Hands-on Lab: Windows Defender Antivirus

Estimated time needed: **20** minutes

Objectives

By completing this lab, you will develop a comprehensive understanding of how to secure a Windows operating system using the functionality of real-time protection provided by **Windows Defender**.

In this hands-on lab, you will explore typical settings to enable protection:

- Exercise 1: Review Windows Security Virus and threat protection.
- Exercise 2: Update threat definitions.
- Exercise 3: Run Windows Defender Antivirus quick scan.
- Exercise 4: Run Windows Defender Antivirus custom scan.

Further in this hands-on lab, you will also explore typical use cases:

- Scenario 1 - Schedule a weekly full scan using Windows Defender Antivirus
- Scenario 2 - Simulate downloading a test malware file and activate Windows Defender Antivirus to block and quarantine the file.

Important Notices about This Lab

About Lab Sessions

Lab sessions are not persisted. This means that every time you connect to this lab, a new environment is created for you. Any data or files you saved in a previous session are no longer available. To avoid losing your data, plan to complete these tasks in a single session.

About the Lab Instructions and Solutions

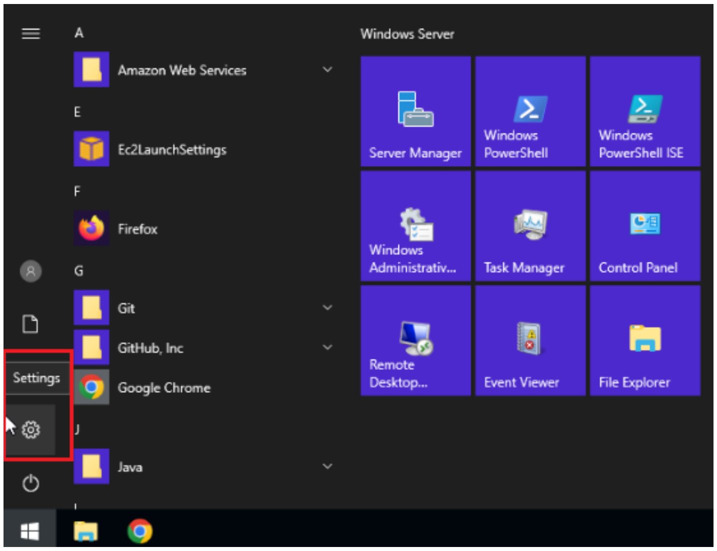
Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

Configuration of Windows Defender Antivirus

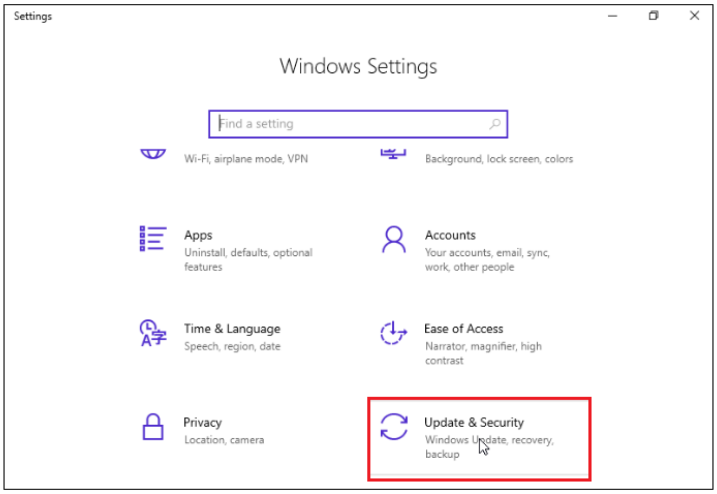
Exercise 1: Review Windows Security Virus & threat protection

In this lab, you'll access and review Windows Security Virus & threat protection. Let's begin with locating and opening Windows Security Virus & threat protection.

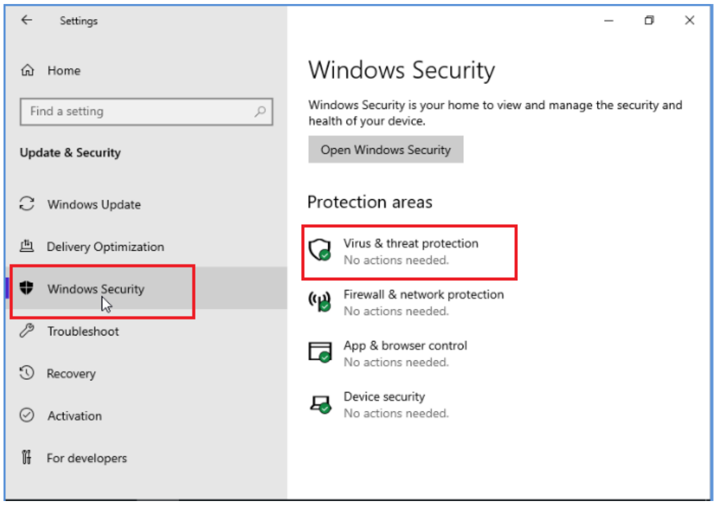
1. Click the Windows **Start** button and select **Settings**.



