Sign in

SigmaHQ / sigma Public

Notifications Fork 2.2k Star 8.3k

Code Issues 11 Pull requests 35 Discussions Actions Wiki Security I

sigma / documentation / logsource-guides / windows / service / security.md

3214 lines (2669 loc) · 152 KB

Preview Code Blame Raw

service: security

ID: dfd8c0f4-e6ad-4e07-b91b-f2fca0ddef64

Content

▶ Details

Description

This logsource guide describes how to enable the necessary logging to make use of SIGMA rules that leverage the `security` service.

Event Source(s)

```
Provider: Microsoft Windows Security Auditing
GUID: {54849625-5478-4994-a5ba-3e3b0328c30d}
Channel: Security
```

Logging Setup

Account Logon

Credential Validation

- Subcategory GUID: `{0CCE923F-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: [Learn More]
- EventID(s):
    - `4774`
    - `4775`
    - `4776`
    - `4777`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Logon
                        - Audit Credential Validation
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923F-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923F-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - [Learn More]

Kerberos Authentication Service

- Subcategory GUID: `{0CCE9242-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High on Kerberos Key Distribution Center servers`
- API Mapping: Learn More
- EventID(s):
  - `4768`
  - `4771`
  - `4772`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Logon
                        - Audit Kerberos Authentication Service
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9242-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9242-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Kerberos Service Ticket Operations

- Subcategory GUID: `{0CCE9240-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`

- Channel: `Security`
- Event Volume: `Very High on Kerberos Key Distribution Center servers`
- API Mapping: Learn More
- EventID(s):
  - `4769`
  - `4770`
  - `4773`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Logon
                        - Audit Kerberos Service Ticket Operations
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9240-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9240-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Account Logon Events

- Subcategory GUID: `{0CCE9241-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):

    - TBD

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Logon
                        - Audit Other Account Logon Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9241-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9241-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - [Learn More]

Account Management

Application Group Management

- Subcategory GUID: `{0CCE9239-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: [Learn More]
- EventID(s):
    - `4783`
    - `4784`
    - `4785`
    - `4786`

  - `4787`
  - `4788`
  - `4789`
  - `4790`
  - `4791`
  - `4792`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Management
                        - Audit Application Group Management
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Computer Account Management

- Subcategory GUID: `{0CCE9236-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low on domain controllers`
- API Mapping: Learn More
- EventID(s):
  - `4741`

    - `4742`
    - `4743`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Management
                        - Audit Computer Account Management
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Distribution Group Management

- Subcategory GUID: `{0CCE9238-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low on Domain Controllers`
- API Mapping: Learn More
- EventID(s):
    - `4749`
    - `4750`
    - `4751`
    - `4752`
    - `4753`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Management
                        - Audit Distribution Group Management
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Account Management Events

- Subcategory GUID: `{0CCE923A-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Typically Low on all types of computers`
- API Mapping: Learn More
- EventID(s):
    - `4782`
    - `4793`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
```

```
      - Advanced Audit Policy Configuration
        - System Audit Policies - Local Group Policy Object
          - Account Management
            - Audit Other Account Management Events
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923A-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923A-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Security Group Management

- Subcategory GUID: `{0CCE9237-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - `4728`
  - `4731`
  - `4732`
  - `4733`
  - `4734`
  - `4735`
  - `4764`
  - `4799`
  - `4727`
  - `4737`
  - `4728`
  - `4729`

  - `4730`
  - `4754`
  - `4755`
  - `4756`
  - `4757`
  - `4758`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Management
                        - Audit Security Group Management
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

User Account Management

- Subcategory GUID: `{0CCE9235-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - `4720`

  - `4722`
  - `4723`
  - `4724`
  - `4725`
  - `4726`
  - `4738`
  - `4740`
  - `4765`
  - `4766`
  - `4767`
  - `4780`
  - `4781`
  - `4794`
  - `4798`
  - `5376`
  - `5377`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Account Management
                        - Audit User Account Management
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Detailed Tracking

