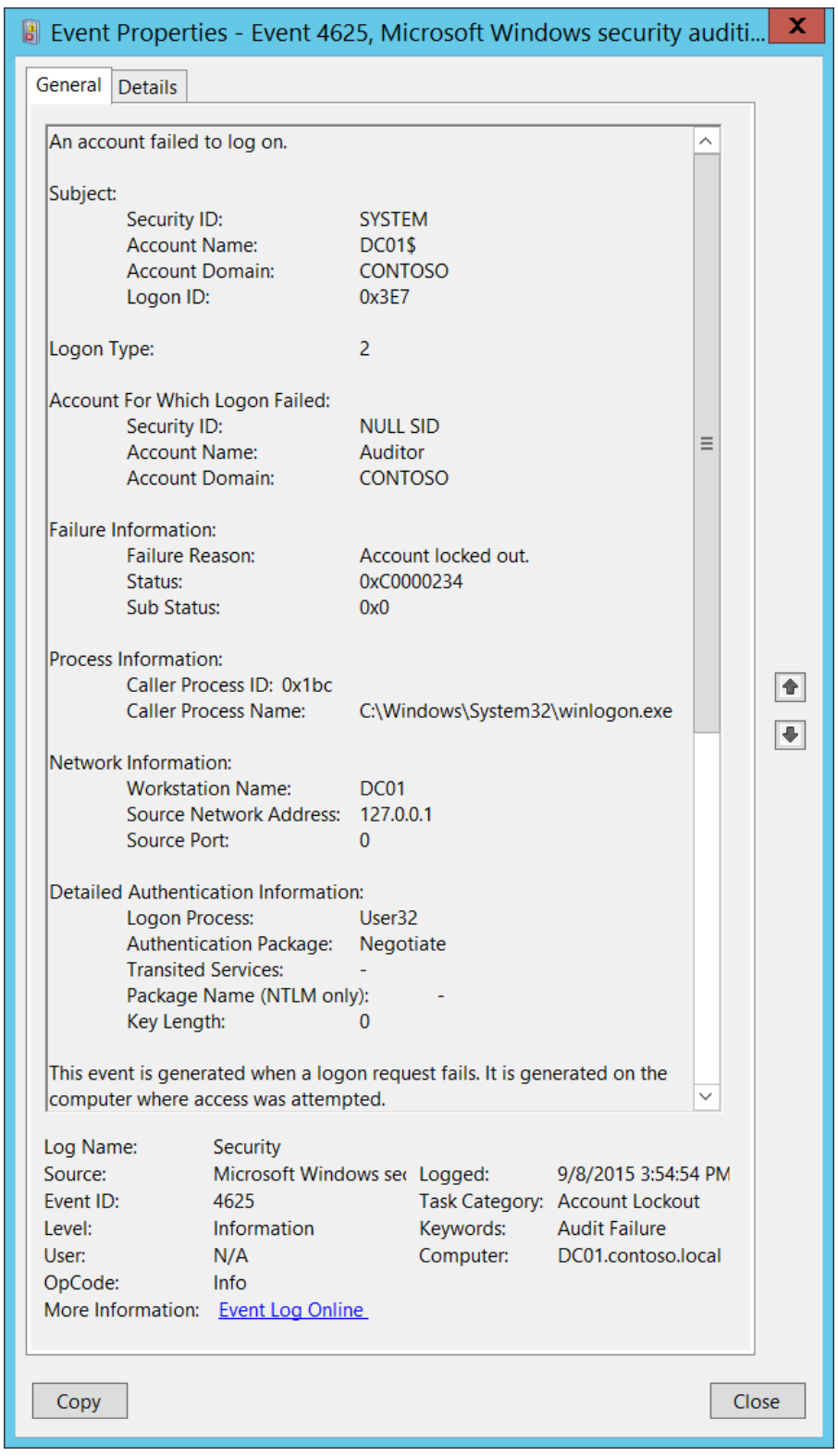
4625(F): An account failed to log on.

Article • 01/03/2022 • 1 contributor



Subcategories: Audit Account Lockout and Audit Logon

Event Description:

This event is logged for any logon failure.

Other Events

Appendix A: Security monitoring recommendations for many audit

It generates on the computer where logon attempt was made, for example, if logon attempt was made on user's workstation, then event will be logged on this workstation.

This event generates on domain controllers, member servers, and workstations.

