Logmanager

Microsoft Security Auditing for Logmanager

version 2.1 – 17.10.2022

WHITEPAPER / GUIDE: How to configure Microsoft Security Auditing via Group Policy to generate and gather most important Windows Security Events. This document applies to Windows 7, 8, 10, 11 and Windows Server 2008 R2, 2012 R2, 2016, 2019 and 2022.

Logmanager

Content:

Logmanager

Abstract

What is Windows Security Auditing?

Security auditing in general is a process of cyclical, systematic review and evaluation of policies and controls that may affect security of a network. In Windows operating systems, security auditing has a different meaning - it relates to a set of controls which when enabled, generate events for specified security-related activities. Such events are available locally via Microsoft Event Viewer tool, or by using Logmanager Beats Agent, events can be collected and in near real time delivered to Logmanager for processing. Monitoring these events in central storage such as Logmanager can provide valuable information to help administrators troubleshoot and investigate operational and security-related activities.

To configure Windows Security Auditing, you need to use so-called Group Policy Objects (GPOs), which contain a set of controls allowing administrators to define how endpoints will behave. You can have different GPOs for different user groups. There are nine basic audit policy settings under **Security Settings\Local Policies\Audit Policy** and 53 settings under **Advanced Audit Policy (AAP) Configuration**. The settings available there address similar controls as the nine basic settings in **Local Policies\Audit Policy**, but they allow administrators to more granularly define types of events to audit. For example, basic audit policy provides a single setting for account logon, while advanced audit policy provides four. As such, enabling a single basic account logon setting would be the equivalent of setting all four advanced account logon settings. Most important AAP are fully explained in this document and contain suggested configuration values.

Important note: Basic audit policy settings are not compatible with advanced audit policy settings. Using both advanced and basic audit policy settings can cause unexpected results in audit reporting.

Goal of this document

Proper configuration of Windows Security Auditing can be an enormous help for your security team during an incident investigation or pro-active prevention. But it is a lot of work to set up. First you need to select which Windows Security Audit controls reflect best your organization procedures and policies and then constantly review and tune them. Bad configuration can create a huge number of events on every Windows system which instead of helping your analysts, will have the opposite effect by creating so-called alert fatigue, or in the worst case scenario overload your SEM/SIEM.

The goal of this document is to provide you with clear recommendations on which Windows Security Auditing controls to select - based on Logmanager experience, and what will be the exact outcome of enabling it. That being said, please do not follow this document blindly – you still need to understand what is going on in your network and apply your judgement to each control you enable.

Logmanager

Prerequisites

Choose right endpoints to monitor

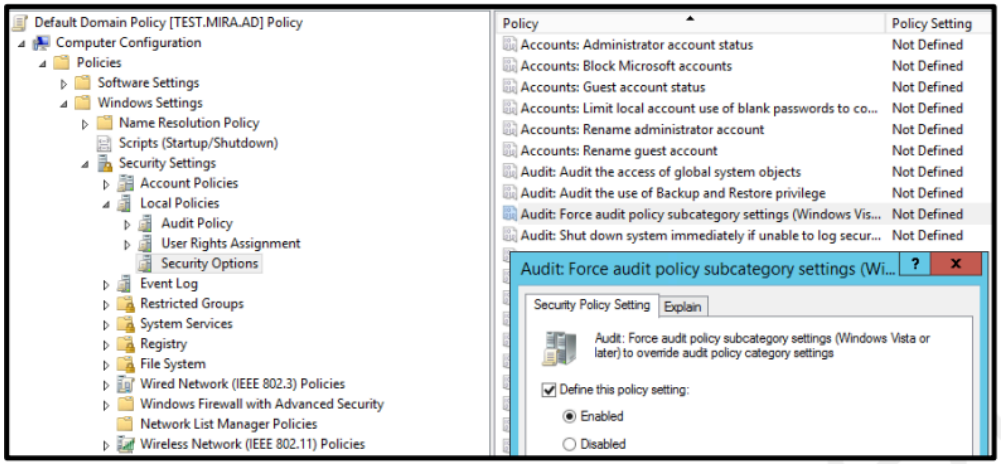
Monitoring every system in your network would be the best approach from a security point of view (and the easiest to configure), but due to the volume of data such monitoring would generate it is not always possible. Due to that most organizations focus on VIP machines – such as CEO computers, accounting workstations, Domain Controllers, File Share servers – anything that has a high potential value for an attacker should be closely monitored. The bottom line is you need to know your assets. After all, how can you expect to secure anything, if you do not precisely know what it is that you are securing? A risk assessment program will help you figure this out.

Forward logs from Windows (Logmanager Beats Agent)

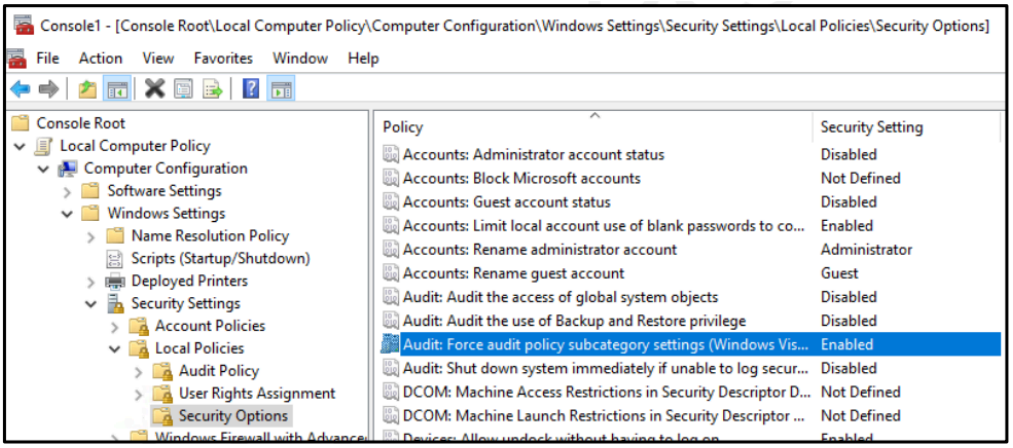
Windows native events forwarding mechanisms are known to be unreliable and hard to set up – due to this we recommend using our own Logmanager Beats Agent to collect Windows Events and forward them to Logmanager. Beats Agent needs to be installed on servers and computers from which you want to collect logs. Requirements and instructions regarding distributing Beats Agent through Group Policy are described in online documentation of Logmanager. Before continuing with this document please make sure that Beats Agent is distributed and installed properly.

