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
  - Operational guide
  - App Control debugging and troubleshooting
  - **Understanding App Control event IDs**
  - Understanding App Control event tags
  - Query App Control events with Advanced hunting
  - Known Issues
  - Managed installer and ISG technical reference and troubleshooting guide
  - CITool.exe technical reference
  - Inbox App Control policies
- AppId Tagging guide
- AppLocker

Understanding App Control events

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

In this article

App Control Events Overview
App Control block events for executables, dlls, and drivers
App Control block events for packaged apps, MSI installers, scripts, and COM objects
App Control policy activation events
Show 2 more

App Control Events Overview

App Control logs events when a policy is loaded, when a file is blocked, or when a file would be blocked if in audit mode. These block events include information that identifies the policy and gives more details about the block. App Control doesn't generate events when a binary is allowed. However, you can turn on allow audit events for files authorized by a managed installer or the Intelligent Security Graph (ISG) as described later in this article.

Core App Control event logs

App Control events are generated under two locations in the Windows Event Viewer:

- **Applications and Services logs - Microsoft - Windows - CodeIntegrity - Operational** includes events about App Control policy activation and the control of executables, dlls, and drivers.
- **Applications and Services logs - Microsoft - Windows - AppLocker - MSI and Script** includes events about the control of MSI installers, scripts, and COM objects.

Most app and script failures that occur when App Control is active can be diagnosed using these two event logs. This article describes in greater detail the events that exist in these logs. To understand the meaning of different data elements, or tags, found in the details of these events, see Understanding App Control event tags.

> **Note**
>
> **Applications and Services logs - Microsoft - Windows - AppLocker - MSI and Script** events are not included on Windows Server Core edition.

App Control block events for executables, dlls, and drivers

These events are found in the **CodeIntegrity - Operational** event log.

Expand table

Event ID	Explanation
3004	This event isn't common and may occur with or without an App Control policy present. It typically indicates a kernel driver tried to load with an invalid signature. For example, the file may not be WHQL-signed on a system where WHQL is required. This event is also seen for kernel- or user-mode code that the developer opted-in to /INTEGRITYCHECK but isn't signed correctly.
3033	This event may occur with or without an App Control policy present and should occur alongside a 3077 event if caused by App Control policy. It often means the file's signature is revoked or a signature with the

Download PDF

	Lifetime Signing EKU has expired. Presence of the Lifetime Signing EKU is the only case where App Control blocks files due to an expired signature. Try using option `20 Enabled:Revoked Expired As Unsigned` in your policy along with a rule (for example, hash) that doesn't rely on the revoked or expired cert. This event also occurs if code compiled with Code Integrity Guard (CIG) tries to load other code that doesn't meet the CIG requirements.
3034	This event isn't common. It's the audit mode equivalent of event 3033.
3076	This event is the main App Control block event for audit mode policies. It indicates that the file would have been blocked if the policy was enforced.
3077	This event is the main App Control block event for enforced policies. It indicates that the file didn't pass your policy and was blocked.
3089	This event contains signature information for files that were blocked or audit blocked by App Control. One of these events is created for each signature of a file. Each event shows the total number of signatures found and an index value to identify the current signature. Unsigned files generate a single one of these events with TotalSignatureCount of 0. These events are correlated with 3004, 3033, 3034, 3076 and 3077 events. You can match the events using the `Correlation ActivityID` found in the **System** portion of the event.

App Control block events for packaged apps, MSI installers, scripts, and COM objects

These events are found in the **AppLocker - MSI and Script** event log.

