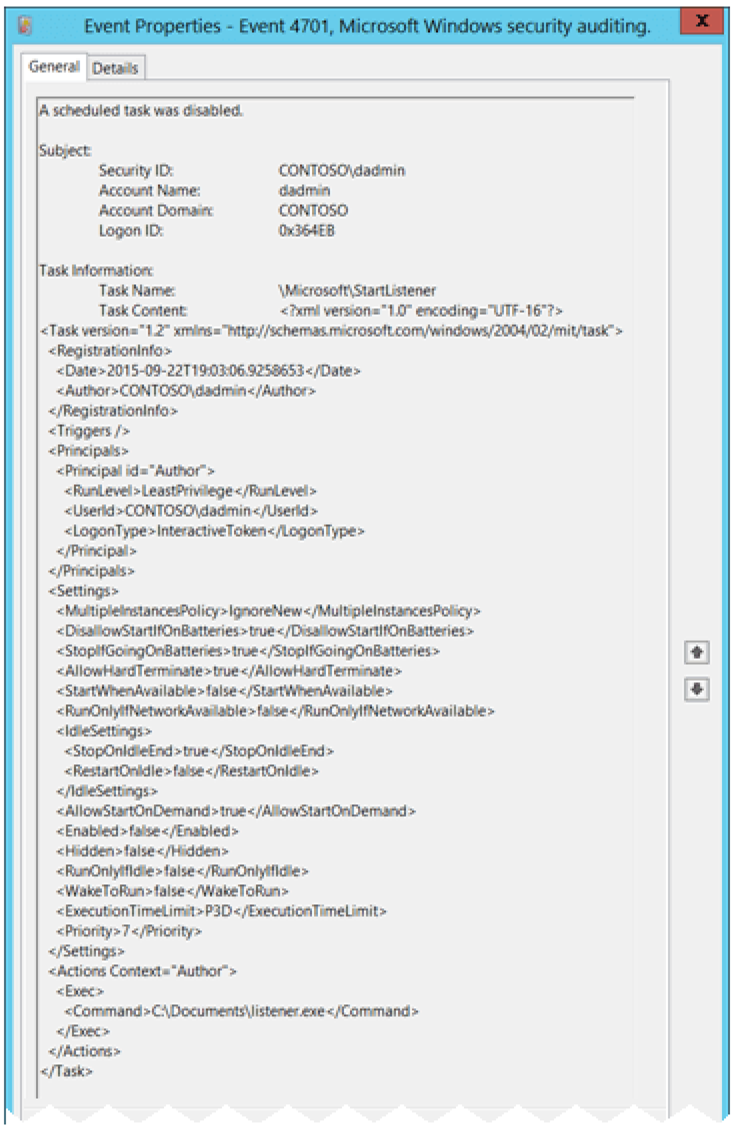
Filter by title

… / Audit Other Object Access Events /

4701(S): A scheduled task was disabled.

Article • 09/07/2021 • 1 contributor


Event Properties - Event 4701, Microsoft Windows security auditing.
General
Details

```
A scheduled task was disabled.

Subject:
        Security ID:            CONTOSO\dadmin
        Account Name:           dadmin
        Account Domain:         CONTOSO
        Logon ID:               0x364EB

Task Information:
        Task Name:              \Microsoft\StartListener
        Task Content:           <?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2015-09-22T19:03:06.9258653</Date>
    <Author>CONTOSO\dadmin</Author>
  </RegistrationInfo>
  <Triggers />
  <Principals>
    <Principal id="Author">
      <RunLevel>LeastPrivilege</RunLevel>
      <UserId>CONTOSO\dadmin</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>false</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Documents\listener.exe</Command>
    </Exec>
  </Actions>
</Task>
```

Subcategory: Audit Other Object Access Events

Event Description:

This event generates every time a scheduled task is disabled.

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

Event 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>4701</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12804</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-23T02:32:45.844066600Z" />
```

Auditing)
File System (Global Object Access Auditing)
Windows security

```
 <EventRecordID>344860</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="4364" />
 <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="TaskName">\\Microsoft\\StartListener</Data>
 <Data Name="TaskContent"><?xml version="1.0" encoding="UTF-16"?> <Task version=
 </EventData>
 </Event>
```

> ⓘ **Note**
>
> Windows 10 Versions 1903 and above augments the event with these additional properties: Event Version 1. ***Event XML:***
>
> Copy
>
> ```
> <Data Name="ClientProcessStartKey">5066549580796854</Data>
> <Data Name="ClientProcessId">3932</Data>
> <Data Name="ParentProcessId">5304</Data>
> <Data Name="RpcCallClientLocality">0</Data>
> <Data Name="FQDN">DESKTOP-Name</Data>
> ```

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 "enable scheduled task" 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.

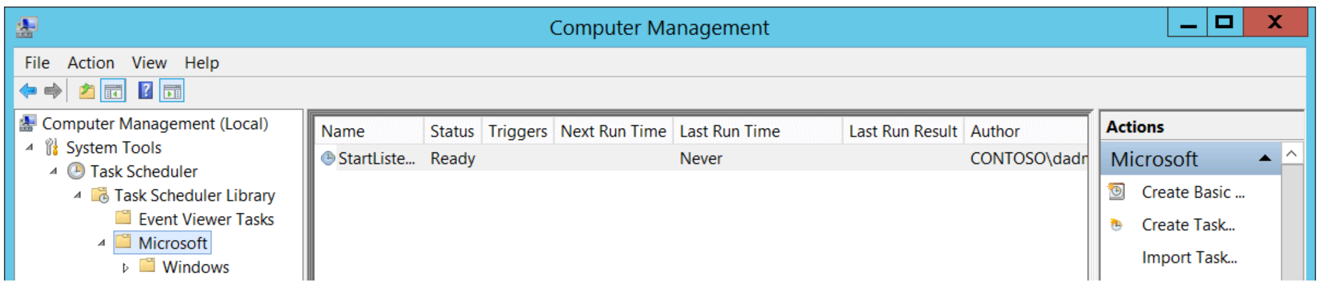
> **Note** A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the 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 "enable scheduled task" 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.”

Task Information:

- **Task Name** [Type = UnicodeString]**:** disabled scheduled task name. The format of this value is “\task_path\task_name”, where task_path is a path in Microsoft **Task Scheduler** tree starting from “**Task Scheduler Library**” node:



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author
StartListe...	Ready			Never		CONTOSO\dadr

- **Task Content** [Type = UnicodeString]: the XML of the disabled task. Here “XML Task Definition Format” you can read more about the XML format for scheduled tasks.

Security Monitoring Recommendations

For 4701(S): A scheduled task was disabled.

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

- If a highly critical scheduled task exists on some computers, and it should never be disabled, monitor for 4701 events with the corresponding **Task Name**.