Turn Smart App Control back on

Manual undo of the Off write. Run Enable-SmartAppControl.ps1 on the normal desktop, then reboot once. Safe Mode is not used. This does not depend on a hypervisor snapshot. A snapshot revert of pre-sac-off remains a valid shortcut if one was taken.

Enforce writes 1. Evaluation writes 2. The script writes that same number to the policy state and to VerifiedAndReputablePolicyStateMinValueSeen. The pair has to match. Optional diagnostic data has to be on or Windows can refuse to keep the mode.

Which mode

Command	Value	After reboot, CiTool -lp
.\Enable-SmartAppControl.ps1	1 Enforce	Friendly Name VerifiedAndReputableDesktop, Is Currently Enforced = true.
.\Enable-SmartAppControl.ps1 -Mode Evaluation	2 Evaluation	Friendly Name VerifiedAndReputableDesktopEvaluation, Is Currently Enforced = true.

The default is Enforce. Evaluation logs what would be blocked and does not block on the signature result. Pick one mode. Do not write 1 and 2 into the two values.

What the restore does not change

SacLearningModeSwitch stays where the disable left it. The testing path sets that switch to 0 for Off, Enforce, and Evaluation, so the restore does not put it back. Execution policy stays Bypass. Defender, the firewall, SmartScreen, and Tamper Protection are not part of this script.

> On builds before the March/April 2026 cumulative updates, the Windows Security toggle cannot return from Off. The registry write is the testing path. If the value reverts to 0 after reboot, this install is not eligible. Reset this PC (Keep my files) is the remaining path. Enterprise management can force Smart App Control off again within about 48 hours.

1. Run Enable-SmartAppControl.ps1

Sign in to the normal desktop as a local admin. Open PowerShell with Run as administrator. The title bar must say Administrator. LocalMachine Bypass from the disable procedure is enough to start the file. Safe Mode is not required.

```
.\Enable-SmartAppControl.ps1
.\Enable-SmartAppControl.ps1 -Mode Evaluation
```

Run one of those commands, not both. The script prints which number it is writing.

Output	Meaning
Backup written: SAC-backup-before-enable-....json	Policy state and MinValueSeen were saved next to the script.
AllowTelemetry = 3. Optional diagnostic data is 3.	Diagnostic data is already Optional. SAC can stay on.
AllowTelemetry is missing or is not 3	Turn on optional diagnostic data, then reboot after this script. Settings, Privacy and security, Diagnostics and feedback.
Setting Smart App Control to Enforce (1)	Or Evaluation (2). The policy write started.
CI\Protected is owned by TrustedInstaller. Taking ownership and retrying...	The minimum needed the same ownership retry the disable uses.
Could not write VerifiedAndReputablePolicyStateMinValueSeen	The policy value was still set. If the UI stays Off after reboot, use Reset this PC.
Reboot required.	Pre-reboot message. Not proof that the mode loaded.

Output	Meaning
Reboot now? [y/N]	Answer N. Reboot yourself after you have read the current values.

Optional diagnostic data must be on or SAC will refuse to stay on. The script prints AllowTelemetry and does not block the write when it is lower than 3. Set diagnostic data to Optional before you trust the result. Confirm in Settings, Privacy and security, Diagnostics and feedback.

2. Reboot once

Code Integrity reads the policy at startup. One clean reboot is the restore.

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

Do not boot Safe Mode between the script and this reboot. safeboot must not be set.

3. Confirm the mode loaded

After the normal desktop is up, elevated Command Prompt or PowerShell:

```
CiTool.exe -lp
```

Enforce is loaded when Friendly Name is VerifiedAndReputableDesktop and Is Currently Enforced is true. Evaluation is loaded when Friendly Name is VerifiedAndReputableDesktopEvaluation and Is Currently Enforced is true. Also open Windows Security, App and browser control, and read the Smart App Control page.

Test-SmartAppControlOff.ps1 is the Off gate. After a successful restore it must print Smart App Control is NOT off. and exit 1. That failure is the expected result of turning the feature back on. Exit 0 means the restore did not load.

If it did not stay on

- Current values never showed 1 or 2: the script did not finish the policy write. Read the error, fix elevation, and run it again. Do not reboot for a restore that did not write.
- The value is 1 or 2 before reboot and 0 after reboot: this install will not keep the mode. Reset this PC (Keep my files), with optional diagnostic data enabled, is the remaining path.
- CiTool shows the other mode: you ran Enforce and Evaluation as two writes. Run the one command you want, reboot once, and read CiTool again.
- AllowTelemetry is not 3 and the UI returns to Off: set optional diagnostic data, run the enable script again, and reboot.
- The guest blocks ordinary programs after the reboot: revert pre-sac-off if you have it. Otherwise Reset this PC (Keep my files).

Execution policy

This restore leaves LocalMachine Bypass in place. Leave it when later prototype steps still run scripts. When you want Windows PowerShell back to the usual machine policy, from an elevated window:

```
Set-ExecutionPolicy -Scope LocalMachine RemoteSigned -Force
```

That command does not change Smart App Control. If MachinePolicy or UserPolicy is set, Group Policy still wins and this command does not clear it. PowerShell 7 keeps its own LocalMachine value. Set that one from pwsh if you turned it on during the disable prep.

Order of operations

- Normal desktop, elevated PowerShell. Not Safe Mode.
- Optional diagnostic data on. AllowTelemetry 3.
- .\Enable-SmartAppControl.ps1 for Enforce, or -Mode Evaluation for Evaluation. One of them.
- Require the current value to match 1 or 2. Answer N, then shutdown /r /t 0.
- CiTool.exe -lp shows the matching Friendly Name currently enforced.
- Test-SmartAppControlOff.ps1 prints Smart App Control is NOT off.
- Leave execution policy Bypass unless you have finished the work that needs it.