Configure Advanced Audit Policy Configuration

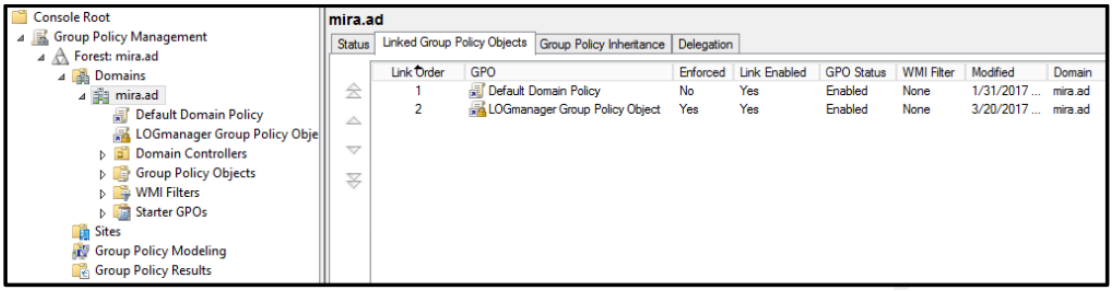
1. Run Group Policy Management console.
2. Make sure that Advanced Audit Policy Configuration settings are not overwritten first as in the screenshot below:
    a. Right-click **Default Domain Policy**, and then click Edit.
    b. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
    c. Double-click **Security Settings**, and then click **Local Policies** and then click **Security Options**.
    d. Double-click **Audit: Force audit policy subcategory settings** (Windows Vista or later) to override audit policy category settings, and then click **Define** this policy setting.
    e. Click **Enabled**, and then click OK.



f. You can check on any domain computers that this policy is properly distributed by RDP to remote computers, log-in as administrator, run command **gpupdate** and check on local computer mmc console, as in the screenshot below.



3. Open subject Domain / Group Policy Objects and create a new GPO. Name it "Logmanager Group Policy Object – *name of subject*". The name of the subject should refer to the target group, where the policy will be applied later on. For example, member_servers or workstations.
4. Edit newly created GPO.
5. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**, and then double-click **Security Settings**, and then double-click **Advanced Audit Policy Configuration**, and then double-click **Audit Policies**.
6. Modify newly created GPO with **Advanced Audit Policies** according to this document (pages 8-72) or simplified document with table only.
7. Link newly created GPO with Default Domain Policy as in the screenshot below.



Advanced Audit Policies offers to change settings in 10 categories. We will modify settings in all categories. Each option in this document contains suggested configuration value and short description of the expected outcome for such configuration change.

Logmanager

Windows Security Controls

Account Logon

Configuring policy settings in this category can help you document domain attempts to authenticate account data, either to a domain controller or a local Security Accounts Manager (SAM). Unlike Logon/Logoff policy settings and events, which track attempts to access a particular computer, settings and events in this category focus on the account database being used.

Credential Validation

Description: This policy setting allows you to audit events generated by validation tests on user account logon credentials. Policy will generate events when an authentication attempt is made using any domain account and NTLM authentication.

Volume: High on domain controllers, low on member servers and workstations.

Microsoft recommendation: Success and Failure. Success auditing to keep track of domain account authentication events using the NTLM protocol. Expect a high volume of events. Just collecting Success auditing events in this subcategory for future use in case of a security incident is not very useful, because events in this subcategory are not always informative.

Failure auditing, to collect information about failed authentication attempts using domain accounts and the NTLM authentication protocol.

Event ID	Description
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.
4822	NTLM authentication failed because the account was a member of the Protected User group.
4823	NTLM authentication failed because access control restrictions are required.

Logmanager recommendation: Leave not configured. These events could be useful if you are using NTLM authentication (which you shouldn't due to the fact it is known to be vulnerable), but even in such case, Logon data is already taken care by Logon/Logoff policies anyway, so there is no reason to double this kind of information, especially since this Policy can be very noisy according to our research.

Logmanager

Kerberos Authentication Service

Description: This policy determines whether 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.

Volume: High on servers with Kerberos Key Distribution Center role (such as DC).

Microsoft recommendation: Success and Failure. Success auditing, because you will see all Kerberos Authentication requests (TGT requests), which are a part of domain account logons. Also, you can see the IP address from which this account requested a TGT, when TGT was requested, which encryption type was used and so on.

Failure auditing, because you will see all failed requests with wrong password, username, revoked certificate, and so on. You will also be able to detect Kerberos issues or possible attack attempts.

Event ID	Description
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.
4773	A Kerberos service ticket request failed.
4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
4824	Kerberos pre-authentication by using DES or RC4 failed because the account was a member of the Protected User group.
4768	A Kerberos authentication ticket (TGT) was requested.

Logmanager recommendation: Success and failure. You can use these events to monitor for Kerberos-based attacks such as Kerberoasting (for example: if a given workstation requests more than one TGT in a short time frame).

Kerberos Service Ticket Operations

Description: This policy 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 who wants to access a protected network resource. Kerberos service ticket operation audit events can be used to track user activity.

Volume: Very High on servers with Kerberos Key Distribution Center role (such as DC).

Microsoft recommendation: Success and Failure. Success auditing, because you will see all Kerberos Service Ticket requests (TGS requests), which are part of service use and access requests by specific accounts. Also, you can see the IP address from which this account requested TGS, when TGS was requested, which encryption type was used, and so on.

Failure auditing, because you will see all failed requests and be able to investigate the reason for failure. You will also be able to detect Kerberos issues or possible attack attempts.

Event ID	Description
4769	A Kerberos service ticket was requested.
4770	A Kerberos service ticket was renewed.
4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.

Logmanager recommendation: Success and failure.

Other Account Logon Events

Description: This policy setting allows you to audit events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets.

Volume: Low

Microsoft recommendation: Leave not configured.

Logmanager recommendation: Leave not configured.

According to Microsoft there are no events in this category, and it is intended for future use only.

Logmanager

Account Management

The security audit policy settings in this category can be used to monitor changes to user and computer accounts and groups.

Application Group Management

Description: This policy generates events for actions related to application groups, such as group creation, modification, addition or removal of group members and some other actions.

Volume: Low

Microsoft recommendation: Leave not configured. Application groups are used by Authorization Manager which is very rarely in use and it is deprecated starting from Windows Server 2012.

Event ID	Description
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.
4791	A basic application group was changed.
4792	An LDAP query group was deleted.

Logmanager recommendation: Leave not configured.

Logmanager

Computer Account Management

Description: This policy determines whether the operating system generates audit events when a computer account is created, changed, or deleted.

It is useful for tracking account-related changes to computers that are members of a domain.

Volume: Low

Microsoft recommendation: Success. Monitoring changes to critical computer objects in Active Directory, such as domain controllers, administrative workstations, and critical servers. It's especially important to be informed if any critical computer account objects are deleted. Additionally, events in this subcategory will give you information about who deleted, created, or modified a computer object, and when the action was taken.

This subcategory does not have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

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

Logmanager recommendation: Success.

Note: Regular users can create Computer Accounts by default. Users who have the Create Computer Objects permission on the Active Directory computers container can also create computer accounts in the domain same way as regular users. The difference is that users with permissions on the container are not restricted to the creation of only 10 computer accounts. Simplified - every AD user can Create Computer Account and make sense to monitor such activity.

Logmanager

Distribution Group Management

Description: This policy determines whether the operating system generates audit events for specific distribution-group management tasks.

Volume: Low

Microsoft recommendation: Leave not configured. Typically, actions related to distribution groups have low security relevance. It is much more important to monitor Security Group changes. However, if you want to monitor for critical distribution groups changes, such as if a member was added to an internal critical distribution group (executives, administrative group, for example), you need to enable this subcategory for Success auditing.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
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.

Logmanager recommendation: Leave not configured. Distribution groups cannot be used to assign permissions to objects (such as file share) and because of that, monitoring it for changes is not that important. But since the data volume of this Policy is low, there is no harm in enabling it – it's up to you to decide.

Logmanager

Other Account Management Events

Description: This policy determines whether the operating system generates user account management audit events.

