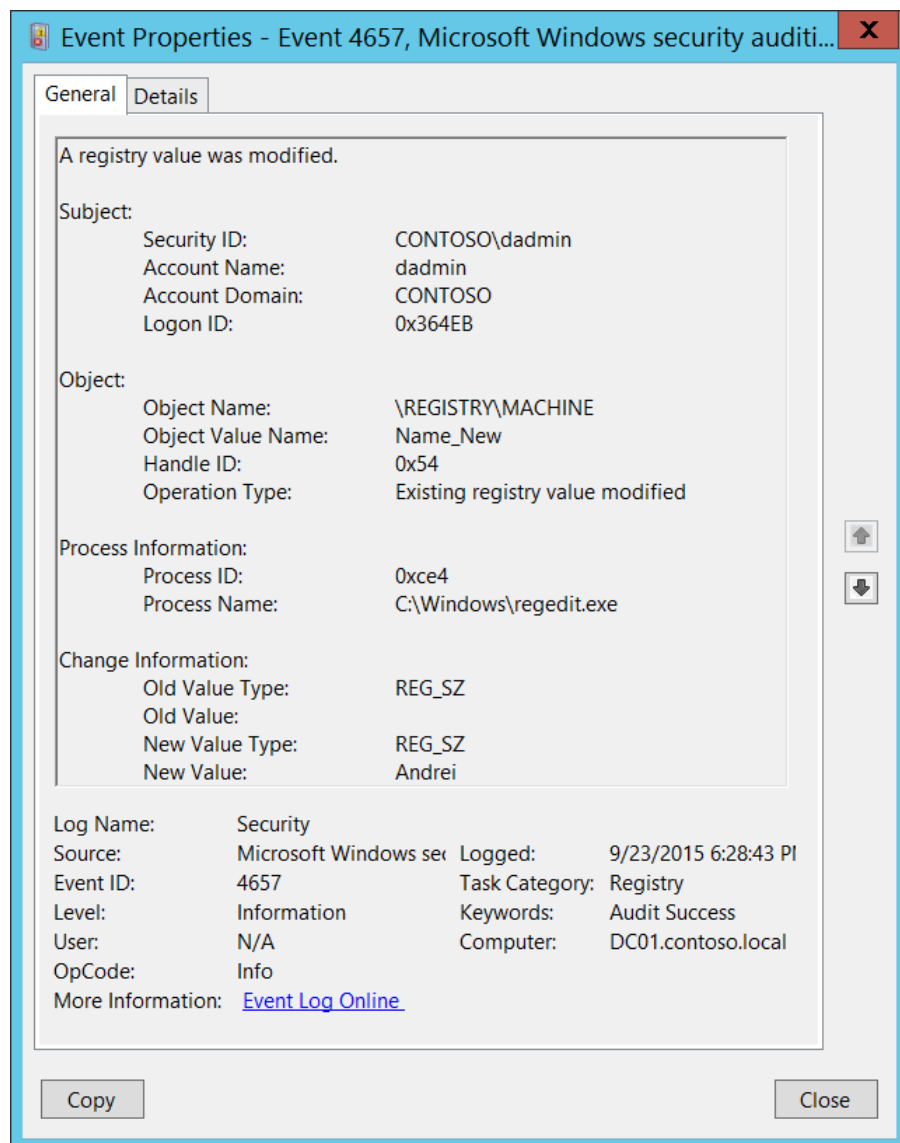


4657(S) A registry value was modified. - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 16:25:44 UTC



Subcategory: [Audit Registry](#)

Event Description:

This event generates when a registry key **value** was modified. It doesn't generate when a registry key was modified.

This event generates only if "Set Value" auditing is set in registry key's [SACL](#).

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>4657</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12801</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-09-24T01:28:43.639634100Z" />
  <EventRecordID>744725</EventRecordID>
  <Correlation />
  <Execution ProcessID="4" ThreadID="4824" />
  <Channel>Security</Channel>
  <Computer>DC01.contoso.local</Computer>
  <Security />
</System>
- <EventData>
  <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">0x364eb</Data>
  <Data Name="ObjectName">\\REGISTRY\\MACHINE</Data>
  <Data Name="ObjectValueName">Name\_New</Data>
  <Data Name="HandleId">0x54</Data>
  <Data Name="OperationType">%%1905</Data>
  <Data Name="OldValueType">%%1873</Data>
  <Data Name="OldValue" />
  <Data Name="NewValueType">%%1873</Data>
  <Data Name="NewValue">Andrei</Data>
  <Data Name="ProcessId">0xce4</Data>
  <Data Name="ProcessName">C:\\Windows\\regedit.exe</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 “modify registry value” 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 “modify registry value” 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.”

