

# Incident Response: Windows Account Logon and logon Events

---

 [hackingarticles.in/incident-response-windows-account-logon-and-logon-events](https://hackingarticles.in/incident-response-windows-account-logon-and-logon-events)

Raj

September 2, 2020

A user when authenticates a Windows endpoint, then an Account Logon event will be generated and will be recorded. These account logon events will be recorded in the Security event log of the system which will be responsible for authentication of the user.

On accessing an account for a resource, a Logon event will be recorded. These logon events will be recorded in the Security event log of the system being accessed.

As an incident responder, if you spot account logon events on a machine other than the Domain Controller, it could be a sign of local user account usage.

Local user account usage is abnormal on domain environments and can indicate a compromise

## Table of Contents

---

- **Introduction**
- **Logon Events**
- **Account Logon Events**
- **Event ID's**
  - **Event ID 4624**
  - **Event ID 4625**
  - **Event ID 4634**
  - **Event ID 4647**
  - **Event ID 4648**
  - **Event ID 4672**
- **Kerberos Authentication Protocol**
  - **Event ID 4768**
  - **Event ID 4769**
  - **Event ID 4776**
  - **Event ID 4778**
  - **Event ID 4779**

## Introduction

---

A windows system has various authentication and logon methods to establish remote sessions between different systems over a network. In this article, we will be learning about different account logon events and authentication protocols like Kerberos.

The methods of Windows authentication range from a simple logon-based thing depending on the user's knowledge like a password, tokens, public key certificates, and biometrics, etc.

An authentication protocol like Kerberos defines rules and conventions and serves the authentication of users, computers, and services. The process of authentication allows an authorized user and services and gives access to resources in a much secure way.

## Logon Events

---

The Audit logon events are usually settings in the policy that records all attempts to log on to the local computer, whether by using a domain account or a local account. Audit Logon/Logoff events generate on the creation and destruction of logon sessions. These events occur on the machine that was accessed.

## Account Logon

---

Account Logon policy setting generates events for any type of credential validation. These events occur on the machine that is authoritative for the credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local machine is authoritative.

So, let's see these event IDs one by one across the Windows server.

## Event ID 4624

---

This event usually is generated for a successful logon. This event will contain information about the host and the name of the account involved. For remote logons, an incident responder should focus on the Network Information section of the event description for remote host information.

The fields Caller Process Name and Caller Process ID in the Process Information section of this event description provides more details about the process of initiating the logon.

| EVENT ID   | DESCRIPTION                            |
|--|--|
| 4624   | An account was successfully logged on. |
| <b>PURPOSE OF MONITORING THIS LOG</b>  |  |
| <ul style="list-style-type: none"><li>• It reveals the account present on local system that had requested the logon.</li><li>• To detect any abnormal or malicious activity.</li></ul> |  |

When a user successfully logs on to a computer, this event will be generated.

The screenshot displays the Windows Security Event Viewer interface. At the top, a header bar indicates 'Security' and 'Number of events: 1,561 (!) New events available'. Below this, a table lists several events. The first four rows are highlighted with a red box, showing 'Audit Success' events with Event ID 4624, Task Category 'Logon', and timestamps from 8/30/2020 7:00:39 AM to 7:00:32 AM. Below the table, a detailed view for 'Event 4624, Microsoft Windows security auditing.' is shown. The 'General' tab is active, displaying the message 'An account was successfully logged on.' (highlighted with a red box). Below this, the 'Subject' section lists: Security ID: SYSTEM, Account Name: DC1\$, Account Domain: IGNITE, and Logon ID: 0x3E7. The 'Logon Information' section lists: Logon Type: 5, Restricted Admin Mode: -, Virtual Account: No, and Elevated Token: Yes. At the bottom, a summary section provides additional details: Log Name: Security, Source: Microsoft Windows security, Logged: 8/30/2020 7:00:39 AM, Event ID: 4624, Task Category: Logon, Level: Information, Keywords: Audit Success, User: N/A, Computer: DC1.ignite.local, OpCode: Info, and a link to 'Event Log Online Help'.

| Keywords      | Event ID | Task Category | Date and Time        |
|---------------|----------|---------------|----------------------|
| Audit Success | 4624     | Logon         | 8/30/2020 7:00:39 AM |
| Audit Success | 4624     | Logon         | 8/30/2020 7:00:39 AM |
| Audit Success | 4624     | Logon         | 8/30/2020 7:00:39 AM |
| Audit Success | 4624     | Logon         | 8/30/2020 7:00:32 AM |

Event 4624, Microsoft Windows security auditing.

