Completely disable Microsoft Defender on Windows 10 Enterprise

Safe Mode, then Disable_Defender2.PS1, then a normal boot and Check_Defender_Disabled.PS1. The scripts are the procedure. Run the files. Do not retype a second registry loop. Defender_Off-Win10.txt is the checklist.

This is a lab procedure for a Windows 10 virtual machine you control. It disables the antivirus engine and its boot drivers. It does not remove the binaries. A later Defender platform update can restore the service start values. Take a hypervisor snapshot named pre-defender-disable before the first change. That snapshot is the clean undo.

What is different from the Windows 11 procedure

On the Windows 11 guest, Disable_Defender2.PS1 only disables the scheduled tasks and prints Start, because those services were already at 4. The Windows 10 script writes Start=4 and then disables the tasks. It does not write SecurityHealthService. Windows 10 has no webthreatdefsvc, no webthreatdefusersvc, and no Smart App Control.

What off means

Group Policy does not write Start=4 while the engine is running and protected. DisableAntiSpyware is a legacy setting and is not the method this procedure uses. Tamper Protection, on Windows 10 version 1903 and later, blocks changes while it is on. WdFilter.sys registers a registry callback over Defender's service keys while that driver is loaded. The writes run in Safe Mode, where WdFilter is not loaded. Start value 4 means Disabled.

Require these results from Check_Defender_Disabled.PS1 after the normal reboot. Exit code 0 and RESULT: PASS are the same gate.

Check	Pass
Safe Mode	The script prints Safe Mode: no.
WinDefend, WdNisSvc	Stopped, Disabled.
Sense	Stopped and Disabled, or the service is missing.
MsMpEng.exe	The script prints MsMpEng.exe: not running.
WdFilter, WdBoot, WdNisDrv	sc qc START_TYPE 4 for each name.
fltmc	The script prints fltmc WdFilter: absent.
Scheduled tasks	At least one task, and every State is Disabled.
Script result	RESULT: PASS and exit code 0.

Win32 exit 1077 means the driver was not started this boot. It does not prove Start is 4. A Manual WdNisDrv that nothing started prints STATE 1 and exit 1077, which is also the healthy restore value. The pass test for WdNisDrv is START_TYPE 4. The runtime line is informational. driverquery matches are installed drivers, and a match is not a failure. Get-MpComputerStatus is non-authoritative. The check script catches a throw from that cmdlet and still prints the START_TYPE, fltmc, and task lines.

What this does not turn off

Windows Firewall and the Windows Security app stay. On older builds that app is still named Windows Defender Security Center. SecurityHealthService is not modified. The Security app can open and report that the threat service has stopped. That is the expected result.

Leave SmartScreen alone. SmartScreen is not Defender Antivirus. Disable_Defender2.PS1 does not change it. Windows 10 has no Smart App Control.

Before you start

- Guest is Windows 10 Enterprise, version 1903 through 22H2. Pro and Education use the same steps. Home has no gpedit.msc, so skip the policy step.

- Local administrator. The guest already boots normally.

- Snapshot name: pre-defender-disable. If Safe Mode comes up black, or the guest will not leave Safe Mode, revert that snapshot. Do not rely on System Restore.

- Mouse integration is often dead in Safe Mode. Ctrl+Alt releases the cursor to the host. Click the console to type again.

- Safe Mode uses the basic display driver. A low-resolution desktop is normal. A black screen for more than a few minutes is not. Revert the snapshot rather than hard-resetting, because a reset with safeboot still set boots Safe Mode again.

1. Turn Tamper Protection off, still in the normal session

Do this before Safe Mode on Windows 10 version 1903 and later. Tamper Protection cannot be flipped from the command line while WdFilter is loaded. If the page has no Tamper Protection switch, the build does not have it. Continue with the rest of the procedure.

- Sign in as a local admin.

- Windows Security, Virus and threat protection, Manage settings. On an older build, open Windows Defender Security Center and then Virus and threat protection.

- Turn Tamper Protection off and accept the UAC prompt.

- On the same page, turn real-time protection off. It may turn itself back on later. The service disable is what sticks.

- Leave SmartScreen alone. Leave the firewall alone.

2. Optional policy layer

Skip this step on Windows 10 Home. This does not stop MsMpEng.exe by itself, and it does not write Start=4. It stops some of the logic that turns the engine back on. Skip it if you only want the service change.

- Win+R, then gpedit.msc.

- Computer Configuration, Administrative Templates, Windows Components, Microsoft Defender Antivirus. On older builds the folder is named Windows Defender Antivirus.

- Turn off Microsoft Defender Antivirus, or Turn off Windows Defender Antivirus, set to Enabled, then OK.

- Under Real-time Protection, set Turn off real-time protection to Enabled.

> Do not reboot into a normal session for the policy alone. A normal reboot lets Defender start again and argue with the policy. The next reboot is into Safe Mode.

3. Force the next boot into Safe Mode

Open an elevated Command Prompt. On Windows 10, Win+X shows Command Prompt (Admin) or Windows PowerShell (Admin). Use Command Prompt for bcdedit. In PowerShell, {current} is a script block.

```
bcdedit /set {current} safeboot minimal
bcdedit /enum {current}
shutdown /r /t 0
```

bcdedit /enum {current} must show safeboot Minimal before you reboot. If it does not, do not reboot. Alternate path: Win+R, msconfig, Boot tab, Safe boot, Minimal, OK, Restart.

> If the console stays black for several minutes, revert the snapshot from the hypervisor. Do not keep resetting the guest.