2. On the Windows Settings page, select **Update & Security**.


Settings
Windows Settings
Find a setting
Wi-Fi, airplane mode, VPN
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

3. Under Update & Security, select **Windows Security**. Here, select **Virus and threat protection**.

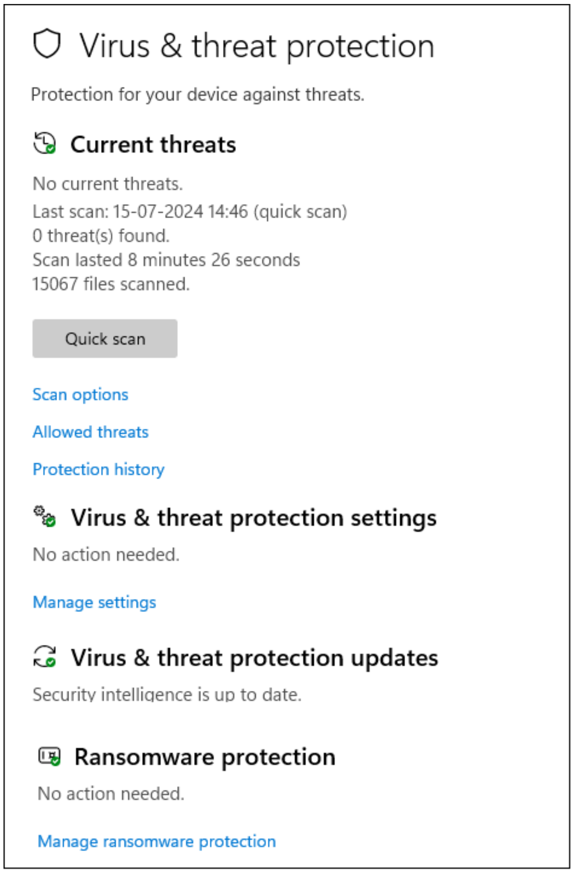

Windows Security is your home to view and manage the security and health of your device.

4. On this screen, you'll see the following features:

- **Current threats**: Here, you can see any threats that have been detected on your device. You can see when the last scan occurred, how long the scan took, and how many files were scanned. Here you can also click the button to start a quick scan or access **scan options** to run a full scan or a custom scan.

- **Virus & threat protection settings**: Here, you can access options for managing your virus and threat protection settings. You can customize your protection level, opt to send sample files to Microsoft, exclude files or folders from scans, or temporarily stop your protection.

- **Virus & threat protection updates**: Here, you can view the last time your virus definitions were updated. You can also opt to manually check for updates.
- **Ransomware protection**: Here, you can choose to enable controlled folder access. This protects memory, files, and folders from unauthorized changes.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 15-07-2024 14:46 (quick scan)
0 threat(s) found.
Scan lasted 8 minutes 26 seconds
15067 files scanned.

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.

Ransomware protection

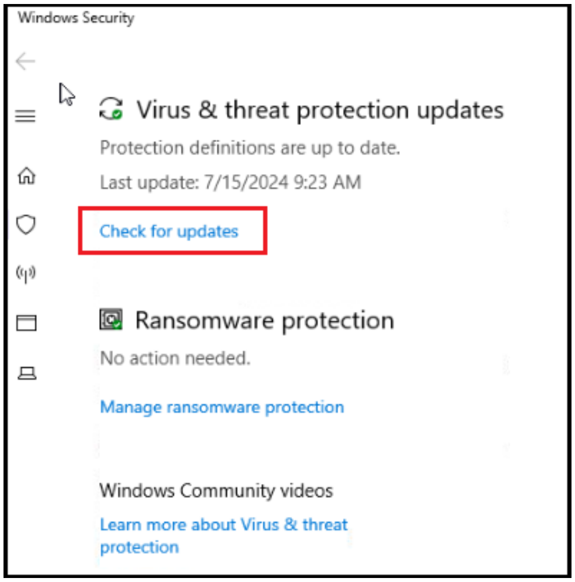
No action needed.

Manage ransomware protection

Exercise 2: Update Threat Definitions

Windows Security uses security intelligence, also known as definitions, to identify known threats. These definitions include information about known threats. These definitions are updated automatically, but if you suspect a problem with your system, you should ensure that threat definitions are up-to-date before you run a scan.

1. Under Virus & threat protection updates, select **Check for updates**.



Windows Security

Virus & threat protection updates

Protection definitions are up to date.

