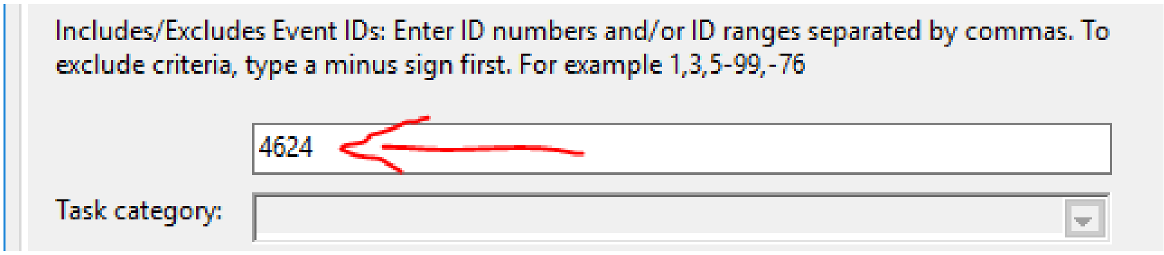
Successful logon
Event ID 4624

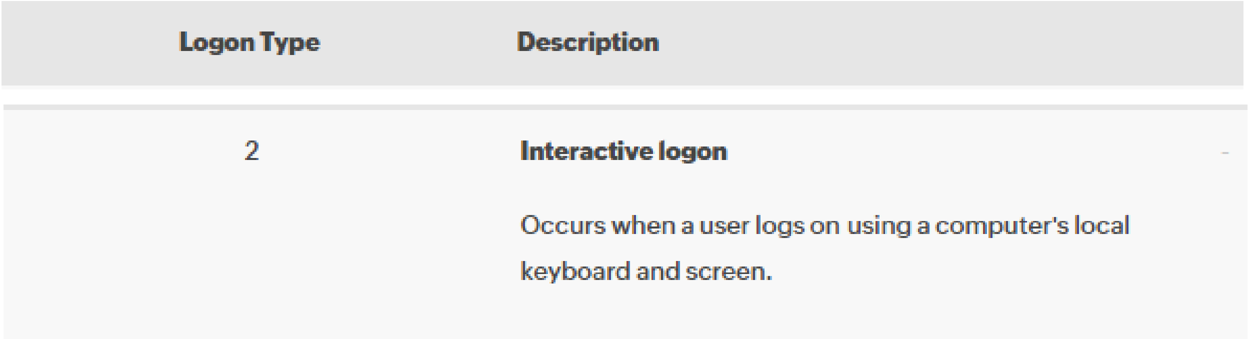


Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

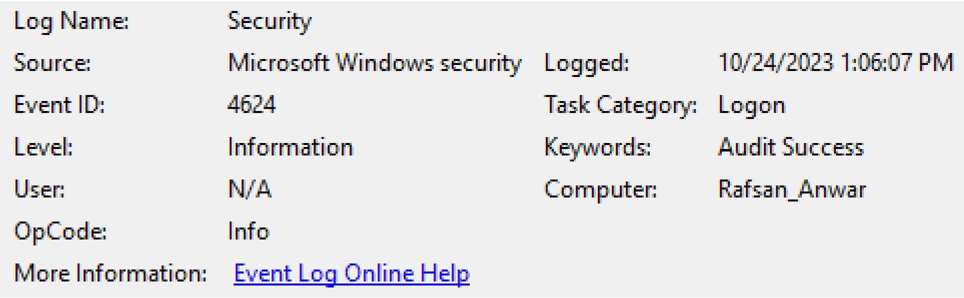
4624

Task category:

Logon Type 2 indicates physical login

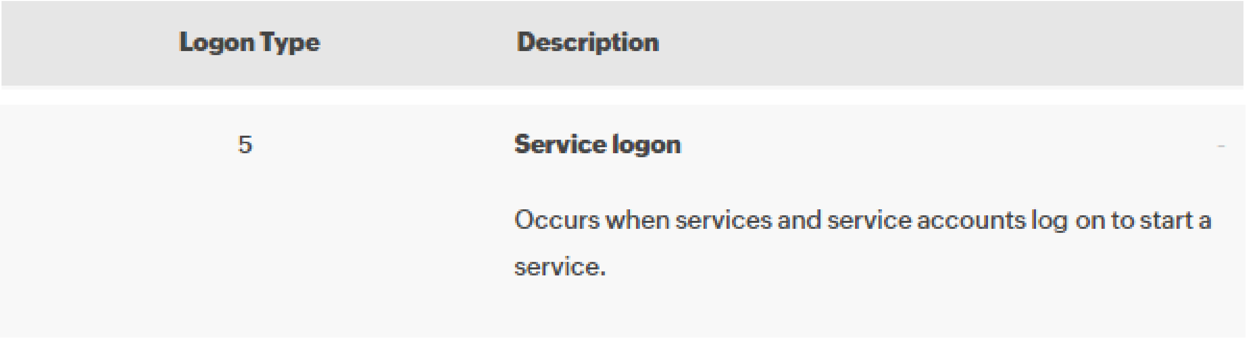


Logon Type	Description
2	**Interactive logon** Occurs when a user logs on using a computer's local keyboard and screen.



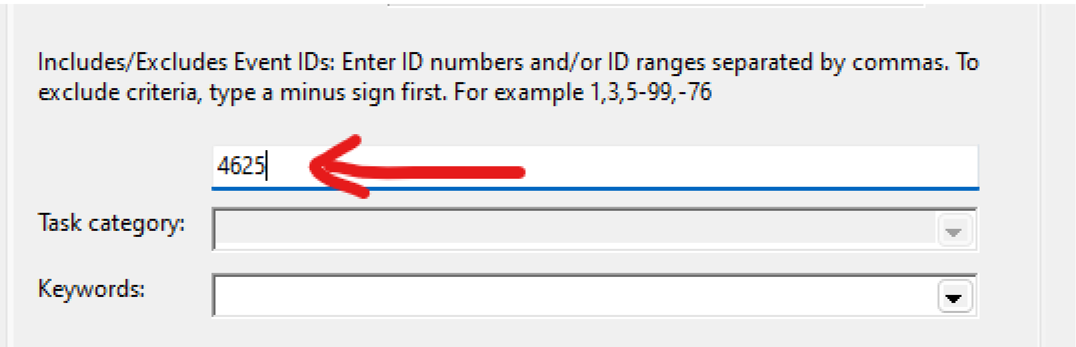
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/24/2023 1:06:07 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Rafsan_Anwar
OpCode:	Info		
More Information:	Event Log Online Help		

Logon Type 5 indicates services that supports logon



Logon Type	Description
5	**Service logon** Occurs when services and service accounts log on to start a service.

# Failed Logon
Event ID 4625



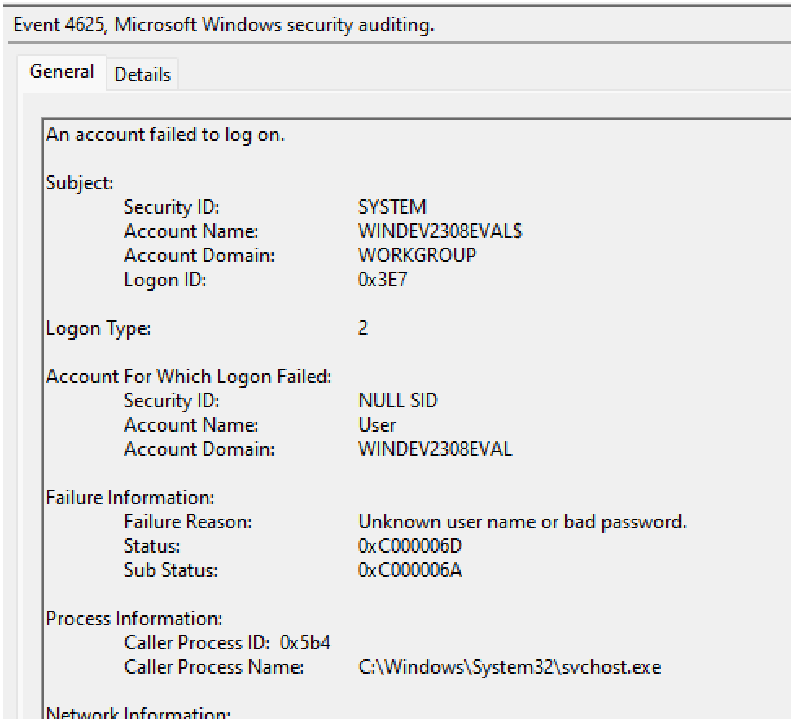
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

Task category:

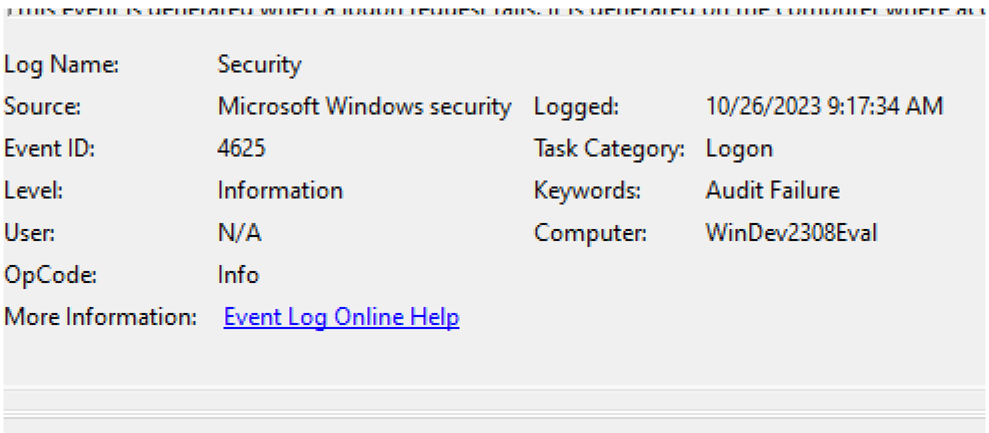
Keywords:

Logon Type 2



Event 4625, Microsoft Windows security auditing.