Volume: Low

Microsoft recommendation: Success. The only reason to enable Success auditing on domain controllers is to monitor "4782(S): The password hash of an account was accessed." Any actions with the account's password hashes should be planned. If this action was not planned, investigate the reason for the change.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

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

Logmanager recommendation: Leave not configured. Event id 4782 is only triggered by usage of Active Directory Migration Toolkit. We haven't seen an attack utilizing this tool, and as such, this event is most likely useless – we didn't manage to trigger it by accessing Accounts hashes using tools such as Mimikatz. Event id 4793 is only generated on member servers and workstations and has no security relevance. Since this policy has extremely low volume of generated events there is no harm in enabling it, but there is no evidence suggesting its usefulness.

Logmanager

Security Group Management

Description: This policy determines whether the operating system generates audit events when specific security group management tasks are performed.

Volume: Low

Microsoft recommendation: Success. Auditing of security groups, to see new group creation events, changes and deletion of critical groups. Also, you will get information about new members of security groups, when a member was removed from a group and when security group membership was enumerated.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4727	A security-enabled global group was created.
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	A security-enabled local group was created.
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.
4799	A security-enabled local group membership was enumerated.

Logmanager recommendation: Success. Monitoring security groups is especially important from a security perspective, as they enable access to resources. Any changes to security groups, adding or removing members, creating new ones, should be planned. If change should occur without prior information, you need to investigate the reasons, as it might be malicious.

Logmanager

User Account Management

Description: This policy determines whether the operating system generates audit events when specific user account management tasks are performed.

Volume: Low

Microsoft recommendation: Success and Failure. This subcategory contains many useful events for monitoring, especially for critical domain accounts, such as domain admins, service accounts, database admins, and so on.

Failure auditing is recommended mostly to see invalid password change and reset attempts for domain accounts, DSRM account password change failures, and failed SID History add attempts.

Event ID	Description
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 administrators' groups.
4781	The name of an account was changed.
4794	An attempt was made to set the Directory Services Restore Mode.
4797	An attempt was made to query the existence of a blank password for an account.
4798	A user's local group membership was enumerated.
5376	Credential Manager credentials were backed up.
5377	Credential Manager credentials were restored from a backup.

Logmanager recommendation: Success and Failure. **It's one of the most important policies to have enabled.** It allows monitoring user accounts creation or change which is required by several security standards such as ISO27001:2013, as well as account lockouts, which is very useful for both security (detecting brute force attempts) and operational purposes (users locking themselves out due to lost password).

Detailed Tracking

Detailed Tracking security policy settings and audit events can be used to monitor the activities of individual applications, to understand how a computer is being used, and the activities of users on that computer.

DPAPI Activity

Description: This policy determines whether the operating system generates audit events when encryption or decryption calls are made into the data protection application interface (DPAPI).

Volume: Low

Microsoft recommendation: Leave not configured. Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for DPAPI troubleshooting.

Event ID	Description
4692	Backup of data protection master key was attempted.
4693	Recovery of data protection master key was attempted.
4694	Protection of auditable protected data was attempted.
4695	Unprotection of auditable protected data was attempted.

Logmanager recommendation: Leave not configured.

Logmanager

PNP Activity

Description: This policy determines when Plug and Play detects an external device. This type of events can be used to track down changes in system hardware and will be logged on the machine where the change took place. For example, when a keyboard is plugged into a computer, a PnP event is triggered.

Volume: Low (depending on how computer is used)

Microsoft recommendation: Success. This subcategory will help identify when and which Plug and Play device was attached, enabled, disabled or restricted by device installation policy. You can track, for example, whether a USB flash drive or stick was attached to a domain controller, which is typically not allowed.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
6416	A new external device was recognized by the System.
6419	A request was made to disable a device
6420	A device was disabled.
6421	A request was made to enable a device.
6422	A device was enabled.
6423	The installation of this device is forbidden by system policy.
6424	The installation of this device was allowed, after having previously been forbidden by policy.

Logmanager recommendation: Success on Servers and important workstations. While it is much more beneficial to enable Audit Removable Storage policy, PNP activity is capable to recognize additional hardware like USB network card, new keyboard and other stuff, usually rarely seen on servers.

Logmanager

Process Creation

Description: This policy determines whether the operating system generates audit events when a process is created (starts). These audit events can help you track user activity and understand how a computer is being used. Information includes the name of the program or the user that created the process.

Volume: Medium to High (depending on system usage).

Microsoft recommendation: Success. It is typically useful to collect Success auditing information for this subcategory for forensic investigations, to find information who, when and with which options\parameters ran a specific process. Additionally, you can analyze process creation events for elevated credentials use, potential malicious process names and so on. The event volume is typically medium-high level, depending on the process activity on the computer.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

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

Logmanager recommendation: Success. Although it can generate a large amount of data, we strongly recommend considering enabling it, as it is very useful for forensics investigations as well as incident detection. Some examples of alerts based on this policy:

- Look for pre-defined process names (ex. mimikatz.exe or cain.exe). Or just create a list of all the processes run during the last period and put it into a lookup table as a whitelist and notify on anything else seen by Logmanager (how to? Check Logmanager user forum)
- **Token Elevation Type** with value **TokenElevationTypeDefault**, when **Account Name** contains a real user account (for example when Account Name doesn't contain the **$** symbol). Typically, this means that UAC is disabled for this account for some reason.
- **Token Elevation Type** with value **TokenElevationTypeFull** on standard workstations, when **Account Name** contains a real user account (for example when Account Name doesn't contain the **$** symbol). This means that a user ran a program using administrative privileges.
- **Token Elevation Type** with value **TokenElevationTypeFull** on standard workstations, when a computer object was used to run the process, but that computer object is not the same computer where the event occurs.
- **CLI** and **PowerShell** commands logging (check Logmanager user forum for detailed instruction).

Process Termination

Description: This policy determines whether the operating system generates audit events when process has exited. This policy setting can help you track user activity and understand how the computer is used.

Volume: Medium to High (depending on system usage).

Microsoft recommendation: Leave not configured. This subcategory typically is not as important as Audit Process Creation subcategory. Using this subcategory, you can, for example, get information about how long the process was run in correlation with 4688 events. If you have a list of critical processes that run on some computers, you can enable this subcategory to monitor for termination of these critical processes.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4689	A process has exited.

Logmanager recommendation: Leave not configured. As mentioned above, monitoring of the terminated processes is not as important as monitoring of the started processes. Sure, unless you are trying to figure out how long a process has run. But since this policy can generate a lot of data, potential benefits are outweighed by processing power required, so our recommendation is to leave it not configured.

RPC Events

Description: This policy determines whether the operating system generates audit events when inbound remote procedure call (RPC) connections are made.

Volume: Unknown – Events in this subcategory occur rarely.

Microsoft recommendation: Leave not configured. Events in this subcategory occur rarely.

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

Logmanager recommendation: Leave not configured. According to Microsoft documentation, it appears that this event almost never occurs.

Logmanager

Token Right Adjusted

Description: This policy allows you to audit events generated by adjusting the privileges of a token.

Volume: High

Microsoft recommendation: With Success auditing for this subcategory, you can get information related to changes to the privileges of a token. However, if you are using an application or system service that dynamically adjusts token privileges, we do not recommend Success auditing because of the high volume of this event that may be generated. As of Windows 10, event 4703 is generated by applications or services that dynamically adjust token privileges. An example of such an application is Microsoft Endpoint Configuration Manager, which makes WMI queries at recurring intervals and quickly generates many 4703 events (with the WMI activity listed as coming from svchost.exe).

