



October 2024
Patch Tuesday

"Patc

User name:
Password:
 / [Forgot?](#)
[Register](#)

[Security Log](#) [Windows](#) [SharePoint](#) [SQL Server](#) [Exchange](#) | [Training](#) [Tools](#) [Newsletter](#) [Webinars](#) [Blog](#)
[Webinars](#) [Training](#) [Encyclopedia](#) [Quick Reference](#) [Book](#)

Encyclopedia

- [Event IDs](#)
- [All Event IDs](#)
- [Audit Policy](#)

Go To Event ID:

[Security Log
Quick Reference
Chart](#)



[Download now!](#)

← Windows Security Log Event ID 4729 →

4729: A member was removed from a security-enabled global group

On this page

- [Description of this event](#)
- [Field level details](#)
- [Examples](#)

The user in Subject: removed the user/group/computer in Member: from the Security Global group in Group:.

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.

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
Type	Success
Corresponding events in Windows 2003 and before	633

Free Security Log Resources by Randy

- [Free Security Log Quick Reference Chart](#)
- [Windows Event Collection: Supercharger Free Edition](#)
- [Free Active Directory Change Auditing Solution](#)
- [Free Course: Security Log Secrets](#)

Description Fields in 4729

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

- Privileges: always "-"

Supercharger Free Edition

test on lab-2008r2-77 ? x

1

2

3

4

5

DescriptionPolicyAllowed ForwardersFiltersSubmit

Collector Domain: lab.local

Add

Name

Included

Delete

domain computers

Included

< Previous

Next >

Centrally manage WEC subscriptions.

Free.

Examples of 4729

A member was removed from 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](#)

Mini-Seminars Covering Event ID 4729

- [Monitoring Active Directory for Security and Compliance: How Far Does the Native Audit Log Take You?](#)
- [Building a Security Dashboard for Your Senior Executives](#)
- [Detecting Compromised Privileged Accounts with the Security Log](#)
- [Real Methods for Detecting True Advanced Persistent Threats Using Logs](#)
- [Monitoring Group Membership Changes in Active Directory](#)
- [Tracking Group Membership Changes in Active Directory](#)
- [Auditing Active Directory Changes with the Windows Security Log](#)
- [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](#)

Upcoming Webinars

Additional Resources

[Tweet](#) [Follow @randyfsmith](#)

[About](#) | [Newsletter](#) | [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](#)