HOW TO GUIDE

Detecting and Responding to Account Management Events: Event Trigger Scenarios

Introduction

Windows security logs play a critical role in maintaining the integrity and security of systems. Account management events, such as user account creation, deletion, or modification, provide key insights into potential security risks and unauthorized activities. Understanding how to trigger these events for testing purposes and crafting appropriate responses empowers administrators and Security Operations Center (SOC) teams to stay ahead of threats. This guide explores the importance of monitoring these events and scenarios for triggering Event ID alerts.

Importance of Viewing Security Logs

Security logs are the backbone of forensic analysis and incident response. These logs provide detailed records for specific types of incidents or breaches, such as unauthorized access attempts, account modifications, and privilege escalations. By analyzing these records, security teams can trace the source of an attack, understand its impact, and implement measures to prevent future occurrences. For example, a log entry showing repeated failed login attempts might indicate a brute-force attack, while an unexpected account creation could signal a compromised administrator account. Such insights are essential for crafting targeted responses and improving overall security posture. They provide a detailed record of system activities, making it possible to:

- **Detect Unauthorized Activities:** Identify malicious actions, such as unauthorized account creation or privilege escalation.
- **Audit System Usage:** Ensure compliance with internal policies and external regulations through regular audits.
- **Investigate Incidents:** Provide a trail of evidence during forensic investigations, aiding in understanding the scope and cause of an attack.
- **Proactively Identify Risks:** Spot unusual patterns that may indicate a security breach before it escalates.

Without diligent monitoring of security logs, organizations risk missing early warning signs of potential threats.

Security Policy Settings

Security policy settings determine how Windows handles and logs events related to account management. These settings can be fine-tuned to ensure optimal monitoring and protection. Key considerations include:

- **Audit Policies:** Enable auditing for account management events to capture Event IDs such as 4720 (User Account Created) or 4724 (Password Reset).
- **Account Lockout Policies:** Configure thresholds to lock accounts after a certain number of failed login attempts, reducing brute-force attack risks.
- **Group Policy Settings:** Use Group Policy to enforce uniform security configurations across systems in an Active Directory environment.
- **Advanced Security Options:** Leverage options such as multi-factor authentication (MFA) and secure password policies to enhance protection.

Properly configured security policies create a robust framework for detecting and preventing account-related threats.

Advantages of Security Settings

Implementing and maintaining strong security settings offers multiple benefits:

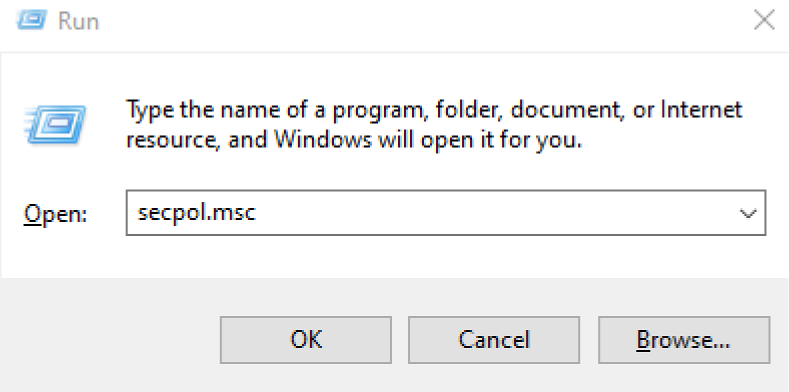
- **Enhanced Threat Detection:** Well-defined policies help detect anomalies and suspicious behavior in real time.
- **Minimized Attack Surface:** Strong password policies, MFA, and restricted access reduce opportunities for attackers.
- **Compliance and Accountability:** Meet regulatory requirements while maintaining a clear record of actions taken on accounts.
- **Streamlined Management:** Consistent settings across systems simplify administration and reduce the likelihood of misconfigurations.
- **Improved Response Times:** Pre-configured alerts and policies allow quicker reactions to security events, minimizing damage.

Viewing Security Logs

Enabling Audit Policies

To enable account management audit policies:

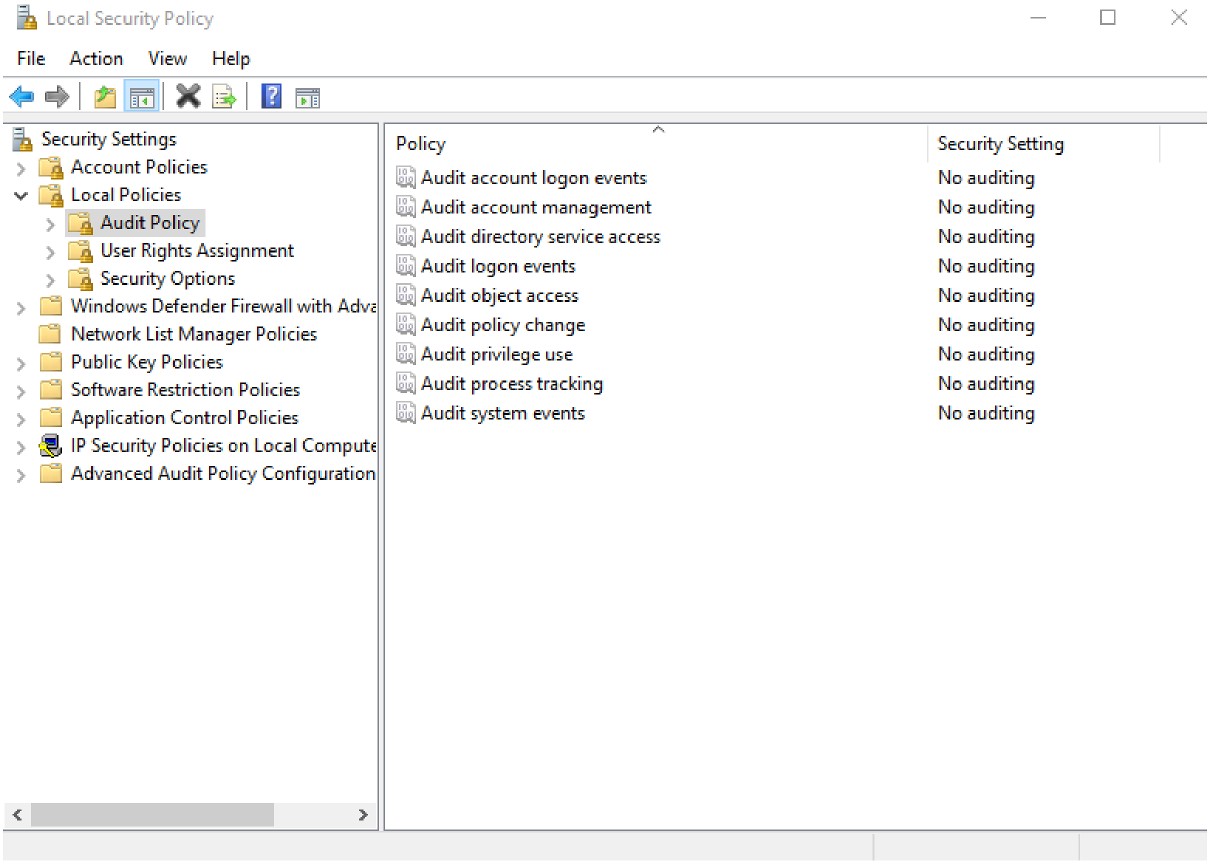
1. Press **Windows+R**, type secpol.msc, and press Enter.
   - **What is secpol.msc?** It stands for "Security Policy Management Console," a tool in Windows used to configure and manage local security policies, such as audit policies for account management events.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