Expand table

Event ID	Explanation
8028	This event indicates that a script host, such as PowerShell, queried App Control about a file the script host was about to run. Since the policy was in audit mode, the script or MSI file should have run, but wouldn't have passed the App Control policy if it was enforced. Some script hosts may have additional information in their logs. Note: Most third-party script hosts don't integrate with App Control. Consider the risks from unverified scripts when choosing which script hosts you allow to run.
8029	This event is the enforcement mode equivalent of event 8028. Note: While this event says that a script was blocked, the script hosts control the actual script enforcement behavior. The script host may allow the file to run with restrictions and not block the file outright. For example, PowerShell runs script not allowed by your App Control policy in Constrained Language Mode.
8036	COM object was blocked. To learn more about COM object authorization, see Allow COM object registration in an App Control for Business policy.
8037	This event indicates that a script host checked whether to allow a script to run, and the file passed the App Control policy.
8038	Signing information event correlated with either an 8028 or 8029 event. One 8038 event is generated for each signature of a script file. Contains the total number of signatures on a script file and an index as to which signature it is. Unsigned script files generate a single 8038 event with TotalSignatureCount 0. These events are correlated with 8028 and 8029 events and can be matched using the `Correlation ActivityID` found in the **System** portion of the event.
8039	This event indicates that a packaged app (MSIX/AppX) was allowed to install or run because the App Control policy is in audit mode. But, it would have been blocked if the policy was enforced.
8040	This event indicates that a packaged app was prevented from installing or running due to the App Control policy.

App Control policy activation events

These events are found in the **CodeIntegrity - Operational** event log.

Expand table

Event ID	Explanation
3095	The App Control policy can't be refreshed and must be rebooted instead.
3096	The App Control policy wasn't refreshed since it's already up-to-date. This event's Details includes useful information about the policy, such as its policy options.
3097	The App Control policy can't be refreshed.

3099	Indicates that a policy has been loaded. This event's Details includes useful information about the App Control policy, such as its policy options.
3100	The App Control policy was refreshed but was unsuccessfully activated. Retry.
3101	App Control policy refresh started for *N* policies.
3102	App Control policy refresh finished for *N* policies.
3103	The system is ignoring the App Control policy refresh. For example, an inbox Windows policy that doesn't meet the conditions for activation.
3105	The system is attempting to refresh the App Control policy with the specified ID.

Diagnostic events for Intelligent Security Graph (ISG) and Managed Installer (MI)

> **Note**
>
> When Managed Installer is enabled, customers using LogAnalytics should be aware that Managed Installer may fire many 3091 events. Customers may need to filter out these events to avoid high LogAnalytics costs.

The following events provide helpful diagnostic information when an App Control policy includes the ISG or MI option. These events can help you debug why something was allowed/denied based on managed installer or ISG. Events 3090, 3091, and 3092 don't necessarily indicate a problem but should be reviewed in context with other events like 3076 or 3077.

Unless otherwise noted, these events are found in either the **CodeIntegrity - Operational** event log or the **CodeIntegrity - Verbose** event log depending on your version of Windows.

Expand table

Event ID	Explanation
3090	*Optional* This event indicates that a file was allowed to run based purely on ISG or managed installer.
3091	This event indicates that a file didn't have ISG or managed installer authorization and the App Control policy is in audit mode.
3092	This event is the enforcement mode equivalent of 3091.
8002	This event is found in the **AppLocker - EXE and DLL** event log. When a process launches that matches a managed installer rule, this event is raised with PolicyName = MANAGEDINSTALLER found in the event Details. Events with PolicyName = EXE or DLL aren't related to App Control.

Events 3090, 3091, and 3092 are reported per active policy on the system, so you may see multiple events for the same file.

ISG and MI diagnostic event details

The following information is found in the details for 3090, 3091, and 3092 events.

Expand table

Name	Explanation
ManagedInstallerEnabled	Indicates whether the specified policy enables managed installer trust
PassesManagedInstaller	Indicates whether the file originated from a MI
SmartlockerEnabled	Indicates whether the specified policy enables ISG trust
PassesSmartlocker	Indicates whether the file had positive reputation according to the ISG
AuditEnabled	True if the App Control policy is in audit mode, otherwise it is in enforce mode
PolicyName	The name of the App Control policy to which the event applies

Enabling ISG and MI diagnostic events

To enable 3090 allow events, create a TestFlags regkey with a value of 0x300 as shown in the following PowerShell command. Then restart your computer.

