

ⓘ 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 4801 S: The workstation was unlocked.
- Event 4802 S: The screen saver was invoked.
- Event 4803 S: The screen saver was dismissed.
- Event 5378 F: The requested credentials delegation was disallowed by policy.
- Event 5632 S, F: A request was made to authenticate to a wireless network.
- Event 5633 S, F: A request was made to authenticate to a wired network.
- > Audit Special Logon
 - Audit Application Generated
 - Audit Certification Services
- > Audit Detailed File Share
- > Audit File Share
- > Audit File System
- > Audit Filtering Platform Connection
- > Audit Filtering Platform Packet Drop
- > Audit Handle Manipulation
- > Audit Kernel Object
- > Audit Other Object Access Events
- > Audit Registry
 - Audit Removable Storage
- > Audit SAM
- > Audit Central Access Policy Staging
- > Audit Audit Policy Change
- > Audit Authentication Policy Change
- > Audit Authorization Policy Change
 - Audit Filtering Platform Policy Change
- > Audit MPSSVC Rule-Level Policy Change
- > Audit Other Policy Change Events
- > Audit Sensitive Privilege Use
- > Audit Non Sensitive Privilege Use


⋯ / [Audit Other Logon/Logoff Events](#) /

⊕ ⋮

4649(S): A replay attack was detected.

Article • 09/07/2021 • [1 contributor](#)

This event generates on domain controllers when KRB_AP_ERR_REPEAT Kerberos response was sent to the client.

Domain controllers cache information from recently received tickets. If the server name, client name, time, and microsecond fields from the Authenticator match recently seen entries in the cache, it will return KRB_AP_ERR_REPEAT. You can read more about this in [RFC-1510](#) . One potential cause for this is a misconfigured network device between the client and server that could send the same packet(s) repeatedly.

There is no example of this event in this document.

Subcategory: [Audit Other Logon/Logoff Events](#)

Event Schema:

A replay attack was detected.

Subject:

- Security ID:%1
- Account Name:%2
- Account Domain:%3
- Logon ID:%4

Credentials Which Were Replayed:

- Account Name:%5
- Account Domain:%6

Process Information:

- Process ID:%12
- Process Name:%13

Network Information:

- Workstation Name:%10

Detailed Authentication Information:

- Request Type:%7
- Logon Process:%8

Authentication Package:%9

Transited Services:%11

This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration."

Required Server Roles: Active Directory domain controller.

Minimum OS Version: Windows Server 2008.

Event Versions: 0.

Security Monitoring Recommendations

For 4649(S): A replay attack was detected.

- This event can be a sign of Kerberos replay attack or, among other things, network device configuration or routing problems. In both cases, we recommend triggering an alert and investigating the reason the event was generated.