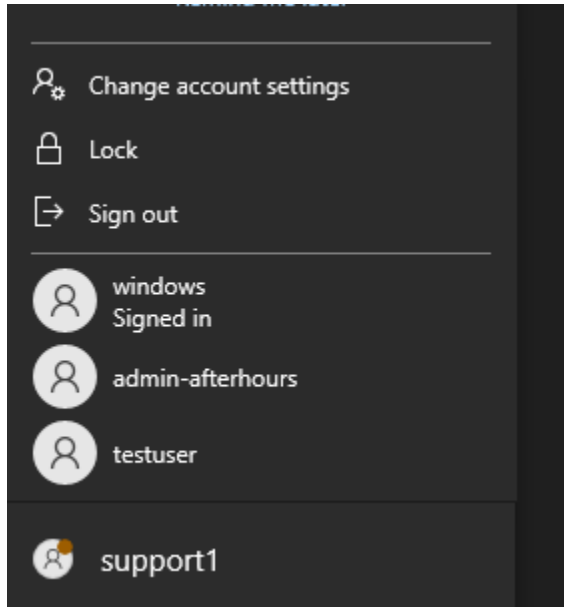


## Scenario 5: Hidden User Account Creation (T1136)

1. Create new windows account:
  - a. `net user support1 Password123! /add`
  - b. `net localgroup administrators support1 /add`



2. Enable Auditing on Windows (if not already):
  - a. `auditpol /set /category:"Account Management" /success:enable /failure:enable`
    - i. This ensures Event IDs 4720, 4728, and 4732 are logged.
3. Configure and Forward Logs to Splunk
  - a. Use **Universal Forwarder** on Windows 10
    - i. Download and install Splunk Universal Forwarder on Windows 10.
    - ii. During setup, input the Splunk server IP (Ubuntu machine) and receiver port (default is 9997).
    - iii. Choose to forward Security Logs.
    - iv. Restart the forwarder:
      1. `net stop splunkforwarder`
      2. `net start splunkforwarder`

```
Administrator: Command Prompt - net start splunkforwarder
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net stop splunkforwarder

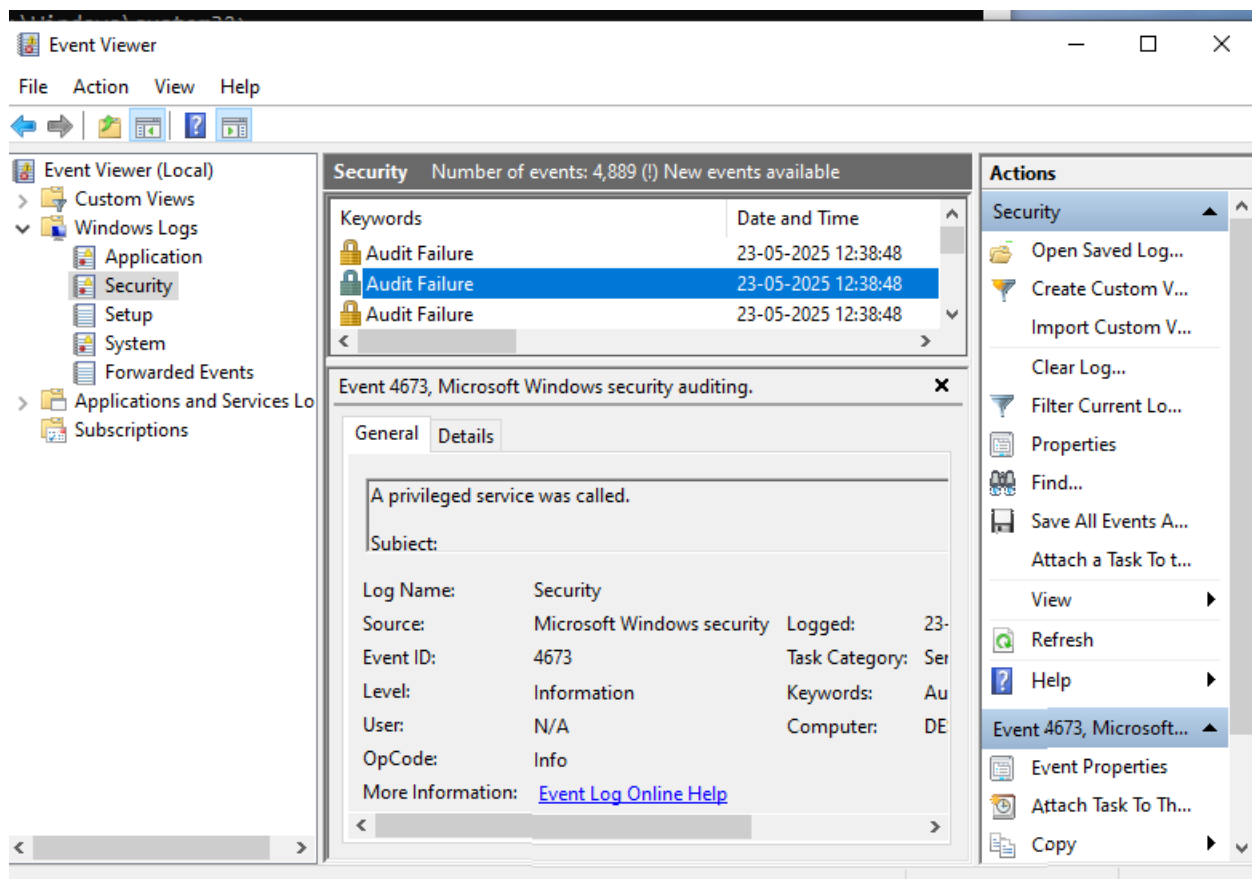
The SplunkForwarder service was stopped successfully.

C:\Windows\system32>net start splunkforwarder
The SplunkForwarder service is starting..
```

