Learn Discover Product documentation Development languages Topics Sign in

We're no longer updating this content regularly. Check the Microsoft Product Lifecycle for information about how this product, service, technology, or API is supported.

Return to main site

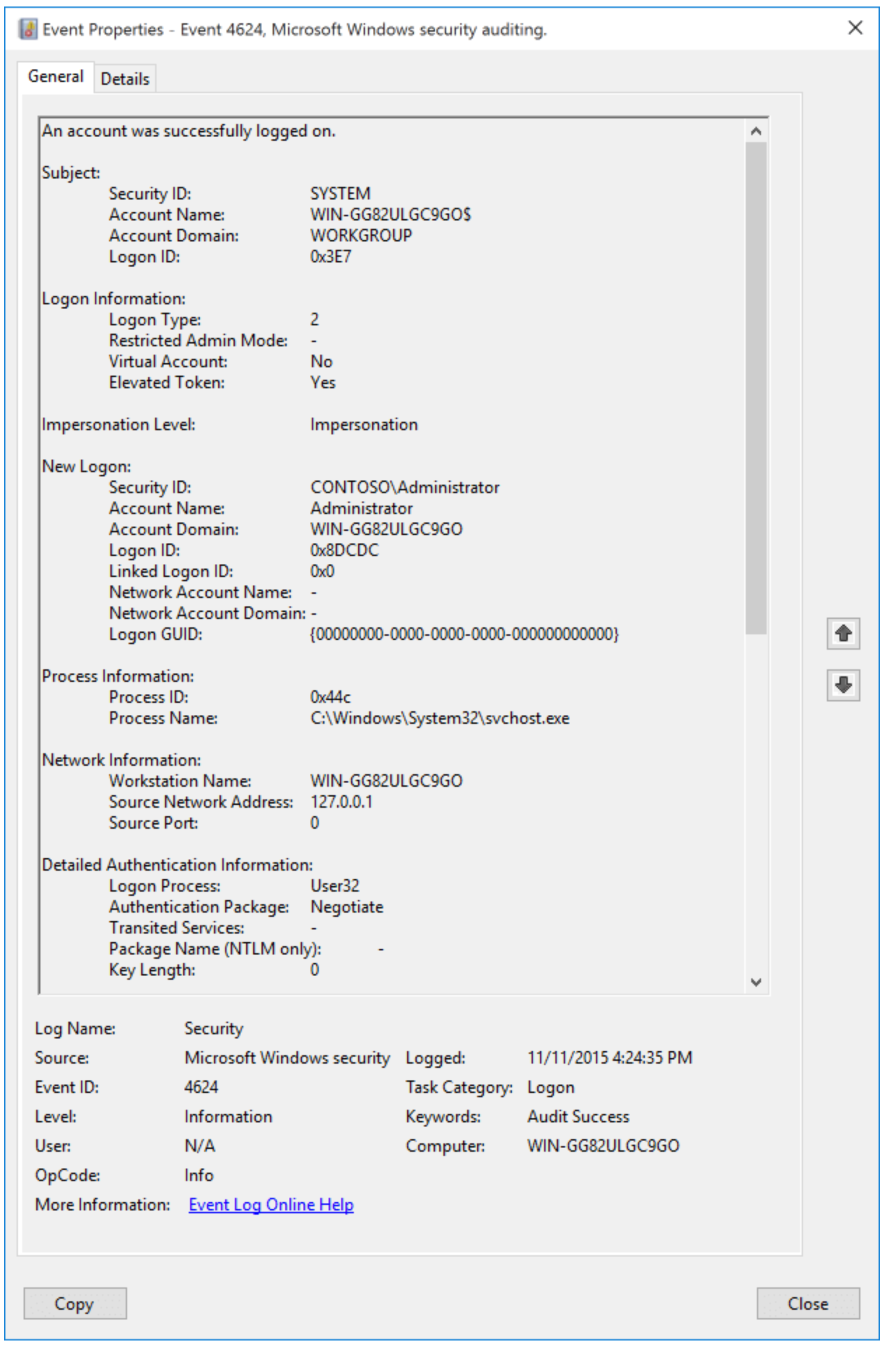
Filter by title

… / Advanced security auditing FAQ / Audit Logon /

4624(S): An account was successfully logged on.

