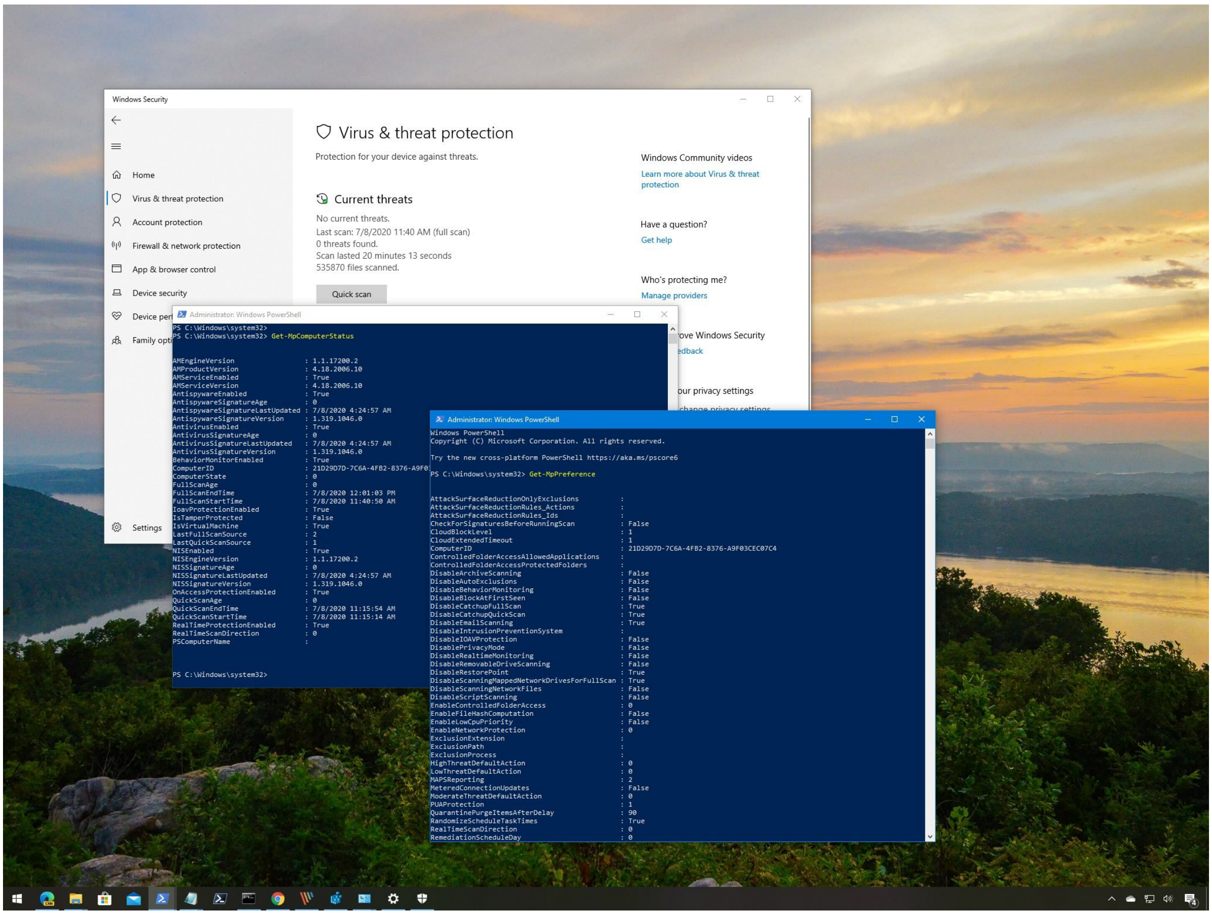
How to manage Microsoft Defender Antivirus with PowerShell on Windows 10

windowscentral.com/how-manage-microsoft-defender-antivirus-powershell-windows-10

Mauro Huculak July 10, 2020

1. Software Apps
2. Windows 10

How-to
By Mauro Huculak
last updated May 18, 2022
You can manage settings and control virtually any aspect of the Microsoft Defender Antivirus using PowerShell commands, and in this guide, we'll help you get started.



Protection for your device against threats.

No current threats.
Last scan: 7/8/2020 11:40 AM (full scan)
0 threats found.
Scan lasted 20 minutes 13 seconds
535870 files scanned.

```
PS C:\Windows\system32>
PS C:\Windows\system32> Get-MpComputerStatus


AMEngineVersion                 : 1.1.17200.2
AMProductVersion                : 4.18.2006.10
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2006.10
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 7/8/2020 4:24:57 AM
AntispywareSignatureVersion     : 1.319.1046.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 7/8/2020 4:24:57 AM
AntivirusSignatureVersion       : 1.319.1046.0
BehaviorMonitorEnabled          : True
ComputerID                      : 21D29D7D-7C6A-4FB2-8376-A9F0
ComputerState                   : 0
FullScanAge                     : 0
FullScanEndTime                 : 7/8/2020 12:01:03 PM
FullScanStartTime               : 7/8/2020 11:40:50 AM
IoavProtectionEnabled           : True
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 2
LastQuickScanSource             : 1
NISEnabled                      : True
NISEngineVersion                : 1.1.17200.2
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 7/8/2020 4:24:57 AM
NISSignatureVersion             : 1.319.1046.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 0
QuickScanEndTime                : 7/8/2020 11:15:54 AM
QuickScanStartTime              : 7/8/2020 11:15:14 AM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Windows\system32>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-MpPreference


AttackSurfaceReductionOnlyExclusions          :
AttackSurfaceReductionRules_Actions           :
AttackSurfaceReductionRules_Ids               :
CheckForSignaturesBeforeRunningScan           : False
CloudBlockLevel                               : 1
CloudExtendedTimeout                          : 1
ComputerID                                    : 21D29D7D-7C6A-4FB2-8376-A9F03CEC07C4
ControlledFolderAccessAllowedApplications     :
ControlledFolderAccessProtectedFolders        :
DisableArchiveScanning                        : False
DisableAutoExclusions                         : False
DisableBehaviorMonitoring                     : False
DisableBlockAtFirstSeen                       : False
DisableCatchupFullScan                        : True
DisableCatchupQuickScan                       : True
DisableEmailScanning                          : True
DisableIntrusionPreventionSystem              :
DisableIOAVProtection                         : False
DisablePrivacyMode                            : False
DisableRealtimeMonitoring                     : False
DisableRemovableDriveScanning                 : False
DisableRestorePoint                           : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles                   : False
DisableScriptScanning                         : False
EnableControlledFolderAccess                  : 0
EnableFileHashComputation                     : False
EnableLowCpuPriority                          : False
EnableNetworkProtection                       : 0
ExclusionExtension                            :
ExclusionPath                                 :
ExclusionProcess                              :
HighThreatDefaultAction                       : 0
LowThreatDefaultAction                        : 0
MAPSReporting                                 : 2
MeteredConnectionUpdates                      : False
ModerateThreatDefaultAction                   : 0
PUAProtection                                 : 1
QuarantinePurgeItemsAfterDelay                : 90
RandomizeScheduleTaskTimes                    : True
RealTimeScanDirection                         : 0
RemediationScheduleDay                        : 0
```

