# Configuring Security Log Audit Settings

[ English ] | [日本語]

## Table of Contents

        - Credential Validation
        - Kerberos Authentication Service
        - Kerberos Service Ticket Operations
    - Account Management
        - Computer Account Management
        - Other Account Management Events
        - Security Group Management
        - User Account Management
    - Detailed Tracking
        - Plug and Play Events
        - Process Creation
        - Process Termination
        - RPC (Remote Procedure Call) Events
        - Token Right Adjusted Events
    - DS (Directory Service) Access
        - Directory Service Access
        - Directory Service Changes
    - Logon/Logoff
        - Account Lockout
        - Group Membership
        - Logoff
        - Logon
        - Other Logon/Logoff Events
        - Special Logon
    - Object Access
        - Certification Services
        - Detailed File Share
        - File Share
        - File System
        - Filtering Platform Connection
        - Filtering Platform Packet Drop
        - Kernel Object
        - Handle Manipulation

# Notes about configuring Security log auditing

- At an organizational level, you can configure the Security log audit policies with Group Policy or InTune. For standalone machines, you can configure with the Local Security Policy Editor (`gpedit.msc`). You can also use PowerShell or Batch scripts with built-in commands such as `auditpol` to configure either standalone machines or use them as startup scripts to configure endpoints at scale.
- You should always enable Security log auditing at the sub-category level (`Computer Configuration > Windows Settings > Security Settings > Advanced security audit policy settings > System Audit Policies` in Group Policy) instead of the broad category level as the latter will usually enable too many events and will override any granular settings you made at the sub-category level.

- In this document, I have ommited sub-categories and event IDs that are not actually used or are not needed for monitoring or DFIR investigations. Only the important ones that you should enable are listed here.
- You cannot turn on or off specific event IDs, only sub-categories at the most granular level. This is unfortunate as sometimes there will be a couple of noisy event IDs that you can not disable unless you disable the entire sub-category.
- The number of sigma rules were taken at 2022/09/24. Be aware that even if there are few or no sigma rules for a certain event, it does not mean that the event is not important.

# Security Event Log Categories and Event IDs

## Account Logon

### Credential Validation

Volume: Depends on NTLM usage. Could be high on DCs and low on clients and servers.

Default settings: `Client OS: No Auditing` | `Server OS: Success`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `Metasploit SMB Authentication`: Detect when someone is running Metasploit on your network.
- `Valid Users Failing to Authenticate from Single Source Using NTLM`: Password guessing.
- `Invalid Users Failing To Authenticate From Single Source Using NTLM`: Username guessing.
- `Failed Logins with Different Accounts from Single Source System`: Password spraying.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4776 | NTLM Authentication | 5 | The original event messages says it is for DCs only but this event gets logged for client OS local authentication as well. |

### Kerberos Authentication Service

> **Note: Enable only for Domain Controllers**

Volume: High.

Default settings: `Client OS: No Auditing` | `Server OS: Success`

Recommended settings: `Client OS: No Auditing` | `Server OS: Success and Failure`

Notable Sigma rules:

- `(4768) PetitPotam Suspicious Kerberos TGT Request`
- `(4768) Disabled Users Failing To Authenticate From Source Using Kerberos`
- `(4768) Invalid Users Failing To Authenticate From Source Using Kerberos`: Username guessing.
- `(4771) Valid Users Failing to Authenticate From Single Source Using Kerberos`: Password guessing.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4768 | Kerberos TGT Request | 3 | |
| 4771 | Kerberos Pre-Auth Failed | 1 | |
| 4772 | Kerberos Authentication Ticket Request Failed | 0 | |

## Kerberos Service Ticket Operations

> **Note: Enable only for Domain Controllers**

Volume: High

Default settings: `Client OS: No Auditing` | `Server OS: Success`

Recommended settings: `Client OS: No Auditing` | `Server OS: Success and Failure`

Notable Sigma rule:

- `(4769) Suspicious Kerberos RC4 Ticket Encryption`: Detects service ticket requests using RC4 encryption. This could be for Kerberoasting (password cracking) or just older systems using legacy encryption.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4769 | Kerberos Service Ticket Request | 1 | |
| 4770 | Kerberos Service Ticket Renewel | 0 | |
| 4773 | Kerberos Service Ticket Request Failed | 0 | This is not actually used. 4769 is used instead. |

# Account Management

## Computer Account Management

Volume: Low on DCs.

Default settings: `Client OS: No Auditing` | `Server OS: Success Only`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `Possible DC Shadow`: Detects DCShadow via create new SPN.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4741 | Computer Account Created | 0 | |
| 4742 | Computer Account Changed | 1 | |
| 4743 | Computer Account Deleted | 0 | |

## Other Account Management Events

Volume: Typically low.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4782 | Account Pasword Hash Was Accessed | 0 | Generated on a DC during password migration of an account using the AD Migration Toolkit or attackers trying to access password hashes. |
| 4793 | Password Policy Checking API Was Called | 0 | Generated during password resets or attackers checking the password policy. |

## Security Group Management

A "security-enabled" group is a group that you can assign access permissions (ACLs). The other type is a Distribution Group, which is "security-disabled" and cannot be assigned access permissions. Since security-enabled groups are most common, we will refer to them simply as "groups". For example, `Local Group Created`, instead of `A security-enabled local group was created.`.