4. In Safe Mode, run Disable_Defender2.PS1

Confirm Safe Mode before running the file. Elevated PowerShell:

```
(Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\SafeBoot\Option `
    -ErrorAction SilentlyContinue).OptionValue
```

1 means Minimal Safe Mode. No key means a normal boot. The title bar must also say Administrator. A stock Windows 10 install is often Restricted, so a .ps1 is refused until you bypass execution policy for this window only. The prompt defaults to N. Answer Y. Do not change the machine policy.

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
.\Disable_Defender2.PS1
```

From an elevated Command Prompt the equivalent is powershell -NoProfile -ExecutionPolicy Bypass -File followed by the full path of Disable_Defender2.PS1.

Script output	Meaning
name: before -> 4	That service is Disabled. Sense may instead print missing.
name: 4 -> 4	It was already Disabled. The script does not write it again.
name: before -> denied (still N)	The write did not stick. RESULT will be FAIL.
missing: WinDefend (or any required name)	RESULT: FAIL. Sense is the only name allowed to be missing.
task = Disabled	That returned task is Disabled.
task = denied, or any other state	RESULT: FAIL. A printed task name is not success by itself.
WARNING: no Defender tasks were returned.	Safe Mode often does not start Task Scheduler. Exit code can still be 0.
RESULT: PASS	Required Start values are 4, and every returned task is Disabled.
RESULT: FAIL	Do not continue to the next step.

RESULT: PASS in Safe Mode is not the final gate. The warning about no tasks is expected there. Do not leave Safe Mode on RESULT: FAIL. A denied line for WinDefend, WdFilter, WdBoot, WdNisSvc, or WdNisDrv stays a failure until a later run prints RESULT: PASS. The script tries every service name so each denial is visible, then exits 1.

5. Leave Safe Mode

Elevated Command Prompt, still inside Safe Mode:

```
bcdedit /deletevalue {current} safeboot
bcdedit /enum {current}
shutdown /r /t 0
```

safeboot must be absent from the enum output before you reboot. If you used msconfig instead of bcdedit, open msconfig, Boot, clear Safe boot, OK, Restart. If the next boot lands in Safe Mode again, the delete did not stick. Run the delete again from that Safe Mode session.

6. Verify after the normal boot

Elevated PowerShell. Same process-scope execution-policy bypass if you run the file. Give the desktop a moment to finish signing in, then:

```
.\Check_Defender_Disabled.PS1
```

The final gate is RESULT: PASS and exit code 0. Safe Mode: yes is a failure even when every Start value is already 4, because a Safe Mode session does not load WdFilter and does not start WinDefend. An empty task list is a failure. fltmc WdFilter: unread is a failure, because the script cannot prove the minifilter is absent. An unreadable START_TYPE is a failure.

The check script never calls Disable-ScheduledTask. A status check must not change the tasks. Silence from MsMpEng.exe is not the pass signal. The script prints MsMpEng.exe: not running, or MsMpEng.exe: running.

What will try to undo this

A cumulative update or a Defender platform update can write the Start values back, especially on WdBoot, WdFilter, and WinDefend. Feature upgrades are the usual case. On a lab VM, pause Windows Update, or re-check with Check_Defender_Disabled.PS1 after any update that brings MsMpEng.exe back.

Check failure	What to run
START_TYPE is not 4, MsMpEng.exe is running, fltmc lists WdFilter, or Safe Mode is still set.	Run Disable_Defender2.PS1 again from Safe Mode. A normal-desktop rerun cannot write Start while WdFilter is loaded.
Every START_TYPE is 4 and the only FAIL lines are task state.	Run Disable_Defender2.PS1 again on the normal desktop. A name that is already 4 is left unchanged, including when a rewrite would be denied.

Undo

Snapshot revert is the clean undo. Manual undo is Restore_Defender_Windows10_Enterprise.pdf and Restore_Defender.PS1. The pre-reboot run writes Start and does not enable tasks. After the reboot, Restore_Defender.PS1 -AfterReboot enables the tasks and checks the restored state. Clear Group Policy if you set it. Turn Tamper Protection back on if this build has it.

Files

File	When	Role
Disable_Defender2.PS1	Safe Mode, elevated. Again on the normal desktop only for task state.	Writes Start=4 and disables returned tasks. Exit 0 only for RESULT: PASS.
Check_Defender_Disabled.PS1	Normal boot, elevated.	Final gate. Exit 0 only for RESULT: PASS.
Restore_Defender.PS1	Normal desktop, elevated.	Pre-reboot writes Start. -AfterReboot enables tasks and verifies.
Defender_Off-Win10.txt	Read before you start.	Checklist. It is not a second registry loop.

Order of operations

- Snapshot.

- Tamper Protection off, and real-time protection off, when those switches exist. Leave SmartScreen alone.

- Optional, and not on Home: both Turn off policies set to Enabled. Do not reboot into a normal session for the policy alone.

- bcdedit /set {current} safeboot minimal, from an elevated Command Prompt. Confirm with bcdedit /enum, then reboot.

- Elevated PowerShell, process-scope Bypass, Disable_Defender2.PS1. Require RESULT: PASS.

- bcdedit /deletevalue {current} safeboot, confirm safeboot is gone, reboot.

- Check_Defender_Disabled.PS1. Require RESULT: PASS. Exit 1077 is not a substitute for START_TYPE 4.

- If Start is not 4 or WdFilter is loaded, repeat the script from Safe Mode. If only task State failed, repeat the script on the normal desktop.