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

Event XML:

XML Copy

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-
 <EventID>4625</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12546</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8010000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-08T22:54:54.962511700Z" />
 <EventRecordID>229977</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="3240" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-18</Data>
 <Data Name="SubjectUserName">DC01$</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x3e7</Data>
 <Data Name="TargetUserSid">S-1-0-0</Data>
 <Data Name="TargetUserName">Auditor</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="Status">0xc0000234</Data>
 <Data Name="FailureReason">%%2307</Data>
 <Data Name="SubStatus">0x0</Data>
 <Data Name="LogonType">2</Data>
 <Data Name="LogonProcessName">User32</Data>
 <Data Name="AuthenticationPackageName">Negotiate</Data>
 <Data Name="WorkstationName">DC01</Data>
 <Data Name="TransmittedServices">-</Data>
 <Data Name="LmPackageName">-</Data>
 <Data Name="KeyLength">0</Data>
 <Data Name="ProcessId">0x1bc</Data>
 <Data Name="ProcessName">C:\\Windows\\System32\\winlogon.exe</Data>
 <Data Name="IpAddress">127.0.0.1</Data>
 <Data Name="IpPort">0</Data>
 </EventData>
 </Event>
```

Required Server Roles: None.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions: 0.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]: SID of account that reported information about logon failure. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will 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 that reported information about logon failure.
- **Account Domain** [Type = UnicodeString]: subject's domain or computer name. Here are some examples of formats:
  - 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 will contain the name of the computer or device that this account belongs to, for example: "Win81".
- **Logon Type** [Type = UInt32]: the type of logon that was performed. "Table 11. Windows Logon Types" contains the list of possible values for this field.

Table 11: Windows Logon Types

Expand table

Logon Type	Logon Title	Description
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 may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
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 do not 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 was not contacted to verify the credentials.

Account For Which Logon Failed:

- **Security ID** [Type = SID]: SID of the account that was specified in the logon attempt. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will 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 that was specified in the logon attempt.
- **Account Domain** [Type = UnicodeString]: domain or computer name. Here are some examples of formats:
  - 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 will contain 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, "4624: An account was successfully logged on."

Failure Information:

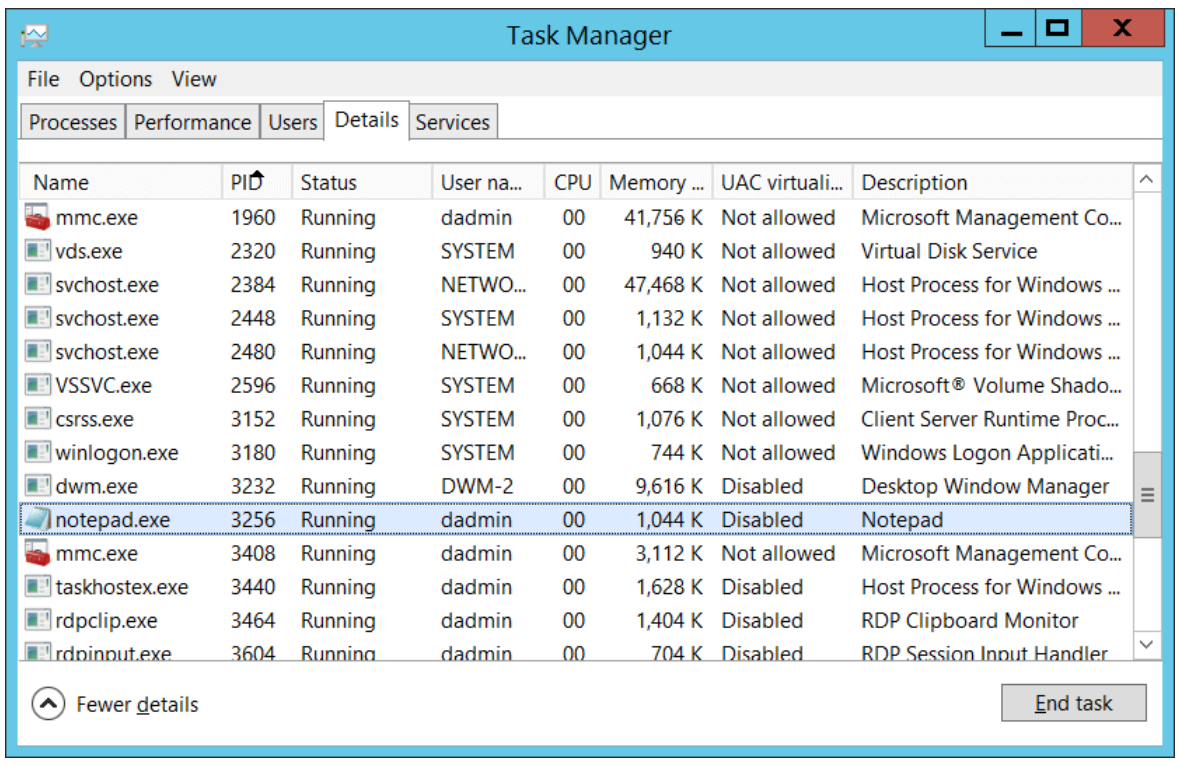
- **Failure Reason** [Type = UnicodeString]: textual explanation of **Status** field value. For this event, it typically has "**Account locked out**" value.
- **Status** [Type = HexInt32]: the reason why logon failed. For this event, it typically has "**0xC0000234**" value.
- **Sub Status** [Type = HexInt32]: additional information about logon failure.

> **Note**
>
> For more information about various Status or Sub Status codes, see NTSTATUS Values.

Process Information:

- **Caller 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):



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**.

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

Detailed Authentication Information:

- **Logon Process** [Type = UnicodeString]**:** the name of the trusted logon process that was used for the logon attempt. 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 cannot be used by one of the systems involved in the authentication or the calling application did not 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 the logon attempt. 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 a length of 128 bits or 56 bits. This parameter is always 0 if "**Authentication Package**" = "**Kerberos**", because it is not applicable for Kerberos protocol. This field will also have "0" value if Kerberos was negotiated using **Negotiate** authentication package.