Article • 09/07/2021 • 1 contributor

In this article


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               WIN-GG82ULGC9GO$
        Account Domain:             WORKGROUP
        Logon ID:                   0x3E7

Logon Information:
        Logon Type:                 2
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                CONTOSO\Administrator
        Account Name:               Administrator
        Account Domain:             WIN-GG82ULGC9GO
        Logon ID:                   0x8DCDC
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x44c
        Process Name:               C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:           WIN-GG82ULGC9GO
        Source Network Address:     127.0.0.1
        Source Port:                0

Detailed Authentication Information:
        Logon Process:              User32
        Authentication Package:     Negotiate
        Transited Services:         -
        Package Name (NTLM only):           -
        Key Length:                 0
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/11/2015 4:24:35 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-GG82ULGC9GO
OpCode:	Info		
More Information:	Event Log Online Help		

Subcategory: Audit Logon

Event Description:

This event generates when a logon session is created (on destination machine). It generates on the computer that was accessed, where the session was created.

> ⓘ Note
>
> For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

XML Copy

```xml
<?xml version="1.0"?>
<Event
    xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    <System>
        <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-547
        <EventID>4624</EventID>
        <Version>2</Version>
        <Level>0</Level>
        <Task>12544</Task>
        <Opcode>0</Opcode>
        <Keywords>0x8020000000000000</Keywords>
        <TimeCreated SystemTime="2015-11-12T00:24:35.079785200Z"/>
        <EventRecordID>211</EventRecordID>
        <Correlation ActivityID="{00D66690-1CDF-0000-AC66-D600DF1CD101}"/>
        <Execution ProcessID="716" ThreadID="760"/>
        <Channel>Security</Channel>
        <Computer>WIN-GG82ULGC9GO</Computer>
        <Security/>
    </System>
    <EventData>
        <Data Name="SubjectUserSid">S-1-5-18</Data>
        <Data Name="SubjectUserName">WIN-GG82ULGC9GO$</Data>
        <Data Name="SubjectDomainName">WORKGROUP</Data>
        <Data Name="SubjectLogonId">0x3e7</Data>
        <Data Name="TargetUserSid">S-1-5-21-1377283216-344919071-3415362939-500<
        <Data Name="TargetUserName">Administrator</Data>
        <Data Name="TargetDomainName">WIN-GG82ULGC9GO</Data>
        <Data Name="TargetLogonId">0x8dcdc</Data>
        <Data Name="LogonType">2</Data>
        <Data Name="LogonProcessName">User32</Data>
        <Data Name="AuthenticationPackageName">Negotiate</Data>
        <Data Name="WorkstationName">WIN-GG82ULGC9GO</Data>
        <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
        <Data Name="TransmittedServices">-</Data>
        <Data Name="LmPackageName">-</Data>
        <Data Name="KeyLength">0</Data>
        <Data Name="ProcessId">0x44c</Data>
        <Data Name="ProcessName">C:\\Windows\\System32\\svchost.exe</Data>
        <Data Name="IpAddress">127.0.0.1</Data>
        <Data Name="IpPort">0</Data>
        <Data Name="ImpersonationLevel">%%1833</Data>
        <Data Name="RestrictedAdminMode">-</Data>
        <Data Name="TargetOutboundUserName">-</Data>
        <Data Name="TargetOutboundDomainName">-</Data>
        <Data Name="VirtualAccount">%%1843</Data>
        <Data Name="TargetLinkedLogonId">0x0</Data>
        <Data Name="ElevatedToken">%%1842</Data>
    </EventData>
</Event>
```

Required Server Roles: None.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions:

- 0 - Windows Server 2008, Windows Vista.

- 1 - Windows Server 2012, Windows 8.
  - Added "Impersonation Level" field.
- 2 - Windows 10.
  - Added "Logon Information:" section.
  - **Logon Type** moved to "Logon Information:" section.
  - Added "Restricted Admin Mode" field.
  - Added "Virtual Account" field.
  - Added "Elevated Token" field.
  - Added "Linked Logon ID" field.
  - Added "Network Account Name" field.
  - Added "Network Account Domain" field.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]**:** SID of account that reported information about successful logon or invokes it. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID can't be resolved, you'll see the source data in the event.

  This field can also contain no subject user information, but the NULL Sid "S-1-0-0" and no user or domain information.

  > ⓘ Note
  >
  > A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it can't ever be used again to identify another user or group. For more information about SIDs, see **Security identifiers**.

