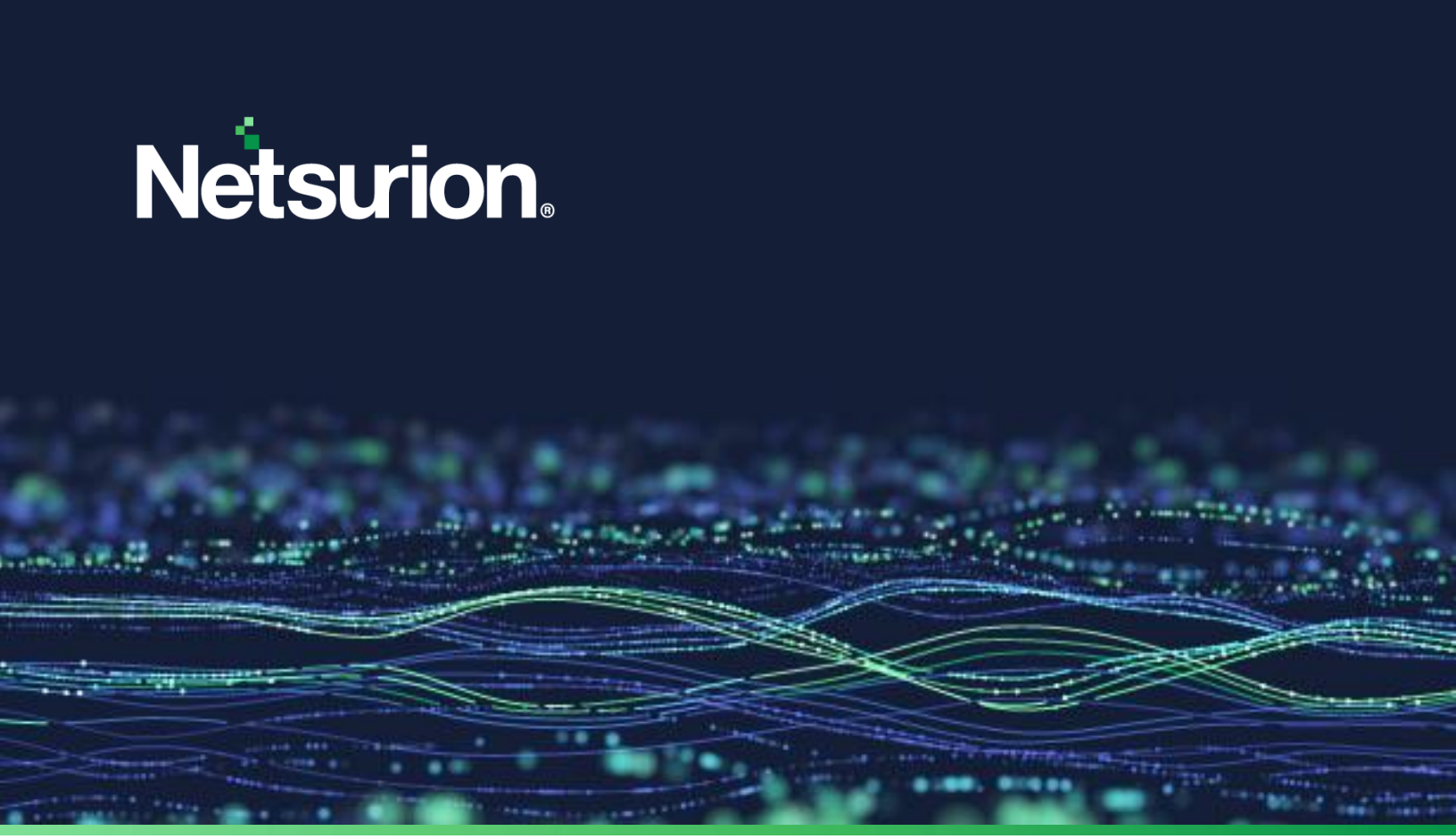

How-To Guide

Configure Advanced Audit Policy for Windows

Publication Date:

June 15, 2023

Abstract

This document describes audit settings available in Windows Server 2008 onwards and Windows 7 onwards and audit events that they generate.

The security audit policy settings under Security Settings\Advanced Audit Policy Configuration can help organizations audit compliance with important business-related and security-related rules by tracking precise defined activities, such as:

- A group administrator has modified settings or data on servers that contain financial information.
- An employee within a defined group has accessed an important file.
- The correct System Access Control List (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access.

These settings allow selecting only the behavior, you want to monitor and exclude audit results for other behaviors. In addition, security audit policies can be applied by using domain group policy, audit policy settings can be modified, tested, and deployed to selected users and groups.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.4 or later.

Audience

Users and system administrators, who want to deploy the Netsurion Open XDR sensors.

Table of Contents

1. Account Logon

1.1 Audit Credential Validation (Enable/Enable)

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events on credentials submitted for a user account logon request.

These events occur on the computer that is authoritative for the credentials:

- For domain accounts, the domain controller is authoritative.
- For local accounts, the local computer is authoritative.

Event volume: High on domain controllers.

Because domain accounts are used frequently than local accounts in enterprise environments, most of the account logon events in a domain environment occur on the domain controllers that are authoritative for the domain accounts. However, these events can occur on any computer, and they may occur in conjunction with or on separate computers from logon/logoff events.

Default: Not configured.

Event ID	Event Message
4774	An account was mapped for logon.
4775	An account could not be mapped for logon.
4776	The domain controller attempted to validate the credentials for an account.
4777	The domain controller failed to validate the credentials for an account

Credential Validation	Enable	Enable

1.2 Audit Kerberos Authentication Service

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to generate audit events for Kerberos authentication ticket-granting ticket (TGT) requests.

If you configure this policy setting, an audit event is generated after a Kerberos authentication TGT request. Success audits record successful attempts and failure audits record unsuccessful attempts.

Event volume: High on Kerberos Key Distribution Center servers.

Default: Not configured.

Event ID	Event Message
4768	4768 A Kerberos authentication ticket (TGT) was requested.
4771	4771 Kerberos pre-authentications failed.
4772	4772 A Kerberos authentication ticket request failed

Kerberos Authentication Service	Enable	Enable

1.3 Account Logon - Audit Kerberos Service Ticket Operations

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates security audit events for Kerberos service ticket requests. Events are generated every time Kerberos is used to authenticate a user to access a protected network resource.

Kerberos service ticket operation audit events can be used to track user activity.