DPAPI Activity

- Subcategory GUID: `{0CCE922D-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - `4692`
  - `4693`
  - `4694`
  - `4695`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
                        - Audit DPAPI Activity
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922D-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922D-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

PNP Activity

- Subcategory GUID: `{0CCE9248-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Varies, depending on how the computer is used. Typically Low.`
- API Mapping: Learn More
- EventID(s):
  - `6416`
  - `6419`
  - `6420`
  - `6421`
  - `6422`
  - `6423`
  - `6424`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
                        - Audit PNP Activity
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9248-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9248-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Process Creation

- Subcategory GUID: `{0CCE922B-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: [Learn More]
- EventID(s):
  - `4688`
  - `4696`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
                        - Audit Process Creation
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922B-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922B-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - [Learn More]

Process Termination

- Subcategory GUID: `{0CCE922C-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`

- Event Volume: `Low to Medium, depending on system usage.`
- API Mapping: [Learn More]
- EventID(s):
  - `4689`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
                        - Audit Process Termination
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922C-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922C-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - [Learn More]

RPC Events

- Subcategory GUID: `{0CCE922E-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: [Learn More]
- EventID(s):
  - `5712`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
                        - Audit RPC Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922E-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922E-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Token Right Adjusted

- Subcategory GUID: `{0CCE924A-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
    - `4703`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Detailed Tracking
            - Audit Token Right Adjusted
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE924A-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE924A-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

DS Access

Detailed Directory Service Replication

- Subcategory GUID: `{0CCE923E-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `These events can create a very high volume of event data on domain controllers`
- API Mapping: Learn More
- EventID(s):
  - `4928`
  - `4929`
  - `4930`
  - `4931`
  - `4934`
  - `4935`
  - `4936`
  - `4937`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - DS Access
                        - Audit Detailed Directory Service Replication
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923E-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923E-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Directory Service Access

- Subcategory GUID: `{0CCE923B-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High on servers running AD DS role services.`
- API Mapping: Learn More
- EventID(s):
  - `4661`
  - `4662`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - DS Access
```

```
                        - Audit Directory Service Access
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923B-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923B-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Directory Service Changes

- Subcategory GUID: `{0CCE923C-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High on Domain Controllers`
- API Mapping: Learn More
- EventID(s):
  - `5136`
  - `5137`
  - `5138`
  - `5139`
  - `5141`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - DS Access
                        - Audit Directory Service Changes
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Directory Service Replication

- Subcategory GUID: `{0CCE923D-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium on Domain Controllers`
- API Mapping: Learn More
- EventID(s):
  - `4932`
  - `4933`

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - DS Access
                        - Audit Directory Service Replication
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923D-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923D-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Logon/Logoff

Account Lockout

- Subcategory GUID: `{0CCE9217-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 4625

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Account Lockout
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9217-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9217-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

User/Device Claims

- Subcategory GUID: `{0CCE9247-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume:
  - `Low on a client computer.`
  - `Medium on a domain controller or network servers.`
- API Mapping: Learn More
- EventID(s):
  - 4626

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit User/Device Claims
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9247-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9247-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Group Membership

- Subcategory GUID: `{0CCE9249-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`

- Event Volume:
  - `Low on a client computer.`
  - `Medium on a domain controller or network servers.`
- API Mapping: Learn More
- EventID(s):
  - 4627

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Group Membership
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE923F-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE923F-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

IPsec Extended Mode

- Subcategory GUID: `{0CCE921A-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
  - 4978

  - 4979
  - 4980
  - 4981
  - 4982
  - 4983
  - 4984

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit IPsec Extended Mode
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921A-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921A-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

IPsec Main Mode

- Subcategory GUID: `{0CCE9218-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
  - 4646

  - 4650
  - 4651
  - 4652
  - 4653
  - 4655
  - 4976
  - 5049
  - 5453

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit IPsec Main Mode
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9218-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9218-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

IPsec Quick Mode

- Subcategory GUID: `{0CCE9219-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More

- EventID(s):
    - 4977
    - 5451
    - 5452

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit IPsec Quick Mode
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9219-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9219-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Logoff

- Subcategory GUID: `{0CCE9216-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
    - 4634
    - 4647

