⊙ 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   ✕
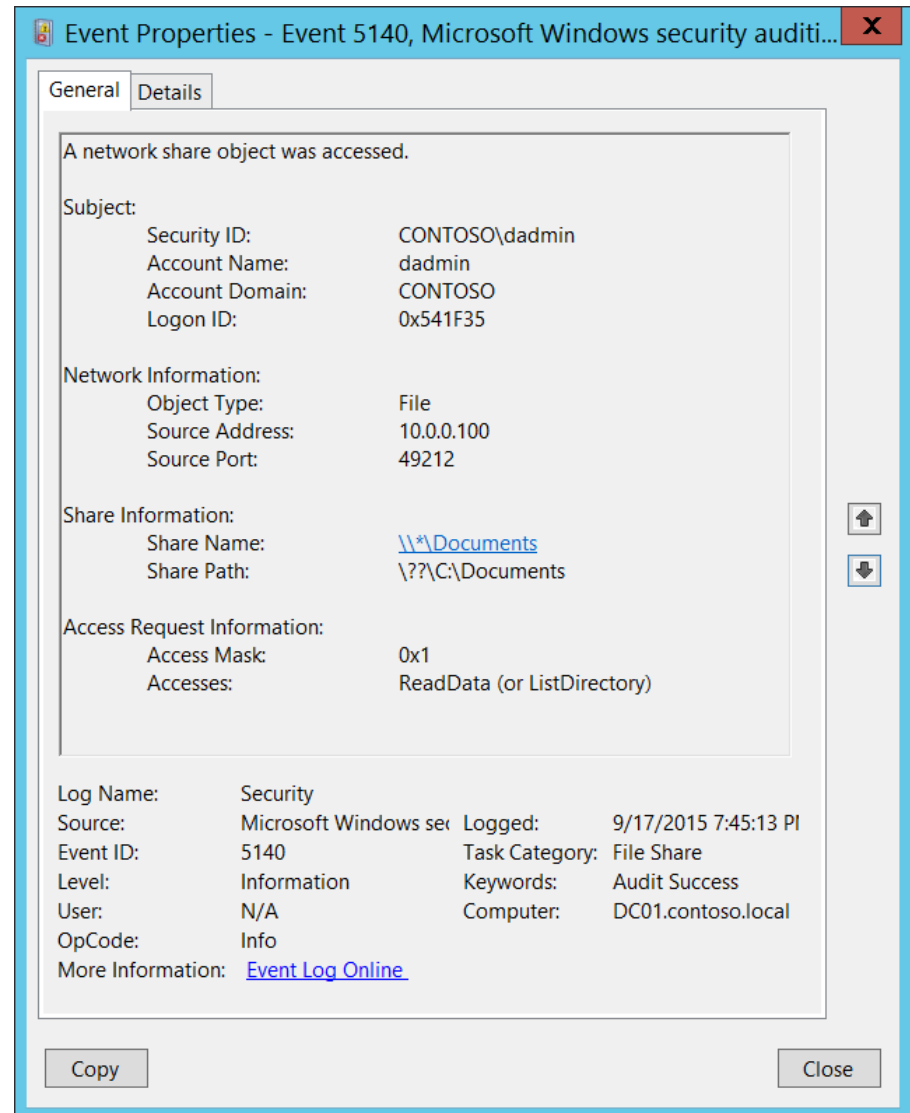
⊕   ⋮

5140(S, F): A network share object was accessed.

Article • 09/08/2021 • 1 contributor

Subcategory: Audit File Share

Event Description:

This event generates every time network share object was accessed.

This event generates once per session, when first access attempt was made.

```
Event Properties - Event 5140, Microsoft Windows security auditi...    X

General   Details

A network share object was accessed.

Subject:
        Security ID:           CONTOSO\dadmin
        Account Name:          dadmin
        Account Domain:        CONTOSO
        Logon ID:              0x541F35

Network Information:
        Object Type:           File
        Source Address:        10.0.0.100
        Source Port:           49212

Share Information:
        Share Name:            \\*\Documents
        Share Path:            \??\C:\Documents

Access Request Information:
        Access Mask:           0x1
        Accesses:              ReadData (or ListDirectory)


Log Name:       Security
Source:         Microsoft Windows se  Logged:        9/17/2015 7:45:13 PI
Event ID:       5140               Task Category:  File Share
Level:          Information        Keywords:       Audit Success
User:           N/A                Computer:       DC01.contoso.local
OpCode:         Info
More Information:   Event Log Online

        Copy                                                Close
```