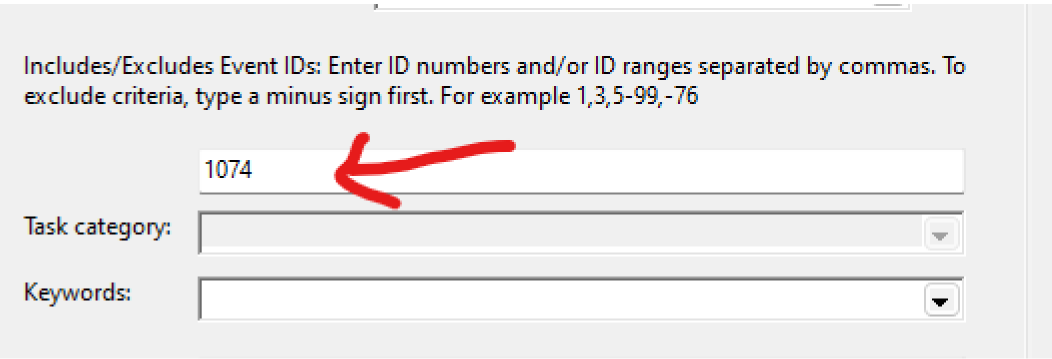
```
An account failed to log on.

Subject:
          Security ID:              SYSTEM
          Account Name:             WINDEV2308EVAL$
          Account Domain:           WORKGROUP
          Logon ID:                 0x3E7

Logon Type:                         2

Account For Which Logon Failed:
          Security ID:              NULL SID
          Account Name:             User
          Account Domain:           WINDEV2308EVAL

Failure Information:
          Failure Reason:           Unknown user name or bad password.
          Status:                   0xC000006D
          Sub Status:               0xC000006A

Process Information:
          Caller Process ID:  0x5b4
          Caller Process Name:      C:\Windows\System32\svchost.exe

Network Information:
```



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/26/2023 9:17:34 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	WinDev2308Eval
OpCode:	Info		
More Information:	Event Log Online Help		

System shutdown logon

Event ID 1074



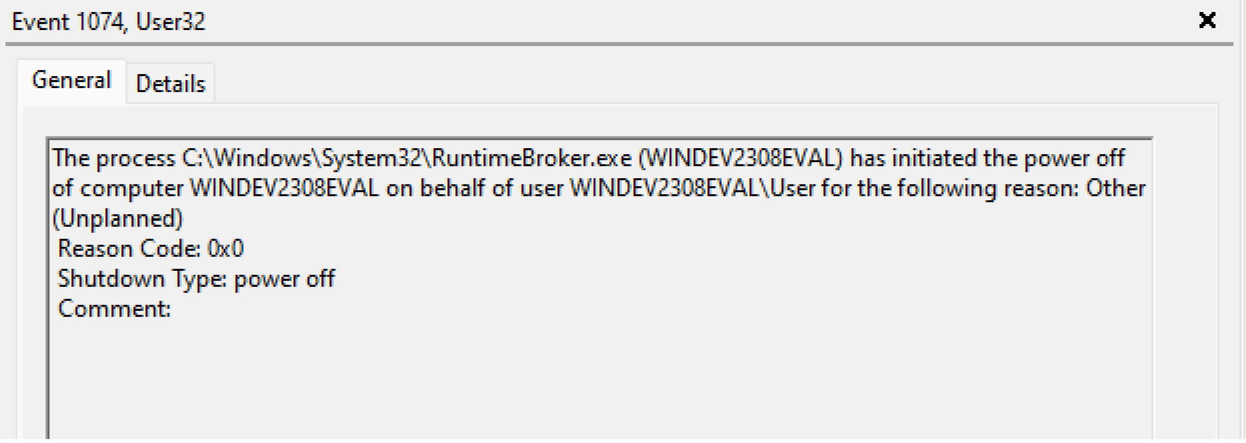
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

1074

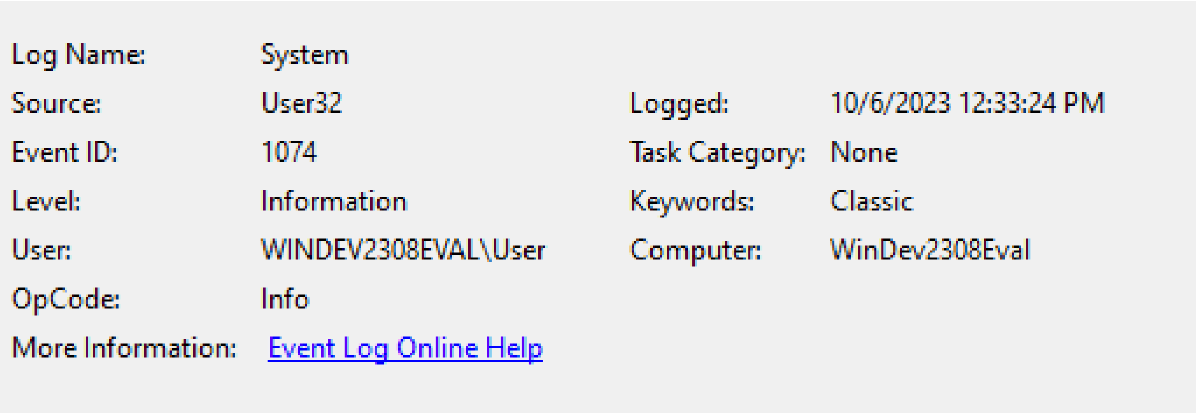
Task category:

Keywords:

Logon Type

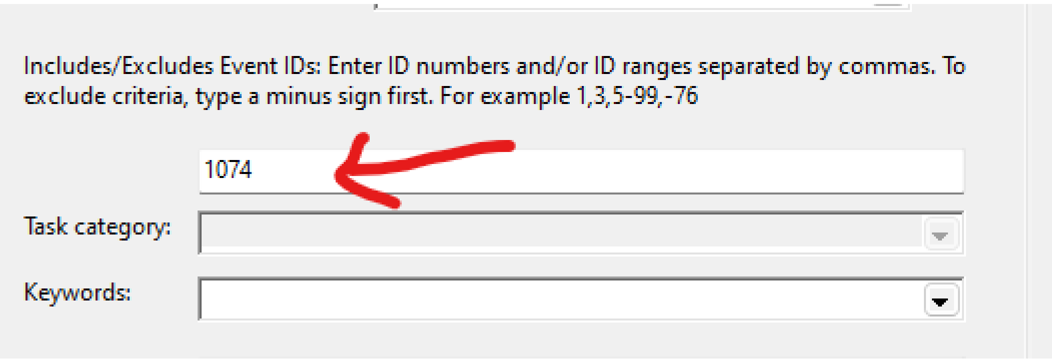


The process C:\Windows\System32\RuntimeBroker.exe (WINDEV2308EVAL) has initiated the power off of computer WINDEV2308EVAL on behalf of user WINDEV2308EVAL\User for the following reason: Other (Unplanned)
 Reason Code: 0x0
 Shutdown Type: power off
 Comment:



Log Name:	System		
Source:	User32	Logged:	10/6/2023 12:33:24 PM
Event ID:	1074	Task Category:	None
Level:	Information	Keywords:	Classic
User:	WINDEV2308EVAL\User	Computer:	WinDev2308Eval
OpCode:	Info		
More Information:	Event Log Online Help		

# System reboot logon
Event ID 1074



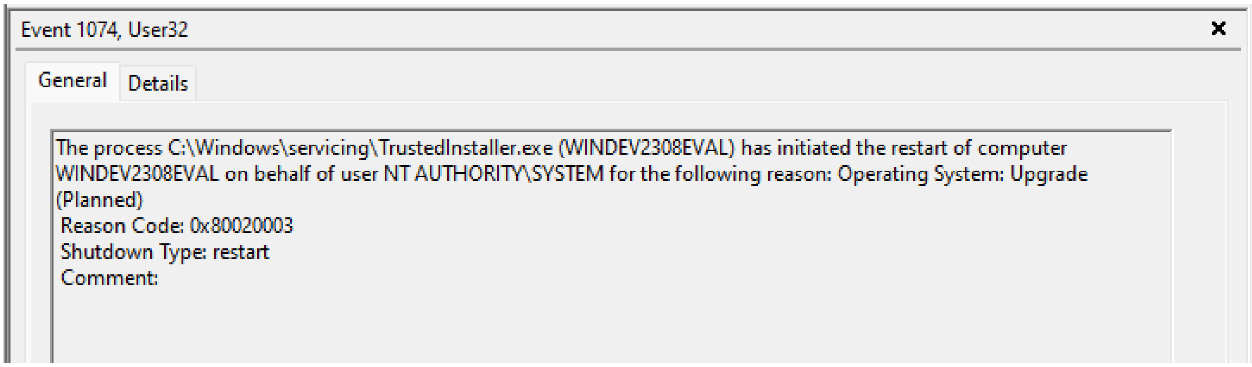
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

1074

Task category:

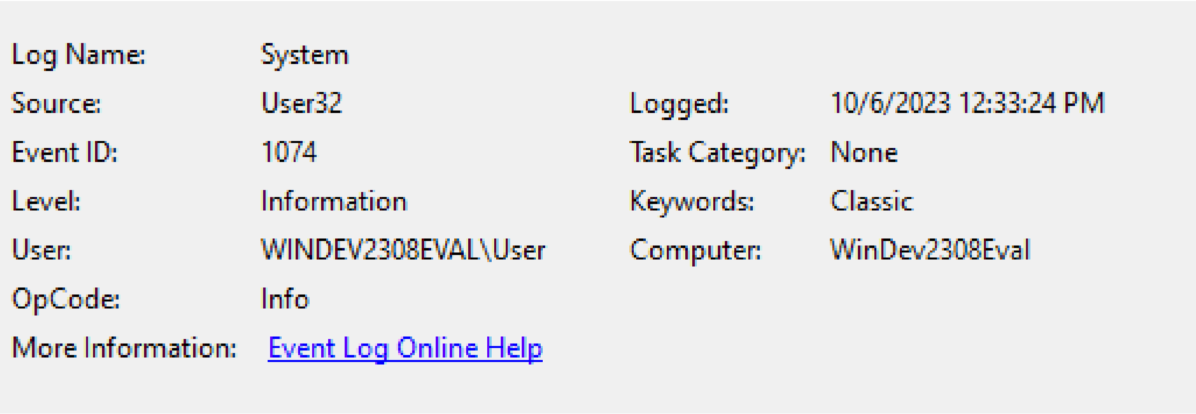
Keywords:

Logon Type



Event 1074, User32

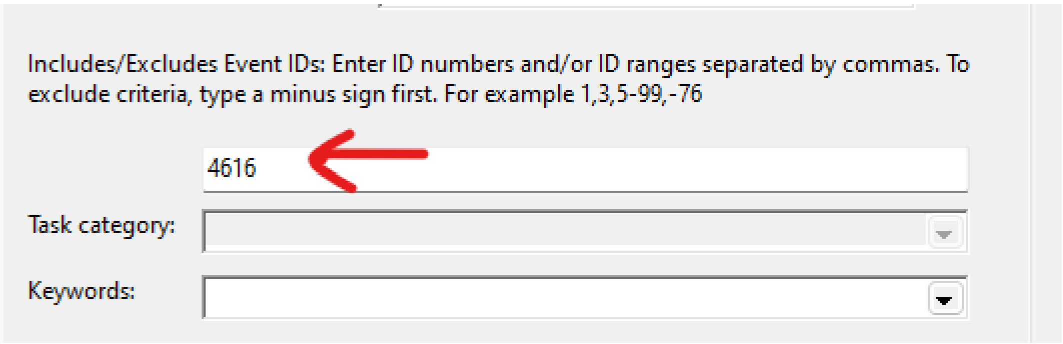
The process C:\Windows\servicing\TrustedInstaller.exe (WINDEV2308EVAL) has initiated the restart of computer WINDEV2308EVAL on behalf of user NT AUTHORITY\SYSTEM for the following reason: Operating System: Upgrade (Planned)
Reason Code: 0x80020003
Shutdown Type: restart
Comment:



Log Name:	System		
Source:	User32	Logged:	10/6/2023 12:33:24 PM
Event ID:	1074	Task Category:	None
Level:	Information	Keywords:	Classic
User:	WINDEV2308EVAL\User	Computer:	WinDev2308Eval
OpCode:	Info		
More Information:	Event Log Online Help		

System time changed

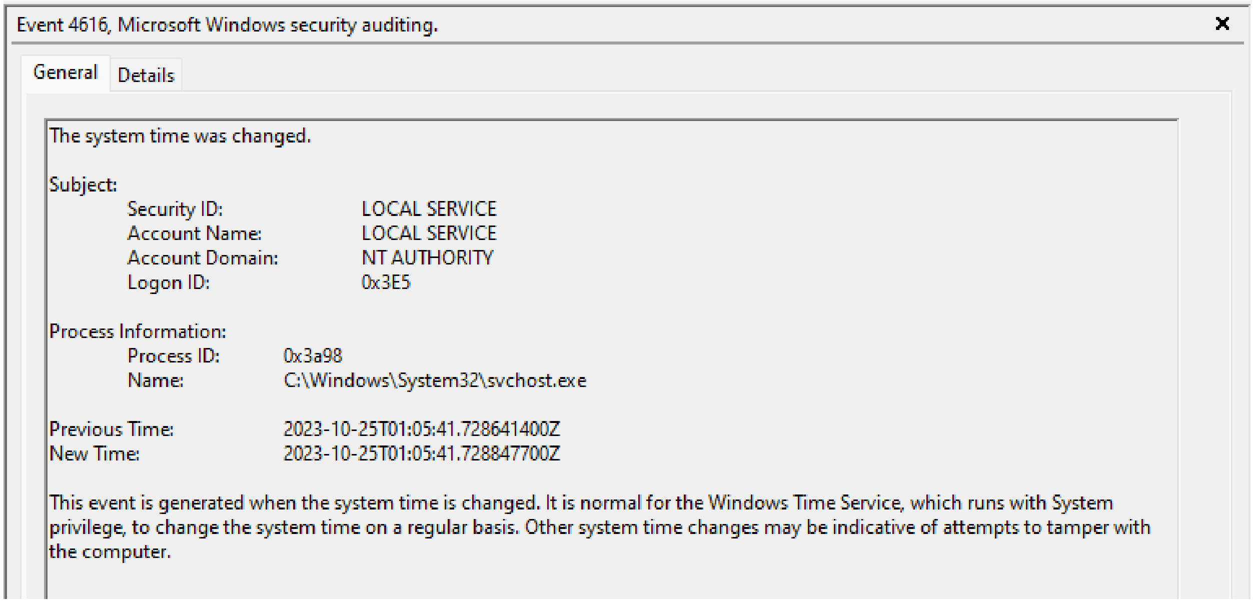
Event ID 4616



Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

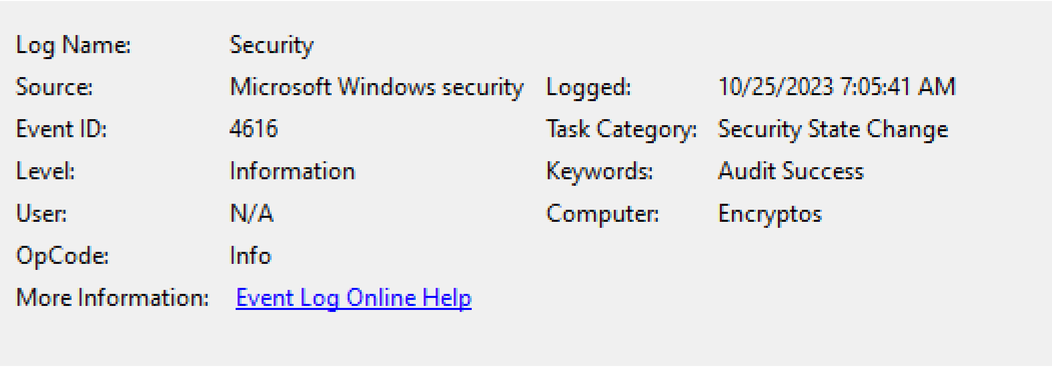
	4616
Task category:	
Keywords:	

Type



Event 4616, Microsoft Windows security auditing.

```
The system time was changed.

Subject:
        Security ID:            LOCAL SERVICE
        Account Name:           LOCAL SERVICE
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E5

Process Information:
        Process ID:     0x3a98
        Name:           C:\Windows\System32\svchost.exe

Previous Time:          2023-10-25T01:05:41.728641400Z
New Time:               2023-10-25T01:05:41.728847700Z

This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System
privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with
the computer.
```



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/25/2023 7:05:41 AM
Event ID:	4616	Task Category:	Security State Change
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Encryptos
OpCode:	Info		
More Information:	Event Log Online Help		

