Restore Microsoft Defender on Windows 10 Enterprise

Manual undo of the Safe Mode Start=4 disable. These are the default Start values for these services on Windows 10, not a reading taken from one guest. Safe Mode is only the fallback if a registry write is denied. SmartScreen is left as it was.

The disable set WinDefend, WdFilter, WdBoot, WdNisDrv, and WdNisSvc to Start 4, and Sense to 4 when that service existed. Disable_Defender2.PS1 also disabled the tasks under \Microsoft\Windows\Windows Defender\. Tamper Protection may have been turned off. Group Policy may have been set. The binaries were not deleted. There is no webthreatdefsvc or webthreatdefusersvc on Windows 10. Do not add those names.

Why a normal session is enough

Safe Mode was required to disable Defender because WdFilter.sys registers a registry callback over those service keys. That driver is now Disabled and not loaded, so it is no longer protecting the keys. An elevated PowerShell window on the normal desktop can write them back. Boot Safe Mode only if Restore_Defender.PS1 prints RESULT: FAIL on a denied write.

> Do not run Start-Service WinDefend before the reboot. WdBoot and WdFilter load at boot. Setting them back to 0 does nothing until the next boot. The pre-reboot script does not enable the scheduled tasks, so a scan task cannot start WinDefend while the minifilter is still unloaded. The script prints Tasks were not changed.

Values to restore

SecurityHealthService was not part of this procedure. Leave it alone when it is still 3. If an older note set it to 4, set that one value back to 3 by hand before you reboot. The current scripts do not write it. If Sense prints missing, it was not installed. Skip it. SmartScreen was not changed.

Name	Disabled	Restore to	Meaning
WdBoot	4	0	Boot-start kernel driver.
WdFilter	4	0	Boot-start file-system minifilter.
WinDefend	4	2	Automatic. This is MsMpEng.exe.
WdNisDrv	4	3	Manual.
WdNisSvc	4	3	Manual.
Sense	4 or missing	3	Manual, when the service exists.
SecurityHealthService	unchanged	3	Not written by the script.

0 is Boot, 2 is Automatic, 3 is Manual, 4 is Disabled. The script prints the names in this order.

```
Set-ItemProperty -LiteralPath `
    'HKLM:\SYSTEM\CurrentControlSet\Services\SecurityHealthService' `
    -Name Start -Value 3 -Type DWord
```

Run that one command only when SecurityHealthService is already 4 because an older note wrote it. Do not run it when the value is already 3.

1. Write the Start values back

Sign in to the normal desktop as a local admin. Open PowerShell with Run as administrator. The title bar must say Administrator. If you run the .ps1, bypass execution policy for this window only. Answer Y. Process scope dies with the window.

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
.\Restore_Defender.PS1
```

Output	Meaning
WdBoot = 0 and WdFilter = 0	Boot drivers are set back. They stay unloaded until reboot.
WinDefend = 2	The engine service is Automatic again. It is not started yet.
WdNisDrv = 3 and WdNisSvc = 3	Manual, which is the Windows 10 default.
Sense = 3, or missing: Sense	Missing is success when the service was never installed.
name: denied (still N)	That write did not stick. Later names were not written.
Later names were not written.	The script stopped. Fix the denial before reboot.
Tasks were not changed.	The tasks stay Disabled until the post-reboot run.
RESULT: PASS	Reboot, then run Restore_Defender.PS1 -AfterReboot.
RESULT: FAIL	Do not reboot for a restore while RESULT is FAIL.

On RESULT: FAIL, stop. From an elevated Command Prompt run bcdedit /set {current} safeboot minimal, confirm safeboot Minimal with bcdedit /enum {current}, and reboot. In Safe Mode, elevated PowerShell, run .\Restore_Defender.PS1 again. Then bcdedit /deletevalue {current} safeboot, confirm safeboot is gone, and only then reboot. A black console in Safe Mode for more than a few minutes means the safeboot flag is set. Revert the snapshot if you cannot leave Safe Mode. A failed run may already have written the names above the denied line. Running the script again writes the full set.

2. Clear Group Policy, if you set it

Skip this step if gpedit.msc was never opened during the disable, including every Windows 10 Home guest. A policy left at Enabled keeps Defender off, or marks it managed, after the services are restored. Not Configured is the original state. Disabled is a different setting.

- Win+R, then gpedit.msc.
- Computer Configuration, Administrative Templates, Windows Components, Microsoft Defender Antivirus, or Windows Defender Antivirus on older builds.
- Turn off Microsoft Defender Antivirus, or Turn off Windows Defender Antivirus, set to Not Configured, then OK.
- Open the Real-time Protection folder. Turn off real-time protection, set to Not Configured, then OK.
- Close gpedit. The reboot in the next step covers the policy.

If you also created DisableAntiSpyware or other values under HKLM\SOFTWARE\Policies\Microsoft\Windows Defender, delete those values. This procedure did not require them. A leftover policy value can still make Windows Security say the setting is managed.

3. Reboot once

Boot drivers load only at boot. One clean reboot is the restore, not a service start. Do not enable the Defender tasks before this reboot.