- **Account Name** [Type = UnicodeString]**:** the name of the account that reported information about successful logon.
- **Account Domain** [Type = UnicodeString]**:** subject's domain or computer name. Formats vary, and include the following information:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "NT AUTHORITY".
  - For local user accounts, this field contains the name of the computer or device that this account belongs to, for example: `Win81`.
- **Logon ID** [Type = HexInt64]**:** hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, "4672(S): Special privileges assigned to new logon."

Logon Information [Version 2]**:**

- **Logon Type** [Version 0, 1, 2] [Type = UInt32]**:** the type of logon that happened. The following table contains the list of possible values for this field.

Logon types and descriptions

Expand table

Logon Type	Logon Title	Description
`0`	`System`	Used only by the System account, for example at system startup.
`2`	`Interactive`	A user logged on to this computer.
`3`	`Network`	A user or computer logged on to this computer from the network.
`4`	`Batch`	Batch logon type is used by batch servers, where processes can be run on behalf of a user without their direct intervention.
`5`	`Service`	The Service Control Manager started a service.
`7`	`Unlock`	This workstation was unlocked.
`8`	`NetworkCleartext`	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials don't traverse the network in plaintext (also called cleartext).
`9`	`NewCredentials`	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
`10`	`RemoteInteractive`	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
`11`	`CachedInteractive`	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller wasn't contacted to verify the credentials.
`12`	`CachedRemoteInteractive`	Same as RemoteInteractive. This type is used for internal auditing.
`13`	`CachedUnlock`	Workstation logon.

- **Restricted Admin Mode** [Version 2] [Type = UnicodeString]**:** Only populated for **RemoteInteractive** logon type sessions. This value is a Yes/No flag indicating if the credentials provided were passed using Restricted Admin mode. Restricted Admin mode was added in Windows 8.1 and Windows Server 2012 R2, but this flag was added to the event in Windows 10.

  Reference: https://blogs.technet.com/b/kfalde/archive/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2.aspx.

  If not a **RemoteInteractive** logon, then this value is the string: `-`

- **Virtual Account** [Version 2] [Type = UnicodeString]**:** a "Yes" or "No" flag, which indicates if the account is a virtual account (for example, "Managed Service Account"), which was introduced in Windows 7 and Windows Server 2008 R2 to identify the account that a given Service uses, instead of just using "NetworkService".

- **Elevated Token** [Version 2] [Type = UnicodeString]**:** a "Yes" or "No" flag. If "Yes", then the session this event represents is elevated and has administrator privileges.

Impersonation Level [Version 1, 2] [Type = UnicodeString]: can have one of these four values:

- SecurityAnonymous (displayed as **empty string**): The server process can't obtain identification information about the client, and it can't impersonate the client. It's defined with no value given, and thus, by ANSI C rules, defaults to a value of zero.
- SecurityIdentification (displayed as "**Identification**"): The server process can obtain information about the client, such as security identifiers and privileges, but it can't impersonate the client. This value is useful for servers that export their own objects, for example, database products that export tables and views. Using the retrieved client-security information, the server can make access-validation decisions without being able to use other services that are using the client's security context.
- SecurityImpersonation (displayed as "**Impersonation**"): The server process can impersonate the client's security context on its local system. The server can't impersonate the client on remote systems. This type is the most common.
- SecurityDelegation (displayed as "**Delegation**"): The server process can impersonate the client's security context on remote systems.

New Logon:

- **Security ID** [Type = SID]**:** SID of account for which logon was performed. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID can't be resolved, you'll see the source data in the event.

  > Note
  >
  > A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it cannot ever be used again to identify another user or group. For more information about SIDs, see **Security identifiers**.

- **Account Name** [Type = UnicodeString]**:** the name of the account for which logon was performed.
- **Account Domain** [Type = UnicodeString]**:** subject's domain or computer name. Formats vary, and include the following information:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "NT AUTHORITY".
  - For local user accounts, this field contains the name of the computer or device that this account belongs to, for example: `Win81`.
- **Logon ID** [Type = HexInt64]**:** hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, "4672(S): Special privileges assigned to new logon."

- **Linked Logon ID** [Version 2] [Type = HexInt64]**:** A hexadecimal value of the paired logon session. If there's no other logon session associated with this logon session, then the value is "**0x0**".

- **Network Account Name** [Version 2] [Type = UnicodeString]**:** User name that's used for outbound (network) connections. Valid only for NewCredentials logon type.