Event volume:

- High on a domain controller that is a Key Distribution Center (KDC).
- Low on domain members.

Default: Not configured

Event ID	Event Message
4769	A Kerberos service ticket was requested.
4770	A Kerberos service ticket was renewed.

Kerberos Service Ticket Operations	Enable	Enable

1.4 Audit Other Account Logon Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows to audit events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets. Examples can include the following:

- Remote Desktop session disconnections.
- New Remote Desktop sessions.
- Locking and unlocking a workstation.
- Invoking a screen saver.
- Dismissing a screen saver.
- Detection of a Kerberos replay attack, in which a Kerberos request with identical information was received twice.

NOTE: This condition could be caused by a network misconfiguration.

- Access to a wireless network granted to a user or computer account.
- Access to a wired 802.1x network granted to a user or computer account.

Event volume: Varies, depending on system use.

Default: Not configured.

Event ID	Event Message
4649	A replay attack was detected.
4778	A session was reconnected to a Window Station.
4779	A session was disconnected from a Window Station.
4800	The workstation was locked.
4801	The workstation was unlocked.
4802	The screen saver was invoked.
4803	The screen saver was dismissed.
5378	The requested credentials delegation was disallowed by policy.
5632	A request was made to authenticate to a wireless network.
5633	A request was made to authenticate to a wired network.

Other Account Logon Events	Enable	Enable

2. Account Management

2.1 Application Group Management

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when application group management tasks are performed, such as:

- An application group is created, changed, or deleted.
- A member is added to or removed from an application group.

Event volume: Low.

Default: Not configured.

Event ID	Event Message
4783	A basic application group was created.
4784	A basic application group was changed.
4785	A member was added to a basic application group.
4786	A member was removed from a basic application group.
4787	A non-member was added to a basic application group.
4788	A non-member was removed from a basic application group.
4789	A basic application group was deleted.
4790	An LDAP query group was created.

Application Group Management	Enable	Enable

2.2 Computer Account Management

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when a computer account is created, changed, or deleted. This policy setting is useful for tracking account-related changes to computers that are members of a domain.

Event volume: Low.

Default: Not configured.

Event ID	Event Message
4741	A computer account was created.
4742	A computer account was changed.
4743	A computer account was deleted

Computer Account Management	Enable	Enable

2.3 Distribution Group Management

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events for the following distribution group management tasks:

- A distribution group is created, changed, or deleted.
- A member is added to or removed from a distribution group.

Event volume: Low.

Default: Not configured.

This subcategory is logged only on domain controllers.

Note: Supported Operating Systems : Windows 2008 R2 onwards and Windows 7 onwards

Event ID	Event Message
4744	A security-disabled local group was created.
4745	A security-disabled local group was changed.
4746	A member was added to a security-disabled local group.
4747	A member was removed from a security-disabled local group.
4748	A security-disabled local group was deleted.
4749	A security-disabled global group was created.
4750	A security-disabled global group was changed.
4751	A member was added to a security-disabled global group.
4752	A member was removed from a security-disabled global group.
4753	A security-disabled global group was deleted.
4759	A security-disabled universal group was created.
4760	A security-disabled universal group was changed.
4761	A member was added to a security-disabled universal group.
4762	A member was removed from a security-disabled universal group.

Distribution Group Management	Enable	Enable

2.4 Audit Other Account Management Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates user account management audit events when:

- The password hash of an account is accessed. This typically happens when the Active Directory Migration Tool (ADMT) is moving password data.
- The password policy checking Application Programming Interface (API) is called. Calls to this function could be part of an attack from a malicious application that is testing whether password complexity policy settings are being applied.

- Changes are made to domain policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy or Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy.

Event volume: Low.

Default: Not configured.

Event ID	Event Message
4782	The password hash for an account was accessed.
4793	The Password Policy Checking API was called

Other Account Management Events	Enable	Enable

2.5 Security Group Management

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when any of the following security group management tasks are performed:

- A security group is created, changed, or deleted.
- A member is added to or removed from a security group.
- A group's type is changed.

Event volume: Low.

Default: Success.

Event ID	Event Message
4727	4727 A security-enabled global group was created.
4728	4728 A member was added to a security-enabled global group.
4729	A member was removed from a security-enabled global group.
4730	A security-enabled global group was deleted.

4731	4731 A security-enabled local group was created.
4732.	4732 A member was added to a security-enabled local group.
4733	A member was removed from a security-enabled local group.
4734	A security-enabled local group was deleted.
4735	A security-enabled local group was changed.
4737	A security-enabled global group was changed.
4754	A security-enabled universal group was created.
4755	A security-enabled universal group was changed.
4756	A member was added to a security-enabled universal group.
4757	A member was removed from a security-enabled universal group.
4758	A security-enabled universal group was deleted.
4764	A group's type was changed.

Security Group Management	Enable	Enable

2.6 User Account Management

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when the following user account management tasks are performed:

- A user account is created, changed, deleted, renamed, disabled, enabled, locked out, or unlocked.
- A user account password is set or changed.
- Security identifier (SID) history is added to a user account.
- The Directory Services Restore Mode password is set.
- Permissions on accounts that are members of the administrator's groups are changed.
- Credential Manager credentials are backed up or restored.

This policy setting is essential for tracking events that involve provisioning and managing user accounts.

Event volume: Low.

Default: Success.

Event ID	Event Message
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.
4725	A user account was disabled.
4726	A user account was deleted.
4738	A user account was changed.
4740	A user account was locked out.
4765	SID History was added to an account.
4766	An attempt to add SID History to an account failed.
4767	A user account was unlocked.
4780	The ACL was set on accounts which are members of administrator groups.
4781	The name of an account was changed
4794	An attempt was made to set the Directory Services Restore Mode.
5376	Credential Manager credentials were backed up
5377	Credential Manager credentials were restored from a backup

User Account Management	Enable	Enable

3. Detailed Tracking

3.1 DPAPI Activity

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when encryption or decryption calls are made into the Data Protection Application Interface (DPAPI), which is used to protect secret information such as stored passwords and key information.

Event volume: Low

Default: Not configured

Event ID	Event Message
4692	Backup of data protection master key was attempted.
4693	The recovery of the data protection master key was attempted.
4694	The protection of auditable protected data was attempted.
4695	Unprotection of auditable protected data was attempted.

DPAPI Activity	Disable	Disable

3.2 Process Creation

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when a process is created (starts) and the name of the program or user that created it.

These audit events can help you understand how a computer is being used and to track user activity.

