Windows logon auditing:

Everything you need to know in only 10 minutes

ManageEngine
ADAudit Plus

Table of Contents

Preface

Logon activity needs to be audited to meet various security, operational, and compliance requirements of an IT environment, such as:

- Detecting **unusual and potentially malicious activities** like a high volume of logon failures.
- Tracking the **active and idle time spent** by users at their workstations.
- Maintaining a **comprehensive audit trail** of logons occurring across the domain.
- And more.

So, it is imperative for administrators to audit logons. However the process of auditing logons has a steep learning curve. This guide provides you with concise information on logon auditing to make it easier for you to get on top of the process. It will take you through the auditing settings you need to configure to enable logging, the event IDs to track, the event fields to pay attention to, and how to overcome the limitations of native auditing.

Difference between authentication and logon

A logon occurs on the computer to which a user gains access, so it gets recorded in the local computer's security log. **Authentication (account logon) is performed by the computer on which the user's account resides,** so it gets recorded in either the local computer's security log (if a local user account is used) or the domain controller's (DC's) security log (if a domain user account is used). Kerberos and NTLM are the two protocols primarily used for authentication by Windows.

When a **local account** is used to log on to a computer, that computer performs both the logon and authentication. This is because local accounts are stored in the local database of member servers and workstations called the Security Account Manager (SAM). When a **domain account** is used to log on to a computer, the accessed computer performs the logon while a DC performs the authentication. This is because domain accounts are stored in the Active Directory database which resides on a DC. [1]

Logon and authentication can be better understood by delving into these **two common real world scenarios.**

First, let us assume Bob **buys a computer for personal use and logs into it.** The only type of account that he can log on with is a local user account, because the computer is standalone and not a part of any domain, and the only resources that he can access are those on the computer. In this case, both authentication and logon occur on the computer, so the corresponding account logon and logoff events are also logged in the very same computer.

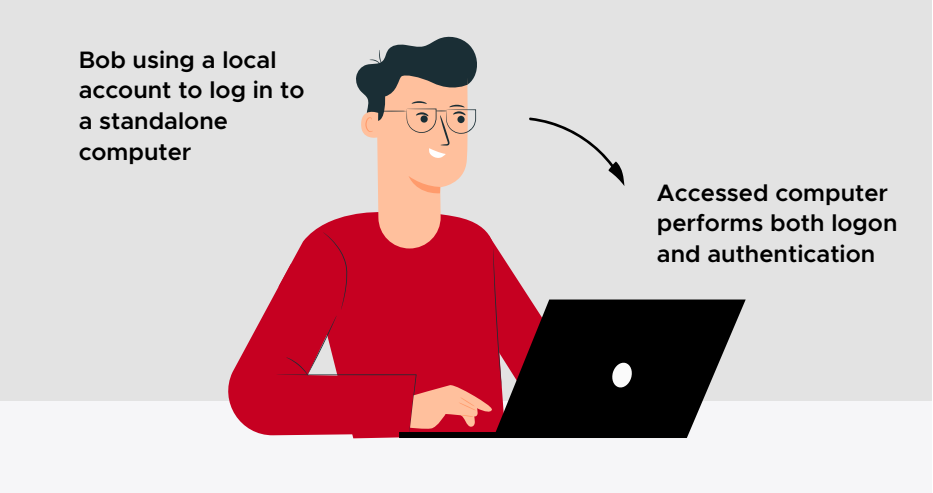

Image illustrating local logon

Next, let's assume Bob **logs into the computer allotted to him at his workplace,** which is a member of a domain. He can log on with either a local user account or a domain user account. In order to access resources on the domain, like a shared folder for example, let's assume he logs on with a domain user account. In this case, the computer can't perform the authentication, because the domain user account and its password hash aren't stored locally.

So the computer requests a DC to authenticate and an authentication event is logged in whichever DC handles the request. Once the user is authenticated, the computer proceeds with creating the logon session for the user and a logon event is recorded in its local security log.