File/folder permission changed

Event ID 4670

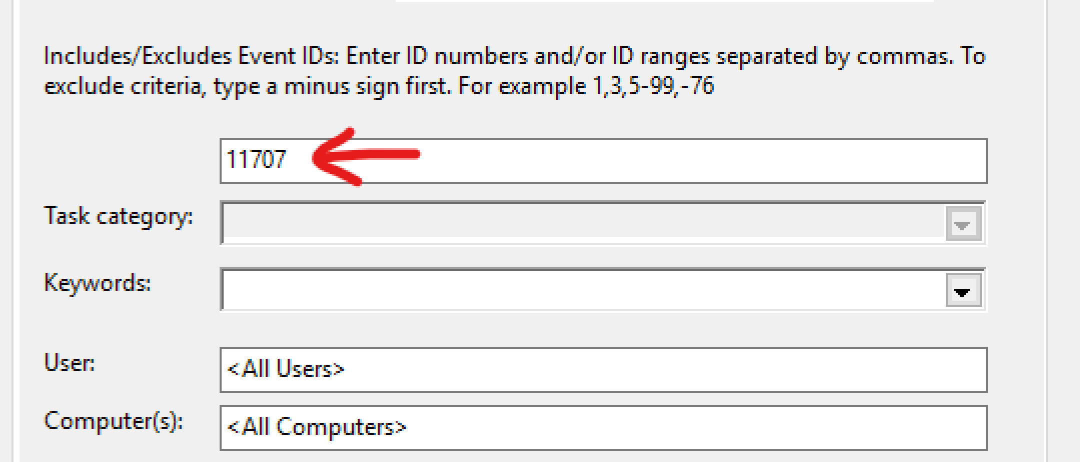
Need More Test

# System registry changed
Event ID 4657

Need More Test

Software installation

Event ID 11707



Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

11707

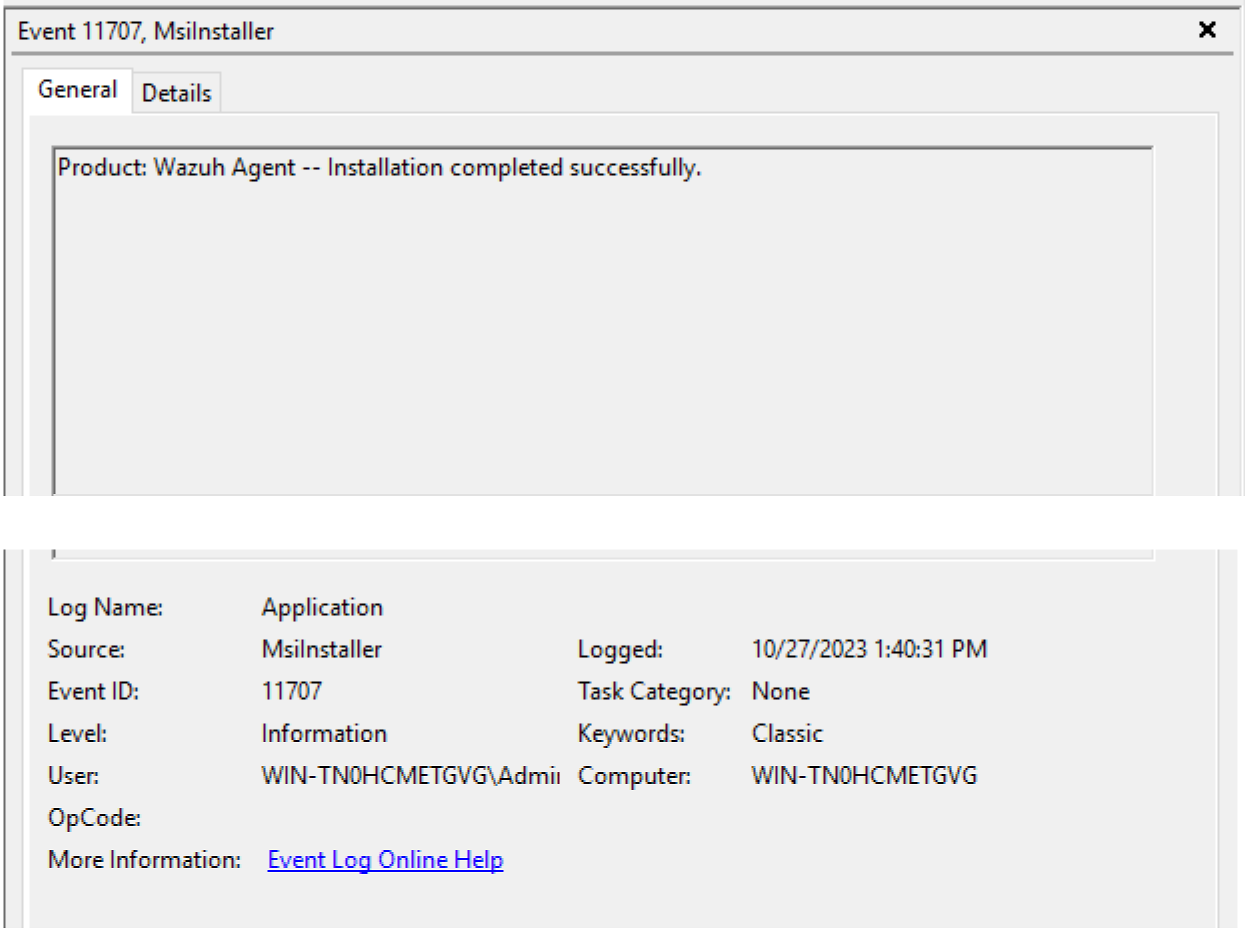
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Type:



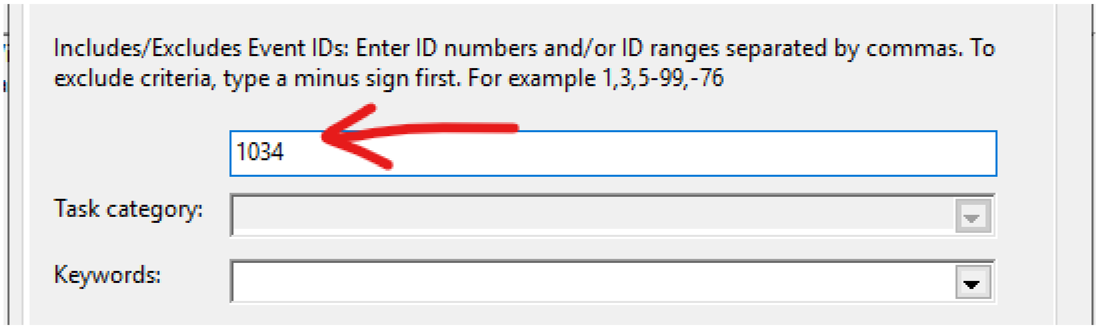
Event 11707, MsiInstaller

Product: Wazuh Agent -- Installation completed successfully.

Log Name:	Application		
Source:	MsiInstaller	Logged:	10/27/2023 1:40:31 PM
Event ID:	11707	Task Category:	None
Level:	Information	Keywords:	Classic
User:	WIN-TN0HCMETGVG\Admii	Computer:	WIN-TN0HCMETGVG
OpCode:			
More Information:	Event Log Online Help		

Software uninstallation

Event ID 1034



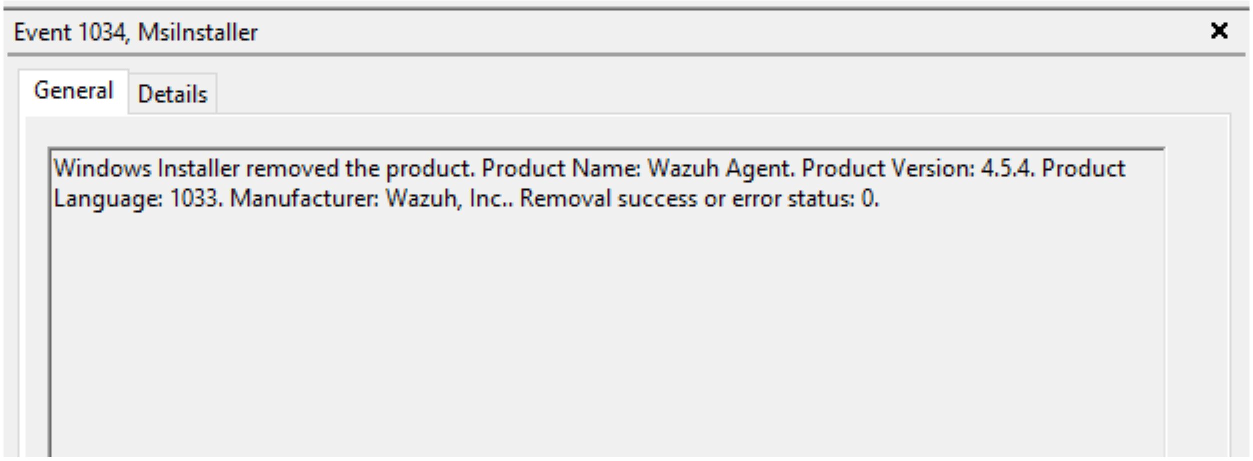
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

1034

Task category:

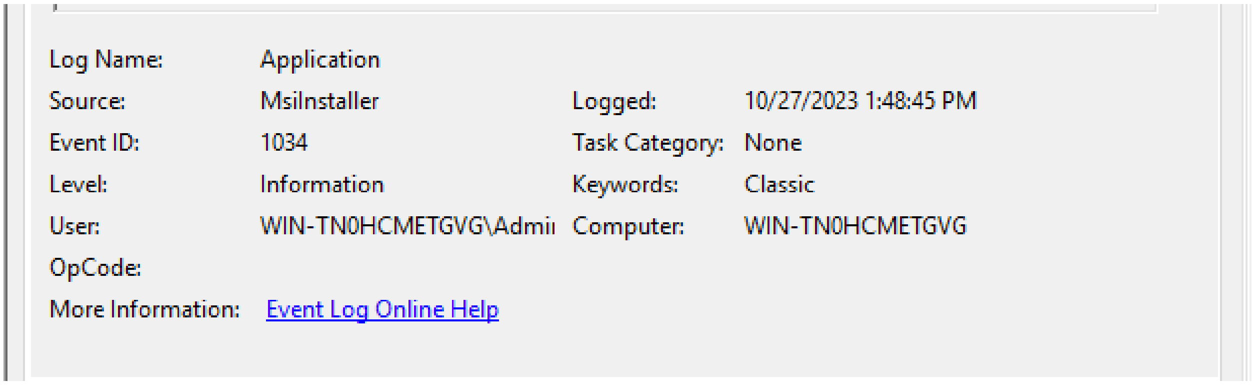
Keywords:

Type:



Event 1034, MsiInstaller

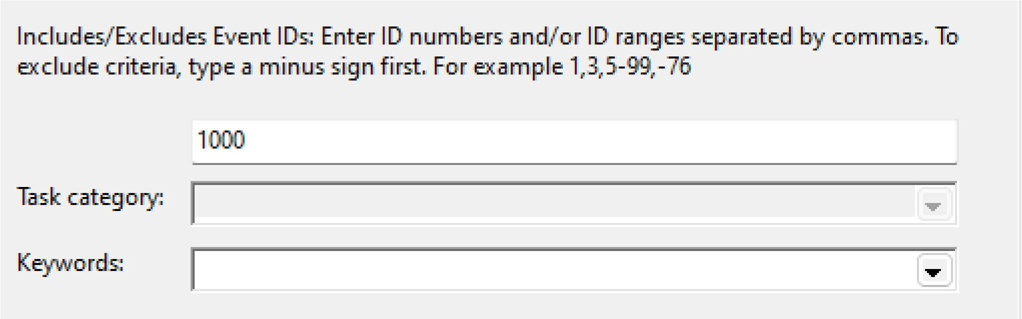
Windows Installer removed the product. Product Name: Wazuh Agent. Product Version: 4.5.4. Product Language: 1033. Manufacturer: Wazuh, Inc.. Removal success or error status: 0.



