System Audit Policy recommendations

By robinharwood

Archived: 2026-04-06 15:16:14 UTC

This article covers the Windows audit policy settings and Microsoft's baseline and advanced recommendations for both workstations and servers. It provides guidance to help administrators choose appropriate audit policies based on their organization's needs.

The Security Compliance Manager (SCM) baseline recommendations shown here, along with the recommended settings to help detect system compromise, are intended only to be a starting baseline guide to administrators. Each organization must make its own decisions regarding the threats they face, their acceptable risk tolerances, and what audit policy categories or subcategories they should enable. Administrators without a thoughtful audit policy in place are encouraged to start with the settings recommended here, and then to modify and test before implementing in their production environment.

The recommendations are for enterprise-class computers, which Microsoft defines as computers that have average security requirements and require a high level of operational functionality. Entities needing higher security requirements should consider more aggressive audit policies.

The following baseline audit policy settings are recommended for normal security computers that aren't known to be under active, successful attack by determined adversaries or malware.

This section contains tables that list the audit setting recommendations that apply to the Windows operating system (OS) for both client and server.

System Audit Policy table legend

Notation	Recommendation
Yes	Enable in general scenarios
No	Don't enable in general scenarios
If	Enable if needed for a specific scenario, or if a role or feature for which auditing is desired is installed on the machine
DC	Enable on domain controllers
[Blank]	No recommendation

These tables contain the Windows default setting, the baseline recommendations, and stronger recommendations for which OS platform you're running.

- Windows Client

- Windows Server

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Account Logon			
Audit Credential Validation	`No | No`	`Yes | No`	`Yes | Yes`
Audit Kerberos Authentication Service			`Yes | Yes`
Audit Kerberos Service Ticket Operations			`Yes | Yes`
Audit Other Account Logon Events			`Yes | Yes`
Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Account Management			
Audit Application Group Management			
Audit Computer Account Management		`Yes | No`	`Yes | Yes`
Audit Distribution Group Management			
Audit Other Account Management Events		`Yes | No`	`Yes | Yes`
Audit Security Group Management		`Yes | No`	`Yes | Yes`
Audit User Account Management	`Yes | No`	`Yes | No`	`Yes | Yes`

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Detailed Tracking			
Audit DPAPI Activity			`Yes | Yes`
Audit Process Creation		`Yes | No`	`Yes | Yes`
Audit Process Termination			
Audit RPC Events			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
DS Access			
Audit Detailed Directory Service Replication			
Audit Directory Service Access			
Audit Directory Service Changes			
Audit Directory Service Replication			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Logon and Logoff			
Audit Account Lockout	`Yes | No`		`Yes | No`
Audit User/Device Claims			
Audit IPsec Extended Mode			
Audit IPsec Main Mode			`IF | IF`
Audit IPsec Quick Mode			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Audit Logoff	`Yes | No`	`Yes | No`	`Yes | No`
Audit Logon [1]	`Yes | Yes`	`Yes | Yes`	`Yes | Yes`
Audit Network Policy Server	`Yes | Yes`		
Audit Other Logon/Logoff Events			
Audit Special Logon	`Yes | No`	`Yes | No`	`Yes | Yes`

[1] Beginning with Windows 10 version 1809, Audit Logon is enabled by default for both Success and Failure. In previous versions of Windows, only Success is enabled by default.

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Object Access			
Audit Application Generated			
Audit Certification Services			
Audit Detailed File Share			
Audit File Share			
Audit File System			
Audit Filtering Platform Connection			
Audit Filtering Platform Packet Drop			
Audit Handle Manipulation			
Audit Kernel Object			
Audit Other Object Access Events			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Audit Registry			
Audit Removable Storage			
Audit SAM			
Audit Central Access Policy Staging			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Policy Change			
Audit Audit Policy Change	`Yes | No`	`Yes | Yes`	`Yes | Yes`
Audit Authentication Policy Change	`Yes | No`	`Yes | No`	`Yes | Yes`
Audit Authorization Policy Change			
Audit Filtering Platform Policy Change			
Audit MPSSVC Rule-Level Policy Change			`Yes`
Audit Other Policy Change Events			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Privilege Use			
Audit Non Sensitive Privilege Use			

Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Audit Other Privilege Use Events			
Audit Sensitive Privilege Use			
Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
System			
Audit IPsec Driver		`Yes | Yes`	`Yes | Yes`
Audit Other System Events	`Yes | Yes`		
Audit Security State Change	`Yes | No`	`Yes | Yes`	`Yes | Yes`
Audit Security System Extension		`Yes | Yes`	`Yes | Yes`
Audit System Integrity	`Yes | Yes`	`Yes | Yes`	`Yes | Yes`
Audit Policy Category or Subcategory	**Windows Default** `Success | Failure`	**Baseline Recommendation** `Success | Failure`	**Stronger Recommendation** `Success | Failure`
Global Object Access Auditing			
Audit IPsec Driver			
Audit Other System Events			
Audit Security State Change			
Audit Security System Extension			
Audit System Integrity			

Effective event log management requires monitoring both workstations and servers. Focusing solely on servers or domain controllers (DC) is a common oversight, as initial signs of malicious activity often appear on

workstations. By including workstations in your monitoring strategy, you gain access to critical early indicators of compromise.