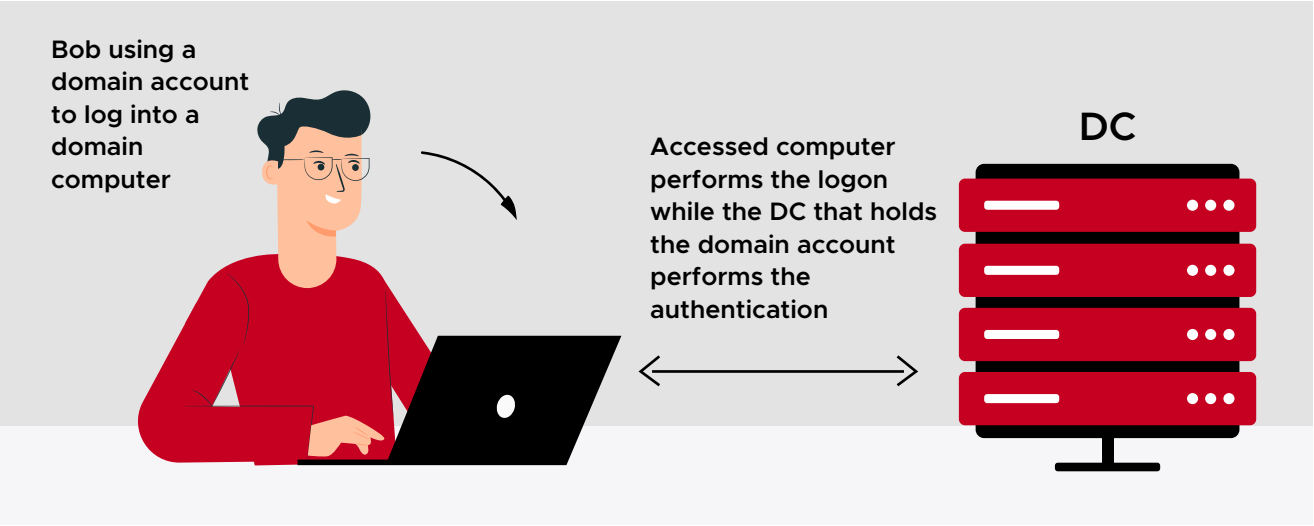

Image illustrating domain logon

Enabling logging via auditing policies

Security auditing must be configured to ensure that events are recorded whenever any logon activity occurs. Security auditing can be configured via audit policy settings or advanced audit policy settings.

Note: It is recommended that advanced audit policy settings are configured on systems running Windows Server 2008 R2 and above or Windows 7 and above. Advanced audit policies will be covered in more detail in this e-book.

Audit policy settings [2] can be found under **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy.**

The 2 categories of audit policy settings related to logon are:

Category	Helps track
Audit account logon events	Authentication of account data
Audit logon events	Accesses to a computer

Advanced audit policies [3] let administrators exercise granular control over which activities get logged, helping reduce event noise. Advanced audit policy settings can be found under **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policy.**

Of the 15 subcategories of advanced audit policy settings, **the 9 most important ones related to logon are:**

Category	Subcategory	Helps track	Event volume	Event IDs logged
Account Logon	Audit Credential Validation	NTLM authentication	High on DCs, low on member servers and workstations	4774, 4775, 4776, and 4777
	Audit Kerberos Authentication Service	Kerberos authentication ticket granting tickets (TGT)	High on DCs, does not get logged on member servers and workstations	4768, 4771, and 4772

	Audit Kerberos Service Ticket Operations	Kerberos service tickets (TGS)	High on DCs, does not get logged on member servers and workstations	4769, 4770, and 4773
	Audit Other Account Logon Events	Information not available (might help track events in the Account Logon category that don't fall under any of the other subcategories)	Information not available	Information not available
Logon/ Logoff	**Audit Account Lockout**	Failed attempt to log on to an account that's locked out	Low on DCs, member servers, and workstations	4625
	Audit Logoff	Logon sessions that are terminated	High on DCs, member servers and workstations	4634 and 4647
	Audit Logon	User attempts to log on to a computer	Medium on DCs and member servers, low on workstations	4624, 4625, 4648, and 4675
	Audit Other Logon/Logoff Events	Remote Desktop session connects and disconnects, workstation lock and unlock events, screen saver invoke and dismiss events, and a few other logon/logoff activities	Low on DCs, member servers and workstations	4649, 4778, 4779, 4800, 4801, 4802, 4803, 5378, 5632, and 5633
	Audit Special Logon	Logon by admins or members of special groups	Medium on DCs and member servers, low on workstations	4964 and 4672

Note: Event volume is not defined in numbers (MB per day, for example) because it varies based on the environment.