Microsoft Defender Antivirus PowerShell (Image credit: Windows Central)
On Windows 10, Microsoft Defender Antivirus (formerly Windows Defender Antivirus) is part of the Windows Security experience, and it provides a robust real-time protection against unwanted viruses, ransomware, spyware, rootkits, and many other forms of malware and hackers. It even happens to be one of our best antivirus software picks.

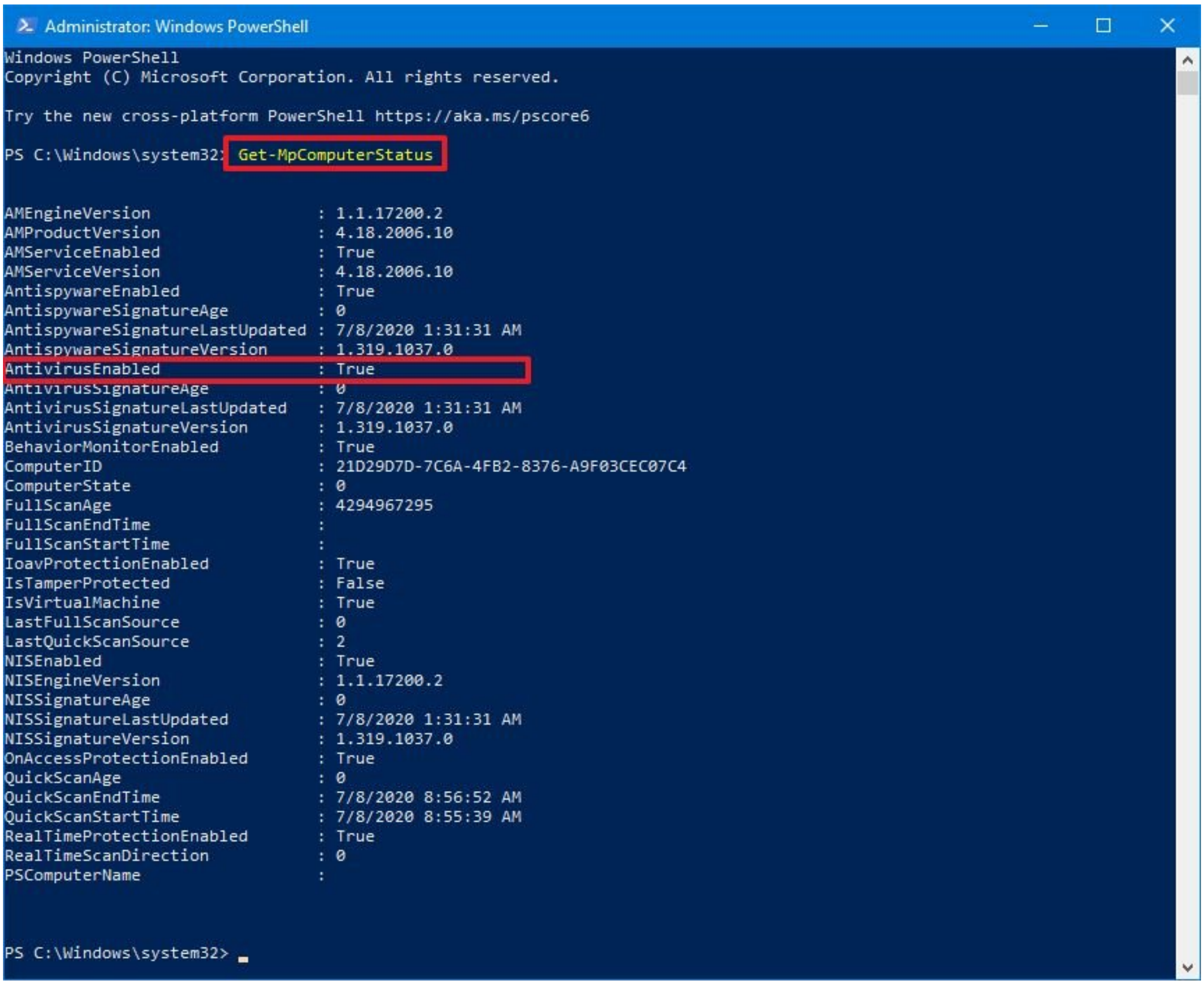
Although you can easily control everyday antivirus tasks through the Windows Security app, you can also manage the anti-malware solution using PowerShell commands, which can come in handy in many scenarios. For example, when you're trying to customize an option that happens not to be available via the graphical user interface (GUI), such as schedule a quick or full scan or signature update. You need to create scripts to automate some Microsoft Defender tasks. Or using commands instead of a GUI can also speed up the configuration process, especially when you need to apply the same settings on multiple installations of Windows 10.

In this Windows 10 guide, we'll walk you through the steps to get started managing Microsoft Defender Antivirus with PowerShell commands.

How to check status of Microsoft Defender

To check the current status of Microsoft Defender using PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to see the Microsoft Defender Antivirus status and press **Enter**:`Get-MpComputerStatus`
4. Confirm the **AntivirusEnabled** is reads **True** to know if the security solution is running.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-MpComputerStatus


