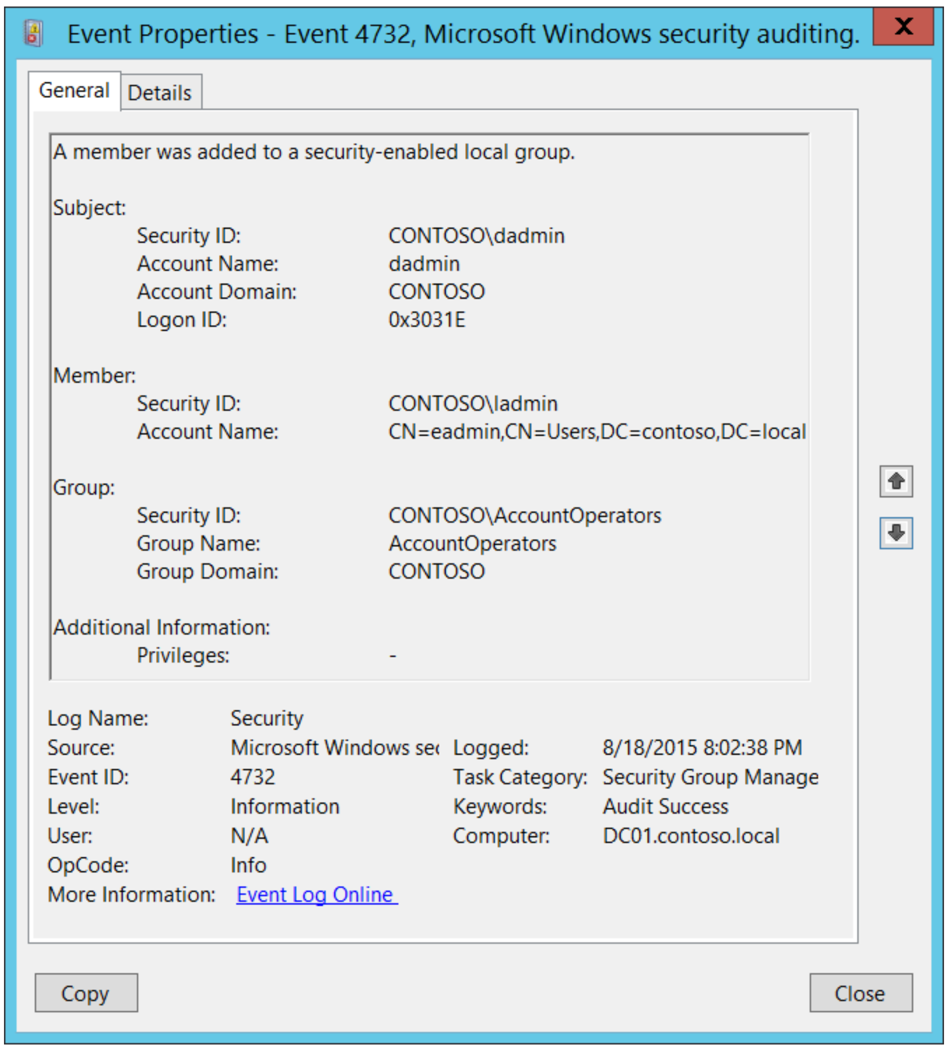
We're no longer updating this content regularly. Check the Microsoft Product Lifecycle for information about how this product, service, technology, or API is supported.

Return to main site

4732(S): A member was added to a security-enabled local group.

Article • 09/07/2021 • 1 contributor



```
Event Properties - Event 4732, Microsoft Windows security auditing.

General  Details

A member was added to a security-enabled local group.

Subject:
        Security ID:            CONTOSO\dadmin
        Account Name:           dadmin
        Account Domain:         CONTOSO
        Logon ID:               0x3031E

Member:
        Security ID:            CONTOSO\ladmin
        Account Name:           CN=eadmin,CN=Users,DC=contoso,DC=local

Group:
        Security ID:            CONTOSO\AccountOperators
        Group Name:             AccountOperators
        Group Domain:           CONTOSO

Additional Information:
        Privileges:             -

Log Name:         Security
Source:           Microsoft Windows se   Logged:          8/18/2015 8:02:38 PM
Event ID:         4732                   Task Category:   Security Group Manage
Level:            Information            Keywords:        Audit Success
User:             N/A                    Computer:        DC01.contoso.local
OpCode:           Info
More Information: Event Log Online

Copy                                                                  Close
```

Subcategory: Audit Security Group Management

Event Description:

This event generates every time a new member was added to a security-enabled (security) local group.

This event generates on domain controllers, member servers, and workstations.

For every added member you will get separate 4732 event.

You will typically see "4735: A security-enabled local group was changed." event without any changes in it prior to 4732 event.

