Application Control for Windows

By jsuther1974

Archived: 2026-04-05 19:57:57 UTC

Your organization's data is one of its most valuable assets... and adversaries want it. No matter what security controls you apply over your data, there are no controls to fully protect your most vulnerable target: the trusted user sitting at the keyboard. When a user runs a process, that process shares the same access to your data that the user has. So your sensitive information is easily transmitted, modified, deleted, or encrypted when a user, intentionally or not, runs malicious software. And with thousands of new malicious files created every day, relying solely on traditional methods like antivirus (AV) solutions gives you an inadequate defense against new attacks.

Application control changes Windows from a place where all code runs unless your AV solution confidently predicts it's bad, to one where code runs only if your policy says so. The cyber threats you face change rapidly, and your defenses need to change too. Government and security organizations, like the Australian Signals Directorate, frequently cite application control as one of the most effective ways to address the threat of executable file-based malware (.exe, .dll, etc.). It works alongside your AV solution to help mitigate security threats by restricting the apps that users can run and even what code runs in the System Core (kernel).

Important

Although application control can significantly harden your computers against malicious code, it's not a replacement for antivirus. You should continue to maintain an active antivirus solution alongside App Control for a well-rounded enterprise security portfolio.

Although we call it application control, the code running on your system isn't always an app. Application control extends beyond apps to also cover scripts and Microsoft installers (MSI), command-line batch files, and even interactive sessions of Windows PowerShell, which run in Constrained Language Mode.

Windows includes two application control technologies you can use depending on your organization's specific scenarios and requirements:

- **App Control for Business (app control)**; and
- **AppLocker**

App Control and Smart App Control

Starting in Windows 11 version 22H2, Smart App Control brings robust application control to consumers and to some small businesses with simpler app portfolios. Smart App Control ensures only signed code runs or code predicted to be safe by our intelligent cloud-powered security service. When code is unsigned and the service is unable to predict with confidence that it's safe to run, then we block it. Over time, the code's reputation might

change as the service processes new signals it receives. Meanwhile, code determined to be unsafe is always blocked.

While Smart App Control is designed for consumers, we believe it's the ideal starting point for most organizations. And since we built it entirely upon App Control for Business, you can create a policy with the same security and compatibility as Smart App Control that also trusts the line-of-business (LOB) apps your organization needs. The service Smart App Control uses to predict what code is safe to run is also available in App Control for Business and called the Intelligent Security Graph (ISG).

Smart App Control starts in evaluation mode and switches off within 48 hours for enterprise managed devices unless the user turns it on first. If you want to proactively turn off Smart App Control across your organization's endpoints, set the **VerifiedAndReputablePolicyState** (DWORD) registry value under `HKLM\SYSTEM\CurrentControlSet\Control\CI\Policy` as shown in the following table. After you change the registry value, you must run CiTool.exe -r for the change to take effect.

Value	Description
0	Off
1	Enforce
2	Evaluation

Important

Once you turn Smart App Control off, it can't be turned on without resetting or reinstalling Windows.

The App Control policy used for Smart App Control comes bundled with the App Control Wizard policy authoring tool and is also found as an example policy at *%windir%/schemas/CodeIntegrity/ExamplePolicies/SmartAppControl.xml*. To use this example policy as a starting point for your own policy, see Use the Smart App Control Policy to build your own base policy. When using the Smart App Control example policy as the basis for your own custom policy, you must remove the option **Enabled:Conditional Windows Lockdown Policy** so it's ready for use as an App Control for Business policy.

Windows edition and licensing requirements

The following table lists the Windows editions that support App Control for Business:

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
Yes	Yes	Yes	Yes

App Control license entitlements are granted by the following licenses:

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
Yes	Yes	Yes	Yes	Yes

For more information about Windows licensing, see Windows licensing overview.

What you should read next

- To learn more about the two application control technologies available in Windows, read App Control for Business and AppLocker Overview.
- To jump right in and get started creating policies, go revisit Smart App Control and Use the Smart App Control policy to build your own starter policy.