If one of your applications or services is generating many 4703 events, you might find that your event-management software has filtering logic that can automatically discard the recurring events, which would make it easier to work with Success auditing for this category.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4703	A user right was adjusted.

Logmanager recommendation: Events generated by this policy could be potentially used to look for compromise attempts – mainly malicious processes being assigned **SeDebugPrivilege**. Reason: Debug privileges are not normally assigned even to administrative token, since it is not needed. Some malicious tools, however, do require it (WCE or Mimikatz), and as such monitoring for token elevation to debug rights can be a sign of a security incident. In simple logic:

- Generate an alert if EventID 4703 appears where enabled privileges are equal to SeDebugPrivilege.

There are some drawbacks to consider:

1. Event id 4703 will be generated often if enabled (for example at logon). This is the main issue – consider enabling this policy only if you have processing power to spare.
2. WMI elevates itself constantly, so it has to be excluded from alert logic.

Logmanager

Domain Services (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.

Detailed Directory Service Replication

Description: This policy determines whether the operating system generates audit events that contain detailed tracking information about data that is replicated between domain controllers. This audit subcategory can be useful to diagnose replication issues.

Volume: Very High

Microsoft recommendation: Leave not configured. Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for Active Directory replication troubleshooting.

Event ID	Description
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.

Logmanager recommendation: Leave not configured.

Logmanager

Directory Service Access

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

Volume: High

Microsoft recommendation: Failure. It is better to track changes to Active Directory objects through the Audit Directory Service Changes subcategory. However, Audit Directory Service Changes don't give you information about failed access attempts, so we recommend Failure auditing in this subcategory to track failed access attempts to Active Directory objects.

Event ID	Description
4662	An operation was performed on an object.
5169	A directory service object was modified.

Logmanager recommendation: Leave not configured. Due to the high potential volume of event enable failure auditing as recommended by Microsoft only if you have a real need for such data and processing power to spare.

Logmanager

Directory Service Changes

Description: This policy determines whether the operating system generates audit events when changes are made to objects in Active Directory Domain Services (AD DS).

Auditing of directory service objects can provide information about the old and new properties of the objects that were changed.

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 audit events to be generated due to settings on the object class in the schema.

Volume: High

Microsoft recommendation: Success. It is important to track actions related to high value or critical Active Directory objects, for example, changes to AdminSDHolder container or Domain Admins group objects. This subcategory shows you what actions were performed. If you want to track failed access attempts for Active Directory objects you need to take a look at Audit Directory Service Access subcategory.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
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.

Logmanager recommendation: Success. While the volume of events is high, this policy allows monitoring for changes being made to critical objects – such as Group Policy Objects. Having this policy enabled can be very useful to track administrator activity. For GPO monitoring to work you need to enable proper SACL on your policies. Check Logmanager forum for a detailed guide on how to enable it.

Directory Service Replication

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

Volume: Medium

Microsoft recommendation: Leave not configured. Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for Active Directory replication troubleshooting.

Event ID	Description
4932	Synchronization of a replica of an Active Directory naming context has begun.
4933	Synchronization of a replica of an Active Directory naming context has ended.

Logmanager recommendation: Leave not configured.

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.

Account Lockout

Description: This policy enables you to audit security events that are 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.

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

Volume: Low

Microsoft recommendation: Failure. We recommend tracking account lockouts, especially for high value domain or local accounts (database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts, and so on).

This subcategory doesn't have Success events, so there is no recommendation to enable Success auditing for this subcategory

Event ID	Description
4625	An account failed to log on.

Logmanager recommendation: Failure.

Logmanager

User / Device Claims

Description: This policy allows you to audit user and device claims information in the account's logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to.

For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.

Important: Enable the **Audit Logon** subcategory to get events from this subcategory.

Volume: Low on a workstation and Medium on a DC.

Microsoft recommendation: If claims are in use in your organization and you need to monitor user/device claims, enable Success auditing for this subcategory.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4626	User/Device claims information.

Logmanager recommendation: Leave not configured unless you have a specific need.

Logmanager

Group Membership

Description: With this policy you can audit group memberships when they're enumerated on the client computer.

This policy allows you to audit the group membership information in the user's logon token. Events in this subcategory are generated on the computer on which a logon session is created.

For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.

Important: Enable the **Audit Logon** subcategory to get events from this subcategory.

Volume: Low on a workstation and Medium on a DC.

Microsoft recommendation: Success. Group membership information for a logged-in user can help to detect that a member of a specific domain or local group logged in to the machine (for example, member of database administrators, built-in local administrators, domain administrators, service accounts group, or other high value groups).

This subcategory doesn't have Failure events, so this subcategory doesn't have a recommendation to enable Failure auditing.

Event ID	Description
4627	Group membership information.

Logmanager recommendation: Success. This event is generated alongside event **4624: An account was successfully logged on** and thus enables tracking a member of a specific group logging in to a computer, for ex. user logging in to a computer in a different department.

Logmanager

IPsec Extended Mode

Description: This policy allows you to audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations.

Volume: Unknown

Microsoft recommendation: Leave not configured. This subcategory is mainly used for IPsec Extended Mode troubleshooting, or for tracing or monitoring IPsec Extended Mode operations.

Event ID	Description
4978	During 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.
4980	IPsec Main Mode and Extended Mode security associations were established.
4981	IPsec Main Mode and Extended Mode security associations were established.
4982	IPsec Main Mode and Extended Mode security associations were established.
4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Logmanager recommendation: Leave not configured unless you have a specific need or run for diagnostic purposes.

Logmanager

IPsec Main Mode

Description: This policy allows you to audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.

Volume: Unknown

Microsoft recommendation: Leave not configured. This subcategory is mainly used for IPsec Main Mode troubleshooting, or for tracing or monitoring IPsec Main Mode operations.

Event ID	Description
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.
4653	An IPsec Main Mode negotiation failed.
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 is not started.

Logmanager recommendation: Leave not configured unless you have a specific need.

Logmanager

IPsec Quick Mode

Description: This policy allows you to audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations.

Volume: Unknown

Microsoft recommendation: Leave not configured. This subcategory is mainly used for IPsec Quick Mode troubleshooting, or for tracing or monitoring IPsec Quick Mode operations.

Event ID	Description
4654	An IPsec Quick Mode negotiation failed.
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.

Logmanager recommendation: Leave not configured unless you have a specific need.

Logmanager

Logoff

Description: This policy determines whether the operating system generates audit events when logon sessions are terminated.

These events occur on the computer that was accessed. For an interactive logon, these events are generated on the computer that was logged on to.

Volume: Low on workstation, High on domain controllers.

Microsoft recommendation: Leave not configured. This subcategory typically generates a huge amount of "4634(S): An account was logged off." events, which typically have little security relevance. It's more important to audit Logon events using Audit Logon subcategory, rather than Logoff events.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4634	An account was logged off.
4647	User initiated logoff.

Logmanager recommendation: Leave not configured, unless you have a specific need, for example correlating User logon with logoff and tracking how user was logged on. If you decide to enable this policy, keep in mind it can generate a high amount of data.

Logmanager

Logon

Description: This policy 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 a network logon, such as accessing a share, events are generated on the computer that hosts the resource that was accessed.

Volume: Low on workstation, High on domain controllers.

