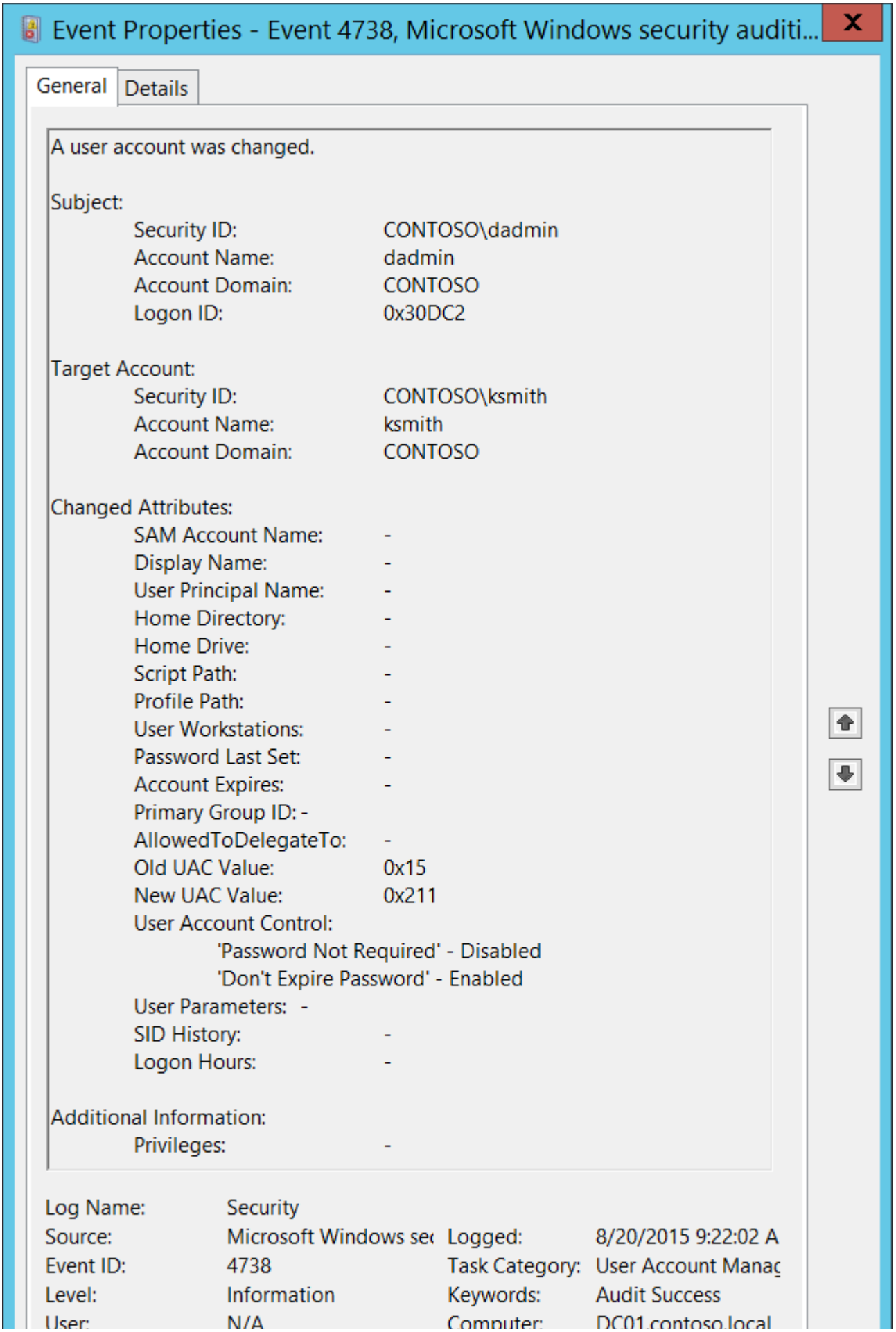
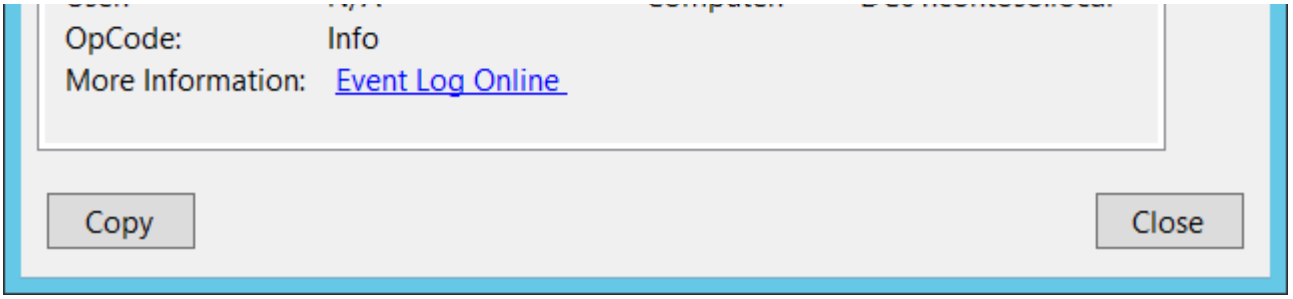
4738(S) A user account was changed. - Windows 10