**General** Details

An account was successfully logged on.

**Subject:**

- Security ID: SYSTEM
- Account Name: DC1\$
- Account Domain: IGNITE
- Logon ID: 0x3E7

**Logon Information:**

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

**Log Name:** Security

**Source:** Microsoft Windows security **Logged:** 8/30/2020 7:00:39 AM

**Event ID:** 4624 **Task Category:** Logon

**Level:** Information **Keywords:** Audit Success

**User:** N/A **Computer:** DC1.ignite.local

**OpCode:** Info

**More Information:** [Event Log Online Help](#)

## Event ID 4625

This event is created on a failed logon attempt. Usually, these logs in a network may indicate password guessing attacks. The Network Information of this event can provide valuable information if a remote host is attempting to log on to the system.

As an incident responder, you can determine more about the reason for the failure by going through the description.

| EVENT ID  | DESCRIPTION                  |
|---|------------------------------|
| 4625  | An account failed to log on. |
| <b>PURPOSE OF MONITORING THIS LOG</b>   |                              |
| <ul style="list-style-type: none"> <li>As it lists every failed attempt on the system that is regardless of logon type, user location or its account type.</li> </ul> |                              |

When a user has a failed login attempt on to a computer, this event will be generated.

The screenshot shows the Windows Security Event Viewer interface. At the top, it says "Security" and "Number of events: 1,561 (!) New events available". Below this is a table of events. One event is highlighted with a red box:

| Keywords      | Event ID | Task Category | Date and Time        |
|---------------|----------|---------------|----------------------|
| Audit Failure | 4625     | Logon         | 8/30/2020 6:59:59 AM |
| Audit Failure | 4625     | Logon         | 8/30/2020 6:12:01 AM |
| Audit Failure | 4625     | Logon         | 8/30/2020 5:23:57 AM |
| Audit Failure | 4625     | Logon         | 8/30/2020 6:59:58 AM |

Below the table, the details for Event 4625 are shown. The "General" tab is selected, and the description "An account failed to log on." is highlighted with a red box. The "Details" tab shows the following information:

**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: CLIENTS  
 Account Domain: IGNITE

At the bottom, there is a summary of the event:

Log Name: Security  
 Source: Microsoft Windows security  
 Event ID: 4625  
 Level: Information  
 User: N/A  
 OpCode: Info  
 More Information: [Event Log Online Help](#)

Logged: 8/30/2020 6:59:59 AM  
 Task Category: Logon  
 Keywords: Audit Failure  
 Computer: DC1.ignite.local

## Event ID 4634

When a user logs off from his system, it is recorded by Event ID 4634. If a system doesn't show an event showing a logoff, you as an incident responder you should not be considered overly suspicious.

| EVENT ID | DESCRIPTION                |
|----------|----------------------------|
| 4634     | An account was logged off. |

## PURPOSE OF MONITORING THIS LOG

It indicates the account logoff of a session including RDP.

Security Number of events: 1,561 (!) New events available

| Keywords      | Event ID | Task Category | Date and Time        |
|---------------|----------|---------------|----------------------|
| Audit Success | 4634     | Logoff        | 8/30/2020 6:29:10 AM |
| Audit Success | 4634     | Logoff        | 8/30/2020 6:03:53 AM |
| Audit Success | 4634     | Logoff        | 8/30/2020 6:30:44 AM |
| Audit Success | 4634     | Logoff        | 8/30/2020 6:29:10 AM |

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

Security ID: SYSTEM  
Account Name: DC1\$  
Account Domain: IGNITE  
Logon ID: 0x1E2BA2

Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4634  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 8/30/2020 6:29:10 AM  
Task Category: Logoff  
Keywords: Audit Success  
Computer: DC1.ignite.local

## Event ID 4647

This event is usually triggered when no user-initiated activities no longer occur. This is different from event 4634, that is generally generated when a session no longer exists because of termination.

