Audit logon events - Windows 10

By vinaypamnani-msft

Archived: 2026-04-06 00:45:11 UTC

Determines whether to audit each instance of a user logging on to or logging off from a device.

Account logon events are generated on domain controllers for domain account activity and on local devices for local account activity. If both account logon and logon audit policy categories are enabled, logons that use a domain account generate a logon or logoff event on the workstation or server, and they generate an account logon event on the domain controller. Additionally, interactive logons to a member server or workstation that use a domain account generate a logon event on the domain controller as the logon scripts and policies are retrieved when a user logs on. For more info about account logon events, see Audit account logon events.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a logon attempt succeeds. Failure audits generate an audit entry when a logon attempt fails.

To set this value to **No auditing**, in the **Properties** dialog box for this policy setting, select the **Define these policy settings** check box and clear the **Success** and **Failure** check boxes.

For information about advanced security policy settings for logon events, see the Logon/logoff section in Advanced security audit policy settings.

You can configure this security setting by opening the appropriate policy under Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy.

Logon events	Description
4624	A user successfully logged on to a computer. For information about the type of logon, see the Logon Types table below.
4625	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
4634	The logoff process was completed for a user.
4647	A user initiated the logoff process.
4648	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
4779	A user disconnected a terminal server session without logging off.

When event 4624 (Legacy Windows Event ID 528) is logged, a logon type is also listed in the event log. The following table describes each logon type.

Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

- Basic security audit policy settings
