WireDiver

Posted on 28 March 2021

← Previous Next →

Disable Windows Defender in powershell – a script to finally get rid of it

Once again, after a Windows update, Windows Defender activated itself again. It finally bothered me enough to take an actual look at how to disable it permanently and reliably, in a fully automated way (a PowerShell script), on my Windows 10 20H2 (build 19042).

WARNING (please read me):
This script is not intended as a "stop/start" solution. It aims at disabeling permanently windows defender, even removing its files if you chose to. I made it as a malware analyst, for my usage, and decided to share it to help others. The "general public" might find another, easier to use solution that suit their need better.
I would also add that some alternative working solutions have been added in the comments of this article (many thanks to their writers !) : it's definitly worth checking.

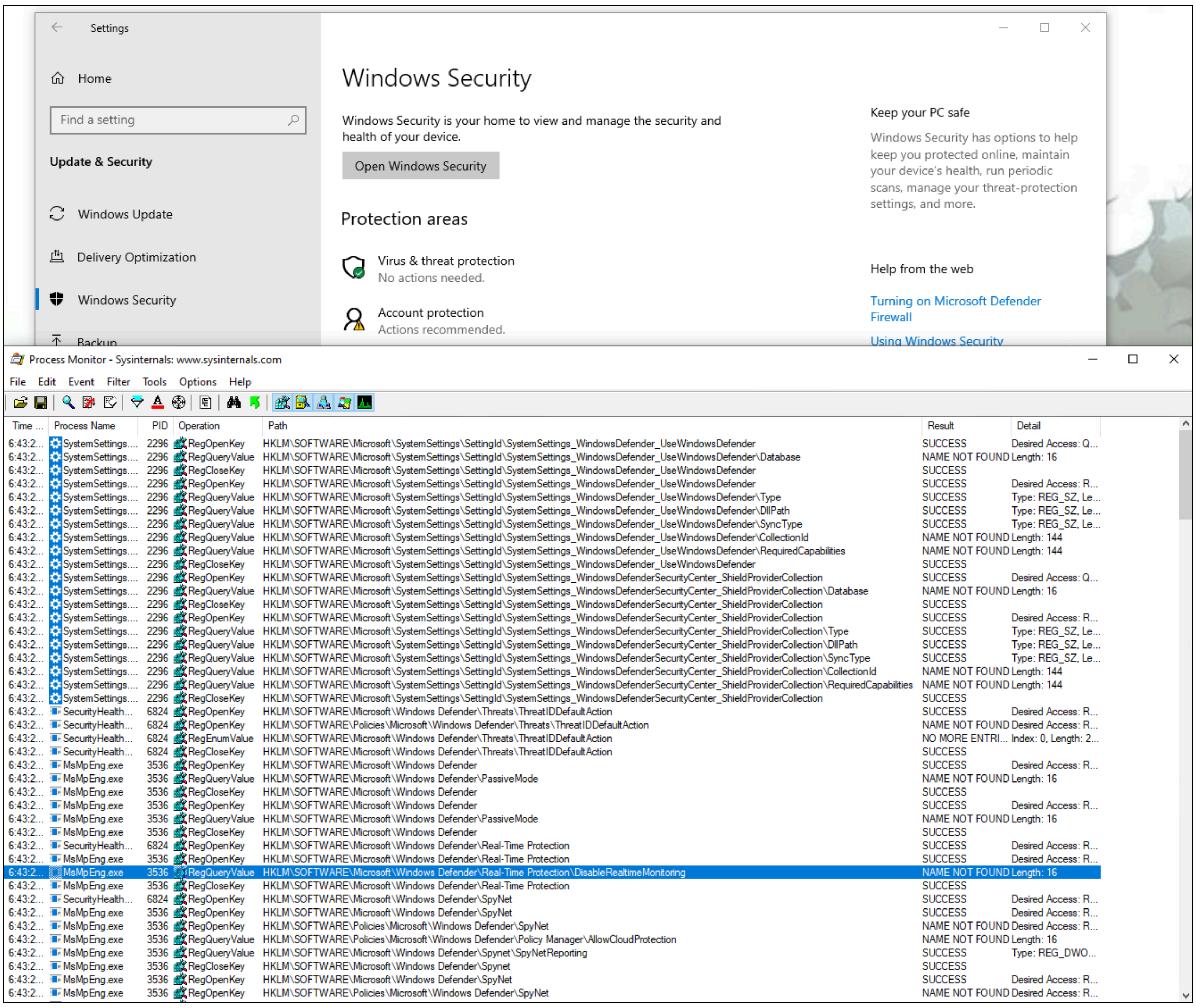
Table of Contents

TL;DR : the final script can be found here : https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1

Registry configuration

First, I took some time to look at the registry configuration, where are the parameters located, and how/when the values were changed. `Procmon`, from SysInternals, is a very convenient tool for this kind of research.

I looked for registry access with "Defender" in the path, and this is the result:



Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Backup

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
Actions recommended.

Keep your PC safe

Windows Security has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

Help from the web

Turning on Microsoft Defender Firewall

Using Windows Security

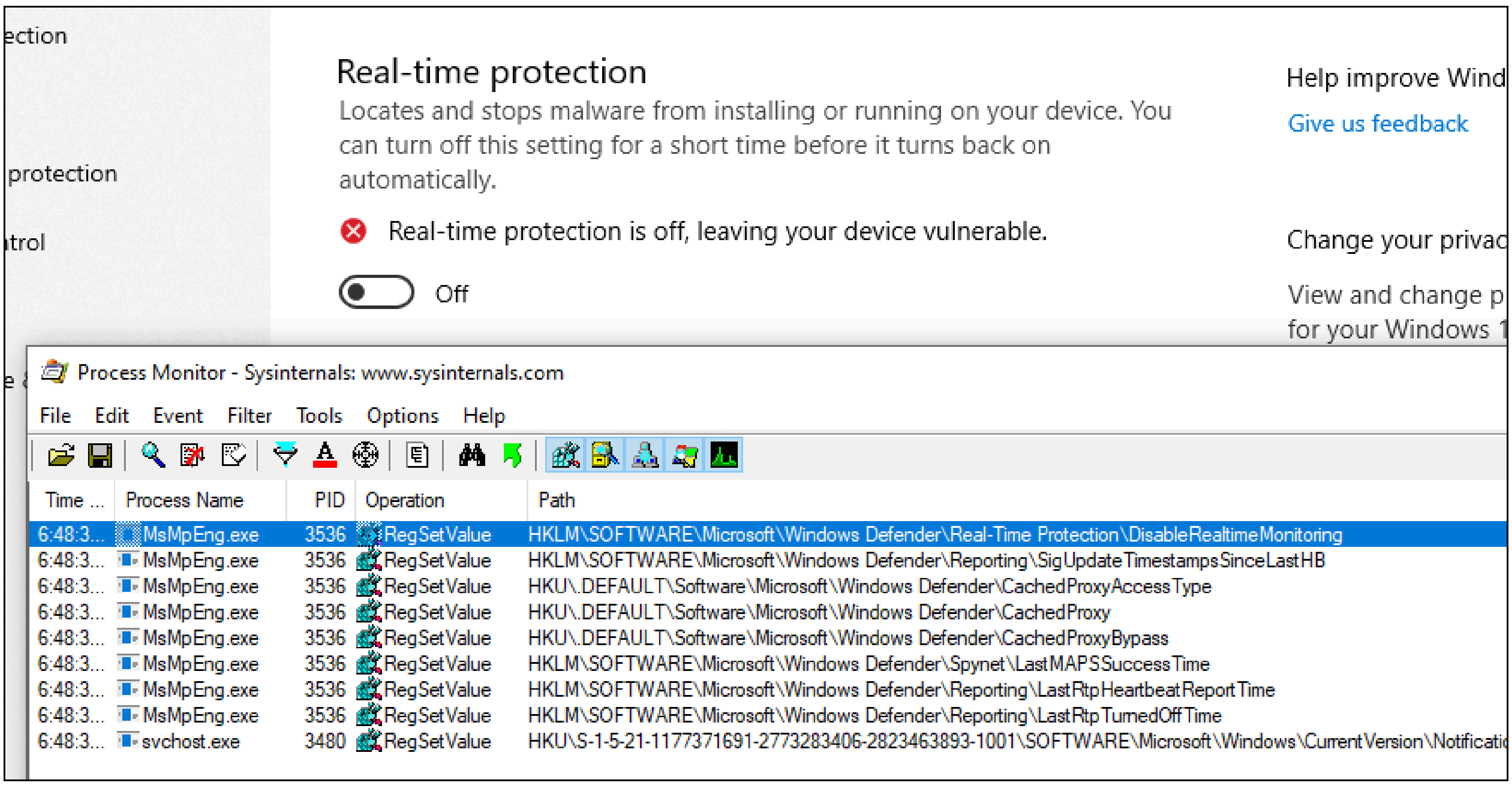
Process Monitor - Sysinternals: www.sysinternals.com

```
Time ...  Process Name      PID   Operation      Path                                                                                                                                 Result            Detail
6:43:2... SystemSettings.... 2296 RegOpenKey     HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender                                  SUCCESS           Desired Access: Q...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\Database                         NAME NOT FOUND    Length: 16
6:43:2... SystemSettings.... 2296 RegCloseKey    HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender                                  SUCCESS
6:43:2... SystemSettings.... 2296 RegOpenKey     HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender                                  SUCCESS           Desired Access: R...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\Type                             SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\DllPath                          SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\SyncType                         SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\CollectionId                     NAME NOT FOUND    Length: 144
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender\RequiredCapabilities             NAME NOT FOUND    Length: 144
6:43:2... SystemSettings.... 2296 RegCloseKey    HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefender_UseWindowsDefender                                  SUCCESS
6:43:2... SystemSettings.... 2296 RegOpenKey     HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection              SUCCESS           Desired Access: Q...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\Database     NAME NOT FOUND    Length: 16
6:43:2... SystemSettings.... 2296 RegCloseKey    HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection              SUCCESS
6:43:2... SystemSettings.... 2296 RegOpenKey     HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection              SUCCESS           Desired Access: R...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\Type         SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\DllPath      SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\SyncType     SUCCESS           Type: REG_SZ, Le...
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\CollectionId NAME NOT FOUND    Length: 144
6:43:2... SystemSettings.... 2296 RegQueryValue  HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection\RequiredCapabilities NAME NOT FOUND Length: 144
6:43:2... SystemSettings.... 2296 RegCloseKey    HKLM\SOFTWARE\Microsoft\SystemSettings\SettingId\SystemSettings_WindowsDefenderSecurityCenter_ShieldProviderCollection              SUCCESS
6:43:2... SecurityHealth...  6824 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction                                                              SUCCESS           Desired Access: R...
6:43:2... SecurityHealth...  6824 RegOpenKey     HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction                                                     NAME NOT FOUND    Desired Access: R...
6:43:2... SecurityHealth...  6824 RegEnumValue   HKLM\SOFTWARE\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction                                                              NO MORE ENTRI...  Index: 0, Length: 2...
6:43:2... SecurityHealth...  6824 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction                                                              SUCCESS
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender                                                                                            SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows Defender\PassiveMode                                                                                NAME NOT FOUND    Length: 16
6:43:2... MsMpEng.exe        3536 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows Defender                                                                                            SUCCESS
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender                                                                                            SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows Defender\PassiveMode                                                                                NAME NOT FOUND    Length: 16
6:43:2... MsMpEng.exe        3536 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows Defender                                                                                            SUCCESS
6:43:2... SecurityHealth...  6824 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection                                                                       SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection                                                                       SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring                                             NAME NOT FOUND    Length: 16
6:43:2... MsMpEng.exe        3536 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection                                                                       SUCCESS
6:43:2... SecurityHealth...  6824 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet                                                                                     SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet                                                                                     SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SpyNet                                                                            NAME NOT FOUND    Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager\AllowCloudProtection                                               NAME NOT FOUND    Length: 16
6:43:2... MsMpEng.exe        3536 RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\SpyNetReporting                                                                     SUCCESS           Type: REG_DWO...
6:43:2... MsMpEng.exe        3536 RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet                                                                                     SUCCESS
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet                                                                                     SUCCESS           Desired Access: R...
6:43:2... MsMpEng.exe        3536 RegOpenKey     HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SpyNet                                                                            NAME NOT FOUND    Desired Access: R...
```