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Logoff
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9216-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9216-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Logon

- Subcategory GUID: `{0CCE9215-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume:
  - `Low on a client computer.`
  - `Medium on a domain controllers or network servers.`
- API Mapping: Learn More
- EventID(s):
  - 4624
  - 4625
  - 4648
  - 4675

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Logon
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9215-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9215-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Network Policy Server

- Subcategory GUID: `{0CCE9243-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium to High on servers that are running Network Policy Server (NPS).`
- API Mapping: Learn More
- EventID(s):
    - 6272
    - 6273
    - 6274
    - 6275
    - 6276
    - 6277
    - 6278

  - 6279
  - 6280

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Network Policy Server
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9243-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9243-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Logon/Logoff Events

- Subcategory GUID: `{0CCE921C-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 4649
  - 4778
  - 4779
  - 4800
  - 4801

  - 4802
  - 4803
  - 5378
  - 5632
  - 5633

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Other Logon/Logoff Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921C-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921C-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Special Logon

- Subcategory GUID: `{0CCE921B-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume:
  - `Low on a client computer.`
  - `Medium on a domain controllers or network servers.`
- API Mapping: Learn More
- EventID(s):

  - 4964
  - 4672

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Logon/Logoff
                        - Audit Special Logon
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921B-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921B-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Object Access

Application Generated

- Subcategory GUID: `{0CCE9222-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
  - 4665
  - 4666
  - 4667

  - 4668

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Application Generated
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9222-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9222-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Certification Services

- Subcategory GUID: `{0CCE9221-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low to medium on servers that provide AD CS role services`
- API Mapping: Learn More
- EventID(s):
  - 4868
  - 4869
  - 4870
  - 4871
  - 4872
  - 4873

  - 4874
  - 4875
  - 4876
  - 4877
  - 4878
  - 4879
  - 4880
  - 4881
  - 4882
  - 4883
  - 4884
  - 4885
  - 4886
  - 4887
  - 4888
  - 4889
  - 4890
  - 4891
  - 4892
  - 4893
  - 4894
  - 4895
  - 4896
  - 4897
  - 4898

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Certification Services
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9221-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9221-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Detailed File Share

- Subcategory GUID: `{0CCE9244-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume:
  - `High on file servers.`
  - `High on domain controllers because of SYSVOL network access required by Group Policy.`
  - `Low on member servers and workstations.`
- API Mapping: Learn More
- EventID(s):
  - 5145

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Detailed File Share
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9244-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9244-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

File Share

- Subcategory GUID: `{0CCE9224-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume:
  - `High on file servers.`
  - `High on domain controllers because of SYSVOL network access required by Group Policy.`
  - `Low on member servers and workstations.`
- API Mapping: Learn More
- EventID(s):
  - 5140
  - 5142
  - 5143
  - 5144
  - 5168

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit File Share
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9224-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9224-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

File System

- Subcategory GUID: `{0CCE921D-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Varies, depending on how file system SACLs are configured`
- API Mapping: Learn More
- EventID(s):
  - 4656
  - 4658
  - 4660
  - 4663
  - 4664
  - 4670
  - 4985
  - 5051

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
            - Audit File System
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921D-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921D-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - [Learn More](#)

Filtering Platform Connection

- Subcategory GUID: `{0CCE9226-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: [Learn More](#)
- EventID(s):
  - 5031
  - 5150
  - 5151
  - 5154
  - 5155
  - 5156
  - 5157
  - 5158
  - 5159

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
  - Windows Settings
    - Security Settings
```

```
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Filtering Platform Connection
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Filtering Platform Packet Drop

- Subcategory GUID: `{0CCE9225-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
  - 5152
  - 5153

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Filtering Platform Packet Drop
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Handle Manipulation

- Subcategory GUID: `{0CCE9223-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
  - 4658
  - 4690

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Handle Manipulation
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9223-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9223-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Kernel Object

- Subcategory GUID: `{0CCE921F-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
  - 4656
  - 4658
  - 4660
  - 4663

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Kernel Object
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921F-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921F-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Object Access Events

