PROCEDURE

Restore Microsoft Defender on Windows 11 Enterprise

Manual undo of the Safe Mode disable, using the before-values recorded on this guest. No VMware snapshot. Safe Mode is only the fallback if a registry write is denied. Smart App Control is left as it was.

On this guest the Defender service and driver Start values are 4, and Disable_Defender2.PS1 disabled the tasks under \Microsoft\Windows\Windows Defender\. Tamper Protection was turned off in the Windows Security UI. Group Policy may also have been set. The binaries were not deleted. Putting Start back, re-enabling the tasks, clearing policy, and rebooting is a full functional restore. disable_Defender.PS1 is archived under __OLD__ and is not used.

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 a Set-ItemProperty in step 1 returns access denied.

DO NOT START THE SERVICE BY HAND

WdBoot and WdFilter are boot-start drivers. Setting them back to 0 does nothing until the next boot. Do not run Start-Service WinDefend before that reboot. A half-started engine with its minifilter still unloaded is not the original state.

Values to restore

These are the before-values recorded on this guest, not generic defaults from another machine. SecurityHealthService never changed; leave it at 3. Smart App Control was not changed; do not touch it on the way back either.

Name	Now	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
webthreatdefusersvc	4	2	Automatic user service
Sense	4	3	Manual
WdNisSvc	4	3	Manual
WdNisDrv	4	3	Manual
webthreatdefsvc	4	3	Manual
SecurityHealthService	3	3	Unchanged. Do not write it

0 is Boot, 2 is Automatic, 3 is Manual, 4 is Disabled. A missing key for Sense or either webthreatdef service means that component was never present. Skip it.

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 save this as a .ps1, a stock Windows 11 guest will refuse it until you bypass execution policy for this window only. Answer Y. Process scope dies with the window; do not change the machine policy.

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

Then run the restore. Interactive paste does not need the policy change.

```
$restore = @{
  WinDefend           = 2
  Sense               = 3
  WdNisSvc            = 3
  WdNisDrv            = 3
  WdBoot              = 0
  WdFilter            = 0
  webthreatdefsvc     = 3
  webthreatdefusersvc = 2
}
foreach ($s in $restore.Keys) {
  $p = "HKLM:\SYSTEM\CurrentControlSet\Services\$s"
  if (Test-Path $p) {
    Set-ItemProperty $p -Name Start -Value $restore[$s] -Type DWord
    '{0} = {1}' -f $s, (Get-ItemProperty $p).Start
  } else {
    "missing: $s"
  }
}
```

Every existing name must print its restore value: WdBoot and WdFilter = 0, WinDefend and webthreatdefusersvc = 2, the rest = 3. Hashtable order is not insertion order. Match the number, not the line position. Do not reboot yet. Do not write SecurityHealthService.

IF A WRITE IS DENIED

Stop. Do not keep retrying from the normal session. 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 the same restore block. Then bcdedit /deletevalue {current} safeboot, confirm safeboot is gone, and only then reboot. A black VMware console in Safe Mode for more than a few minutes means the safeboot flag is set and a hard reset will not clear it.

2. Re-enable the scheduled tasks

Disable_Defender2.PS1 disabled every task under \Microsoft\Windows\Windows Defender\. Reverse that in the same elevated window, still before the reboot. Do not edit Disable_Defender2.PS1.

```
Get-ScheduledTask -TaskPath '\Microsoft\Windows\Windows Defender\' `
  -ErrorAction SilentlyContinue |
  ForEach-Object { Enable-ScheduledTask -InputObject $_; $_.TaskName }

Get-ScheduledTask -TaskPath '\Microsoft\Windows\Windows Defender\' `
  -ErrorAction SilentlyContinue |
  Format-Table TaskName, State -AutoSize
```

State should be Ready, not Disabled. An empty list means the task path was already gone; that is not a failure. Continue.

3. Clear Group Policy, if you set it

Skip this step if gpedit.msc was never opened during the disable. A policy left at Enabled will keep Defender off, or mark it managed, after the services are restored. Not Configured is the original state. Disabled is not the same thing.

