



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

ⓘ 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](#)



# 4706(S): A new trust was created to a domain.

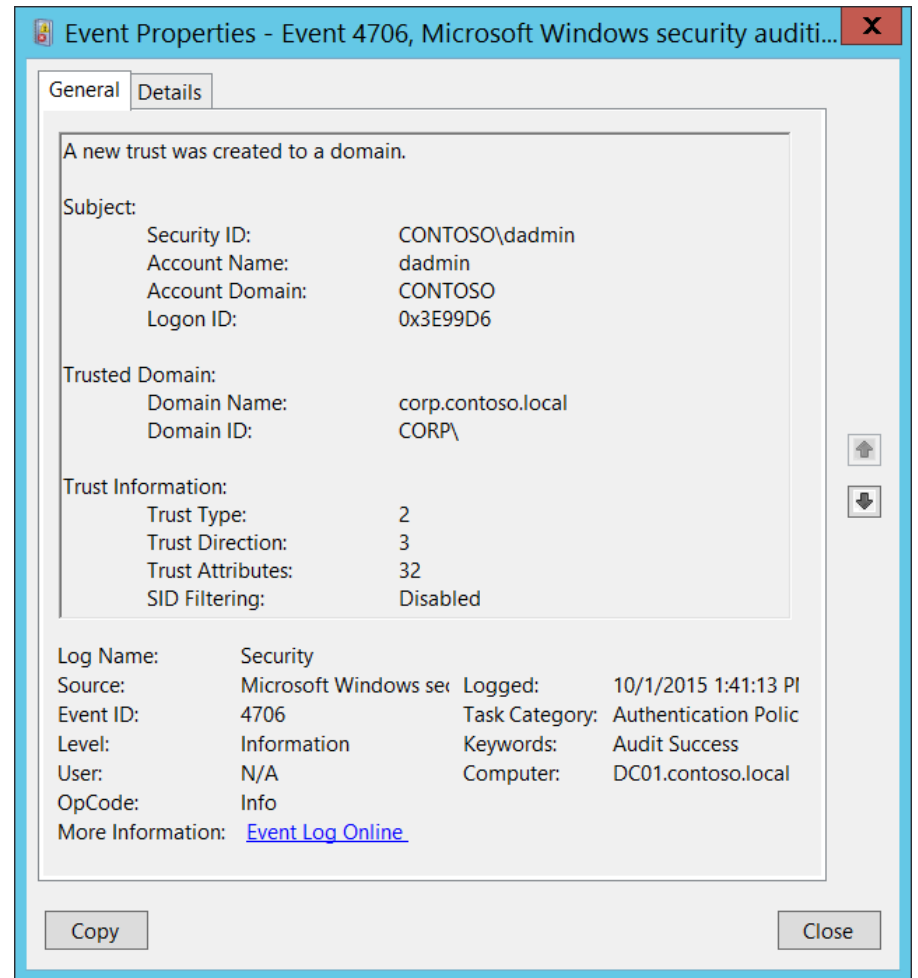
Article • 09/07/2021 • 1 contributor

**Subcategory:** [Audit Authentication Policy Change](#)

## **Event Description:**

This event generates when a new trust was created to a domain.

This event is generated only on domain controllers.



See [Security Monitoring Recommendations](#) for this event.

### Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/eventlog">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{5A0C9647-6F4E-4188-B76A-3C7400A5B8A1}" />
  <EventID>4706</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13569</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-10-01T20:41:13.189445500Z" />
  <EventRecordID>1049759</EventRecordID>
```

```
<Correlation />
<Execution ProcessID="500" ThreadID="4900" />
<Channel>Security</Channel>
<Computer>DC01.contoso.local</Computer>
<Security />
</System>
- <EventData>
  <Data Name="DomainName">corp.contoso.local</Data>
  <Data Name="DomainSid">S-1-5-21-2226861337-2836268956-24331
  <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-
  <Data Name="SubjectUserName">dadmin</Data>
  <Data Name="SubjectDomainName">CONTOSO</Data>
  <Data Name="SubjectLogonId">0x3e99d6</Data>
  <Data Name="TdoType">2</Data>
  <Data Name="TdoDirection">3</Data>
  <Data Name="TdoAttributes">32</Data>
  <Data Name="SidFilteringEnabled">%%1796</Data>
</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 domain trust" 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 domain trust" 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."