Log Name:	Application		
Source:	MsiInstaller	Logged:	10/27/2023 1:48:45 PM
Event ID:	1034	Task Category:	None
Level:	Information	Keywords:	Classic
User:	WIN-TN0HCMETGVG\Admi	Computer:	WIN-TN0HCMETGVG
OpCode:			
More Information:	Event Log Online Help		

Software error/crush

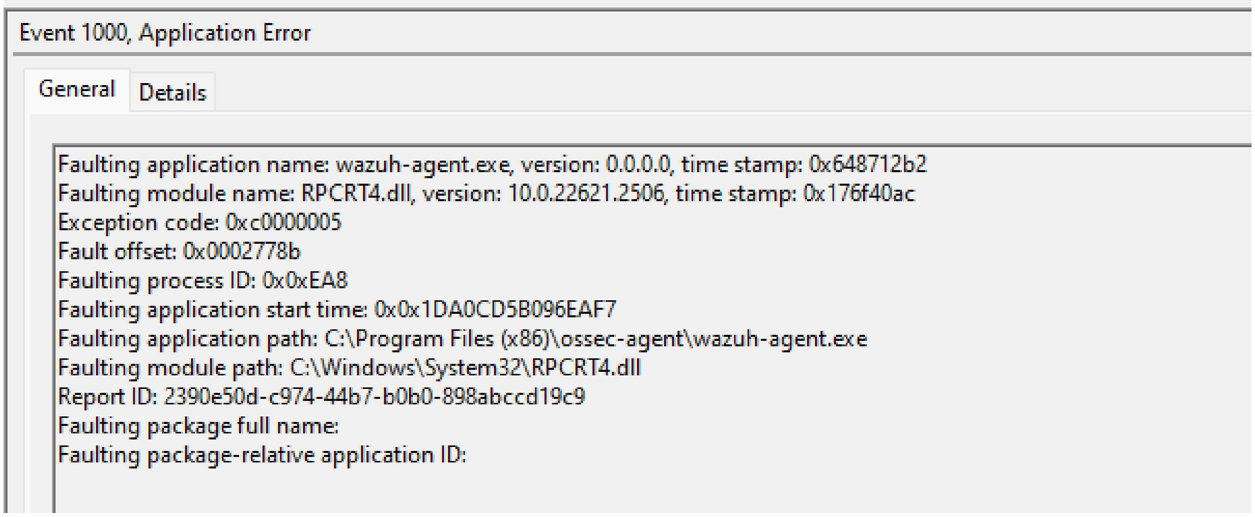
Event ID 1000



Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

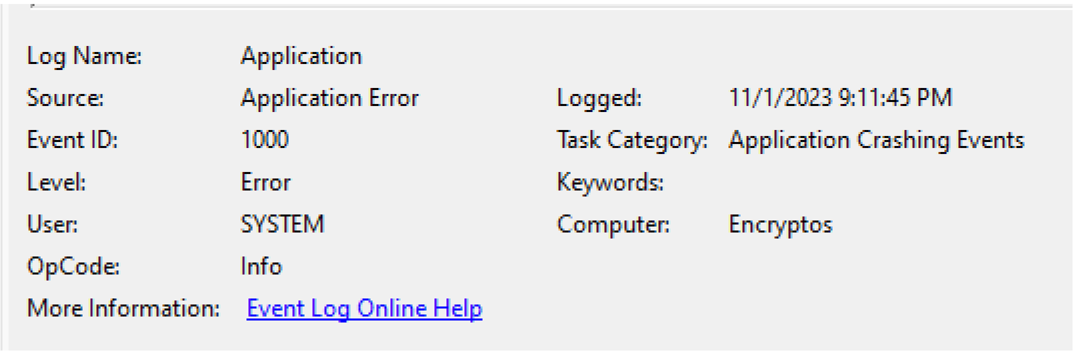
	1000
Task category:	
Keywords:	

Types:



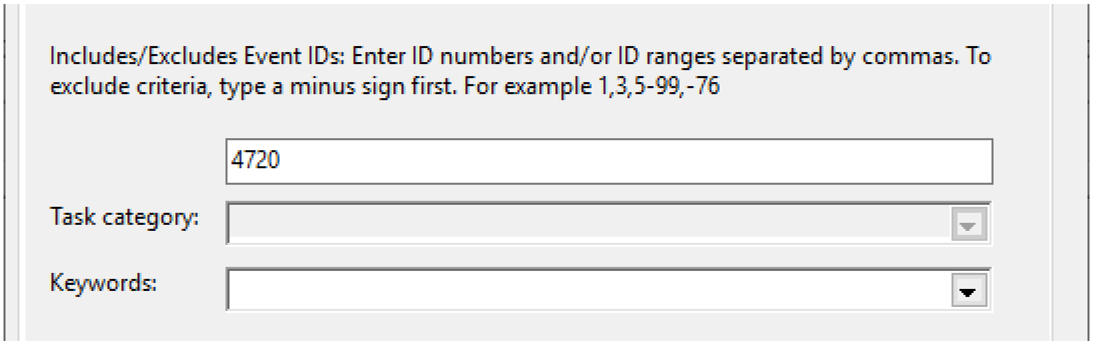
Event 1000, Application Error

```
Faulting application name: wazuh-agent.exe, version: 0.0.0.0, time stamp: 0x648712b2
Faulting module name: RPCRT4.dll, version: 10.0.22621.2506, time stamp: 0x176f40ac
Exception code: 0xc0000005
Fault offset: 0x0002778b
Faulting process ID: 0x0xEA8
Faulting application start time: 0x0x1DA0CD5B096EAF7
Faulting application path: C:\Program Files (x86)\ossec-agent\wazuh-agent.exe
Faulting module path: C:\Windows\System32\RPCRT4.dll
Report ID: 2390e50d-c974-44b7-b0b0-898abccd19c9
Faulting package full name:
Faulting package-relative application ID:
```



Log Name:	Application		
Source:	Application Error	Logged:	11/1/2023 9:11:45 PM
Event ID:	1000	Task Category:	Application Crashing Events
Level:	Error	Keywords:	
User:	SYSTEM	Computer:	Encryptos
OpCode:	Info		
More Information:	Event Log Online Help		

# User Creation
Event ID 1034



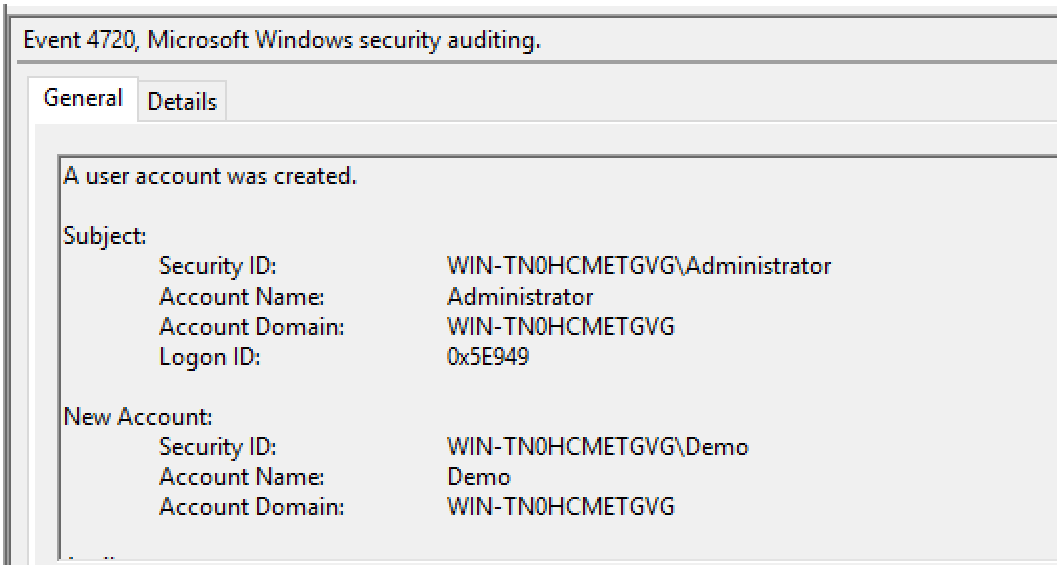
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4720

Task category:

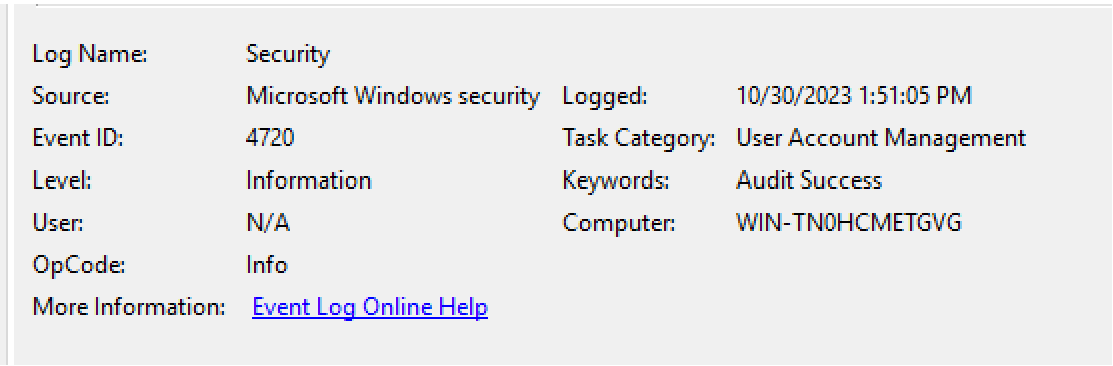
Keywords:

Type:



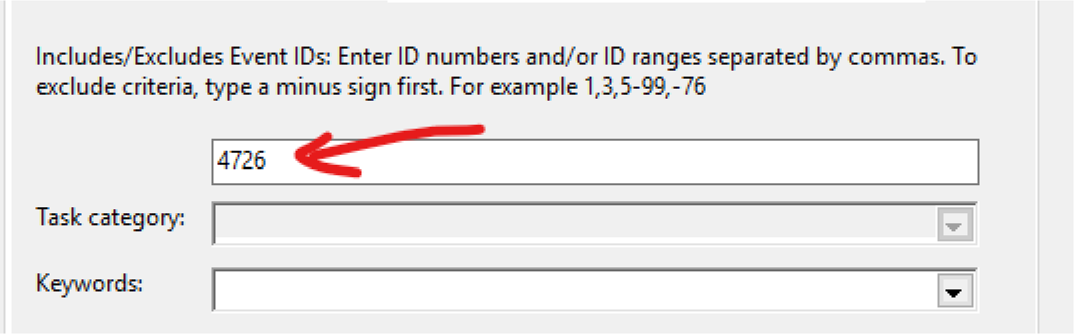
Event 4720, Microsoft Windows security auditing.

```
A user account was created.

Subject:
	Security ID:		WIN-TN0HCMETGVG\Administrator
	Account Name:		Administrator
	Account Domain:		WIN-TN0HCMETGVG
	Logon ID:		0x5E949

New Account:
	Security ID:		WIN-TN0HCMETGVG\Demo
	Account Name:		Demo
	Account Domain:		WIN-TN0HCMETGVG
```



```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         10/30/2023 1:51:05 PM
Event ID:          4720                         Task Category:  User Account Management
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       WIN-TN0HCMETGVG
OpCode:            Info
More Information:  Event Log Online Help
```

# User Deletion
Event ID 4726



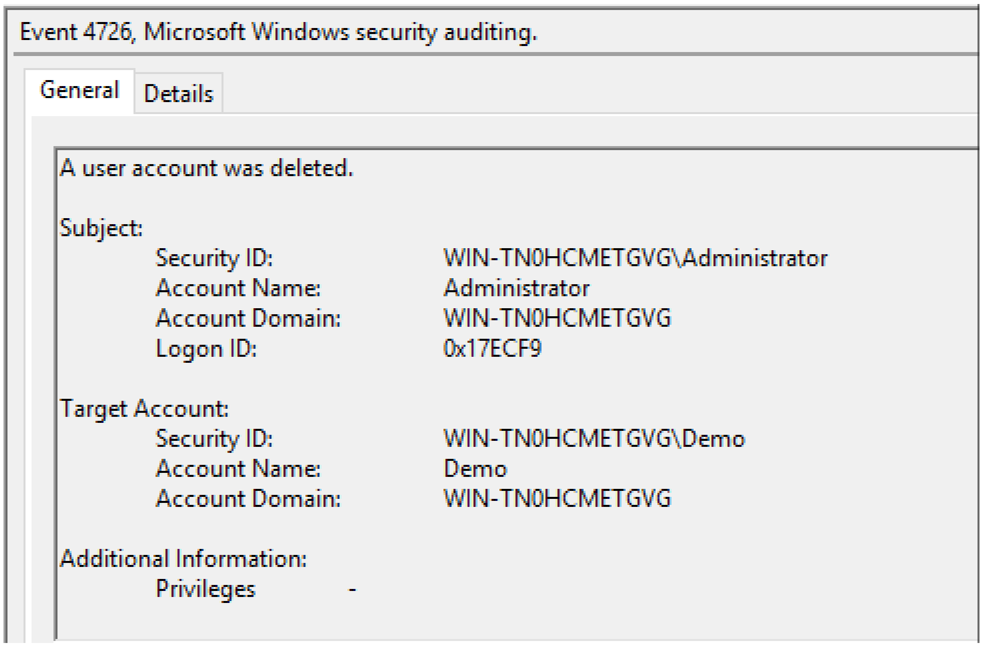
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4726

Task category:

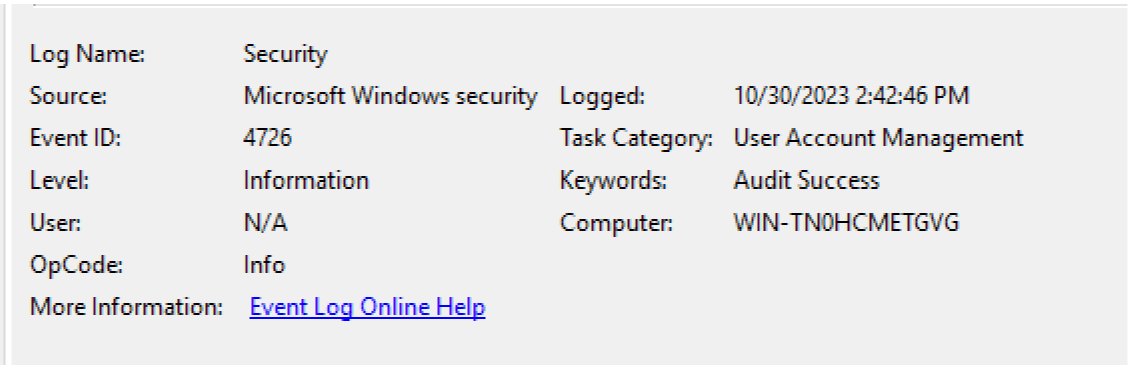
Keywords:

Type:



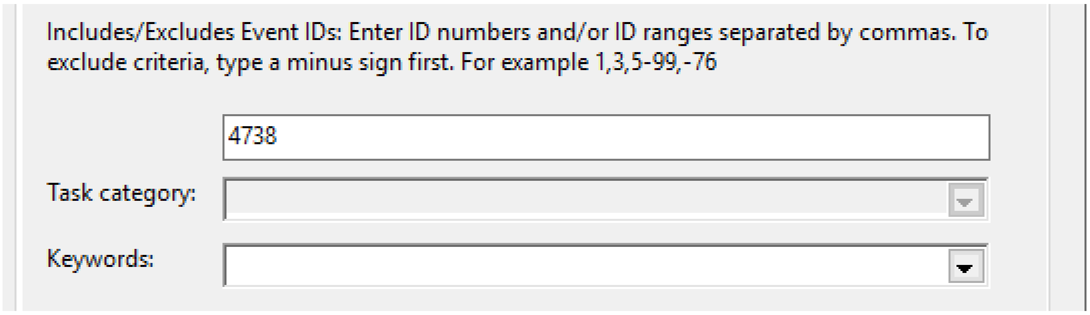
Event 4726, Microsoft Windows security auditing.

```
A user account was deleted.

Subject:
        Security ID:            WIN-TN0HCMETGVG\Administrator
        Account Name:           Administrator
        Account Domain:         WIN-TN0HCMETGVG
        Logon ID:               0x17ECF9

Target Account:
        Security ID:            WIN-TN0HCMETGVG\Demo
        Account Name:           Demo
        Account Domain:         WIN-TN0HCMETGVG

Additional Information:
        Privileges      -
```



```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          10/30/2023 2:42:46 PM
Event ID:          4726                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN-TN0HCMETGVG
OpCode:            Info
More Information:  Event Log Online Help
```

# Change user type
Event ID 4738



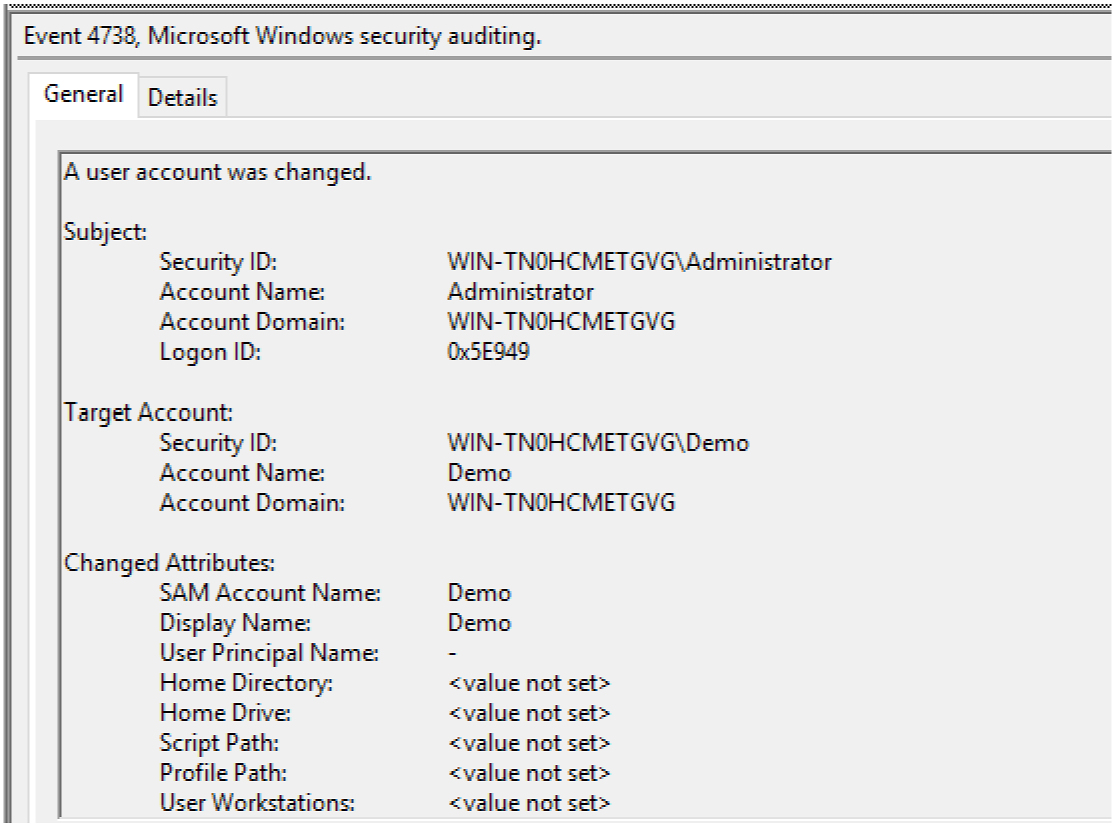
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4738