  If not **NewCredentials** logon, then this value will be the string: `-`

- **Network Account Domain** [Version 2] [Type = UnicodeString]**:** Domain for the user that's used for outbound (network) connections. Valid only for NewCredentials logon type.

  If not **NewCredentials** logon, then this value will be the string: `-`

- **Logon GUID** [Type = GUID]: a GUID that can help you correlate this event with another event that can contain the same **Logon GUID**, "4769(S, F): A Kerberos service ticket was requested event on a domain controller.

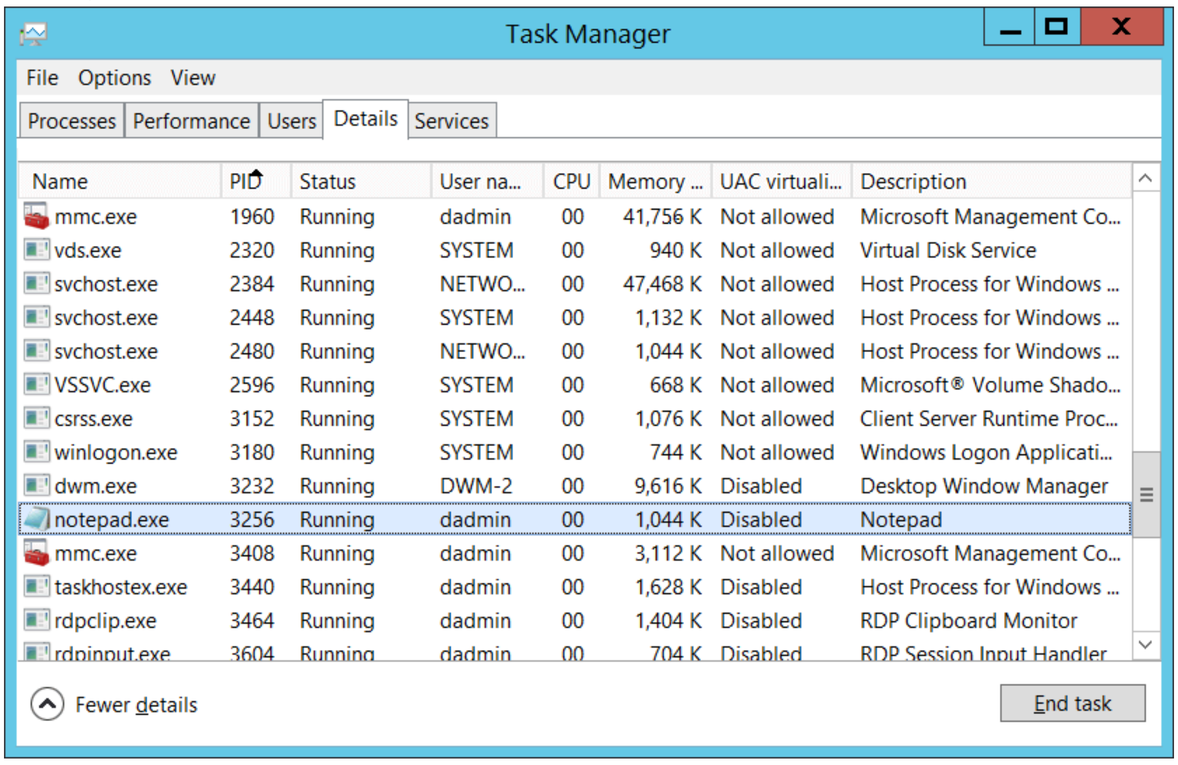
  It also can be used for correlation between a 4624 event and several other events (on the same computer) that can contain the same **Logon GUID**, "4648(S): A logon was attempted using explicit credentials" and "4964(S): Special groups have been assigned to a new logon."

  This parameter might not be captured in the event, and in that case appears as "{00000000-0000-0000-0000-000000000000}".

  > ⓘ Note
  >
  > **GUID** is an acronym for 'Globally Unique Identifier'. It is a 128-bit integer number used to identify resources, activities, or instances.