AMEngineVersion                 : 1.1.17200.2
AMProductVersion                : 4.18.2006.10
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2006.10
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 7/8/2020 1:31:31 AM
AntispywareSignatureVersion     : 1.319.1037.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 7/8/2020 1:31:31 AM
AntivirusSignatureVersion       : 1.319.1037.0
BehaviorMonitorEnabled          : True
ComputerID                      : 21D29D7D-7C6A-4FB2-8376-A9F03CEC07C4
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.17200.2
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 7/8/2020 1:31:31 AM
NISSignatureVersion             : 1.319.1037.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 0
QuickScanEndTime                : 7/8/2020 8:56:52 AM
QuickScanStartTime              : 7/8/2020 8:55:39 AM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Windows\system32> _
```

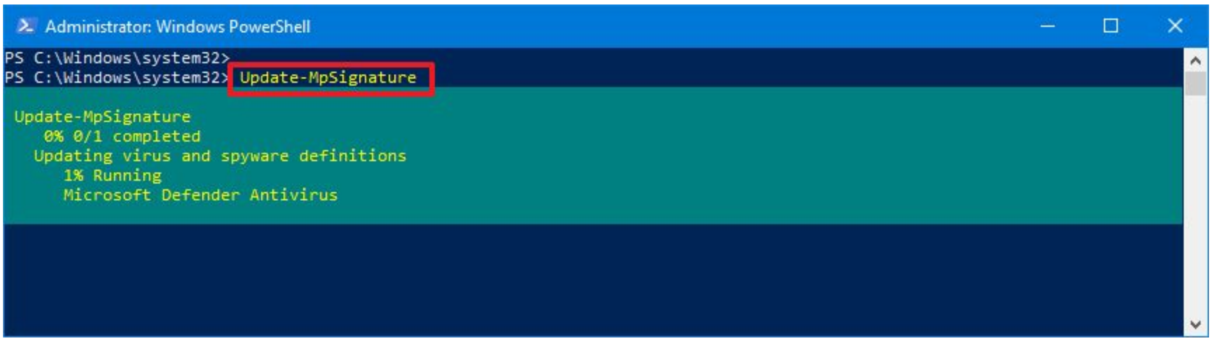
Source: Windows Central (Image credit: Source: Windows Central)

In addition to checking whether the antivirus is running, the command output also displays other important information, such as the version of the engine and product version, real-time protection status, last time updated, and more.

How to check for updates on Microsoft Defender

To use PowerShell to update Microsoft Defender Antivirus with the latest definition, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to check to update Microsoft Defender Antivirus and press **Enter**:`Update-MpSignature`



```
PS C:\Windows\system32>
PS C:\Windows\system32> Update-MpSignature

Update-MpSignature
   0% 0/1 completed
  Updating virus and spyware definitions
     1% Running
     Microsoft Defender Antivirus
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, if new updates are available, they will download and install on your device.

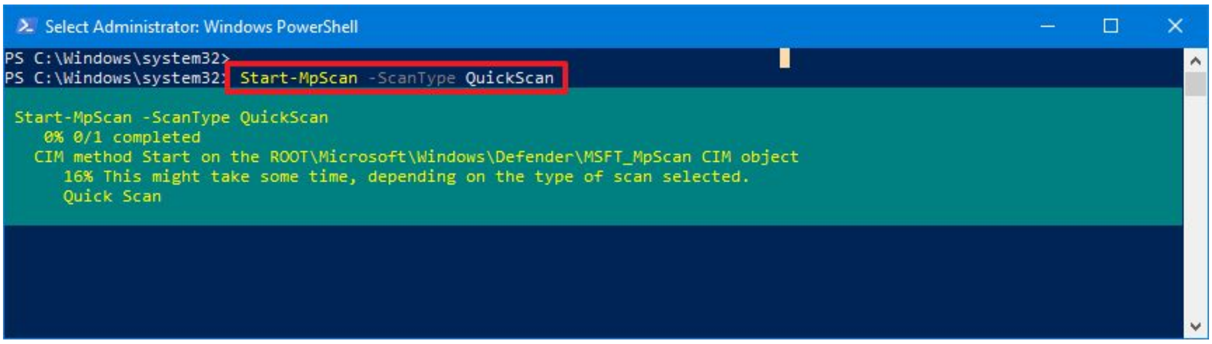
Get the Windows Central Newsletter

All the latest news, reviews, and guides for Windows and Xbox diehards.

How to perform quick virus scan with Microsoft Defender

To complete a quick scan using PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to start a quick virus scan and press **Enter**:`Start-MpScan -ScanType QuickScan`



```
PS C:\Windows\system32>
PS C:\Windows\system32> Start-MpScan -ScanType QuickScan

Start-MpScan -ScanType QuickScan
   0% 0/1 completed
  CIM method Start on the ROOT\Microsoft\Windows\Defender\MSFT_MpScan CIM object
     16% This might take some time, depending on the type of scan selected.
     Quick Scan
```

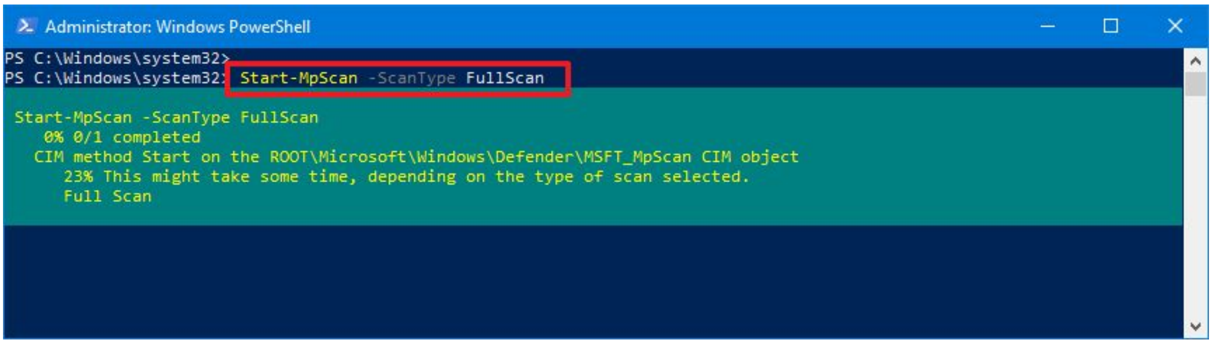
Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, Microsoft Defender Antivirus will perform a quick virus scan on your device.

