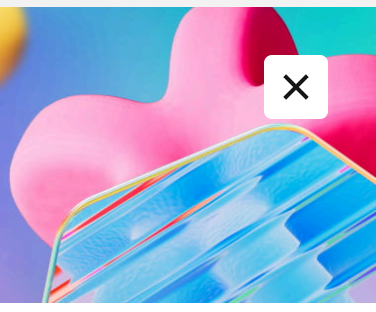
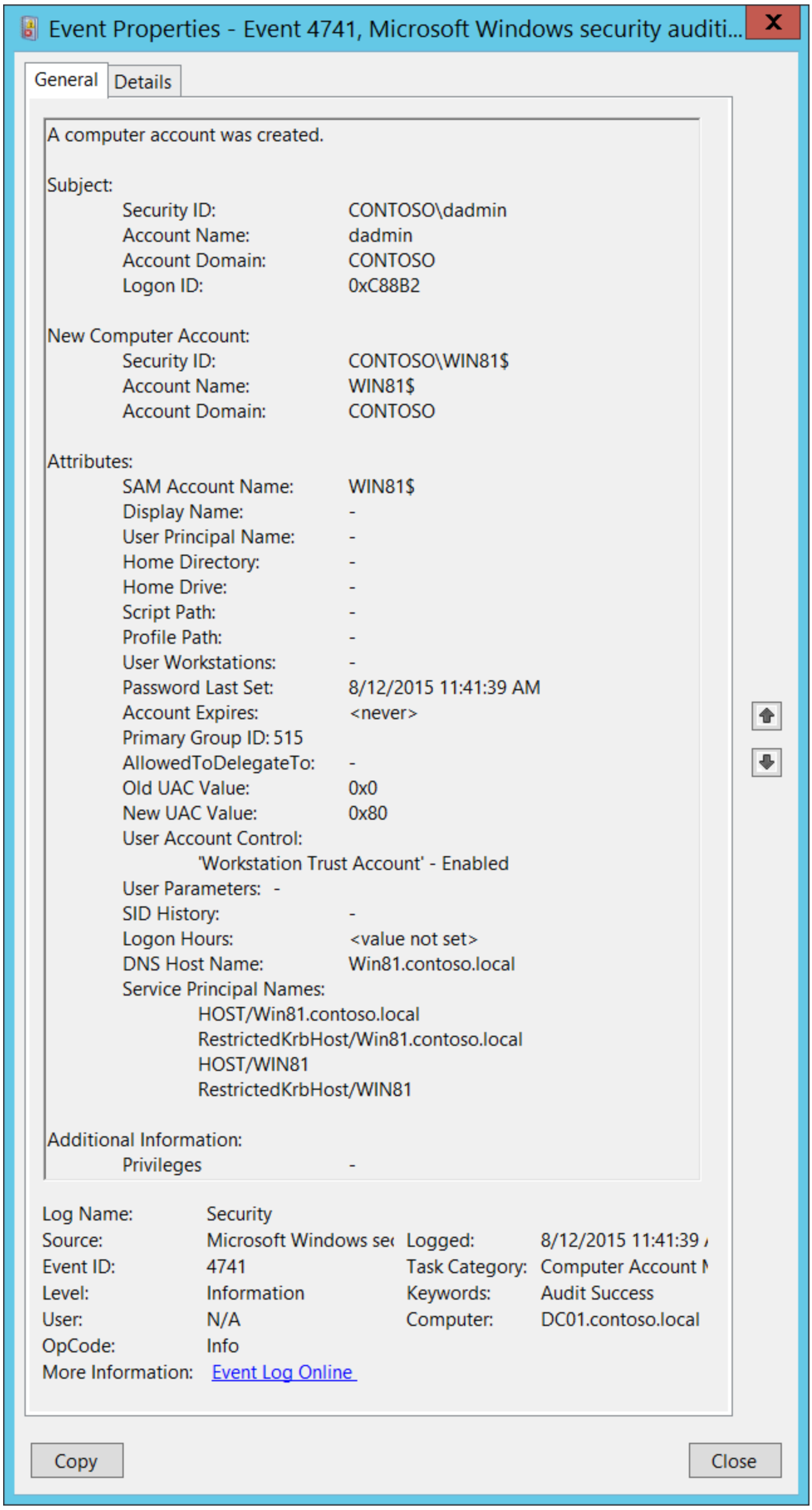


4741(S): A computer account was created.

Article • 09/07/2021 • 1 contributor

- Audit Filtering Platform Packet Drop
- Audit Handle Manipulation
- Audit Kernel Object



Subcategory: Audit Computer Account Management

Event Description:

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

This event generates only on domain controllers.

