Audit Registry

By Archiveddocs

Archived: 2026-04-05 19:07:17 UTC

Applies To: Windows 7, Windows Server 2008 R2

This security policy setting determines whether the operating system audits user attempts to access registry objects. Audit events are only generated for objects that have configured system access control lists (SACLs) specified, 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 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.

Event volume: Low to medium, depending on how registry SACLs are configured

Default: Not configured

If this policy setting is configured, the following events are generated. The events appear on computers running Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows Vista.

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