#### Trusted Domain:


- **Domain Name** [Type = UnicodeString]: the name of new trusted domain.
- **Domain ID** [Type = SID]: SID of new trusted domain. 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.

Trust Information:

- **Trust Type** [Type = UInt32]: the type of new trust. The following table contains possible values for this field:

 Expand table

Value	Attribute Value	Description
1	TRUST_TYPE_DOWNLEVEL	The domain controller of the trusted domain is a computer running an operating system earlier than Windows 2000.
2	TRUST_TYPE_UPLEVEL	The domain controller of the trusted domain is a computer running Windows 2000 or later.
3	TRUST_TYPE_MIT	The trusted domain is running a non-Windows, RFC4120-compliant Kerberos distribution. This type of trust is distinguished in that (1) a <a href="#">SID</a> is not required for the <a href="#">TDO</a> , and (2) the default key types include the DES-CBC and DES-CRC encryption types (see <a href="#">[RFC4120]</a>  section 8.1).
4	TRUST_TYPE_DCE	The trusted domain is a DCE realm. Historical reference, this value is not used in Windows.

- **Trust Direction** [Type = UInt32]: the direction of new trust. The following table contains possible values for this field:

 Expand table

Value	Attribute Value	Description
-------	-----------------	-------------

0	TRUST_DIRECTION_DISABLED	The trust relationship exists, but it has been disabled.
1	TRUST_DIRECTION_INBOUND	The trusted domain trusts the primary domain to perform operations such as name lookups and authentication.
2	TRUST_DIRECTION_OUTBOUND	The primary domain trusts the trusted domain to perform operations such as name lookups and authentication.
3	TRUST_DIRECTION_BIDIRECTIONAL	Both domains trust one another for operations such as name lookups and authentication.

- **Trust Attributes** [Type = UInt32]: the decimal value of attributes for new trust. You need convert decimal value to hexadecimal and find it in the table below. The following table contains possible values for this field:

 Expand table

Value	Attribute Value	D
0x1	TRUST_ATTRIBUTE_NON_TRANSITIVE	If b d t tr in se >
0x2	TRUST_ATTRIBUTE_UPLEVEL_ONLY	If o a lir o

0x4	TRUST_ATTRIBUTE_QUARANTINED_DOMAIN	If q o P
0x8	TRUST_ATTRIBUTE_FOREST_TRANSITIVE	If fc d a o O 2 S V s o 2 V s C fc le g
0x10	TRUST_ATTRIBUTE_CROSS_ORGANIZATION	If d o b se 3 O 2 S V S C fc le g
0x20	TRUST_ATTRIBUTE_WITHIN_FOREST	If d O

		21 Si W Si
0x40	TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL	If tc e: Fi st TI tr tr e: se O 21 Si W Si O O h. TI C fc le g
0x80	TRUST_ATTRIBUTE_USES_RC4_ENCRYPTION	TI tr w H st ( at cc sc vi re se O




0x200	TRUST_ATTRIBUTE_CROSS_ORGANIZATION_NO_TGT_DELEGATION	If the domain trust is set to O2V
0x400	TRUST_ATTRIBUTE_PIM_TRUST	If a trust is MSH, P, E2, E, h, TI, C, tr, fu, D, g

- **SID Filtering** [Type = UnicodeString]: [SID Filtering](#) state for the new trust:
  - Enabled
  - Disabled



## Security Monitoring Recommendations

For 4706(S): A new trust was created to a domain.

- Any changes related to Active Directory domain trusts (especially creation of the new trust) must be monitored and alerts should be triggered. If this change was not planned, investigate the reason for the change.

 English (United States)

 Your Privacy Choices


 Theme 

[Manage cookies](#)


[Previous Versions](#)

[Blog](#) 

[Contribute](#)

[Privacy](#) 

[Terms of Use](#)

[Trademarks](#) 

© Microsoft 2024