#### 4. Verify Events in Windows Event Viewer

##### a. **Event Viewer** → Windows Logs → **Security**

- i. Event ID 4720: A new account was created.
- ii. Event ID 4728 or 4732: The account was added to a privileged group.



5. Detect in Splunk (Ubuntu):  
a. index=wineventlog | head 10

New Search

index=\* | head 10

10 events (5/22/25 12:30:00.000 PM to 5/23/25 12:51:46.000 PM) No Event Sampling

Events (10) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View List

SELECTED FIELDS

- host: 1
- source: 1
- sourcetype: 1

INTERESTING FIELDS

- index: 1
- linecount: 1
- splunk\_server: 1

Time Event

5/23/25 12:46:13.000 PM 05/23/2025 12:46:13 PM

LogName=Security

EventCode=4673

EventType=8

ComputerName=DESKTOP-PERTPN8

SourceName=Microsoft Windows security auditing.

Type=Information

RecordNumber=19983

Keywords=Audit Failure

TaskCategory=Sensitive Privilege Use

OpCode=Info

Message=A privileged service was called.

Subject:

Security ID: S-1-5-88-972488765-139171986-783781252-3188962998-3738692313

Account Name: SplunkForwarder

Account Domain: NT SERVICE

Logon ID: 0xA32042

Service:

Domain: EcumidPo...

splunk-enterprise

New Search

index=\* | head 10

10 events (5/22/25 12:30:00.000 PM to 5/23/25 12:51:46.000 PM) No Event Sampling

Events (10) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View List

SELECTED FIELDS

- host: 1
- source: 1
- sourcetype: 1

INTERESTING FIELDS

- index: 1
- linecount: 1
- splunk\_server: 1

Time Event

5/23/25 12:46:13.000 PM 05/23/2025 12:46:13 PM

LogName=Security

EventCode=4673

EventType=8

ComputerName=DESKTOP-PERTPN8

SourceName=Microsoft Windows security auditing.

Type=Information

RecordNumber=19983

Keywords=Audit Failure

TaskCategory=Sensitive Privilege Use

OpCode=Info

Message=A privileged service was called.

Subject:

Security ID: S-1-5-88-972488765-139171986-783781252-3188962998-3738692313

Account Name: SplunkForwarder

Account Domain: NT SERVICE

Logon ID: 0xA32042

Here are some powerful use cases you can start with:

Goal	Event Code	Description
Detect user creation	4720	New user account created
Detect group addition	4728 , 4732	User added to group
Detect login attempts	4624 , 4625	Successful/failed logins
Detect privilege use	4670 , 4672	Admin privilege use

This is multiple logs in few seconds:

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** `http://127.0.0.1:8000/en-US/app/search/search?q=search index%3D* | head 10&display.page.search.mode=fast&dispatch.sample_ratio=1&workload_pool=6&earliest=-24h%40h&latest=`
- Navigation:** < Hide Fields, All Fields, Format, Show: 20 Per Page, View: List
- Results Table:**

	Time	Event
>	5/23/25 12:46:10.000 PM	05/23/2025 12:46:10 PM LogName=Security EventCode=4673 EventType=0 ComputerName=DESKTOP-PERTPN8 Show all 29 lines host = DESKTOP-PERTPN8   source = WinEventLog\Security   sourcetype = WinEventLog\Security
>	5/23/25 12:46:10.000 PM	05/23/2025 12:46:10 PM LogName=Security EventCode=4673 EventType=0 ComputerName=DESKTOP-PERTPN8 Show all 29 lines host = DESKTOP-PERTPN8   source = WinEventLog\Security   sourcetype = WinEventLog\Security
>	5/23/25 12:46:09.000 PM	05/23/2025 12:46:09 PM LogName=Security EventCode=4673 EventType=0 ComputerName=DESKTOP-PERTPN8 Show all 29 lines host = DESKTOP-PERTPN8   source = WinEventLog\Security   sourcetype = WinEventLog\Security
>	5/23/25 12:46:09.000 PM	05/23/2025 12:46:09 PM LogName=Security EventCode=4673 EventType=0 ComputerName=DESKTOP-PERTPN8 Show all 29 lines host = DESKTOP-PERTPN8   source = WinEventLog\Security   sourcetype = WinEventLog\Security
>	5/23/25 12:46:08.000 PM	05/23/2025 12:46:08 PM LogName=Security EventCode=4673 EventType=0 ComputerName=DESKTOP-PERTPN8 Show all 29 lines host = DESKTOP-PERTPN8   source = WinEventLog\Security   sourcetype = WinEventLog\Security