**Login Searches**

Monitoring login activity is a key aspect of workstation security and user behavior analysis. This document outlines several Splunk searches designed to track successful and unsuccessful login attempts across various logon types. These queries help identify interactive logins, remote access, and service-based logins, while filtering out background system accounts and noise.

**Successful Logins**

* **All Successful Logins**  
   Retrieves all successful login events (EventCode=4624). Filters out system accounts such as machine accounts (ending with $), as well as background service accounts like UMFD and DWM. Useful for a general overview of interactive and non-interactive user activity.

index=wineventlog EventCode=4624  
| mvexpand Account\_Name  
| where NOT like (Account\_Name, "%$") AND NOT like(Account\_Name, "UMFD%") AND NOT like (Account\_Name, "DWM%")  
| stats count by Account\_Name, ComputerName, Logon\_Type

A screenshot of a computer

AI-generated content may be incorrect.

* **Physical Logins**  
   Focuses on logins that occurred physically at the machine (Logon\_Type=2). These are interactive logins where a user wasat the device. Useful for identifying who is logging into workstations in person.

index=wineventlog EventCode=4624 Logon\_Type=2  
| mvexpand Account\_Name  
| where NOT like (Account\_Name, "%$") AND NOT like(Account\_Name, "UMFD%") AND NOT like (Account\_Name, "DWM%")  
| stats count by Account\_Name, ComputerName, Logon\_Type

* **Network Logins**  
   Captures remote login attempts, including successful (EventCode=4624) and failed (EventCode=4625) events. Filters for logon types 5 (service logons) and 10 (Remote Desktop/remote interactive). This version also filters results to a specific machine.

index=wineventlog EventCode=4624 AND (Logon\_Type=5 OR Logon\_Type=10)  
| mvexpand Account\_Name  
| where NOT like ("Account\_Name", "%$")  
| search ComputerName="806-LT2-CCOOK"

**Failed Logins**  
  
To keep track of the failed logins, all previous searches can be used with the EventCode=4625.

* **Brute Force Detection**

index=wineventlog EventCode=4625  
| bin \_time span=5min  
| stats count by \_time, ComputerName  
| where count >=5

- This search is set to run as a job every 5 minutes. It checks the last 5 minutes of logs to see if the count of failed login attempts is greater than or equal to 5. If the result is greater than one an alert is created on the alerts board.  
  
A screenshot of a computer

AI-generated content may be incorrect.