	Audit Policy Subcategories	What to Enable		Where to Enable & Expected Volume			Associated Events	Description
		Success	Failures	Workstations	Servers	DCs		
Account Logon	**Audit Credential Validation**	Yes	Yes	Low	Low	High	4774: An account was mapped for logon. 4775: An account could not be mapped for logon. 4776: The computer attempted to validate the credentials for an account. 4777: The domain controller failed to validate the credentials for an account.	Determines whether the operating system generates audit events on credentials that are submitted for a user account logon request. The main reason to enable this auditing subcategory is to handle local accounts authentication attempts and, for domain accounts, NTLM authentication in the domain. It is especially useful for monitoring unsuccessful attempts, to find brute-force attacks, account enumeration, and potential account compromise events on domain controllers.
	Audit Kerberos Authentication Service	Yes	Yes	Do not enable	Do not enable	High	4768: A Kerberos service ticket was requested. 4771: A Kerberos service ticket was renewed. 4772: A Kerberos service ticket request failed.	An audit event is generated after a Kerberos authentication TGT request. An audit event is generated after a Kerberos authentication TGT request. Success audits record successful attempts and Failure audits record unsuccessful attempts.
	Audit Kerberos Service Ticket Operations	Yes	Yes	Do not enable	Do not enable	Very High	4769: A Kerberos service ticket was requested. 4770: A Kerberos service ticket was renewed. 4771: A Kerberos service ticket request failed.	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.
Account Management	**Audit Computer Account Management**	Yes	No	Do not enable	Do not enable	Low	4741: A computer account was created. 4742: A computer account was changed. 4743: A computer account was deleted.	Determines whether the operating system generates audit events when a computer account is created, changed, or deleted. This policy setting is useful for tracking account-related changes to computers that are members of a domain.
	Audit Other Account Management Events	Yes	No	Do not enable	Do not enable	Low	4782: The password hash of an account was accessed.	Determines whether the operating system generates user account management audit events. This subcategory allows you to audit next events: - The password hash of a user account was accessed. This happens during an Active Directory Management Tool password migration. - The Password Policy Checking API was called. Password Policy Checking API allows an application to check password compliance against an application-provided account database or single account and verify that passwords meet the complexity, aging, minimum length, and history reuse requirements of a password policy.
	Audit Security Group Management	Yes	No	Low	Low	Low	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. 4764: A group's type was changed. 4799: A security-enabled local group membership was enumerated.	Determines whether the operating system generates audit events when specific security group management tasks are performed. This subcategory allows you to audit events generated by changes to security groups such as the following: - Security group is created, changed, or deleted. - Member is added or removed from a security group. - Group type is changed.
	Audit User Account Management	Yes	Yes	Low	Low	Low	4720: A user account was created. 4722: A user account was enabled. 4723: An attempt was made to change an account's password. 4724: An attempt was made to reset an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4765: SID History was added to an account. 4766: An attempt to add SID History to an account failed. 4767: A user account was unlocked. 4780: The ACL was set on accounts which are members of administrator's groups. 4781: The name of an account was changed. 4794: An attempt was made to set the Directory Services Restore Mode administrator password. 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.	Determines whether the operating system generates audit events when specific user account management tasks are performed. This policy setting allows you to audit changes to user accounts. Events include the following: - A user account is created, changed, deleted, renamed, disabled, enabled, locked out or unlocked. - A user account's password is set or changed. - A security identifier (SID) is added to the SID History of a user account, or fails to be added. - The Directory Services Restore Mode password is configured. - Permissions on administrative user accounts are changed. - A user's local group membership was enumerated. - Credential Manager credentials are backed up or restored.
Detailed Tracking	**Audit Process Creation**	Yes	Yes	Medium	Medium	Medium	4688: A new process has been created. 4696: A primary token was assigned to process.	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.
Logon and Logoff	**Audit Account Lockout**	Yes	Yes	Low	Low	Low	4625: An account failed to log on.	Generated when an account cannot log on to a computer because the account is locked out and is essential for understanding user activity and detecting potential attacks.
	Audit Logon	Yes	Yes	Low	Medium	Medium	4624: An account was successfully logged on. 4625: An account failed to log on. 4648: A logon was attempted using explicit credentials. 4675: SIDs were filtered.	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.
	Audit Other Logon/Logoff Events	Yes	Yes	Low	Low	Low	4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5378: The requested credentials delegation was disallowed by policy. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network.	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 the computer account. - A user is granted access to a wired 802.1x network. It can be either a user account or the computer account. Logon events are essential to understanding user activity and detecting potential attacks.
	Audit Special Logon	Yes	No	Low	Medium	Medium	4964: Special groups have been assigned to a new logon. 4672: Special privileges assigned to new logon.	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.
Object Access	**Audit Certification Services**	Yes	No	Do not enable	Low - Medium (if Certificate Services is installed)	Low - Medium (if Certificate Services is installed)	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.	Determines whether the operating system generates events when Active Directory Certificate Services (AD CS) operations are performed.
	Audit Detailed File Share	No	Yes	Low	High (if configured as file server) Low (with no network shares)	High (Group Policies need network access to SYSVOL)	5145: A network share object was checked to see whether client can be granted desired access.	Allows you to audit attempts to access files and folders on a shared folder. 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.
	Audit File Share	Yes	Yes	Low	High (if configured as file server) Low (with no network shares)	High (Group Policies need network access to SYSVOL)	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.	Audit events related to file shares: creation, deletion, modification, and access attempts. Also, it shows failed SMB SPN checks. 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.
	Audit Other Object Access	Yes	Yes	Low	Low	Low	4671: An application attempted to access a blocked ordinal through the TBS. 4691: Indirect access to an object was requested. 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. 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. 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.	Access Events allows you to monitor operations with scheduled tasks, COM+ objects and indirect object access requests.
	Audit Removable Storage	Yes	No	Low	Low	Low	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.	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 object's SACL.
Policy Change	**Audit Policy Change**	Yes	No	Low	Low	Low	4715: The audit policy (SACL) on an object was changed. 4719: System audit policy was changed. 4817: Auditing settings on object were changed. 4902: The Per-user audit policy table was created. 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. 4904: An attempt was made to register a security event source. 4905: An attempt was made to unregister a security event source.	Determines whether the operating system generates audit events when changes are made to audit policy.
	Audit Authentication Policy Change	Yes	No	Low	Low	Low	4670: Permissions on an object were changed 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4716: Trusted domain information was modified. 4713: Kerberos policy was changed. 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.	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.
	Audit MPSSVC Rule-Level Policy Change	Yes	Yes	Medium	Medium	Medium	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:	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. - Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