- Subcategory GUID: `{0CCE9227-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium to High`
- API Mapping: Learn More
- EventID(s):
  - 4671
  - 4691
  - 4698
  - 4699
  - 4700
  - 4701
  - 4702
  - 5148
  - 5149
  - 5888
  - 5889
  - 5890

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Other Object Access Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9227-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9227-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Registry

- Subcategory GUID: `{0CCE921E-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low to Medium, depending on how registry SACLs are configured.`
- API Mapping: Learn More
- EventID(s):
  - 4656
  - 4657
  - 4658
  - 4660
  - 4663
  - 4670
  - 5039

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Registry
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE921E-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE921E-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Removable Storage

- Subcategory GUID: `{0CCE9245-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
  - 4656
  - 4658
  - 4663

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Removable Storage
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9245-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9245-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

SAM

- Subcategory GUID: `{0CCE9220-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High on domain controllers`
- API Mapping: Learn More
- EventID(s):
  - 4661

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit SAM
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9220-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9220-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Central Access Policy Staging

- Subcategory GUID: `{0CCE9246-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
  - 4818

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Object Access
                        - Audit Central Access Policy Staging
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9246-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9246-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Policy Change

Audit Policy Change

- Subcategory GUID: `{0CCE922F-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`

- API Mapping: Learn More
- EventID(s):
  - 4715
  - 4719
  - 4817
  - 4902
  - 4906
  - 4907
  - 4908
  - 4912
  - 4904
  - 4905

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Policy Change
                        - Audit Audit Policy Change
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Authentication Policy Change

- Subcategory GUID: `{0CCE9230-69AE-11D9-BED3-505054503030}`

- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 4670
  - 4706
  - 4707
  - 4716
  - 4713
  - 4717
  - 4718
  - 4739
  - 4864
  - 4865
  - 4866
  - 4867

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Policy Change
                        - Audit Authentication Policy Change
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9230-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9230-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Authorization Policy Change

- Subcategory GUID: `{0CCE9231-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium to High`
- API Mapping: Learn More
- EventID(s):
  - 4703
  - 4704
  - 4705
  - 4670
  - 4911
  - 4913

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Policy Change
                        - Audit Authorization Policy Change
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9231-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9231-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Filtering Platform Policy Change

- Subcategory GUID: `{0CCE9233-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
    - 4709
    - 4710
    - 4711
    - 4712
    - 5040
    - 5041
    - 5042
    - 5043
    - 5044
    - 5045
    - 5046
    - 5047
    - 5048
    - 5440
    - 5441
    - 5442
    - 5443
    - 5444
    - 5446
    - 5448
    - 5449

  - 5450
  - 5456
  - 5457
  - 5458
  - 5459
  - 5460
  - 5461
  - 5462
  - 5463
  - 5464
  - 5465
  - 5466
  - 5467
  - 5468
  - 5471
  - 5472
  - 5473
  - 5474
  - 5477

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Policy Change
                        - Audit Filtering Platform Policy Change
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9233-69AE-11D9-BED3-505054503030}, /success:enable
```

```
# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9233-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

MPSSVC Rule-Level Policy Change

- Subcategory GUID: `{0CCE9232-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium`
- API Mapping: Learn More
- EventID(s):
    - 4944
    - 4945
    - 4946
    - 4947
    - 4948
    - 4949
    - 4950
    - 4951
    - 4952
    - 4953
    - 4954
    - 4956
    - 4957
    - 4958

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
        - System Audit Policies - Local Group Policy Object
          - Policy Change
            - Audit MPSSVC Rule-Level Policy Change
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9232-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9232-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Policy Change Events

- Subcategory GUID: `{0CCE9234-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium to High`
- API Mapping: Learn More
- EventID(s):
  - 4714
  - 4819
  - 4826
  - 4909
  - 4910
  - 5063
  - 5064
  - 5065
  - 5066
  - 5067
  - 5068
  - 5069
  - 5070

  - 5447
  - 6144
  - 6145

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Policy Change
                        - Audit Other Policy Change Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9234-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9234-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Privilege Use