We get a first idea of the configuration location, most interesting keys seems to be under `HKLM\SOFTWARE\Microsoft\Windows Defender`.

Then I proceeded to check the keys for each parameter.

First on the list is the “Real-Time protection”, modifying the key `HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring`



ection

protection

trol

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

Help improve Wind

Give us feedback

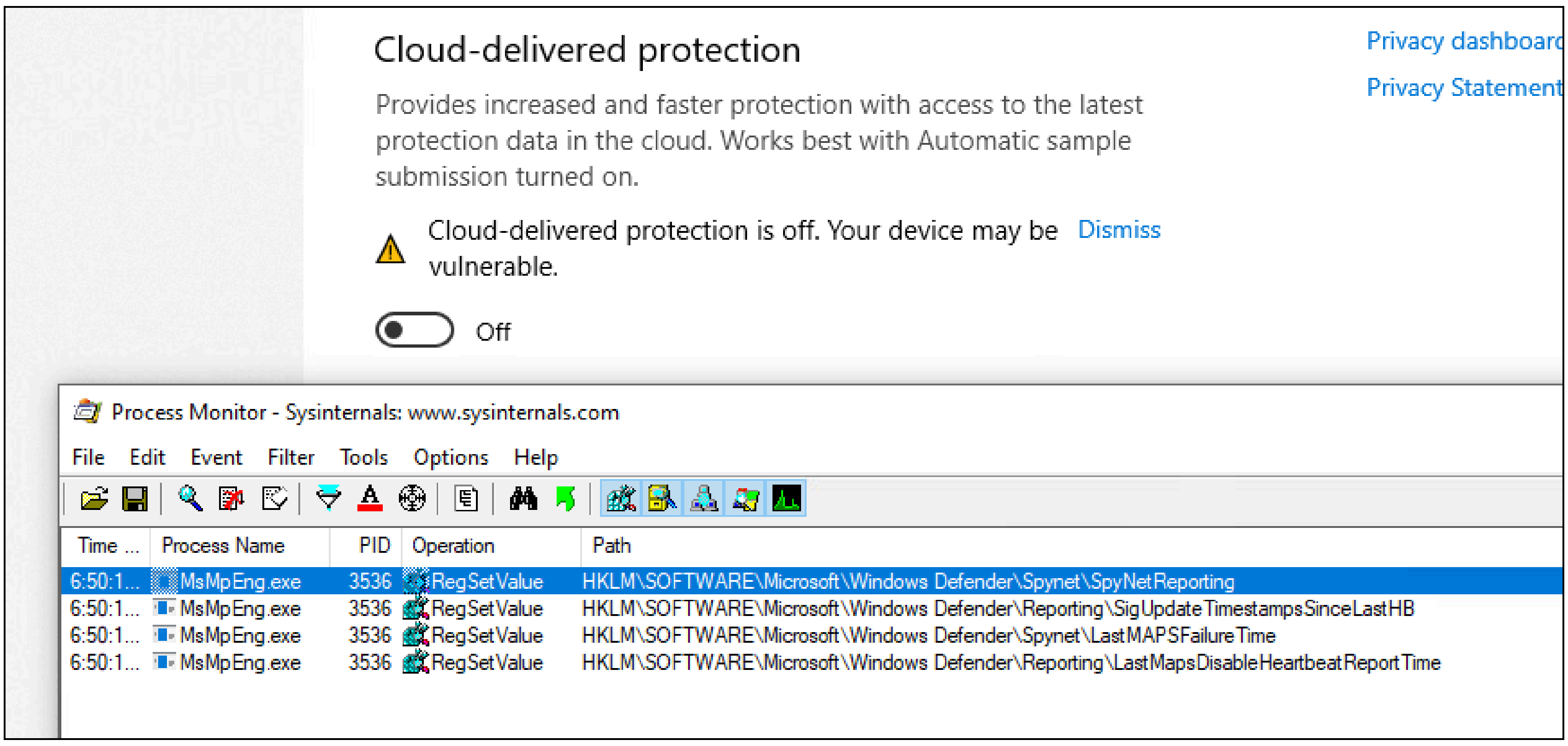
Change your privac

View and change p for your Windows 1

Process Monitor - Sysinternals: www.sysinternals.com

```
Time ...  Process Name  PID   Operation      Path
6:48:3... MsMpEng.exe   3536  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
6:48:3... MsMpEng.exe   3536  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB
6:48:3... MsMpEng.exe   3536  RegSetValue    HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxyAccessType
6:48:3... MsMpEng.exe   3536  RegSetValue    HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxy
6:48:3... MsMpEng.exe   3536  RegSetValue    HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxyBypass
6:48:3... MsMpEng.exe   3536  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\LastMAPSSuccessTime
6:48:3... MsMpEng.exe   3536  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\LastRtpHeartbeatReportTime
6:48:3... MsMpEng.exe   3536  RegSetValue    HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\LastRtpTurnedOffTime
6:48:3... svchost.exe   3480  RegSetValue    HKU\S-1-5-21-1177371691-2773283406-2823463893-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Notificati
```

Then the “cloud-delivered protection”, with the key `HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet\SpyNetReporting` :



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.

⚠ Cloud-delivered protection is off. Your device may be vulnerable.