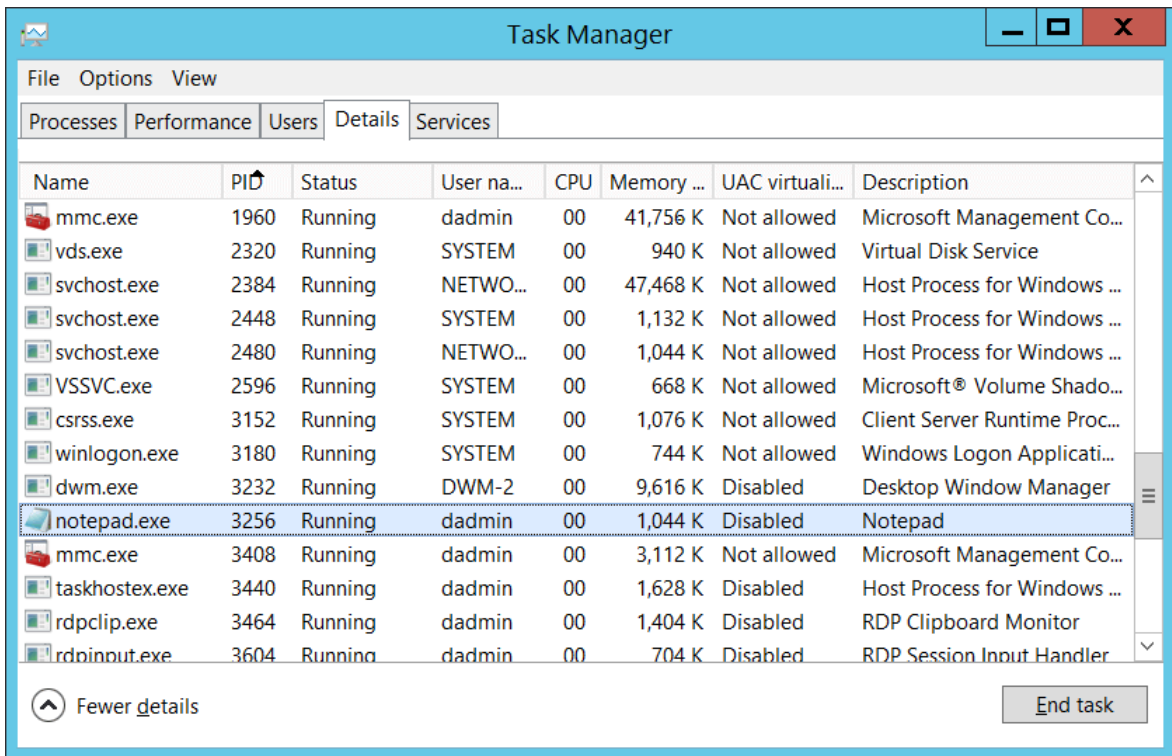
Object:

- **Object Name** [Type = UnicodeString]: full path and name of the registry key which value was modified. The format is: \REGISTRY\HIVE\PATH where:
 - HIVE:
 - HKEY_LOCAL_MACHINE = \REGISTRY\MACHINE
 - HKEY_CURRENT_USER = \REGISTRY\USER\[USER_SID], where [USER_SID] is the SID of current user.

- HKEY_CLASSES_ROOT = \REGISTRY\MACHINE\SOFTWARE\Classes
 - HKEY_USERS = \REGISTRY\USER
 - HKEY_CURRENT_CONFIG =
 \REGISTRY\MACHINE\SYSTEM\ControlSet001\Hardware Profiles\Current
- PATH – path to the registry key.
- **Object Value Name** [Type = UnicodeString]: the name of modified registry key value.
 - **Handle ID** [Type = Pointer]: hexadecimal value of a handle to **Object Name**. This field can help you correlate this event with other events that might contain the same Handle ID, for example, “[4656](#): A handle to an object was requested.” This parameter might not be captured in the event, and in that case appears as “0x0”.
 - **Operation Type** [Type = UnicodeString]: the type of performed operation with registry key value. Most common operations are:
 - New registry value created
 - Registry value deleted
 - Existing registry value modified

Process Information:

- **Process ID** [Type = Pointer]: hexadecimal Process ID of the process through which the registry key value was modified. 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**.

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

Change Information:

- **Old Value Type** [Type = UnicodeString]: old type of changed registry key value. Registry key value types:

Value Type	Description
REG_SZ	String
REG_BINARY	Binary
REG_DWORD	DWORD (32-bit) Value
REG_QWORD	QWORD (64-bit) Value
REG_MULTI_SZ	Multi-String Value
REG_EXPAND_SZ	Expandable String Value

- **Old Value** [Type = UnicodeString]: old value for changed registry key value.
- **New Value Type** [Type = UnicodeString]: new type of changed registry key value. See table above for possible values.

- **New Value** [Type = UnicodeString]: new value for changed registry key value.

Security Monitoring Recommendations

For 4657(S): A registry value was modified.

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 **Object Name** is a sensitive or critical registry key for which you need to monitor any modification of its values, monitor all [4657](#) events.
- If **Object Name** has specific values (**Object Value Name**) and you need to monitor modifications of these values, monitor for all [4657](#) events.

Source: <https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4657>