title	description	ms.prod	ms.technology	ms.localizationpriority	ms.col
Understanding Application Control event IDs	Learn what different Windows Defender Application Control event IDs signify.	windows-client	itpro-security	medium	M365-securit compli

Understanding Application Control events

Applies to

- Windows 10
- Windows 11
- Windows Server 2016 and later (limited events)

A Windows Defender Application Control policy logs events locally in Windows Event Viewer in either enforced or audit mode. These events are generated under two locations:

- Events about Application Control policy activation and the control of executables, dlls, and drivers appear in **Applications and Services logs** > **Microsoft** > **Windows** > **CodeIntegrity** > **Operational**
- Events about the control of MSI installers, scripts, and COM objects appear in **Applications and Services logs** > **Microsoft** > **Windows** > **AppLocker** > **MSI and Script**

> **Note**
>
> These event IDs are not included on Windows Server Core edition.

Windows CodeIntegrity Operational log

Event ID	Explanation
3004	This event isn't common and may occur with or without an Application 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.
3033	This event isn't common. It often means the file's signature is revoked or expired. Try using option `20 Enabled:Revoked Expired As Unsigned` in your policy along with a non-signature rule (for example, hash) to address issues with revoked or expired certs.
3034	This event isn't common. It's the audit mode equivalent of event 3033 described above.
3076	This event is the main Application 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 Application 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 would have been blocked by Application Control. One 3089 event is created for each signature of a file. The event shows the total number of signatures found and an index value to identify the current signature. Unsigned files produce a single 3089 event with TotalSignatureCount 0. 3089 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.

3099	Indicates that a policy has been loaded. This event also includes information about the Application Control policy options that were specified by the policy.

Windows AppLocker MSI and Script log

Event ID	Explanation
8028	This event indicates that a script host, such as PowerShell, queried Application 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. Some script hosts may have additional information in their logs. Note: Most third-party script hosts don't integrate with Application 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 described above. Note: While this event says that a script was blocked, the actual script enforcement behavior is implemented by the script host. The script host may allow the file to run with restrictions and not block the file outright. For example, PowerShell will allow a script to run but only in Constrained Language Mode.
8036	COM object was blocked. To learn more about COM object authorization, see Allow COM object registration in a Windows Defender Application 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 will generate a single 8038 event with TotalSignatureCount 0. 8038 events are correlated with 8028 and 8029 events and can be matched using the `Correlation ActivityID` found in the **System** portion of the event.

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.

Events 3090, 3091 and 3092 prove helpful diagnostic information when the ISG or MI option is enabled by any Application Control policy. These events can help you debug why something was allowed/denied based on managed installer or ISG. These events don't necessarily indicate a problem but should be reviewed in context with other events like 3076 or 3077 described above.

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 Application Control policy is in audit mode.
3092	This event is the enforcement mode equivalent of 3091.

The above events 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.

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 Application Control policy is in audit mode, otherwise it is in enforce mode
PolicyName	The name of the Application 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.

```
reg add hklm\system\currentcontrolset\control\ci -v TestFlags -t REG_DWORD -d 0x30(
```

3091 and 3092 events are inactive on some versions of Windows. The above steps will also turn on those events.

Event ID 3099 Options

The Application Control policy rule option values can be derived from the "Options" field in the Details section of the Code integrity 3099 event. To parse the values, first convert the hex value to binary. To derive and parse these values, follow the below workflow.

- Access Event Viewer.
- Access the Code integrity 3099 event.
- Access the details pane.
- Identify the hex code listed in the "Options" field.
- Convert the hex code to binary.