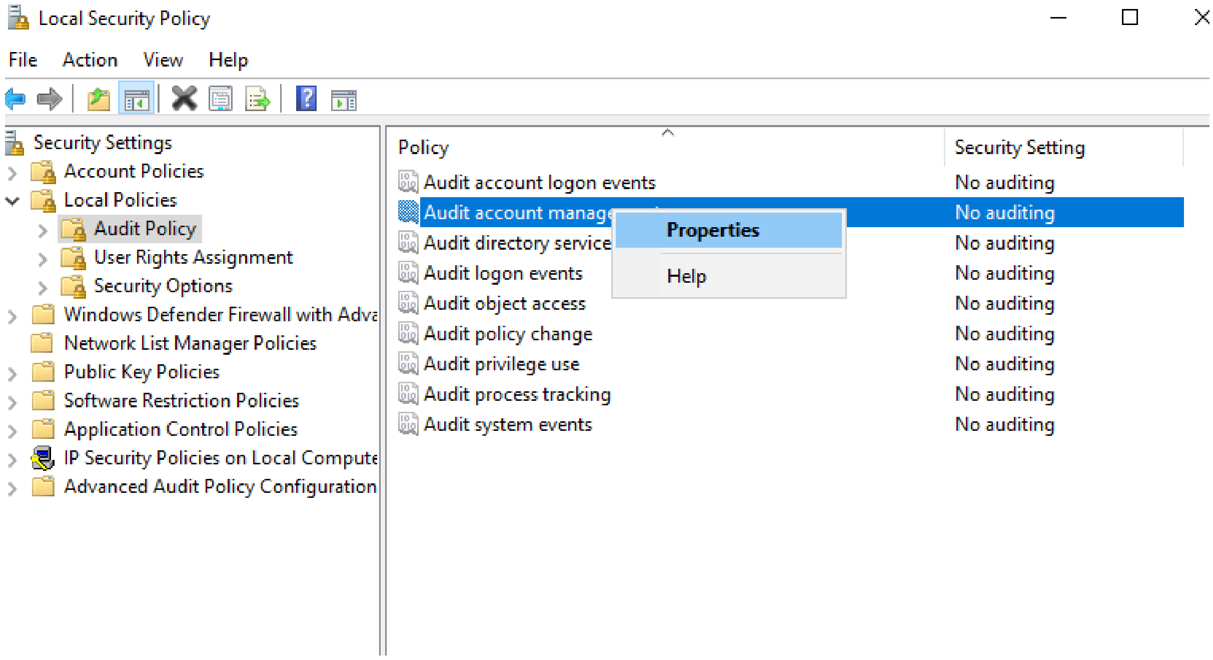
Open: secpol.msc

2. Navigate to **Local Policies > Audit Policy**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

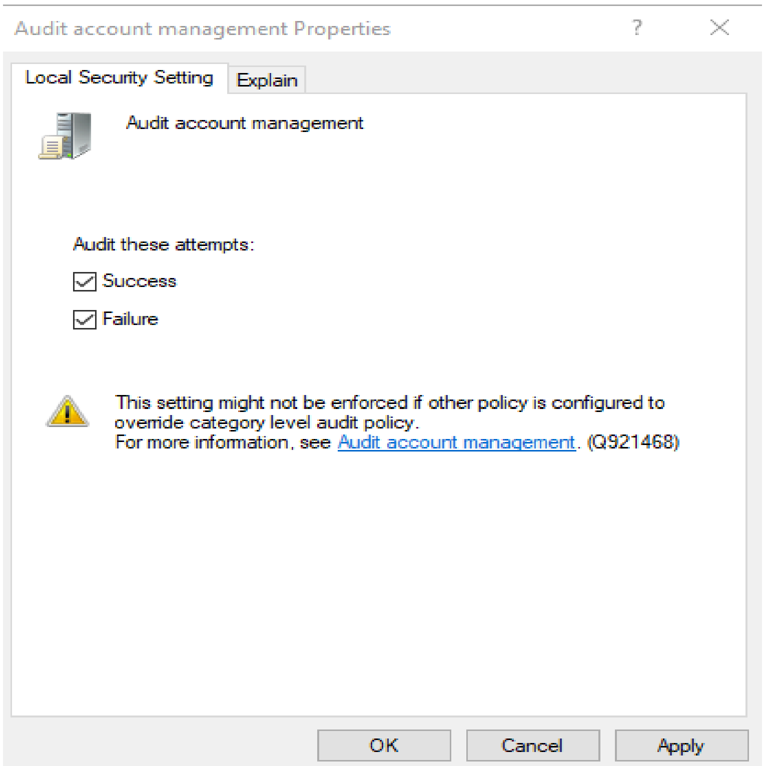
3. Right-click **Audit account management** and select **Properties**.



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Properties
Help

Policy	Security Setting
Audit account logon events	No auditing
Audit account manage	No auditing
Audit directory service	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

4. Check both **Success** and **Failure** boxes, then click **OK**.



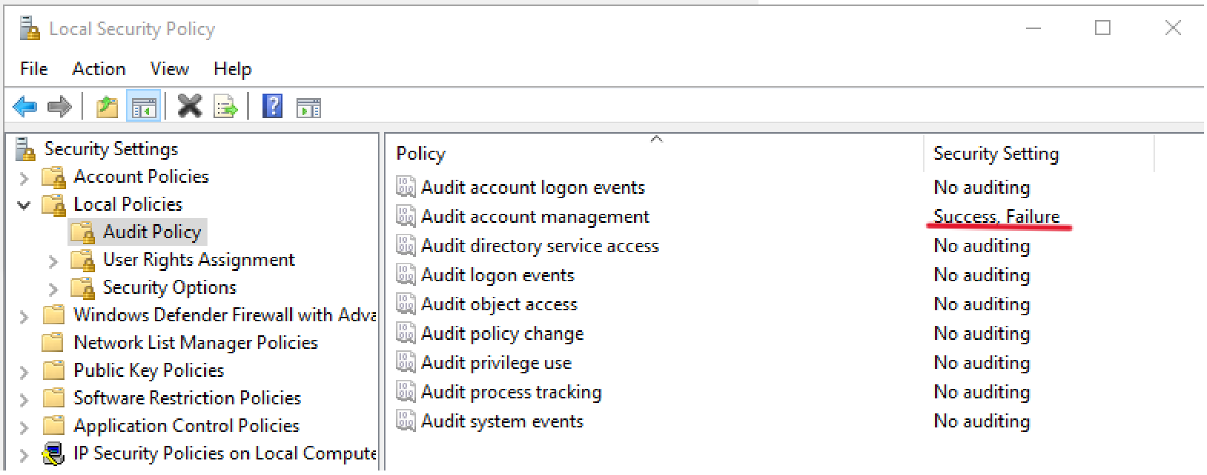
Audit account management

Audit these attempts:

☑ Success

☑ Failure

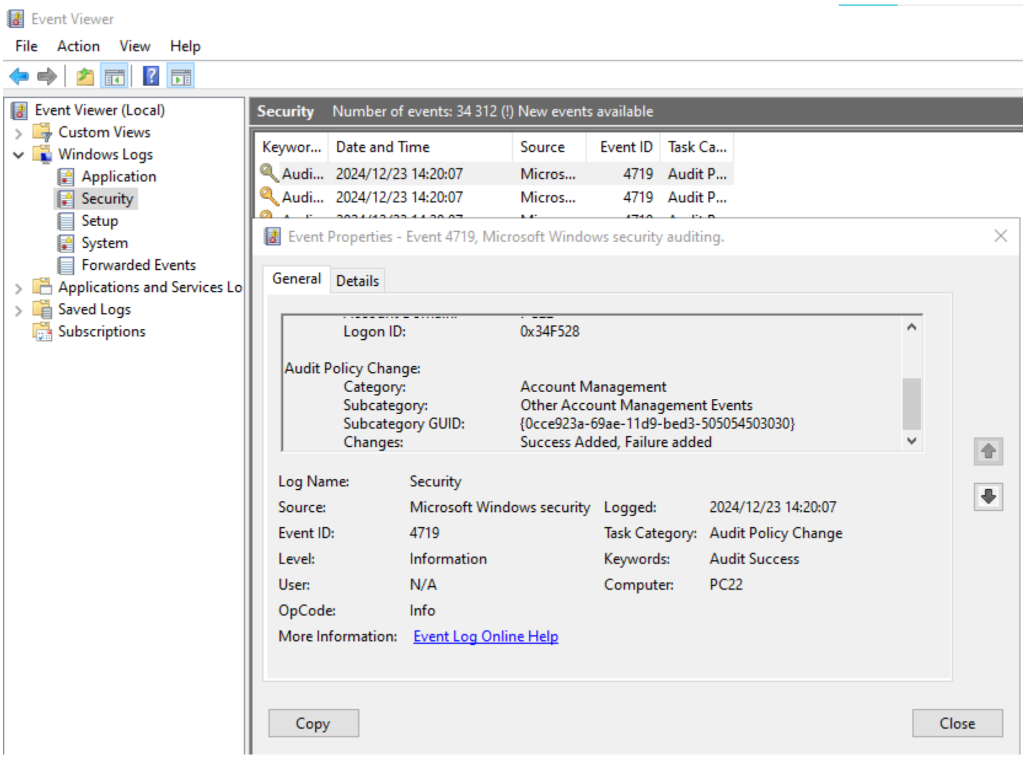
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account management. (Q921468)



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Once enabled, logs for account management activities will begin recording in the Event Viewer.



Security Number of events: 34 312 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	2024/12/23 14:20:07	Micros...	4719	Audit P...
Audi...	2024/12/23 14:20:07	Micros...	4719	Audit P...