Task category:

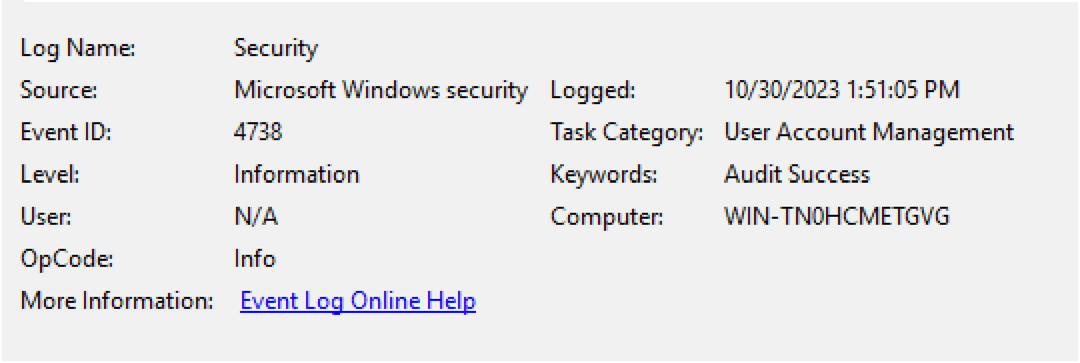
Keywords:

Type:



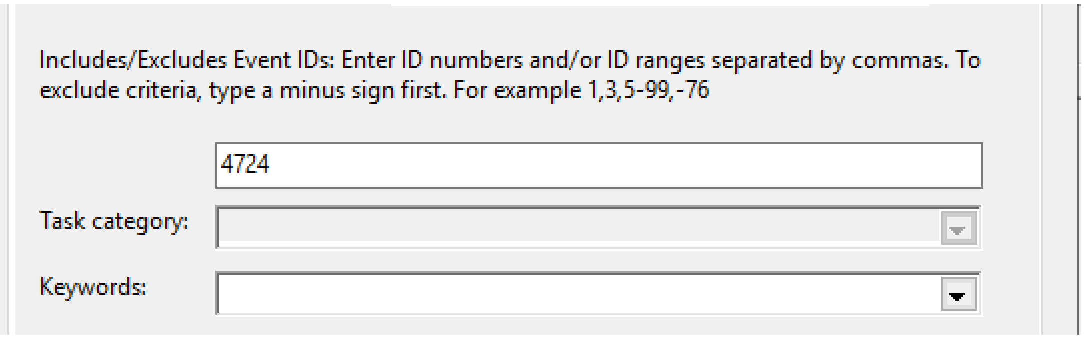
Event 4738, Microsoft Windows security auditing.

```
A user account was changed.

Subject:
        Security ID:            WIN-TN0HCMETGVG\Administrator
        Account Name:           Administrator
        Account Domain:         WIN-TN0HCMETGVG
        Logon ID:               0x5E949

Target Account:
        Security ID:            WIN-TN0HCMETGVG\Demo
        Account Name:           Demo
        Account Domain:         WIN-TN0HCMETGVG

Changed Attributes:
        SAM Account Name:       Demo
        Display Name:           Demo
        User Principal Name:    -
        Home Directory:         <value not set>
        Home Drive:             <value not set>
        Script Path:            <value not set>
        Profile Path:           <value not set>
        User Workstations:      <value not set>
```



```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          10/30/2023 1:51:05 PM
Event ID:          4738                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        WIN-TN0HCMETGVG
OpCode:            Info
More Information:  Event Log Online Help
```

# User password set/removed/changed
Event ID 4724



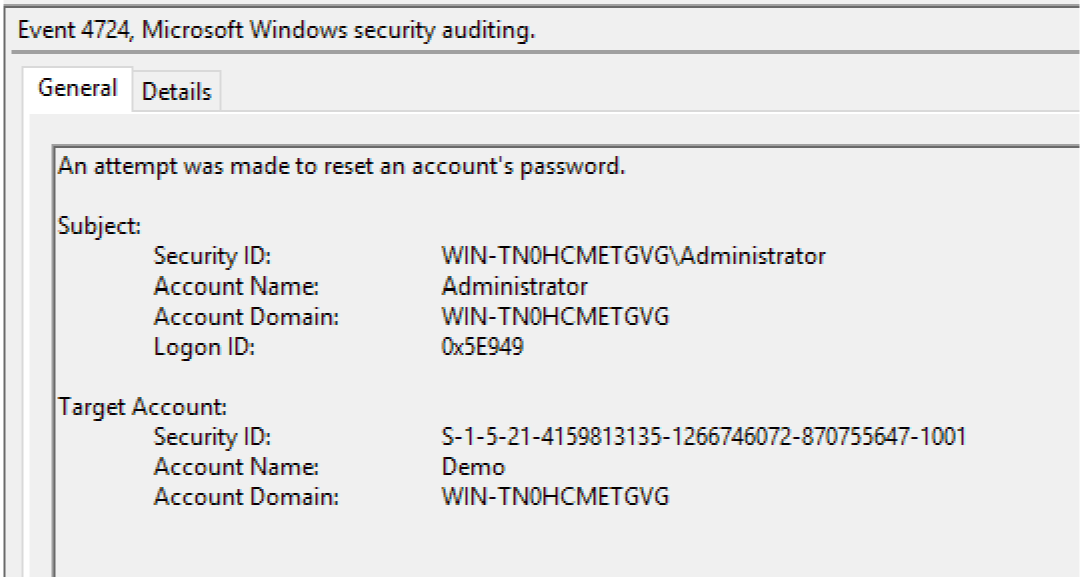
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4724

Task category:

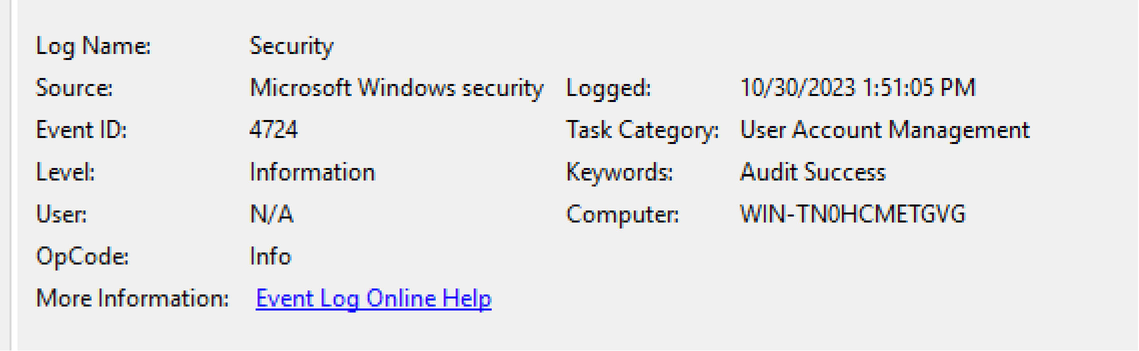
Keywords:

Type:



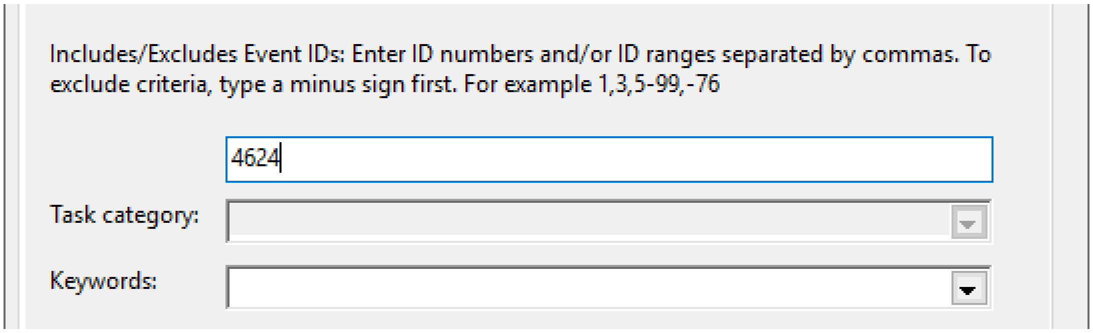
Event 4724, Microsoft Windows security auditing.

```
An attempt was made to reset an account's password.

Subject:
        Security ID:            WIN-TN0HCMETGVG\Administrator
        Account Name:           Administrator
        Account Domain:         WIN-TN0HCMETGVG
        Logon ID:               0x5E949

Target Account:
        Security ID:            S-1-5-21-4159813135-1266746072-870755647-1001
        Account Name:           Demo
        Account Domain:         WIN-TN0HCMETGVG
```



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/30/2023 1:51:05 PM
Event ID:	4724	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-TN0HCMETGVG
OpCode:	Info		
More Information:	Event Log Online Help		