:::image type="content" source="images/event-3099-options.png" alt-text="Event 3099 policy rule options.":::

For a simple solution for converting hex to binary, follow these steps:

1. Open the Calculator app.
2. Select the menu icon. :::image type="icon" source="images/calculator-menu-icon.png" border="false":::
3. Select **Programmer** mode.
4. Select **HEX**. :::image type="icon" source="images/hex-icon.png" border="false":::
5. Enter your hex code. For example, `80881000`.
6. Switch to the **Bit Toggling Keyboard**. :::image type="icon" source="images/bit-toggling-keyboard-icon.png" border="false":::

:::image type="content" source="images/calculator-with-hex-in-binary.png" alt-text="An example of the calculator app in programmer mode, with a hex code converted into binary.":::

This view will provide the hex code in binary form, with each bit address shown separately. The bit addresses start at 0 in the bottom right. Each bit address correlates to a specific event policy-rule option. If the bit address holds a value of 1, the setting is in the policy.

Next, use the bit addresses and their values from the table below to determine the state of each policy rule-option. For example, if the bit address of 16 holds a value of 1, then the **Enabled: Audit Mode (Default)** option is in the policy. This setting means that the policy is in audit mode.

Bit Address	Policy Rule Option
2	`Enabled:UMCI`
3	`Enabled:Boot Menu Protection`
4	`Enabled:Intelligent Security Graph Authorization`
5	`Enabled:Invalidate EAs on Reboot`
7	`Required:WHQL`
10	`Enabled:Allow Supplemental Policies`
11	`Disabled:Runtime FilePath Rule Protection`
13	`Enabled:Revoked Expired As Unsigned`
16	`Enabled:Audit Mode (Default)`
17	`Disabled:Flight Signing`
18	`Enabled:Inherit Default Policy`
19	`Enabled:Unsigned System Integrity Policy (Default)`
20	`Enabled:Dynamic Code Security`
21	`Required:EV Signers`
22	`Enabled:Boot Audit on Failure`
23	`Enabled:Advanced Boot Options Menu`
24	`Disabled:Script Enforcement`
25	`Required:Enforce Store Applications`

27	`Enabled:Managed Installer`
28	`Enabled:Update Policy No Reboot`

Appendix

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

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 application control policy.
3024	Windows application control was unable to refresh the boot catalog file.
3026	The catalog loaded is signed by a signing certificate that has been revoked by Microsoft and/or the certificate issuing authority.
3032	The file under validation is revoked by the system or the file has a signature that has been revoked.
3033	The file under validation didn't meet the requirements to pass the application control policy.
3034	The file under validation wouldn't meet the requirements to pass the Application Control policy if it was enforced. The file was allowed since the policy is in audit mode.
3036	The signed file under validation is signed by a code signing certificate that has been revoked by Microsoft or the certificate issuing authority.

3064	If the Application Control policy was enforced, a user mode DLL under validation wouldn't meet the requirements to pass the application control policy. The DLL was allowed since the policy is in audit mode.
3065	If the Application Control policy was enforced, a user mode DLL under validation wouldn't meet the requirements to pass the application control policy.
3074	Page hash failure while hypervisor-protected code integrity was enabled.
3075	This event measures the performance of the Application Control policy check during file validation.
3076	This event is the main Application 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 Application 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 application control policy.
3080	If the Application Control policy was in enforced mode, the file under validation wouldn't have met the requirements to pass the application control policy.
3081	The file under validation didn't meet the requirements to pass the application control policy.
3082	If the Application Control policy was in enforced mode, the non-WHQL driver would have been denied by the policy.
3084	Code Integrity will enforce the WHQL driver signing requirements on this boot session.
3085	Code Integrity won't enforce the 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 would have been blocked by Application 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 Application Control policy is in audit mode.
3092	This event is the enforcement mode equivalent of 3091.
3095	The Application Control policy can't be refreshed and must be rebooted instead.
3096	The Application Control policy wasn't refreshed since it's already up-to-date.
3097	The Application Control policy can't be refreshed.
3099	Indicates that a policy has been loaded. This event also includes information about the options that were specified by the Application Control policy.
3100	The application control policy was refreshed but was unsuccessfully activated. Retry.
3101	The system started refreshing the Application Control policy.
3102	The system finished refreshing the Application Control policy.
3103	The system is ignoring the Application 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 Application 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	The file under validation is signed by a certificate that has been explicitly revoked by Windows.