Advanced Audit Policy Configuration settings

By robinharwood

Archived: 2026-04-05 21:13:34 UTC

The Advanced Audit Policy Configuration settings are found under **Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies** in Group Policy. These settings enable organizations to monitor compliance with key business and security requirements by tracking specific activities, such as:

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 provide granular control over which activities are monitored, allowing you to focus on events that are most relevant to your organization. You can exclude auditing for actions that aren't important or that generate unnecessary log volume. Additionally, because these policies can be managed through domain Group Policy Objects, you can easily modify, test, and deploy audit configurations to specific users and groups as needed.

- **Account Logon**

  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, which track attempts to access a particular computer, settings and events in this category focus on the account database that is used. This category includes the following subcategories:

  ▶ Expand Audit Credential Validation policy
  ▶ Expand Audit Kerberos Authentication Service policy
  ▶ Expand Audit Kerberos Service Ticket Operations policy
  ▶ Expand Audit Other Account Logon Events

- **Account Management**

  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:

  ▶ Expand Audit Application Group Management policy
  ▶ Expand Audit Computer Account Management policy

- **Detailed Tracking**

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

- ▶ Expand Audit DPAPI Activity policy
- ▶ Expand Audit PNP Activity policy
- ▶ Expand Audit Process Creation policy
- ▶ Expand Audit Process Termination policy
- ▶ Expand Audit RPC Events policy
- ▶ Expand Audit Token Right Adjustment policy

- **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. This category includes the following subcategories:

  - ▶ Expand Audit Detailed Directory Service Replication policy
  - ▶ Expand Audit Directory Service Access policy
  - ▶ Expand Audit Directory Service Changes policy
  - ▶ Expand Audit Directory Service Replication policy

- **Logon/Logoff**

  Logon/Logoff security policy settings and audit events allow you to track attempts to sign into a computer interactively or over a network. These events are useful for tracking user activity and identifying potential attacks on network resources. This category includes the following subcategories:

  - ▶ Expand Audit Account Lockout policy
  - ▶ Expand Audit User / Device Claims
  - ▶ Expand Audit Group Membership policy
  - ▶ Expand Audit IPsec Extended Mode policy
  - ▶ Expand Audit IPsec Main Mode policy
  - ▶ Expand Audit IPsec Quick Mode policy
  - ▶ Expand Audit Logoff policy
  - ▶ Expand Audit Logon policy
  - ▶ Expand Audit Network Policy Server policy
  - ▶ Expand Audit Other Logon/Logoff Events policy
  - ▶ Expand Audit Special Logon policy

- **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. This category includes the following subcategories:

- ▶ Expand Audit Application Generated policy
- ▶ Expand Audit Certification Services policy
- ▶ Expand Audit Detailed File Share policy
- ▶ Expand Audit File Share policy
- ▶ Expand Audit File System policy
- ▶ Expand Audit Filtering Platform Connection policy
- ▶ Expand Audit Filtering Platform Packet Drop policy
- ▶ Expand Audit Handle Manipulation policy
- ▶ Expand Audit Kernel Object policy
- ▶ Expand Audit Other Object Access Events policy
- ▶ Expand Audit Registry policy
- ▶ Expand Audit Removable Storage policy
- ▶ Expand Audit SAM policy
- ▶ Expand Audit Central Access Policy Staging policy

- **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, monitoring changes or attempts to change these policies can be an important aspect of security management for a network. This category includes the following subcategories:

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

- **Privilege Use**

  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:

▶ Expand Audit Non-Sensitive Privilege Use policy
▶ Expand Audit Other Privilege Use Events policy
▶ Expand Audit Sensitive Privilege Use policy

- **System**

  System security policy settings and audit events allow you to track system-level changes to a computer that aren't included in other categories and that have potential security implications. This category includes the following subcategories:

▶ Expand Audit IPsec Driver policy
▶ Expand Audit Other System Events policy
▶ Expand Audit Security State Change policy
▶ Expand Audit Security System Extension policy
▶ Expand Audit System Integrity policy

- **Global Object Access**

  Global Object Access Auditing policy settings allow administrators to define computer 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 are able to prove that every resource in the system is protected by an audit policy 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, setting the Global Object Access Auditing policy to log all the activity for a specific user and enabling the policy to track "Access denied" events for the file system or registry can help administrators quickly identify which object in a system is denying a user access.

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

▶ Expand File System (Global Object Access Auditing) policy
▶ Expand Registry (Global Object Access Auditing) policy