Event Properties - Event 4719, Microsoft Windows security auditing.

```
        Logon ID:               0x34F528

Audit Policy Change:
        Category:               Account Management
        Subcategory:            Other Account Management Events
        Subcategory GUID:       {0cce923a-69ae-11d9-bed3-505054503030}
        Changes:                Success Added, Failure added
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2024/12/23 14:20:07
Event ID:	4719	Task Category:	Audit Policy Change
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC22
OpCode:	Info		
More Information:	Event Log Online Help		

Accessing Event Viewer

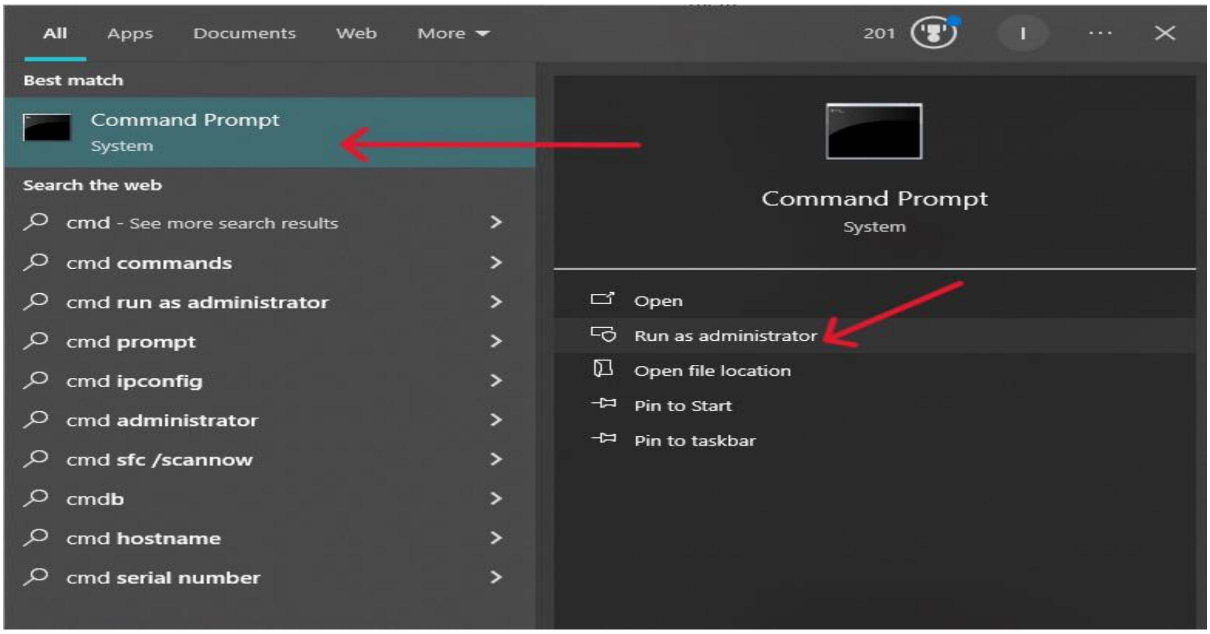
1. Press **Windows+R**, type eventvwr.msc, and press Enter.
2. Navigate to **Windows Logs > Security** to view account management events.

Event Trigger Scenarios

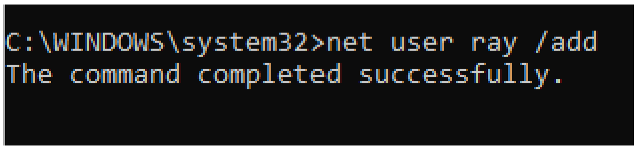
Triggering specific Event IDs allows administrators to simulate real-world scenarios for both testing and training purposes, providing valuable insights into system behavior and response readiness. Below are scenarios illustrating how to trigger specific Event IDs and respond to them:

1. Event ID 4720: User Account Created

Navigate to command prompt and run as administrator

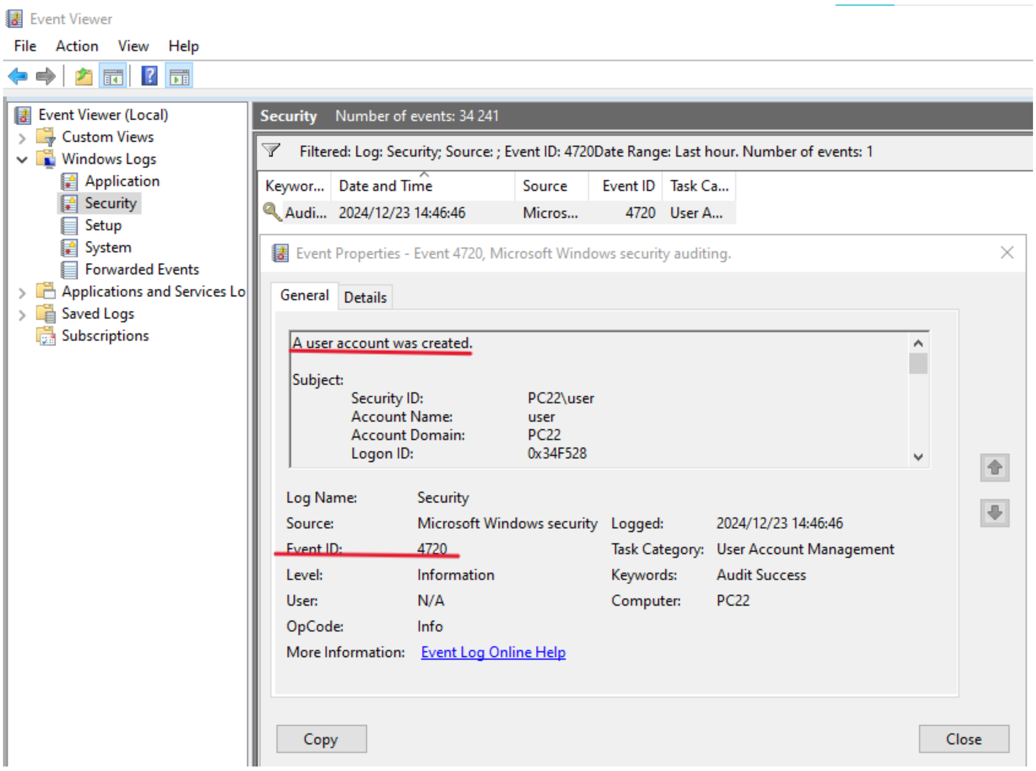


- **Trigger:** Use the command net user <username> /add. Example: net user ray /add



```
C:\WINDOWS\system32>net user ray /add
The command completed successfully.
```

Navigating to event viewer security events, you should see the triggered event id 4720 as per below:



Security Number of events: 34 241

Filtered: Log: Security; Source: ; Event ID: 4720Date Range: Last hour. Number of events: 1

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	2024/12/23 14:46:46	Micros...	4720	User A...

Event Properties - Event 4720, Microsoft Windows security auditing.

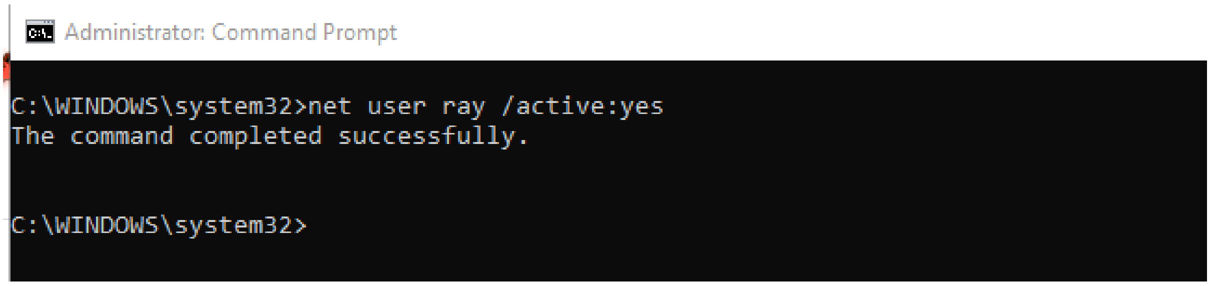
```
A user account was created.