A domain local group is a security or distribution group that can contain universal groups, global groups, other domain local groups from its own domain, and accounts from any domain in the forest. You can give domain local security groups rights and permissions on resources that reside only in the same domain where the domain local group is located.

A global group is a group that can be used in its own domain, in member servers and in workstations of the domain, and in trusting domains. In all those locations, you can give a global group rights and permissions and the global group can become a member of local groups. However, a global group can contain user accounts that are only from its own domain.

A universal group is a security or distribution group that contains users, groups, and computers from any domain in its forest as members. You can give universal security groups rights and permissions on resources in any domain in the forest.

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `User Added to Local Administrators`

- `Operation Wocao Activity` : Detects China-based cyber espionage.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4731 | Local Group Created | 0 | |
| 4732 | Member Added To Local Group | 1 | |
| 4733 | Member Removed From Local Group | 0 | |
| 4734 | Local Group Deleted | 0 | |
| 4764 | Group Type Changed | 0 | |
| 4799 | Local Group Membership Enumerated | 1 | |
| 4727 | Global Group Created | 0 | |
| 4737 | Global Group Changed | 0 | |
| 4728 | Member Added To Global Group | 0 | |
| 4729 | Member Removed From Global Group | 0 | |
| 4730 | Global Group Deleted | 0 | |
| 4754 | Universal Group Created | 0 | |
| 4755 | Universal Group Changed | 0 | |
| 4756 | Member Added To Universal Group | 0 | |
| 4757 | Member Removed From Universal Group | 0 | |
| 4758 | Universal Group Deleted | 0 | |

## User Account Management

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `Hidden Local User Creation`: Detects hidden user accounts most likely used as a backdoor account.
- `Suspicious Windows ANONYMOUS LOGON Local Account Created`
- `Local User Creation`
- `Active Directory User Backdoors`
- `Weak Encryption Enabled and Kerberoast`
- `Addition of SID History to Active Directory Object`: An attacker can use the SID history attribute to gain additional privileges.
- `Possible Remote Password Change Through SAMR`: Detects a possible remote NTLM hash change through SAMR API SamiChangePasswordUser() or SamSetInformationUser().
- `Suspicious Computer Account Name Change CVE-2021-42287`: Detects the renaming of an existing computer account to a account name that doesn't contain a $ symbol as seen in attacks against CVE-2021-42287
- `Password Change on Directory Service Restore Mode (DSRM) Account`: The Directory Service Restore Mode (DSRM) account is a local administrator account on Domain Controllers. Attackers may change the password to gain persistence.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4720 | User Account Created | 3 | |
| 4722 | User Account Enabled | 0 | |
| 4723 | Account Password Change | 0 | |
| 4724 | Account Password Reset | 0 | |
| 4725 | User Account Disabled | 0 | |
| 4726 | User Account Deleted | 0 | |
| 4738 | User Account Changed | 4 | |
| 4740 | User Account Lockout | 0 | |
| 4765 | SID History Added To Account | 0 | |
| 4766 | Attempt To Add SID History To Account Failed | 0 | |
| 4767 | User account was unlocked | 0 | |
| 4780 | ACL Set On Administrators Group Member | 0 | |

| | | | |
|---|---|---|---|
| 4781 | Account Name Changed | 1 | |
| 4794 | DSRM Administrator Password Set | 1 | |
| 4798 | User's Local Group Membership Enumerated | 0 | |
| 5376 | Credential Manager Credentials Backup | 0 | |
| 5377 | Credential Manager Credentials Restored | 0 | |

# Detailed Tracking

## Plug and Play Events

This is important if you want to track physical attacks (Rubber Ducky, etc..) or someone exfiltrating data via USB devices.

Volume: Depends but typically low.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(6416) External Disk Drive Or USB Storage Device`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 6416 | New External Device | 1 | |
| 6419 | Request To Disable Device | 0 | |
| 6420 | Device Disabled | 0 | |
| 6421 | Request To Enable Device | 0 | |
| 6422 | Device Enabled | 0 | |
| 6423 | Device Installation Blocked | 0 | |
| 6424 | Device Installation Allowed After Being Blocked | 0 | |

## Process Creation

Note: A separate setting needs to be enabled to log command line information which is extremely important. `Computer Configuration > Windows Settings > Administrative Templates > System > Audit Process Creation > Include command line in process creation events` in Group Policy.

If you do not have Sysmon installed and configured to monitor Process Creation, then you should enable this as about half of Sigma's detection rules rely on process creation with command line options enabled.

Volume: High.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` if sysmon is not configured.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4688 | Process Creation | 902 | |
| 4696 | Primary Token Assigned To Process | 0 | |

## Process Termination

You may want to keep this disabled to save file space.

