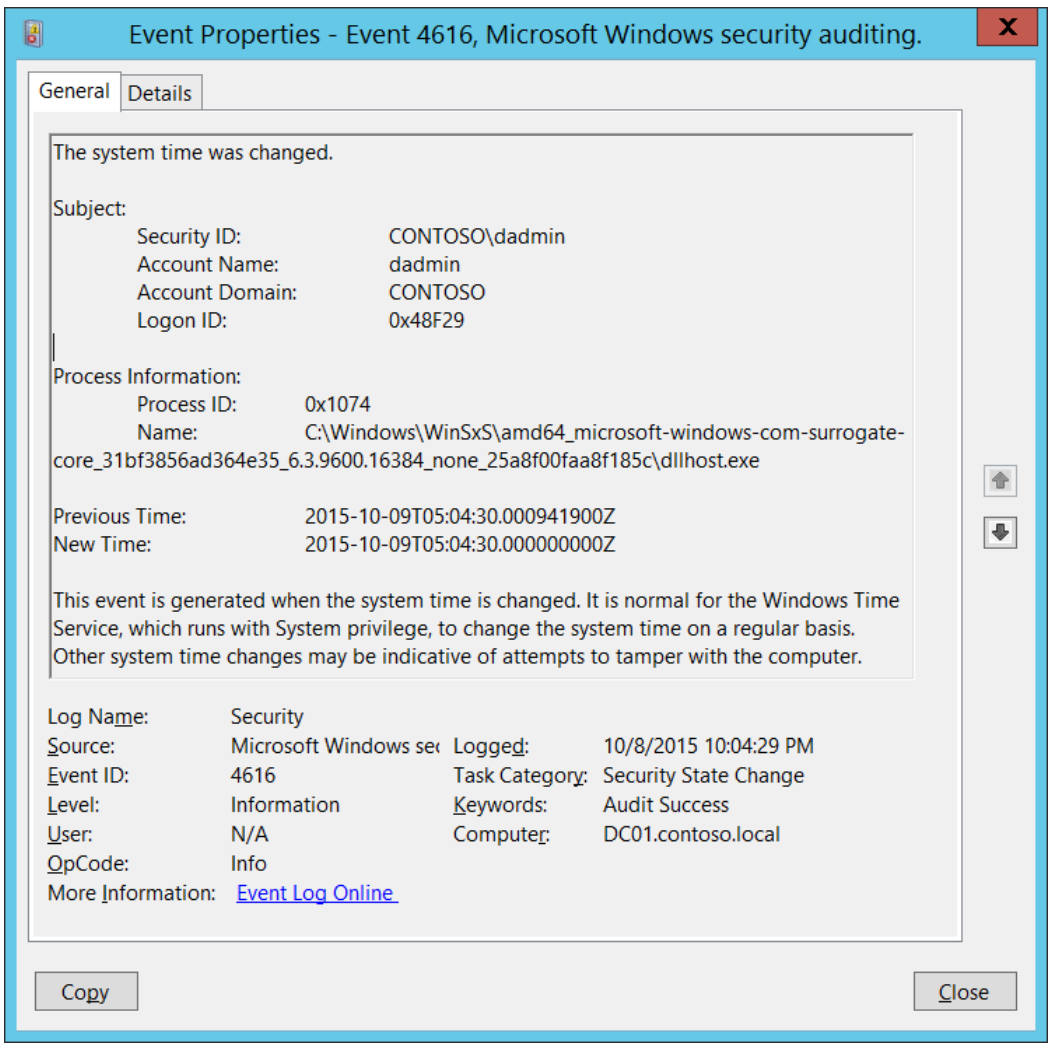
Filter by title

- Audit File System
- Audit Filtering Platform Connection
- Audit Filtering Platform Packet Drop
- Audit Handle Manipulation
- Audit Kernel Object
- Audit Other Object Access Events
- Audit Registry
- Audit Removable Storage
- Audit SAM
- Audit Central Access Policy Staging
- Audit Audit Policy Change
- Audit Authentication Policy Change
- Audit Authorization Policy Change
- Audit Filtering Platform Policy Change
- Audit MPSSVC Rule-Level Policy Change
- Audit Other Policy Change Events
- Audit Sensitive Privilege Use
- Audit Non Sensitive Privilege Use
- Audit Other Privilege Use Events
- Audit IPsec Driver
- Audit Other System Events
- Audit Security State Change
  - Audit Security State Change
  - Event 4608 S: Windows is starting up.
  - **Event 4616 S: The system time was changed.**
  - Event 4621 S: Administrator recovered system from CrashOnAuditFail.
- Audit Security System Extension
- Audit System Integrity
- Other Events
- Appendix A: Security monitoring recommendations for many audit events
- Registry (Global Object Access Auditing)
- File System (Global Object Access Auditing)

Windows security

4616(S): The system time was changed.

Article • 09/07/2021 • 1 contributor



Subcategory: Audit Security State Change

Event Description:

This event generates every time system time was changed.

This event is always logged regardless of the "Audit Security State Change" sub-category setting.

You will typically see these events with “**Subject\Security ID**” = “**LOCAL SERVICE**”, these are normal time correction actions.