Last update: 7/15/2024 9:23 AM

Check for updates

Ransomware protection

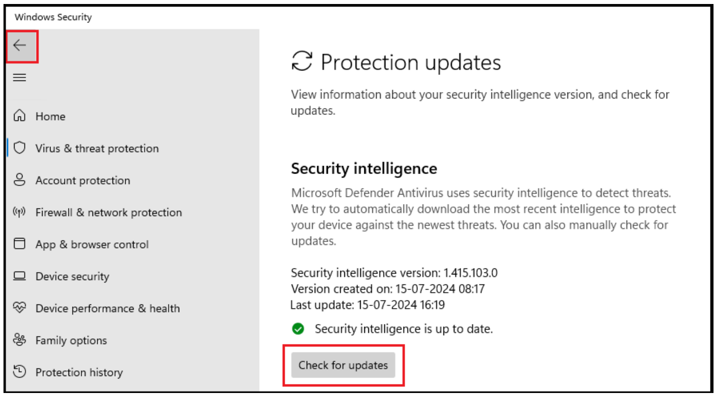
No action needed.

Manage ransomware protection

Windows Community videos

Learn more about Virus & threat protection

2. You can view details for the most recent update to your threat definitions. Select **Check for updates**. This process could take a few minutes. When the update has completed, the **Check for updates** button will return, and you should notice that the last update time and date have changed. Select the back button to return to the **Virus & threat protection** screen.



Protection updates

View information about your security intelligence version, and check for updates.

Security intelligence

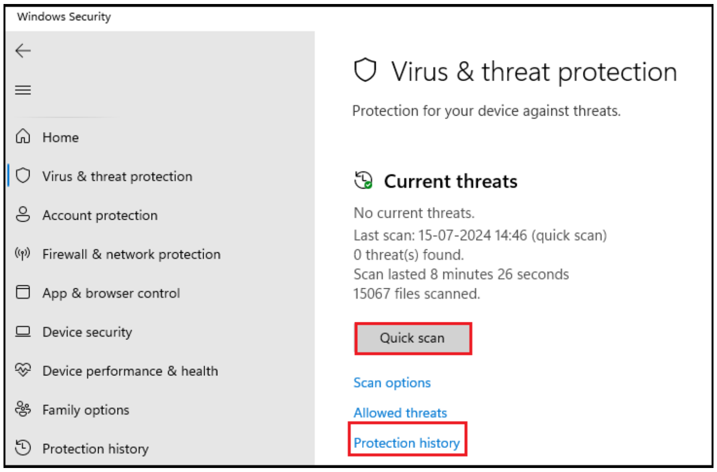
Microsoft Defender Antivirus uses security intelligence to detect threats. We try to automatically download the most recent intelligence to protect your device against the newest threats. You can also manually check for updates.

Security intelligence version: 1.415.103.0
Version created on: 15-07-2024 08:17
Last update: 15-07-2024 16:19

Security intelligence is up to date.

Exercise 3: Run Antivirus Quick Scan

1. Now we can run an antivirus scan. Click the **Quick scan** button on the **Virus & threat protection** screen. The scan will take several minutes to run. When complete, the **Quick scan** button will reappear. Click **Protection history** to view any recent findings.



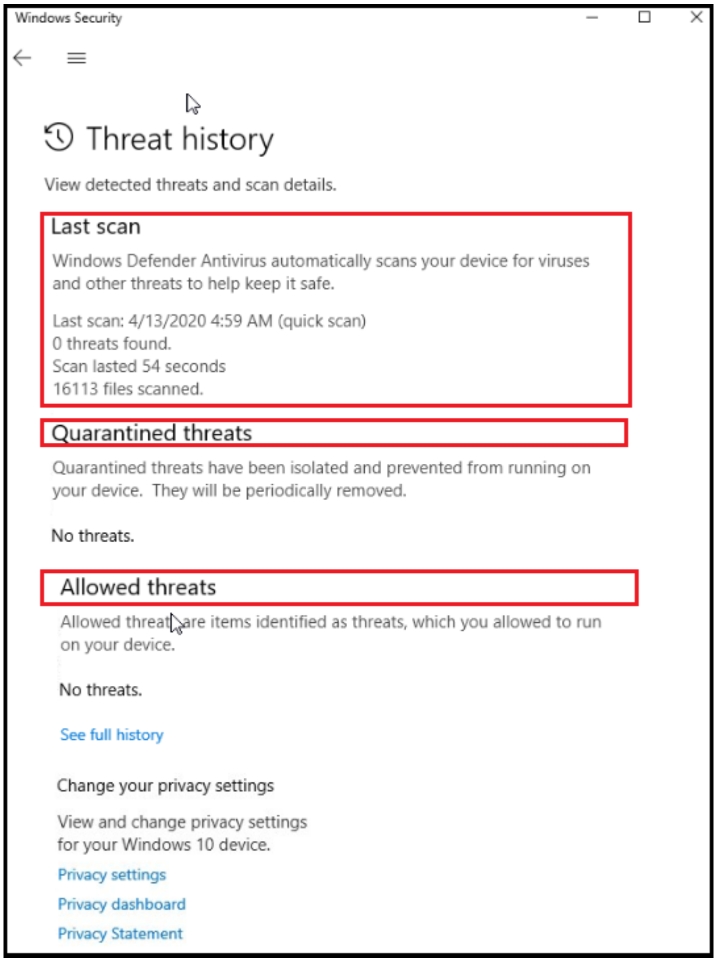
Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 15-07-2024 14:46 (quick scan)
0 threat(s) found.
Scan lasted 8 minutes 26 seconds
15067 files scanned.

