# Audit Other Object Access Events - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 13:31:26 UTC

Audit Other Object Access Events allows you to monitor operations with scheduled tasks, COM+ objects and indirect object access requests.

**Event volume**: Low.

| Computer Type | General Success | General Failure | Stronger Success | Stronger Failure | Comments |
|---|---|---|---|---|---|
| Domain Controller | Yes | Yes | Yes | Yes | We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack. |
| Member Server | Yes | Yes | Yes | Yes | We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack. |
| Workstation | Yes | Yes | Yes | Yes | We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack. |

**Events List:**

- 4671(-): An application attempted to access a blocked ordinal through the TBS.
- 4691(S): Indirect access to an object was requested.
- 5148(F): The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
- 5149(F): The DoS attack has subsided and normal processing is being resumed.

- 4698(S): A scheduled task was created.
- 4699(S): A scheduled task was deleted.
- 4700(S): A scheduled task was enabled.
- 4701(S): A scheduled task was disabled.
- 4702(S): A scheduled task was updated.
- 5888(S): An object in the COM+ Catalog was modified.
- 5889(S): An object was deleted from the COM+ Catalog.
- 5890(S): An object was added to the COM+ Catalog.

---