#Remote login success
Event ID 4624



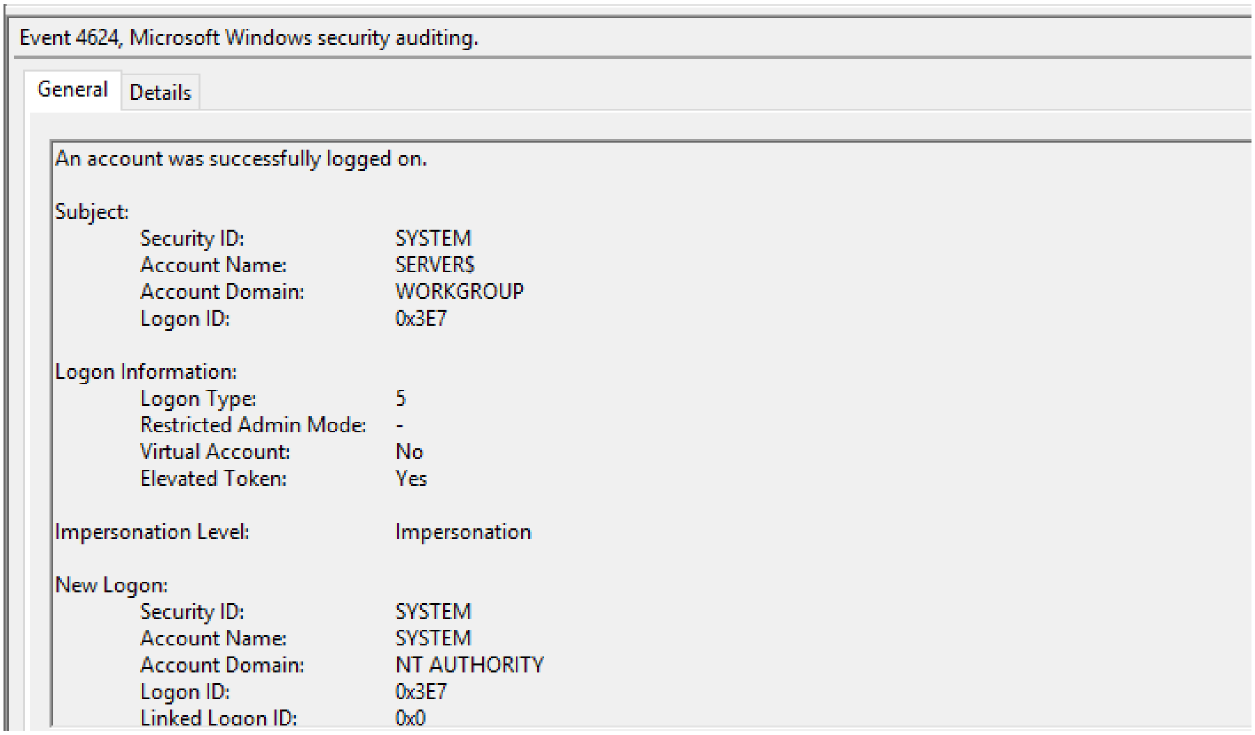
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624

Task category:

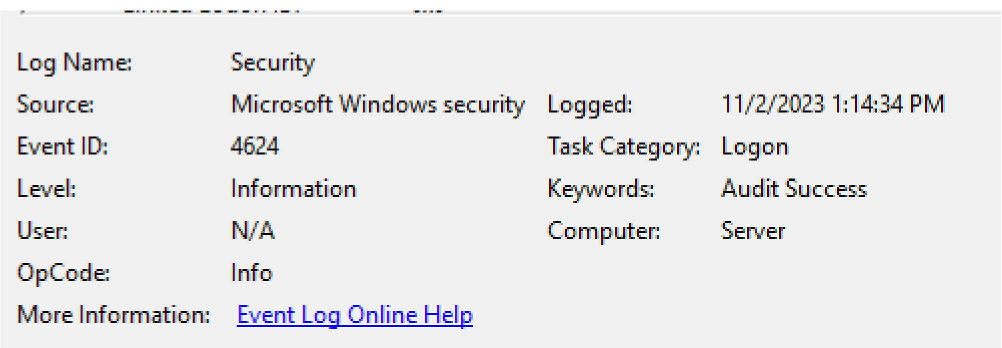
Keywords:

Types: 5



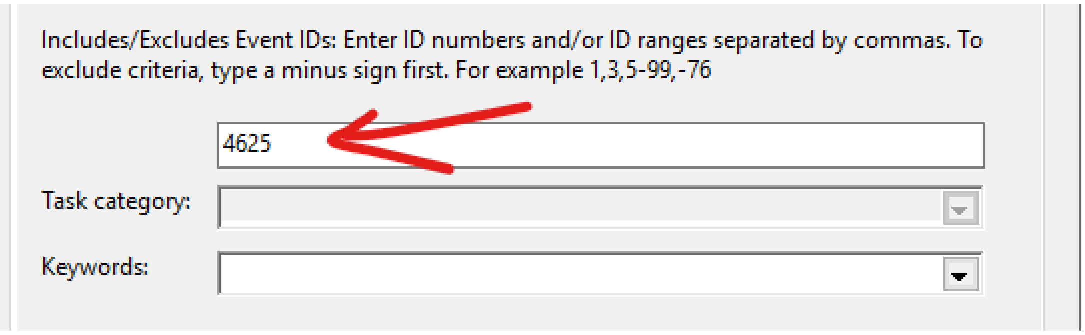
Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
          Security ID:              SYSTEM
          Account Name:             SERVER$
          Account Domain:           WORKGROUP
          Logon ID:                 0x3E7

Logon Information:
          Logon Type:               5
          Restricted Admin Mode:    -
          Virtual Account:          No
          Elevated Token:           Yes

Impersonation Level:                Impersonation

New Logon:
          Security ID:              SYSTEM
          Account Name:             SYSTEM
          Account Domain:           NT AUTHORITY
          Logon ID:                 0x3E7
          Linked Logon ID:          0x0
```



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/2/2023 1:14:34 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Server
OpCode:	Info		
More Information:	Event Log Online Help		

# Remote login failed
Event ID 4625



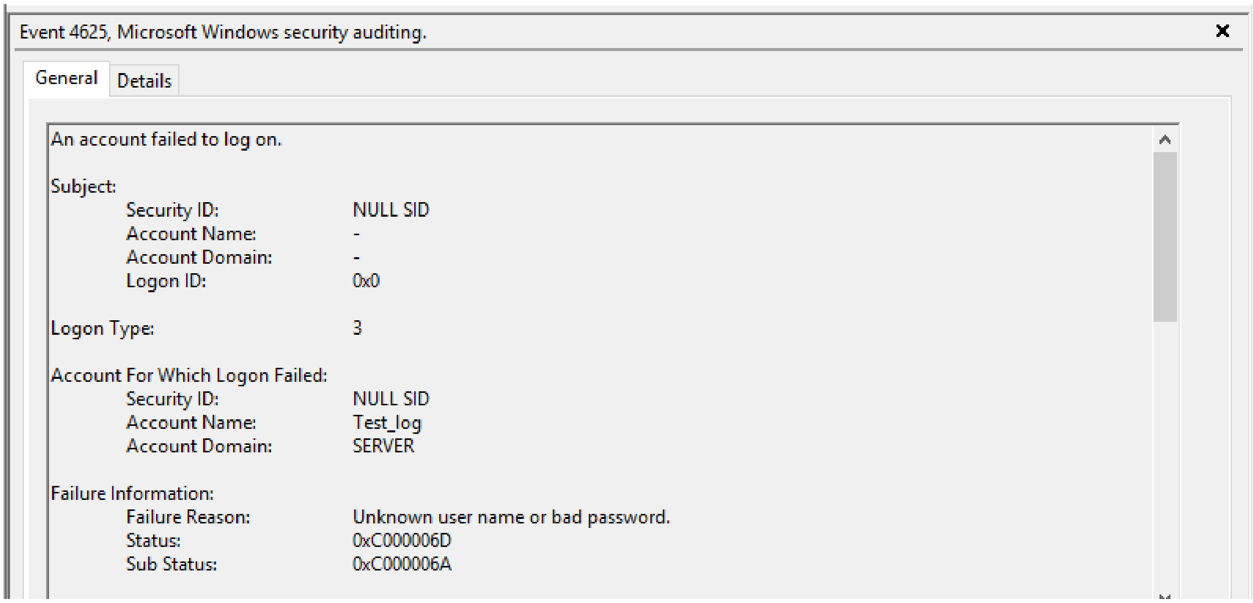
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

Task category:

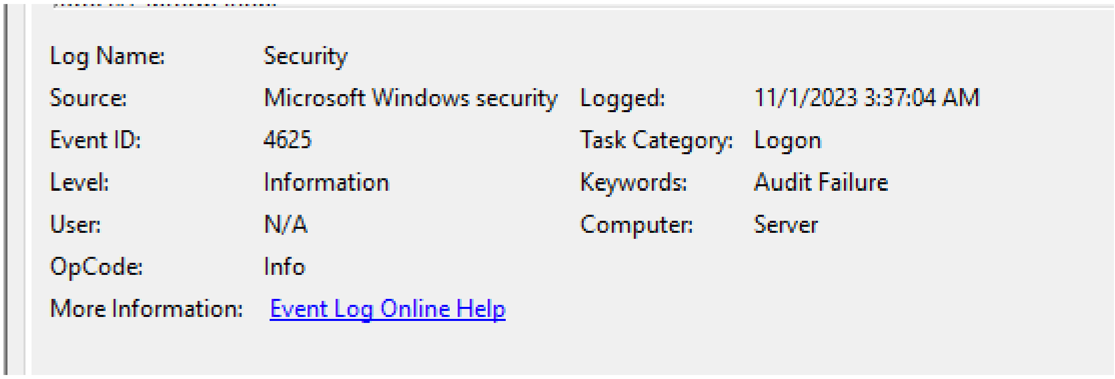
Keywords:

Type:



Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Test_log
        Account Domain:         SERVER

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A
```



Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/1/2023 3:37:04 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	Server
OpCode:	Info		
More Information:	Event Log Online Help		

# Malware detection
Event ID 1116

Need More Test

# Windows Defender off/on
Event ID 5001

Need More Test