10 key points to keep in mind while enabling logging [4]

We recommend that you apply audit policies on a **per-computer basis** rather than per-user.

To enable logging on all computers in a domain, link the Group Policy Object (GPO) that contains the auditing settings to the domain. **To enable logging on specific computers in a domain,** link the GPO that contains the auditing settings to an organizational unit (OU) that contains the specific computers.

To configure auditing settings for a domain or an OU, ensure that you are logged in as a member of the **Domain Admins group.**

Choose what category or subcategory of auditing settings to configure. Keep in mind what **activities, resources, and users** you want to track and the **event volume** generated by a particular category or subcategory of settings. If you do not plan well, you might miss out on logging critical activity or end up logging too many activities, which will hinder auditors from spotting the suspicious ones.

Depending on the event volume generated, ensure that suitable **event log size and retention settings** are configured to prevent logs from getting overwritten. Event log settings can be found under **Computer Configuration > Policies > Windows Settings > Security Settings > Event Log.**

If you are configuring advanced audit policy settings (recommended), ensure force audit policy subcategory settings is enabled in order to override audit policy settings. To do so, navigate to **Local Polices > Security Options,** and enable **Audit: Force audit policy subcategory settings to override audit policy category settings.**

7

8

9

10

For each auditing setting, you can specify whether to **log success, log failure, log both,** or not log at all.

Microsoft's audit policy recommendations [5] for client computers running on Windows 7 and above and servers running on Windows Server 2008 and needing high security requirements are listed in the below table.

Subcategory	Recommendations
Audit Credential Validation	Log both success and failure
Audit Kerberos Authentication Service	Log both success and failure
Audit Kerberos Service Ticket Operations	Log both success and failure
Audit Other Account Logon Events	Log both success and failure
Audit Account Lockout	Log success
Audit Logoff	Log success
Audit Logon	Log both success and failure
Audit Special Logon	Log both success and failure

Note: In addition to the recommendations in the table above, you should:

- Log both success and failure for the Audit Other Logon/Logoff Events subcategory for only servers.
- Log both success and failure for the Audit IPsec Main Mode under specific scenarios for both servers and client computers.

To view a consolidated list of all auditing settings that will be applied, run the **Group Policy Results Wizard** found under the Group Policy Management Console.

To ensure that auditing settings are applied instantly instead of waiting for the next scheduled refresh, right-click on the domain or OU to which you linked the GPO and click on **Group Policy Update.**

12 critical event IDs to keep track of [6]

Once all auditing settings have been applied, corresponding events will be logged. To view these events, open the **Event Viewer,** navigate to Windows Logs > Security. Double-click on an event to view its properties.

Of the 69 events related to account logon and logon/logoff, **the 12 most important ones are:**

Category	Event ID	Description
Account Logon	4768	A Kerberos authentication ticket (TGT) was requested
	4769	A Kerberos service ticket was requested
	4771	Kerberos pre-authentication failed
Logon/Logoff	4624	Successful logon
	4625	Failed logon attempt
	4647	User-initiated logoff
	4778	Remote desktop session reconnected
	4779	Remote desktop session disconnected
	4800	Workstation locked
	4801	Workstation unlocked
	4802	Screen saver invoked
	4803	Screen saver dismissed

Note: This is not inclusive of Event IDs in legacy versions of Windows such as client computers running on Windows XP or earlier and servers running on Windows Server 2003 or earlier.

Logon types and failure codes

Logon types [7]

Logon types describe how a logon occurs on a computer. The logon type is one of the event fields of logon event ID, **4624**. The logon type helps with detecting potentially malicious activities such as a batch logon (type 4) being used by a member of a domain administrator group.