This event generates when a user logon is of remote type and the logoff was with some standard method.

| EVENT ID  | DESCRIPTION            |
|---|------------------------|
| 4647  | User initiated logoff. |
| <b>PURPOSE OF MONITORING THIS LOG</b>   |                        |
| As it shows a difference between logs that result due to idle sessions and where a user himself logs off from his system. |                        |

Security Number of events: 1,561 (!) New events available

| Keywords           | Event ID | Task Category | Date and Time        |
|--------------------|----------|---------------|----------------------|
| Event ID: 4647 (1) |          |               |                      |
| Audit Success      | 4647     | Logoff        | 8/30/2020 7:00:01 AM |

Event 4647, Microsoft Windows security auditing.

General Details

User initiated logoff:

Subject:

|                 |                      |
|-----------------|----------------------|
| Security ID:    | IGNITE\Administrator |
| Account Name:   | Administrator        |
| Account Domain: | IGNITE               |
| Logon ID:       | 0x3E355              |

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4647

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 8/30/2020 7:00:01 AM

Task Category: Logoff

Keywords: Audit Success

Computer: DC1.ignite.local

## Event ID 4648

---

A logon was attempted using explicit credentials. When a user attempts to use credentials that are of other than his, or if there is a user account control bypass to open a process with administrator permissions, this event is logged.

| EVENT ID  | DESCRIPTION                                       |
|---|---|
| 4648  | A logon was attempted using explicit credentials. |
| <b>PURPOSE OF MONITORING THIS LOG</b>   |   |
| To keep an eye on processes in this event<br>To monitor when and how a particular account is accessed.<br>To monitor actions of high value accounts |   |

Security Number of events: 1,561 (!) New events available

| Keywords      | Event ID | Task Category | Date and Time        |
|---------------|----------|---------------|----------------------|
| Audit Success | 4648     | Logon         | 8/30/2020 7:59:12 AM |
| Audit Success | 4648     | Logon         | 8/30/2020 7:54:35 AM |
| Audit Success | 4648     | Logon         | 8/30/2020 7:00:23 AM |
| Audit Success | 4648     | Logon         | 8/30/2020 7:01:31 AM |

Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:

Security ID: SYSTEM  
Account Name: DC1\$  
Account Domain: IGNITE  
Logon ID: 0x3E7  
Logon GUID: {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:

Account Name: Administrator  
Account Domain: IGNITE  
Logon GUID: {ef95fad6-4d8c-4cdb-ba8a-62b021558786}

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4648  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 8/30/2020 7:59:12 AM  
Task Category: Logon  
Keywords: Audit Success  
Computer: DC1.ignite.local

## Event ID 4672

When a set of sensitive privileges are assigned to a new logon session, this event is generated for that particular new logon. This event is usually recorded in the event viewer as and when a single local system account logon triggers this event.

| EVENT ID   | DESCRIPTION                               |
|--|---|
| 4672   | Special privileges assigned to new logon. |
| PURPOSE OF MONITORING THIS LOG   |   |
| <ul style="list-style-type: none"> <li>To make sure that certain privileges are never granted</li> <li>To monitor certain sensitive privileges.</li> </ul> |   |



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

| Keywords            | Event... | Task Category | Date and Time        |
|---------------------|----------|---------------|----------------------|
| Event ID: 4672 (10) |          |               |                      |
| Audit Success       | 4672     | Special Logon | 8/30/2020 4:58:46 AM |
| Audit Success       | 4672     | Special Logon | 8/30/2020 4:58:43 AM |
| Audit Success       | 4672     | Special Logon | 8/30/2020 4:58:46 AM |
| Audit Success       | 4672     | Special Logon | 8/30/2020 5:00:43 AM |
| Audit Success       | 4672     | Special Logon | 8/30/2020 4:58:58 AM |

Event 4672, Microsoft Windows security auditing.

**General** Details

Special privileges assigned to new logon.

Subject:

Security ID: SYSTEM  
Account Name: DC1\$  
Account Domain: IGNITE  
Logon ID: 0x127F8E

Privileges:

SeSecurityPrivilege  
SeBackupPrivilege  
SeRestorePrivilege  
SeTakeOwnershipPrivilege

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4672  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 8/30/2020 4:58:46 AM  
Task Category: Special Logon  
Keywords: Audit Success  
Computer: DC1.ignite.local

## Kerberos Authentication Protocol

Kerberos is an **authentication protocol** that works on the basis of tickets that allows the **nodes** to communicate over a non-secure network to prove their identity to each other in a secure manner.