Subject:
        Security ID:            PC22\user
        Account Name:           user
        Account Domain:         PC22
        Logon ID:               0x34F528
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:         2024/12/23 14:46:46
Event ID:         4720                         Task Category:  User Account Management
Level:            Information                  Keywords:       Audit Success
User:             N/A                          Computer:       PC22
OpCode:           Info
More Information: Event Log Online Help
```

- **Response:**
  - Investigate: Verify whether the account creation was authorized. Check the account creator and source system.
  - Analyze Logs: Cross-reference with other logs for suspicious activity.
  - Containment: Disable unauthorized accounts and escalate to the incident response team.
  - Document: Record details about the account creation and associated activities.
  -

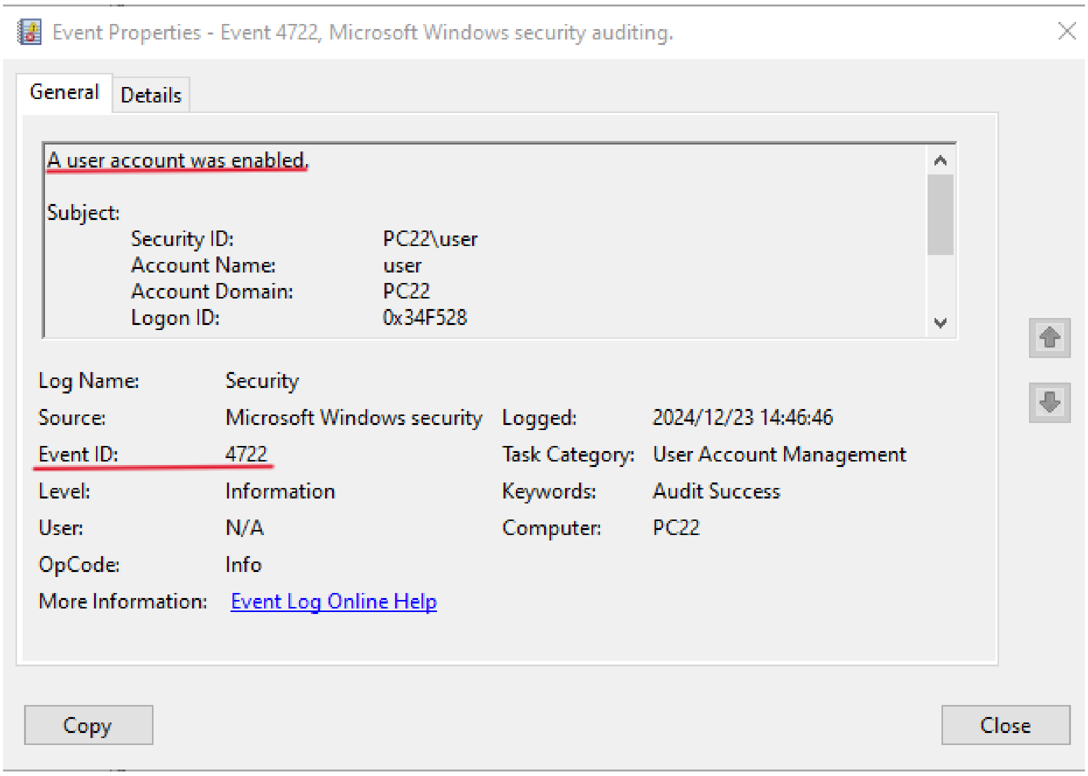
2. Event ID 4722: User Account Enabled

- **Trigger:** Use the command net user <username> /active:yes. Example: net user ray /active:yes



```
C:\WINDOWS\system32>net user ray /active:yes
The command completed successfully.


C:\WINDOWS\system32>
```

Navigating to event viewer security events, you should see the triggered event id 4722 as per below:



Event Properties - Event 4722, Microsoft Windows security auditing.
General
Details
Copy
Close

A user account was enabled.

Subject:

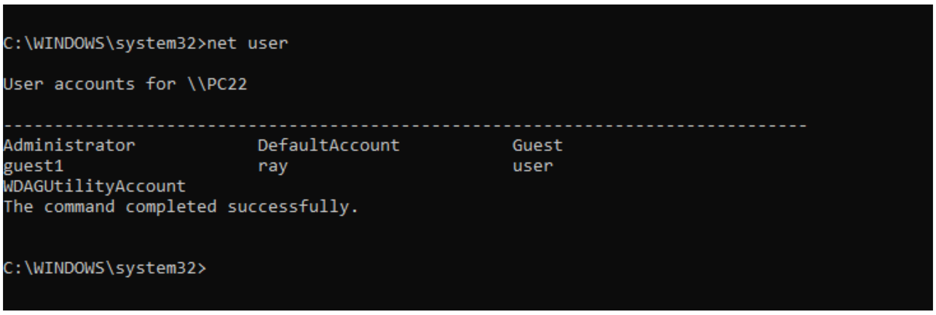
```
        Security ID:            PC22\user
        Account Name:           user
        Account Domain:         PC22
        Logon ID:               0x34F528
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:         2024/12/23 14:46:46
Event ID:         4722                         Task Category:  User Account Management
Level:            Information                  Keywords:       Audit Success
User:             N/A                          Computer:       PC22
OpCode:           Info
More Information: Event Log Online Help
```

- **Response:**
  - Investigate: Confirm if re-enabling the account aligns with policy.
  - Monitor Activity: Track the account's behavior for anomalies.
  - Take Action: Disable unauthorized accounts and check for other compromises.
  - Document: Record the event details, including the account enabler and time of action.

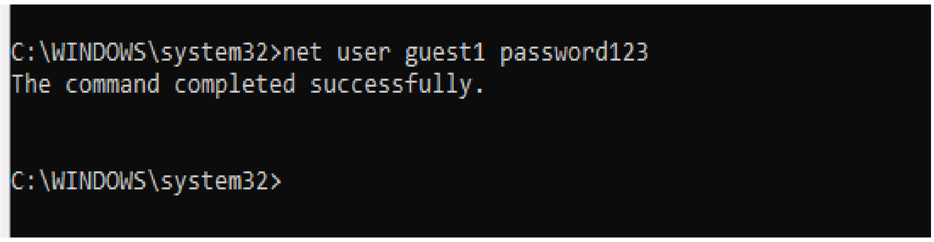
3. Event ID 4724: Password Reset Attempt

Using the net user command, a list of users were found. In this example we choose user guest1



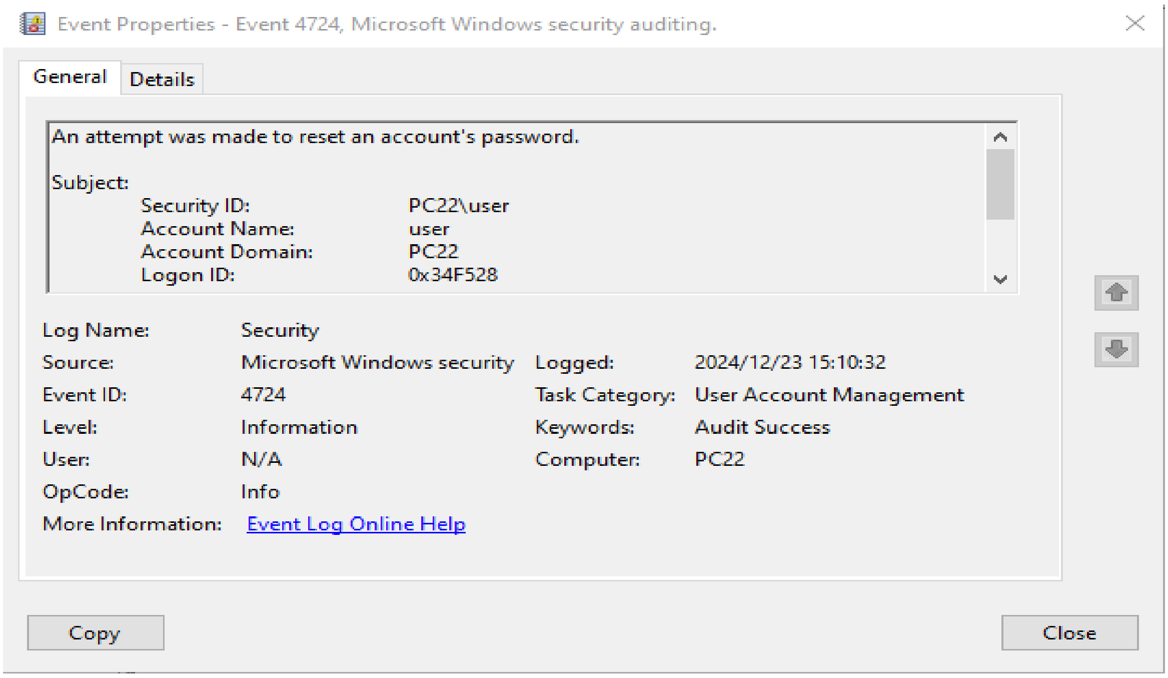
```
C:\WINDOWS\system32>net user

User accounts for \\PC22

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
guest1                   ray                      user
WDAGUtilityAccount
The command completed successfully.


C:\WINDOWS\system32>
```

- **Trigger:** Use the command net user <username> <newpassword>. Example: net user guest1 NewPass123!



```
C:\WINDOWS\system32>net user guest1 password123
The command completed successfully.