> ⓘ **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>4741</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>13825</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-08-12T18:41:39.201898100Z" />
 <EventRecordID>170254</EventRecordID>
 <Correlation />
 <Execution ProcessID="520" ThreadID="1096" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="TargetUserName">WIN81$</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="TargetSid">S-1-5-21-3457937927-2839227994-823803824-6116</Data>
 <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0xc88b2</Data>
 <Data Name="PrivilegeList">-</Data>
 <Data Name="SamAccountName">WIN81$</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">8/12/2015 11:41:39 AM</Data>
 <Data Name="AccountExpires">%%1794</Data>
 <Data Name="PrimaryGroupId">515</Data>
 <Data Name="AllowedToDelegateTo">-</Data>
 <Data Name="OldUacValue">0x0</Data>
 <Data Name="NewUacValue">0x80</Data>
 <Data Name="UserAccountControl">%%2087</Data>
 <Data Name="UserParameters">-</Data>
 <Data Name="SidHistory">-</Data>
 <Data Name="LogonHours">%%1793</Data>
 <Data Name="DnsHostName">Win81.contoso.local</Data>
 <Data Name="ServicePrincipalNames">HOST/Win81.contoso.local RestrictedKrbHost/W
 </EventData>
 </Event>
```

Required Server Roles: Active Directory domain controller.

Minimum OS Version: Windows Server 2008.

Event Versions: 0.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]**:** SID of account that requested the “create Computer object” 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 Computer object" operation.
- **Account Domain** [Type = UnicodeString]: subject's domain 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".
- **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 Computer Account:

- **Security ID** [Type = SID]: SID of created computer 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 computer account that was created. For example: WIN81$
- **Account Domain** [Type = UnicodeString]: domain name of created computer account. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL

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 computer object. For example: WIN81$.
- **Display Name** [Type = UnicodeString]: the value of **displayName** attribute of new computer object. It is a name displayed in the address book for a particular account (typically – user account). This is usually the combination of the user's first name, middle initial, and last name. For computer objects, it is optional, and typically is 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 `-`.
- **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 computer object. For computer objects, it is optional, and typically is 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 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 computer object. For computer objects, it is optional, and typically is 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 computer object. For computer objects, it is optional, and typically is 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 `-`.

- **Script Path** [Type = UnicodeString]: specifies the path of the account's logon script. This parameter contains the value of **scriptPath** attribute of new computer object. For computer objects, it is optional, and typically is 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 `-`.

- **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 computer object. For computer objects, it is optional, and typically is 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 `-`.

- **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. This parameter contains the value of **userWorkstations** attribute of new computer object. For computer objects, it is optional, and typically is 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 `-`.

- **Password Last Set** [Type = UnicodeString]: last time the account's password was modified. For manually created computer account, using Active Directory Users and Computers snap-in, this field typically has value `<never>`. For computer account created during standard domain join procedure this field will contains time when computer object was created, because password creates during domain join procedure. For example: 8/12/2015 11:41:39 AM. This parameter contains the value of **pwdLastSet** attribute of new computer object.

- **Account Expires** [Type = UnicodeString]: the date when the account expires. This parameter contains the value of **accountExpires** attribute of new computer object. For computer objects, it is optional, and typically is 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 `-`.

- **Primary Group ID** [Type = UnicodeString]: Relative Identifier (RID) of computer'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 computer accounts has the following values:

- 516 (Domain Controllers) – for domain controllers.
- 521 (Read-only Domain Controllers) – for read-only domain controllers (RODC).
- 515 (Domain Computers) – for member servers and workstations.

  See the well-known security principals for more information. This parameter contains the value of **primaryGroupID** attribute of new computer object.

- **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 computer account. Typically it is set to `-` for new computer objects. This parameter contains the value of **AllowedToDelegateTo** attribute of new computer object. See description of **AllowedToDelegateTo** field for "4742: A computer 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 computer's account properties, then you will see `<value changed, but not displayed>` in this field in "4742(S): A computer account was changed." This parameter might not be captured in the event, and in that case appears as `-`.
- **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 computer 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 computer object. For computer objects, it is optional, and typically is not set. You can change this attribute by using Active Directory Users and Computers, or through a script, for example. You will see `<value not set>` value for new created computer accounts in event 4741.