Of the 12 different logon types, **the 6 most common ones are:**

Logon type	Title	Logon occurs
2	Interactive	Via a computer's console
3	Network	When a resource (a shared folder for example) is accessed from a computer on the network
4	Batch Job	When a scheduled task runs as a specified account
5	Service	When a service runs as a specified account
10	RemoteInter-active	Via a remote session
11	CachedInter-active	Via cached domain credentials, such as when a user logs on to their computer when away from the network **Note:** Cached credentials are typically stored for the last 10 users logged on to a computer. When the eleventh user logs on to the computer, the cached credentials of the first user gets overwritten (the default value of 10 can be reset)

(Logon failure) Status codes [8]

These codes pinpoint the reason for logon failures, they are one of the event fields listed in the logon failure event ID, **4625.**

Of the many different codes, **the 10 most common ones are:**

Code	Logon failed because of
0xC0000064	Wrong user name
0xC000006A	Wrong user password
0xC0000234	Locked out user account being used
0xC0000072	Disabled user account being used
0xC000006F	Logon occurring outside authorized hours
0xC0000070	Logon occurring from an unauthorized workstation
0xC00000193	An expired user account being used
0xC0000071	An expired password being used
0xC0000133	Time sync missing between clocks on DC and other computer
0xC000015b	User not being granted the requested logon type at the computer

(Kerberos) Failure Codes [9]

These codes pinpoint the reason a Kerberos service ticket was denied, they are one of the event fields listed in Kerberos authentication event ID **4769.**

Of the many different codes, **the 8 most common are:**

Code	A Kerberos service ticket was denied because of
0x6	Wrong user name
0x7	A DC not being able to find the server's name
0x9	The master key is missing for the client or server
0xC	A logon restriction in place on a user's account, like a workstation restriction for example
0x12	A disabled, expired, or locked out user account being used
0x17	An expired password being used
0x18	A wrong user password
0x25	A missing time sync between clocks on the DC and the computer

Note: A sudden spike in failed authentication or logon activity due to wrong user name or password can be signs of a possible brute-force attack.

A few other important event fields to pay attention to

Only event fields specific to the important Account Logon via Kerberos and Logon/Logoff event IDs, namely 4768, 4769, 4771, 4624, 4625, and 4647, are covered here.

Event ID	Event field	Description	Helps track
4768, 4769, and 4771	**Client Address**	IP address of computer	Logon attempts from outside your internal IP range
4624, and 4625	**Source Network Address**		
4768	**User ID**	Security identifier (SID) of account	Logon from an account that should never be used, such as an expired or disabled one
4771, 4624, 4625, and 4647	**Security ID**		
4768, 4769, 4771, 4624, 4625, and 4647	**Account Name**	Logon name of account (computer account names end with $ character)	Logon from accounts that don't comply with your company's naming conventions (applicable only if you have a specific naming convention in place)
4624 and 4647	**Logon ID**	Hexadecimal value that helps correlate logon event ID 4624 with logoff initiated event ID 4647	Duration of a logon session
4624 and 4625	**Process Name**	Full path and the name of the executable	Potentially malicious software or software that is not authorized to request logon

How to overcome the limitations of native auditing

Event Viewer simply provides a view of event data. It is not designed to help administrators with auditing, as it has a few limitations. This section will shed light on three major limitations of auditing using Event Viewer and how ADAudit Plus helps overcome them.

Limitation 1

DCs, member servers, and workstations log only the logons occurring on them, and security logs do not get replicated between computers. So, **an organization's logon audit trail is fragmented across multiple computers.** You can leverage Windows Event Forwarding (WEF) to read logs on any computer and forward the events you choose to one or more Windows Event Collector (WEC) servers. However, successful WEF deployment requires expertise.

How ADAudit Plus helps overcome the limitation:

ADAudit Plus compiles data from all configured computers across the domain and **provides a central repository of logon information.**

Limitation 2

Each logon activity creates multiple events. Considering the huge volume of events that get logged, **using native tools to spot a critical event is a labor-intensive process that's like looking for a needle in a haystack.** You can attach a task to the security log and ask Windows to send you an email notification whenever a particular event ID is generated.

However, Windows can't raise red flags. For example, Windows can send you an email every time event ID 4776 is generated, but it will not be able to notify you about logon attempts from unauthorized computers, attempts occurring outside business hours, or attempts from expired accounts.