Event volume: Low – Medium (Varies on System Usage)

Default: Not configured.

Event ID	Event Message
4688	A new process has been created.
4696	A primary token was assigned to a process.

Process Creation	Enable	Enable

3.3 Process Termination

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows generating audit events when an attempt is made to end a process.

Success audits record successful attempts and Failure audits record unsuccessful attempts.

If you do not configure this policy setting, no audit event is generated when a process ends.

These audit events can help you understand how a computer is being used and to track user activity.

Event volume: Low – Medium (Varies on System Usage)

Default: Not configured.

Event ID	Event Message
4689	A process has exited

Process Termination	Enable	Enable

3.4 RPC Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when Inbound Remote Procedure Call (RPC) connections are made.

Event volume: High on RPC Servers.

Default: Not configured.

Event ID	Event Message
5712	A Remote Procedure Call (RPC) was attempted.

RPC Events	Enable	Enable

4. DS Access

DS Access security audit policy settings provide a detailed audit trail of attempts to access and modify objects in Active Directory Domain Services (AD DS). These audit events are logged only on domain controllers.

4.1 Detailed Directory Service Replication.

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting can be used to generate security audit events with detailed tracking information about the data that is replicated between domain controllers. This audit subcategory can be useful to diagnose replication issues.

Event volume: Very High.

Default: Not configured.

Event ID	Event Message
4928	An Active Directory replica source naming context was established.
4929	An Active Directory replica source naming context was removed.
4930	An Active Directory replica source naming context was modified.
4931	An Active Directory replica destination naming context was modified.
4934	Attributes of an Active Directory object were replicated.
4935	Replication failure begins.
4936	Replication failure ends.
4937	A lingering object was removed from a replica.

Detailed Directory Service Replication	Disable	Disable

4.2 Directory Service Access

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates events when an Active Directory Domain Services (AD DS) object is accessed.

NOTE: Audit events will only be generated on objects with configured system access control lists (SACLs), and only when they are accessed in a manner that matches the SACL settings.

These events are like the Directory Service Access events in previous versions of Windows Server operating systems.

Event volume: High on servers running AD DS role services; none on client computers.

Default: Not configured.

Event ID	Event Message
4662	An operation was performed on an object.

Directory Service Access	Enable	Enable

4.3 Directory Service Changes

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when changes are made to objects in Active Directory Domain Services (AD DS). The type of changes that are reported are:

- Create
- Delete
- Modify
- Move
- Undelete

Directory Service Changes auditing, where appropriate, indicates the old and new values of changed properties of the objects that were changed.

NOTE:

Audit events are generated only for objects with configured System Access Control Lists (SACLs), and only when they are accessed in a manner that matches their SACL settings. Some objects and properties do not cause an audit to be generated due to settings on the object class in the schema.

This subcategory only logs events on domain controllers. Changes to Active Directory objects are important events to track and understand the state of the network policy.

Event volume: High (DC's); No Events on clients.

Default: Not configured.

Event ID	Event Message
5136	A directory service object was modified.
5137	A directory service object was created.
5138	A directory service object was undeleted.
5139	A directory service object was moved.
5141	A directory service object was deleted.

Directory Service Changes	Enable	Enable

4.4 Directory Service Replication

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when replication between two domain controllers begins and ends.

Event volume: Medium (DC's); No Events on clients.

Default: Not configured.

Event ID	Event Message
5136	A directory service object was modified.
5137	A directory service object was created.

Directory Service Replication	Disable	Disable

5. Logon / Logoff

Logon/Logoff security policy settings and audit events allow you to track attempts to log on to a computer interactively or over a network. These events are particularly useful for tracking user activity and identifying potential attacks on network resources.

5.1 Account Lockout

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to audit security events generated by a failed attempt to log on to an account that is locked out.

If you configure this policy setting, an audit event is generated when an account cannot log on to a computer because the account is locked out. Success audits record successful attempts and failure audits record unsuccessful attempts.

Account lockout events are essential for understanding user activity and detecting potential attacks.

Event ID	Event Message
4625	An account failed to logon.

Account lockout	Enable	Enable

5.2 IPsec Extended Mode

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events for the results of the Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations.

Event volume: High

Default: Not configured.

Event ID	Event Message
4978	During the Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
4979	IPsec Main Mode and Extended Mode security associations were established. This event provides event data in the following categories: Main Mode Local Endpoint, Main Mode Remote Endpoint, Main Mode Cryptographic Information, Main Mode Security Association, Main Mode Additional Information, and Extended Mode Information.
4980	IPsec Main Mode and Extended Mode security associations were established. This event provides event data in the following categories: Main Mode Local Endpoint, Main Mode Remote Endpoint, Main Mode Cryptographic Information, Main Mode Security Association, Main Mode Additional Information, and Extended Mode Local Endpoint, Extended Remote Endpoint, and Extended Mode Additional Information.
4981	IPsec Main Mode and Extended Mode security associations were established. This event provided event audit data in the following categories: Local Endpoint Local Certificate, Remote Endpoint, Remote Certificate, Cryptographic Information, Security Association Information, Additional Information, and Extended Mode Information.
4982	IPsec Main Mode and Extended Mode security associations were established. This event provided event audit data in the following categories: Local Endpoint Local Certificate, Remote Endpoint, Remote Certificate, Cryptographic Information, Security Association Information, Additional Information, and Extended Mode Local Endpoint, Extended Mode Remote Endpoint, and Extended Mode Additional Information.
4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. This event provided event audit data in the following categories: Local Endpoint Local Certificate, Remote Endpoint, Remote Certificate, and Failure Information.
4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. This event provided event audit data in the following categories: Local Endpoint Local Certificate, Remote Endpoint, Additional Information, and Failure Information

IPsec Extended Mode	Disable	Disable

5.3 IPsec Main Mode

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates events for the results of the Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.

Event volume: High

Default: Not configured

Event ID	Event Message
4646	Security ID: %1
4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
4652	An IPsec Main Mode negotiation failed. NOTE: This event provided event audit data in the following categories: Local Endpoint, Local Certificate, Remote Endpoint, Remote Certificate, Additional Information, and Failure Information.
4653	An IPsec Main Mode negotiation failed. NOTE: This event provided event audit data in the following categories: Local Endpoint, Remote Endpoint, Additional Information, and Failure Information.
4655	An IPsec Main Mode security association ended
4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
5049	An IPsec Security Association was deleted.
5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service are not started.