How to perform full virus scan with Microsoft Defender

To complete a full scan using commands on Windows 10, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to start a full virus scan and press **Enter**:`Start-MpScan -ScanType FullScan`



```
PS C:\Windows\system32>
PS C:\Windows\system32> Start-MpScan -ScanType FullScan

Start-MpScan -ScanType FullScan
   0% 0/1 completed
  CIM method Start on the ROOT\Microsoft\Windows\Defender\MSFT_MpScan CIM object
     23% This might take some time, depending on the type of scan selected.
     Full Scan
```

Source: Windows Central (Image credit: Source: Windows Central)

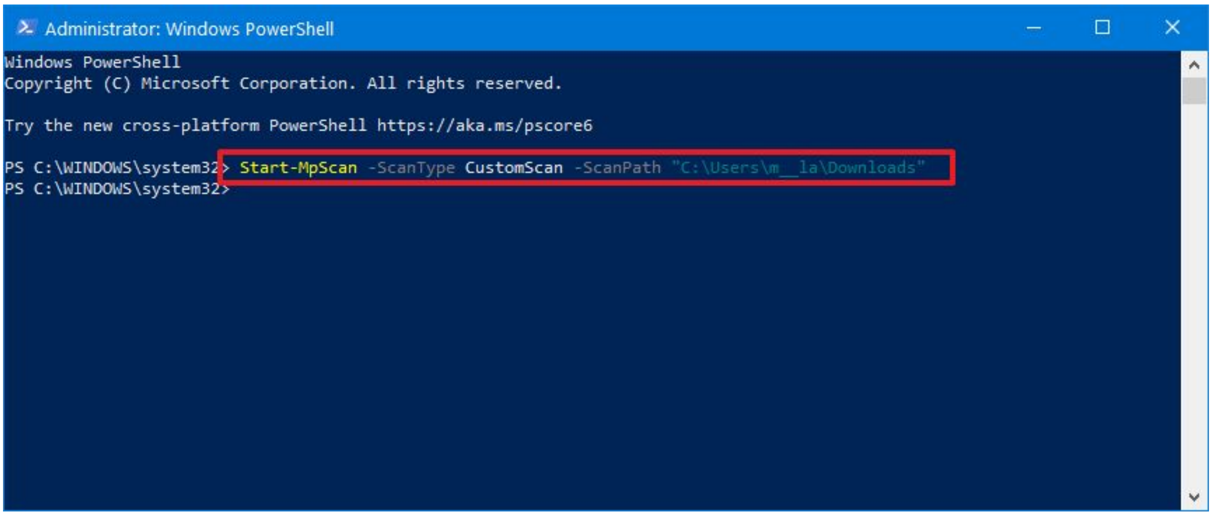
Once you complete the steps, the antivirus for Windows 10 will scan the entire system for any malware and malicious code.

How to perform custom virus scan with Microsoft Defender

To set up a custom scan using PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.

3. Type the following command to perform a custom Microsoft Defender Antivirus scan and press **Enter**:`Start-MpScan -ScanType CustomScan -ScanPath PATH\TO\FOLDER-FILES`In the command, make sure to update the path with the folder location you want to scan.For example, this command scans the Downloads folder:`Start-MpScan -ScanType CustomScan -ScanPath "C:\Users\user\Downloads"`



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Start-MpScan -ScanType CustomScan -ScanPath "C:\Users\m__la\Downloads"
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, Microsoft Defender will only scan for viruses in the location you specified.

How to perform offline virus scan with Microsoft Defender

Microsoft Defender Antivirus also provides an offline scan option, which will come in handy when an unwanted malware infects the device which the antivirus isn't able to remove while Windows 10 is fully loaded.

To start an offline scan, use these steps:

Quick note: Before proceeding, make sure to save any work you may have open, as the command will immediately restart the device to perform an offline scan.

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to start an offline virus scan and press **Enter**:`Start-MpWDOScan`

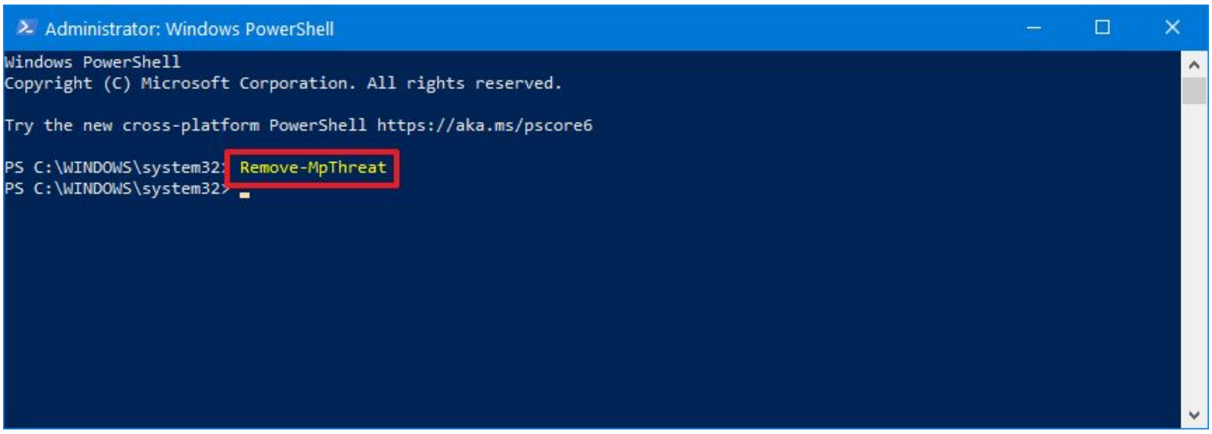
Once you complete the steps, the device will restart automatically. It'll boot into the recovery environment, and it'll perform a full scan to remove viruses that otherwise wouldn't be possible to detect during the normal operation of Windows 10. After the scan, the device will restart automatically, and then you can view the scan report on **Windows Security** > **Virus & thread protection** > **Protection history**.

See this comprehensive guide to learn about offline scanning with Microsoft Defender Antivirus.

How to delete active threat on Microsoft Defender

To remove all active threats from your computer, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to eliminate active threat using Microsoft Defender and press **Enter**:`Remove-MpThreat`



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Remove-MpThreat
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, the anti-malware solution will eliminate any active threats on the computer. Although this is an interesting command, it'll only work for threats that the antivirus hasn't already mitigated.