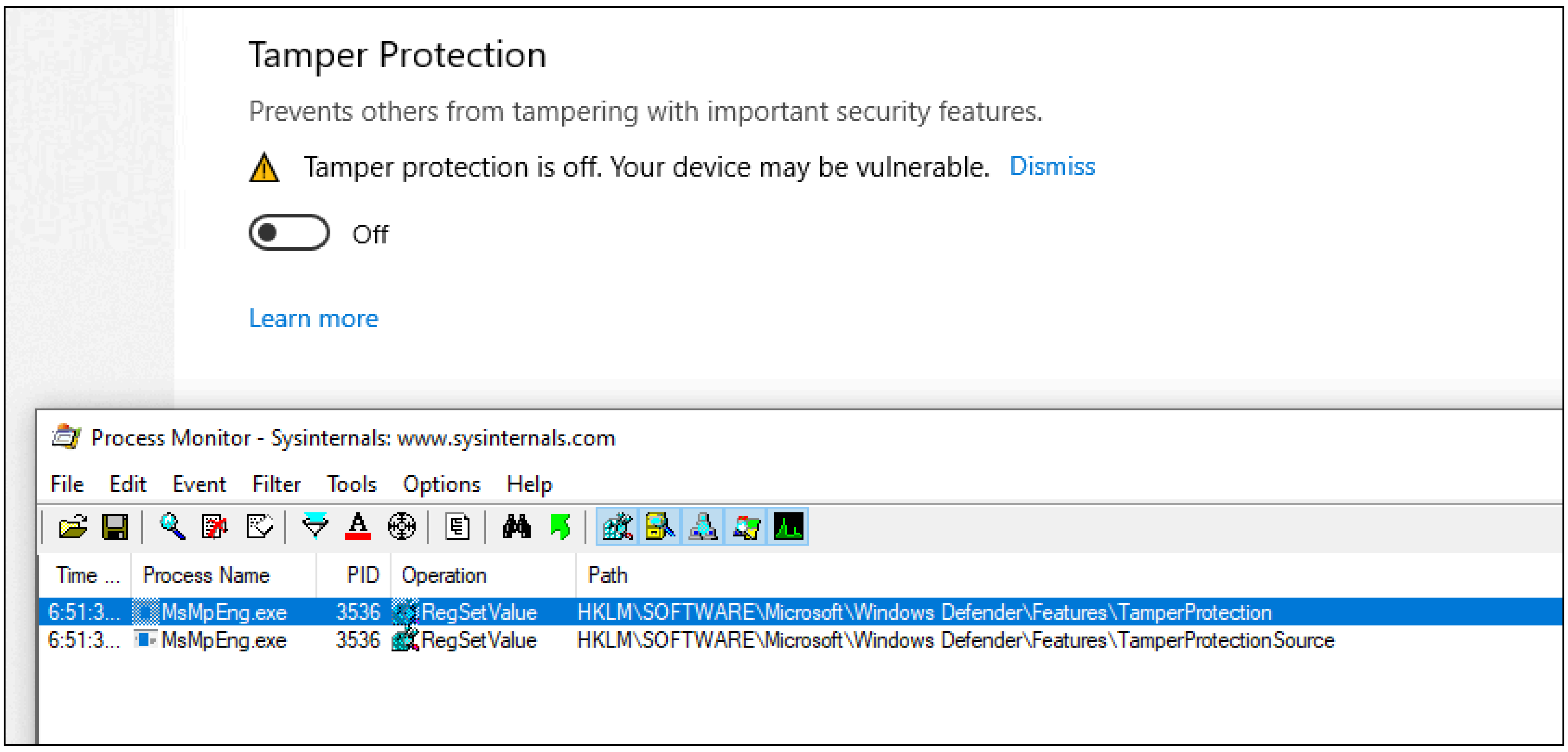
Off

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path
6:50:1...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\SpyNetReporting
6:50:1...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB
6:50:1...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\LastMAPSFailureTime
6:50:1...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\LastMapsDisableHeartbeatReportTime

(For reference, the key for “Automatic sample submission” is `HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet\SubmitSampleConsent`)

The “Tamper Protection” is next, using 2 keys: `HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection` (4 when disabled) and `HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtectionSource` (2 when disabled)



Tamper Protection

Prevents others from tampering with important security features.

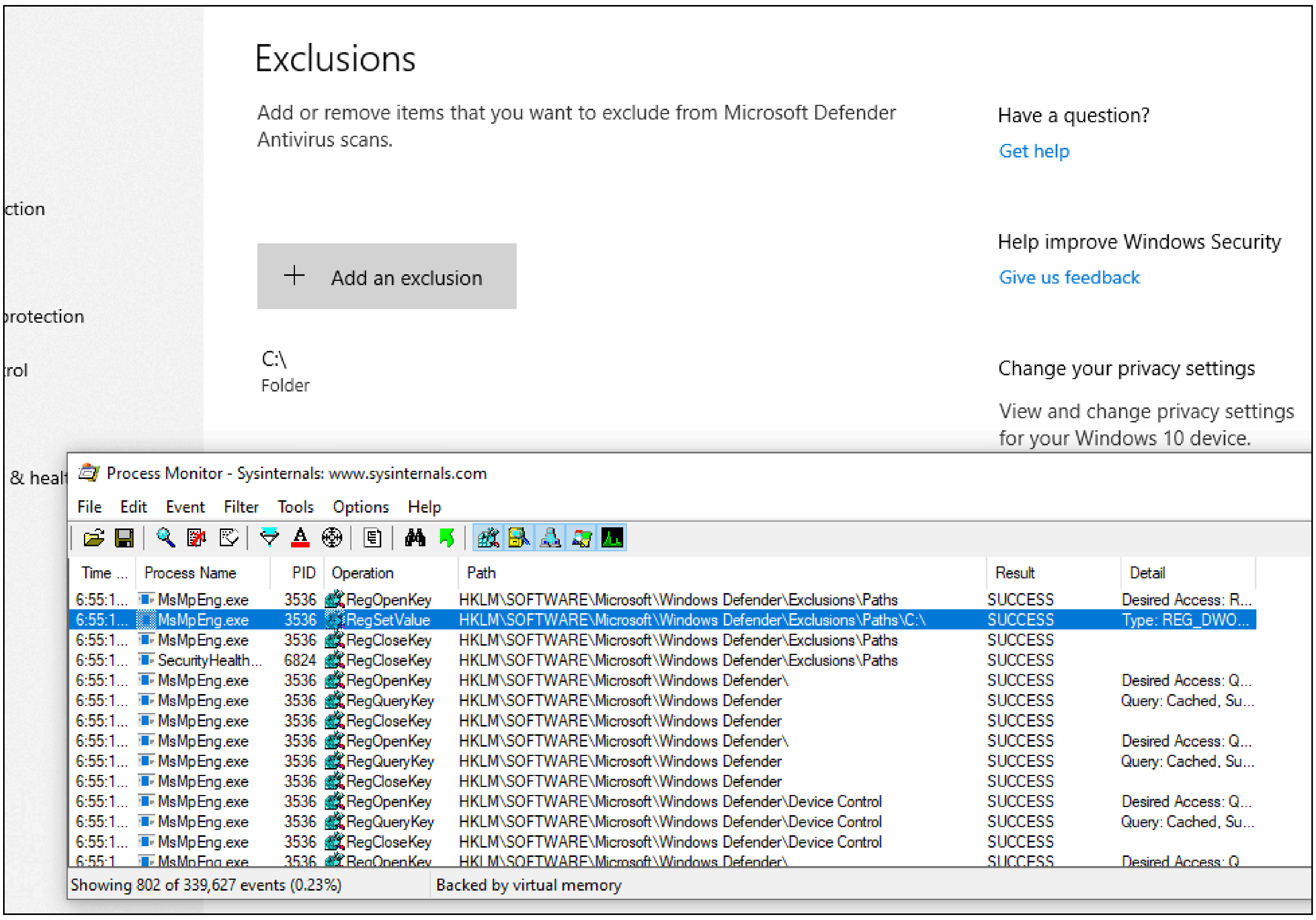
⚠ Tamper protection is off. Your device may be vulnerable.

Off

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path
6:51:3...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection
6:51:3...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtectionSource

And lastly, exclusions are stored in subkeys of `HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions` depending on their type:



Exclusions

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

ction
rotection
rol
& healt
+ Add an exclusion
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings

C:\
Folder

View and change privacy settings for your Windows 10 device.

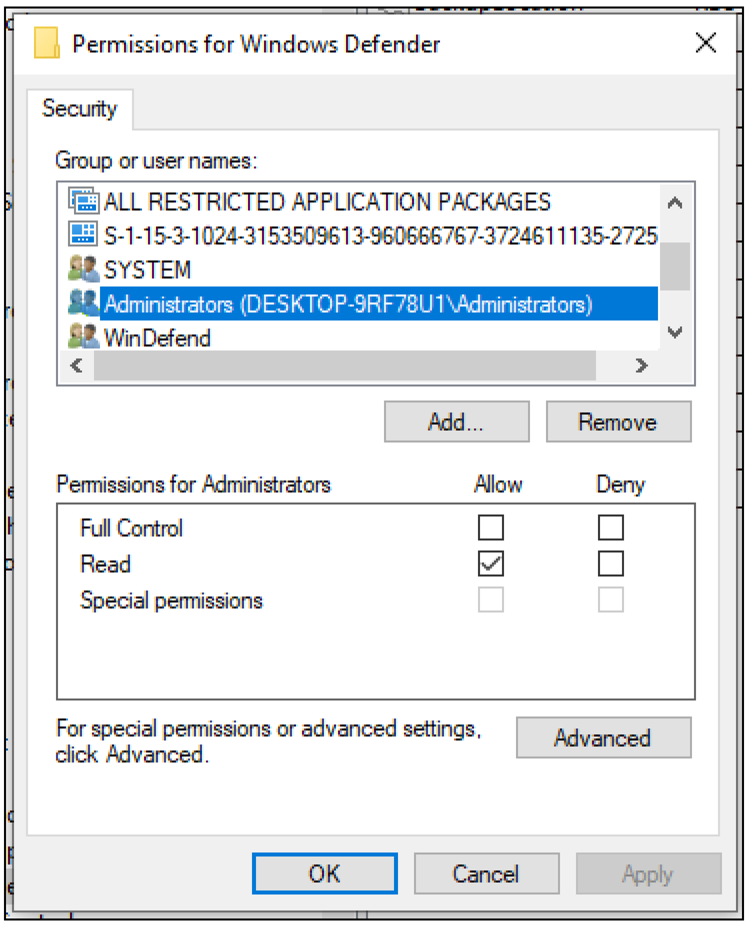
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:55:1...	MsMpEng.exe	3536	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	SUCCESS	Desired Access: R...
6:55:1...	MsMpEng.exe	3536	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\	SUCCESS	Type: REG_DWO...
6:55:1...	MsMpEng.exe	3536	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	SUCCESS	
6:55:1...	SecurityHealth...	6824	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	SUCCESS	
6:55:1...	MsMpEng.exe	3536	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender\	SUCCESS	Desired Access: Q...
6:55:1...	MsMpEng.exe	3536	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows Defender	SUCCESS	Query: Cached, Su...
6:55:1...	MsMpEng.exe	3536	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows Defender	SUCCESS	
6:55:1...	MsMpEng.exe	3536	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender\	SUCCESS	Desired Access: Q...
6:55:1...	MsMpEng.exe	3536	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows Defender	SUCCESS	Query: Cached, Su...
6:55:1...	MsMpEng.exe	3536	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows Defender	SUCCESS	
6:55:1...	MsMpEng.exe	3536	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Device Control	SUCCESS	Desired Access: Q...
6:55:1...	MsMpEng.exe	3536	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Device Control	SUCCESS	Query: Cached, Su...
6:55:1...	MsMpEng.exe	3536	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows Defender\Device Control	SUCCESS	
6:55:1	MsMpEng.exe	3536	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows Defender\	SUCCESS	Desired Access: Q