Volume: High.

Default settings: `No Auditing`

Recommended settings: `No Auditing` unless you want to track the lifespan of processes.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4689 | Process Exited | 1 | |

## RPC (Remote Procedure Call) Events

Volume: High on RPC servers.

Default settings: `No Auditing`

Recommended settings: `Unknown. Needs testing.`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5712 | RPC Attempt | 0 | Logged when inbound RPC connection is made. |

### Token Right Adjusted Events

Volume: High.

Default settings: `No Auditing`

Recommended settings: `Unknown. Needs testing.`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4703 | User's Token Changed | 0 | |

## DS (Directory Service) Access

> **Note: Enable only for Domain Controllers**

### Directory Service Access

Volume: High on servers running AD DS role services.

Default settings: `Client OS: No Auditing` | `Server OS: Success`

Recommended settings: `Client OS: No Auditing` | `ADDS Server: Success and Failure`

Notable Sigma rules:

- `AD Object WriteDAC Access`
- `Active Directory Replication from Non Machine Account`
- `AD User Enumeration`: Detects access to a domain user from a non-machine account. (Requires the "Read all properties" permission on the user object to be audited for the "Everyone" principal.)
- `DPAPI Domain Backup Key Extraction`: Detects tools extracting LSA secret DPAPI domain backup key from Domain Controllers.
- `WMI Persistence`: Detects malware that autostarts via WMI.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4661 | Handle To Object Requested | 2 | |
| 4662 | Operation Performed On Object | 6 | |

### Directory Service Changes

Volume: High on DCs.

Default settings: `No Auditing`

Recommended settings: `Client OS: No Auditing` | `ADDS Server: Success and Failure`

Notable Sigma rules:

- `Powerview Add-DomainObjectAcl DCSync AD Extend Right`: Backdooring domain object to grant the rights associated with DCSync to a regular user or machine account.
- `Active Directory User Backdoors`: Detects scenarios where one can control another users or computers account without having to use their credentials.
- `Possible DC Shadow`
- `Suspicious LDAP-Attributes Used`: Detects LDAPFragger, a C2 tool that lets attackers route Cobalt Strike beacon data over LDAP attributes.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5136 | Directory Service Object Modified | 6 | |
| 5137 | Directory Service Object Created | 0 | |
| 5138 | Directory Service Object Undeleted | 0 | |
| 5139 | Directory Service Object Moved | 0 | |
| 5141 | Directory Service Object Deleted | 0 | |

## Logon/Logoff

### Account Lockout

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `Scanner PoC for CVE-2019-0708 RDP RCE Vuln` : Detects scans for the BlueKeep vulnerability.
- `Failed Logon From Public IP`
- `Multiple Users Failing to Authenticate from Single Process`
- `Multiple Users Remotely Failing To Authenticate From Single Source`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4625 | Logon Failed Due To Lockout | 4 | |

## Group Membership

Volume: Adds an extra log about a user's group membership to every logon.

Default settings: `No Auditing`

Recommended settings: ACSC recommends `Success and Failure` but this is probably not needed if you can easily lookup what groups a user belongs to.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4627 | Group Membership Information | 0 | Shows what group a user belongs to when they log in. |

## Logoff

Volume: High.

Default settings: `Success`

Recommended settings: `Success`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4634 | Logoff | 0 | |

| | | | |
|---|---|---|---|
| 4647 | User Initiated Logoff | 0 | |

## Logon

Volume: Low on clients, medium on DCs or network servers.

Default settings: `Client OS: Success` | `Server OS: Success and Failure`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `Admin User Remote Logon`
- `Successful Overpass the Hash Attempt`
- `Pass the Hash Activity`
- `RDP Login from Localhost`
- `Login with WMI`
- `KrbRelayUp Attack Pattern`
- `RottenPotato Like Attack Pattern`
- `Failed Logon From Public IP`
- `Suspicious Remote Logon with Explicit Credentials`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4624 | Logon | 11 | |
| 4625 | Logon Failed | 4 | |
| 4648 | Explicit Logon | 2 | |

## Other Logon/Logoff Events

Volume: Low.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4649 | Possible Kerberos Replay Attack | 0 | |
| 4778 | Session Reconnected To Window Station | 0 | Logged at source for RDP or Fast User Switching. |
| 4779 | Session Disconnected From Window Station | 0 | Logged at source for RDP or Fast User Switching. |
| 4800 | Computer Locked | 0 | |
| 4801 | Computer Unlocked | 0 | |
| 4802 | Screensaver Started | 0 | |
| 4803 | Screensaver Stopped | 0 | |
| 5378 | CredSSP Credentials Delegation Blocked | 0 | Usually when WinRM double-hop session was not properly set. |
| 5632 | 802.1x Authentication To Wireless Network | 0 | |
| 5633 | 802.1x Authentication To Wired Network | 0 | |

## Special Logon

"Special groups" and "Special Privileges" can be thought of as Administrator groups or privileges.

Volume: Low on client. Medium on DC or network servers.