Microsoft recommendation: Success and Failure. Audit Logon events, for example, will give you information about which account, when, using which Logon Type, from which machine logged on to this machine.

Failure events will show you failed logon attempts and the reason why these attempts failed.

Event ID	Description
4624	An account was successfully logged on.
4625	An account failed to log on.
4626	User/Device claims information.
4648	A logon was attempted using explicit credentials.
4675	SIDs were filtered.

Logmanager recommendation: Success and Failure. It is crucial to monitor user logon to track activity across systems, as well as detecting brute force attacks.

Logmanager

Network Policy Server

Description: This policy allows you to audit events generated by RADIUS (IAS) and Network Access Protection (NAP) activity related to user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock.

If you configure this subcategory, an audit event is generated for each IAS and NAP user access request.

This subcategory generates events only if the NAS or IAS role is installed on the server.

Volume: Medium to High on servers that are running Network Policy Server (NPS).

Microsoft recommendation: If a server has the Network Policy Server (NPS) role installed and you need to monitor access requests and other NPS-related events, enable this subcategory.

Event ID	Description
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.

Logmanager recommendation: Enable, if NPS role on a given server is active and role is in use to provide AAA for remote access and 802.1X (Port-based Network Access Control) purposes. Useful for diagnostics purposes when tracking why a user cannot connect.

Logmanager

Other Logon/Logoff Events

Description: This policy determines whether Windows generates audit events for other logon or logoff events.

These other logon or logoff events include:

- A Remote Desktop session connects or disconnects.
- 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 be either a user account or a computer account.
- A user is granted access to a wired 802.1x network. It can be either a user account or a computer account.

Volume: Low

Microsoft recommendation: Success and Failure. We recommend Success auditing, to track possible Kerberos replay attacks, terminal session connect and disconnect actions, network authentication events, and some other events. The volume of these events is typically very low.

Failure events will show you when requested credentials CredSSP delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.

Event ID	Description
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.
4825	A user was denied the access to Remote Desktop.
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.

Logmanager recommendation: Success and Failure. We have not seen much of those events in our lab but since expected volume according to Microsoft is low, there is no harm in enabling this policy.

Logmanager

Special Logon

Description: This policy determines whether the operating system generates audit events under special sign on (or log on) circumstances.

This subcategory allows you to audit events generated by special logons such as the following:

- The use of a special logon, which is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level.
- A logon by a member of a Special Group. Special Groups enable you to audit events generated when a member of a certain group has logged on to your network. You can configure a list of group security identifiers (SIDs) in the registry. If any of those SIDs are added to a token during logon and the subcategory is enabled, an event is logged.

Volume: Low on workstation, Medium on domain controllers.

Microsoft recommendation: Success. This subcategory is very important because of Special Groups related events; you must enable this subcategory for Success audit if you use this feature. At the same time this subcategory allows you to track account logon sessions to which sensitive privileges were assigned.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4964	Special groups have been assigned to a new logon.
4672	Special privileges assigned to new logon.

Logmanager recommendation: Success. If this policy is enabled you can, for example, monitor for every Domain Administrators logon to a non-administrative workstation.

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.

Application Generated

Description: This policy generates events for actions related to Authorization Manager applications.

Volume: Unknown

Microsoft recommendation: If you use Authorization Manager in your environment and you need to monitor events related to Authorization Manager applications, enable this subcategory.

Event ID	Description
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.

Logmanager recommendation: Leave not configured.

Logmanager

Certification Services

Description: This policy determines whether the operating system generates events when Active Directory Certificate Services (AD CS) operations are performed.

Volume: Low to Medium on servers with AD CS role.

Microsoft recommendation: If a server has the Active Directory Certificate Services (AD CS) role installed and you need to monitor AD CS related events, enable this subcategory.

Event ID	Description
4868	The certificate manager denied a pending certificate request.
4869	Certificate Services received a resubmitted certificate request.
4870	Certificate Services revoked a certificate.
4871	Certificate Services received a request to publish the certificate revocation list (CRL).
4872	Certificate Services published the certificate revocation list (CRL).
4873	A certificate request extension changed.
4874	One or more certificate request attributes changed.
4875	Certificate Services received a request to shut down.
4876	Certificate Services backup started.
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.
4899	A Certificate Services template was updated.
4900	Certificate Services template security was updated.

Logmanager recommendation: Leave not configured unless you have a specific need.

Logmanager

Detailed File Share

Description: This policy allows you 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 and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.

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.

Volume: High on file server, and domain controllers, Low on workstations

Microsoft recommendation: Failure. Audit Success for this subcategory on domain controllers typically will lead to high volume of events, especially for SYSVOL share.

We recommend monitoring Failure access attempts: the volume should not be high. You will be able to see who was not able to get access to a file or folder on a network share on a computer.

If a server or a workstation has shared network folders that typically get many access requests (File Server, for example), the volume of events might be high. If you really need to track all successful access events for every file or folder located on a shared folder, enable Success auditing or use the Audit File System subcategory, although that subcategory excludes some information in Audit Detailed File Share, for example, the client's IP address.

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

Logmanager recommendation: Enable on servers with SMB shares, but keep in mind that this policy generates high volume of data due to the fact it applies to every file share. It is in some cases better to use the Audit **File System** policy for monitoring access activity on important files,since it allows you to be much more selective regarding files and folders you want to monitor via usage of SACLs. On the other hand, configuring SACLs is more complicated than just enabling **Detailed File Share** policy.

Main benefit of event generated by this policy is the fact that it contains IP address of the source attempting an access – but events in **Audit File System** policy still contain Username, which should be enough in some situations.

Logmanager

File Share

Description: This policy allows you to audit events related to file shares: creation, deletion, modification, and access attempts. Also, it shows failed SMB SPN checks.

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

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

Volume: High on file server, and domain controllers, Low on workstations

Microsoft recommendation: Success and Failure. We recommend Success auditing because it's important to track deletion, creation, and modification events for network shares.

We recommend Failure auditing to track failed SMB SPN checks and failed access attempts to network shares.

Event ID	Description
5140	A network share object was accessed.
5142	A network share object was added.
5143	A network share object was modified.
5144	A network share object was deleted.
5168	Spn check for SMB/SMB2 failed.

Logmanager recommendation: Leave not configured, if You already enabled **Detailed File Share** policy on Your servers with SMB shares. **File Share** policy obviously generates less detailed data than **Detailed File Share** policy.

Logmanager

File System

Description: This policy determines whether the operating system generates audit events when users attempt to access file system objects.

Audit events are generated only 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 any 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.

Volume: Varies, depending on SACLs.

Microsoft recommendation: We strongly recommend that you develop a File System Security Monitoring policy and define appropriate SACLs for file system objects for different operating system templates and roles. Do not enable this subcategory if you have not planned how to use and analyze the collected information. It is also important to delete non-effective, excess SACLs. Otherwise, the auditing log will be overloaded with useless information.

Failure events can show you unsuccessful attempts to access specific file system objects. Consider enabling this subcategory for critical computers first, after you develop a File System Security Monitoring policy for them.

Event ID	Description
4656	A handle to an object was requested.
4658	The handle to an object was closed.
4660	An object was deleted.
4663	An attempt was made to access an object.
4664	An attempt was made to create a hard link.
4985	The state of a transaction has changed.
5051	A file was virtualized.
4670	Permissions on an object were changed.