So, let us understand the basics of Kerberos and then go ahead with Kerberos authentication protocol and the proceed with the event logs.

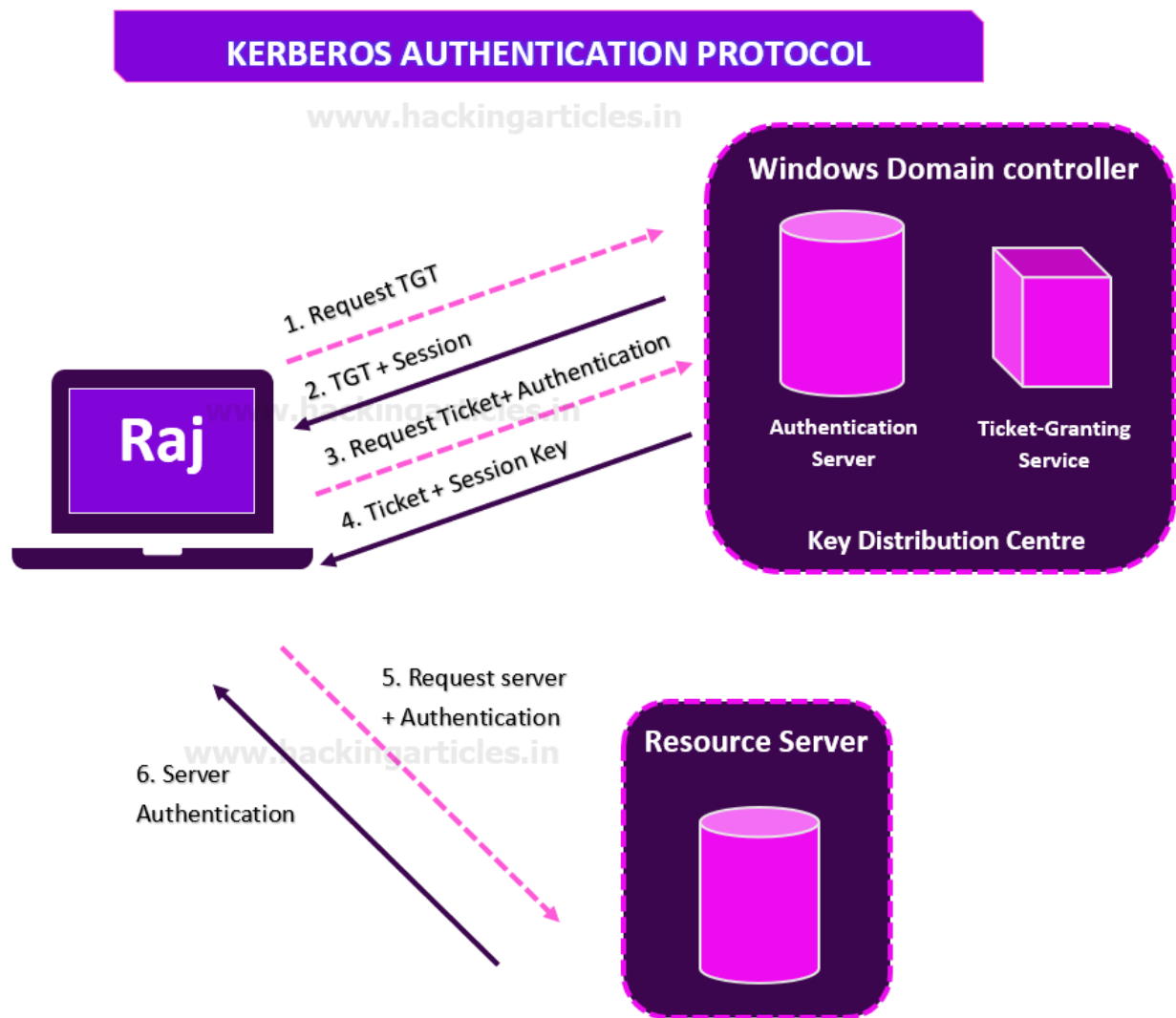
**Client:** A user that requests communication service request.