By vinaypamnani-msft

Archived: 2026-04-06 00:45:37 UTC


Event Properties - Event 4738, Microsoft Windows security auditi...
General
Details
A user account was changed.
Subject:
Security ID: CONTOSO\dadmin
Account Name: dadmin
Account Domain: CONTOSO
Logon ID: 0x30DC2
Target Account:
Security ID: CONTOSO\ksmith
Account Name: ksmith
Account Domain: CONTOSO
Changed Attributes:
SAM Account Name: -
Display Name: -
User Principal Name: -
Home Directory: -
Home Drive: -
Script Path: -
Profile Path: -
User Workstations: -
Password Last Set: -
Account Expires: -
Primary Group ID: -
AllowedToDelegateTo: -
Old UAC Value: 0x15
New UAC Value: 0x211
User Account Control:
'Password Not Required' - Disabled
'Don't Expire Password' - Enabled
User Parameters: -
SID History: -
Logon Hours: -
Additional Information:
Privileges: -
Log Name: Security
Source: Microsoft Windows se
Logged: 8/20/2015 9:22:02 A
Event ID: 4738
Task Category: User Account Manag
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01.contoso.local



Subcategory: Audit User Account Management

Event Description:

This event generates every time user object is changed.

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

For each change, a separate 4738 event will be generated.

You might see this event without any changes inside, that is, where all **Changed Attributes** appear as `-`. This usually happens when a change is made to an attribute that is not listed in the event. In this case there is no way to determine which attribute was changed. For example, if the discretionary access control list (DACL) is changed, a 4738 event will generate, but all attributes will be `-`.

Some changes do not invoke a 4738 event.

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>4738</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>13824</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-08-20T16:22:02.792454100Z" />
 <EventRecordID>175413</EventRecordID>
 <Correlation />
 <Execution ProcessID="520" ThreadID="1508" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
```

```
- <EventData>
 <Data Name="Dummy">-</Data>
 <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">-</Data>
 <Data Name="DisplayName">-</Data>
 <Data Name="UserPrincipalName">-</Data>
 <Data Name="HomeDirectory">-</Data>
 <Data Name="HomePath">-</Data>
 <Data Name="ScriptPath">-</Data>
 <Data Name="ProfilePath">-</Data>
 <Data Name="UserWorkstations">-</Data>
 <Data Name="PasswordLastSet">-</Data>
 <Data Name="AccountExpires">-</Data>
 <Data Name="PrimaryGroupId">-</Data>
 <Data Name="AllowedToDelegateTo">-</Data>
 <Data Name="OldUacValue">0x15</Data>
 <Data Name="NewUacValue">0x211</Data>
 <Data Name="UserAccountControl">%%2050 %%2089</Data>
 <Data Name="UserParameters">-</Data>
 <Data Name="SidHistory">-</Data>
 <Data Name="LogonHours">-</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 “change 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 "change 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."

Target Account:

- **Security ID** [Type = SID]**:** SID of account that was changed. 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 account that was changed.
- **Account Domain** [Type = UnicodeString]**:** target account'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 local user accounts, this field will contain the name of the computer or device that this account belongs to, for example: "Win81".

Changed Attributes:

If attribute was not changed it will have “–“ value.

Unfortunately, for local accounts, all fields, except changed attributes, will have previous values populated. Also, the User Account Control field will have values only if it was modified. Changed attributes will have new values, but it is hard to understand which attribute was really changed.

- **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). If the value of **sAMAccountName** attribute of user object was changed, you will see the new value here. For example: ladmin. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **Display Name** [Type = UnicodeString]: 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. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. If the value of **displayName** attribute of user object was changed, you will see the new value here. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **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. If the value of **userPrincipalName** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field is not applicable and always has `-` value.

- **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. If the value of **homeDirectory** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **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:”. If the value of **homeDrive** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **Script Path** [Type = UnicodeString]**:** specifies the path of the account’s logon script. If the value of **scriptPath** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **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. If the value of **profilePath** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **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 computer object. If the value of **userWorkstations** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field is not applicable and always appears as `<value not set>`.

- **Password Last Set** [Type = UnicodeString]**:** last time the account's password was modified. If the value of **pwdLastSet** attribute of user object was changed, you will see the new value here. For example: 8/12/2015 11:41:39 AM. This value will be changed, for example, after manual user account password reset. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **Account Expires** [Type = UnicodeString]: the date when the account expires. If the value of **accountExpires** attribute of user object was changed, you will see the new value here. . For example, "9/21/2015 12:00:00 AM". You can change this attribute by using Active Directory Users and Computers, or through a script, for example. For local accounts, this field always has some value—if the account's attribute was not changed it will contain the current value of the attribute.

- **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.

This field will contain some value if user's object primary group was changed. You can change user's primary group using Active Directory Users and Computers management console in the **Member Of** tab of user object properties. You will see a RID of new primary group as a field value. For example, RID 513 (Domain Users) is a default primary group for users.

Typical **Primary Group** values for user accounts:

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

  See the well-known security principals for more information. If the value of **primaryGroupID** attribute of user object was changed, you will see the new value here.