2. This page shows you the results of the last scan. You see the files identified as a threat and quarantined, so they cannot damage your device. You then see files identified as potential threats but allowed to continue running.



Threat history

View detected threats and scan details.

Last scan

Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.

Last scan: 4/13/2020 4:59 AM (quick scan)
0 threats found.
Scan lasted 54 seconds
16113 files scanned.

Quarantined threats

Quarantined threats have been isolated and prevented from running on your device. They will be periodically removed.

No threats.

Allowed threats

Allowed threats are items identified as threats, which you allowed to run on your device.

No threats.

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Exercise 4: Run Antivirus Custom Scan

Run a custom scan that only scans the files in the **Downloads** folder.

▸ Click here for a hint.
▸ Click here for the solution.

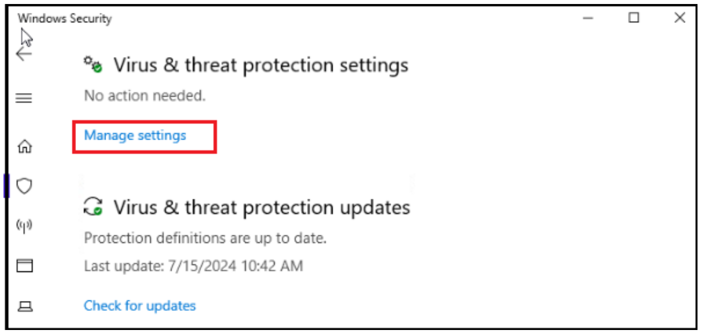
Typical Use cases of Windows Defender Antivirus

Scenario 1

Roshan is an employee working from home and needs to access company resources securely while ensuring his personal computer remains protected from potential threats. Enable Windows Defender Antivirus to secure his system and setup scheduled scans to automatically scan his system fully.

The steps below will help you schedule a weekly full scan using Windows Defender Antivirus via Task Scheduler.

1. **Enable Antivirus Protection**
   - Open Virus Protection:
     - Follow steps 1 to 3 mentioned in Exercise 1 above to open **Virus & threat protection**
   - Enable Virus & Threat Protection:
     - Under the Virus & threat protection settings, click on Manage settings.

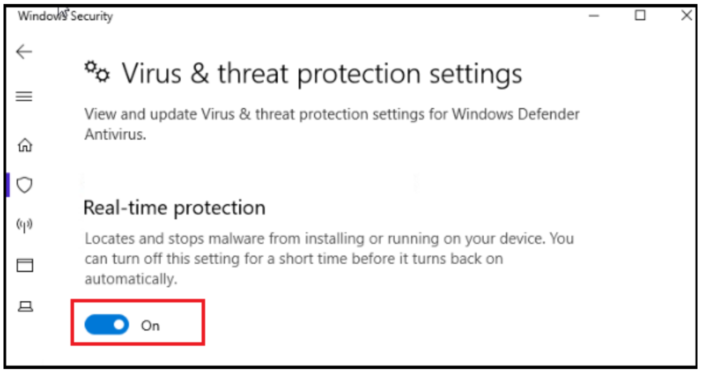

Windows Security
Virus & threat protection settings
Manage settings
Virus & threat protection updates
Check for updates

No action needed.

Protection definitions are up to date.

Last update: 7/15/2024 10:42 AM

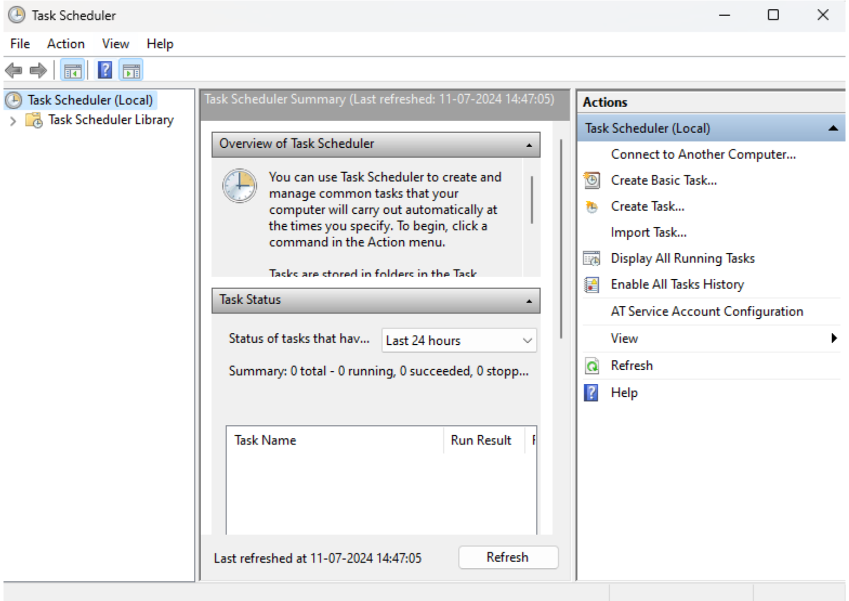
     - Turn **On** Real-time Protection:
       Ensure the Real-time protection toggle is turned on. This will enable continuous monitoring of your system for threats.