- **DNS Host Name** [Type = UnicodeString]: name of computer account as registered in DNS. The value of **dNSHostName** attribute of new computer object. For manually created computer account objects this field has value `-`.

- **Service Principal Names** [Type = UnicodeString]: The list of SPNs, registered for computer account. For new computer accounts it will typically contain HOST SPNs and RestrictedKrbHost SPNs. The value of **servicePrincipalName** attribute of new computer object. For manually created computer objects it is typically equals `-`. This is an example of **Service Principal Names** field for new domain joined workstation:

  HOST/Win81.contoso.local

  RestrictedKrbHost/Win81.contoso.local

  HOST/WIN81

  RestrictedKrbHost/WIN81

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 the table below:

Expand table

Privilege Name	User Right Group Policy Name	Description
SeAssignPrimaryTokenPrivilege	Replace a process-level token	Required to assign the *primary token* of a process. With this privilege, the user can initiate a process to replace the default token associated with a started subprocess.
SeAuditPrivilege	Generate security audits	With this privilege, the user can add entries to the security log.
SeBackupPrivilege	Back up files and directories	- Required to perform backup operations. With this privilege, the user can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system. This privilege causes the system to grant all read access control to any file, regardless of the *access control list* (ACL) specified for the file. Any access request other than read is still evaluated with the ACL. The following access rights are granted if this privilege is held: READ_CONTROL ACCESS_SYSTEM_SECURITY FILE_GENERIC_READ FILE_TRAVERSE
SeChangeNotifyPrivilege	Bypass traverse checking	Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. With this privilege, the user can traverse directory trees even though the user may not have permissions on the traversed directory. This privilege does not allow the user to list the contents of a directory, only to traverse directories.
SeCreateGlobalPrivilege	Create global objects	Required to create named file mapping objects in the global namespace during Terminal Services sessions.
SeCreatePagefilePrivilege	Create a pagefile	With this privilege, the user can create and change the size of a pagefile.
SeCreatePermanentPrivilege	Create permanent	Required to create a permanent object. This privilege is useful to kernel-mode

	shared objects	components that extend the object namespace. Components that are running in kernel mode already have this privilege inherently; it is not necessary to assign them the privilege.
SeCreateSymbolicLinkPrivilege	Create symbolic links	Required to create a symbolic link.
SeCreateTokenPrivilege	Create a token object	Allows a process to create a token which it can then use to get access to any local resources when the process uses NtCreateToken() or other token-creation APIs. When a process requires this privilege, we recommend using the LocalSystem account (which already includes the privilege), rather than creating a separate user account and assigning this privilege to it.
SeDebugPrivilege	Debug programs	Required to debug and adjust the memory of a process owned by another account. With this privilege, the user can attach a debugger to any process or to the kernel. Developers who are debugging their own applications do not need this user right. Developers who are debugging new system components need this user right. This user right provides complete access to sensitive and critical operating system components.
SeEnableDelegationPrivilege	Enable computer and user accounts to be trusted for delegation	Required to mark user and computer accounts as trusted for delegation. With this privilege, the user can set the **Trusted for Delegation** setting on a user or computer object. The user or object that is granted this privilege must have write access to the account control flags on the user or computer object. A server process running on a computer (or under a user context) that is trusted for delegation can access resources on another computer using the delegated credentials of a client, as long as the account of the client does not have the **Account cannot be delegated** account control flag set.
SeImpersonatePrivilege	Impersonate a client after authentication	With this privilege, the user can impersonate other accounts.
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Required to increase the base priority of a process. With this privilege, the user can use a process with Write property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Required to increase the quota assigned to a process. With this privilege, the user can change the maximum memory that can be consumed by a process.
SeIncreaseWorkingSetPrivilege	Increase a process working set	Required to allocate more memory for applications that run in the context of users.
SeLoadDriverPrivilege	Load and unload device drivers	Required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers.

SeLockMemoryPrivilege	Lock pages in memory	Required to lock physical pages in memory. With this privilege, the user can use a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Exercising this privilege could significantly affect system performance by decreasing the amount of available random access memory (RAM).
SeMachineAccountPrivilege	Add workstations to domain	With this privilege, the user can create a computer account. This privilege is valid only on domain controllers.
SeManageVolumePrivilege	Perform volume maintenance tasks	Required to run maintenance tasks on a volume, such as remote defragmentation.
SeProfileSingleProcessPrivilege	Profile single process	Required to gather profiling information for a single process. With this privilege, the user can use performance monitoring tools to monitor the performance of non-system processes.
SeRelabelPrivilege	Modify an object label	Required to modify the mandatory integrity level of an object.
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Required to shut down a system using a network request.