Showing 802 of 339,627 events (0.23%) Backed by virtual memory

Now, one thing to note is that the Administrator (meaning members of the BUILTIN\Administrators group) cannot change those keys (only SYSTEM can):



Permissions for Windows Defender

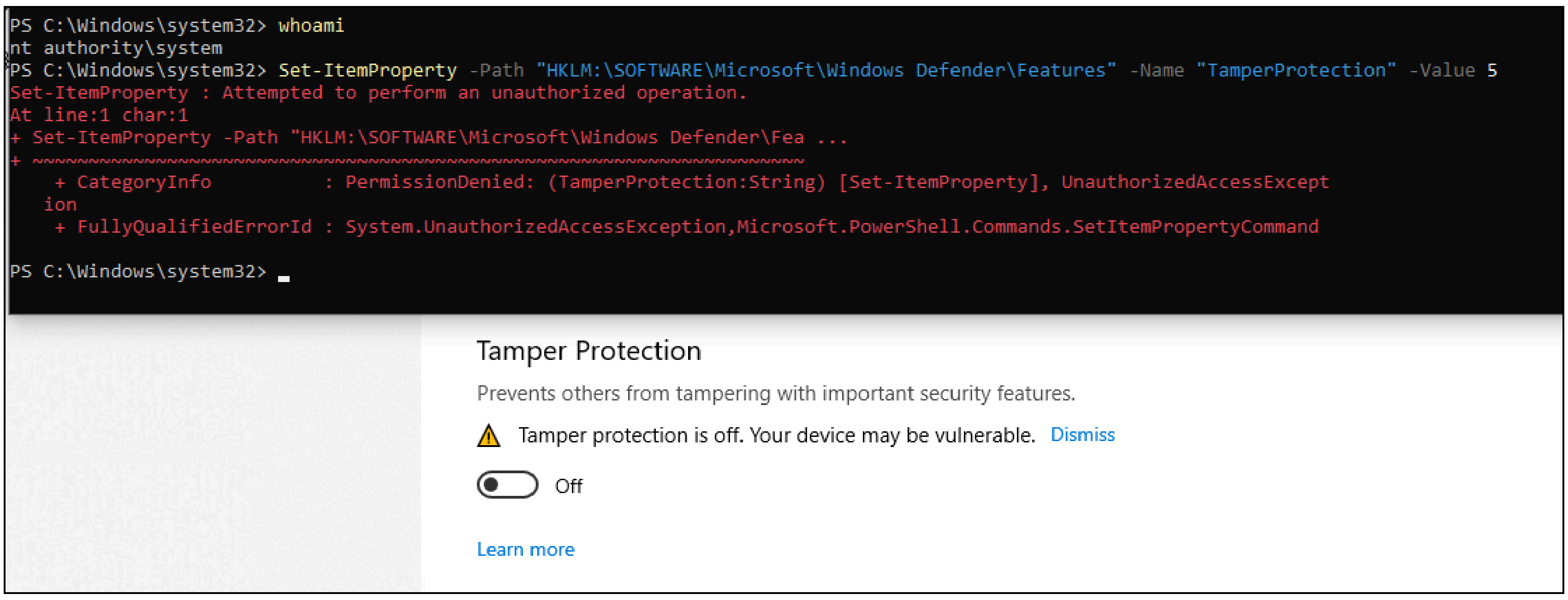
Group or user names:

- ALL RESTRICTED APPLICATION PACKAGES
- S-1-15-3-1024-3153509613-960666767-3724611135-2725
- SYSTEM
- Administrators (DESKTOP-9RF78U1\Administrators)
- WinDefend

Permissions for Administrators	Allow	Deny
Full Control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

An even as SYSTEM, with tamper protection off, writing is still not authorized:



```
PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender\Features" -Name "TamperProtection" -Value 5
Set-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1
+ Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender\Fea ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (TamperProtection:String) [Set-ItemProperty], UnauthorizedAccessExcept
   ion
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

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

Tamper Protection

Prevents others from tampering with important security features.

⚠ Tamper protection is off. Your device may be vulnerable. Dismiss

Off

Learn more

So here we are :

- There is not option to disable "Tamper Protection" in powershel (that's the point ….).
- We can't edit the configuration directly in the registry, even as SYSTEM.

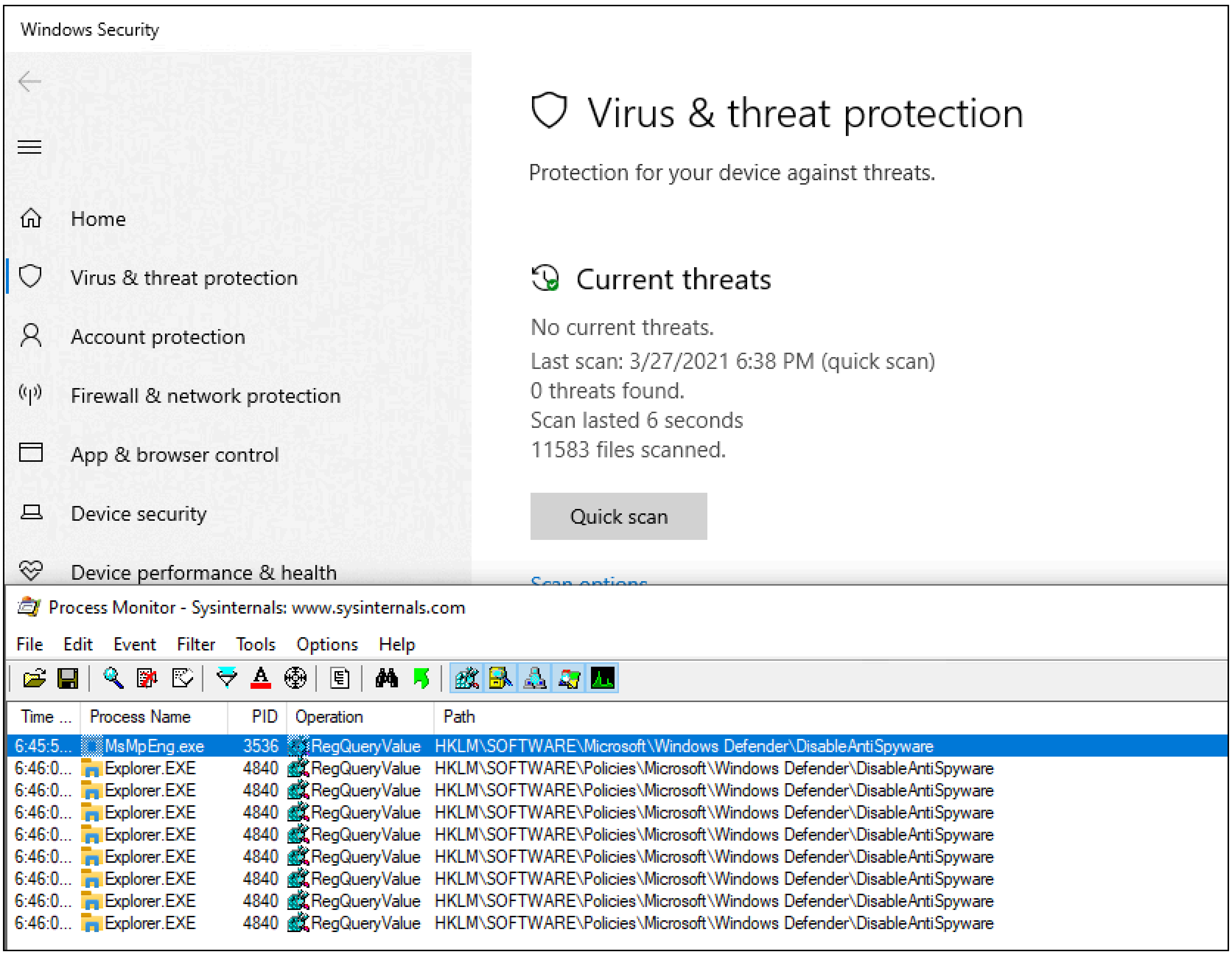
What I used to do was using `Set-MpPreference` to add whole drives as exception, but sometimes I would still get alerts : Defender is still running and analyzing my actions.

Of course, Microsoft provides ways and documentation to disable Defender, so let's check them out.

Disable Defender: the Microsoft way

DisableAntiSpyware

Searching on the internet (like here), there seems to be a registry key for that, named `DisableAntiSpyware`. It is indeed read when opening the configuration:


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Quick scan
Scan options
Process Monitor - Sysinternals: www.sysinternals.com
File
Edit
Event
Filter
Tools
Options
Help

Virus & threat protection

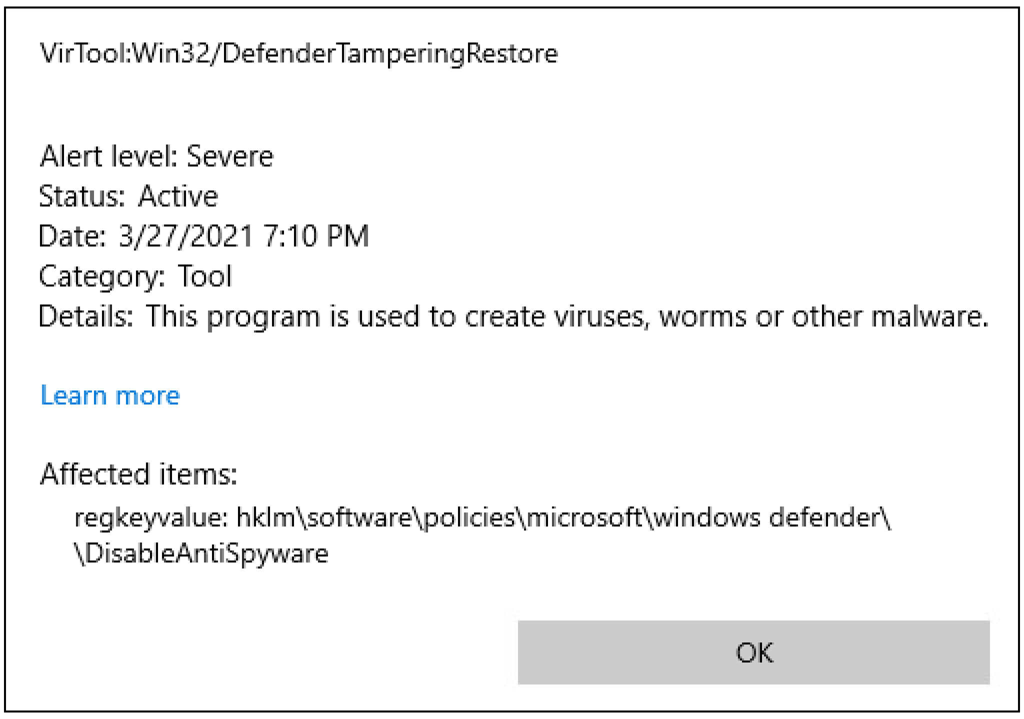
Protection for your device against threats.

Current threats

No current threats.
Last scan: 3/27/2021 6:38 PM (quick scan)
0 threats found.
Scan lasted 6 seconds
11583 files scanned.

