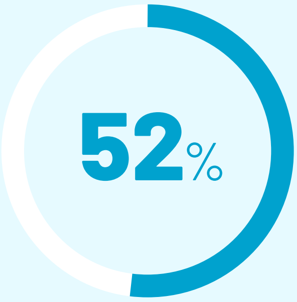
ManageEngine
ADAudit Plus

Top 8 Active Directory audit reports to share with your CISO

www.adauditplus.com

Introduction

Every chief information security officer (CISO) needs visibility into what’s happening across their Active Directory environment. But raw logs and technical reports often fail to deliver the clarity needed.



of United States-based businesses reported a data breach in the past year, highlighting the crucial role CISOs play in incident response and prevention

That’s where focused, high-level AD auditing reports come in. These help security leaders make informed decisions, detect threats, and meet compliance obligations.

First of all...Why is AD auditing important?

Before diving into reports, it's worth asking: why does Active Directory auditing matter in the first place? AD is the core of your identity and access infrastructure. If something goes wrong there, everything else is at risk. Auditing gives you the visibility to identify misconfigurations, detect threats early, and prove compliance.

Here's what makes it essential:

It helps you spot suspicious activity

From unusual logon times and unexpected account usage to privilege misuse, auditing brings hidden security threats to the surface. It gives you the visibility needed to catch risky behavior before it turns into a security incident.

It holds people accountable

Auditing records reveals who made what change, when it was made, and where it happened. This helps ensure accountability across your organization and supports quick remediation when mistakes or malicious actions occur.

It keeps you compliant

Regulatory standards like HIPAA, SOX, and the GDPR require continuous tracking of access and account changes. Without proper auditing, demonstrating compliance during assessments becomes a challenge and increases the risk of penalties.

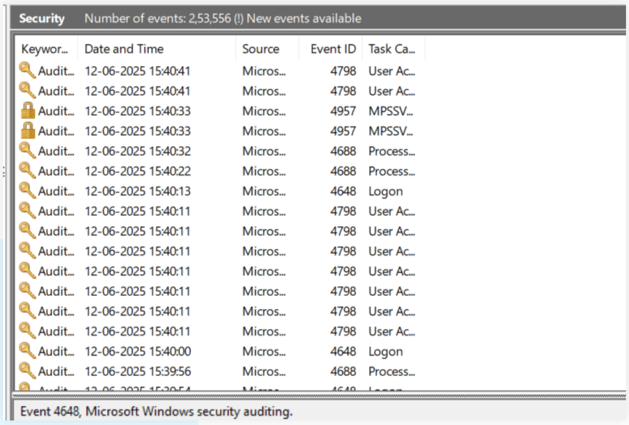
It speeds up investigations

When a security event happens, audit logs provide a clear timeline of what occurred. These help your team quickly trace actions, identify the cause, and respond effectively without wasting time.

Why native Active Directory auditing falls short

- The Windows Event Viewer generates an overwhelming volume of logs that are difficult to filter, correlate, or interpret.
- Inconsistent audit policy configuration can cause missed security events, audit gaps, and added administrative overhead.

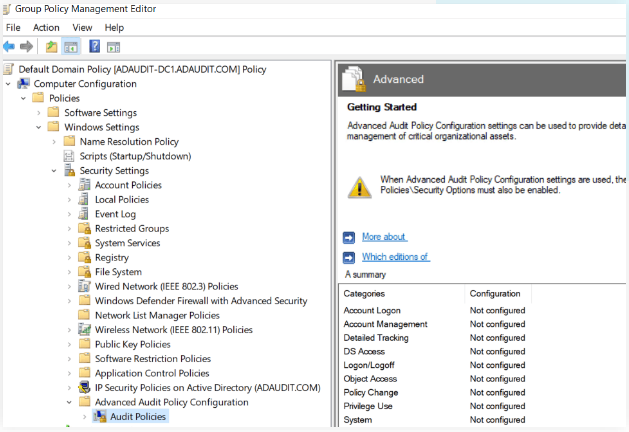
- Reporting on AD using native tools lacks consolidation and clarity, especially for executive-level visibility.
- There's no built-in option to schedule or export clean, executive-ready Active Directory audit reports.
- For CISOs, this means delays in spotting trends, tracking privileged activity, or enforcing accountability unless IT steps in each time.