C:\WINDOWS\system32>
```

- **Triggered event:**



Event Properties - Event 4724, Microsoft Windows security auditing.

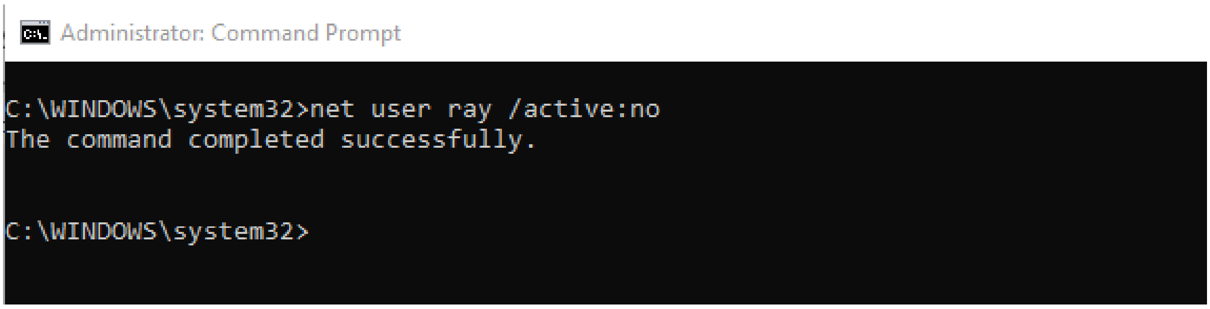
```
An attempt was made to reset an account's password.

Subject:
        Security ID:            PC22\user
        Account Name:           user
        Account Domain:         PC22
        Logon ID:               0x34F528
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2024/12/23 15:10:32
Event ID:	4724	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC22
OpCode:	Info		
More Information:	Event Log Online Help		

- **Response:**
  - Investigate: Determine who initiated the reset and ensure it aligns with policy.
  - Analyze Context: Look for preceding events, such as multiple failed login attempts (Event ID 4625).
  - Containment: Force a password reset and enforce MFA.
  - Document: Record findings and actions taken.

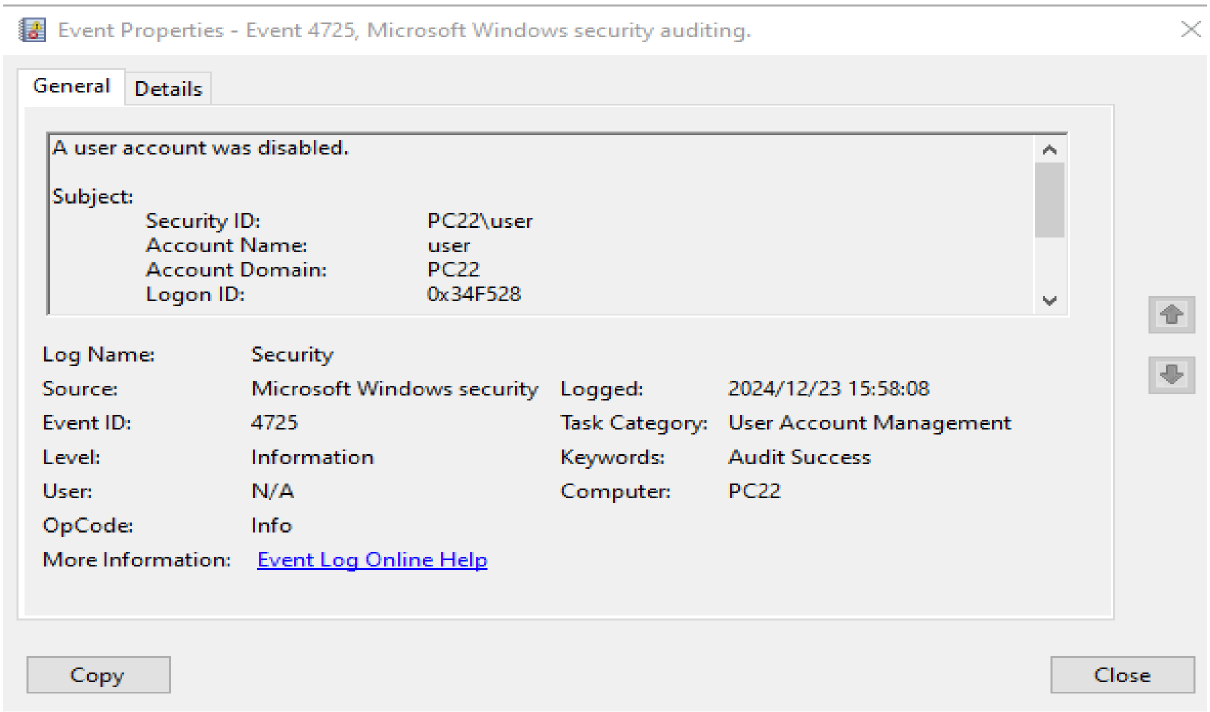
4. Event ID 4725: User Account Disabled

- **Trigger:** Use the command net user <username> /active:no. Example: net user ray /active:no.



```
C:\WINDOWS\system32>net user ray /active:no
The command completed successfully.


C:\WINDOWS\system32>
```

- **Triggered event:**


Event Properties - Event 4725, Microsoft Windows security auditing.
General
Details
Copy
Close

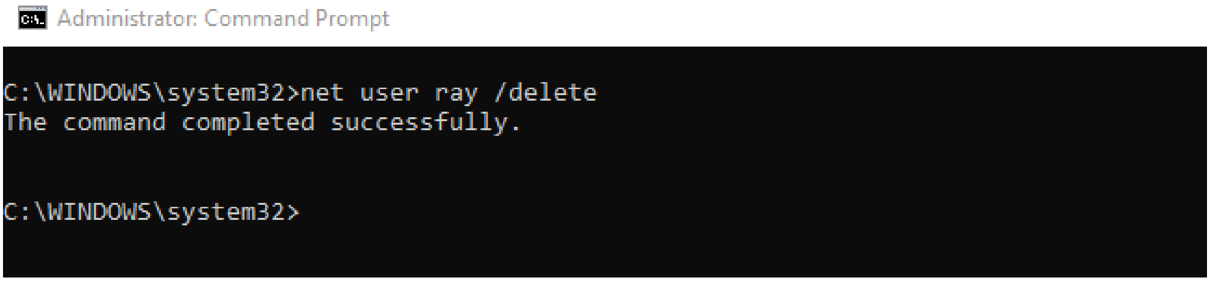
```
A user account was disabled.

Subject:
        Security ID:        PC22\user
        Account Name:       user
        Account Domain:     PC22
        Logon ID:           0x34F528
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2024/12/23 15:58:08
Event ID:	4725	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC22
OpCode:	Info		
More Information:	Event Log Online Help		

- **Response:**
  - Investigate: Verify whether the action aligns with administrative tasks.
  - Assess Impact: Ensure disabling the account doesn't disrupt operations.
  - Review History: Check prior activities on the account for compromise indicators.
  - Document: Record the reason for disabling and the responsible administrator.

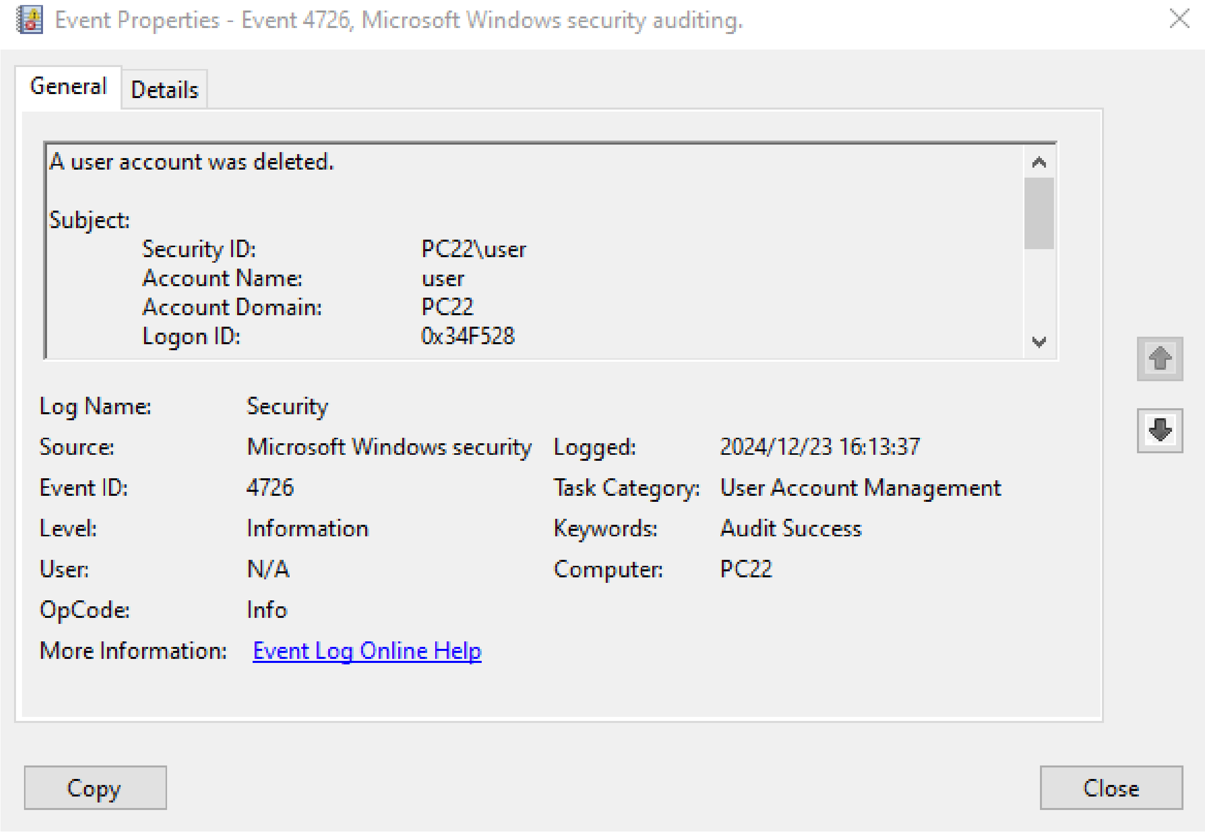
5. Event ID 4726: User Account Deleted

- **Trigger:** Use the command net user <username> /delete. Example: net user ray /delete



```
C:\WINDOWS\system32>net user ray /delete
The command completed successfully.


