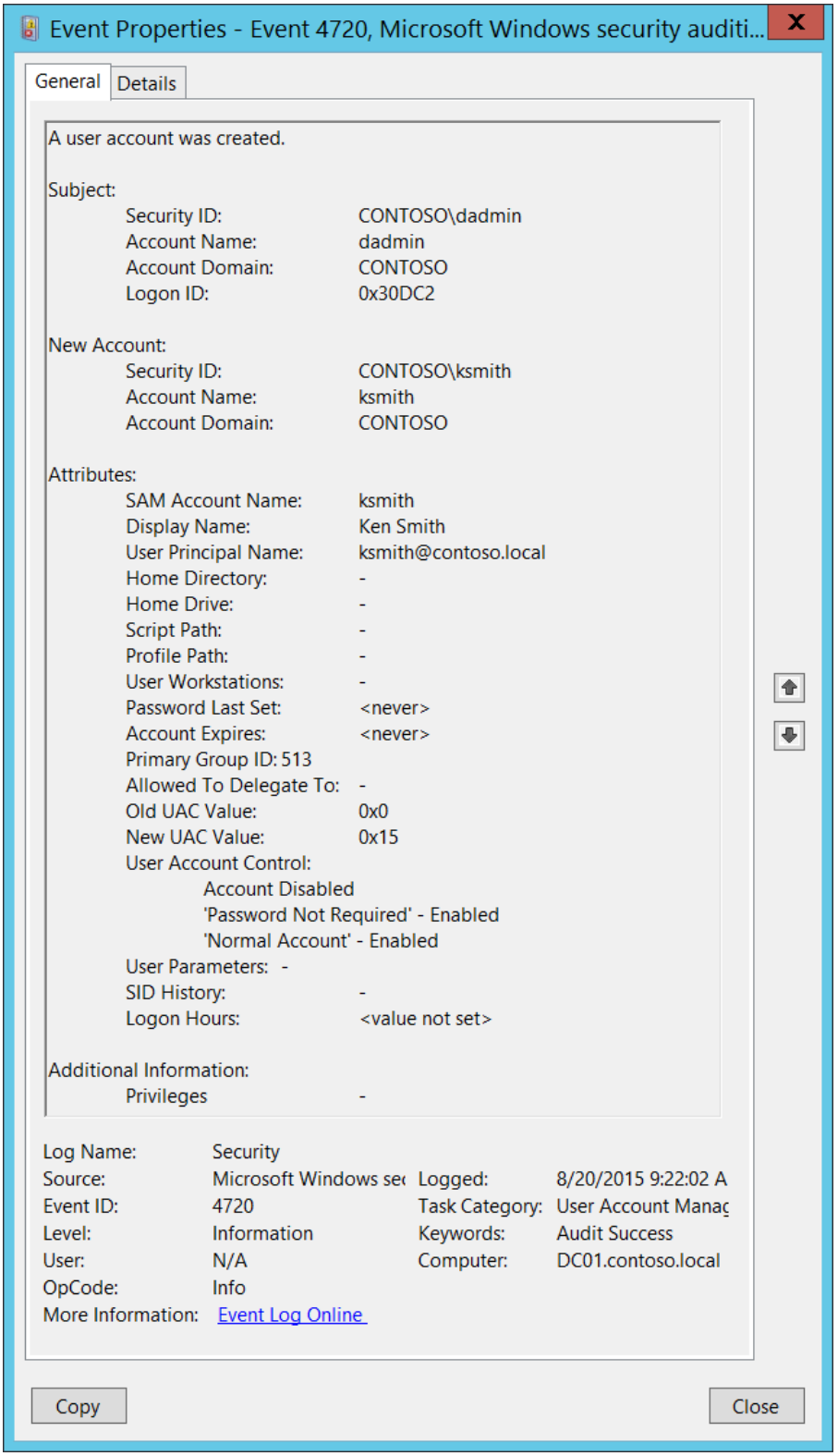
4720(S) A user account was created. - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 19:41:35 UTC



Subcategory: Audit User Account Management

Event Description:

This event generates every time a new user object is created.