> **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>4616</EventID>
 <Version>1</Version>
 <Level>0</Level>
```

```
<Task>12288</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-10-09T05:04:29.995794600Z" />
<EventRecordID>1101699</EventRecordID>
<Correlation />
<Execution ProcessID="4" ThreadID="148" />
<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">0x48f29</Data>
<Data Name="PreviousTime">2015-10-09T05:04:30.000941900Z</Data>
<Data Name="NewTime">2015-10-09T05:04:30.000000000Z</Data>
<Data Name="ProcessId">0x1074</Data>
<Data Name="ProcessName">C:\\Windows\\WinSxS\\amd64\_microsoft-windows-com-surr
</EventData>
</Event>
```


Required Server Roles: None.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions:

- 0 - Windows Server 2008, Windows Vista.
- 1 - Windows Server 2008 R2, Windows 7.
  - Added “Process Information” section.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]**:** SID of account that requested the “change system time” 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**.

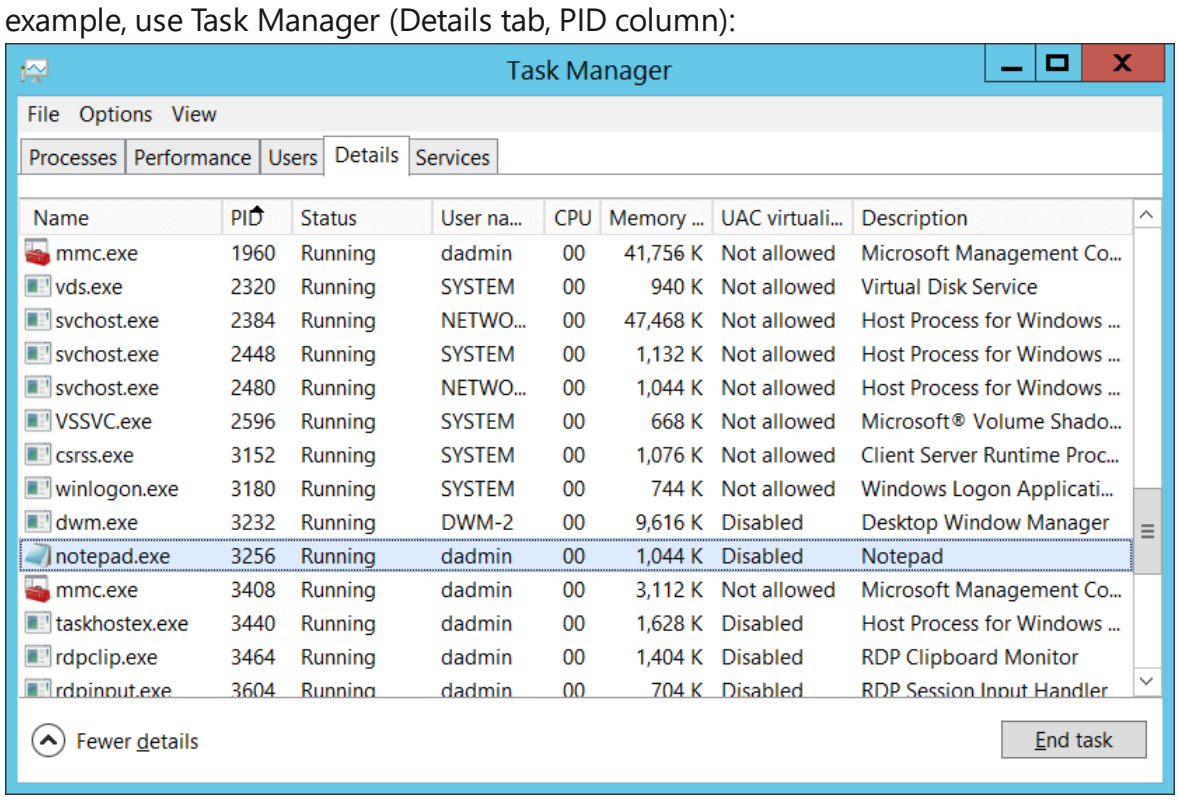
- **Account Name** [Type = UnicodeString]**:** the name of the account that requested the “change system time” operation.
- **Account Domain** [Type = UnicodeString]**:** subject’s domain or computer name. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase 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.”

Process Information [Version 1]:

- **Process ID** [Type = Pointer] [Version 1]: hexadecimal Process ID of the process that changed the system time. 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**.

- **Name** [Type = UnicodeString] [Version 1]: full path and the name of the executable for the process.

Previous Time [Type = FILETIME]: previous time in ***UTC*** time zone. The format is **YYYY-MM-DDThh:mm:ss.nnnnnnnZ**:

- Y - years
- M - months
- D - days
- T - the beginning of the time element, as specified in ISO 8601 .
- h - hours
- m - minutes
- s - seconds
- n - fractional seconds
- Z - the zone designator for the zero UTC offset. "09:30 UTC" is therefore represented as "09:30Z". "14:45:15 UTC" would be "14:45:15Z".

New Time [Type = FILETIME]: new time that was set in ***UTC*** time zone. The format is **YYYY-MM-DDThh:mm:ss.nnnnnnnZ**:

- Y - years
- M - months
- D - days
- T - the beginning of the time element, as specified in ISO 8601 .
- h - hours
- m - minutes
- s - seconds
- n - fractional seconds
- Z - the zone designator for the zero UTC offset. "09:30 UTC" is therefore represented as "09:30Z". "14:45:15 UTC" would be "14:45:15Z".

Security Monitoring Recommendations

For 4616(S): The system time was changed.

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

- Report all "**Subject\Security ID**" not equals **"LOCAL SERVICE"**, which means that the time change was not made by Windows Time service.
- Report all "**Process Information\Name**" not equals **"C:\Windows\System32\svchost.exe"** (path to svchost.exe can be different, you can search for "svchost.exe" substring), which means that the time change was not made by Windows Time service.
- 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**."