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

⌄ Security auditing

  Security auditing

  › Basic security audit policies

  ⌄ Advanced security audit policies

    Advanced security audit policies

    Planning and deploying advanced security audit policies

  ⌄ Advanced security auditing FAQ

    Advanced security auditing FAQ

⊕   ⋮

4964(S): Special groups have been assigned to a new logon.

Article • 09/08/2021 • 1 contributor

Subcategory: Audit Special Logon

Event Description:

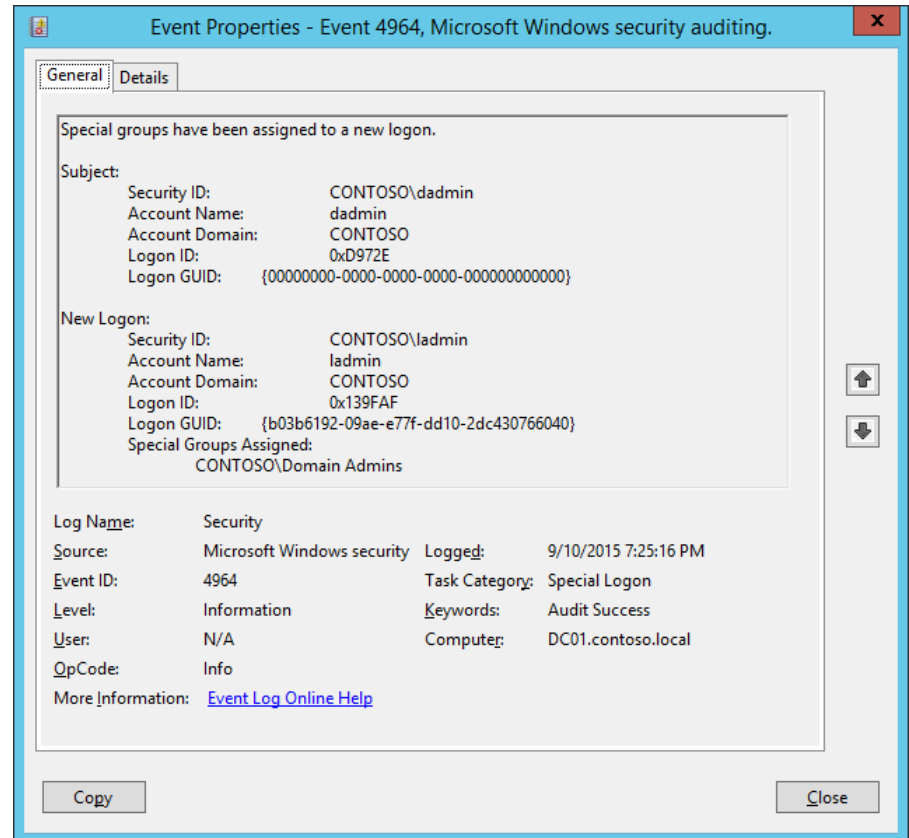This event occurs when an account that is a member of any defined Special Group ⧉ logs in.

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

Which editions of
Windows support
advanced audit policy
configuration

How to list XML elements
in \<EventData>

> Using advanced security
auditing options to

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/eve
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid='
<EventID>4964</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12548</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-09-11T02:25:16.236443300Z" />
<EventRecordID>238923</EventRecordID>
<Correlation />
<Execution ProcessID="504" ThreadID="5008" />
<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">0xd972e</Data>
<Data Name="LogonGuid">{00000000-0000-0000-0000-00000000000
<Data Name="TargetUserSid">S-1-5-21-3457937927-2839227994-8
<Data Name="TargetUserName">ladmin</Data>
<Data Name="TargetDomainName">CONTOSO</Data>
<Data Name="TargetLogonId">0x139faf</Data>
<Data Name="TargetLogonGuid">{B03B6192-09AE-E77F-DD10-2DC43
<Data Name="SidList">%{S-1-5-21-3457937927-2839227994-82386
</EventData>
</Event>
```

Required Server Roles: None.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions: 0.

> **Note** Special Groups is a new feature in Windows Vista and in Windows Server 2008. The Special Groups feature lets the administrator find out when a member of a certain group logs on to the computer. The Special Groups feature lets an administrator set a list of group security identifiers (SIDs) in the registry.

> To add Special Groups perform the following actions:

> 1. Open Registry Editor.

> 2. Locate and then click the following registry subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit

> 3. On the Edit menu, point to New, and then click String Value.

> 4. Type SpecialGroups, and then press ENTER.

> 5. Right-click SpecialGroups, and then click Modify.

> 6. In the Value date box, type the group SIDs, and then click OK.

> A semicolon character (;) can be used to delimit the SID list. For example, you can use the following string that contains a semicolon to delimit two SIDs:

> S-1-5-32-544;S-1-5-32-123-54-65

> For more information see: https://blogs.technet.com/b/askds/archive/2008/03/11/special-groups-auditing-via-group-policy-preferences.aspx ⃗

Field Descriptions:

Subject:

- **Security ID** [Type = SID]: SID of account that requested logon for **New Logon** account. 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 logon for **New Logon** account.

- **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."

- **Logon GUID** [Type = GUID]: a GUID that can help you correlate this event with another event that can contain the same **Logon GUID**, "4769(S, F): A Kerberos service ticket was requested event on a domain controller.

  It also can be used for correlation between a 4964 event and several other events (on the same computer) that can contain the same **Logon GUID**, "4648(S): A logon was attempted using explicit credentials" and "4624(S): An account was successfully logged on."

  This parameter might not be captured in the event, and in that case appears as "{00000000-0000-0000-0000-000000000000}".

> **Note** GUID is an acronym for 'Globally Unique Identifier'. It is a 128-bit integer number used to identify resources, activities or instances.

New Logon:

- **Security ID** [Type = SID]: SID of account that performed the logon. 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.

- **Account Name** [Type = UnicodeString]: the name of the account that performed the logon.

- **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."

- **Logon GUID** [Type = GUID]: a GUID that can help you correlate this event with another event that can contain the same **Logon GUID**, "4769(S, F): A Kerberos service ticket was requested event on a domain controller.

  It also can be used for correlation between a 4964 event and several other events (on the same computer) that can contain the same **Logon GUID**, "4648(S): A logon was attempted using

explicit credentials" and "4624(S): An account was successfully logged on."

This parameter might not be captured in the event, and in that case appears as "{00000000-0000-0000-0000-000000000000}".

- **Special Groups Assigned** [Type = UnicodeString]: the list of special group SIDs, which **New Logon\Security ID** is a member of.

Security Monitoring Recommendations

For 4964(S): Special groups have been assigned to a new logon.

- Generally speaking, every 4964 event should be monitored, because the purpose of Special Groups is to define a list of critical or important groups (Domain Admins, Enterprise Admins, service account groups, and so on) and trigger an event every time a member of these groups logs on to a computer. For example, you can monitor for every Domain Administrators logon to a non-administrative workstation.

English (United States)   Your Privacy Choices   ☼ Theme ⌄

Manage cookies   Previous Versions   Blog ⊡   Contribute   Privacy ⊡   Terms of Use   Trademarks ⊡

© Microsoft 2024