

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

Return to main site

✕

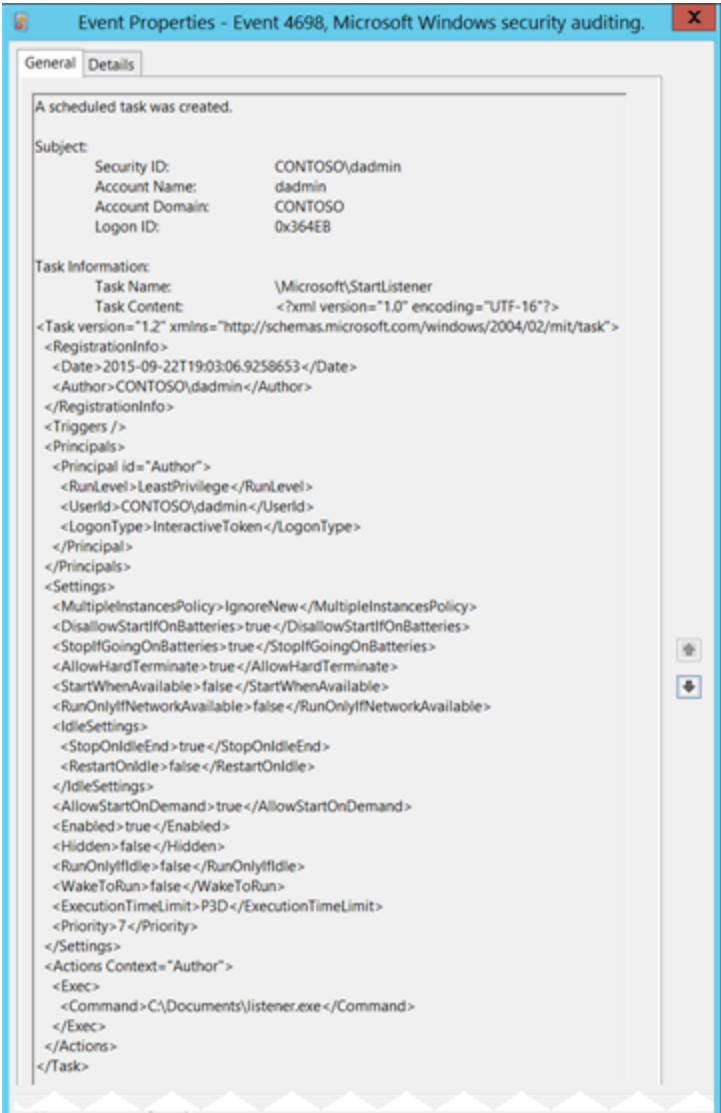
 Filter by title

⋮ / [Audit Other Object Access Events](#) /

4698(S): A scheduled task was created.

Article • 09/07/2021 • [1 contributor](#)



Subcategory: [Audit Other Object Access Events](#)

Event Description:

This event generates every time a new scheduled task is created.

Note For recommendations, see [Security Monitoring Recommendations](#) for this event.

- Event 4699 S: A scheduled task was deleted.
- Event 4700 S: A scheduled task was enabled.
- Event 4701 S: A scheduled task was disabled.
- Event 4702 S: A scheduled task was updated.
- Event 5888 S: An object in the COM+ Catalog was modified.
- Event 5889 S: An object was deleted from the COM+ Catalog.
- Event 5890 S: An object was added to the COM+ Catalog.

- > 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 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

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>4698</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12804</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-09-23T02:03:06.944522200Z" />
  <EventRecordID>344740</EventRecordID>
  <Correlation />
  <Execution ProcessID="516" ThreadID="5048" />
  <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:

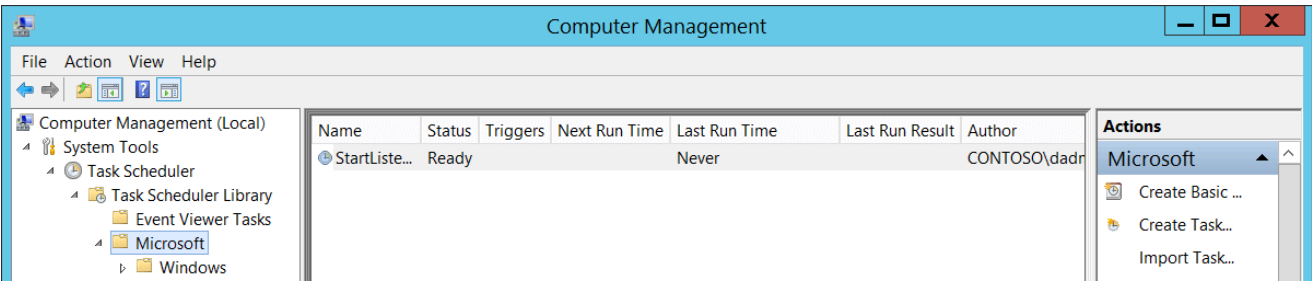
- **Security ID** [Type = SID]: SID of account that requested the “create scheduled task” operation. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

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 “create 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]: new 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:



- **Task Content** [Type = UnicodeString]: the [XML](#) content of the new task. For more information about the XML format for scheduled tasks, see “[XML Task Definition Format](#).”

Security Monitoring Recommendations

For 4698(S): A scheduled task was created.

Important For this event, also see [Appendix A: Security monitoring recommendations for many audit events](#).

- We recommend monitoring all scheduled task creation events, especially on critical computers or devices. Scheduled tasks are often used by malware to stay in the system after reboot or for other malicious actions.
- Monitor for new tasks located in the **Task Scheduler Library** root node, that is, where **Task Name** looks like ‘\TASK_NAME’. Scheduled tasks that are created manually or by malware are often located in the **Task Scheduler Library** root node.
- In the new task, if the **Task Content**: XML contains **<LogonType>Password</LogonType>** value, trigger an alert. In this case, the password for the account that will be used to run the scheduled task will be saved in Credential Manager in cleartext format, and can be extracted using Administrative privileges.