```
Time ...  Process Name   PID   Operation      Path
6:45:5... MsMpEng.exe    3536  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
6:46:0... Explorer.EXE   4840  RegQueryValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
```

2 Keys are read, one in the “main configuration” key, and one under `HKLM\SOFTWARE\Policies`. This second one, we can write, to let’s go for it!
I created it, Defender was still running, without warning or anything, so it doesn’t seem to have any effect. But it gets better, it is actually considered a Severe security alert!



VirTool:Win32/DefenderTamperingRestore

Alert level: Severe
Status: Active
Date: 3/27/2021 7:10 PM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

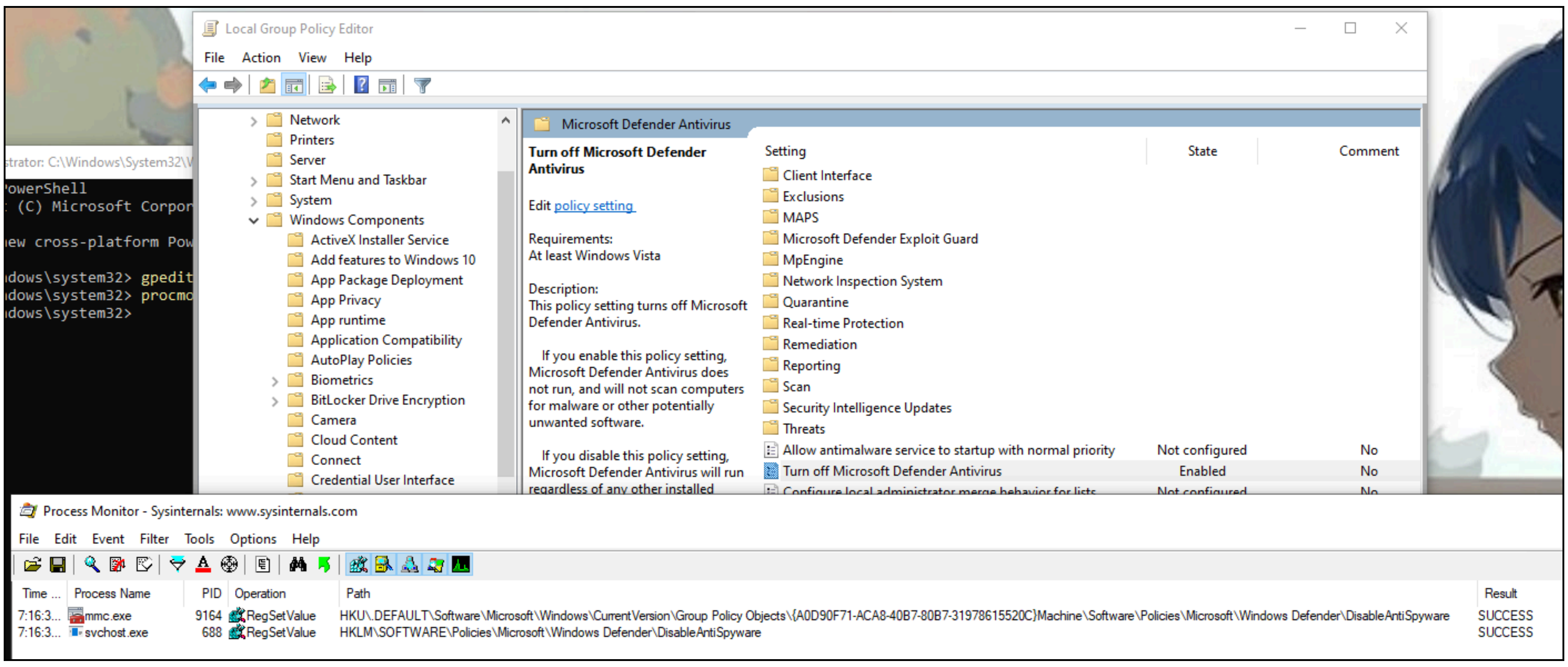
Learn more

Affected items:
regkeyvalue: hklm\software\policies\microsoft\windows defender\\DisableAntiSpyware

Maybe we need to be more subtle, and use `gpedit` to edit this policy, let’s try that!

GPO

Here is what we get when editing the policy with `gpedit` :



```
strator: C:\Windows\System32\W
owerShell
: (C) Microsoft Corpor

ew cross-platform Pow

dows\system32> gpedit
dows\system32> procmo
dows\system32>
```

Turn off Microsoft Defender Antivirus

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting turns off Microsoft Defender Antivirus.

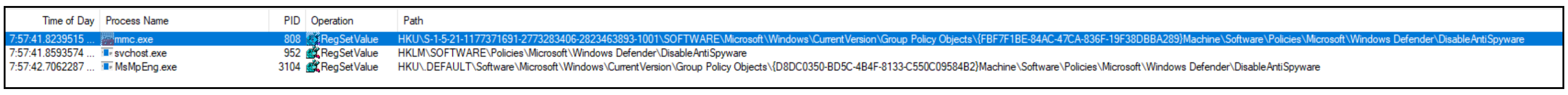
If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.

If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed

Setting	State	Comment
Client Interface		
Exclusions		
MAPS		
Microsoft Defender Exploit Guard		
MpEngine		
Network Inspection System		
Quarantine		
Real-time Protection		
Remediation		
Reporting		
Scan		
Security Intelligence Updates		
Threats		
Allow antimalware service to startup with normal priority	Not configured	No
Turn off Microsoft Defender Antivirus	Enabled	No
Configure local administrator merge behavior for lists	Not configured	No