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

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

Event XML:

```
 - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4720</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>13824</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-08-20T16:22:02.759912000Z" />
 <EventRecordID>175408</EventRecordID>
 <Correlation />
 <Execution ProcessID="520" ThreadID="1508" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="TargetUserName">ksmith</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="TargetSid">S-1-5-21-3457937927-2839227994-823803824-6609</Data>
 <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x30dc2</Data>
 <Data Name="PrivilegeList">-</Data>
 <Data Name="SamAccountName">ksmith</Data>
 <Data Name="DisplayName">Ken Smith</Data>
 <Data Name="UserPrincipalName">ksmith@contoso.local</Data>
 <Data Name="HomeDirectory">-</Data>
 <Data Name="HomePath">-</Data>
 <Data Name="ScriptPath">-</Data>
 <Data Name="ProfilePath">-</Data>
 <Data Name="UserWorkstations">-</Data>
 <Data Name="PasswordLastSet">%%1794</Data>
 <Data Name="AccountExpires">%%1794</Data>
 <Data Name="PrimaryGroupId">513</Data>
 <Data Name="AllowedToDelegateTo">-</Data>
 <Data Name="OldUacValue">0x0</Data>
 <Data Name="NewUacValue">0x15</Data>
 <Data Name="UserAccountControl">%%2080 %%2082 %%2084</Data>
 <Data Name="UserParameters">-</Data>
 <Data Name="SidHistory">-</Data>
```

```
<Data Name="LogonHours">%%1793</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 requested the “create user account” operation. 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 requested the “create user account” operation.
- **Account Domain** [Type = UnicodeString]**:** subject’s domain or computer name. Formats vary, and include the following:
  - 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.”

New Account:

- **Security ID** [Type = SID]**:** SID of created user account. 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.
- **Account Name** [Type = UnicodeString]**:** the name of the user account that was created. For example: dadmin.
- **Account Domain** [Type = UnicodeString]**:** domain name of created user account. Formats vary, and include the following:
    - Domain NETBIOS name example: CONTOSO
    - Lowercase full domain name: contoso.local
    - Uppercase full domain name: CONTOSO.LOCAL
    - For local accounts, this field will contain the name of the computer to which this new account belongs, for example: “Win81”.

Attributes:

- **SAM Account Name** [Type = UnicodeString]: logon name for account used to support clients and servers from previous versions of Windows (pre-Windows 2000 logon name). The value of **sAMAccountName** attribute of new user object. For example: ksmith. For local account this field contains the name of new user account.
- **Display Name** [Type = UnicodeString]: the value of **displayName** attribute of new user object. It is a name displayed in the address book for a particular account .This is usually the combination of the user's first name, middle initial, and last name. For example, Ken Smith. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. Local accounts contain **Full Name** attribute in this field, but for new local accounts this field typically has value “**<value not set>**”.
- **User Principal Name** [Type = UnicodeString]: internet-style login name for the account, based on the Internet standard RFC 822. By convention this should map to the account's email name. This parameter contains the value of **userPrincipalName** attribute of new user object. For example, ksmith@contoso.local. For local users this field is not applicable and has value “**-**“. You can change this attribute by using Active Directory Users and Computers, or through a script, for example.
- **Home Directory** [Type = UnicodeString]: user's home directory. If **homeDrive** attribute is set and specifies a drive letter, **homeDirectory** should be a UNC path. The path must be a network UNC of the form \\Server\Share\Directory. This parameter contains the value of **homeDirectory** attribute of new user object. For new local accounts this field typically has value “**<value not set>**”. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as “**-**”.
- **Home Drive** [Type = UnicodeString]**:** specifies the drive letter to which to map the UNC path specified by **homeDirectory** account’s attribute. The drive letter must be specified in the form “DRIVE_LETTER:”. For example – “H:”. This parameter contains the value of **homeDrive** attribute of new user object. You can

change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as "-". For new local accounts this field typically has value "**<value not set>**".

- **Script Path** [Type = UnicodeString]**:** specifies the path of the account's logon script. This parameter contains the value of **scriptPath** attribute of new user object. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as "-". For new local accounts this field typically has value "**<value not set>**".

- **Profile Path** [Type = UnicodeString]: specifies a path to the account's profile. This value can be a null string, a local absolute path, or a UNC path. This parameter contains the value of **profilePath** attribute of new user object. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as "-". For new local accounts this field typically has value "**<value not set>**".

- **User Workstations** [Type = UnicodeString]: contains the list of NetBIOS or DNS names of the computers from which the user can logon. Each computer name is separated by a comma. The name of a computer is the **sAMAccountName** property of a user object. This parameter contains the value of **userWorkstations** attribute of new user object. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as "-". For local users this field is not applicable and typically has value "**<value not set>**".

- **Password Last Set** [Type = UnicodeString]**:** last time the account's password was modified. For manually created user account, using Active Directory Users and Computers snap-in, this field typically has value "**<never>"**. This parameter contains the value of **pwdLastSet** attribute of new user object.

- **Account Expires** [Type = UnicodeString]: the date when the account expires. This parameter contains the value of **accountExpires** attribute of new user object. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. This parameter might not be captured in the event, and in that case appears as "-". For manually created local and domain user accounts this field typically has value "**<never>**".

- **Primary Group ID** [Type = UnicodeString]: Relative Identifier (RID) of user's object primary group.