C:\WINDOWS\system32>
```

- **Triggered event:**


Event Properties - Event 4726, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A user account was deleted.

Subject:
        Security ID:        PC22\user
        Account Name:       user
        Account Domain:     PC22
        Logon ID:           0x34F528
```

Log Name: Security

Source: Microsoft Windows security

Logged: 2024/12/23 16:13:37

Event ID: 4726

Task Category: User Account Management

Level: Information

Keywords: Audit Success

User: N/A

Computer: PC22

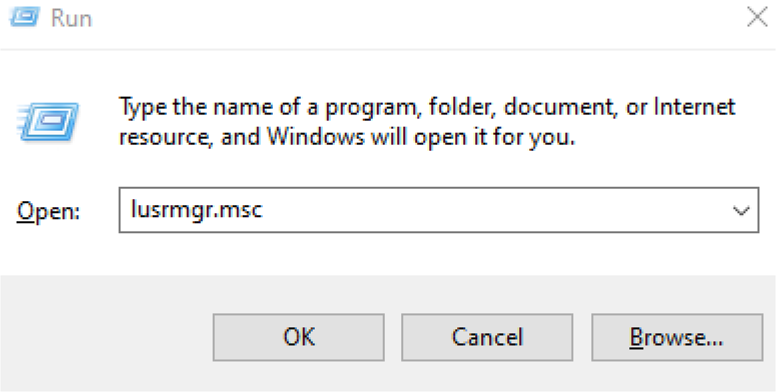
OpCode: Info

More Information: Event Log Online Help

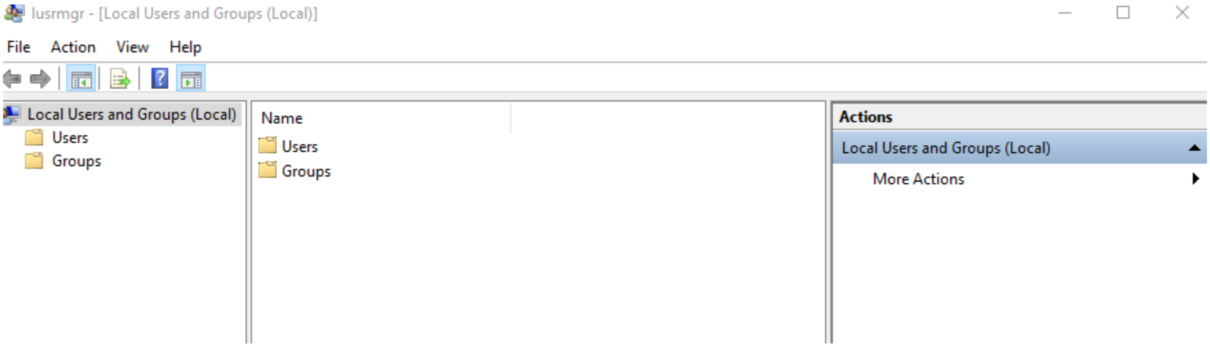
- **Response:**
  - Investigate: Confirm whether the account deletion was authorized.
  - Review Logs: Analyze activities before deletion for suspicious patterns.
  - Verify Backups: Ensure critical data isn't lost.
  - Document: Record the deletion details and administrator involved.

6. Event ID 4731: Security-Enabled Group Created

5. **Trigger:** Press **Windows+R**, type **lusrmgr.msc** and press Enter.

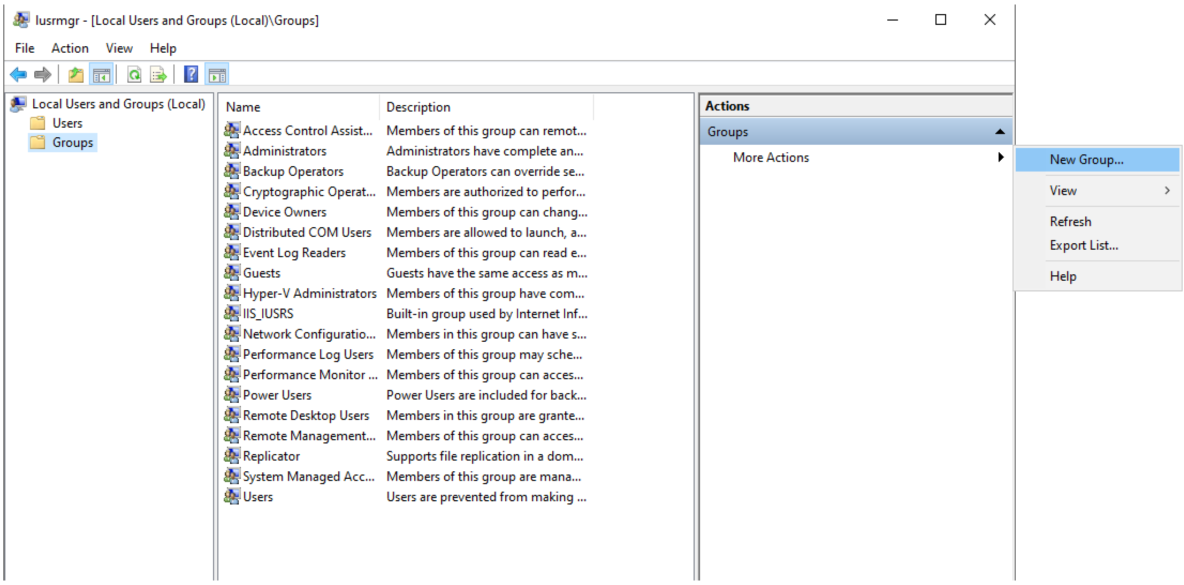


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: lusrmgr.msc
OK
Cancel
Browse...

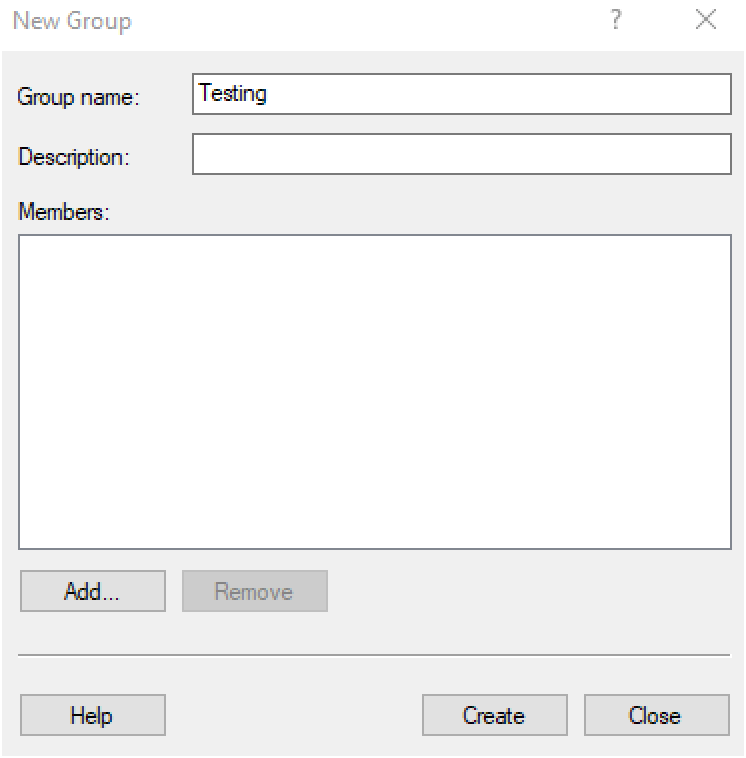


lusrmgr - [Local Users and Groups (Local)]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Users
Groups
Actions
Local Users and Groups (Local)
More Actions

To create a new group. Example: Group named "Testing" Go to groups , click more actions and new group