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

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-
 <EventID>4732</EventID>
```

› Audit Filtering Platform Packet Drop

› Audit Handle Manipulation

› Audit Kernel Object

```
 <Version>0</Version>
 <Level>0</Level>
 <Task>13826</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-08-19T03:02:38.563110400Z" />
 <EventRecordID>174856</EventRecordID>
 <Correlation />
 <Execution ProcessID="512" ThreadID="1092" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="MemberName">CN=eadmin,CN=Users,DC=contoso,DC=local</Data>
 <Data Name="MemberSid">S-1-5-21-3457937927-2839227994-823803824-500</Data>
 <Data Name="TargetUserName">AccountOperators</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="TargetSid">S-1-5-21-3457937927-2839227994-823803824-6605</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">0x3031e</Data>
 <Data Name="PrivilegeList">-</Data>
 </EventData>
 </Event>
```

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 "add member to the group" 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 "add member to the group" 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."

Member:

- **Security ID** [Type = SID]**:** SID of account that was added to the group. Event Viewer automatically tries to resolve SIDs and show the group name. If the SID cannot be resolved, you will see the source data in the event.
- **Account Name** [Type = UnicodeString]: distinguished name of account that was added to the group. For example: "CN=Auditor,CN=Users,DC=contoso,DC=local". For local groups this field typically has "-" value, even if new member is a domain account. For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "-".

> **Note** The LDAP API references an LDAP object by its **distinguished name (DN)**. A DN is a sequence of relative distinguished names (RDN) connected by commas.
>
> An RDN is an attribute with an associated value in the form attribute=value; . These are examples of RDNs attributes:
>
> • DC - domainComponent
>
> • CN - commonName
>
> • OU - organizationalUnitName
>
> • O - organizationName

Group:

- **Security ID** [Type = SID]**:** SID of the group to which new member was added. Event Viewer automatically tries to resolve SIDs and show the group name. If the SID cannot be resolved, you will see the source data in the event.
- **Group Name** [Type = UnicodeString]**:** the name of the group to which new member was added. For example: ServiceDesk
- **Group Domain** [Type = UnicodeString]: domain or computer name of the group to which the new member was added. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For a local group, this field will contain the name of the computer to which this new group belongs, for example: "Win81".
  - Built-in groups: Builtin

Additional Information:

- **Privileges** [Type = UnicodeString]: the list of user privileges which were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as "-". See full list of user privileges in "Table 8. User Privileges.".

Security Monitoring Recommendations

For 4732(S): A member was added to a security-enabled local group.

Expand table

Type of monitoring required	Recommendation
Addition of members to local or domain security groups: You might need to monitor the addition of members to local or domain security groups.	If you need to monitor each time a member is added to a local or domain security group, to see who added the member and when, monitor this event. Typically, this event is used as an informational event, to be reviewed if needed.
High-value local or domain security groups: You might have a list of critical local or domain security groups in the organization, and need to specifically monitor these groups for the addition of new members (or for other changes). Examples of critical local or domain groups are built-in local administrators group, domain admins, enterprise admins, and so on.	Monitor this event with the "**Group\Group Name**" values that correspond to the high-value local or domain security groups.
High-value accounts: You might have high-value domain or local accounts for which you need to monitor each action. Examples of high-value accounts are database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts and so on.	Monitor this event with the "**Subject\Security ID**" and "**Member\Security ID**" that correspond to the high-value account or accounts.
Anomalies or malicious actions: You might have specific requirements for detecting anomalies or monitoring potential malicious actions. For example, you might need to monitor for use of an account outside of working hours.	When you monitor for anomalies or malicious actions, use the "**Subject\Security ID**" (with other information) to monitor how or when a particular account is being used.
Non-active accounts: You might have non-active, disabled, or guest accounts, or other accounts that should never be used.	Monitor this event with the "**Subject\Security ID**" and "**Member\Security ID**" that correspond to the accounts that should never be used.
Account allowlist: You might have a specific allowlist of accounts that are the only ones allowed to perform actions corresponding to particular events.	If this event corresponds to an "allowlist-only" action, review the "**Subject\Security ID**" for accounts that are outside the allowlist.
Accounts of different types: You might want to ensure that certain actions are performed only by certain account types, for example, local or domain account, machine or user account, vendor or employee account, and so on.	If this event corresponds to an action you want to monitor for certain account types, review the "**Subject\Security ID**" to see whether the account type is as expected.
External accounts: You might be monitoring accounts from another domain, or "external" accounts that are not allowed to perform certain actions (represented by certain specific events).	Monitor this event for the "**Subject\Account Domain**" corresponding to accounts from another domain or "external" accounts.
Restricted-use computers or devices: You might have certain computers, machines, or devices on which certain people (accounts) should not typically perform any actions.	Monitor the target **Computer:** (or other target device) for actions performed by the "**Subject\Security ID**" that you are concerned about.
Account naming conventions: Your organization might have specific naming conventions for account names.	Monitor "**Subject\Account Name**" for names that don't comply with naming conventions.
Mismatch between type of account (user or computer) and the group it was added to: You might want to monitor to ensure that a computer account was not added to a group intended for users, or a user account was not added to a group intended for computers.	Monitor the type of account added to the group to see if it matches what the group is intended for.