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

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.

2. Schedule Weekly scans
   - **Open Task Scheduler**
     - Press `Windows + R`, type `taskschd.msc`, and press Enter to open Task Scheduler.
   - **Create a New Task**
     - In Task Scheduler, click on **Create Task** in the Actions pane on the right.



Task Scheduler Summary (Last refreshed: 11-07-2024 14:47:05)

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

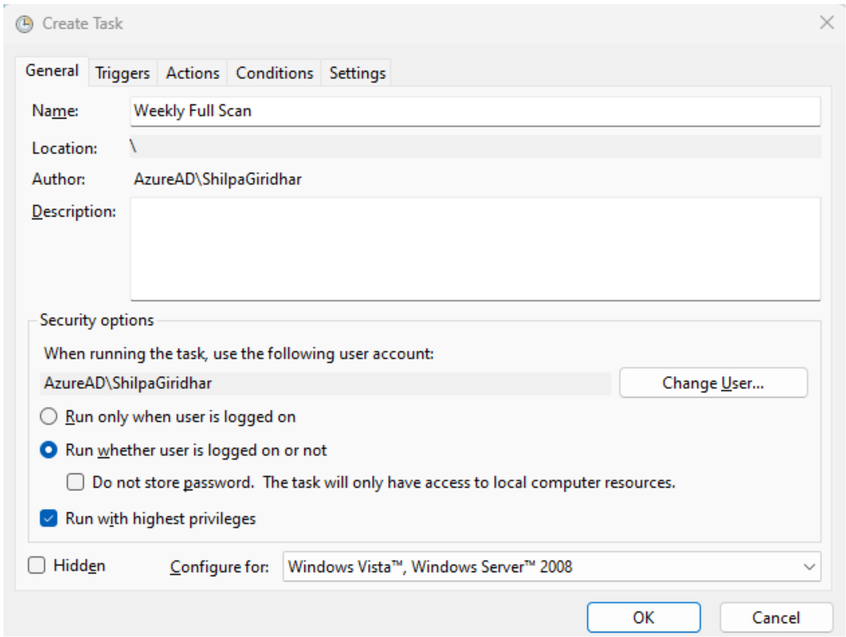
Tasks are stored in folders in the Task

Status of tasks that hav... Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 stopp...

Last refreshed at 11-07-2024 14:47:05

   - **General Settings**
     - In the **General** tab, name your task (e.g., “Weekly Full Scan”).
     - Optionally, add a description.
     - Select **Run whether user is logged on or not**.



Create Task

Name: Weekly Full Scan

Location: \

Author: AzureAD\ShilpaGiridhar

Description:

Security options

When running the task, use the following user account:

AzureAD\ShilpaGiridhar

○ Run only when user is logged on

● Run whether user is logged on or not

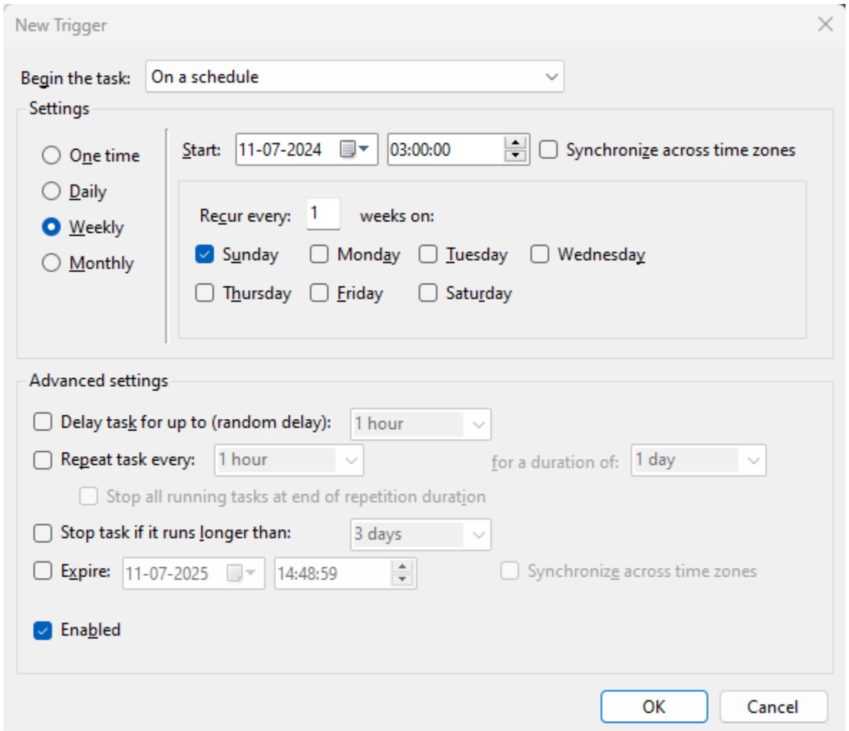
□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

- **Specify Triggers**
  - Go to the **Triggers** tab and click on **New**.
  - Set **Begin the task** to **On a schedule**.
  - Select **Weekly** and set the start time to `3:00 AM`.
  - Choose **Sunday** and click **OK**.