SeRestorePrivilege	Restore files and directories	Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL. Additionally, this privilege enables you to set any valid user or group SID as the owner of a file. The following access rights are granted if this privilege is held: WRITE_DAC WRITE_OWNER ACCESS_SYSTEM_SECURITY FILE_GENERIC_WRITE FILE_ADD_FILE FILE_ADD_SUBDIRECTORY DELETE With this privilege, the user can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories and determines which users can set any valid security principal as the owner of an object.
SeSecurityPrivilege	Manage auditing and security log	Required to perform a number of security-related functions, such as controlling and viewing audit events in security event log. With this privilege, the user can specify object access auditing options for individual resources, such as files, Active Directory objects, and registry keys. A user with this privilege can also view and clear the security log.
SeShutdownPrivilege	Shut down the system	Required to shut down a local system.
SeSyncAgentPrivilege	Synchronize directory service data	This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers.

		With this privilege, the user can synchronize all directory service data. This is also known as Active Directory synchronization.
SeSystemEnvironmentPrivilege	Modify firmware environment values	Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
SeSystemProfilePrivilege	Profile system performance	Required to gather profiling information for the entire system. With this privilege, the user can use performance monitoring tools to monitor the performance of system processes.
SeSystemtimePrivilege	Change the system time	Required to modify the system time. With this privilege, the user can change the time and date on the internal clock of the computer. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Required to take ownership of an object without being granted discretionary access. This privilege allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object. With this privilege, the user can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.
SeTcbPrivilege	Act as part of the operating system	This privilege identifies its holder as part of the trusted computer base. This user right allows a process to impersonate any user without authentication. The process can therefore gain access to the same local resources as that user.
SeTimeZonePrivilege	Change the time zone	Required to adjust the time zone associated with the computer's internal clock.
SeTrustedCredManAccessPrivilege	Access Credential Manager as a trusted caller	Required to access Credential Manager as a trusted caller.
SeUndockPrivilege	Remove computer from docking station	Required to undock a laptop. With this privilege, the user can undock a portable computer from its docking station without logging on.
SeUnsolicitedInputPrivilege	Not applicable	Required to read unsolicited input from a *terminal* device.

Table 8. User Privileges.

Security Monitoring Recommendations

For 4741(S): A computer account was created.

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

- If your information security monitoring policy requires you to monitor computer account creation, monitor this event.
- Consider whether to track the following fields and values:

Expand table

Field and value to track	Reason to track
SAM Account Name: empty or `-`	This field must contain the computer account name. If it is empty or **-**, it might indicate an anomaly.
Display Name is not - **User Principal Name** is not - **Home Directory** is not - **Home Drive** is not - **Script Path** is not - **Profile Path** is not - **User Workstations** is not - **AllowedToDelegateTo** is not -	Typically these fields are **-** for new computer accounts. Other values might indicate an anomaly and should be monitored.
Password Last Set is `<never>`	This typically means this is a manually created computer account, which you might need to monitor.
Account Expires is not `<never>`	Typically this field is `<never>` for new computer accounts. Other values might indicate an anomaly and should be monitored.
Primary Group ID is any value other than 515.	Typically, the **Primary Group ID** value is one of the following: **516** for domain controllers **521** for read only domain controllers (RODCs) **515** for servers and workstations (domain computers) If the **Primary Group ID** is 516 or 521, it is a new domain controller or RODC, and the event should be monitored. If the value is not 516, 521, or 515, it is not a typical value and should be monitored.
Old UAC Value is not 0x0	Typically this field is **0x0** for new computer 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>`	This should always be `<value not set>` for new computer accounts.

- Consider whether to track the following account control flags:

Expand table

User account control flag to track	Information about the flag
'**Encrypted Text Password Allowed**' – Enabled	Should not be set for computer accounts. By default, it will not be set, and it cannot be set in the account properties in Active Directory Users and Computers.
'**Server Trust Account**' – Enabled	Should be enabled **only** for domain controllers.
'**Don't Expire Password**' – Enabled	Should not be enabled for new computer accounts, because the password automatically changes every 30 days by default. For computer accounts, this flag cannot be set in the account properties in Active Directory Users and Computers.
'**Smartcard Required**' – Enabled	Should not be enabled for new computer accounts.
'**Trusted For Delegation**' – Enabled	Should not be enabled for new member servers and workstations. It is enabled by default for new domain controllers.

'Not Delegated' – Enabled	Should not be enabled for new computer accounts.
'Use DES Key Only' – Enabled	Should not be enabled for new computer accounts. For computer accounts, it cannot be set in the account properties in Active Directory Users and Computers.
'Don't Require Preauth' – Enabled	Should not be enabled for new computer accounts. For computer accounts, it cannot be set in the account properties in Active Directory Users and Computers.
'Trusted To Authenticate For Delegation' – Enabled	Should not be enabled for new computer accounts by default.