

October 2024 "Patch Tuesday - Five User name Password: Login / Forgot?

Security Log	Window	s SharePoint	SQL Server	Exchange	1	Training	Tools	Newsletter	Webinars	Blog
Webinars	Training	Encyclopedia	Quick Reference	Book						

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy



Security Log Quick Reference Chart



Windows Security Log Event ID 4728 >

4728: A member was added to a securityenabled global group

On this page

- Description of this event
- Field level details
- Examples

The user in Subject: added the user/group/computer in Member: to the Security Global group in Group:.

Operating Systems Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022 Category Account Management Subcategory Security Group Management Success Type Corresponding events 632 in Windows 2003 and before

In Active Directory Users and Computers "Security Enabled" groups are simply referred to as Security groups. AD has 2 types of groups: Security and Distribution. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Security (security enabled) groups can be used for permissions, rights and as distribution lists.

Global means the group can be granted access in any trusting domain but may only have members from its own domain.

This event is only logged on domain controllers.

Server 2016 adds the "Expiration time" field in version 2 of this event.

Free Security Log Resources by Randy

- Free Security Log Quick Reference Chart
- Windows Event Collection: Supercharger Free Edtion
- Free Active Directory Change Auditing Solution
- Free Course: Security Log Secrets

Description Fields in 4728

Subject:

The user and logon session that performed the action.

- Security ID: The SID of the account.
- Account Name: The account logon name.
- Account Domain: The domain or in the case of local accounts computer name.
- Logon ID is a semi-unique (unique between reboots) number that identifies the logon session. Logon ID allows you to correlate backwards to the logon event (4624) as well as with other events logged during the same logon session.

Member:

- Security ID: The SID of the group's member
- Account Name: The distinguished name of the group's member

Group:

- Security ID: The SID of the affected group
- Group Name: Name of affected group
- Group Domain: Domain of affected group

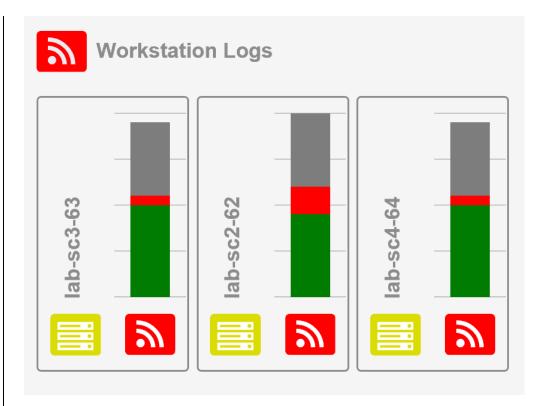
Additional Information:

- Privileges: always "-"
- Expiration time: (2016 and later)

Supercharger Enterprise

Load Balancing for Windows Event Collection

Cookies help us deliver the best experience on our website. By using our website, you agree to the use of cookies.



Examples of 4728

Windows 10 and 2016+

```
An account was successfully logged on.
A member was added to a security-enabled global group.
Subject:
   Security ID: ACME\Administrator
   Account Name: Administrator
   Account Domain: ACME
   Logon ID: 0x27a79
Member:
   Security ID: ACME\gkhan
   Account Name: cn=Ghenghis Khan, CN=Users, DC=acme, DC=local
Group:
   Security ID: S-1-5-21-3108364787-189202583-342365621-1108
   Group Name: Historical Figures
   Group Domain: ACME
Additional Information:
   Privileges: -
Expiration time:
```

Windows 2012r2

```
An account was successfully logged on.
A member was added to a security-enabled global group.
Subject:
   Security ID: ACME\Administrator
  Account Name: Administrator
  Account Domain: ACME
  Logon ID: 0x27a79
Member:
  Security ID: ACME\gkhan
  Account Name: cn=Ghenghis Khan, CN=Users, DC=acme, DC=local
Group:
   Security ID: S-1-5-21-3108364787-189202583-342365621-1108
   Group Name: Historical Figures
  Group Domain: ACME
Additional Information:
   Privileges: -
```

Top 10 Windows Security Events to Monitor

Free Tool for Windows Event Collection

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventlD=4728

- Security Log Deep Dive: Mapping Active Directory Authentication and Account Management Events to MITRE ATT&CK TTPs
- Assessing the Security of Your Active Directory: User Accounts
- Assessing Your Active Directory: Group Related Risks

Upcoming Webinars

Additional Resources







A bout | New sletter | Contact Ultimate IT Security is a division of Monterey Technology Group, Inc. ©2006-2024 Monterey Technology Group, Inc. All rights reserved.

Disclaimer: We do our best to provide quality information and expert commentary but use all information at your own risk. For complaints, please contact abuse@ultimatewindowssecurity.com.

Terms of Use | Privacy