```
Time ...  Process Name  PID   Operation    Path                                                                                                                                                                      Result
7:16:3... mmc.exe       9164  RegSetValue  HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{A0D90F71-ACA8-40B7-80B7-31978615520C}Machine\Software\Policies\Microsoft\Windows Defender\DisableAntiSpyware  SUCCESS
7:16:3... svchost.exe    688  RegSetValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware                                                                                                      SUCCESS
```

The previous key is actually written by a service (`svchost.exe -k netsvcs -p -s gpsvc`) and another one is written in a policy object. This time is doesn’t raise a security alert, so the second key must be necessary. I also noted that a 3rd key is written when the tamper protection is off:



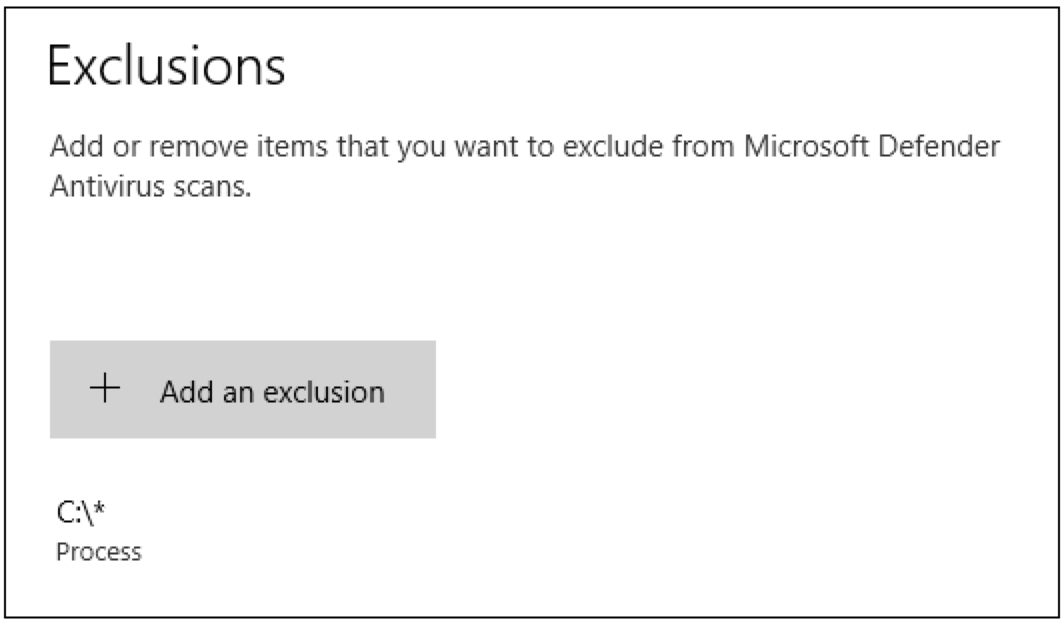
```
Time of Day       Process Name  PID   Operation    Path
7:57:41.8239515 ... mmc.exe       808   RegSetValue  HKU\S-1-5-21-1177371691-2773283406-2823463893-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{FBF7F1BE-84AC-47CA-836F-19F38DBBA289}Machine\Software\Policies\Microsoft\Windows Defender\DisableAntiSpyware
7:57:41.8593574 ... svchost.exe   952   RegSetValue  HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
7:57:42.7062287 ... MsMpEng.exe   3104  RegSetValue  HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{D8DC0350-BD5C-4B4F-8133-C550C09584B2}Machine\Software\Policies\Microsoft\Windows Defender\DisableAntiSpyware
```

This 3rd key is written by `MsMpEng.exe` which happens to be the binary run by the Microsoft Defender service: this is the Defender userland engine. So, we should be good to go then?

Well, nothing is disabled yet, and after reboot …. the policy is removed! So this seems to be completely ignored.

Temporary solution

I finally managed to disable it, by adding a process exclusion (including `regedit.exe`):

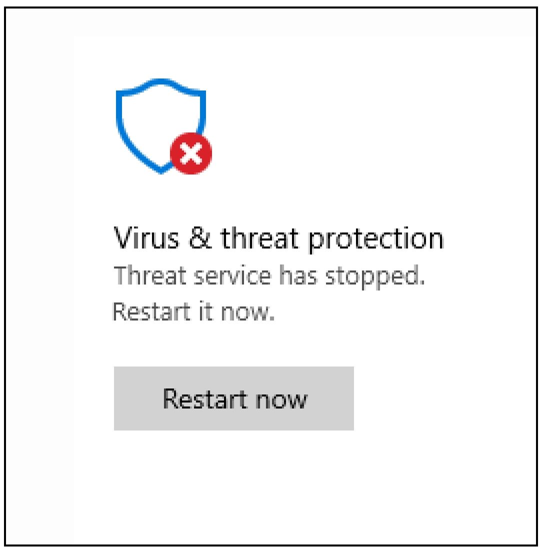


Exclusions

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

C:\*
Process

Then, with “Tamper Protection” off, and as SYSTEM, the key `HKLM\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware` finally becomes writable. Setting its value to 1 immediately stops Windows Defender:



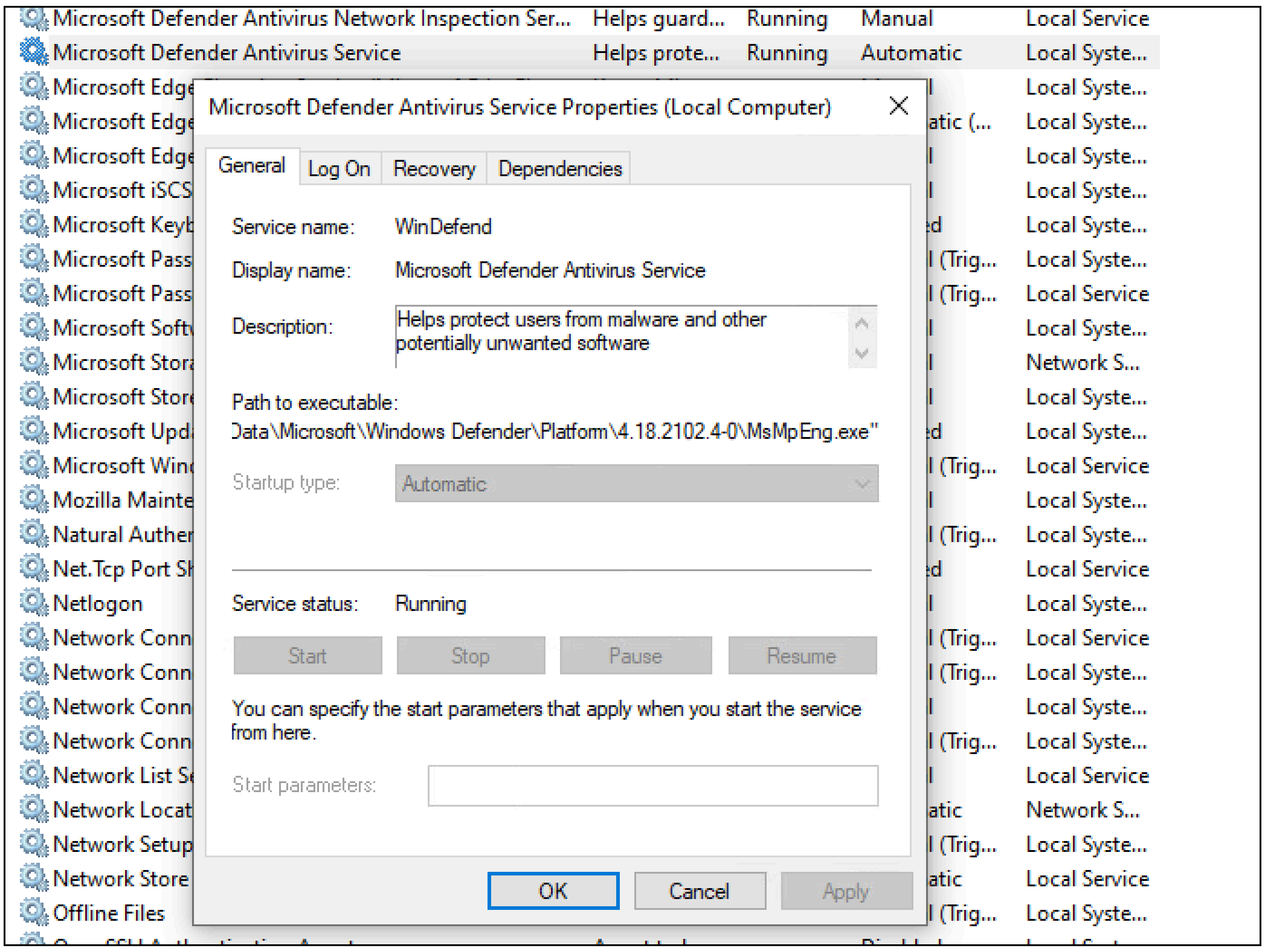
Virus & threat protection
Threat service has stopped.
Restart it now.

So here we are! But …. no 🙂 This is still overwritten on reboot! This a good enough temporary solution, but as we need to disable the “Tamper Protection”, it cannot be scripted in PowerShell.

Disable Defender: the hacker way

How it works

So I did not found any way to configure Defender itself to stop running. But it actually runs in a Service, so maybe there is something there. The service cannot be modified using `services.msc` as we would usually do:



Microsoft Defender Antivirus Network Inspection Ser...	Helps guard...	Running	Manual	Local Service
Microsoft Defender Antivirus Service	Helps prote...	Running	Automatic	Local Syste...

Microsoft Defender Antivirus Service Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: WinDefend

Display name: Microsoft Defender Antivirus Service

Description: Helps protect users from malware and other potentially unwanted software

Path to executable:
Data\Microsoft\Windows Defender\Platform\4.18.2102.4-0\MsMpEng.exe"

Startup type: Automatic

Service status: Running

Start | Stop | Pause | Resume

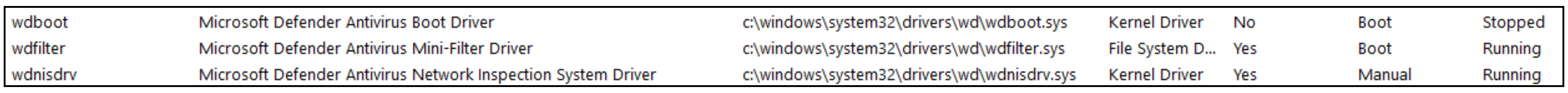
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

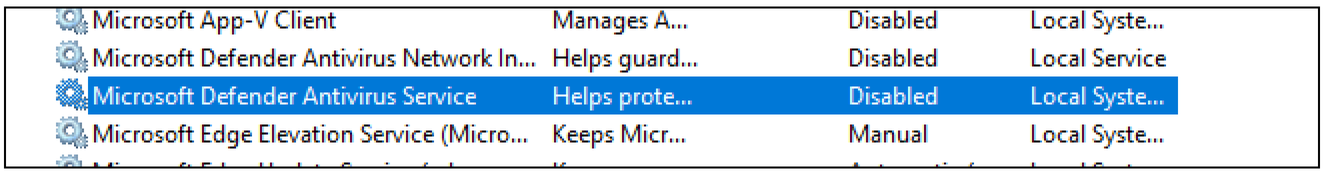
See how everything is greyed out?

We can also find the kernel drivers used by Defender, with `msinfo32`:



wdboot	Microsoft Defender Antivirus Boot Driver	c:\windows\system32\drivers\wd\wdboot.sys	Kernel Driver	No	Boot	Stopped
wdfilter	Microsoft Defender Antivirus Mini-Filter Driver	c:\windows\system32\drivers\wd\wdfilter.sys	File System D...	Yes	Boot	Running
wdnisdrv	Microsoft Defender Antivirus Network Inspection System Driver	c:\windows\system32\drivers\wd\wdnisdrv.sys	Kernel Driver	Yes	Manual	Running

But, and that's what we're going to use : we can edit (at least for now) the registry keys associated to those services and drivers, in `HKLM\SYSTEM\CurrentControlSet\Services\`. We set they `Start` value to 4, meaning "Disabled", and after next reboot, the services and driver will not be loaded / started, and so Defender will not be working anymore ! And indeed, after the reboot :



Microsoft App-V Client	Manages A...	Disabled	Local Syste...
Microsoft Defender Antivirus Network In...	Helps guard...	Disabled	Local Service
Microsoft Defender Antivirus Service	Helps prote...	Disabled	Local Syste...
Microsoft Edge Elevation Service (Micro...	Keeps Micr...	Manual	Local Syste...

We're good to go, finally! It's weird that we can edit those registry keys, when `services.msc` doesn't let us modify the service, but well … It works! Let's script the whole thing.

Scripting in PowerShell

I put everything in a convenient script that disables what it can directly in defender (`Set-MpPreference`), then modify the registry to disable the services, and set itself up to run again after reboot, to complete the removal. I'll break it down below.

First, I make sure to elevate to Administrator (mandatory, and actually used when the scripted is run after rebooting), and SYSTEM if `psexec` is available. SYSTEM is optional, but we need it to write in the registry to modify the parameters in case Defender would still re-enable itself one day (because it sure will …).

```
if(-Not $($(whoami) -eq "nt authority\system")) {
    $IsSystem = $false

    # Elevate to admin (needed when called after reboot)
    if (-Not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(
        Write-Host "    [i] Elevate to Administrator"
        $CommandLine = "-ExecutionPolicy Bypass `"" + $MyInvocation.MyCommand.Path + "`" " + $MyInvocation.Unboun
        Start-Process -FilePath PowerShell.exe -Verb Runas -ArgumentList $CommandLine
        Exit
    }

    # Elevate to SYSTEM if psexec is available
    $psexec_path = $(Get-Command PsExec -ErrorAction 'ignore').Source
    if($psexec_path) {
        Write-Host "    [i] Elevate to SYSTEM"
        $CommandLine = " -i -s powershell.exe -ExecutionPolicy Bypass `"" + $MyInvocation.MyCommand.Path + "`" "
        Start-Process -WindowStyle Hidden -FilePath $psexec_path -ArgumentList $CommandLine
        exit
    } else {
        Write-Host "    [i] PsExec not found, will continue as Administrator"
    }

} else {
    $IsSystem = $true
}
```

Then the script use the `Set-MpPreference` command to disable everything we can, adding exception for all drive leter, and disabling all available engines.

```
67..90|foreach-object{
    $drive = [char]$_
    Add-MpPreference -ExclusionPath "$($drive):\" -ErrorAction SilentlyContinue
    Add-MpPreference -ExclusionProcess "$($drive):\*" -ErrorAction SilentlyContinue
}

Write-Host "    [+] Disable scanning engines (Set-MpPreference)"

Set-MpPreference -DisableArchiveScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableBehaviorMonitoring 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableIntrusionPreventionSystem 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableIOAVProtection 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableRemovableDriveScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableBlockAtFirstSeen 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableScanningNetworkFiles 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableScriptScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableRealtimeMonitoring 1 -ErrorAction SilentlyContinue

Write-Host "    [+] Set default actions to Allow (Set-MpPreference)"

Set-MpPreference -LowThreatDefaultAction Allow -ErrorAction SilentlyContinue
Set-MpPreference -ModerateThreatDefaultAction Allow -ErrorAction SilentlyContinue
Set-MpPreference -HighThreatDefaultAction Allow -ErrorAction SilentlyContinue
```

Then the services and drivers are disabled, and the script checks if it need to reboot :

```
$need_reboot = $false

# WdNisSvc Network Inspection Service
# WinDefend Antivirus Service
# Sense : Advanced Protection Service

$svc_list = @("WdNisSvc", "WinDefend", "Sense")
foreach($svc in $svc_list) {
    if($(Test-Path "HKLM:\SYSTEM\CurrentControlSet\Services\$svc")) {
        if( $(Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\$svc").Start -eq 4) {
            Write-Host "        [i] Service $svc already disabled"
        } else {
            Write-Host "        [i] Disable service $svc (next reboot)"
            Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\$svc" -Name Start -Value 4
            $need_reboot = $true
        }
    } else {
        Write-Host "        [i] Service $svc already deleted"
    }
}

Write-Host "    [+] Disable drivers"

# WdnisDrv : Network Inspection System Driver
# wdfilter : Mini-Filter Driver
# wdboot : Boot Driver

$drv_list = @("WdnisDrv", "wdfilter", "wdboot")
```

```powershell
foreach($drv in $drv_list) {
    if($(Test-Path "HKLM:\SYSTEM\CurrentControlSet\Services\$drv")) {
        if( $(Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\$drv").Start -eq 4) {
            Write-Host "        [i] Driver $drv already disabled"
        } else {
            Write-Host "        [i] Disable driver $drv (next reboot)"
            Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\$drv" -Name Start -Value 4
            $need_reboot = $true
        }
    } else {
        Write-Host "        [i] Driver $drv already deleted"
    }
}

# Check if service running or not
if($(GET-Service -Name WinDefend).Status -eq "Running") {
    Write-Host "    [+] WinDefend Service still running (reboot required)"
    $need_reboot = $true
} else {
    Write-Host "    [+] WinDefend Service not running"
}
```

To execute after reboot, a shortcut is added in `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\`, and deleted after use.

```powershell
$link_reboot = "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\disable-defender.lnk"
Remove-Item -Force "$link_reboot" -ErrorAction 'ignore' # Remove the link (only execute once after reboot)

if($need_reboot) {
    Write-Host "    [+] This script will be started again after reboot." -BackgroundColor DarkRed -ForegroundColo

    $powershell_path = '"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"'
    $cmdargs = "-ExecutionPolicy Bypass `"" + $MyInvocation.MyCommand.Path + "`" " + $MyInvocation.UnboundArgumen

    $res = New-Item $(Split-Path -Path $link_reboot -Parent) -ItemType Directory -Force
    $WshShell = New-Object -comObject WScript.Shell
    $shortcut = $WshShell.CreateShortcut($link_reboot)
    $shortcut.TargetPath = $powershell_path
    $shortcut.Arguments = $cmdargs
    $shortcut.WorkingDirectory = "$(Split-Path -Path $PSScriptRoot -Parent)"
    $shortcut.Save()
```

Finally, if we don’t need to reboot, we can finish cleaning up : configure the registry, and delete the files if we wish to :

```powershell
} else {
    if($IsSystem) {

        # Configure the Defender registry to disable it (and the TamperProtection)
        # editing HKLM:\SOFTWARE\Microsoft\Windows Defender\ requires to be SYSTEM

        Write-Host "    [+] Disable all functionnalities with registry keys (SYSTEM privilege)"

        # Cloud-delivered protection:
        Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" -Name SpyNetRepor
        # Automatic Sample submission
        Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" -Name SubmitSampl
        # Tamper protection
        Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender\Features" -Name TamperProtection -Value

        # Disable in registry
        Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Defender" -Name DisableAntiSpyware -Value 1
        Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender" -Name DisableAntiSpyware -Val

    } else {
        Write-Host "    [W] (Optional) Cannot configure registry (not SYSTEM)"
    }


    if($MyInvocation.UnboundArguments -And $($MyInvocation.UnboundArguments.tolower().Contains("-delete"))) {

        # Delete Defender files
        function Delete-Show-Error {
            $path_exists = Test-Path $args[0]
            if($path_exists) {
                Remove-Item -Recurse -Force -Path $args[0]
            } else {
                Write-Host "    [i] $($args[0]) already deleted"
            }
        }

        Write-Host ""
        Write-Host "[+] Delete Windows Defender (files, services, drivers)"

        # Delete files
        Delete-Show-Error "C:\ProgramData\Windows\Windows Defender\"
        Delete-Show-Error "C:\ProgramData\Windows\Windows Defender Advanced Threat Protection\"

        # Delete drivers
        Delete-Show-Error "C:\Windows\System32\drivers\wd\"

        # Delete service registry entries
        foreach($svc in $svc_list) {
            Delete-Show-Error "HKLM:\SYSTEM\CurrentControlSet\Services\$svc"
        }

