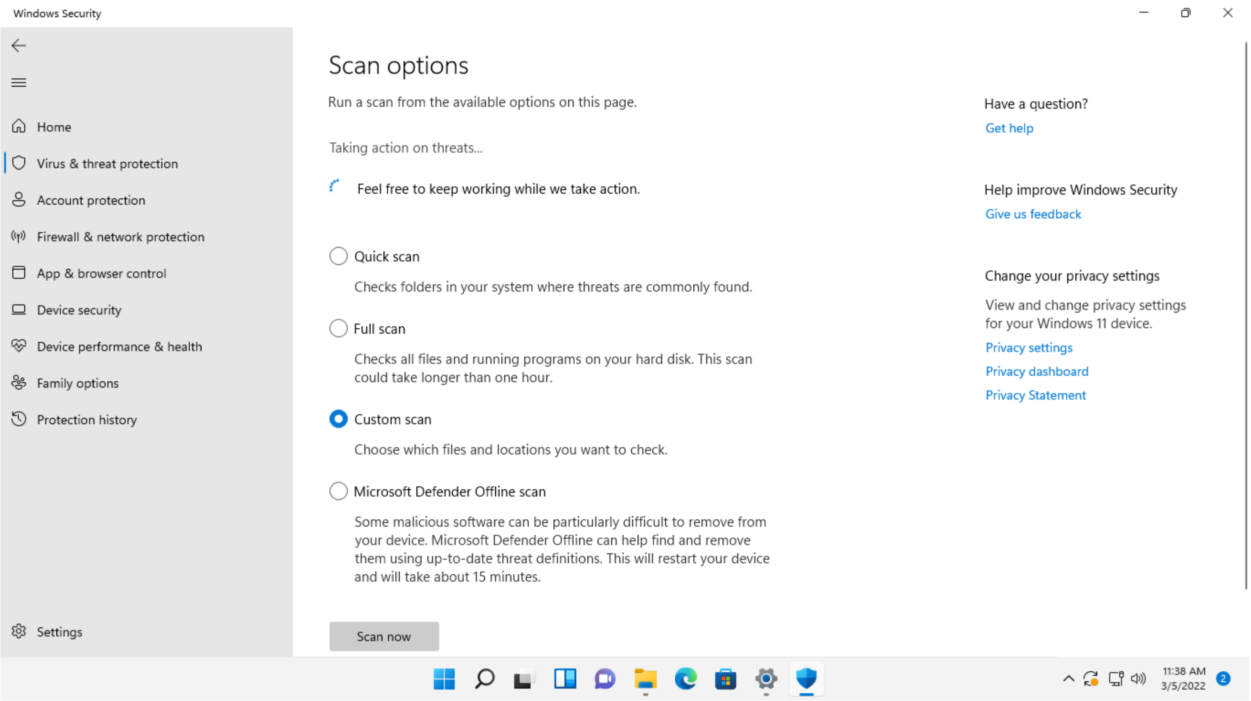
Privacy dashboard

Privacy Statement

Step 8:

Windows Security performs the quarantine process for the detected threat.

Please wait a moment for this to run.



Scan options

Run a scan from the available options on this page.

Taking action on threats...

Feel free to keep working while we take action.

○ 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

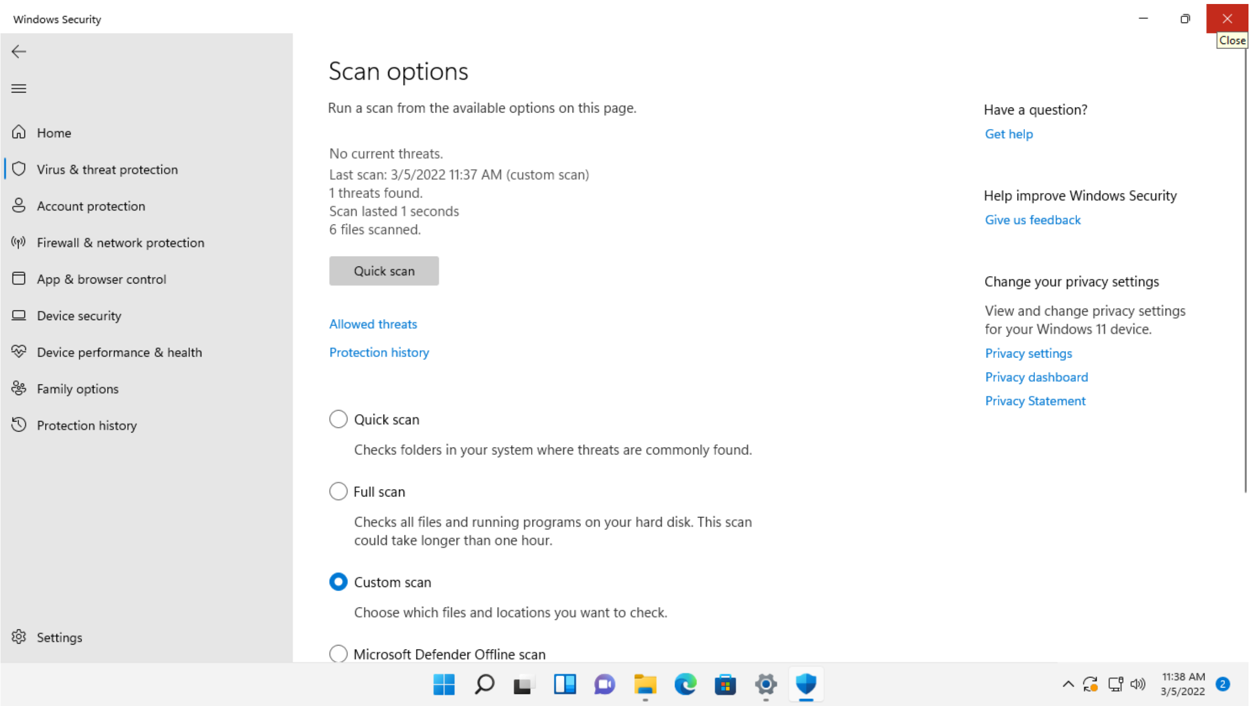
Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Scan now
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
11:38 AM
3/5/2022

Step 9:

The threat was successfully quarantined.

Close the **Windows Security** window.



Scan options

Run a scan from the available options on this page.

No current threats.
Last scan: 3/5/2022 11:37 AM (custom scan)
1 threats found.
Scan lasted 1 seconds
6 files scanned.

○ 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

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
11:38 AM
3/5/2022