Non Sensitive Privilege Use

- Subcategory GUID: `{0CCE9229-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Very High`
- API Mapping: Learn More
- EventID(s):
  - 4673
  - 4674

  - 4985

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - Privilege Use
                        - Audit Non Sensitive Privilege Use
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9229-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9229-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other Privilege Use Events

- Subcategory GUID: `{0CCE922A-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: TBD
- API Mapping: Learn More
- EventID(s):
  - 4985

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
    - Security Settings
      - Advanced Audit Policy Configuration
        - System Audit Policies - Local Group Policy Object
          - Object Access
            - Privilege Use
             - Audit Other Privilege Use Events
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE922A-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE922A-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Sensitive Privilege Use

- Subcategory GUID: `{0CCE9228-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `High`
- API Mapping: Learn More
- EventID(s):
  - 4673, 4674, 4985

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
  - Windows Settings
    - Security Settings
      - Advanced Audit Policy Configuration
        - System Audit Policies - Local Group Policy Object
          - Object Access
            - Privilege Use
```

```
             - Audit Sensitive Privilege Use
              - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9228-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9228-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

System

IPsec Driver

- Subcategory GUID: `{0CCE9213-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Medium`
- API Mapping: Learn More
- EventID(s):
  - 4960
  - 4961
  - 4962
  - 4963
  - 4965
  - 5478
  - 5479
  - 5480
  - 5483
  - 5484
  - 5485

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - System
                        - Audit IPsec Driver
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9213-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9213-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Other System Events

- Subcategory GUID: `{0CCE9214-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 5024
  - 5025
  - 5027
  - 5028
  - 5029
  - 5030
  - 5032

  - 5033
  - 5034
  - 5035
  - 5037
  - 5058
  - 5059
  - 6400
  - 6401
  - 6402
  - 6403
  - 6404
  - 6405
  - 6406
  - 6407
  - 6408
  - 6409

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - System
                        - Audit Other System Events
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9214-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9214-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Security State Change

- Subcategory GUID: `{0CCE9210-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
    - 4608
    - 4616
    - 4621

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - System
                        - Audit Security State Change
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9210-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9210-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Security System Extension

- Subcategory GUID: `{0CCE9211-69AE-11D9-BED3-505054503030}`

- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`
- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 4610
  - 4611
  - 4614
  - 4622
  - 4697

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - System
                        - Audit Security System Extension
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9211-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9211-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

System Integrity

- Subcategory GUID: `{0CCE9212-69AE-11D9-BED3-505054503030}`
- Provider: `Microsoft Windows Security Auditing`
- Channel: `Security`

- Event Volume: `Low`
- API Mapping: Learn More
- EventID(s):
  - 4612
  - 4615
  - 4618
  - 4816
  - 5038
  - 5056
  - 5062
  - 5057
  - 5060
  - 5061
  - 6281
  - 6410

If you're using `gpedit.msc` or similar you can enable logging for this category by following the structure below

```
- Computer Configuration
    - Windows Settings
        - Security Settings
            - Advanced Audit Policy Configuration
                - System Audit Policies - Local Group Policy Object
                    - System
                        - Audit System Integrity
                            - Success and Failure
```

Alternatively you can enable logging via `auditpol` using the following command(s):

```
# Enable Success audit Only
auditpol /set /subcategory:{0CCE9212-69AE-11D9-BED3-505054503030}, /success:enable

# Enable both Success and Failure auditing
auditpol /set /subcategory:{0CCE9212-69AE-11D9-BED3-505054503030}, /success:enable
```

If you want to learn more about this sub-category. You can do so via MSDN - Learn More

Global Object Access Auditing

TBD

Full Event(s) List

▶ Expand Full List

Event Fields

Provider: Microsoft Windows Security Auditing / EventID: 4624

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4627

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4663

▶ Expand Details

Provider: Microsoft Windows Security Auditing / EventID: 4670

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4672

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4673

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4688

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4689

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4702

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4703

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 4957

▶ Expand

Provider: Microsoft Windows Security Auditing / EventID: 5447

▶ Expand