        # Delete drivers registry entries
        foreach($drv in $drv_list) {
            Delete-Show-Error "HKLM:\SYSTEM\CurrentControlSet\Services\$drv"
        }
    }
}

Write-Host ""
Read-Host -Prompt "Press any key to continue"
```

And we are done ! Final result can be downloaded here : https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1

It can be executed from anywhere in the file system. The parameter `-Delete` will delete the files linked to Defender after reboot. And it should work fine, until the Tamper Protection also protects the services ergistry key, which is bound to happen someday. I'm actually surprised it doesn't already …

This entry was posted in **Tooling** and tagged **antivirus**, **powershell** by **Jeremy**. Bookmark the **permalink**.

18 THOUGHTS ON "DISABLE WINDOWS DEFENDER IN POWERSHELL – A SCRIPT TO FINALLY GET RID OF IT"

CRC on **8 August 2024 at 16:29** said:

Worked, thank you been looking for a fix.

Reply↓

Jman on **14 April 2024 at 13:56** said:

Can you confirm If I did this correctly.
After using this script as best I could (I just ran it a handful of times in safe mode), now there is the usual windows defender icon in my system tray that has a red x.
In defender it says: "Your virus and threat protection is managed by your organization" With a red X saying "No active anti-virus provider"…
Does this mean I did it correctly? I see the Defender folders still in Program Files, & thought they would be deleted.

Reply↓

G Slayden on **7 April 2023 at 10:37** said:

Seems like you could have–just once–done a “Recovery” boot to get into the WindowsPE Recovery Environment, which gives easy access to the whole “real” registry hive while it’s in an unprotected (and unchanging “frozen”) state. So then you could trivially make any kind of changes either with the offline REG.EXE at that point, or even load the whole “real” hive into RE, for full-blown editing by having the RE environment host it, by using *it’s own* “toy” hive… I do it all the time….

Reply↓

Dan on **24 January 2023 at 04:30** said:

hi there, I’m on windows 10 and I’ve disabled Windows Update and set the execution policy, rebooted into safemode and while debugging the script, this is what I see:
basically permission denied despite having elevated permissions

```
[+] Disable Windows Defender (as nt authority\system)
[+] Add exclusions
[+] Disable scanning engines (Set-MpPreference)
[+] Set default actions to Allow (Set-MpPreference)
[+] Disable services
[i] Disable service WdNisSvc (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\users\desei\disable-defender.ps1:114 char:13
+ Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Se …
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : PermissionDenied: (Start:String) [Set-ItemProperty],
UnauthorizedAccessException
+ FullyQualifiedErrorId :
System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItem
PropertyCommand
```

`[i] Disable service WinDefend (next reboot)`

```
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\users\desei\disable-defender.ps1:114 char:13
+ Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Se …
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : PermissionDenied: (Start:String) [Set-ItemProperty],
UnauthorizedAccessException
+ FullyQualifiedErrorId :
System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItem
PropertyCommand
```

`[i] Service Sense already deleted`
`[+] Disable drivers`
`[i] Disable driver WdnisDrv (next reboot)`

```
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\users\desei\disable-defender.ps1:135 char:13
+ Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Se …
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : PermissionDenied: (Start:String) [Set-ItemProperty],
UnauthorizedAccessException
+ FullyQualifiedErrorId :
System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItem
PropertyCommand
```

`[i] Disable driver wdfilter (next reboot)`

```
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\users\desei\disable-defender.ps1:135 char:13
+ Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Se …
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[i] Disable driver wdboot (next reboot)

Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\users\desei\disable-defender.ps1:135 char:13
+ Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Se …
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[+] WinDefend Service still running (reboot required)
[+] This script will be started again after reboot.

Press any key to continue:
```

Reply↓

Jack on **11 January 2023 at 13:14** said:

On Windows 11 psexec cannot be run in safe mode cause the service is not available. I have tried to have the service psexesvc in safe mode but without success. I have run it without psexec and work well but registry was edited manually 😉

Reply↓

Johnny Smithy on **8 December 2022 at 04:19** said:

I tried doing what Doug said and running it in Safe Mode, Admin Elevated Powershell window with the set-executionpolicy remotesigned command enabled but Windows Defender always prevents it from running.

It used to work on previous versions of Windows 10 😔

Reply↓

Johnny Smithy
on **9 December 2022 at 00:01** said:

I figured out what was the problem: I needed to disable Windows Updates completely before going into Safe Mode and running the script. Did that and it worked flawlessly, Defender is GONE.

Reply↓

Nick on **10 July 2022 at 12:38** said:

for anyone having issues with this in 2022 it is due to windows defender itself preventing you from changing certain options.

Boot into safe mode (Hold shift and click restart)
Run powershell as Admin
run the command “set-executionpolicy remotesigned” (Allow scripts)

Place the script in C:\ drive and type
“cd c:\”
“.\disableDefender.ps1”

Restart once told and its done.

Reply↓

Lugan on **6 May 2022 at 01:35** said:

Look at first comment by Doug… he has the answer to make this work.

Finally the pesky windows defender has been disabled. Never thought I’d see the day.

Reply↓

xxx on **26 April 2022 at 12:41** said:

Does anyone have any idea what changed recently?

Reply↓

Tony on **6 October 2021 at 22:23** said:

If you want this fully automated, recommend adding these three lines of code.

First command: Disabling UAC will allow the script to complete without the UAC elevation prompt that I’m seeing after restarting the machine and the script attempts to continue.

```
#Disable UAC
New-ItemProperty -Path
HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name
EnableLUA -PropertyType DWord -Value 0 -Force
```

Second command: is to restart computer. This should go after line 152

```
#Restart Computer
Restart-Computer -Force
```

Third command: re-enable UAC. This should go towards the end of the script, before the very last write-host and read-host commands.

```
#Enable UAC
New-ItemProperty -Path
HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name
EnableLUA -PropertyType DWord -Value 0 -Force
```

Reply↓

GLIDERFROMNORTH on **5 October 2021 at 10:07** said:

Now I want a script to Enable Windows Defender, Undo all the changes that this script does..
Note I have made some changes where drivers are intact as this script delete the drivers.
please would you help me understand this or provide me wih the script or explain this script or concept so that I can make a script to enable the windows defender or use one if you already have it.

Reply↓

Jeremy
on **5 October 2021 at 19:36** said:

Hi, sorry for the inconvenience, but this script was never made or advertised for being a “start/stop” solution. I made it because I'm a malware analyst, and defender was being … well let's stay correct and just call it really annoying. Removing all its file was a sure way to make sure it would not delete the samples I was working on again.
I can't think of a way to get the files back, you may need to reinstall or repair windows. I'll add a warning on the article to avoid any further people making your mistake.
Best regards

Reply↓

ROMULO CARLOS REIS ALVES on **17 August 2021 at 21:08** said:

Hello.

Your post help me to stop Defender on newer Win10 builds, and then I can run a script wich install a lot of software. If it helps, at beggining of my script I have these lines:

```
powershell -command add-mppreference -exclusionpath ‘c:\'
powershell -command add-mppreference -exclusionprocess ‘c:\'
powershell -command Set-MpPreference -EnableControlledFolderAccess Disabled
powershell -command Set-MpPreference -DisableBehaviorMonitoring 1
powershell -command Set-MpPreference -DisableRealtimeMonitoring 1
```

Then, like the friend stated above, I can use AdvancedRun to stop and disable the service:

```
advancedrun.exe /exefilename c:\windows\system32\net.exe /commandline ‘stop windefend' /runas 8 /run
advancedrun.exe /exefilename c:\windows\system32\sc.exe /commandline ‘config windefend start= disabled' /runas 8 /run
```

I still receive the warning about it is disabled, but for my propouses it's fine, as it re-enable Defender at the end of installations. My script now run flawless like before.

Thank you!

Reply↓

jorge on **25 July 2021 at 15:37** said:

dont work

ps1 full of errors.

thanks anyway

Reply↓

Mr David Fishwick on **11 July 2021 at 14:43** said:

Er is that really necessary, all that? Easier way to disable:
1. Turn off real time protection and tamper protection in the app.
2. Open Regedit. Navigate to HKLM/Software/Policies/Windows Defender. Place the DsiableAntiSpyware key in manually and set to 1.
3. Navigate to HKLM/System/CurrentControlSet/wscsvc. Change the start value to 4. This disables the Security Service on the next boot.
4. Restart. The Security Service fails to start and the Defender service stops running (eventually…….). Note that the DisableAntiSpyware key is NOT removed this time.
5. To re-enable security centre, change the Start value back to 2 and restart again.
6. Security will be re-enabled but Defender remains OFF. This persists until the DisableAntiSpyware key is removed manually.
7. To re-enable Defender, simply remove the DisableAntiSpyware key manually. Press the "Restart Now" under Virus and Threat Protection and Defender (and its service) will immediately turn back on.

Reply↓

Jeremy
on **13 July 2021 at 19:23** said:

Hi ! Not "necessary" for sure, but I like to automate everything, and that's the solution I came with. But doing it manually can be indeed quite simple, as you mentionned.

Reply↓

Doug on **28 May 2021 at 08:26** said:

in latest insider build (21390), even elevation to SYSTEM is not enough to disable the services and drivers in registry, I had to use AdvancedRun from nirsoft to launch the script as TrustedInstaller to make it work…

Reply↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Categories

- **Tutorial**
- **Reverse**
- **Malware**
- **Tooling**

Socials

✉ jeremy [dot] beaume {at} protonmail [dot] com

Github

https://www.linkedin.com/in/beaumejeremy/