Process Information:

- **Process ID** [Type = Pointer]: hexadecimal Process ID of the process that attempted the logon. Process ID (PID) is a number used by the operating system to uniquely identify an active process. To see the PID for a specific process you can, for example, use Task Manager (Details tab, PID column):



Name	PID	Status	User na...	CPU	Memory ...	UAC virtuali...	Description
mmc.exe	1960	Running	dadmin	00	41,756 K	Not allowed	Microsoft Management Co...
vds.exe	2320	Running	SYSTEM	00	940 K	Not allowed	Virtual Disk Service
svchost.exe	2384	Running	NETWO...	00	47,468 K	Not allowed	Host Process for Windows ...
svchost.exe	2448	Running	SYSTEM	00	1,132 K	Not allowed	Host Process for Windows ...
svchost.exe	2480	Running	NETWO...	00	1,044 K	Not allowed	Host Process for Windows ...
VSSVC.exe	2596	Running	SYSTEM	00	668 K	Not allowed	Microsoft® Volume Shado...
csrss.exe	3152	Running	SYSTEM	00	1,076 K	Not allowed	Client Server Runtime Proc...
winlogon.exe	3180	Running	SYSTEM	00	744 K	Not allowed	Windows Logon Applicati...
dwm.exe	3232	Running	DWM-2	00	9,616 K	Disabled	Desktop Window Manager
notepad.exe	3256	Running	dadmin	00	1,044 K	Disabled	Notepad
mmc.exe	3408	Running	dadmin	00	3,112 K	Not allowed	Microsoft Management Co...
taskhostex.exe	3440	Running	dadmin	00	1,628 K	Disabled	Host Process for Windows ...
rdpclip.exe	3464	Running	dadmin	00	1,404 K	Disabled	RDP Clipboard Monitor
rdpinput.exe	3604	Running	dadmin	00	704 K	Disabled	RDP Session Input Handler

  If you convert the hexadecimal value to decimal, you can compare it to the values in Task Manager.

  You can also correlate this process ID with a process ID in other events, for example, "4688: A new process has been created" **Process Information\New Process ID**.

- **Process Name** [Type = UnicodeString]**:** full path and the name of the executable for the process.

Network Information:

- **Workstation Name** [Type = UnicodeString]**:** machine name from which a logon attempt was performed.
- **Source Network Address** [Type = UnicodeString]**:** IP address of machine from which logon attempt was performed.
  - IPv6 address or IPv4 address of a client.
  - `::1` or `127.0.0.1` means localhost.
- **Source Port** [Type = UnicodeString]: The source port that was used for logon attempt from remote machine.
  - 0 for interactive logons.

> ⓘ **Note**
>
> The fields for IP address/port and workstation name are populated depending on the authentication context and protocol used. LSASS will audit the information the authenticating service shares with LSASS. For example, network logons with Kerberos likely have no workstation information, and NTLM logons have no TCP/IP details.

Detailed Authentication Information:

- **Logon Process** [Type = UnicodeString]**:** the name of the trusted logon process that was used for the logon. See event "4611: A trusted logon process has been registered with the Local Security Authority" description for more information.
- **Authentication Package** [Type = UnicodeString]**:** The name of the authentication package that was used for the logon authentication process. Default packages loaded on LSA startup are located in "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig" registry key. Other packages can be loaded at runtime. When a new package is loaded a "4610: An authentication package has been loaded by the Local Security Authority" (typically for NTLM) or "4622: A security package has been loaded by the Local Security Authority" (typically for Kerberos) event is logged to indicate that a new package has been loaded along with the package name. The most common authentication packages are:
  - **NTLM** - NTLM-family Authentication
  - **Kerberos** - Kerberos authentication.
  - **Negotiate** - the Negotiate security package selects between Kerberos and NTLM protocols. Negotiate selects Kerberos unless it can't be used by one of the systems involved in the authentication or the calling application didn't provide sufficient information to use Kerberos.
- **Transited Services** [Type = UnicodeString] [Kerberos-only]**:** the list of transmitted services. Transmitted services are populated if the logon was a result of a S4U (Service For User) logon process. S4U is a Microsoft extension to the Kerberos Protocol to allow an application service to obtain a Kerberos service ticket on behalf of a user - most commonly done by a front-end website to access an internal resource on behalf of a user. For more information about S4U, see https://msdn.microsoft.com/library/cc246072.aspx
- **Package Name (NTLM only)** [Type = UnicodeString]**:** The name of the LAN Manager subpackage (NTLM-family protocol name) that was used during logon. Possible values are:
  - "NTLM V1"
  - "NTLM V2"

    - "LM"

      Only populated if "**Authentication Package**" = "**NTLM**".

