



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies



Learn

Discover ▾

Product documentation ▾

Development languages ▾

Topics ▾



[Sign in](#)

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

[Return to main site](#)



Filter by title

[Learn](#) / [Previous versions](#) / [Windows](#) / [Security auditing](#) / [Ac](#)



▾ Security auditing

Security auditing

▸ Basic security audit policies

▾ Advanced security audit policies

Advanced security audit policies

Planning and deploying advanced security audit policies

▾ Advanced security auditing FAQ

Advanced security auditing FAQ

# 5038(F): Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.

Article • 09/08/2021 • [1 contributor](#)

Which editions of  
Windows support  
advanced audit policy  
configuration  
How to list XML elements  
in \<EventData>  
> Using advanced security  
auditing options to  
.. . . .

The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.

This event generates by [Code Integrity](#) feature, if signature of a file isn't valid.

Code Integrity is a feature that improves the security of the operating system by validating the integrity of a driver or system file each time it's loaded into memory. Code Integrity detects whether an unsigned driver or system file is being loaded into the kernel, or whether a system file has been modified by malicious software that is being run by a user account with administrative permissions. On x64-based versions of the operating system, kernel-mode drivers must be digitally signed.

There's no example of this event in this document.

**Subcategory:** [Audit System Integrity](#)

**Event Schema:**

*Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.*

*File Name: %filepath\filename%*

## Security Monitoring Recommendations

- We recommend monitoring for this event, especially on high value assets or computers, because it can be a sign of a software or configuration issue, or a malicious action.