Logmanager recommendation: Success on the servers, where necessary to monitor file system mostly for unauthorize changes. As mentioned, this policy allows for very granular monitoring of important files, not just those residing on the file share. By setting appropriate SACLs on important files, any successful access attempt on them will generate an event with detailed information on access type – for example: read, write, delete. Consider enabling failure auditing as well to catch possible unauthorized attempts to access files.

Logmanager

Filtering Platform Connection

Description: This policy determines whether the operating system generates audit events when connections are allowed or blocked by the Windows Filtering Platform.

Windows Filtering Platform (WFP) enables independent software vendors (ISVs) to filter and modify TCP/IP packets, monitor or authorize connections, filter Internet Protocol security (IPsec)- protected traffic, and filter remote procedure calls (RPCs).

This subcategory contains Windows Filtering Platform events about blocked and allowed connections, blocked and allowed port bindings, blocked and allowed port listening actions, and blocked to accept incoming connections applications.

Volume: Very High

Microsoft recommendation: Success auditing for this subcategory typically generates a very high volume of events, for example, one event for every connection that was made to the system. It is much more important to audit Failure events (blocked connections, for example).

Event ID	Description
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
5150	The Windows Filtering Platform has 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.

Logmanager recommendation: Leave not configured unless you know what you are doing and have a specific need for monitoring this kind of events. This policy will generate a massive amount of data and can easily overload your SEM/SIEM if enabled for too many servers/endpoints at once. Additionally, it is worth noticing, some events will be doubled by your Firewall logs, if connection will be made to/from outside of your network. That being said, it is definitely useful from security point of view to monitor network connections made to and from your servers – especially east-west traffic, which could be transparent to your router and border Firewall.

Important: *Proceed with caution if you will decide on enabling this policy, rollout it endpoint by endpoint and monitor amounts of data being generated.*

Logmanager

Filtering Platform Packet Drop

Description: This policy determines whether the operating system generates audit events when packets are dropped by the Windows Filtering Platform.

Windows Filtering Platform (WFP) enables independent software vendors (ISVs) to filter and modify TCP/IP packets, monitor or authorize connections, filter Internet Protocol security (IPsec)- protected traffic, and filter remote procedure calls (RPCs).

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

Volume: Very High

Microsoft recommendation: Failure events volume typically is very high for this subcategory and typically used for troubleshooting. If you need to monitor blocked connections, it is better to use "5157(F): The Windows Filtering Platform has blocked a connection," because it contains almost the same information and generates per-connection, not per-packet.

There is no recommendation to enable Success auditing, because Success events in this subcategory rarely occur.

Event ID	Description
5146	The Windows Filtering Platform has blocked a packet.
5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
5152	The Windows Filtering Platform blocked a packet.
5153	A more restrictive Windows Filtering Platform filter has blocked a packet.

Logmanager recommendation: Leave not configured.

Important: *Proceed with caution if you will decide on enabling this policy, rollout it endpoint by endpoint and monitor amounts of data being generated.*

Handle Manipulation

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

Volume: High

Microsoft recommendation: Typically, information about the duplication or closing of an object handle has little to no security relevance and is hard to parse or analyze.

There is no recommendation to enable this subcategory for Success or Failure auditing, unless you know exactly what you need to monitor in Object's Handles level.

Event ID	Description
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.

Logmanager recommendation: Leave not configured.

Kernel Object

Description: This policy determines whether the operating system generates audit events when users attempt to access the system kernel, which includes mutexes and semaphores.

Only kernel objects with a matching system access control list (SACL) generate security audit events. The audits generated are usually useful only to developers.

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

Volume: High

Microsoft recommendation: Leave not configured. Typically Kernel object auditing events have little to no security relevance and are hard to parse or analyze. Also, the volume of these events is typically very high.

There is no recommendation to enable this subcategory, unless you know exactly what you need to monitor at the Kernel objects level.

Event ID	Description
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.

Logmanager recommendation: Leave not configured.

Logmanager

Other Object Access Events

Description: This policy allows you to monitor operations with scheduled tasks, COM+ objects and indirect object access requests.

Volume: Low

Microsoft recommendation: We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack.

Event ID	Description
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.
5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
5149	The DoS attack has subsided and normal processing is being resumed.
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.

Logmanager recommendation: Success. Failure auditing only works for event 5148/5149 which is aimed at detecting ICMP DoS attacks which is outdated and is not used anymore.

Logmanager

Registry

Description: This policy allows you to audit attempts to access registry objects. A security audit event is generated only for objects that have system access control lists (SACLs) specified, and only if the type of access requested, such as Read, Write, 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 any 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.

Volume: High, but generally depending on how many registry objects are being monitored.

Microsoft recommendation: We strongly recommend that you develop a Registry Objects Security Monitoring policy and define appropriate SACLs for registry objects for different operating system templates and roles. Do not enable this subcategory if you have not planned how to use and analyze the collected information. It is also important to delete non-effective, excess SACLs. Otherwise, the auditing log will be overloaded with useless information.

Failure events can show you unsuccessful attempts to access specific registry objects.

Consider enabling this subcategory for critical computers first, after you develop a Registry Objects Security Monitoring policy for them.

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

Logmanager recommendation: Success. We recommend monitoring important system keys for modification – such actions can alert you about suspicious activity. Consult our guide on user forum to learn details on how to set this up. Example alerts:

- Windows Defender is disabled
- Path/Extension/Process Exclusion is added to Windows Defender
- File association change
- Modification to winlogon keys
- Application added to system startup
- Windows Firewall is disabled

Logmanager

Removable Storage

Description: This policy allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated for all objects and all types of access requested, with no dependency on the object's SACL.

Volume: Unknown – depending on removable storage usage.

Microsoft recommendation: This subcategory will help identify when and which files or folders were accessed or modified on removable devices.

It is often useful to track actions with removable storage devices and the files or folders on them, because malicious software very often uses removable devices as a method to get into the system. At the same time, you will be able to track which files were written or executed from a removable storage device.

You can track, for example, actions with files or folders on USB flash drives or sticks that were inserted into domain controllers or high value servers, which is typically not allowed.

We recommend Failure auditing to track failed access attempts.

Event ID	Description
4656	A handle to an object was requested.
4658	The handle to an object was closed.
4663	An attempt was made to access an object.

Logmanager recommendation: Success. Enabling this policy can be useful on VIP machines, but we do not recommend that you enable this category on a file server that hosts file shares on a removable storage device. When Removable Storage Auditing is configured, any attempt to access the removable storage device will generate an audit event.

SAM

Description: This policy enables you to audit events that are generated by attempts to access Security Account Manager (SAM) objects.

The Security Account Manager (SAM) is a database that is present on computers running Windows operating systems that stores user accounts and security descriptors for users on the local computer.

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.

Only a 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 in which the account and password information is stored in the system, bypassing any Account Management events.

Volume: High

Microsoft recommendation: There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at Security Account Manager level.

Event ID	Description
4661	A handle to an object was requested.

Logmanager recommendation: Leave not configured.

Central Access Policy Staging

Description: This policy allows you to audit access requests where a permission granted or denied by a proposed policy differs from the current central access policy on an object.

If you configure this policy setting, an audit event is generated each time a user accesses an object and the permission granted by the current central access policy on the object differs from that granted by the proposed policy.

Volume: Unknown

Microsoft recommendation: Enable this subcategory if you need to test or troubleshoot Dynamic Access Control Proposed Central Access Policies.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy.

