

[Manage cookies](#)

 Feedback

Page 1 of 12

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.

Expand table

Page 3 of 12

Correlation ActivityID	System

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

Correlation ActivityID	System

App Control policy activation events


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

 Expand table

Event ID	Explanation

N
N


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
	<i>Optional</i>
	AppLocker - EXE and DLL

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

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.

```
reg add hklm\system\currentcontrolset\control\ci -v TestFlags 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

<i>Optional</i>



Feedback

Was this page helpful? Yes No



 English (United States)

 Your Privacy Choices

 Theme 

[Manage cookies](#)



