



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

Microsoft Ignite

Nov 19–22, 2024

Register now >



Learn

Discover >

Product documentation >

Development languages >

Topics >



Sign in

ⓘ 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](#)



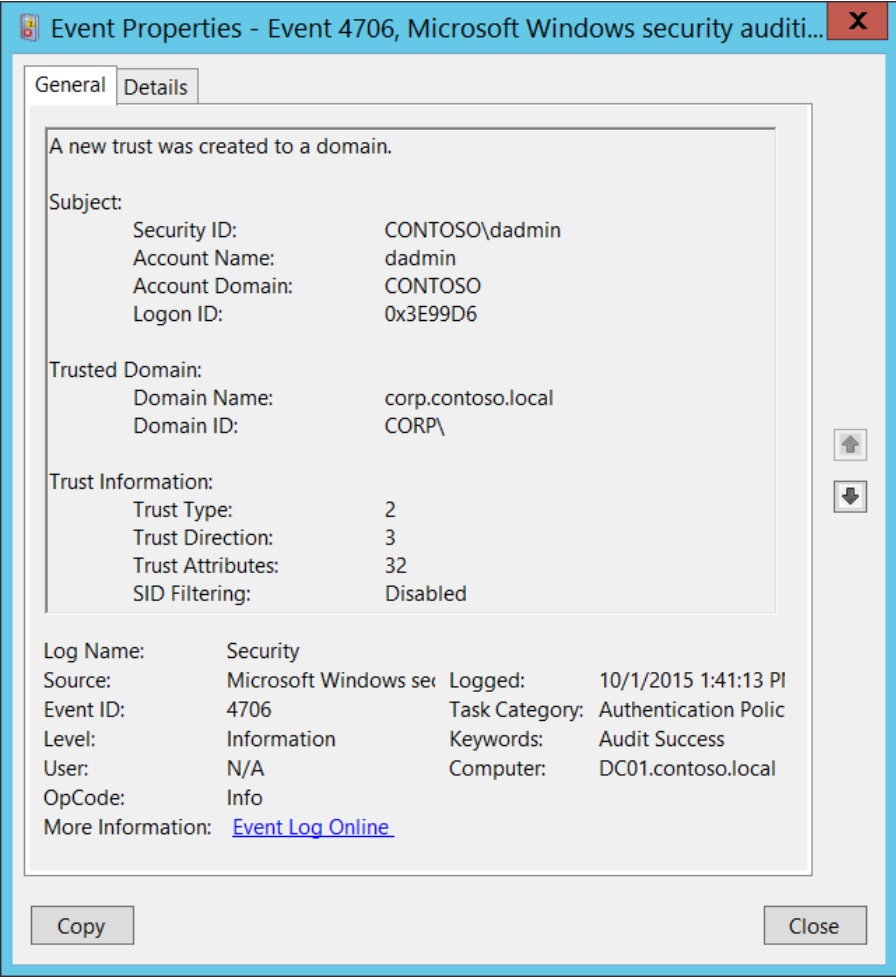
Filter by title

... / [Audit Authentication Policy Change](#) /



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.

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-B3E1-40855A19EE40}" />
  <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 />
```

Auditing
File System (Global Object Access
Auditing)
Windows security

```
<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-1-5-21-2226861337-2836268956-2433141405</Data>  
  <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">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 SID is not required for the TDO , and (2) the default key types include the DES-CBC and DES-CRC encryption types (see [RFC4120] [↗] 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	Description
0x1	TRUST_ATTRIBUTE_NON_TRANSITIVE	If this bit is set, then the trust relationship cannot be used transitively. For example, if domain A trusts domain B, and domain B, in turn trusts domain C, and the trust relationship from A to C has this attribute set, then a user in domain A cannot authenticate to a server in domain C over the trust relationship >C trust linkage.
0x2	TRUST_ATTRIBUTE_UPLEVEL_ONLY	If this bit is set in the attribute value, then only Windows 2000 or later domain controllers and newer clients may use the trust relationship.

		link. Netlogon does not con objects that have this flag se
0x4	TRUST_ATTRIBUTE_QUARANTINED_DOMAIN	If this bit is set, the trusted quarantined and is subject t of SID Filtering as described PAC] section 4.1.2.2 .
0x8	TRUST_ATTRIBUTE_FOREST_TRANSITIVE	If this bit is set, the trust lin forest trust [MS-KILE] betwe domains of two forests , bot are running in a forest funct of DS_BEHAVIOR_WIN2003 Only evaluated on Windows 2003 operating system, Wir Server 2008 operating syste Windows Server 2008 R2 of system, Windows Server 20 operating system, Windows 2012 R2 operating system, Windows Server 2016 oper system. Can only be set if forest and forest are running in a fores level of DS_BEHAVIOR_WIN. greater.
0x10	TRUST_ATTRIBUTE_CROSS_ORGANIZATION	If this bit is set, then the tru domain or forest that is not organization . The behavior c by this bit is explained in [M section 3.3.5.7.5 and [MS-A 3.1.5 . Only evaluated on Windows 2003, Windows Server 2008 Server 2008 R2, Windows S Windows Server 2012 R2, a Server 2016. Can only be set if forest and forest are running in a fores level of DS_BEHAVIOR_WIN. greater.
0x20	TRUST_ATTRIBUTE_WITHIN_FOREST	If this bit is set, then the tru domain is within the same f Only evaluated on Windows 2003, Windows Server 2008 Server 2008 R2, Windows S Windows Server 2012 R2, a Server 2016.
0x40	TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL	If this bit is set, then a cross to a domain is to be treated external trust for the purpo Filtering. Cross-forest trusts stringently filtered than exte This attribute relaxes those trusts to be equivalent to ex trusts. For more informatior each trust type is filtered, se section 4.1.2.2 . Only evaluated on Windows 2003, Windows Server 2008 Server 2008 R2, Windows S Windows Server 2012 R2, a Server 2016. Only evaluated if SID Filterir Only evaluated on cross-for having TRUST_ATTRIBUTE_FOREST_ Can only be set if forest and forest are running in a fores

		level of DS_BEHAVIOR_WIN greater.
0x80	TRUST_ATTRIBUTE_USES_RC4_ENCRYPTION	This bit is set on trusts with trustType set to TRUST_TYP which are capable of using F Historically, MIT Kerberos di supported only DES and 3D ([RFC4120] , [RFC3961] , adopted the RC4HMAC enc common to Windows 2000 so trusted domains deployir versions of the MIT distribu required this bit. For more ii see "Keys and Trusts", sectic Only evaluated on TRUST_T
0x200	TRUST_ATTRIBUTE_CROSS_ORGANIZATION_NO_TGT_DELEGATION	If this bit is set, tickets grant this trust MUST NOT be tru: delegation. The behavior co this bit is as specified in [MS section 3.3.5.7.5. Only supported on Window 2012, Windows Server 2012 Windows Server 2016.
0x400	TRUST_ATTRIBUTE_PIM_TRUST	If this bit and the TATE bit a a cross-forest trust to a dor treated as Privileged Identit; Management trust for the p SID Filtering. For more infor how each trust type is filter PAC section 4.1.2.2. Evaluated only on Windows 2016 Evaluated only if SID Filterin Evaluated only on cross-fore having TRUST_ATTRIBUTE_FOREST_ Can be set only if the forest trusted forest are running ir functional level of DS_BEHAVIOR_WINTHRESH greater.

- **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.