IPsec Main Mode	Disable	Disable

5.4 IPsec Quick Mode

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates events for the results of the Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.

Event volume: High

Default: Not configured

Event ID	Event Message
4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
5451	An IPsec Quick Mode security association was established.
5452	An IPsec Quick Mode security association ended

IPsec Quick Mode	Disable	Disable

5.5 Account Logoff

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when logon sessions are terminated. These events occur on the computer that was accessed. In the case of an interactive logon, these would be generated on the computer that was logged on to.

NOTE:

There is no failure event in this subcategory because failed logoffs (such as when a system abruptly shuts down) do not generate an audit record.

Logon events are essential to understanding user activity and detecting potential attacks. Logoff events are not 100 percent reliable. For example, the computer can be turned off without a proper logoff and shutdown taking place; in this case, a logoff event will not be generated.

Event volume: Low

Default: Success

Event ID	Event Message
4634	An account was logged off. (Link back to 4624 – Logon ID)
4647	User initiated logoff. (For Interactive / Remote Interactive)

Also, refer to Event ID 4647 which Windows logs instead of this event in the case of interactive logons when the user logs out.

This event signals the end of a logon session and can be correlated back to the logon event 4624 using the Logon ID.

For network connections (such as to a file server), it will appear that users log on and off many times a day. This phenomenon is caused by the way the Server service terminates idle connections.

If a user turns off his/her computer, Windows does not have an opportunity to log the logoff event until the system restarts. Therefore, some logoff events are logged much later than the time at which they occur.

ANONYMOUS LOGONs are routine events on Windows networks.

Microsoft's comments:

This event does not necessarily indicate the time that a user has stopped using a system. For example, if the computer is shut down or loses network connectivity it may not record a logoff event at all.

Account Logoff	Enable	Enable

5.6 Account Logon

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when a user attempts to log on to a computer. These events are related to the creation of logon sessions and occur on the computer that was accessed. For an interactive logon, events are generated on the computer that was logged on to. For network logon, such as accessing a share, events are generated on the computer hosting the resource that was accessed.

The following events are recorded:

- Logon success and failure.

- Logon attempts by using explicit credentials. This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the Runas command.
- Security identifiers (SIDs) are filtered.

Logon events are essential for tracking user activity and detecting potential attacks.

Event volume: Low (client computer); Medium (DC's and N/W Server)

Default: Success for client computers; success and failure for servers.

Event ID	Event Message
4624	An account was successfully logged on.
4625	An account failed to log on.
4648	A logon was attempted using explicit credentials.
4675	SIDs were filtered.

Account Logon	Enable	Enable

5.7 Network Policy Server (NPS)

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events for RADIUS (IAS) and Network Access Protection (NAP) activity on user access requests (Grant, Deny, Discard, Quarantine, Lock, and Unlock).

NAP events can be used to understand the overall health of the network.

Event volume: Medium–High (Servers running NPS); Medium on other Servers and client computers.

Default: Success / Failure.

Event ID	Event Message
6272	Network Policy Server granted access to a user.
6273	Network Policy Server denied access to a user.
6274	Network Policy Server discarded the request for a user.
6275	Network Policy Server discarded the accounting request for a user.
6276	Network Policy Server quarantined a user.
6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6278	Network Policy Server granted full access to a user because the host met the defined health policy.
6279	Network Policy Server locked the user account due to repeated failed authentication attempts.
6280	Network Policy Server unlocked the user account.

Network Policy Server	Enable	Enable

5.8 Other Logon/Logoff Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether Windows generates audit events for other logon or logoff events, such as:

- A Remote Desktop session disconnects or connects.
- A workstation is locked or unlocked.
- A screen saver is invoked or dismissed.
- A replay attack is detected. This event indicates that a Kerberos request was received twice with identical information. This condition could also be caused by network misconfiguration.
- A user is granted access to a wireless network. It can either be a user account or the computer account.
- A user is granted access to a wired 802.1x network. It can either be a user account or the computer account.

Logon events are essential to understand user activity and detect potential attacks.

Event volume: Low Windows

Windows Default: Not Configured

Event ID	Event Message
4649	A replay attack was detected.
4778	A session was reconnected to a window station.
4779	A session was disconnected from a Window Station.
4800	The workstation was locked.
4801	The workstation was unlocked.
4802	The screen saver was invoked.
4803	The screen saver was dismissed.
5378	The requested credentials delegation was disallowed by policy.
5632	A request was made to authenticate to a wireless network.
5633	A request was made to authenticate to a wired network.

Other Logon/Logoff Events	Enable	Enable

5.9 Special Logon

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when:

- A special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level.
- A member of a special group logs on. Special Groups is a Windows feature that enables the administrator to find out when a member of a certain group has logged on. The administrator can set a list of group security identifiers (SIDs) in the registry. If any of these SIDs is added to a token during logon and this auditing subcategory is enabled, a security event is logged. For more information about this feature, refer article 947223 in the Microsoft Knowledge Base.

Users holding special privileges can potentially make changes to the system. It is recommended to track their activity.

Event volume: Low

Default: Success

Event ID	Event Message
4964	Special groups have been assigned to new logon.

Special Logon	Enable	Enable

6. Object Access

Object Access policy settings and audit events allow you to track attempts to access specific objects or types of objects on a network or computer. To audit attempts to access a file, directory, registry key, or any other object, you must enable the appropriate Object Access auditing subcategory for success and/or failure events. For example, the File System subcategory needs to be enabled to audit file operations, and the Registry subcategory needs to be enabled to audit registry accesses. Proving that these audit policies are in effect to an external auditor is even more difficult. There is no easy way to verify that the proper SACLs are set on all inherited objects. To address this issue, refer to Global Object Access Auditing.

6.1 Application Generated

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when applications attempt to use the Windows Auditing application programming interfaces (APIs). The following events can generate audit activity:

- Creation, deletion, and initialization of an application client context.
- Application operations.

Applications designed to use the Windows Auditing APIs can use this subcategory to log auditing events related to their function. The level, volume, relevance, and importance of these audit events depend on the application generating them. The operating system logs the events as they are generated by the application.

Event volume: Varies on installed application's use of Windows Auditing.

Default: Not Configured.

Event ID	Event Message
4665	An attempt was made to create an application client context.
4666	An application attempted an operation.
4667	An application client context was deleted.
4668	An application was initialized.