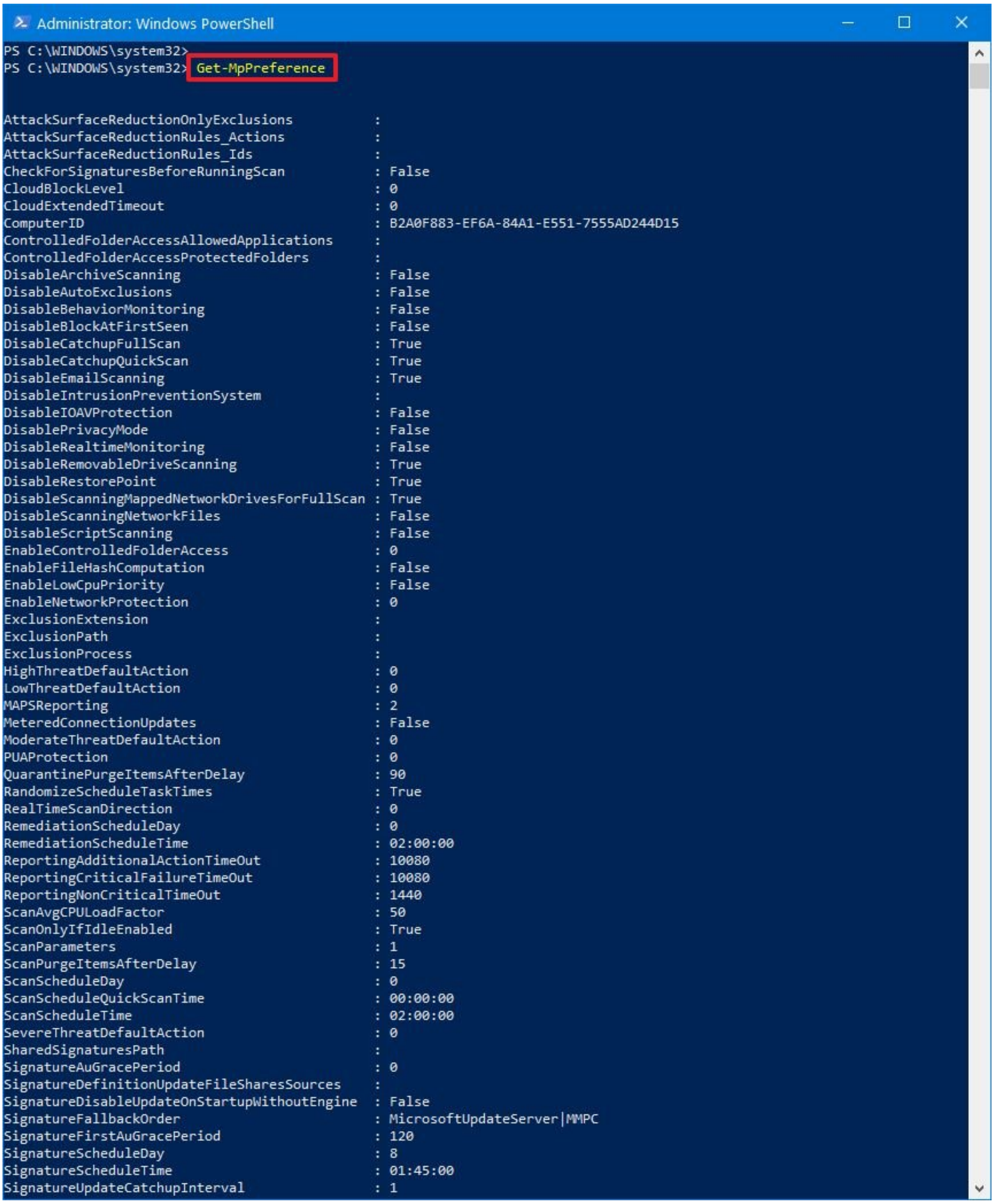
How to change preferences on Microsoft Defender

Using PowerShell commands, it's also possible to configure various features of the Microsoft Defender Antivirus. For example, you can exclude locations and files, specify quarantine retention period, run different scans, schedule virus scans, change scan preferences, and much more.

List preferences

To list all the available preferences for Microsoft Defender with PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to get a full list of the current configurations for the Microsoft Defender Antivirus and press **Enter**:`Get-MpPreference`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-MpPreference


AttackSurfaceReductionOnlyExclusions          :
AttackSurfaceReductionRules_Actions           :
AttackSurfaceReductionRules_Ids               :
CheckForSignaturesBeforeRunningScan           : False
CloudBlockLevel                               : 0
CloudExtendedTimeout                          : 0
ComputerID                                    : B2A0F883-EF6A-84A1-E551-7555AD244D15
ControlledFolderAccessAllowedApplications     :
ControlledFolderAccessProtectedFolders        :
DisableArchiveScanning                        : False
DisableAutoExclusions                         : False
DisableBehaviorMonitoring                     : False
DisableBlockAtFirstSeen                       : False
DisableCatchupFullScan                        : True
DisableCatchupQuickScan                       : True
DisableEmailScanning                          : True
DisableIntrusionPreventionSystem              :
DisableIOAVProtection                         : False
DisablePrivacyMode                            : False
DisableRealtimeMonitoring                     : False
DisableRemovableDriveScanning                 : True
DisableRestorePoint                           : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles                   : False
DisableScriptScanning                         : False
EnableControlledFolderAccess                  : 0
EnableFileHashComputation                     : False
EnableLowCpuPriority                          : False
EnableNetworkProtection                       : 0
ExclusionExtension                            :
ExclusionPath                                 :
ExclusionProcess                              :
HighThreatDefaultAction                       : 0
LowThreatDefaultAction                        : 0
MAPSReporting                                 : 2
MeteredConnectionUpdates                      : False
ModerateThreatDefaultAction                   : 0
PUAProtection                                 : 0
QuarantinePurgeItemsAfterDelay                : 90
RandomizeScheduleTaskTimes                    : True
RealTimeScanDirection                         : 0
RemediationScheduleDay                        : 0
RemediationScheduleTime                       : 02:00:00
ReportingAdditionalActionTimeOut              : 10080
ReportingCriticalFailureTimeOut               : 10080
ReportingNonCriticalTimeOut                   : 1440
ScanAvgCPULoadFactor                          : 50
ScanOnlyIfIdleEnabled                         : True
ScanParameters                                : 1
ScanPurgeItemsAfterDelay                      : 15
ScanScheduleDay                               : 0
ScanScheduleQuickScanTime                     : 00:00:00
ScanScheduleTime                              : 02:00:00
SevereThreatDefaultAction                     : 0
SharedSignaturesPath                          :
SignatureAuGracePeriod                        : 0
SignatureDefinitionUpdateFileSharesSources    :
SignatureDisableUpdateOnStartupWithoutEngine  : False
SignatureFallbackOrder                        : MicrosoftUpdateServer|MMPC
SignatureFirstAuGracePeriod                   : 120
SignatureScheduleDay                          : 8
SignatureScheduleTime                         : 01:45:00
SignatureUpdateCatchupInterval                : 1
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, you'll understand all the settings that you can configure with the built-in antivirus.