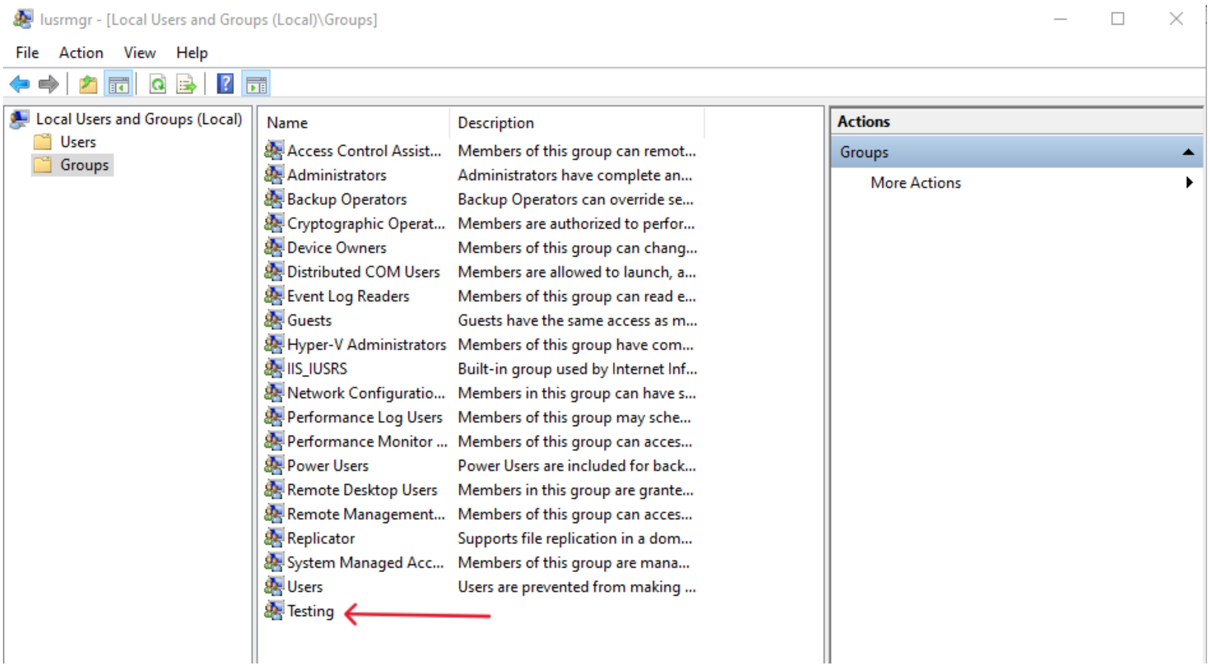
Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...



Group name: Testing

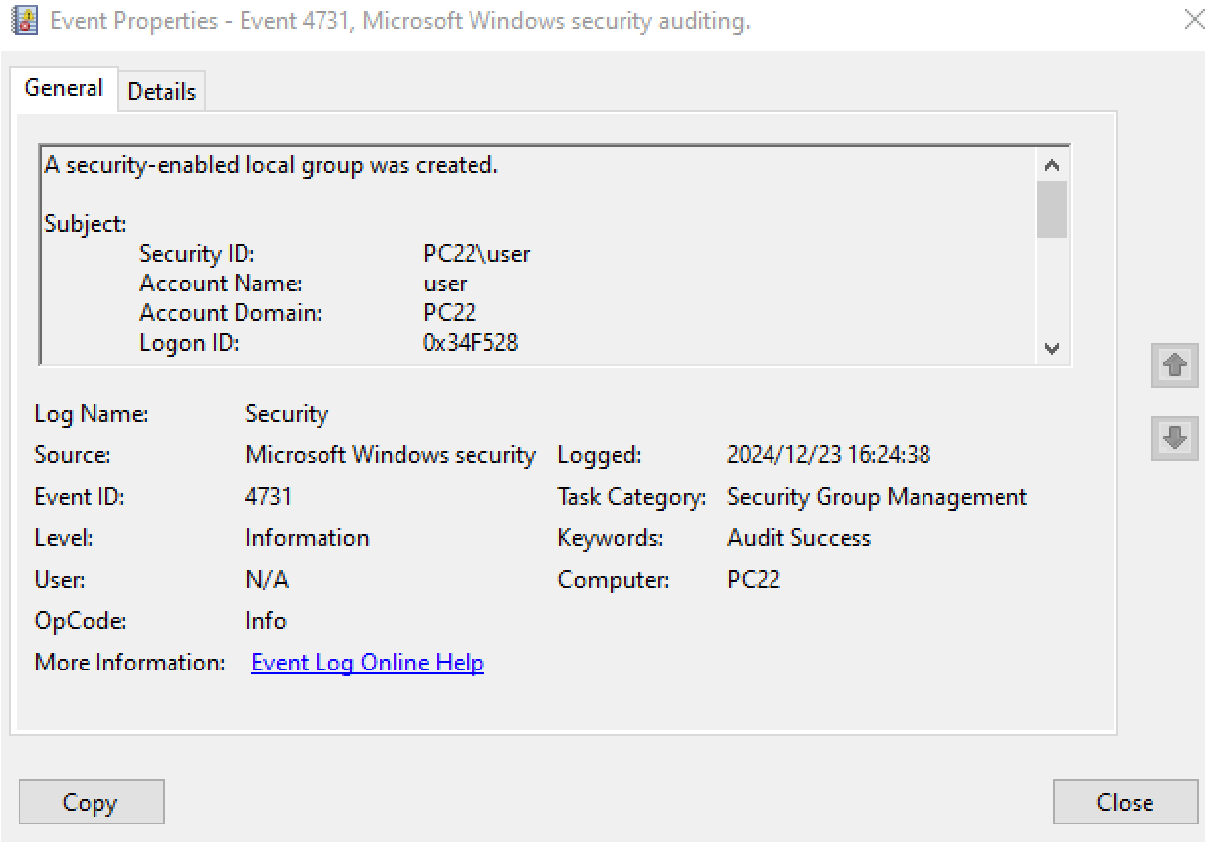
Description:

Members:


lusrmgr - [Local Users and Groups (Local)\Groups]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Actions
Groups
More Actions

Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...
Testing	

- **Triggered event:**


Event Properties - Event 4731, Microsoft Windows security auditing.
General
Details
Copy
Close

A security-enabled local group was created.

Subject:

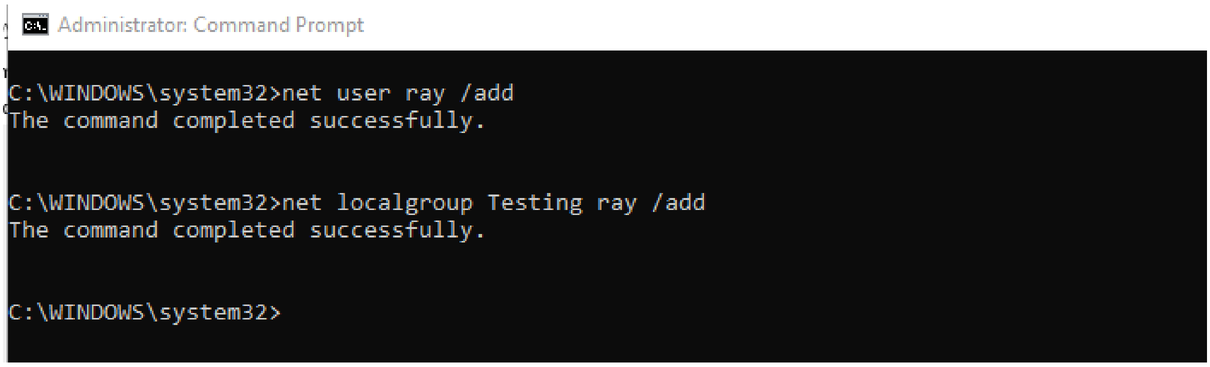
Security ID:	PC22\user
Account Name:	user
Account Domain:	PC22
Logon ID:	0x34F528

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2024/12/23 16:24:38
Event ID:	4731	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC22
OpCode:	Info		
More Information:	Event Log Online Help		

- **Response:**
  - Investigate: Validate the necessity and policy compliance.
  - Review Members: Prevent privilege escalation by auditing group membership.
  - Audit Purpose: Confirm the intended purpose of the group.
  - Document: Record the group name, creator, and rationale.