Application Generated	Enable	Enable

6.2 Certification Services

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates events when Active Directory Certificate Services (AD CS) operations are performed, such as:

- AD CS starts, shuts down, is backed up, or is restored.
- Certificate revocation list (CRL)-related tasks are performed.
- Certificates are requested, issued, or revoked.
- Certificate manager settings for AD CS are changed.
- The configuration and properties of the certification authority (CA) are changed.
- AD CS templates are modified.
- Certificates are imported.
- A CA certificate is published to Active Directory Domain Services.
- Security permissions for AD CS role services are modified.
- Keys are archived, imported, or retrieved.
- The OCSP Responder Service is started or stopped.

Monitoring these operational events is important to ensure that AD CS role services are functioning properly.

Event volume: Low - Medium on servers hosting AD CS role services.

Default: Not Configured.

Event ID	Event Message
4877	Certificate Services backup completed.
4878	Certificate Services restore started.
4879	Certificate Services restore completed.
4880	Certificate Services started.
4881	Certificate Services stopped
4882	The security permissions for Certificate Services changed.
4883	Certificate Services retrieved an archived key.
4884	Certificate Services imported a certificate into its database.
4885	The audit filter for Certificate Services changed.
4886	Certificate Services received a certificate request.
4887	Certificate Services approved a certificate request and issued a certificate.
4888	Certificate Services denied a certificate request.
4889	Certificate Services set the status of a certificate request to pending.
4890	The certificate manager settings for Certificate Services changed.
4891	A configuration entry changed in Certificate Services.
4892	A property of Certificate Services changed.
4893	Certificate Services archived a key.
4894	Certificate Services imported and archived a key.
4895	Certificate Services published the CA certificate to Active Directory Domain Services.
4896	One or more rows have been deleted from the certificate database.
4897	Role separation enabled.
4898	Certificate Services loaded a template.

Certification Services	Enable	Enable

6.3 Detailed File Share

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows to audit attempts to access files and folders on a shared folder. The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection established between a client computer and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.

NOTE: There are no system access control lists (SACLs) for shared folders. If this policy setting is enabled, access to all shared files and folders on the system is audited.

Event volume: High on File Servers / DC due to SYSVOL n/w access required by Group Policy.

Default: Not Configured.

Event ID	Event Message
5145	A network share object was checked to see whether the client can be granted desired access.

Detailed File Share	Disable	Disable

6.4 File Share

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when a file share is accessed.

Audit events are not generated when shares are created, deleted, or when share permissions change.

NOTE: There are no system access control lists (SACLs) for shares; therefore, once this setting is enabled, access to all shares on the system will be audited.

Combined with File System auditing, File Share auditing allows you to track what content was accessed, the source (IP address and port) of the request, and the user account used for the access.

Event volume: High on a file server or domain controller (due to SYSVOL access by client computers for policy processing)

Default: Not Configured.

Event ID	Event Message
5140	A network share object was accessed. **NOTE:** Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards
5142	A network share object was added.
5143	A network share object was modified.
5144	A network share object was deleted.

File Share	Enable	Enable

6.5 File System

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits user attempts to access file system objects. Audit events are only generated for objects that have configured system access control lists (SACLs), and only if the type of access requested (such as Write, Read, or Modify) and the account making the request match the settings in the SACL.

If success auditing is enabled, an audit entry is generated each time an account successfully accesses a file system object that has a matching SACL. If failure auditing is enabled, an audit entry is generated each time any user unsuccessfully attempts to access a file system object that has a matching SACL

These events are essential for tracking activity for file objects that are sensitive or valuable and require extra monitoring.

Event volume: Varies, depending on how file system SACLs are configured.

No audit events are generated for the default file system SACLs.

Default: Not Configured.

Event ID	Event Message
4664	An attempt was made to create a hard link.
4985	The state of a transaction has changed.
5051	A file was virtualized.

File System	Enable	Enable

6.6 Filtering Platform

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when connections are allowed or blocked by the Windows Filtering Platform, such as when:

- Windows Firewall service blocks an application from accepting incoming connections on the network.
- Windows Filtering Platform allows or blocks a connection.
- Windows Filtering Platform permits or blocks a bind to a local port.
- Windows Filtering Platform permits or blocks the listening of an application or service on a port for incoming connections.

Event volume: High

Default: Not Configured

Event ID	Event Message
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
5140	A network share object was accessed. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards
5150.	The Windows Filtering Platform blocked a packet.
5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
5156	The Windows Filtering Platform has allowed a connection.
5157	The Windows Filtering Platform has blocked a connection.
5158	The Windows Filtering Platform has permitted a bind to a local port.
5159	The Windows Filtering Platform has blocked a bind to a local port.

Filtering Platform Connection	Disable	Disable

6.7 Filtering Platform Packet Drop

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to audit packets that are dropped by the Windows Filtering Platform.

A high rate of dropped packets may indicate attempts to gain unauthorized access to computers on your network.

Event volume: High

Default setting: Not configured

Event ID	Event Message
5152	Windows Filtering Platform blocked a packet.
5153	A more restrictive Windows Filtering Platform filter has blocked a packet.

Filtering Platform Packet Drop	Disable	Disable

6.8 Handle Manipulation

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when a handle to an object is opened or closed.

Only objects with configured system access control lists (SACLs) generate these events, and only if the attempted handle operation matches the SACL.

NOTE: Handle Manipulation events are only generated for object types where the corresponding File System or Registry Object Access subcategory is enabled. For more information, refer the Audit File System or Audit Registry.

Event volume: High, depending on how SACLs are configured

Default: Not configured

Event ID	Event Message
4656	A handle to an object was requested.
4658	The handle to an object was closed.
4690	An attempt was made to duplicate a handle to an object.

Handle Manipulation	Disable	Disable

6.9 Kernel Object

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching system access control list (SACL) generate security audit events.

NOTE:

The Audit: Audit the access of global system objects policy setting controls the default SACL of kernel objects.

The audits generated are usually only useful to developers.

Typically kernel objects are given SACLs only if the AuditBaseObjects or AuditBaseDirectories auditing options are enabled.

Event volume: High, if you have enabled one of the Global Object Access Auditing settings

Default: Not configured.

Event ID	Event Message
4659	A handle to an object was requested with intent to delete.
4660	An object was deleted.
4661	A handle to an object was requested.
4663	An attempt was made to access an object

Kernel Object	Enable	Enable

6.10 Other Object Access Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events for the management of Task Scheduler jobs or COM+ objects.

For scheduler jobs, the following are audited:

- Job created.
- Job deleted.
- Job enabled.
- Job disabled.
- Job updated.