Logmanager recommendation: Leave not configured.

Logmanager

Policy Change

Policy Change audit events allow you to track 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.

Audit Policy Change

Description: This policy determines whether the operating system generates audit events when changes are made to audit policy.

Volume: Low

Microsoft recommendation: Almost all events in this subcategory have security relevance and should be monitored.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4715	The audit policy (SACL) on an object was changed.
4719	System audit policy was changed.
4817	Auditing settings on an object were changed.
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 object were changed.
4908	Special Groups Logon table modified.
4912	Per User Audit Policy was changed.

Logmanager recommendation: Success. EventID 4719 can be especially important as it allows detailed monitoring of Advanced Audit Policy settings. Any changes made to any subcategory in AAP will be logged with information - who made the change and to which policy.

Logmanager

Authentication Policy Change

Description: This policy determines whether the operating system generates audit events when changes are made to authentication policy.

Changes made to authentication policy include:

- Creation, modification, and removal of forest and domain trusts.
- Changes to Kerberos policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy.
- When any of the following user logon rights is 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-level and forest-level trust and privileges that are granted to user accounts or groups.

Volume: Low

Microsoft recommendation: On domain controllers, it is important to enable Success audit for this subcategory to be able to get information related to operations with domain and forest trusts, changes in Kerberos policy and some other events included in this subcategory.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4713	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	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.

Logmanager recommendation: Success.

Logmanager

Authorization Policy Change

Description: This policy allows you to audit assignment and removal of user rights in user right policies, changes in security token object permission, resource attributes changes and Central Access Policy changes for file system objects.

Volume: Depends

Microsoft recommendation: With Success auditing for this subcategory, you can get information related to changes in user rights policies, or changes of resource attributes or Central Access Policy applied to file system objects.

However, if you are using an application or system service that makes changes to system privileges through the AdjustPrivilegesToken API, we do not recommend Success auditing because of the high volume of events "4703(S): A user right was adjusted" that may be generated. As of Windows 10, event 4703 is generated by applications or services that dynamically adjust token privileges. An example of such an application is Microsoft Endpoint Configuration Manager, which makes WMI queries at recurring intervals and quickly generates a large number of 4703 events (with the WMI activity listed as coming from svchost.exe).

If one of your applications or services is generating a large number of 4703 events, you might find that your event-management software has filtering logic that can automatically discard the recurring events, which would make it easier to work with Success auditing for this category.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
4703	A user right was adjusted.
4704	A user right was assigned.
4705	A user right was removed.
4706	A new trust was created to a domain.
4707	A trust to a domain was removed.
4714	Encrypted data recovery policy was changed.
4911	Resource attributes of the object were changed.
4913	Central Access Policy on the object was changed.

Logmanager recommendation: Leave not configured.

Logmanager

Filtering Platform Policy Change

Description: This policy allows you to audit events generated by changes to the Windows Filtering Platform (WFP), such as the following:

- IPsec services status.
- Changes to IPsec policy settings.
- Changes to Windows Filtering Platform Base Filtering Engine policy settings.
- Changes to WFP providers and engine.

Volume: Unknown

Microsoft recommendation: No recommendation.

Event ID	Description
4709	IPsec Services was started.
4710	IPsec Services was disabled.
4711	May contain any one of the following: PAStore Engine applied 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 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.
5047	A change has been made to IPsec settings. A Crypto Set was modified.
5048	A change has been made to IPsec settings. A Crypto Set was deleted.

5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
5446	A Windows Filtering Platform callout has been changed.
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 locally cached copy of Active Directory storage IPsec policy on the computer.
5459	PAStore Engine failed to apply 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 quick mode filter.

Logmanager recommendation: Leave not configured unless you have a specific need for events in this subcategory.

Logmanager

MPSSVC Rule-Level Policy Change

Description: This policy determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe).

The Microsoft Protection Service, which is used by Windows Firewall, is an integral part of the computer's threat protection against malware. 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.

Volume: Medium

Microsoft recommendation: Success events shows you changes in Windows Firewall rules and settings, active configuration and rules after Windows Firewall Service startup and default configuration restore actions. Failure events may help to identify configuration problems with Windows Firewall rules or settings.

Event ID	Description
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 Windows Firewall exception list. A rule was added.
4947	A change has been made to Windows Firewall exception list. A rule was modified.
4948	A change has been made to 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:

Logmanager recommendation: Success and Failure.

Logmanager

Other Policy Change Events

Description: This policy contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Volume: Low

Microsoft recommendation: We do not recommend Success auditing because of the event "5447: A Windows Filtering Platform filter has been changed"—this event generates many times during group policy updates and typically is used for troubleshooting purposes for Windows Filtering Platform filters. But you would still need to enable Success auditing for this subcategory if, for example, you must monitor changes in Boot Configuration Data or Central Access Policies.

We recommend Failure auditing, to detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.

Event ID	Description
4819	Central Access Policies on the machine have been changed.
4826	Boot Configuration Data loaded.
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 security policy in the group policy objects.

Logmanager recommendation: Leave not configured.

Logmanager

Privilege Use

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

Non-Sensitive Privilege Use

Description: This policy contains events that show usage of non-sensitive privileges. This is the list of non-sensitive privileges:

Access Credential Manager as a trusted caller	Create global objects
Add workstations to domain	Create permanent shared objects
Adjust memory quotas for a process	Create symbolic links
Bypass traverse checking	Force shutdown from a remote system
Change the system time	Increase a process working set
Change the time zone	Increase scheduling priority
Create a page file	Lock pages in memory
Modify an object label	Profile system performance
Perform volume maintenance tasks	Remove computer from docking station
Profile single process	Shut down the system
Synchronize directory service data	

This subcategory also contains informational events from filesystem Transaction Manager.

Volume: Very High

Microsoft recommendation: We do not recommend Success auditing because the volume of events is very high and typically, they are not as important as events from Audit Sensitive Privilege Use subcategory.

You can enable Failure auditing if you need information about failed attempts to use nonsensitive privileges, for example, SeShutdownPrivilege or SeRemoteShutdownPrivilege.

Event ID	Description
4673	A privileged service was called.
4674	An operation was attempted on a privileged object.
4985	The state of a transaction has changed.

Logmanager recommendation: Leave not configured. The volume of data configured by this policy is high but potential gains are low – there is too little information in the events to determine what operation actually occurred as it is not clear which privilege is required for which operation.

Logmanager

Sensitive Privilege Use

Description: This policy contains events that show the usage of sensitive privileges. This is the list of sensitive privileges:

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

The use of two privileges, "Back up files and directories" and "Restore files and directories," generate events only if the "Audit: Audit the use of Backup and Restore privilege" Group Policy setting is enabled on the computer or device. We do not recommend enabling this Group Policy setting because of the high number of events recorded.

This subcategory also contains informational events from the file system Transaction Manager.

Volume: High

Microsoft recommendation: We recommend tracking Success and Failure for this subcategory of events, especially if the sensitive privileges were used by a user account.

Event ID	Description
4673	A privileged service was called.
4674	An operation was attempted on a privileged object.
4985	The state of a transaction has changed.

Logmanager recommendation: Leave not configured. The volume of data configured by this policy is high but potential gains are low – there is too little information in the events to determine what operation actually occurred as it is not clear which privilege is required for which operation.

Other Privilege Use Events

Description: This policy should not have any events in it, but for some reason Success auditing will enable generation of event 4985(S): The state of a transaction has changed.