New Trigger

Begin the task: On a schedule

Settings

○ One time

○ Daily

● Weekly

○ Monthly

Start: 11-07-2024 03:00:00 □ Synchronize across time zones

Recur every: 1 weeks on:

☑ Sunday □ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 11-07-2025 14:48:59 □ Synchronize across time zones

☑ Enabled

- **Specify Actions**
  - Go to the **Actions** tab and click on **New**.
  - Set **Action** to **Start a program**.
  - In the **Program/script** field, enter:

```
C:\Program Files\Windows Defender\MpCmdRun.exe
```

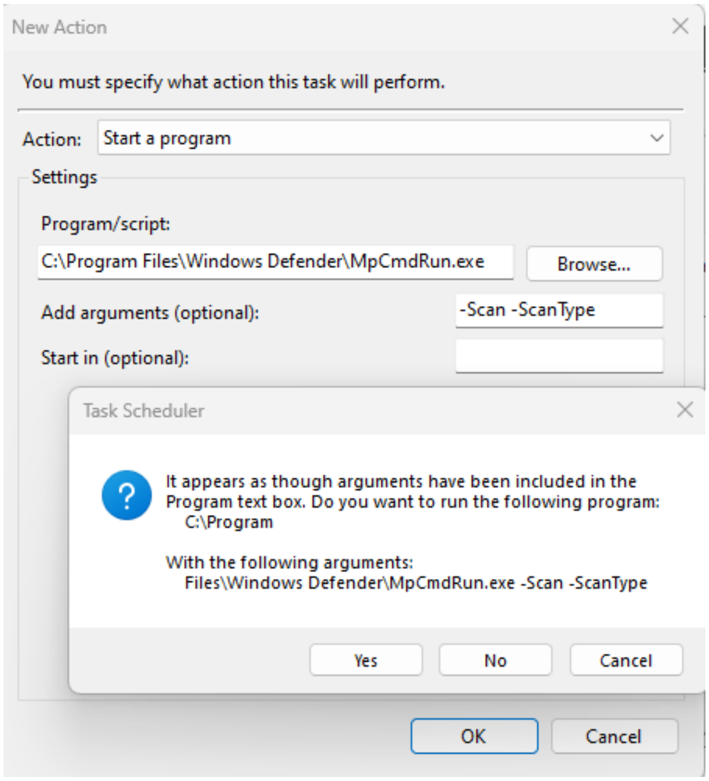
Copied!

  - In the **Add arguments** field, enter:

```
-Scan -ScanType
```

Copied!

  - Click **OK**. You will be promted with confirmation to add arguments to specified program.
  - Click **Yes** to accept this condition.



You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\Program Files\Windows Defender\MpCmdRun.exe

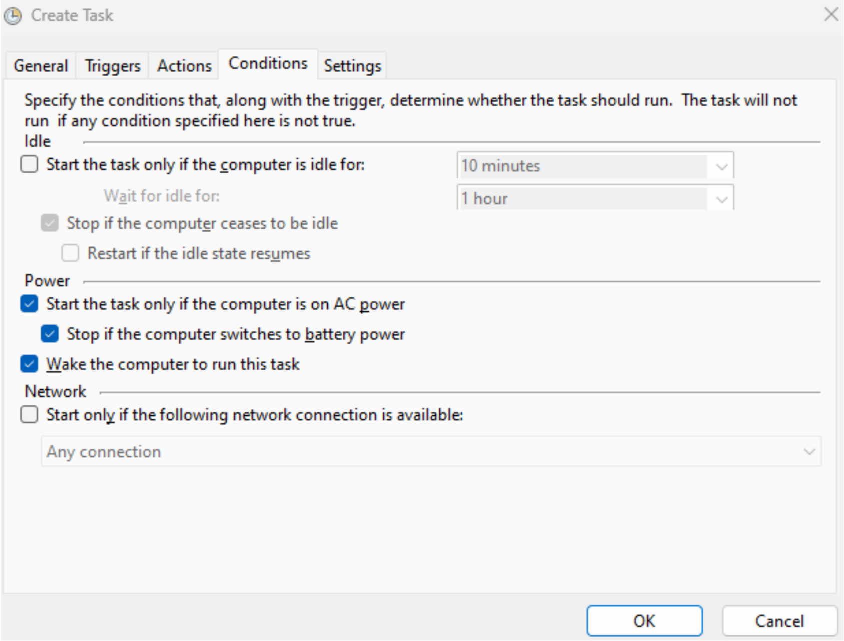
Add arguments (optional): -Scan -ScanType

Start in (optional):

It appears as though arguments have been included in the Program text box. Do you want to run the following program:
C:\Program

With the following arguments:
Files\Windows Defender\MpCmdRun.exe -Scan -ScanType

- **Specify Conditions**
  - Go to the **Conditions** tab.
  - Check **Start the task only if the computer is on AC power** to avoid running the scan on battery power.
  - Optionally, set **Wake the computer to run this task** if your computer is usually asleep at this time.



Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

☑ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

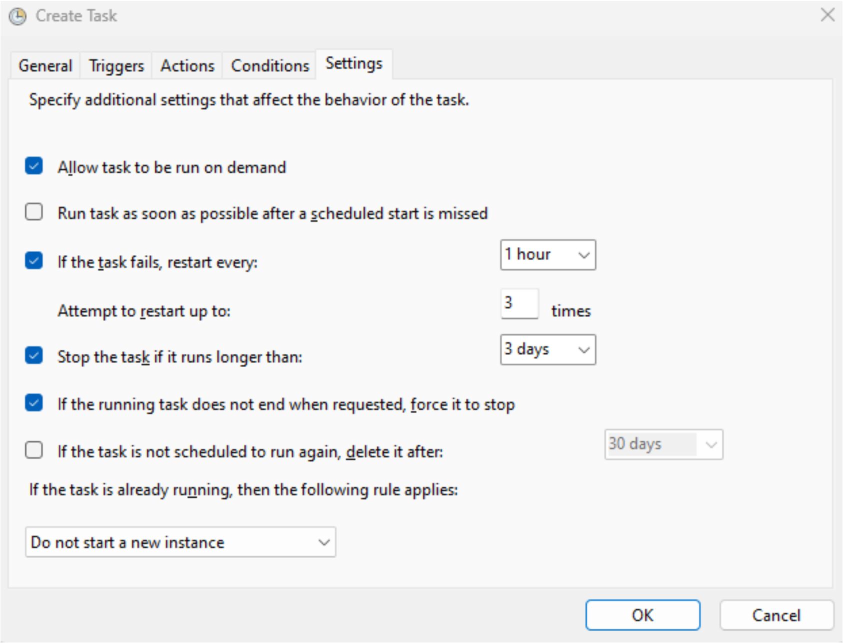
☑ Wake the computer to run this task

Network

□ Start only if the following network connection is available:

Any connection

- **Settings**
  - Go to the **Settings** tab.
  - Check **Allow task to be run on demand**.
  - Ensure **If the task fails, restart every** is checked with **1 hour** and appropriate retry settings.
  - Click **OK** to save the task.



Create Task

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 1 hour

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

- **Conclusion**

  These steps will schedule a weekly full scan using Windows Defender Antivirus, ensuring your system is regularly checked for threats.

Scenario 2

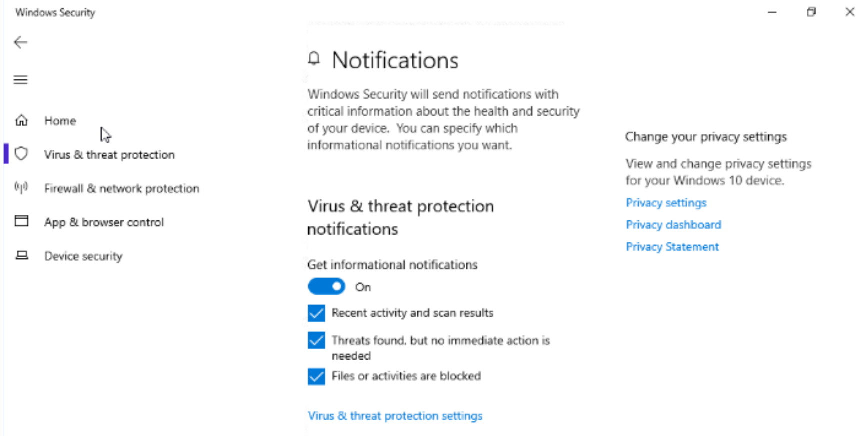
You can simulate downloading a test file that is known to contain harmless malware for testing purposes (such as the EICAR test file) and activate Windows Defender Antivirus to block and quarantine the file.

1. **Enable Antivirus Protection**

   Follow all the steps mentioned in the Scenario 1 to Enable Antivirus Protection.

2. **Enable Notifications**

   - In the Windows Security app, click on Virus & threat protection.
   - Manage Notifications:
     - Scroll down to the Virus & threat protection settings section.
     - Click on **Manage settings**.
     - Scroll down to **Notifications** and click on **Change notification settings**.
   - Enable Notifications:
     - Ensure that the toggles for Recent activity and scan results, Threats found, but no immediate action is needed, and Files or activities are blocked are turned on.