- **Key Length** [Type = UInt32]**:** the length of NTLM Session Security key. Typically it has 128-bit or 56-bit length. This parameter is always 0 if "**Authentication Package**" = "**Kerberos**", because it isn't applicable for Kerberos protocol. This field also has a `0` value if Kerberos was negotiated using **Negotiate** authentication package.

Security Monitoring Recommendations

For 4624(S): An account was successfully logged on.

Expand table

Type of monitoring required	**Recommendation**
High-value accounts: You might have high-value domain or local accounts for which you need to monitor each action. Examples of high-value accounts are database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts and so on.	Monitor this event with the **"New Logon\Security ID"** that corresponds to the high-value account or accounts.
Anomalies or malicious actions: You might have specific requirements for detecting anomalies or monitoring potential malicious actions. For example, you might need to monitor for use of an account outside of working hours.	When you monitor for anomalies or malicious actions, use the **"New Logon\Security ID"** (with other information) to monitor how or when a particular account is being used.
Non-active accounts: You might have nonactive, disabled, or guest accounts, or other accounts that should never be used.	Monitor this event with the **"New Logon\Security ID"** that corresponds to the accounts that should never be used.
Account allowlist: You might have a specific allowlist of accounts that are the only ones allowed to perform actions corresponding to particular events.	If this event corresponds to an "allowlist-only" action, review the **"New Logon\Security ID"** for accounts that are outside the allowlist.
Accounts of different types: Make sure that certain actions run only by certain account types. For example, local or domain account, machine or user account, or vendor or employee account.	If this event corresponds to an action you want to monitor for certain account types, review the **"New Logon\Security ID"** to see whether the account type is as expected.
External accounts: You might be monitoring accounts from another domain, or "external" accounts that aren't allowed to perform certain actions (represented by certain specific events).	Monitor this event for the **"Subject\Account Domain"** corresponding to accounts from another domain or "external" accounts.
Restricted-use computers or devices: You might have certain computers, machines, or devices on which certain people (accounts) shouldn't typically perform any actions.	Monitor the target **Computer:** (or other target device) for actions performed by the **"New Logon\Security ID"** that you're concerned about.
Account naming conventions: Your organization might have specific naming conventions for account names.	Monitor "**Subject\Account Name**" for names that don't comply with naming conventions.

- Because this event is typically triggered by the SYSTEM account, we recommend that you report it whenever **"Subject\Security ID"** isn't SYSTEM.

- If "**Restricted Admin**" mode must be used for logons by certain accounts, use this event to monitor logons by "**New Logon\Security ID**" in relation to "**Logon Type**"=10 and "**Restricted Admin Mode**"="Yes". If "**Restricted Admin Mode**"="No" for these accounts, trigger an alert.

- If you need to monitor all logon events for accounts with administrator privileges, monitor this event with "**Elevated Token**"="Yes".

- If you need to monitor all logon events for managed service accounts and group managed service accounts, monitor for events with "**Virtual Account**"="Yes".
- To monitor for a mismatch between the logon type and the account that uses it (for example, if **Logon Type** 4-Batch or 5-Service is used by a member of a domain administrative group), monitor **Logon Type** in this event.
- If your organization restricts logons in the following ways, you can use this event to monitor accordingly:
  - If the user account **"New Logon\Security ID"** should never be used to log on from the specific **Computer:**.
  - If **New Logon\Security ID** credentials shouldn't be used from **Workstation Name** or **Source Network Address**.
  - If a specific account, such as a service account, should only be used from your internal IP address list (or some other list of IP addresses). In this case, you can monitor for **Network Information\Source Network Address** and compare the network address with your list of IP addresses.
  - If a particular version of NTLM is always used in your organization. In this case, you can use this event to monitor **Package Name (NTLM only)**, for example, to find events where **Package Name (NTLM only)** doesn't equal **NTLM V2**.
  - If NTLM isn't used in your organization, or shouldn't be used by a specific account (**New Logon\Security ID**). In this case, monitor for all events where **Authentication Package** is NTLM.
  - If the **Authentication Package** is NTLM. In this case, monitor for **Key Length** not equal to 128, because all Windows operating systems starting with Windows 2000 support 128-bit Key Length.
- If you monitor for potentially malicious software, or software that isn't authorized to request logon actions, monitor this event for **Process Name**.
- If you have a trusted logon processes list, monitor for a **Logon Process** that isn't from the list.