- Win+R → gpedit.msc.
- Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus.
- Turn off Microsoft Defender Antivirus → Not Configured → OK.
- Open the Real-time Protection folder. Turn off real-time protection → Not Configured → OK.
- Close gpedit. Do not reboot for the policy alone; the reboot in the next step covers it.

If you also created DisableAntiSpyware or other values under HKLM\SOFTWARE\Policies\Microsoft\Windows Defender, delete those values. This guest's disable did not require them, and current Defender platforms ignore DisableAntiSpyware on onboarded devices, but a leftover policy value can still make Windows Security say the setting is managed.

4. Reboot once

Boot drivers load only at boot. One clean reboot is the restore, not a service start.

```
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.

5. Confirm the engine is back

After the normal desktop is up, elevated PowerShell. Give the guest a minute after logon; WinDefend is Automatic and may still be starting.

```
Get-Service WinDefend, WdNisSvc, Sense |
  Format-Table Name, Status, StartType
Get-Process MsMpEng -ErrorAction SilentlyContinue
sc.exe qc WdFilter
sc.exe qc WdBoot
sc.exe query WdFilter
fltmc | findstr /i WdFilter
Get-MpComputerStatus | Select AMServiceEnabled, AntivirusEnabled, `
  RealTimeProtectionEnabled, IsTamperProtected
```

Check	Restored
WinDefend	Running, StartType Automatic
WdNisSvc, Sense	Stopped or Running, StartType Manual. Manual does not mean failed.
MsMpEng.exe	Present. This is the engine.
WdFilter and WdBoot config	START_TYPE 0 BOOT_START, not 4
sc query WdFilter	STATE 4 RUNNING
fltmc	WdFilter listed as a loaded minifilter
Get-MpComputerStatus	AMServiceEnabled and AntivirusEnabled True
Defender scheduled tasks	State Ready, not Disabled

RealTimeProtectionEnabled may still be False until step 6. IsTamperProtected should still be False, because Tamper Protection was turned off in the UI and has not been turned back on yet. Trust sc query and fltmc if Get-MpComputerStatus lags. driverquery matching WdFilter proves nothing either way; it lists installed drivers, not loaded ones.

If the engine did not come back

- Start values still 4: the step 1 write did not stick. Repeat it. If access is denied, use the Safe Mode fallback in the red box above, then reboot with safeboot cleared.
- Start values are correct but WdFilter is STOPPED: you did not reboot, or safeboot is still set. bcdedit /enum {current}, clear safeboot if it is present, reboot again.
- WinDefend will not stay Running and policy still says Enabled: step 3 was skipped. Set both policies back to Not Configured and reboot.
- fltmc has no WdFilter while sc qc says BOOT_START: the driver failed to load. Check sc query WdFilter for the exit code before changing anything else.

6. Turn Tamper Protection back on

Do this only after step 5 shows WinDefend Running and WdFilter loaded. Turning it on earlier can block a retry of the registry restore.

- Windows Security → Virus & threat protection → Manage settings.

- Turn Tamper Protection on. Accept the UAC prompt.
- On the same page, Real-time protection should already be on. If it is off, turn it on.
- Leave the firewall and Smart App Control as they were. This restore does not change them.

Final check:

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

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

RESTORED

WinDefend Running and Automatic, MsMpEng.exe present, WdFilter BOOT_START and listed in fltmc, Defender tasks Ready, both Group Policy settings Not Configured, and Tamper Protection on. SecurityHealthService was never part of the disable and needs no repair. Smart App Control was left alone and needs no repair.

Order of operations

- Normal desktop, elevated PowerShell. Process-scope Bypass only if you run a .ps1.
- Write Start back to the table above. Do not touch SecurityHealthService. Do not touch Smart App Control.
- Enable the tasks under \Microsoft\Windows\Windows Defender\.
- If gpedit was used: both “turn off” policies back to Not Configured.
- Reboot once. Do not Start-Service WinDefend first.
- Confirm WinDefend Running, MsMpEng present, WdFilter running and in fltmc, tasks Ready.
- Tamper Protection on, then real-time protection on if it is still off.

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