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

Change your privacy settings

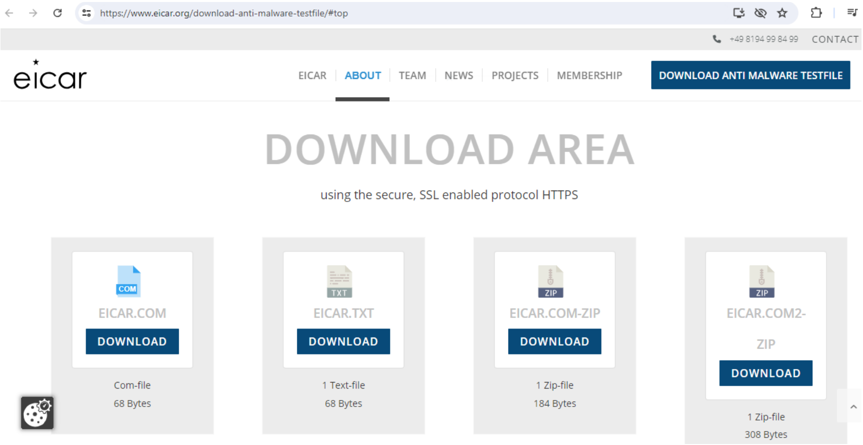
View and change privacy settings for your Windows 10 device.

3. **Download a Sample File for Testing**

The EICAR Anti-Virus Test File, often referred to as the EICAR test file, is a standardized test file developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO). It is designed to safely test the response of antivirus software without the risk of using real malware.

The EICAR test file contains a specific string of characters. When this string is executed or scanned by antivirus software, it should trigger a detection alert.

- Visit the EICAR website:- EICAR's official website.
- On the EICAR download page, you will find links to different versions of the test file (e.g., .com, .txt, .zip).
- Click on the EICAR.COM-ZIP link to download the file.



https://www.eicar.org/download-anti-malware-testfile/#top

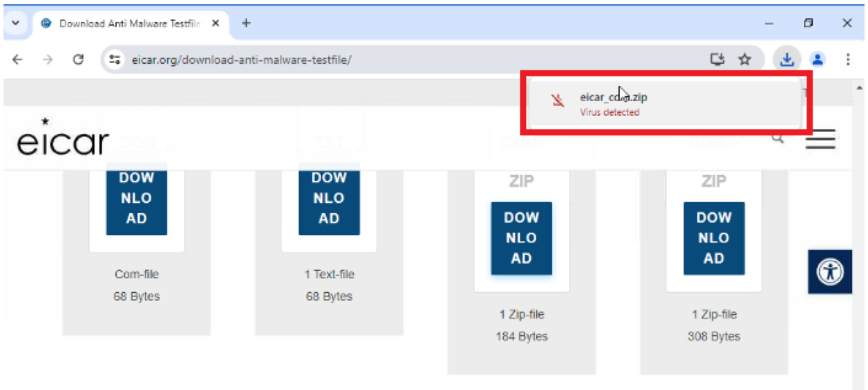
DOWNLOAD AREA

using the secure, SSL enabled protocol HTTPS

EICAR.COM	EICAR.TXT	EICAR.COM-ZIP	EICAR.COM2-ZIP
DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD
Com-file 68 Bytes	1 Text-file 68 Bytes	1 Zip-file 184 Bytes	1 Zip-file 308 Bytes

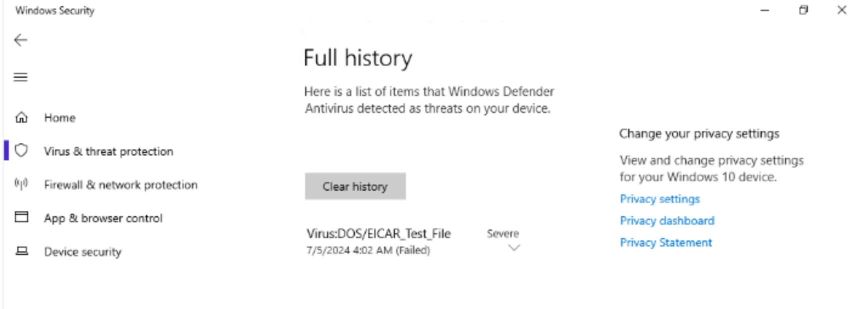
4. **Observing Detection**

- During the download process, observe how Windows Defender reacts. As the file is being written to the disk, Windows Defender scans it in real-time. If the file contains known malware signatures or behaves suspiciously (like trying to modify system settings or files), Windows Defender immediately flags it.
- As soon as the file is detected, Windows Defender triggers an alert. You will see real-time alerts and actions being taken without any need for manual scans.



5. **Reviewing Alerts and Logs**

- Upon detection, Windows Defender takes immediate action. It will quarantine the file, preventing it from executing and spreading malware on the system.
- A notification pops up, informing the user of the detected threat and the action taken. You can click on the notification to open Windows Security or you can open Windows Security and navigate to the “Virus & threat protection” section to view the history of detected items, actions taken, and detailed reports.



Full history

Here is a list of items that Windows Defender Antivirus detected as threats on your device.

Virus:DOS/EICAR_Test_File Severe
7/5/2024 4:02 AM (Failed)

Change your privacy settings

View and change privacy settings for your Windows 10 device.

- Review the threat's severity, the recommended actions, and options for handling the threat.

Conclusion

- Real-time protection continues to monitor the system, scanning other files, and processes in real-time to ensure no other threats are present.

Author(s)

Shilpa Giridhar