Windows Security Log Event ID 4670

Archived: 2026-04-05 16:11:36 UTC

4670: Permissions on an object were changed

On this page

Windows logs this event when someone changes the access control list on an object. The event identifies the object, who changed the permissions and the old an new permissions.

Of course the object's audit policy must have auditing enabled for "Write DAC"/"Change Permissions" or "Take Ownership" permissions for the user who just modified this object's access control list or a group to which the user belongs.

Also, this event is logged based on the status of the Object Access subcategory - not the status of "Authorization Policy Change" subcategory. For instance to log this event for file permission changes, the "File System" subcategory must be enabled for success.

Note the following problem is fixed in more recent versions of Windows. Definitely in Windows 8/2012. Not sure about Win7 and Win2008R2: This event has been observed as above after deleting an access control entry from the file's ACL. However the event was not logged after simply blocking permission inheritance and copying existing ACEs. Evidently this event is only logged when the effective permissions are changed not inheritance settings.

This event is NOT logged when Active Directory object permissions are changed.

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 4670

Subject:

The user and logon session that changed permissions of the object.

- 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.

Object:

This is the object whose permissions were changed.

- Object Server: always "Security"
- Object Type: "File" for file or folder but can be other types of objects such as Key, SAM, SERVICE OBJECT, etc.
- Object Name: The name of the object being accessed
- Handle ID: is a semi-unique (unique between reboots) number that identifies all subsequent audited events while the object is open. Handle ID allows you to correlate to other events logged (Open 4656, Access 4663, Close 4658)

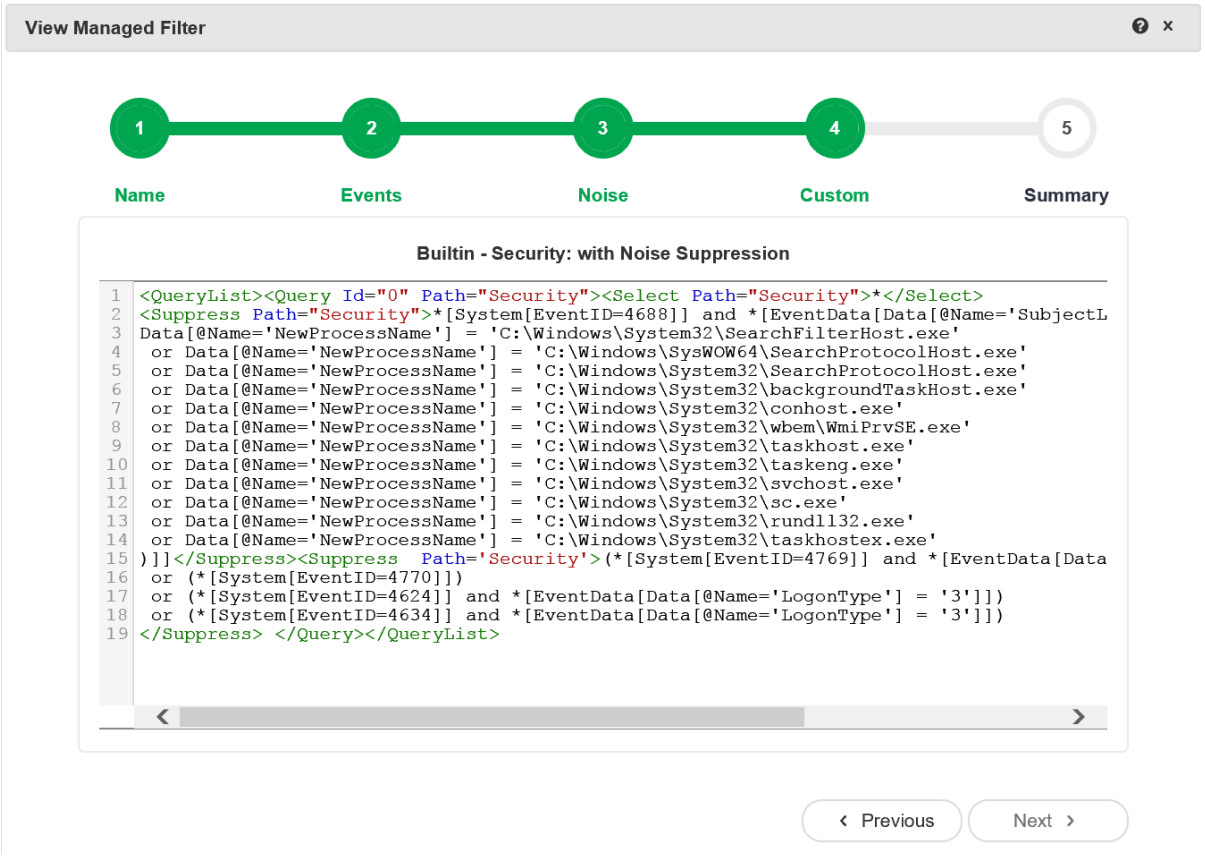
Process Information:

- Process Name: Identifies the program executable that accessed the object.
- Process ID: The process ID specified when the executable started as logged in 4688.

Permissions Change:

- Original Security Descriptor: The old ACL of the object in SDDL format (Security Descriptor Definition Language). See http://msdn2.microsoft.com/en-us/library/aa379567.aspx
- New Security Descriptor: The new ACL of the object in SDDL format (Security Descriptor Definition Language)

Supercharger Free Edition



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

Free.

Examples of 4670

File System example:

Permissions on an object were changed.

Subject:

Security ID: WIN-R9H529RIO4Y\Administrator
Account Name: Administrator
Account Domain: WIN-R9H529RIO4Y
Logon ID: 0x1fd23

Object:

Object Server: Security
Object Type: File
Object Name: C:\Users\Administrator\testfolder\New Text Document.txt
Handle ID: 0x564

Process:

Process ID: 0x8c0
Process Name: C:\Windows\explorer.exe

Permissions Change:

Original Security Descriptor: D:PAI(A;;FA;;;LA)(A;;FA;;;SY) (A;;FA;;;BA)
New Security Descriptor: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)

Registry key example:

Permissions on an object were changed.

Subject:

Security ID: ACME\administrator
Account Name: administrator
Account Domain: ACME
Logon ID: 0x176293

Object:

Object Server: Security
Object Type: Key
Object Name: \REGISTRY\MACHINE\SOFTWARE\MTG
Handle ID: 0x2c8

Process:

Process ID: 0x7e0
Process Name: C:\Windows\regedit.exe

Permissions Change:

Original Security Descriptor: D:AI(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)

New Security Descriptor: D:ARAI(A;CI;KA;;;WD)(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)