**Resource Server:** The server with the service the user wants to access.

**Authentication Server:** It performs client authentication, issues TGS on successful authentication.

**Key Distribution Centre:** Database, Authentication Server and Ticket Granting Server collectively is called Key Distribution Centre.

**Ticket Granting Server:** It is an application server that provides the issuing of service tickets as a service.



## Event ID 4768

On successful issuance of a TGT, it will show that a user account was authenticated by the domain controller. The Keywords field would indicate whether the authentication attempt was successful or failed.

| EVENT ID | DESCRIPTION                                    |
|----------|--|
| 4768     | A Kerberos service ticket (TGT) was requested. |

**PURPOSE OF MONITORING THIS LOG**

- To keep a watch on accounts whose Account Name corresponds with high-value accounts, that includes administrators, built-in local administrators, domain administrators, and service accounts.

Security Number of events: 423 (!) New events available

| Keywords            | Event... | Task Category                   | Date and Time        |
|---------------------|----------|---------------------------------|----------------------|
| Event ID: 4768 (5)  |          |                                 |                      |
| Audit Success       | 4768     | Kerberos Authentication Service | 8/30/2020 4:35:38 AM |
| Audit Success       | 4768     | Kerberos Authentication Service | 8/30/2020 4:23:58 AM |
| Audit Success       | 4768     | Kerberos Authentication Service | 8/30/2020 4:26:42 AM |
| Audit Success       | 4768     | Kerberos Authentication Service | 8/30/2020 4:23:52 AM |
| Audit Success       | 4768     | Kerberos Authentication Service | 8/30/2020 4:24:06 AM |
| Event ID: 4769 (16) |          |                                 |                      |

Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name: Administrator  
 Supplied Realm Name: IGNITE  
 User ID: IGNITE\Administrator

Service Information:

Service Name: krbtgt  
 Service ID: IGNITE\krbtgt

Log Name: Security  
 Source: Microsoft Windows security  
 Event ID: 4768  
 Level: Information  
 User: N/A  
 OpCode: Info  
 More Information: [Event Log Online Help](#)

Logged: 8/30/2020 4:35:38 AM  
 Task Category: Kerberos Authentication Service  
 Keywords: Audit Success  
 Computer: DC1.ignite.local

## Event ID 4769

Once the client successfully receives a ticket-granting ticket from the KDC, it will store that TGT and send it to the TGS with the Service Principal Name (SPN) of the resource that the client wants to access. TGTs are valid for a certain period of time only.

| EVENT ID | DESCRIPTION                              |
|----------|--|
| 4769     | A Kerberos service ticket was requested. |

**PURPOSE OF MONITORING THIS LOG**

- To keep a track of logon attempts that are outside an internal IP range.

Security Number of events: 423 (!) New events available

| Keywords      | Event... | Task Category                      | Date and Time        |
|---------------|----------|------------------------------------|----------------------|
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:23:52 AM |
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:35:38 AM |
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:26:42 AM |
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:23:52 AM |
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:23:52 AM |
| Audit Success | 4769     | Kerberos Service Ticket Operations | 8/30/2020 4:24:01 AM |

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:

Account Name: DC1S@IGNITE.LOCAL  
Account Domain: IGNITE.LOCAL  
Logon GUID: {751280ad-01a9-8cf5-cd66-01682d39774a}

Service Information:

Service Name: krbtgt  
Service ID: IGNITE\krbtgt

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4769  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 8/30/2020 4:23:52 AM  
Task Category: Kerberos Service Ticket Operations  
Keywords: Audit Success  
Computer: DC1.ignite.local

## Event ID 4776

When the computer logon is to be verified, this event is created. It contains additional information about the remote host in the event of a remote logon attempt. The Keywords field indicates whether the authentication attempt succeeded or failed

| EVENT ID  | DESCRIPTION  |
|---|--|
| 4776  | The computer attempted to validate the credentials for an account. |
| <b>PURPOSE OF MONITORING THIS LOG</b>   |  |
| <ul style="list-style-type: none"><li>• To identify multiple logons attempts with to check for brute-force attacks on your network.</li><li>• To check for attempts from unauthorized endpoints, or attempts outside of business hours, with malicious intent for high-value accounts</li></ul> |  |