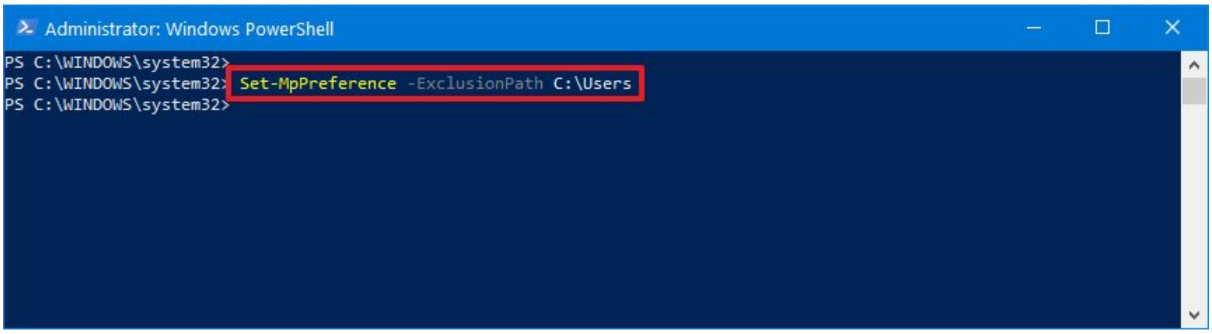
The following commands are some examples of the preferences that you can customize using PowerShell.

Exclude locations

Microsoft Defender Antivirus includes an option to exclude folder locations from real-time and scheduled scanning.

To exclude a folder path with PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to exclude a folder and press **Enter**:`Set-MpPreference -ExclusionPath PATH\TO\FOLDER`In the command, make sure to replace "PATH\TO\FOLDER" with the path you want to exclude.For example, this command excludes the Users folder from being scanned:`Set-MpPreference -ExclusionPath C:\Users`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -ExclusionPath C:\Users
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, Microsoft Defender will ignore the folders you specified during real-time and scheduled scanning.

If you want to remove a folder from the exclusion list, you can use this command:

```
Remove-MpPreference -ExclusionPath &#34;PATH\TO\FOLDER-FILES&#34;
```

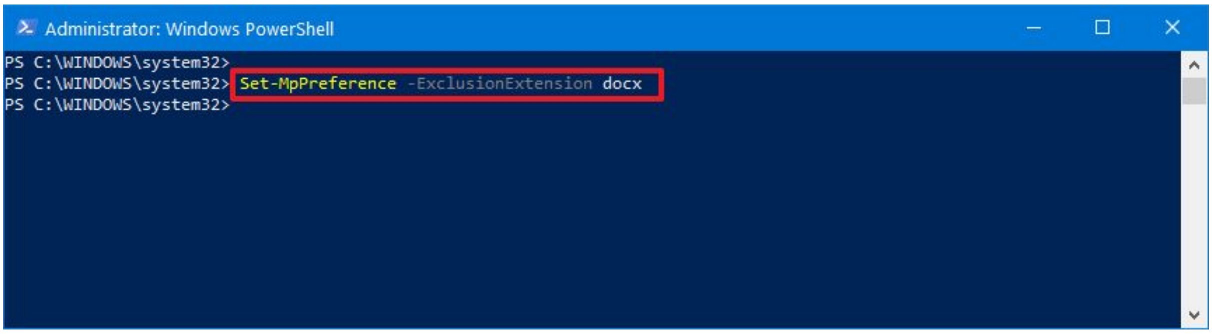
, and don't forget to update the command with the path you wish to remove.

Exclude file type

Also, to exclude locations, you can prevent certain file types from being scan with Microsoft Defender.

To exclude a file type with PowerShell, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to exclude a file type and press **Enter**:`Set-MpPreference -ExclusionExtension EXTENSION`In the command, make sure to replace "EXTENSION" with the extension you want to exclude.For example, this command excludes the Microsoft Word files from being scanned:`Set-MpPreference -ExclusionExtension docx`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -ExclusionExtension docx
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, the file extension will be added to the database of formats that need to be ignored during malware real-time, custom, or scheduled scanning.

If you need to remove an extension from the exclusion list, then you can use this command:

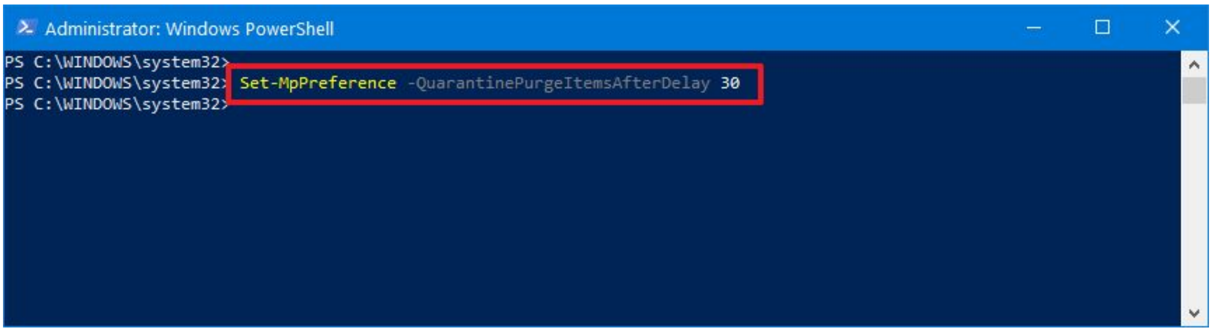
```
Remove-MpPreference -ExclusionExtension EXTENSION
```

and don't forget to update the command with the extension you wish to remove.

Quarantine time before deletion

You can also specify the number of days to keep threats in quarantine with these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to specify the days to keep items in quarantine and press **Enter**:`Set-MpPreference -QuarantinePurgeItemsAfterDelay DAYS`In the command, make sure to replace "DAYS" for the number of days you want to keep items.For example, this command keeps items for 30 days before being deleted:`Set-MpPreference -QuarantinePurgeItemsAfterDelay 30`**Quick tip:** You can use the value of "0" (zero) or no value to set keep items indefinitely.