> **Note Relative identifier (RID)** is a variable length number that is assigned to objects at creation and becomes part of the object's Security Identifier (SID) that uniquely identifies an account or group within a domain.

Typically, **Primary Group** field for new user accounts has the following values:

- 513 (Domain Users. For local accounts this RID means Users) – for domain and local users.

  See this article </windows/security/identity-protection/access-control/security-identifiers> for more information. This parameter contains the value of **primaryGroupID** attribute of new user object.

- **Allowed To Delegate To** [Type = UnicodeString]: the list of SPNs to which this account can present delegated credentials. Can be changed using Active Directory Users and Computers management console in **Delegation** tab of user account, if this account has at least one SPN registered. This parameter contains the value of **AllowedToDelegateTo** attribute of new user object. For local user accounts this field is not applicable and typically has value "**-**". For new domain user accounts it is typically has value "**-**". See description of **AllowedToDelegateTo** field for "4738(S): A user account was changed." event for more details.

> **Note** **Service Principal Name (SPN)** is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. A given service instance can have multiple SPNs if there are multiple names that clients might use for authentication. For example, an SPN always includes the name of the host computer on which the service instance is running, so a service instance might register an SPN for each name or alias of its host.

- **Old UAC Value** [Type = UnicodeString]: is always "0x0" for new accounts.
- **New UAC Value** [Type = UnicodeString]: specifies flags that control password, lockout, disable/enable, script, and other behavior for the user or computer account. This parameter contains the value of the SAM implementation of account flags (definition differs from userAccountControl in AD). For a list of account flags you may see here, refer to [MS-SAMR]: USER_ACCOUNT Codes.
- **User Parameters** [Type = UnicodeString]: if you change any setting using Active Directory Users and Computers management console in Dial-in tab of user's account properties, then you will see **<value changed, but not displayed>** in this field in "4738: A user account was changed." This parameter might not be captured in the event, and in that case appears as "-". For new local accounts this field typically has value "**<value not set>**".
- **SID History** [Type = UnicodeString]: contains previous SIDs used for the object if the object was moved from another domain. Whenever an object is moved from one domain to another, a new SID is created and becomes the objectSID. The previous SID is added to the **sIDHistory** property. This parameter contains the value of **sIDHistory** attribute of new user object. This parameter might not be captured in the event, and in that case appears as "-".
- **Logon Hours** [Type = UnicodeString]: hours that the account is allowed to logon to the domain. The value of **logonHours** attribute of new user object. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. You will typically see "**<value not set>**" value for new manually created user accounts in event 4720. For new local accounts this field is not applicable and typically has value "**All**".

Additional Information:

- **Privileges** [Type = UnicodeString]: the list of user privileges which were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as "-". See full list of user privileges in "Table 8. User Privileges.".

Security Monitoring Recommendations

For 4720(S): A user account was created.

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

- Some organizations monitor every 4720 event.
- Consider whether to track the following fields and values:

Field and value to track	Reason to track
SAM Account Name is empty or -	This field must contain the user account name. If it is empty or -, it might indicate an anomaly.
User Principal Name is empty or -	Typically this field should not be empty for new user accounts. If it is empty or -, it might indicate an anomaly.
Home Directory is not - **Home Drive** is not - **Script Path** is not - **Profile Path** is not - **User Workstations** is not -	Typically these fields are - for new user accounts. Other values might indicate an anomaly and should be monitored. For local accounts these fields should display **<value not set>**.
Password Last Set is **<never>**	This typically means this is a manually created user account, which you might need to monitor.
Password Last Set is a time in the future	This might indicate an anomaly.
Account Expires is not **<never>**	Typically this field is **<never>** for new user accounts. Other values might indicate an anomaly and should be monitored.
Primary Group ID is not 513	Typically, the **Primary Group** value is 513 for domain and local users. Other values should be monitored.
Allowed To Delegate To is not -	Typically this field is - for new user accounts. Other values might indicate an anomaly and should be monitored.
Old UAC Value is not 0x0	Typically this field is **0x0** for new user accounts. Other values might indicate an anomaly and should be monitored.
SID History is not -	This field will always be set to - unless the account was migrated from another domain.
Logon Hours value other than **<value not set>** or** “All”**	This should always be **<value not set>** for new domain user accounts, and **“All”** for new local user accounts.

- Consider whether to track the following user account control flags:

User account control flag to track	**Information about the flag**
'Normal Account' – Disabled	Should not be disabled for user accounts.
'Encrypted Text Password Allowed' – Enabled **'Smartcard Required'** – Enabled **'Not Delegated'** – Enabled **'Use DES Key Only'** – Enabled **'Don't Require Preauth'** – Enabled **'Trusted To Authenticate For Delegation'** – Enabled	By default, these flags should not be enabled for new user accounts created with the “Active Directory Users and Computers” snap-in.
'Server Trust Account' – Enabled	Should never be enabled for user accounts. Applies only to domain controller (computer) accounts.
'Don't Expire Password' – Enabled	Should be monitored for critical accounts, or all accounts if your organization does not allow this flag. By default, this flag should not be enabled for new user accounts created with the “Active Directory Users and Computers” snap-in.
'Trusted For Delegation' – Enabled	By default, this flag should not be enabled for new user accounts created with the “Active Directory Users and Computers” snap-in. It is enabled by default only for new domain controllers.

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720