Volume: Unknown

Microsoft recommendation: This auditing subcategory doesn't have any informative events inside.

Event ID	Description
4985	The state of a transaction has changed.

Logmanager recommendation: Leave not configured.

Logmanager

System

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

IPsec Driver

Description: This policy allows you to audit events generated by IPSec drivers such as the following:

- Startup and shutdown of the IPsec services.
- Network packets dropped due to integrity check failure.
- Network packets dropped due to replay check failure.
- Network packets dropped due to being in plaintext.
- Network packets received with incorrect Security Parameter Index (SPI). This may indicate that either the network card is not working correctly or the driver needs to be updated.
- Inability 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 that is provided by the IPsec filter.

Volume: Medium

Microsoft recommendation: There is no recommendation for this subcategory.

Event ID	Description
4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that 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 has started successfully.
5479	IPsec Services has 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 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 plug-and-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.

Logmanager recommendation: Leave not configured.

Logmanager

Other System Events

Description: This policy contains Windows Firewall Service and Windows Firewall driver start and stop events, failure events for these services and Windows Firewall Service policy processing failures.

Audit Other System Events determines whether the operating system audits various system events.

The system events in this category include:

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

Volume: Low

Microsoft recommendation: We recommend enabling Success and Failure auditing because you will be able to get Windows Firewall Service and Windows Firewall Driver status events.

Event ID	Description
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 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.
5050	An attempt to programmatically disable the Windows Firewall was rejected because this API is not supported on Windows Vista.
5058	Key file operation.
5059	Key migration operation.
5071	Key access denied by Microsoft key distribution service.
6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
6401	BranchCache: Received invalid data from a peer. Data discarded.

6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.
6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
6405	BranchCache: %2 instance(s) of event id %1 occurred.
6406	%1 registered to Windows Firewall to control filtering for the following: %2
6407	1%
6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2
6409	BranchCache: A service connection point object could not be parsed.

Logmanager recommendation: Success and Failure. Volume of the events is low and you will be able to track the state of Windows Defender and Firewall – you can setup and alert if either gets disabled.

Logmanager

Security State Change

Description: This policy contains Windows startup, recovery, and shutdown events, and information about changes in system time.

Volume: Low

Microsoft recommendation: Success. The volume of events in this subcategory is very low and all of them are important events and have security relevance.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

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

Logmanager recommendation: Success. Event 4621 will tell you that system crashed because it could not record new Security events – which would enable malicious actor to interfere with system without being tracked. We were unable to generate this event in our lab, but due to the low volume of data generated by this policy, there is no harm in enabling it.

__Note:__ CrashOnAuditFail has to be enabled in policy "Audit: Shut down system immediately if unable to log security audits" for event 4621 to be generated.

Logmanager

Security System Extension

Description: This policy contains information about the loading of an authentication package, notification package, or security package, plus information about trusted logon process registration events.

Changes to security system extensions in the operating system include the following activities:

- Security extension code is loaded (for example, an authentication, notification, or security package). 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 extension code are Security Support Providers, such as Kerberos and NTLM.
- 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.

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

Volume: Low

Microsoft recommendation: Success. The main reason why Success auditing is recommended for this subcategory is "4697(S): A service was installed in the system."

For other events it is strongly recommended monitoring an allow list of allowed security extensions (authenticated packages, logon processes, notification packages, and security packages). Otherwise, it's hard to pull useful information from these events, except event 4611 which typically should have "SYSTEM" as value for "Subject" field.

This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

Event ID	Description
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.

Logmanager recommendation: Success. Event 4697 will inform you whenever there is a new service added to a system, which should be a planned activity, especially on high-value assets. If this event triggers an unexpected value, investigate the reason.

Logmanager

System Integrity

Description: This policy determines whether the operating system audits events that violate the integrity of the security subsystem.

Activities that violate the integrity of the security subsystem include the following:

- Audited events are lost due to a failure of the auditing system.
- A process uses an invalid local procedure call (LPC) port in an attempt 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.
- Cryptographic tasks are performed.

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

Volume: Low

Microsoft recommendation: Success and Failure. The main reason why we recommend Success auditing for this subcategory is to be able to get RPC integrity violation errors and auditing subsystem errors (event 4612). However, if you are planning to manually invoke "4618(S): A monitored security event pattern has occurred", then you also need to enable Success auditing for this subcategory.

The main reason why we recommend Failure auditing for this subcategory is to be able to get Code Integrity failure events.

Event ID	Description
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	A cryptographic primitive operation failed.
5060	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.

6410	Code integrity determined that a file does not meet the security requirements to load into a process.
6417	The FIPS mode crypto self-tests succeeded.
6418	The FIPS mode crypto self-tests failed.

Logmanager recommendation: Leave not configured. We had not been able to trigger events in this category.

Logmanager

Global Object Access Auditing

Global Object Access Auditing policy settings allow administrators to define computer system access control lists (SACLs) per object type for either the file system or registry. The specified SACL is then automatically applied to every object of that type.

Registry (Global Object Access Auditing)

This topic for the IT professional describes the Advanced Security Audit policy setting, Registry (Global Object Access Auditing), which enables you to configure a global system access control list (SACL) on the registry of a computer.

If you select the Configure security check box on this policy's property page, you can add a user or group to the global SACL. This enables you to define computer system access control lists (SACLs) per object type for the registry. The specified SACL is then automatically applied to every registry object type.

This policy setting must be used in combination with the Registry security policy setting under Object Access.

File System (Global Object Access Auditing)

This topic for the IT professional describes the Advanced Security Audit policy setting, File System (Global Object Access Auditing), which enables you to configure a global system access control list (SACL) on the file system for an entire computer.

If you select the Configure security check box on the policy's property page, you can add a user or group to the global SACL. This enables you to define computer system access control lists (SACLs) per object type for the file system. The specified SACL is then automatically applied to every file system object type.

If both a file or folder SACL and a global SACL are configured on a computer, the effective SACL is derived by combining the file or folder SACL and the global SACL. This means that an audit event is generated if an activity matches either the file or folder SACL or the global SACL. This policy setting must be used in combination with the File System security policy setting under Object Access.

Logmanager

Whitepaper author note

This document is exclusively written for security administrators who utilize Logmanager Security Event Management systems. Logmanager does not apply any licensing scheme and is capable of handling an excessive amount of the logs (up to 3000EPS). This is necessary, because advanced audit configuration can create a lot of data. All this without excessive complexity and/or additional load of source systems CPU. Sure, Logmanager processes up to the physical limit of the given appliance model. Upon collection of logs in near-real time, Logmanager is capable of transforming collected data into a well-defined powerful database. Collected data can be accessed by operators via a set of predefined customizable dashboards or structured and full text searches. Logmanager provides easy to use graphical display, automated classification, customizable alerts, alerts with thresholds, correlations, access to data via REST API and overall system scalability. All this to deliver wide visibility into collected machine data, not only from Windows, but from hundreds of other supported sources. We apply no limits while bringing radical simplicity to complex use cases.

Please visit www.logmanager.com for more information.

Warning: Using this guide with other SEM/SIEM solutions can create an excessively high number of logs and overload your 3rd party system or deplete your product license scheme quickly. Consider replacing Your SEM/SIEM with Logmanager. We do not apply any licensing restrictions.

Many thanks for choosing Logmanager.