Default settings: `Success`

Recommended settings: `Success and Failure`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4672 | Admin Logon | 0 | |
| 4964 | Logon From Admin Group | 0 | |

# Object Access

## Certification Services

> **Note: Enable only for servers providing AD CS role services.**

Volume: Low to medium.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` for AD CS role servers.

Notable Sigma rules:

- `ADCS Certificate Template Configuration Vulnerability with Risky EKU`
- `ADCS Certificate Template Configuration Vulnerability`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4898 | Certificate Services Loaded A Template | 2 | |

> **Note: Many event IDs are enabled. Only the one with sigma rules is shown above.**

## Detailed File Share

Volume: Very high for file servers and DCs, however, may be necessary if you want to track who is accessing what files as well as detect various lateral movement.

> **Warning: There are no SACLs (System Access Control Lists) for shared folders so everything is logged.**

Default settings: `No Auditing`

Recommended settings: `No Auditing` due to the high noise level. Enable if you can though.

Notable Sigma rules:

- `Remote Task Creation via ATSVC Named Pipe`
- `Persistence and Execution at Scale via GPO Scheduled Task`
- `Impacket PsExec Execution`
- `Possible Impacket SecretDump Remote Activity`

- `First Time Seen Remote Named Pipe`
- `Possible PetitPotam Coerce Authentication Attempt`
- `Suspicious Access to Sensitive File Extensions`
- `Transferring Files with Credential Data via Network Shares`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5145 | Network Share File Access | 17 | |

## File Share

Volume: High for file servers and DCs.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(5140) Access to ADMIN$ Share`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5140 | Network Share Connection | 1 | Can be combined with File System auditing to track what files were accessed. |
| 5142 | Network Share Created | 0 | |
| 5143 | Network Share Modified | 0 | |
| 5144 | Network Share Deleted | 0 | |
| 5168 | SPN Check For SMB/SMB2 Failed | 0 | |

## File System

You need to separately configure audit permissions on files and/or folders in order for access to be logged. For example, by right-clicking, opening Properties, Security tab, Advanced, Auditing tab and

then adding a Principal and what permissions to monitor. It is recommended only to monitor access to sensitive files as there will be too much noise if too many files are enabled for logging.

Volume: Depends on SACL rules.

Default settings: `No Auditing`

Recommended settings: Enable SACLs for sensitive files.

Notable Sigma rules:

- `(4663) ISO Image Mount`
- `(4663) Suspicious Teams Application Related ObjectAcess Event`: Detects access to MS Teams authentication tokens.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4656 | Object Handle Requested | 0 | Fails if the process does not have the right permissions. You need to enable the `Handle Manipulation` subcategory to record these events. |
| 4658 | Object Handle Closed | 0 | You need to enable the `Handle Manipulation` subcategory to record these events. |
| 4660 | Object Deleted | 0 | |
| 4663 | Object Access | 2 | Differs from 4656 in that there are only success events. |
| 4664 | Attempt To Create Hard Link | 0 | |
| 4670 | Object Permissions Changed | 0 | |
| 4985 | State Of A Transaction Changed | 0 | Used for Transaction Manager and not relevant for security. |
| 5051 | A File Was Virtualized | 0 | Rarely occurs during LUAFV virtualization. Not relevant for security. |

> **Note: EID 4656, 4658, 4660, 4663, 4670 are also used for access to registry and kernel objects as well as removable storage access but need to be configured separately.**

## Filtering Platform Connection

Logs when WFP (Windows Filtering Platform) allows or blocks port bindings and network connections.

Volume: High.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` if you have enough space and are not monitoring network connections with sysmon. This should cause a high amount of events though.

Notable Sigma rules:

- `(5156) Enumeration via the Global Catalog`: To detect Bloodhound and similar tools.
- `(5156) RDP over Reverse SSH Tunnel WFP`
- `(5156) Remote PowerShell Sessions Network Connections (WinRM)`
- `(5156) Suspicious Outbound Kerberos Connection`: Detects suspicious outbound network activity via kerberos default port indicating possible lateral movement or first stage PrivEsc via delegation.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5031 | WFP Blocked Incoming Connection | 0 | |
| 5150 | WFP Blocked A Packet | 0 | |
| 5151 | A More Restrictive WFP Filter Blocked A Packet | 0 | |
| 5154 | Process Listening For Connections | 0 | |
| 5155 | Process Blocked To Listen For Connections | 0 | |
| 5156 | Network Connection | 4 | |
| 5157 | Network Connection Blocked | 0 | |
| 5158 | Process Binded To Port | 0 | |
| 5159 | Process Blocked To Bind To Port | 0 | |

## Filtering Platform Packet Drop

Volume: High.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` if you have enough space and are not monitoring network connections with sysmon. This should cause a high amount of events though.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 5152 | WFP Blocked A Packet | 0 | |
| 5153 | A More Restrictive WFP Filter Blocked A Packet | 0 | |

## Kernel Object

This feature is mainly for kernel developers. This audits attempts to access the kernel objects, such as mutexes, symbolic links, named pipes, etc... Only kernel objects with SACLs generate security audit events. By default, kernel objects will not have SACLS defined so they will not be audited. You can enable auditing of all kernel objects by enabling `Audit the access of global system objects` (GPO: `Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Audit the access of global system objects`) which will define SACLS for all kernel objects, however, it is not recommended as you will probably generate too many unneeded events. On Windows 11, access to the lsass process seems to be enabled by default, which is good to monitor.