For COM+ objects, the following are audited:

- Catalog object added.
- Catalog object updated.
- Catalog object deleted.

Event volume: Low.

Default setting: Not configured.

Event ID	Event Message
4671	An application attempted to access a blocked ordinal through the TBS.
4691	Indirect access to an object was requested.
4698	A scheduled task was created.
4699	A scheduled task was deleted.
4700	A scheduled task was enabled.
4701	A scheduled task was disabled.
4702	A scheduled task was updated.

Event ID	Event Message
5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards
5149	The DoS attack has subsided, and normal processing is being resumed. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards
5888	An object in the COM+ Catalog was modified.
5889	An object was deleted from the COM+ Catalog.
5890	An object was added to the COM+ Catalog.

Other Object Access Events	Optional*	Optional*

*If you choose to track Scheduled Tasks through auditing, you can turn this Audit Sub Category on.

6.11 Registry

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits user attempts to access registry objects. Audit events are only generated for objects that have configured system access control lists (SACLs) specified, and only if the type of access requested (such as Write, Read, or Modify) and the account making request match the settings in the SACL.

If success auditing is enabled, an audit entry is generated each time an account successfully accesses a registry object that has a matching SACL. If failure auditing is enabled, an audit entry is generated each time any user unsuccessfully attempts to access a registry object that has a matching SACL.

Event volume: Low – Medium (Depending on SACL configuration)

Default: Not Configured.

Event ID	Event Message
4657	A registry value was modified.
5039	A registry key was virtualized.

Registry	Enable	Enable

6.12 SAM - Security Accounts Manager

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows to audit events generated by attempts to access SAM objects. SAM objects include the following:

- SAM_ALIAS: A local group
- SAM_GROUP: A group that is not a local group
- SAM_USER: A user account SAM_DOMAIN: A domain
- SAM_SERVER: A computer account

If you configure this policy setting, an audit event is generated when a SAM object is accessed. Success audits record successful attempts, and failure audits record unsuccessful attempts.

NOTE:

Only SACL for SAM_SERVER can be modified.

Changes to user and group objects are tracked by the Account Management audit category. However, user accounts with enough privileges could potentially alter the files where the account and password information are stored in the system, bypassing any Account Management events.

Event volume: High on domain controllers.

NOTE: For information about reducing the number of events generated in this subcategory, please refer article 841001 in Microsoft Knowledge Base.

Default: Not Configured

Event ID	Event Message
4659	A handle to an object was requested with intent to delete.
4660	An object was deleted.
4661	A handle to an object was requested.
4663	An attempt was made to access an object.

SAM	Disable	Disable

7. Policy Change

Policy Change audit events allow tracking changes to important security policies on a local system or network. Because policies are typically established by administrators to help secure network resources, any changes or attempts to change these policies can be an important aspect of security management for a network.

7.1 Audit Policy Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when changes are made to audit policy, including:

- Permissions and audit settings on the audit policy object (by using auditpol/set /sd).
- Changing the system audit policy.
- Registration and de-registration of security event sources.
- Changing per-user audit settings.
- Changing the value of CrashOnAuditFail.
- Changing audit settings on an object (for example, modifying the system access control list (SACL) for a file or registry key.)

NOTE:

SACL change auditing is performed when SACL for an object has changed and the Policy Change category is configured. Discretionary access control list (DACL) and owner change auditing are performed when Object Access auditing is configured and the object's SACL is set for auditing of the DACL or owner change.

Changes made to the Special Groups list.

NOTE: Changes to the audit policy are critical security events.

Event volume: Low

Default: Success

Event ID	Event Message
4715	The audit policy (SACL) on an object was changed.
4719	The system audit policy was changed.
4817	Auditing settings on an object were changed. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards
4902	The Per-user audit policy table was created
4904	An attempt was made to register a security event source.
4905	An attempt was made to unregister a security event source.
4906	The CrashOnAuditFail value has changed.
4907	Auditing settings on the object were changed.
4908	Special Groups Logon table modified.
4912	Per the User Audit Policy was changed.

Audit Policy Change	Enable	Enable

7.2 Authentication Policy Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when changes are made to authentication policy, including:

- Creation, modification, and removal of forest and domain trusts. Windows Advanced Audit Policy Configuration
- Changes to Kerberos policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy.

NOTE:

The audit event is logged when the policy is applied, not when settings are modified by the administrator.

When any of the following user rights are granted to a user or group:

- Access this computer from the network

- Allow logon locally
- Allow logon through Remote Desktop
- Logon as a batch job
- Logon as a service
- Namespace collision, such as when an added trust collides with an existing namespace name.

This setting is useful for tracking changes in domain and forest level trust and privileges granted to user accounts or groups.

Event volume: Low

Default: Success

Event ID	Event Message
4713	The Kerberos policy was changed.
4716	Trusted domain information was modified.
4717	System security access was granted to an account.
4718	System security access was removed from an account.
4739	The Domain Policy was changed.
4864	A namespace collision was detected.
4865	A trusted forest information entry was added.
4866	A trusted forest information entry was removed.
4867	A trusted forest information entry was modified

Authentication Policy Change	Enable	Enable

7.3 Authorization Policy Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when the following changes are made to the authorization policy:

- Assigning or removing of user rights (privileges) such as SeCreateTokenPrivilege, except for the system access rights that are audited by using the Audit Authentication Policy Change subcategory.
- Changing the Encrypting File System (EFS) policy.

Event volume: Low

Default: Not configured

Event ID	Event Message
4704	A user right was assigned.
4705	A user right was removed.
4706	A new trust was created to a domain
4707	Trust in a domain was removed.
4714	Encrypted data recovery policy was changed.

Authentication Policy Change	Enable	Enable

7.4 Filtering Platform Policy Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events for:

- IPsec services status.
- Changes to IPsec settings.
- Status and changes to the Windows Filtering Platform engine and providers.
- IPsec Policy Agent service activities.

