 Filter by title

Application Control for Windows

▾ About application control for Windows

- About application control for Windows
- App Control and AppLocker Overview
- App Control and AppLocker Feature Availability
- Virtualization-based protection of code integrity

▸ Design guide

▸ Deployment guide

▸ Operational guide

▸ AppId Tagging guide

▾ AppLocker

- AppLocker
- Administer AppLocker
- AppLocker design guide
- AppLocker deployment guide
- ▾ AppLocker technical reference
 - AppLocker technical reference
 - What Is AppLocker?**
 - Requirements to use AppLocker
 - AppLocker policy use scenarios
- How AppLocker works
 - AppLocker architecture and components
 - AppLocker processes and interactions
 - AppLocker functions
 - Security considerations for AppLocker
- Tools to Use with AppLocker

What Is AppLocker?

Article • 10/01/2024 • 1 contributor • Applies to:  Windows 11,  Windows 10

 [Feedback](#)

This article for the IT professional describes what AppLocker is.

Windows includes two technologies that can be used for application control, depending on your organization's specific scenarios and requirements: App Control for Business and AppLocker. For information to help you choose when to use App Control or AppLocker, see [App Control and AppLocker overview](#).

AppLocker helps you create rules to allow or deny apps from running based on information about the apps' files. You can also use AppLocker to control which users or groups can run those apps.

Using AppLocker, you can:

- Control the following types of apps and files: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.mst, .msi and .msp), and DLL files (.dll and .ocx), and packaged apps and packaged app installers (appx).
- Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create rules based on the publisher attribute that is persistent through updates, or you can create rules for a specific version of a file.
- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all Windows processes to run except Registry Editor (Regedit.exe).
- Use audit-only mode to deploy the policy and understand its effect before enforcing it.
- Import and export rules. The import and export affects the entire policy. For example, if you export a policy, all of the rules from all of the rule collections are exported, including the enforcement settings for the rule collections. If you import a policy, all criteria in the existing policy are overwritten.
- Streamline creating and managing AppLocker rules by using Windows PowerShell cmdlets.


For information about the application control scenarios that AppLocker addresses, see [AppLocker policy use scenarios](#).


Related articles

- [AppLocker technical reference](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

Additional resources

Training

Module

[Explore advanced protection methods - Training](#)

This module explores additional tools used to provide additional layers of security within an organization.

Certification

[Microsoft Certified: Information Protection and Compliance Administrator Associate - Certifications](#)





Demonstrate the fundamentals of data security, lifecycle management, information security, and compliance to protect a Microsoft 365 deployment.




Events

 Download PDF

Nov 20, 12 AM - Nov 22, 12 AM

Gain the competitive edge you need with powerful AI and Cloud solutions by attending Microsoft Ignite online.
[Register now](#)

 English (United States)  Your Privacy Choices  Theme 

[Manage cookies](#) [Previous Versions](#) [Blog](#)  [Contribute](#) [Privacy](#)  [Terms of Use](#) [Trademarks](#)  © Microsoft 2024