



Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID:

Go

Security Log
Quick Reference
Chart



Download now!

Windows Security Log Event ID 634

634: Security Enabled Global Group Deleted

On this page

- Description of this event
- Field level details
- Examples

Security global group deletedType:

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.

Scope:

AD has 3 scopes of groups: Local, Global, Universal. See knowledge base article 326265.

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 634

- Target Account Name: %1
- Target Domain: %2
- Target Account ID: %3
- Caller User Name: %4
- Caller Domain: %5
- Caller Logon ID: %6
- Privileges: %7

Supercharger Free Edition

View Managed Filter

1

2

3

4

5

Name

Events

Noise

Custom

Summary

Builtin - Security: with Noise Suppression

1<QueryList><Query Id="0" Path="Security"><Select Path="Security">*</Select>

2<Suppress Path="Security">*[System[EventID=4688]] and *[EventData[Data[@Name='SubjectI

3Data[@Name='NewProcessName'] = 'C:\Windows\System32\SearchFilterHost.exe'

4or Data[@Name='NewProcessName'] = 'C:\Windows\SysWOW64\SearchProtocolHost.exe'

5or Data[@Name='NewProcessName'] = 'C:\Windows\System32\SearchProtocolHost.exe'

6or Data[@Name='NewProcessName'] = 'C:\Windows\System32\backgroundTaskHost.exe'

7or Data[@Name='NewProcessName'] = 'C:\Windows\System32\conhost.exe'

8or Data[@Name='NewProcessName'] = 'C:\Windows\System32\wbem\WmiPrvSE.exe'

9or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskhost.exe'

10or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskeng.exe'

11or Data[@Name='NewProcessName'] = 'C:\Windows\System32\svchost.exe'

12or Data[@Name='NewProcessName'] = 'C:\Windows\System32\sc.exe'

13or Data[@Name='NewProcessName'] = 'C:\Windows\System32\rundll32.exe'

14or Data[@Name='NewProcessName'] = 'C:\Windows\System32\taskhost.exe'

15]]</Suppress><Suppress Path="Security">*[System[EventID=4769]] and *[EventData[Data

16or (*[System[EventID=4770]])

17or (*[System[EventID=4624]] and *[EventData[Data[@Name='LogonType'] = '3']])

18or (*[System[EventID=4634]] and *[EventData[Data[@Name='LogonType'] = '3']])

19</Suppress> </Query></QueryList>

< Previous

Next >

Supercharger's built-in Xpath filters leave the noise behind.

Free.

Examples of 634

Security Enabled Global Group Deleted:
Target Account Name:AccountingStaff
Target Domain:ELMW2
Target Account ID:AccountingStaff
Caller User Name:Administrator
Caller Domain:ELMW2
Caller Logon ID: (0x0,0x12D622)
Privileges:-

[Top 10 Windows Security Events to Monitor](#)

[Free Tool for Windows Event Collection](#)

Mini-Seminars Covering Event ID 634

- [Monitoring Active Directory for Security and Compliance: How Far Does the Native Audit Log Take You?](#)

Upcoming Webinars

Additional Resources

 Share

 Post

 Follow @randyfsmith