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -QuarantinePurgeItemsAfterDelay 30
PS C:\WINDOWS\system32>
```

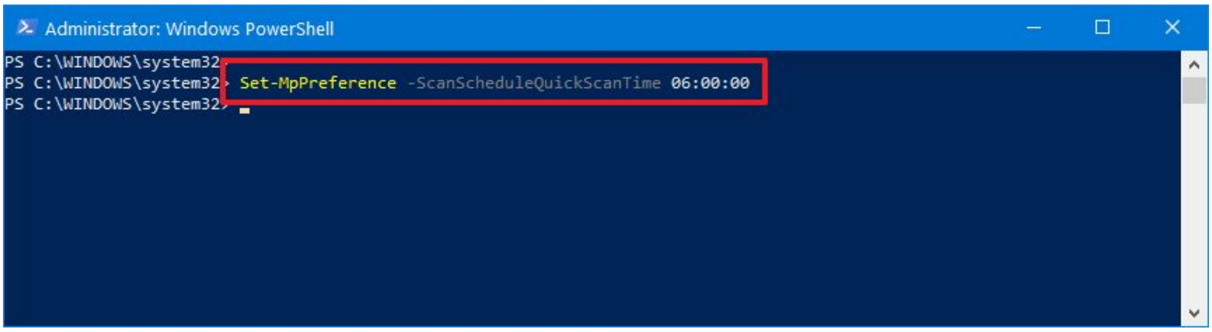
Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, items in the Quarantine folder will be deleted automatically after the period you specified.

Schedule quick scan

To schedule a daily quick malware scan with a PowerShell command, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to schedule a daily quick scan and press **Enter**:`Set-MpPreference -ScanScheduleQuickScanTime SCAN-TIME`In the command, make sure to replace "SCAN-TIME" with the time in 24-hour format you want to run the scan.For example, this command schedules a quick scan every day at 6:00 am, local time:`Set-MpPreference -ScanScheduleQuickScanTime 06:00:00`**Quick tip:** You can specify no time value or set the time to two hours after midnight to reset the settings to their defaults.



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -ScanScheduleQuickScanTime 06:00:00
PS C:\WINDOWS\system32> _
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, Microsoft Defender will perform a quick scan during the time you specified.

Schedule full scan

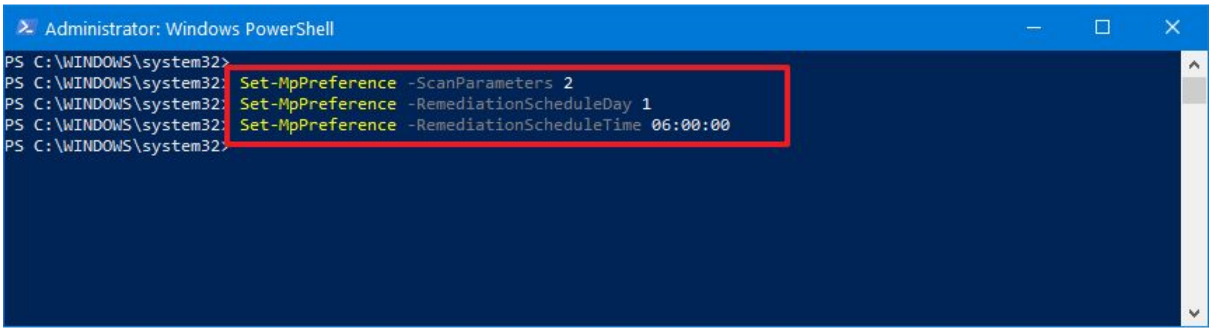
Using PowerShell commands, you can also specify the day and time to perform a full malware scan.

To schedule a full malware scan on Windows 10, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to schedule a full scan and press **Enter**:`Set-MpPreference -ScanParameters 2`**Quick note:** The number "2" in the parameter is what specifies Microsoft Defender a full scan.

4. Type the following command to set a scan day and press **Enter**:`Set-MpPreference -RemediationScheduleDay SCAN-DAY`In the command, change the "SCAN-DAY" for the day (number) you wan to run the scan. Here are the available options:
    - **0 –** Everyday
    - **1 –** Sunday
    - **2 –** Monday
    - **3 –** Tuesday
    - **4 –** Wednesday
    - **5 –** Thursday
    - **6 –** Friday
    - **7 –** Saturday
    - **8 –** Never

   For example, this command schedule the full scan for Sundays:`Set-MpPreference -RemediationScheduleDay 1`**Quick tip:** You can revert to the default scanning schedule using option number `8`.



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -ScanParameters 2
PS C:\WINDOWS\system32> Set-MpPreference -RemediationScheduleDay 1
PS C:\WINDOWS\system32> Set-MpPreference -RemediationScheduleTime 06:00:00
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

5. Type the following command to specify a time for the scan and press **Enter**:`Set-MpPreference -RemediationScheduleTime SCAN-TIME`In the command, change "SCAN-TIME" with the time in 24-hour format you want to run the scan.For example, this command schedules a full scan at 6:00 am, local time:`Set-MpPreference -RemediationScheduleTime 06:00:00`

After you complete the steps, Microsoft Defender Antivirus will run a full scan on the day and time you specified in the preferences.

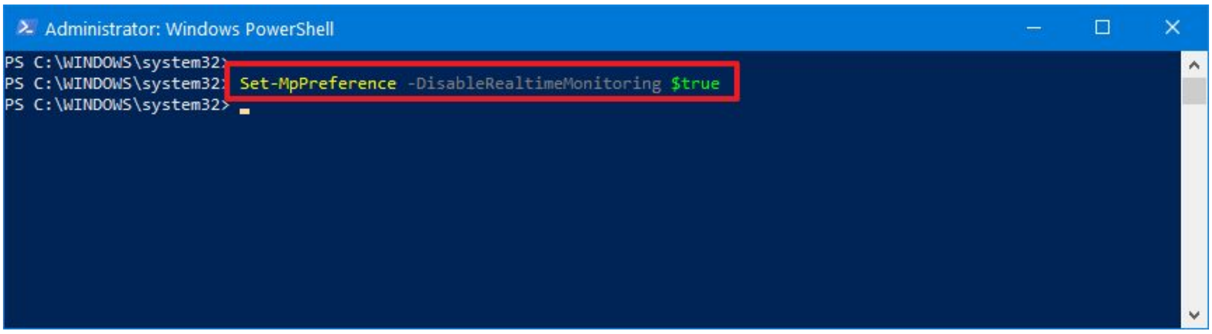
Disable antivirus

Although Microsoft Defender offers a command to disable the antivirus, it's guarded by the **Tamper Protection** feature, which you can only disable through the **Virus & threat protection settings** available in the Windows Security app.

To disable the antivirus, turn off Tamper Protection, and then use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.

3. Type the following command to temporarily disable Microsoft Defender Antivirus and press **Enter**:`Set-MpPreference -DisableRealtimeMonitoring $true`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\WINDOWS\system32> _
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, the real-time antivirus protection will be disabled until the next reboot. Or you can run this command:

```
Set-MpPreference -DisableRealtimeMonitoring $false
```

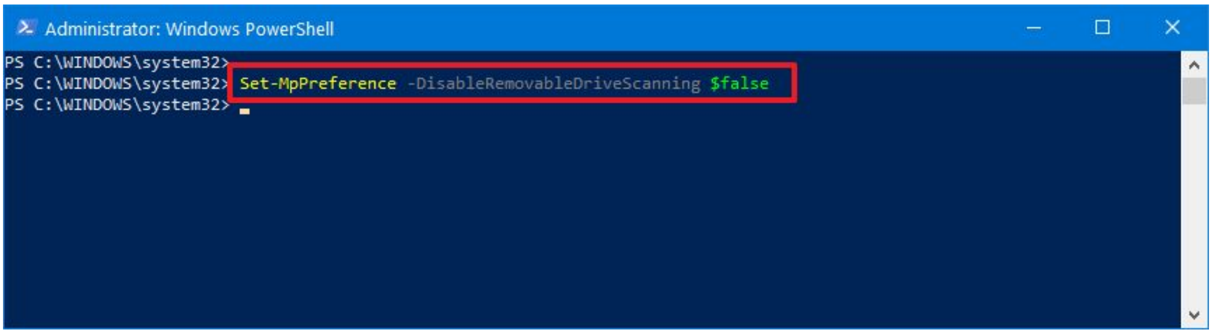
turn on real-time immediately via PowerShell.

If you want to disable the Microsoft Defender Antivirus permanently, you have to follow these instructions.

Enable external drive scanning

By default, the antivirus built-in to Windows 10 doesn't scan for malicious and unwanted programs inside removable storage, but you can change this behavior with these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to allow scanning for removable drives during a quick or full scan and press **Enter**:`Set-MpPreference -DisableRemovableDriveScanning $false`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -DisableRemovableDriveScanning $false
PS C:\WINDOWS\system32> _
```

Source: Windows Central (Image credit: Source: Windows Central)

After you complete the steps, the anti-malware feature will scan external storage devices during a full scan.

If you want to revert the changes, use the same instructions, but on **step No. 3**, use this command:

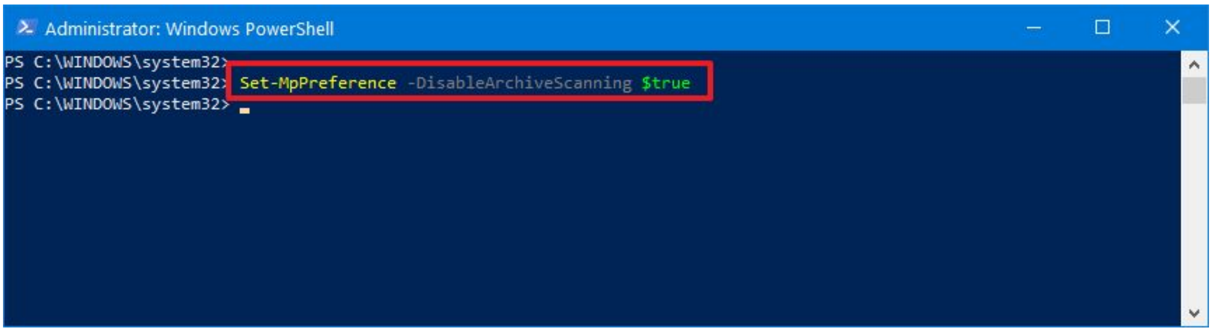
```
Set-MpPreference -DisableRemovableDriveScanning $true
```

.

Disable archive scanning

By default, the antivirus scans .zip, .cab, and other archive files, but if you have a reason not to scan archives, you can disable the option with these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to allow scanning for archives files during a quick or full scan and press **Enter**:`Set-MpPreference -DisableArchiveScanning $true`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -DisableArchiveScanning $true
PS C:\WINDOWS\system32> _
```

Source: Windows Central (Image credit: Source: Windows Central)

Once you complete the steps, Microsoft Defender won't scan archive files.

If you want to undo the settings, you can use the same instructions, but on **step No. 3**, use this command:

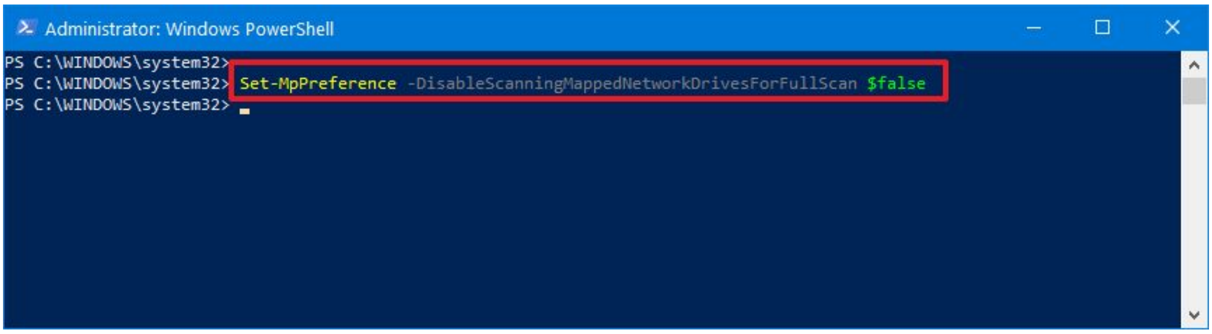
```
Set-MpPreference -DisableArchiveScanning $false
```

.

Enable network drive scanning

To allow Microsoft Defender Antivirus to scan network drives, use these steps:

1. Open **Start**.
2. Search for **PowerShell**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to enable network drive scan during a quick or full scan and press **Enter**:`Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan $false`



```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan $false
PS C:\WINDOWS\system32>
```

Source: Windows Central (Image credit: Source: Windows Central)

After your complete the steps, network drives will be scanned for malicious and unwanted programs during a full scan.

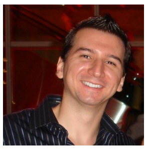
If you want to roll back the original settings, you can use the same instructions, but on **step No. 3**, use this command:

```
Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan $true
```

.

You can always check this Microsoft support page to learn about the settings you can configure for the antivirus.

Mauro Huculak



Mauro Huculak is technical writer for WindowsCentral.com. His primary focus is to write comprehensive how-tos to help users get the most out of Windows 10 and its many related technologies. He has an IT background with professional certifications from Microsoft, Cisco, and CompTIA, and he's a recognized member of the Microsoft MVP community.

TOPICS
Windows 10 Help