```
shutdown /r /t 0
```

If you had to use Safe Mode in step 1, safeboot must already be deleted before this reboot. bcdedit /enum {current} must not show safeboot.

4. Enable the tasks and confirm the engine

After the normal desktop is up, wait a minute. WinDefend is Automatic and may still be starting. Then, in elevated PowerShell:

```
.\Restore_Defender.PS1 -AfterReboot
```

This run enables every task under \Microsoft\Windows\Windows Defender\ and then checks the restored state. An empty task list is a failure. The query returning nothing does not mean the task path was removed. Disable-ScheduledTask does not delete those tasks. Exit code 0 and RESULT: PASS are the gate for this phase. If the engine is still starting, run the same command again.

Check	Restored
Safe Mode	Safe Mode: no.
WinDefend	Running, and Automatic. AutomaticDelayedStart also passes.
WdNisSvc	Manual, and Stopped or Running.
Sense	Manual and Stopped or Running, or missing.
MsMpEng.exe	MsMpEng.exe: running.
WdFilter and WdBoot	START_TYPE 0. WdBoot does not have to be running.
WdNisDrv	START_TYPE 3. The post-reboot check reads this. A missed write fails.
WdFilter state	STATE 4, and fltmc WdFilter: listed.
Tasks	At least one task, each Ready, Running, or Queued.
Get-MpComputerStatus	Printed as non-authoritative. It does not decide RESULT.

> Real-time protection may still be off after RESULT: PASS. IsTamperProtected stays false until you turn Tamper Protection back on, and it stays false on a build that has no Tamper Protection switch. The script prints a reminder that those two switches are still manual steps.

If the engine did not come back

- RESULT: FAIL and a START_TYPE is still the disabled value: the step 1 write did not stick. Repeat Restore_Defender.PS1. If a write is denied, use the Safe Mode fallback, then reboot with safeboot cleared.
- START_TYPE values are correct but WdFilter STATE is not 4: you did not reboot, or safeboot is still set. Run bcdedit /enum {current}, clear safeboot if it is present, and reboot again.
- WinDefend will not stay Running and policy still says Enabled: the Group Policy step was skipped. Set both policies back to Not Configured and reboot.
- fltmc WdFilter: absent while START_TYPE is 0: the driver failed to load. Read WdFilter STATE before changing anything else.
- The only FAIL lines are tasks: rerun Restore_Defender.PS1 -AfterReboot. Do not rewrite Start for a task-only failure.

5. Turn Tamper Protection back on

Do this only after step 4 prints RESULT: PASS, and only on a build that has the switch. Turning it on earlier can block a retry of the registry restore.

- Windows Security, Virus and threat protection, Manage settings.
- Turn Tamper Protection on. Accept the UAC prompt.
- On the same page, turn real-time protection on if it is off.

- Leave the firewall and SmartScreen as they were. This restore does not change them.

Final check, on a build that has Tamper Protection:

```
Get-MpComputerStatus | Select-Object AMServiceEnabled, `
    AntivirusEnabled, RealTimeProtectionEnabled, IsTamperProtected
```

All four should be True. That is the original protection state on Windows 10 1903 and later: engine running, real-time scanning on, tamper protection on.

> Restored means WinDefend Running and Automatic, MsMpEng.exe present, WdFilter START_TYPE 0 and listed in fltmc, WdNisDrv START_TYPE 3, Defender tasks Ready, Running, or Queued, both Group Policy settings Not Configured if you had set them, and Tamper Protection on when the build has that switch. SecurityHealthService needs a manual repair only if an older note set it to 4. SmartScreen was left alone.

Order of operations

- Normal desktop, elevated PowerShell. Process-scope Bypass, then .\Restore_Defender.PS1.
- Require RESULT: PASS. Do not touch SecurityHealthService unless an older note left it at 4.
- Do not enable tasks in this step. Do not Start-Service WinDefend.
- If gpedit was used: both Turn off policies back to Not Configured.
- Reboot once. safeboot must already be clear.
- Wait a minute, then .\Restore_Defender.PS1 -AfterReboot. Require RESULT: PASS.
- Tamper Protection on, then real-time protection on if it is still off.

This does not depend on a hypervisor snapshot. A snapshot revert remains a valid shortcut if one was taken before the disable, but it is not part of this procedure.