Note

For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/eve
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid='
 <EventID>5140</EventID>
 <Version>1</Version>
 <Level>0</Level>
 <Task>12808</Task>
 <Opcode>0</Opcode>
```

```
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-09-18T02:45:13.581231400Z" />
<EventRecordID>268495</EventRecordID>
<Correlation />
<Execution ProcessID="4" ThreadID="772" />
<Channel>Security</Channel>
<Computer>DC01.contoso.local</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-
<Data Name="SubjectUserName">dadmin</Data>
<Data Name="SubjectDomainName">CONTOSO</Data>
<Data Name="SubjectLogonId">0x541f35</Data>
<Data Name="ObjectType">File</Data>
<Data Name="IpAddress">10.0.0.100</Data>
<Data Name="IpPort">49212</Data>
<Data Name="ShareName">\\\\\*\\Documents</Data>
<Data Name="ShareLocalPath">\\??\\C:\\Documents</Data>
<Data Name="AccessMask">0x1</Data>
<Data Name="AccessList">%%4416</Data>
</EventData>
</Event>
```

Required Server Roles: None.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions:

- 0 - Windows Server 2008, Windows Vista.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]: SID of account that requested access to network share object. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID can't be resolved, you'll 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 access to network share object.

- **Account Domain** [Type = UnicodeString]: subject's domain or computer name. Formats vary, and include the following ones:

  - 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."

Network Information:

- **Object Type** [Type = UnicodeString]: The type of an object that was accessed during the operation. Always "**File**" for this event.

  The following table contains the list of the most common **Object Types**:

  ⛶ **Expand table**

Directory	Event	Timer	Device
Mutant	Type	File	Token
Thread	Section	WindowStation	DebugObject
FilterCommunicationPort	EventPair	Driver	IoCompletion
Controller	SymbolicLink	WmiGuid	Process
Profile	Desktop	KeyedEvent	Adapter
Key	WaitablePort	Callback	Semaphore
Job	Port	FilterConnectionPort	ALPC Port

- **Source Address** [Type = UnicodeString]: source IP address from which access was performed.

  - IPv6 address or ::ffff:IPv4 address of a client.

  - ::1 or 127.0.0.1 means localhost.

- **Source Port** [Type = UnicodeString]: source TCP or UDP port that was used from remote or local machine to request the access.
  - 0 for local access attempts.

Share Information:

- **Share Name** [Type = UnicodeString]: the name of accessed network share. The format is: *\SHARE_NAME.

- **Share Path** [Type = UnicodeString]: the full system (NTFS) path for accessed share. The format is: \\??\PATH. Can be empty, for

example for **Share Name**: *\IPC$.

Access Request Information:

- **Access Mask** [Type = HexInt32]: the sum of hexadecimal values of requested access rights. See Table of file access codes for different hexadecimal values for access rights. It always has "**0x1**" value for this event.

- **Accesses** [Type = UnicodeString]: the list of access rights that were requested by **Subject\Security ID**. These access rights depend on **Object Type**. Has always "**ReadData (or ListDirectory)**" value for this event.

Security Monitoring Recommendations

For 5140(S, F): A network share object was accessed.

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

- If you have high-value computers for which you need to monitor all access to all shares or specific shares ("**Share Name**"), monitor this event. For example, you could monitor share **C$** on domain controllers.

- Monitor this event if the **Network Information\Source Address** isn't from your internal IP range.

- Monitor this event if the **Network Information\Source Address** shouldn't be able to connect with the specific computer (**Computer:**).

- If you need to monitor access attempts to local shares from a specific IP address ("**Network Information\Source Address**"), use this event.

- If you need to monitor for specific Access Types (for example, ReadData or WriteData), for all or specific shares ("**Share Name**"), monitor this event for the "**Access Type**."

🌐 **English (United States)**   ✓✗ **Your Privacy Choices**   ☀ **Theme** ⌄