Volume: High if auditing access of global object access is enabled.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` but do not enable `Audit the access of global system objects` as you will generate too many `4663: Object Access` events.

Notable Sigma rules:

- `(4656) Generic Password Dumper Activity on LSASS`
- `(4663) Suspicious Multiple File Rename Or Delete Occurred`: Detects multiple file rename or delete events occurrence within a specified period of time by a same user (these events may indicate ransomware activity).

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4656 | Object Handle Requested | 4 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4658 | Object Handle Closed | 0 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4660 | Object Deleted | 0 | |
| 4663 | Object Access | 2 | |

> **Note: EID 4656, 4658, 4660, 4663 are also used for access to registry and file system objects as well as removable storage access but need to be configured separately.**

## Handle Manipulation

This subcategory needs to be enabled to enable events like `4656`, `4658` and `4661` in other subcategories. It also enables an additional event `4690`, however, this event not useful for investigations. It is recommended to enable this subcategory in order to enable more useful events in other subcategories.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4690 | An attempt was made to duplicate a handle to an object | 0 | |

## Other Object Access Events

It is important to enable as malware will often abuse tasks for persistence and lateral movement.

Volume: Low.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

Notable Sigma rules:

- `(4698) Rare Schtasks Creations`: Detects rare scheduled tasks creations that only appear a few times per time frame and could reveal password dumpers, backdoor installs or other types of malicious code.
- `(4699) Scheduled Task Deletion`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4691 | Indirect Access To Object | 0 | |
| 4698 | Task Created | 2 | |
| 4699 | Task Deleted | 1 | |
| 4700 | Task Enabled | 0 | |
| 4701 | Task Disabled | 1 | |
| 4702 | Task Updated | 0 | |
| 5148 | WFP Detected DoS Attack And Is Blocking Source Packets | 0 | |
| 5149 | DoS Attack Has Subsided And Normal Processing Resumed | 0 | |
| 5888 | COM+ Catalog Object Modified | 0 | |
| 5889 | COM+ Catalog Object Deleted | 0 | |
| 5890 | COM+ Catalog Object Added | 0 | |

## Registry

Many attacks and malware use the registry so it is a great place for evidence, however, it is difficult to only log only what is needed for detection and if you enable all registry access globally, there will be extreme volume of events and possible performance degradation.

Volume: Depends on SACLs.

Default settings: `No Auditing`

Recommended settings: Set SACLs for only the registry keys that you want to monitor.

Notable Sigma rules:

- `(4656) SAM Registry Hive Handle Request`: Attackers will try to access the SAM registry hive to obtain password hashes.
- `(4656) SCM Database Handle Failure`: Detects non-system users failing to get a handle of the SCM database.
- `(4657) COMPlus_ETWEnabled Registry Modification`: Potential adversaries stopping ETW providers recording loaded .NET assemblies.
- `(4657) NetNTLM Downgrade Attack`
- `(4657) Sysmon Channel Reference Deletion`: Potential threat actor tampering with Sysmon manifest and eventually disabling it.
- `(4657) Creation of a Local Hidden User Account by Registry`
- `(4657) UAC Bypass via Sdclt`
- `(4657) Disable Security Events Logging Adding Reg Key MiniNt`
- `(4657) PrinterNightmare Mimimkatz Driver Name`
- `(4657) Security Support Provider (SSP) Added to LSA Configuration`: Detects the addition of a SSP to the registry. Upon a reboot or API call, SSP DLLs gain access to encrypted and plaintext passwords stored in Windows.
- `(4657) Suspicious Run Key from Download`
- `(4657) Suspicious Camera and Microphone Access`
- `(4657) Usage of Sysinternals Tools`
- `(4657) Common Autorun Keys Modification`
- `(4657) Disable Sysmon Event Logging Via Registry`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4656 | Object Handle Requested | 2 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4657 | Registry Value Modified | 182 | |
| 4658 | Object Handle Closed | 0 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4660 | Object Deleted | 0 | |
| 4663 | Object Access | 0 | |

| | | | |
|---|---|---|---|
| 4670 | Object Permissions Changed | 0 | |

> **Note: EID 4656, 4658, 4660, 4663, 4670 are also used for access to kernel and file system objects as well as removable storage access but need to be configured separately.**

## Removable Storage

This logs all file access to removable storage regardless of SACL settings. You may want to enable to track employees exfiltrating data via USB storage.

Volume: Depends on how much removable storage is used.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` if you want to monitor external device usage.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4656 | Object Handle Requested | 0 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4658 | Object Handle Closed | 0 | You need to enable the `Handle Manipulation` subcategory to record this event. |
| 4663 | Object Access | 0 | |

> **Note: EID 4656, 4658, 4663 are also used for access to registry, kernel and file system objects but need to be configured separately.**

## SAM

This will log attempts to access Security Account Manager (SAM) objects, such as user and computer accounts, groups, security descriptors, etc...

Volume: High volume of events on Domain Controllers.

Default settings: `No Auditing`

Recommended settings: `Success and Failure` if you can but may cause too high volume of noise so should be tested beforehand.

Notable Sigma rules:

- `(4661) Reconnaissance Activity`: Detects activity such as "net user administrator /domain" and "net group domain admins /domain".
- `(4661) AD Privileged Users or Groups Reconnaissance`: Detect privileged users or groups recon based on 4661 eventid and known privileged users or groups SIDs.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4661 | Object Handle Requested | 2 | You need to enable the `Handle Manipulation` subcategory to record this event. |

# Policy Change

## Audit Policy Change

Changes to audit policy that are audited include:

- Changing permissions and audit settings on the audit policy object (by using “auditpol /set /sd” command).
- Changing the system audit policy.
- Registering and unregistering security event sources.
- Changing per-user audit settings.
- Changing the value of CrashOnAuditFail.
- Changing audit settings on an object (for example, modifying the system access control list (SACL) for a file or registry key).
- Changing anything in the Special Groups list.

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(4719) Disabling Windows Event Auditing`: Detects anti-forensics via local GPO policy.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4715 | The audit policy (SACL) on an object was changed. | 0 | Logged regardless of Audit Policy Change settings. |
| 4719 | System audit policy was changed. | 1 | Logged regardless of Audit Policy Change settings. |
| 4817 | Auditing settings on object were changed. | 0 | Logged regardless of Audit Policy Change settings. |
| 4902 | The Per-user audit policy table was created. | 0 | |
| 4904 | An attempt was made to register a security event source. | 0 | |
| 4905 | An attempt was made to unregister a security event source. | 0 | |
| 4906 | The CrashOnAuditFail value has changed. | 0 | Logged regardless of Audit Policy Change settings. |
| 4907 | Auditing settings on object were changed. | 0 | |
| 4908 | Special Groups Logon table modified. | 0 | Logged regardless of Audit Policy Change settings. |
| 4912 | Per User Audit Policy was changed. | 0 | Logged regardless of Audit Policy Change settings. |

## Authentication Policy Change

Changes made to authentication policy include:

- Creation, modification, and removal of forest and domain trusts.
- Changes to Kerberos policy under `Computer Configuration > Windows Settings > Security Settings > Account Policies > Kerberos Policy`.
- When any of the following user logon rights is granted to a user or group:
  - Access this computer from the network

    - Allow logon locally
    - Allow logon through Remote Desktop
    - Logon as a batch job
    - Logon as a service
- Namespace collision, such as when an added trust collides with an existing namespace name.

This setting is useful for tracking changes in domain-level and forest-level trust and privileges that are granted to user accounts or groups.

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(4706) Addition of Domain Trusts`: Addition of domains is seldom and should be verified for legitimacy.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4670 | Object permissions changed. | 0 | |
| 4706 | A new trust was created to a domain. | 1 | |
| 4707 | A trust to a domain was removed. | 0 | |
| 4713 | Kerberos policy was changed. | 0 | |
| 4716 | Trusted domain information was modified. | 0 | |
| 4717 | System security access was granted to an account. | 0 | |
| 4718 | System security access was removed from an account. | 0 | |
| 4739 | Domain Policy was changed. | 0 | |
| 4864 | A namespace collision was detected. | 0 | |
| 4865 | A trusted forest information entry was added. | 0 | |
| 4866 | A trusted forest information entry was removed. | 0 | |

| | | | |
|---|---|---|---|
| 4867 | A trusted forest information entry was modified. | 0 | |

## Authorization Policy Change

Audits assignment and removal of user rights in user right policies, changes in security token object permission, resource attributes changes and Central Access Policy changes for file system objects.

You can get information related to changes in user rights policies, or changes of resource attributes or Central Access Policy applied to file system objects. However, if you are using an application or system service that makes changes to system privileges through the AdjustPrivilegesToken API, it is not recommended to enable due to the high volume of events.

Volume: Medium to High.

Default settings: `No Auditing`

Recommended settings: `Unknown. Needs testing.`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4703 | A user right was adjusted. | 0 | As of Windows 10, this event is generated by applications and services that dynamically adjust token privileges. An example is Microsoft Endpoint Configuration Manager, which makes WMI queries at recurring intervals generating a large amount of events from the svchost.exe process. |
| 4704 | A user right was assigned. | 0 | |
| 4705 | A user right was removed. | 0 | |
| 4670 | Object permissions changed. | 0 | |
| 4911 | Resource attributes of the | 0 | |

| | | | |
|---|---|---|---|
| | object were changed. | | |
| 4913 | Central Access Policy on the object was changed. | 0 | |

## Filtering Platform Policy Change

Audit events generated by changes to the Windows Filtering Platform (WFP), such as the following:

- IPsec services status.
- Changes to IPsec policy settings.
- Changes to Windows Filtering Platform Base Filtering Engine policy settings.
- Changes to WFP providers and engine.