Security Monitoring Recommendations

For 4625(F): An account failed to log on.

> ⓘ **Important**
>
> For this event, also see **Appendix A: Security monitoring recommendations for many audit events**.

- If you have a pre-defined "**Process Name**" for the process reported in this event, monitor all events with "**Process Name**" not equal to your defined value.

- You can monitor to see if "**Process Name**" is not in a standard folder (for example, not in **System32** or **Program Files**) or is in a restricted folder (for example, **Temporary Internet Files**).

- If you have a pre-defined list of restricted substrings or words in process names (for example, "**mimikatz**" or "**cain.exe**"), check for these substrings in "**Process Name**."

- If **Subject\Account Name** is a name of service account or user account, it may be useful to investigate whether that account is allowed (or expected) to request logon for **Account For Which Logon Failed\Security ID**.

- 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 you have a high-value domain or local account for which you need to monitor every lockout, monitor all 4625 events with the "**Subject\Security ID**" that corresponds to the account.

- We recommend monitoring all 4625 events for local accounts, because these accounts typically should not be locked out. Monitoring is especially relevant for critical servers,

administrative workstations, and other high-value assets.

- We recommend monitoring all 4625 events for service accounts, because these accounts should not be locked out or prevented from functioning. Monitoring is especially relevant for critical servers, administrative workstations, and other high value assets.
- If your organization restricts logons in the following ways, you can use this event to monitor accordingly:
  - If the **"Account For Which Logon Failed \Security ID"** should never be used to log on from the specific **Network Information\Workstation Name**.
  - 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)** does not equal **NTLM V2**.
  - If NTLM is not used in your organization, or should not 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 **Logon Process** is not from a trusted logon processes list.
- Monitor for all events with the fields and values in the following table:

Expand table

Field	Value to monitor for
Failure Information\Status or **Failure Information\Sub Status**	0XC000005E – "There are currently no logon servers available to service the logon request." This issue is typically not a security issue, but it can be an infrastructure or availability issue.
Failure Information\Status or **Failure Information\Sub Status**	0xC0000064 – "User logon with misspelled or bad user account". Especially if you get several of these events in a row, it can be a sign of a user enumeration attack.
Failure Information\Status or **Failure Information\Sub Status**	0xC000006A – "User logon with misspelled or bad password" for critical accounts or service accounts. Especially watch for a number of such events in a row.
Failure Information\Status or **Failure Information\Sub Status**	0XC000006D – "This is either due to a bad username or authentication information" for critical accounts or service accounts. Especially watch for a number of such events in a row.
Failure Information\Status or **Failure Information\Sub Status**	0xC000006F – "User logon outside authorized hours".

Failure Information\Status or **Failure Information\Sub Status**	0xC0000070 – "User logon from unauthorized workstation".
Failure Information\Status or **Failure Information\Sub Status**	0xC0000072 – "User logon to account disabled by administrator".
Failure Information\Status or **Failure Information\Sub Status**	0XC000015B – "The user has not been granted the requested logon type (aka logon right) at this machine".
Failure Information\Status or **Failure Information\Sub Status**	0XC0000192 – "An attempt was made to logon, but the Netlogon service was not started". This issue is typically not a security issue but it can be an infrastructure or availability issue.
Failure Information\Status or **Failure Information\Sub Status**	0xC0000193 – "User logon with expired account".
Failure Information\Status or **Failure Information\Sub Status**	0XC0000413 – "Logon Failure: The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine".