

ⓘ 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

Event 4612 S: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.

Event 4615 S: Invalid use of LPC port.

Event 4618 S: A monitored security event pattern has occurred.

Event 4816 S: RPC detected an integrity violation while decrypting an incoming message.

Event 5038 F: Code integrity determined that the image hash of a file is not valid.

Event 5056 S: A cryptographic self-test was performed.

Event 5062 S: A kernel-mode cryptographic self-test was performed.

Event 5057 F: A cryptographic primitive operation failed.

Event 5060 F: Verification operation failed.

Event 5061 S, F: Cryptographic operation.

Event 6281 F: Code Integrity determined that the page hashes of an image file are not valid.

Event 6410 F: Code integrity determined that a file does not meet the security requirements to load into a process.

Other Events

Appendix A: Security monitoring recommendations for many audit events

Registry (Global Object Access Auditing)

File System (Global Object Access Auditing)

Windows security

6281(F): Code Integrity determined that the page hashes of an image file aren't valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.

Article • 09/09/2021 • 1 contributor

The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.

[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.

This event generates when [code Integrity](#) determined that the page hashes of an image file aren't valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. This event also generates when signing certificate was revoked. The invalid hashes could indicate a potential disk device error.

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

Subcategory: [Audit System Integrity](#)

Event Schema:

Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.

File Name:%1

Required Server Roles: None.

Minimum OS Version: Windows Server 2008 R2, Windows 7.

Event Versions: 0.

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.