



## Windows Event Log for User Logon/Logoff

---

- Windows records successful or failed logon/logoff events under the Security events category. Logon events are very useful for tracking user activity.
- Event ID - 4624 – **Successful Logon**
- Event ID - 4625 – Failed Logon
- Event ID - 4634 – **Successful Logoff**
- Event ID - 4624 – Successful Network Logon



# Logon Type

---

- In addition to date, time, username, hostname, and success/failure status of a logon, we can also determine by exactly what means a logon was attempted.

Logon type values:

- |    |  |
|----|--|
| 2  | Logon via console                              |
| 3  | Network Logon                                  |
| 4  | Batch Logon                                    |
| 5  | Windows Service Logon                          |
| 7  | Credentials used to unlock screen              |
| 8  | Network logon sending credentials (cleartext)  |
| 9  | Different credentials used than logged on user |
| 10 | Remote interactive logon (RDP)                 |
| 11 | Cached credentials used to logon               |



# Filter Event Logs for Logon

---

- Event Viewer is a built-in tool for exploring event logs.
- By default, it displays the live system event logs. It can also be used to explore the saved/exported event log files.
  1. Open the saved event log files using event viewer.
  2. Event viewer will open the log file under 'saved logs' category.
  3. Click on 'Filter Current Log' from Actions menu on the right. A window will open.
  4. Select 'Filter' tab and enter the event IDs (e.g. 4624,4634) in the Event ID box and select 'OK'.
  5. Filtered event logs will be displayed.
  6. Click on 'Details' tab in lower pane for more details of the event.

# Filter Event Logs for Logon

Win\_7\_64\_secure\_coding

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - System
  - Forwarded Events
- Applications and Services Logs
  - Saved Logs
    - Event\_Logs**
    - Subscriptions

Event\_Logs Number of events: 384

Filtered: Advanced filter

Level

- Information
- Information
- Information
- Information
- Information
- Information

Event 4624, Microsoft Windows

General Details

Friendly View

+ System

- EventData

SubjectUser

SubjectUser

SubjectDomain

SubjectLogonType

TargetUser

TargetUser

TargetDomain

TargetLogonType

LogonProcess

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs: file:///C:/Users/skm/Desktop/Win\_Registry\_Fon

☐ By source Event sources:

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

4624,4634

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Actions

Event\_Logs

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...**
- Clear Filter
- Properties
- Find...
- Save Filtered Log File
- Save Filter to Custom View
- View
- Delete
- Rename
- Refresh
- Help

Event 4624, Microsoft Windows

- Event Properties
- Save Selected Events
- Copy
- Refresh
- Help



# Manually Filter Event Logs

---

- Open 'Filter Current Log' window. (Follow step 1-3 from previous section.)
- Select 'XML' tab.
- Check the 'Edit query manually' box and hit 'ok' for confirmation.
- Enter the XML query to filter and click 'ok'.
- E.g. To filter all logon attempts by using explicit credentials:

```
<QueryList>
  <Query Id="0" Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\Event_Logs.evtx">
    <Select Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\Event_Logs.evtx ">*
      [System[(EventID=4624)] and *[EventData[Data[@Name=LogonType] and (Data=2)]]</Select>
    </Query>
  </QueryList>
```

# Manually Filter Event Logs (Contd.)

The screenshot displays the Windows Event Viewer interface. The main pane shows a list of event logs with 'Event Logs' selected. The 'Filter Current Log' dialog box is open, showing the 'Filter' tab. The dialog contains the following text:

To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\
  \Event_Logs.evtx">
    <Select Path="file://C:\Users\IPAR\Desktop\Cases\Win_Registry_Forensics\
  \Event_Logs.evtx">*[System[(EventID=4624)]] and *[EventData[Data[@Name='LogonType']
  and (Data=2)]]</Select>
  </Query>
</QueryList>
```

The 'Edit query manually' checkbox is checked and highlighted with a purple oval. The 'OK' and 'Cancel' buttons are at the bottom right of the dialog.

On the right side of the Event Viewer, the 'Actions' pane is visible, showing options like 'Open Saved Log...', 'Create Custom View...', 'Filter Current Log...', 'Clear Filter', 'Properties', 'Find...', 'Save Filtered Log File As...', 'Save Filter to Custom View...', 'View', 'Delete', 'Rename', 'Refresh', 'Help', 'Event Properties', 'Save Selected Events...', 'Copy', 'Refresh', and 'Help'.