Volume: Low.

Default settings: `No Auditing`

Recommended settings: `Unknown, Needs testing.`

> There are too many events that are enabled with this sub-category to list up and no sigma detection rules that use these event IDs at the moment.

## MPSSVC Rule-Level Policy Change

Audit MPSSVC Rule-Level Policy Change determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe). The Microsoft Protection Service, which is used by Windows Firewall, is an integral part of the computer's threat protection against malware. The tracked activities include:

- Active policies when the Windows Firewall service starts.
- Changes to Windows Firewall rules.
- Changes to the Windows Firewall exception list.
- Changes to Windows Firewall settings.
- Rules ignored or not applied by the Windows Firewall service.
- Changes to Windows Firewall Group Policy settings.

Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

Volume: Low.

Default settings: `No Auditing`

Recommended settings: `Unknown. Needs testing.`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4944 | Active policy when FW started. | 0 | |
| 4945 | Rule listed when FW started. | 0 | |
| 4946 | Rule added to FW exception list. | 0 | |
| 4947 | Rule modified to FW exception list. | 0 | |
| 4948 | Rule deleted from FW exception list. | 0 | |
| 4949 | FW settings restored to default. | 0 | |
| 4950 | FW setting changed. | 0 | |
| 4951 | FW rule ignored because major version number was not recognized. | 0 | |
| 4952 | Parts of FW rule ignored because minor version number was not recognized. | 0 | |
| 4953 | FW rule could not be parsed. | 0 | |
| 4954 | FW Group Policy settings changed. New settings applied. | 0 | |
| 4956 | FW active profile changed. | 0 | |
| 4957 | FW did not apply rule. | 0 | |
| 4958 | FW did not apply rule because rule referred to items not configured on this computer. | 0 | |

There are no sigma detection rules for this sub-category at the moment.

### Other Policy Change Events

Audit Other Policy Change Events contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Volume: Low.

Default settings: `No Auditing`

Recommended settings: `No Auditing` (Note: ACSC recommends `Success and Failure`, however, this results in a lot of noise of `5447 (A Windows Filtering Platform filter has been changed)` events being generated.)

> There are too many events that are enabled with this sub-category to list up and no sigma detection rules that use these event IDs at the moment.

## Privilege Use

### Non Sensitive Use Events

Audit Non-Sensitive Privilege Use contains events that show usage of non-sensitive privileges:

- Access Credential Manager as a trusted caller
- Add workstations to domain
- Adjust memory quotas for a process
- Bypass traverse checking
- Change the system time
- Change the time zone
- Create a page file
- Create global objects
- Create permanent shared objects
- Create symbolic links
- Force shutdown from a remote system
- Increase a process working set
- Increase scheduling priority

- Lock pages in memory
- Modify an object label
- Perform volume maintenance tasks
- Profile single process
- Profile system performance
- Remove computer from docking station
- Shut down the system
- Synchronize directory service data

Volume: Very high.

Default settings: `No Auditing`

Recommended settings: `No Auditing`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4673 | A privileged service was called. | 0 | |
| 4674 | An operation was attempted on a privileged object. | 0 | |
| 4985 | The state of a transaction has changed. | 0 | |

> **Note: Non-sensitive and sensitive privilege use events use the same event ID.**

## Sensitive Privilege Use

Audit Sensitive Privilege Use contains events that show the usage of sensitive privileges:

- Act as part of the operating system
- Back up files and directories
- Restore files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers

- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Take ownership of files or other objects

The use of two privileges, "Back up files and directories" and "Restore files and directories," generate events only if the `Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Audit: Audit the access of global system objects` Group Policy setting is enabled. However, it is not recommended to enable this Group Policy setting because of the high number of events recorded.

Volume: High.

Default settings: `No Auditing`

Recommended settings: `Success and Failure. However, this may be too noisy.`

Notable Sigma rules:

- `(4673) User Couldn't Call a Privileged Service 'LsaRegisterLogonProcess'`: The 'LsaRegisterLogonProcess' function verifies that the application making the function call is a logon process by checking that it has the SeTcbPrivilege privilege set. Possible Rubeus tries to get a handle to LSA.
- `(4673) Suspicious Driver Loaded By User`: Detects the loading of drivers via 'SeLoadDriverPrivilege' required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers. If you exclude privileged users/admins and processes, which are allowed to do so, you are maybe left with bad programs trying to load malicious kernel drivers. This will detect Ghost-In-The-Logs (https://github.com/bats3c/Ghost-In-The-Logs) and the usage of Sysinternals and various other tools. So you have to work with a whitelist to find the bad stuff.
- `(4674) SCM Database Privileged Operation`: Detects non-system users performing privileged operation os the SCM database.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4673 | A privileged service was called. | 2 | |
| 4674 | An operation was attempted on a privileged object. | 1 | |

| | | | |
|---|---|---|---|
| 4985 | The state of a transaction has changed. | 0 | |

> **Note: Non-sensitive and sensitive privilege use events use the same event ID.**

# System

## Other System Events

Audit Other System Events contains Windows Firewall Service and Windows Firewall driver start and stop events, failure events for these services and Windows Firewall Service policy processing failures:

- Startup and shutdown of the Windows Firewall service and driver.
- Security policy processing by the Windows Firewall service.
- Cryptography key file and migration operations.
- BranchCache events.