Event volume: Low

Default: Not configured

Event ID	Event Message
4709	IPsec Services was started.
4710	IPsec Services were disabled.
4711	May contain any one of the following: • PAStore Engine applied a locally cached copy of Active Directory storage IPsec policy on the computer. • PAStore Engine applied Active Directory storage IPsec policy on the computer. • PAStore Engine applied local registry storage IPsec policy on the computer. • PAStore Engine failed to apply a locally cached copy of Active Directory storage IPsec policy on the computer. • PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. • PAStore Engine failed to apply local registry storage IPsec policy on the computer. • PAStore Engine failed to apply some rules of the active IPsec policy on the computer. • PAStore Engine failed to load directory storage IPsec policy on the computer. • PAStore Engine loaded directory storage IPsec policy on the computer. • PAStore Engine failed to load local storage IPsec policy on the computer. • PAStore Engine loaded local storage IPsec policy on the computer. • PAStore Engine polled for changes to the active IPsec policy and detected no changes.
4712	IPsec Services encountered a potentially serious failure.
5040	A change has been made to IPsec settings. An Authentication Set was added.
5041	A change has been made to IPsec settings. An Authentication Set was modified.
5042	A change has been made to IPsec settings. An Authentication Set was deleted.
5043	A change has been made to IPsec settings. A Connection Security Rule was added.

5044	A change has been made to IPsec settings. A Connection Security Rule was modified.
5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.
5046	A change has been made to IPsec settings. A Crypto Set was added.
5448	A Windows Filtering Platform provider has been changed.
5449	A Windows Filtering Platform provider context has been changed.
5450	A Windows Filtering Platform sub-layer has been changed.
5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.
5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
5458	PAStore Engine applied a locally cached copy of Active Directory storage IPsec policy on the computer.
5459	PAStore Engine failed to apply a locally cached copy of Active Directory storage IPsec policy on the computer.
5460	PAStore Engine applied local registry storage IPsec policy on the computer.
5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.
5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.
5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.
5464	PAStore Engine polled for changes to the active IPsec policy detected changes and applied them to IPsec Services.
5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully
5466	PAStore Engine polled for changes to the Active Directory IPsec policy determined that Active Directory cannot be reached and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied

5467	PAStore Engine polled for changes to the Active Directory IPsec policy determined that Active Directory can be reached and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
5468	PAStore Engine polled for changes to the Active Directory IPsec policy determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
5471	PAStore Engine loaded local storage IPsec policy on the computer.
5472	PAStore Engine failed to load local storage IPsec policy on the computer.
5473	PAStore Engine loaded directory storage IPsec policy on the computer.
5474	PAStore Engine failed to load directory storage IPsec policy on the computer.
5477	PAStore Engine failed to add a quick mode filter.

Filtering Platform Policy Change	Disable	Disable

7.5 MPSSVC Rule-Level Policy Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe), which is used by Windows Firewall. The tracked activities include:

- Active policies when the Windows Firewall service starts.
- Changes to Windows Firewall rules.
- Changes to the Windows Firewall exception list.
- Changes to Windows Firewall settings.
- Rules ignored or not applied by the Windows Firewall service.
- Changes to Windows Firewall Group Policy settings.

Changes to firewall rules are important to understand the security state of the computer and how well it is protected against network attacks.

Event volume: Low.

Default: Not configured.

Event ID	Event Message
4944	The following policy was active when the Windows Firewall started.
4945	A rule was listed when the Windows Firewall started.
4946	A change has been made to the Windows Firewall exception list. A rule was added.
4947	A change has been made to the Windows Firewall exception list. A rule was modified.
4948	A change has been made to the Windows Firewall exception list. A rule was deleted.
4949	Windows Firewall settings were restored to the default values.
4950	A Windows Firewall setting has changed.
4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.
4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
4953	A rule has been ignored by Windows Firewall because it could not parse the rule.
4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.
4956	Windows Firewall has changed the active profile
4957	Windows Firewall did not apply the following rule.
4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

MPSSVC Rule-Level Policy Change	Disable	Disable

7.6 Other Policy Change Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system generates events for security policy changes that are not otherwise audited in the Policy Change category, such as the following: • Trusted Platform Module (TPM) configuration changes. • Kernel-mode cryptographic self-tests. • Cryptographic provider operations. • Cryptographic context operations or modifications

Event volume: Low

Default: Not configured

Event ID	Event Message
4670	Permissions on an object were changed.
4909	The local policy settings for the TBS were changed.
4910	The group policy settings for the TBS were changed.
5063	A cryptographic provider operation was attempted.
5064	A cryptographic context operation was attempted.
5065	A cryptographic context modification was attempted.
5066	A cryptographic function operation was attempted.
5067	A cryptographic function modification was attempted.
5068	A cryptographic function provider operation was attempted.
5069	A cryptographic function property operation was attempted.
5070	A cryptographic function property modification was attempted.
5447	A Windows Filtering Platform filter has been changed.
6144	Security policy in the group policy objects has been applied successfully.
6145	One or more errors occurred while processing the security policy in group policy objects.

Other Policy Change Events	Disable	Enable

8. Privilege Use

Privileges on a network are granted for users or computers to completed defined tasks. Privilege Use security policy settings and audit events allow you to track the use of certain privileges on one or more systems.

8.1 Non-Sensitive Privilege Use

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to audit events generated using non-sensitive privileges (user rights).

The following privileges are non-sensitive:

- Access Credential Manager as a trusted caller.
- Access this computer from the network.
- Add workstations to the domain.
- Adjust memory quotas for a process.
- Allow log on locally, allow log on through Terminal Services.
- Bypass traverse checking.
- Change the system time.
- Create a page file.
- Create global objects.
- Create permanent shared objects.
- Create symbolic links.
- Deny access to this computer from the network.
- Deny log on as a batch job.
- Deny log on as a service.
- Deny log on locally.
- Deny log on through Terminal Services.
- Force shutdown from a remote system.
- Increase a process working set.
- Increase scheduling priority.
- Lock pages in memory.
- Log on as a batch job.
- Log on as a service.
- Modify an object label.
- Perform volume maintenance tasks.
- Profile single process.
- Profile system performance.
- Unplug the computer from the docking station.
- Shut down the system.
- Synchronize directory service data.

Event volume: Very high

Default: Not configured

Event ID	Event Message
4672	Special privileges assigned to new logon.
4673	A privileged service was called.
4674	An operation was attempted on a privileged object.

Non-Sensitive Privilege Use	Enable	Enable

8.2 Sensitive Privilege Use

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to audit events generated when sensitive privileges (user rights) such as the following are used:

A privileged service is called.

One of the following privileges are called:

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

Event volume: Very high

Default: Not configured

Event ID	Event Message
4672	Special privileges assigned to new logon.
4673	A privileged service was called.
4674	An operation was attempted on a privileged object.

Sensitive Privilege Use	Enable	Enable

8.3 Other Privilege Use Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting is not used in this version of Windows

Event volume: N/A

Other Privilege Use Events	Enable	Enable

9. System

System security policy settings and audit events allow you to track system-level changes to a computer that is not included in other categories and that have potential security implications.