7. Event ID 4732: Member Added to Security-Enabled Group

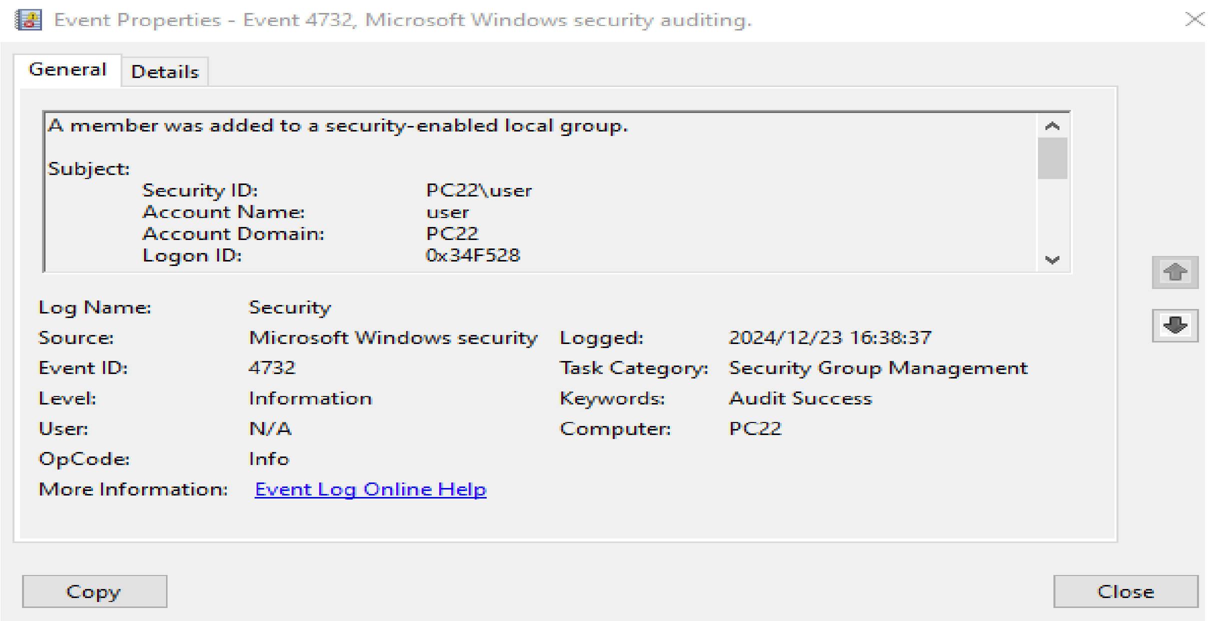
- **Trigger:** Use the command net localgroup <groupname> <username> /add. Example: net localgroup Testing ray /add



```
C:\WINDOWS\system32>net user ray /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup Testing ray /add
The command completed successfully.


C:\WINDOWS\system32>
```

- **Response:**
  - Investigate: Ensure the addition aligns with policy.
  - Check Timing: Look for anomalies in timing and origin.
  - Containment: Remove unauthorized members and review logs for misuse.
  - Document: Record changes and responsible parties.

- **Triggered event:**

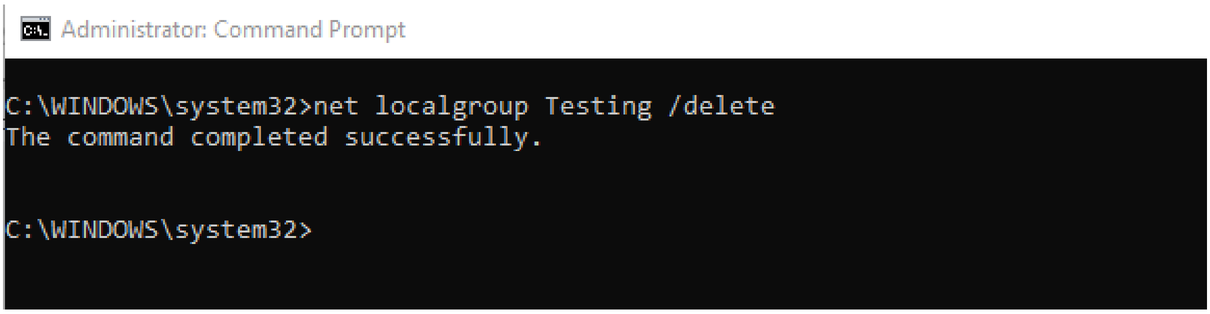

Event Properties - Event 4732, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            PC22\user
        Account Name:           user
        Account Domain:         PC22
        Logon ID:               0x34F528
```

Log Name: Security
Source: Microsoft Windows security
Logged: 2024/12/23 16:38:37
Event ID: 4732
Task Category: Security Group Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC22
OpCode: Info
More Information: Event Log Online Help

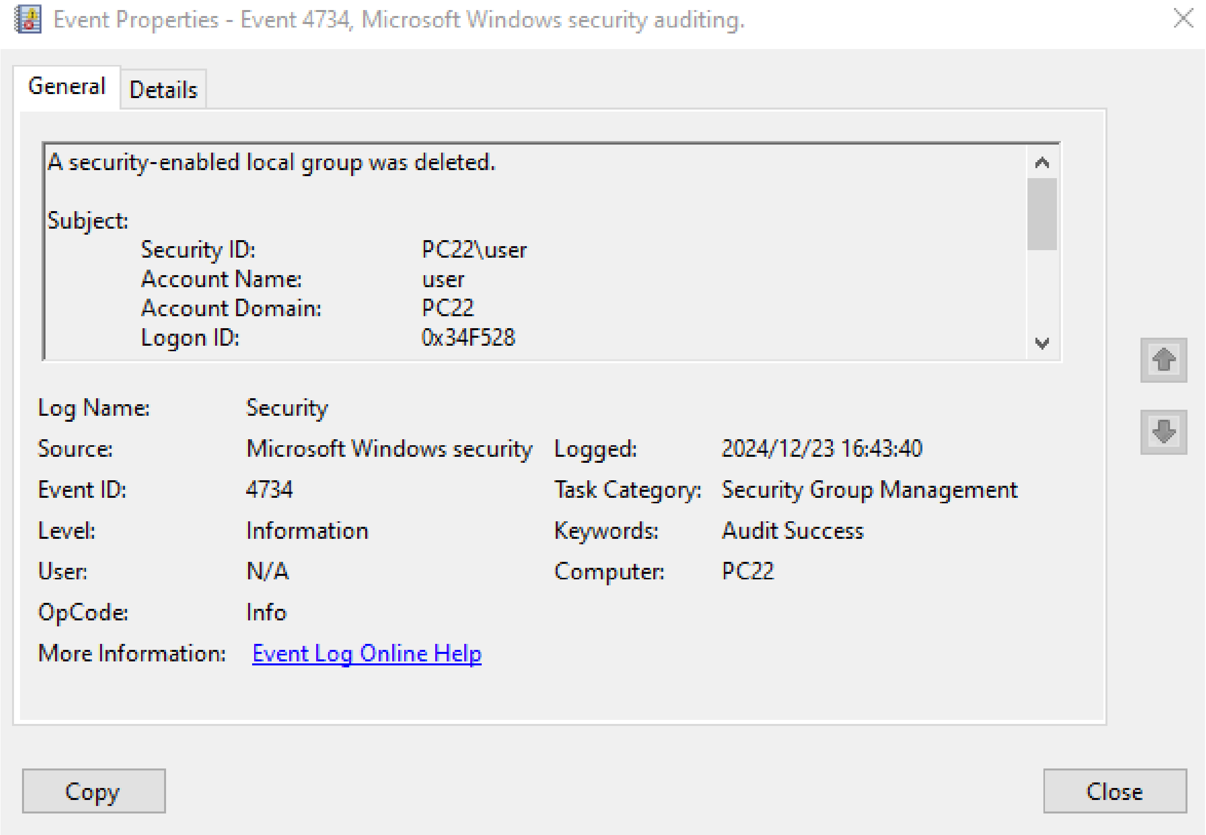
8. Event ID 4734: Security-Enabled Local Group Deleted

- **Trigger:** Use the command net localgroup <groupname> /delete. Example: net localgroup Testing /delete



```
C:\WINDOWS\system32>net localgroup Testing /delete
The command completed successfully.


C:\WINDOWS\system32>
```

- **Triggered event:**



Event Properties - Event 4734, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A security-enabled local group was deleted.

Subject:
        Security ID:        PC22\user
        Account Name:       user
        Account Domain:     PC22
        Logon ID:           0x34F528
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          2024/12/23 16:43:40
Event ID:          4734                         Task Category:   Security Group Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        PC22
OpCode:            Info
More Information:  Event Log Online Help
```

- **Response:**
  - Investigate: Confirm intentional deletion aligns with policy.
  - Assess Impact: Ensure no disruption to users or services.
  - Correlate Events: Identify surrounding activities indicating malicious intent.
  - Document: Record the deletion details and responsible administrator.

General Best Practices

- **Continuous Monitoring:** Use SIEM tools to correlate events and detect patterns.
- **Automated Alerts:** Configure real-time alerts for critical Event IDs.
- **Incident Response Plan:** Maintain a documented plan to address security incidents effectively.
- **User Education:** Train employees on security awareness to reduce insider threats.
- **Periodic Audits:** Regularly review user accounts, group memberships, and privileges.

By following these practices, organizations can proactively detect and mitigate threats associated with account management events, ensuring robust system security. Summarizing the key takeaways, organizations should focus on enabling detailed audit policies, responding effectively to account management events, and maintaining continuous monitoring through SIEM tools to stay ahead of potential threats.