Before you deploy any audit policy in a production environment, administrators should carefully review, test, and validate the policy to ensure it meets organizational security and operational requirements.

A perfect event ID to generate a security alert should contain the following attributes:

- High likelihood that occurrence indicates unauthorized activity
- Low number of false positives
- Occurrence should result in an investigative/forensics response

Two types of events should be monitored and alerted:

- Events where an occurrence is a strong indicator of unauthorized or suspicious activity.
- An accumulation of events above an expected and accepted baseline.

An example of the first event is:

If Domain Admins are forbidden from signing into the computers that aren't DCs, a single occurrence of a Domain Admin member logging on to an end-user workstation should generate an alert and be investigated. This type of alert is easy to generate by using the Audit Special Logon event 4964 (Special groups were assigned to a new logon). Other examples of single instance alerts include:

- If *Server A* should never connect to *Server B*, alert when they connect to each other.
- Alert if a standard user account is unexpectedly added to a privileged or sensitive security group.
- If employees in *factory location A* never work at night, alert when a user logs on at night.
- Alert if an unauthorized service is installed on a DC.
- Investigate if a regular end-user attempts to directly sign into a SQL Server for which they have no clear reason for doing so.
- If you have no members in your Domain Admin group, and someone adds themselves there, check it immediately.

An example of the second event is:

A high number of failed logon attempts might signal a password guessing attack. To detect this, organizations should first determine what is a normal rate of failed logons in their environment. Then alerts can be triggered when that baseline is exceeded.

For a comprehensive list of events that you should include when you monitor for signs of compromise, see Appendix L: Events to Monitor.

The following are the accounts, groups, and attributes that you should monitor to help you detect attempts to compromise your Active Directory Domain Services installation.

- Systems for disabling or removal of antivirus and anti-malware software (automatically restart protection when it's manually disabled)
- Administrator accounts for unauthorized changes
- Activities that are performed by using privileged accounts (automatically remove account when suspicious activities are completed or the allotted time expired)
- Privileged and VIP accounts in AD DS. Monitor for changes to attributes on the Account tab, such as:
    - cn
    - name
    - sAMAccountName
    - userPrincipalName
    - userAccountControl

  In addition to monitoring the accounts, restrict who can modify the accounts to as small a set of administrative users as possible. Refer to Appendix L: Events to Monitor for a list of recommended events to monitor, their criticality ratings, and an event message summary.
- Group servers by the classification of their workloads, which allows you to quickly identify the servers that should be the most closely monitored and most stringently configured
- Changes to the properties and membership of following AD DS groups:
    - Administrators
    - Domain Admins
    - Enterprise Admins
    - Schema Admins
- Disabled privileged accounts (such as built-in Administrator accounts in Active Directory and on member systems) for enabling the accounts
- Management accounts to log all writes to the account
- Built-in Security Configuration Wizard to configure service, registry, audit, and firewall settings to reduce the server's attack surface. Use this wizard if you implement jump servers as part of your administrative host strategy.

Review the following links for additional information about monitoring AD DS:

- Global Object Access Auditing is Magic
- Introducing Auditing Changes in Windows 2008
- Cool Auditing Tricks in Vista and 2008
- One-Stop Shop for Auditing in Windows Server 2008 and Windows Vista
- AD DS Auditing Step-by-Step Guide

All Event ID recommendations are accompanied by a criticality rating as follows:

Rating	Description
High	Event IDs with a high criticality rating should always and immediately be alerted and investigated.
Medium	An Event ID with a medium criticality rating could indicate malicious activity, but it must be accompanied by some other abnormality. An example can include an unusual number occurring in a particular time period, unexpected occurrences, or occurrences on a computer that normally wouldn't be expected to log the event. A medium-criticality event might also be collected as a metric and then compared over time.
Low	And Event ID with a low criticality events shouldn't garner attention or cause alerts, unless correlated with medium or high criticality events.

These recommendations are meant to provide a baseline guide for an administrator. All recommendations should be thoroughly reviewed before implementing in a production environment.

- Advanced Audit Policy Configuration settings