PowerShell Copy

```
reg add hklm\system\currentcontrolset\control\ci -v TestFlags -t REG_DWORD -d 0x300
```

Events 3091 and 3092 are inactive on some versions of Windows and are turned on by the preceding command.

Appendix

A list of other relevant event IDs and their corresponding description.

Expand table

Event ID	Description
3001	An unsigned driver was attempted to load on the system.
3002	Code Integrity couldn't verify the boot image as the page hash couldn't be found.
3004	Code Integrity couldn't verify the file as the page hash couldn't be found.
3010	The catalog containing the signature for the file under validation is invalid.
3011	Code Integrity finished loading the signature catalog.
3012	Code Integrity started loading the signature catalog.
3023	The driver file under validation didn't meet the requirements to pass the App Control policy.
3024	Windows App Control was unable to refresh the boot catalog file.
3026	Microsoft or the certificate issuing authority revoked the certificate that signed the catalog.
3032	The file under validation is revoked or the file has a signature that is revoked.
3033	The file under validation didn't meet the requirements to pass the App Control policy.
3034	The file under validation wouldn't meet the requirements to pass the App Control policy if it was enforced. The file was allowed since the policy is in audit mode.
3036	Microsoft or the certificate issuing authority revoked the certificate that signed the file being validated.
3064	If the App Control policy was enforced, a user mode DLL under validation wouldn't meet the requirements to pass the App Control policy. The DLL was allowed since the policy is in audit mode.
3065	If the App Control policy was enforced, a user mode DLL under validation wouldn't meet the requirements to pass the App Control policy.
3074	Page hash failure while hypervisor-protected code integrity was enabled.
3075	This event measures the performance of the App Control policy check during file validation.
3076	This event is the main App Control block event for audit mode policies. It indicates that the file would have been blocked if the policy was enforced.
3077	This event is the main App Control block event for enforced policies. It indicates that the file didn't pass your policy and was blocked.
3079	The file under validation didn't meet the requirements to pass the App Control policy.
3080	If the App Control policy was in enforced mode, the file under validation wouldn't have met the requirements to pass the App Control policy.
3081	The file under validation didn't meet the requirements to pass the App Control policy.
3082	If the App Control policy was enforced, the policy would have blocked this non-WHQL driver.
3084	Code Integrity is enforcing WHQL driver signing requirements on this boot session.
3085	Code Integrity isn't enforcing WHQL driver signing requirements on this boot session.
3086	The file under validation doesn't meet the signing requirements for an isolated user mode (IUM) process.
3089	This event contains signature information for files that were blocked or audit blocked by App Control. One 3089 event is created for each signature of a file.

3090	*Optional* This event indicates that a file was allowed to run based purely on ISG or managed installer.
3091	This event indicates that a file didn't have ISG or managed installer authorization and the App Control policy is in audit mode.
3092	This event is the enforcement mode equivalent of 3091.
3095	The App Control policy can't be refreshed and must be rebooted instead.
3096	The App Control policy wasn't refreshed since it's already up-to-date.
3097	The App Control policy can't be refreshed.
3099	Indicates that a policy has been loaded. This event also includes information about the options set by the App Control policy.
3100	The App Control policy was refreshed but was unsuccessfully activated. Retry.
3101	The system started refreshing the App Control policy.
3102	The system finished refreshing the App Control policy.
3103	The system is ignoring the App Control policy refresh.
3104	The file under validation doesn't meet the signing requirements for a PPL (protected process light) process.
3105	The system is attempting to refresh the App Control policy.
3108	Windows mode change event was successful.
3110	Windows mode change event was unsuccessful.
3111	The file under validation didn't meet the hypervisor-protected code integrity (HVCI) policy.
3112	Windows has revoked the certificate that signed the file being validated.
3114	Dynamic Code Security opted the .NET app or DLL into App Control policy validation. The file under validation didn't pass your policy and was blocked.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

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