9.1 IPSEC Driver

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits the activities of the IPsec driver and reports any of the following events:

- Startup and shutdown of IPsec services.
- Packets dropped due to integrity check failure.
- Packets dropped due to replay check failure.
- Packets dropped due to being in plaintext.
- Packets received with an incorrect Security Parameter Index (SPI). (This can indicate malfunctioning hardware or interoperability problems.)
- Failure to process IPsec filters.
- A high rate of packet drops by the IPsec filter driver may indicate attempts to gain access to the network by unauthorized systems.

- Failure to process IPsec filters poses a potential security risk because some network interfaces may not get the protection provided by the IPsec filter.

Event volume: Medium

Default: Not configured

Event ID	Event Message
4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue, or those packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations
4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
5478	IPsec Services have started successfully.
5479	IPsec Services have been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem
5483	IPsec Services failed to initialize the RPC server. IPsec Services could not be started
5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
5485	IPsec Services failed to process some IPsec filters on a plugand-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

Ipsec Driver	Disable	Disable

9.2 Other System Events

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits any of the following events:

- Startup and shutdown of the Windows Firewall service and driver.
- Security policy processing by the Windows Firewall service.
- Cryptography key file and migration operations.

NOTE:

Failure to start the Windows Firewall service may result in a computer that is not fully protected against network threats.

Event volume: Low

Default: Success and failure

Event ID	Event Message
5024	The Windows Firewall Service has started successfully.
5025	The Windows Firewall Service has been stopped.
5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with the currently enforced policy.
5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
5030	The Windows Firewall Service failed to start.
5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
5033	The Windows Firewall Driver has started successfully.
5034	The Windows Firewall Driver has been stopped.
5035	The Windows Firewall Driver failed to start.
5037	The Windows Firewall Driver detected critical runtime error. Terminating.
5058	Key file operation.
5059	Key migration operation.
6400	BranchCache: Received an incorrectly formatted response while discovering the availability of content. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6401	BranchCache: Received invalid data from a peer. Data discarded. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6402	BranchCache: The message to the hosted cache offering its data is incorrectly formatted. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.

	NOTE: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6405	BranchCache: %2 instance(s) of Event ID %1 occurred. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6406	%1 registered to Windows Firewall to control filtering for the following: %2 **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6407	1% **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards.
6408	Registered product %1 failed, and Windows Firewall is now controlling filtering for %2 **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards

Other System Events	Disable	Disable

9.3 Security State Change

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits changes in the security state of a system and reports any of the following events:

- System startup and shutdown.
- Change of system time.
- System recovery from CrashOnAuditFail. This event is logged after a system reboots following CrashOnAuditFail.

NOTE:

Some auditable activity may not be recorded when a system reboots due to CrashOnAuditFail.

System startup and shutdown events are important to understand system usage.

Event volume: Low

Default: Success

Event ID	Event Message
4608	Windows is starting up.
4609	Windows is shutting down.
4616	The system time was changed.
4621	The administrator recovered the system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

Security State Change	Enable	Enable

9.4 Security System Extension

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits events related to security system extensions, including any of the following events:

- When a security extension code is loaded (such as authentication, notification, or security package). A security extension code registers with the Local Security Authority and will be used and trusted to authenticate logon attempts, submit logon requests, and be notified of any account or password changes. Examples of this are Kerberos and NTLM.
- When a service is installed. An audit log is generated when a service is registered with the Service Control Manager. The audit log contains information about the service name, binary, type, start type, and service account

NOTE:

Attempts to install or load security system extensions or services are critical system events that could indicate a security breach.

Event volume: Low

These events are expected to appear more on a domain controller than on client computers or member servers.

Default: Not configured

Event ID	Event Message
4610	An authentication package has been loaded by the Local Security Authority.
4611	A trusted logon process has been registered with the Local Security Authority.
4614	A notification package has been loaded by the Security Account Manager.
4622	A security package has been loaded by the Local Security Authority.
4697	A service was installed in the system.

Security System Extension	Enable	Enable

9.5 Security System Integrity

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting determines whether the operating system audits events that violate the integrity of the security subsystem, which can include any of the following events:

- Audited events are lost due to a failure of the auditing system.
- A process uses an invalid local procedure call (LPC) port to impersonate a client, reply to a client address space, read to a client address space, or write from a client address space.
- A remote procedure call (RPC) integrity violation is detected.
- A code integrity violation with an invalid hash value of an executable file is detected. • The cryptographic tasks are performed.

NOTE:

Violations of security subsystem integrity are critical and could indicate a potential security attack.

Event volume: Low

Default: Success and failure

Event ID	Event Message
4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
4615	Invalid use of LPC port.
4618	A monitored security event pattern has occurred.
4816	RPC detected an integrity violation while decrypting an incoming message.
5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
5056	A cryptographic self-test was performed.
5057	Cryptographic primitive operation failed.
5060	The verification operation failed.
5061	Cryptographic operation.
5062	A kernel-mode cryptographic self-test was performed.
6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error. **NOTE**: Supported Operating Systems Windows 2008 R2 onwards and Windows 7 onwards

System Integrity	Enable	Enable

10. Global Object Access Auditing

System security policy settings and audit events allow you to track system-level changes to a computer that is not included in other categories and that have potential security implications.

10.1 Registry (GOAA)

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to configure a global System Access Control List (SACL) on the registry for a computer. If you select the **Configure** security check box, you can add a user or group to the global SACL. This policy setting must be used in combination with the **Registry** security policy setting under **Object Access**.

Event volume: High – Very High (Depending on the Configuration)

Default: Not Configured

Registry (GOAA)	Optional	Optional

10.2 File System (GOAA)

Applies to: Windows Server 2008 onwards and Windows 7 onwards.

This security policy setting allows you to configure a global System Access Control List (SACL) on the file system for an entire computer. If both, file or folder SACL and a global SACL are configured on a computer, the effective SACL is derived from combining the file or folder SACL and the global SACL. This means that an audit event is generated if an activity matches either file or folder SACL or the global SACL.

If you select the **Configure** security check box, you can add a user or group to the global SACL. This policy setting must be used in combination with the **File System** security policy setting under **Object Access**.

Event volume: High – Very High (Depending on the Configuration)

Default: Not Configured

Related Event ID's 560 / 4656

File System (GOAA)	Optional	Optional

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support