How ADAudit Plus helps overcome the limitation:

ADAudit Plus sorts through large reservoirs of event data and instantly pulls the information you are looking for. The solution lets you **define thresholds based on volume, time, and other criteria to detect critical activities** such as the ones discussed above (logon attempts from an unauthorized computer, attempts occurring outside business hours, or attempts from an expired account). You can also choose to get instantly notified via email and SMS of critical activities.

Limitation 3

In some cases, Windows provides severely limited information, which impedes the **correlation necessary to get the full picture.** For example, to calculate the duration of a logon session, logon event ID 4624 needs to be correlated with the logoff-initiated event ID 4647 using the Logon ID event field.

How ADAudit Plus helps overcome the limitation: ADAudit Plus **processes logs and establishes a connection between them** to provide you with the full picture. For example, its User Work Hours report correlates multiple events related to user logon and log off times, workstation lock and unlock times, and screen saver start and stop times to provide you with information on the active and idle time spent by users at their workstations.

Other highlights of ADAudit Plus: ADAudit Plus provides several other critical functions to help you easily meet your security, operational, and compliance requirements.

With ADAudit Plus, you can:

- Track **suspicious activities** such as a spike in logon failures, users logged on to multiple computers, authentication occurring via NTLM protocol, and more.
- Leverage user behavior analytics **(UBA)** to establish activity patterns and spot subtle anomalies such as an unusual time of logon for a particular user.
- Execute scripts to automate **response actions,** like shutting down a device or disabling an account.
- Monitor **employee attendance** and actual work hours.
- Automate the generation of logon audit trails to pass **compliance audits** such as SOX, HIPAA, PCI DSS, GLBA, FISMA, the GDPR, and ISO 27001.

What's more, you can go from downloading ADAudit Plus to receiving logon notifications and reports in **an hour.**

Learn more about how ADAudit Plus can help you audit:

- Logon and logoff
- Logon failures
- Account lockouts
- Remote employee working hours
- Remote desktop connections

Related resources and references

Related resources:

- How to configure advanced audit policies
- Windows security event log library
- How to audit account logon events
- How to audit Kerberos authentication events
- How to keep track of employee hours
- Logon auditing webinar

References:

- [1] Local and domain logon
- [2] Basic audit policy settings
- [3] Advanced audit policy settings
- [4] Advanced security auditing FAQ
- [5] Audit policy recommendations
- [6] Events to monitor
- [7] Logon types
- [8] (Logon failure) Status codes
- [9] (Kerberos) Failure Codes
- Randy Franklin Smith

About ManageEngine ADAudit Plus

ADAudit Plus is a UBA-driven auditor that helps **keep your Active Directory (AD), Azure AD, file servers (Windows, NetApp, EMC, Synology and Hitachi), Windows servers, and workstations secure and compliant** by providing full visibility into all activities.

Recently named a 2020 Gartner Peer Insights Customers' Choice for SIEM, ADAudit Plus helps you:

- Get instantly **notified of changes** in your Windows Server environment.
- Gain complete visibility into Windows **logon** activity.
- Monitor the **active and idle time** spent by employees at their workstations.
- Detect and troubleshoot Active Directory (AD) **account lockouts.**
- Get a consolidated audit trail of **privileged user activities.**
- Track changes and sign ons in **Azure AD.**
- Audit file changes across **Windows, NetApp, EMC, Synology, and Hitachi** servers.
- Track changes to files residing on Windows systems to ensure **system integrity.**
- Mitigate **insider threats** by leveraging UBA and response automation.
- Get audit-ready **compliance reports** for SOX, the GDPR, and other IT mandates.

ADAudit Plus is **licensed on a per-server basis,** and pricing starts at **$595 annually.**

Website:
https://www.manageengine.com/products/active-directory-audit/

Live demo:
https://demo.adauditplus.com/

30-day trial:
https://www.manageengine.com/products/active-directory-audit/download.html

Schedule a demo:
https://www.manageengine.com/products/active-directory-audit/demo-form.html

Live chat:
https://www.manageengine.com/products/active-directory-audit/support.html

Phone number:
+1.408.916.9891

Email:
support@adauditplus.com

Authored by:
Mahidhar Adarsh, product marketer, ManageEngine