- **AllowedToDelegateTo** [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 at least one SPN is registered for user account. If the SPNs list on **Delegation** tab of a user account was changed, you will see the new SPNs list in **AllowedToDelegateTo** field (note that you will see the new list instead of changes) of this event. This is an example of **AllowedToDelegateTo**:

- dcom/WIN2012
- dcom/WIN2012.contoso.local

If the value of **msDS-AllowedToDelegateTo** attribute of user object was changed, you will see the new value here.

The value can be `<value not set>`, for example, if delegation was disabled.

For local accounts, this field is not applicable and always has `-` value.

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]: specifies flags that control password, lockout, disable/enable, script, and other behavior for the user or computer account. This parameter contains the previous value of the SAM implementation of account flags (definition differs from userAccountControl in AD).
- **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). If the value was changed, you will see the new value here. For a list of account flags you may see here, refer to [MS-SAMR]: USER_ACCOUNT Codes.
- **User Account Control** [Type = UnicodeString]**:** shows the list of changes in **userAccountControl** attribute. You will see a line of text for each change. See possible values in here: User's or Computer's account UAC flags. In the "User Account Control field text" column, you can see the text that will be displayed in the **User Account Control** field in 4738 event.
- **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. For local accounts, this field is not applicable and always has `<value not set>` value.
- **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. If the value of **sIDHistory** attribute of user object was changed, you will see the new value here.

- **Logon Hours** [Type = UnicodeString]: hours that the account is allowed to logon to the domain. If the value of **logonHours** attribute of user object was changed, you will see the new value here. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. Here is an example of this field:

  Sunday 12:00 AM - 7:00 PM

  Sunday 9:00 PM -Monday 1:00 PM

  Monday 2:00 PM -Tuesday 6:00 PM

  Tuesday 8:00 PM -Wednesday 10:00 AM

  For 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.".

For 4738(S): A user account was changed.

- Some organizations monitor every 4738 event.
- If you have critical user computer accounts (for example, domain administrator accounts or service accounts) for which you need to monitor each change, monitor this event with the **"Target Account\Account Name"** that corresponds to the critical account or accounts.
- If you have user accounts for which any change in the services list on the **Delegation** tab should be monitored, monitor this event when **AllowedToDelegateTo** is not -. This value means the services list was changed.
- Consider whether to track the following fields:

Field to track	Reason to track
Display Name **User Principal Name** **Home Directory** **Home Drive** **Script Path** **Profile Path** **User Workstations** **Password Last Set**	We recommend monitoring all changes for these fields for critical domain and local accounts.

Field to track	Reason to track
Account Expires **Primary Group ID** **Logon Hours**	
Primary Group ID is not 513	Typically, the **Primary Group** value is 513 for domain and local users. Other values should be monitored.
For user accounts for which the services list (on the **Delegation** tab) should not be empty: **AllowedToDelegateTo** is marked `<value not set>`	If **AllowedToDelegateTo** is marked `<value not set>` on user accounts that previously had a services list (on the **Delegation** tab), it means the list was cleared.
SID History is not -	This field will always be set to - unless the account was migrated from another domain.

- 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.
'Password Not Required' – Enabled	Should not typically be enabled for user accounts because it weakens security for the account.
'Encrypted Text Password Allowed' – Enabled	Should not typically be enabled for user accounts because it weakens security for the account.
'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.
'Smartcard Required' – Enabled	Should be monitored for critical accounts.
'Password Not Required' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**."
'Encrypted Text Password Allowed' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**."

User account control flag to track	**Information about the flag**
'Don't Expire Password' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**."
'Smartcard Required' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**."
'Trusted For Delegation' – Enabled	Means that Kerberos Constraint or Unconstraint delegation was enabled for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action.
'Trusted For Delegation' – Disabled	Means that Kerberos Constraint or Unconstraint delegation was disabled for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action. Also, if you have a list of user accounts for which delegation is critical and should not be disabled, monitor this for those accounts.
'Trusted To Authenticate For Delegation' – Enabled	Means that Protocol Transition delegation was enabled for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action.
'Trusted To Authenticate For Delegation' – Disabled	Means that Protocol Transition delegation was disabled for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action. Also, if you have a list of user accounts for which delegation is critical and should not be disabled, monitor this for those accounts.
'Not Delegated' – Enabled	Means that **Account is sensitive and cannot be delegated** was checked for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action.
'Not Delegated' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**." Means that **Account is sensitive and cannot be delegated** was unchecked for the user account. We recommend monitoring this to discover whether it is an approved action (done by an administrator), a mistake, or a malicious action.
'Use DES Key Only' – Enabled	Should not typically be enabled for user accounts because it weakens security for the account's Kerberos authentication.
'Don't Require Preauth' – Enabled	Should not be enabled for user accounts because it weakens security for the account's Kerberos authentication.
'Use DES Key Only' – Disabled	Should be monitored for all accounts where the setting should be "**Enabled**."

User account control flag to track	**Information about the flag**
'Don't Require Preauth' – Disabled	Should be monitored for all accounts where the setting should be “**Enabled**.”

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738