Security Number of events: 423 (!) New events available

| Keywords           | Event... | Task Category         | Date and Time        |
|--------------------|----------|-----------------------|----------------------|
| Event ID: 4776 (2) |          |                       |                      |
| Audit Success      | 4776     | Credential Validation | 8/30/2020 4:35:16 AM |
| Audit Success      | 4776     | Credential Validation | 8/30/2020 4:19:40 AM |

Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Logon Account: administrator  
Source Workstation: CLIENT  
Error Code: 0x0

Log Name: Security  
Source: Microsoft Windows security Logged: 8/30/2020 4:35:16 AM  
Event ID: 4776 Task Category: Credential Validation  
Level: Information Keywords: Audit Success  
User: N/A Computer: DC1.ignite.local  
OpCode: Info  
More Information: [Event Log Online Help](#)

## Event ID 4778

This event is created when a session is reconnected to a Windows station. If a user reconnects with an existing Terminal Services session, or switches to an existing desktop using Fast User Switching, event 4778 is generated. This event is also triggered when a user reconnects to a virtual host.

| EVENT ID   | DESCRIPTION                                    |
|--|--|
| 4778   | A session was reconnected to a Window Station. |
| <b>PURPOSE OF MONITORING THIS LOG</b> <ul style="list-style-type: none"> <li>• To check on sessions when Fast User Switching has been disabled</li> <li>• To keep an eye when remote desktop connections are not allowed for certain users.</li> </ul> |  |

Security Number of events: 3,564 (!) New events available

| Keywords      | Event... | Task Category             | Date and Time        |
|---------------|----------|---------------------------|----------------------|
| Audit Success | 4778     | Other Logon/Logoff Events | 8/30/2020 8:56:00 AM |
| Audit Success | 4778     | Other Logon/Logoff Events | 8/30/2020 8:55:41 AM |

Event 4778, Microsoft Windows security auditing.

General Details

A session was reconnected to a Window Station.

Subject:

Account Name: Administrator  
Account Domain: IGNITE  
Logon ID: 0x4E848

Session:

Session Name: Console

Additional Information:

Client Name: Unknown

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4778  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 8/30/2020 8:56:00 AM  
Task Category: Other Logon/Logoff Events  
Keywords: Audit Success  
Computer: DC1.ignite.local

## Event ID 4779

If a user disconnects from an existing Terminal Services session, or switches away from an existing desktop using Fast User Switching, this event is generated. This event is also created when a user disconnects from a virtual host.

| EVENT ID   | DESCRIPTION                                       |
|--|---|
| 4779   | A session was disconnected from a Window Station. |
| <b>PURPOSE OF MONITORING THIS LOG</b> <ul style="list-style-type: none"> <li>To make sure that non-active, external or any restricted accounts are not used.</li> <li>To make sure that only specific accounts can perform certain actions.</li> </ul> |   |

Security Number of events: 3,564 (!) New events available

| Keywords           | Event... | Task Category             | Date and Time        |
|--------------------|----------|---------------------------|----------------------|
| Event ID: 4779 (2) |          |                           |                      |
| Audit Success      | 4779     | Other Logon/Logoff Events | 8/30/2020 8:55:40 AM |
| Audit Success      | 4779     | Other Logon/Logoff Events | 8/30/2020 8:55:46 AM |

Event 4779, Microsoft Windows security auditing.

General Details

A session was disconnected from a Window Station.

Subject:

Account Name: Administrator  
Account Domain: IGNITE  
Logon ID: 0x4E848

Session:

Session Name: Console

Additional Information:

Client Name: Unknown

Log Name: Security

Source: Microsoft Windows security Logged: 8/30/2020 8:55:40 AM

Event ID: 4779 Task Category: Other Logon/Logoff Events

Level: Information Keywords: Audit Success

User: N/A Computer: DC1.ignite.local

OpCode: Info

More Information: [Event Log Online Help](#)

You can also try out some other event ID's from below.



| EVENT ID | DESCRIPTION  |
|----------|--|
| 4770     | A service ticket was renewed. The account name, service name, client IP address, and encryption type are recorded. |
| 4771     | Kerberos pre-authentication failed.  |
| 4772     | A Kerberos authentication ticket request failed.   |
| 4773     | A Kerberos service ticket request failed.  |

**Author:** Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on [Here](#)