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
      - Tools to Use with AppLocker
      - **Using Event Viewer with AppLocker**

Download PDF

Using Event Viewer with AppLocker

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

Feedback

In this article

Review the AppLocker logs in Windows Event Viewer
Related articles

This article lists AppLocker events and describes how to use Event Viewer with AppLocker.

The AppLocker log contains information about applications affected by AppLocker rules. Each event in the log contains details such as the following information:

- Which file is affected and the path of that file
- Which packaged app is affected and the package identifier of the app
- Whether the file or packaged app is allowed or blocked
- The rule type (path, file hash, or publisher)
- The rule name
- The security identifier (SID) for the user or group identified in the rule

Review the entries in the Event Viewer to determine if any applications aren't included in the rules that you automatically generated. For instance, some line-of-business apps are installed to nonstandard locations, such as the root of the active drive (for example, `%SystemDrive%`).

For info about what to look for in the AppLocker event logs, see Monitor app usage with AppLocker.

> **Note**
>
> The AppLocker event logs are very verbose and can result in a large number of events depending on the policies deployed, particularly in the *AppLocker - EXE and DLL* event log. If you're using an event forwarding and collection service, like LogAnalytics, you may want to adjust the configuration for that event log to only collect Error events or stop collecting events from that log altogether.

Review the AppLocker logs in Windows Event Viewer

1. Open Event Viewer.
2. In the console tree under **Application and Services Logs\Microsoft\Windows**, select **AppLocker**.

The following table contains information about the events that you can use to determine the apps affected by AppLocker rules.

Expand table

Event ID	Level	Event message	Description
8000	Error	AppID policy conversion failed. Status * <%1> *	Indicates that the policy wasn't applied correctly to the computer. The status message is provided for troubleshooting purposes.
8001	Information	The AppLocker policy was applied successfully to this computer.	Indicates that the AppLocker policy was successfully applied to the computer.
8002	Information	*<File name> * was allowed to run.	Indicates an AppLocker rule allowed the .exe or .dll file.

8003	Warning	*<File name> * was allowed to run but would have been prevented from running if the AppLocker policy were enforced.	Shown only when the **Audit only** enforcement mode is enabled. Indicates that the AppLocker policy would block the .exe or .dll file if the enforcement mode setting was **Enforce rules**.
8004	Error	*<File name> * was prevented from running.	AppLocker blocked the named EXE or DLL file. Shown only when the **Enforce rules** enforcement mode is enabled.
8005	Information	*<File name> * was allowed to run.	Indicates an AppLocker rule allowed the script or .msi file.
8006	Warning	*<File name> * was allowed to run but would have been prevented from running if the AppLocker policy were enforced.	Shown only when the **Audit only** enforcement mode is enabled. Indicates that the AppLocker policy would block the script or .msi file if the **Enforce rules** enforcement mode was enabled.
8007	Error	*<File name> * was prevented from running.	AppLocker blocked the named Script or MSI. Shown only when the **Enforce rules** enforcement mode is enabled.
8008	Warning	*<File name> *: AppLocker component not available on this SKU.	Indicates an edition of Windows that doesn't support AppLocker.
8020	Information	*<File name> * was allowed to run.	Added in Windows Server 2012 and Windows 8.
8021	Warning	*<File name> * was allowed to run but would have been prevented from running if the AppLocker policy were enforced.	Added in Windows Server 2012 and Windows 8.
8022	Error	*<File name> * was prevented from running.	Added in Windows Server 2012 and Windows 8.
8023	Information	*<File name> * was allowed to be installed.	Added in Windows Server 2012 and Windows 8.
8024	Warning	*<File name> * was allowed to run but would have been prevented from running if the AppLocker policy were enforced.	Added in Windows Server 2012 and Windows 8.
8025	Error	*<File name> * was prevented from running.	Added in Windows Server 2012 and Windows 8.
8027	Error	No packaged apps can be executed while Exe rules are being enforced and no Packaged app rules have been configured.	Added in Windows Server 2012 and Windows 8.
8028	Warning	*<File name> * was allowed to run but would have been prevented if the Config CI policy were enforced.	Added in Windows Server 2016 and Windows 10.
8029	Error	*<File name> * was prevented from running due to Config CI policy.	Added in Windows Server 2016 and Windows 10.
8030	Information	ManagedInstaller check SUCCEEDED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8031	Information	SmartlockerFilter detected file * being written by process *	Added in Windows Server 2016 and Windows 10.
8032	Error	ManagedInstaller check FAILED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8033	Warning	ManagedInstaller check FAILED during Appid verification of * . Allowed to run due to Audit AppLocker Policy.	Added in Windows Server 2016 and Windows 10.
8034	Information	ManagedInstaller Script check FAILED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8035	Error	ManagedInstaller Script check SUCCEEDED during Appid verification of *	Added in Windows Server 2016 and Windows 10.
8036	Error	* was prevented from running due to Config CI policy	Added in Windows Server 2016 and Windows 10.
8037	Information	* passed Config CI policy and was allowed to run.	Added in Windows Server 2016 and Windows 10.

8038	Information	Publisher info: Subject: * Issuer: * Signature index * (* total)	Added in Windows Server 2016 and Windows 10.
8039	Warning	Package family name * version * was allowed to install or update but would have been prevented if the Config CI policy	Added in Windows Server 2016 and Windows 10.
8040	Error	Package family name * version * was prevented from installing or updating due to Config CI policy	Added in Windows Server 2016 and Windows 10.

Related articles

- Tools to use with AppLocker

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module

Manage and monitor Windows Server event logs - Training

Learn how Event Viewer provides a convenient and accessible location for you to observe events that occur. Access event information quickly and conveniently. Learn how to interpret the data in the event log.

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

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