Advanced security audit policy settings - Windows 10

By officedocspr

Archived: 2026-04-29 02:11:46 UTC

This reference for IT professionals provides information about:

- The advanced audit policy settings available in Windows
- The audit events that these settings generate.

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

- A group administrator has modified settings or data on servers that contain finance information.
- An employee within a defined group has accessed an important file.
- The correct system access control list (SACL) - as a verifiable safeguard against undetected access - is applied to either of the following:
    - every file and folder
    - registry key on a computer
    - file share.

You can access these audit policy settings through the Local Security Policy snap-in (secpol.msc) on the local computer or by using Group Policy.

These advanced audit policy settings allow you to select only the behaviors that you want to monitor. You can exclude audit results for the following types of behaviors:

- That are of little or no concern to you
- That create an excessive number of log entries.

In addition, because security audit policies can be applied by using domain Group Policy Objects, audit policy settings can be modified, tested, and deployed to selected users and groups with relative simplicity. Audit policy settings under **Security Settings\Advanced Audit Policy Configuration** are available in the following categories:

Configuring policy settings in this category can help you document attempts to authenticate account data on a domain controller or on a local Security Accounts Manager (SAM). Unlike Logon and Logoff policy settings and events, Account Logon settings and events focus on the account database that is used. This category includes the following subcategories:

- Audit Credential Validation
- Audit Kerberos Authentication Service
- Audit Kerberos Service Ticket Operations

- Audit Other Account Logon Events

The security audit policy settings in this category can be used to monitor changes to user and computer accounts and groups. This category includes the following subcategories:

- Audit Application Group Management
- Audit Computer Account Management
- Audit Distribution Group Management
- Audit Other Account Management Events
- Audit Security Group Management
- Audit User Account Management

Detailed Tracking security policy settings and audit events can be used for the following purposes:

- To monitor the activities of individual applications and users on that computer
- To understand how a computer is being used.

This category includes the following subcategories:

- Audit DPAPI Activity
- Audit PNP activity
- Audit Process Creation
- Audit Process Termination
- Audit RPC Events
- Audit Token Right Adjusted

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. This category includes the following subcategories:

- Audit Detailed Directory Service Replication
- Audit Directory Service Access
- Audit Directory Service Changes
- Audit Directory Service Replication

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. This category includes the following subcategories:

- Audit Account Lockout
- Audit User/Device Claims
- Audit IPsec Extended Mode
- Audit Group Membership
- Audit IPsec Main Mode
- Audit IPsec Quick Mode
- Audit Logoff

- Audit Logon
- Audit Network Policy Server
- Audit Other Logon/Logoff Events
- Audit Special Logon

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, 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; the Registry subcategory needs to be enabled to audit registry accesses.

Proving that these audit policies are in effect to an external auditor is more difficult. There is no easy way to verify that the proper SACLs are set on all inherited objects. To address this issue, see Global Object Access Auditing.

This category includes the following subcategories:

- 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 Registry
- Audit Removable Storage
- Audit SAM
- Audit Central Access Policy Staging

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, tracking changes (or its attempts) to these policies is an important aspect of security management for a network. This category includes the following subcategories:

- Audit Audit Policy Change
- Audit Authentication Policy Change
- Audit Authorization Policy Change
- Audit Filtering Platform Policy Change
- Audit MPSSVC Rule-Level Policy Change
- Audit Other Policy Change Events

Permissions 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 permissions on one or more systems. This

category includes the following subcategories:

- Audit Non-Sensitive Privilege Use
- Audit Sensitive Privilege Use
- Audit Other Privilege Use Events

System security policy settings and audit events allow you to track the following types of system-level changes to a computer:

- Not included in other categories
- Have potential security implications.

This category includes the following subcategories:

- Audit IPsec Driver
- Audit Other System Events
- Audit Security State Change
- Audit Security System Extension
- Audit System Integrity

Global Object Access Auditing policy settings allow administrators to define computer system access control lists (SACLs) per object type for the file system or for the registry. The specified SACL is then automatically applied to every object of that type. Auditors can prove that every resource in the system is protected by an audit policy. They can do this task by viewing the contents of the Global Object Access Auditing policy settings. For example, if auditors see a policy setting called "Track all changes made by group administrators," they know that this policy is in effect.

Resource SACLs are also useful for diagnostic scenarios. For example, administrators quickly identify which object in a system is denying a user access by:

- Setting the Global Object Access Auditing policy to log all the activities for a specific user
- Enabling the policy to track "Access denied" events for the file system or registry can help

Note

If a file or folder SACL and a Global Object Access Auditing policy setting (or a single registry setting SACL and a Global Object Access Auditing policy setting) are configured on a computer, the effective SACL is derived from combining the file or folder SACL and the Global Object Access Auditing policy. This means that an audit event is generated if an activity matches the file or folder SACL or the Global Object Access Auditing policy.

This category includes the following subcategories:

- File System (Global Object Access Auditing)
- Registry (Global Object Access Auditing)

- Basic security audit policy settings