	Audit Other Policy Change Events	No	Yes	Low	Low	Low	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.	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.
System	**Audit Other System Events**	Yes	Yes	Low	Low	Low	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 was stopped. 5035: The Windows Firewall Driver failed to start. 5037: The Windows Firewall Driver detected critical runtime error. Terminating. 5058: Key file operation. 5059: Key migration operation. 6400: BranchCache: Received an incorrectly formatted response while discovering 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.	Contains Windows Firewall Service and Windows Firewall driver start and stop events, failure events for these services and Windows Firewall Service policy processing failures. 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.
	Audit Security State Change	Yes	No	Low	Low	Low	4608: Windows is starting up. 4616: The system time was changed. 4621: Administrator recovered system from CrashOnAuditFail.	Contains Windows startup, recovery, and shutdown events, and information about changes in system time. 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.
	Audit Security System Extension	Yes	No	Low	Low	Low	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.	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.
	Audit System Integrity	Yes	Yes	Low	Low	Low	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. 5062: A kernel-mode cryptographic self-test was performed. 5057: A cryptographic primitive operation failed. 5060: Verification operation failed. 5061: Cryptographic operation. 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.	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.

Notes: Based on Microsoft recommendations found at the following URLs:
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-credential-validation
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-account-logon-events

Asterix (ATC Standard)					
ATMA					
BACNet					
Common Industrial Protocol (CIP)					
Component Network over IP (CN/IP)					
Constrained Application Protocol (CoAP)					
Controller Area Network (CAN) over Ethernet (ISO 11898)					
Crimson					
Cygnet					
Distributed Interactive Simulation (DIS)	https://en.wikipedia.org/wiki/Distributed_Interactive_Simulation				
Direct Message Protocol (DMP)	https://wiki.wireshark.org/Protocols/dmp				
Distributed Network Protocol (DNP3)	https://en.wikipedia.org/wiki/DNP3				
ECHONET Lite					
ELCOM 90					
Elipse E3					
Ether S Bus					
Eher S I/O					
EtherCat					
Ethernet/IP					
Ethernet Global Data					
FBNet					
HDCP2 over TCP					
Hart IP					
Historical Oltec GmbH					
ICCP					
IEC 60870-5-104					
Train Communication Network (TCN) Train Real-time Data Protocol (TRDP) (IEC 61375-2-3)					
Manufacturing Message Specification (MMS) (IEC 61850)					
IENA					
Integrated Network Enhanced Telemetry (iNetX)					
KNXnet/IP					
MTConnect					
Modbus					
Modbus ASCII					
Modbus CANOpen					
Motorola MDLC					
OPC Classic (Data Access - DA, Alarms & Events - AE, Historical Data Access - HDA, Complex Data, Data eXchange, XML-DA)					
OPC Unified Architecture (UA) XML					
OPC Unified Architecture (UA) Binary					
Robot Operating System (ROS)					
Remote Operations Controller Protocol (ROC)					
STANAG 4406 Military Messaging					
SafetyNET p Protocol					
Scalable service-Oriented Middleware over IP (SOME/IP)					
The Unity protocol (UMAS)					
Totalflow Protocol					
ZigBee Encapsulation Protocol					
xPL Protocol					
BSAP (Bristol Standard Asynchronous/Synchronous Protocol)					
DLMS/COSEM - IEC62056					

IEC61400					
MELSEC Q 3E Binary Frame					
MELSOFT protocol					
Omron FINS protocol					
Priva Building Management					
Profinet CBA					
S7 Protocol					
Synchrophasor Protocol (IEEE C37.118)					

		Palo Alto	Check Point	Ultra Electronics	Tofino
Modbus					
	Function	Y	Y		
	Unit ID	N	Y		
	Address	N	Y		
	Value	N	writes only		
CIP					
	Function		Y		
	Unit ID		Y		
	Address		N		
	Value		N		
DNP3					
	Function		Y		
	Address		Y		
	Group		Y		
	Value		N		
IEC 104					
	Function		Y		
	Unit ID		Y		
	Address		Y		
	Value		Y		