Volume: Low.

Default settings: `Success and Failure`

Recommended settings: `Unknown. Needs testing.`

> There are too many events that are enabled with this sub-category to list up and no sigma detection rules that use these event IDs at the moment.

## Security State Change

Audit Security State Change contains Windows startup, recovery, and shutdown events, and information about changes in system time.

Volume: Low.

Default settings: `Success`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(4616) Unauthorized System Time Modification`: Detect scenarios where a potentially unauthorized application or user is modifying the system time.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4608 | Windows is starting up. | 0 | |
| 4616 | The system time was changed. | 1 | |
| 4621 | Administrator recovered system from CrashOnAuditFail. | 0 | |

## Security System Extension

This policy setting allows you to audit events related to security system extensions or services such as the following:

- A security system extension, such as an authentication, notification, or security package is loaded and is registered with the Local Security Authority (LSA). It is used to authenticate logon attempts, submit logon requests, and any account or password changes. Examples of security system extensions are Kerberos and NTLM.
- A service is installed and registered with the Service Control Manager. The audit log contains information about the service name, binary, type, start type, and service account.

Volume: Low, but more on DCs.

Default settings: `No Auditing`

Recommended settings: `Success and Failure`

Notable Sigma rule:

- `(4611) Register new Logon Process by Rubeus` : Detects potential use of Rubeus via registered new trusted logon process.
- `(4697) Invoke-Obfuscation Obfuscated IEX Invocation`
- `(4697) Invoke-Obfuscation Via Use Rundll32`
- `(4697) Invoke-Obfuscation Via Use MSHTA`
- `(4697) CobaltStrike Service Installations`
- `(4697) Credential Dumping Tools Service Execution`
- `(4697) Malicious Service Installations`
- `(4697) Meterpreter or Cobalt Strike Getsystem Service Installation`

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4610 | An authentication package has been loaded by the Local Security Authority. | 0 | Should be monitored with an allowlist. |
| 4611 | A trusted logon process has been registered with the Local Security Authority. | 1 | Should display "SYSTEM" in the "Subject" field. |
| 4614 | A notification package has been loaded by the Security Account Manager. | 0 | |
| 4622 | A security package has been loaded by the Local Security Authority. | 0 | |
| 4697 | A service was installed in the system. | 20 | This is the most important event in this sub-category. Requires Win 10/2016+. |

## System Integrity

Audit System Integrity determines whether the operating system audits events that violate the integrity of the security subsystem:

- Audited events are lost due to a failure of the auditing system.
- A process uses an invalid local procedure call (LPC) port in an attempt to impersonate a client, reply to a client address space, read to a client address space, or write from a client address space.
- A remote procedure call (RPC) integrity violation is detected.
- A code integrity violation with an invalid hash value of an executable file is detected.
- Cryptographic tasks are performed.

According to Microsoft, violations of security subsystem integrity are critical and could indicate a potential security attack.

Volume: Low.

Default settings: `Sucess, Failure`

Recommended settings: `Success and Failure`

Currently, there are no sigma rules for this sub-category.

| Event ID | Description | Sigma Rules | Notes |
|---|---|---|---|
| 4612 | Potential Log Loss Due To Lack Of Resources | 0 | This is important to monitor. |
| 4615 | Invalid use of LPC port. | 0 | |
| 4618 | A monitored security event pattern has occurred. | 0 | This event can only be invoked manually. |
| 4816 | RPC Integrity Violation | 0 | Orginally `RPC detected an integrity violation while decrypting an incoming message.` |
| 5038 | Code Integrity Error: Invalid Image Hash | 0 | Originally `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.` |
| 5056 | A cryptographic self-test was performed. | 0 | |
| 5057 | A cryptographic primitive operation failed. | 0 | |
| 5060 | Verification operation failed. | 0 | |
| 5061 | Cryptographic operation. | 0 | |

| | | | |
|---|---|---|---|
| 5062 | A kernel-mode cryptographic self-test was performed. | 0 | |
| 6281 | Code Integrity Error: Invalid Image Page Hash | 0 | Originally `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.` |
| 6410 | Code Integrity Error: Requirements Not Met | 0 | |

## Global Object Access Auditing

You can configure all `File system` and `Registry` access to be recorded here but it is not recommended for production due to the very high amount of logs you will generate. It is recommended to turn on when simulating attacks to find out what registry and files are changed in order to write detection rules.