Security Number of events: 2,53,556 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	12-06-2025 15:40:41	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:41	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:33	Micros...	4957	MPSSV...
Audit...	12-06-2025 15:40:33	Micros...	4957	MPSSV...
Audit...	12-06-2025 15:40:32	Micros...	4688	Process...
Audit...	12-06-2025 15:40:22	Micros...	4688	Process...
Audit...	12-06-2025 15:40:13	Micros...	4648	Logon
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:11	Micros...	4798	User Ac...
Audit...	12-06-2025 15:40:00	Micros...	4648	Logon
Audit...	12-06-2025 15:39:56	Micros...	4688	Process...

Event 4648, Microsoft Windows security auditing.



- Default Domain Policy [ADAUDIT-DC1.ADAUDIT.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Defender Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Application Control Policies
          - IP Security Policies on Active Directory (ADAUDIT.COM)
          - Advanced Audit Policy Configuration
            - Audit Policies

Advanced

Getting Started

Advanced Audit Policy Configuration settings can be used to provide deta management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the Policies\Security Options must also be enabled.

More about

Which editions of

A summary

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured

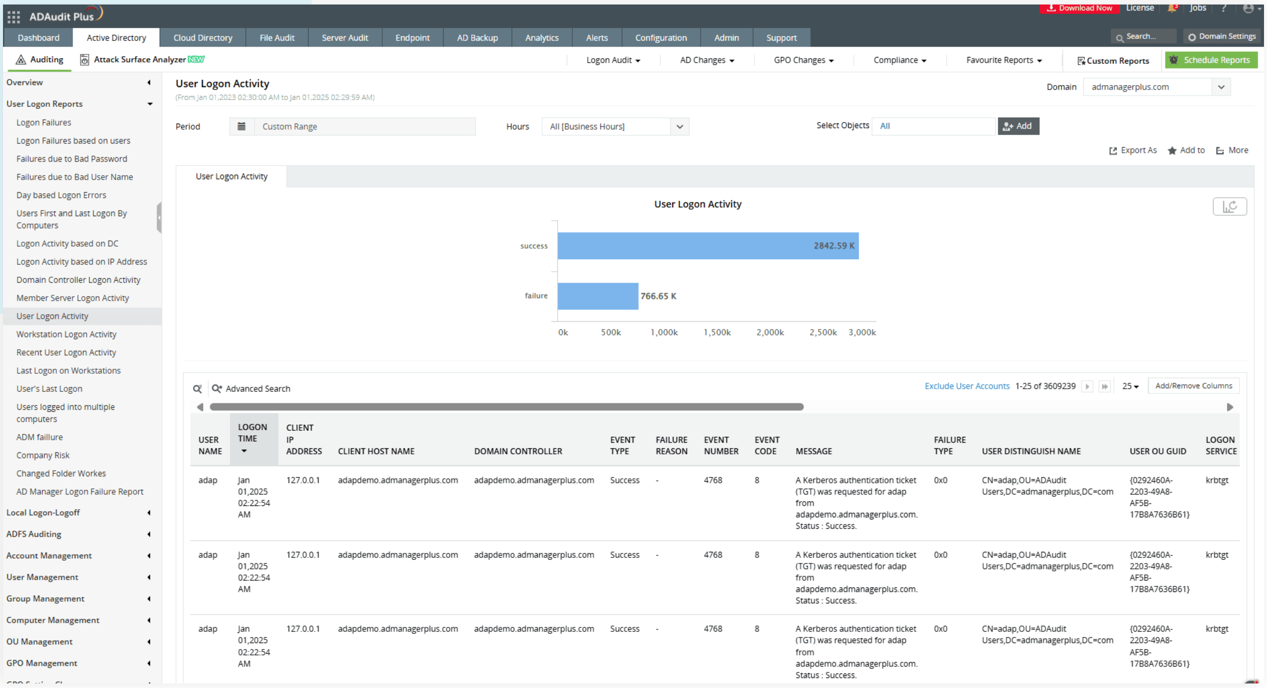
AD reports every CISO should have at their fingertips

If a major breach hits your organization, the last thing you want is to be caught off guard. These are the eight must-have AD reports every CISO needs to stay ahead of emerging threats and maintain full visibility into AD activity.

1. User logon and logoff report

Knowing who accessed the network, when, and from where is essential for both security and compliance.

This report captures the logon and logoff activity across domain controllers, servers, and workstations, including RADIUS-based access. It helps CISOs identify suspicious logon times, unauthorized access, and track remote work patterns across the organization.



User Logon Activity
(From Jan 01,2023 02:30:00 AM to Jan 01,2025 02:29:59 AM)

Domain: admanagerplus.com

Period: Custom Range

Hours: All [Business Hours]

Select Objects: All

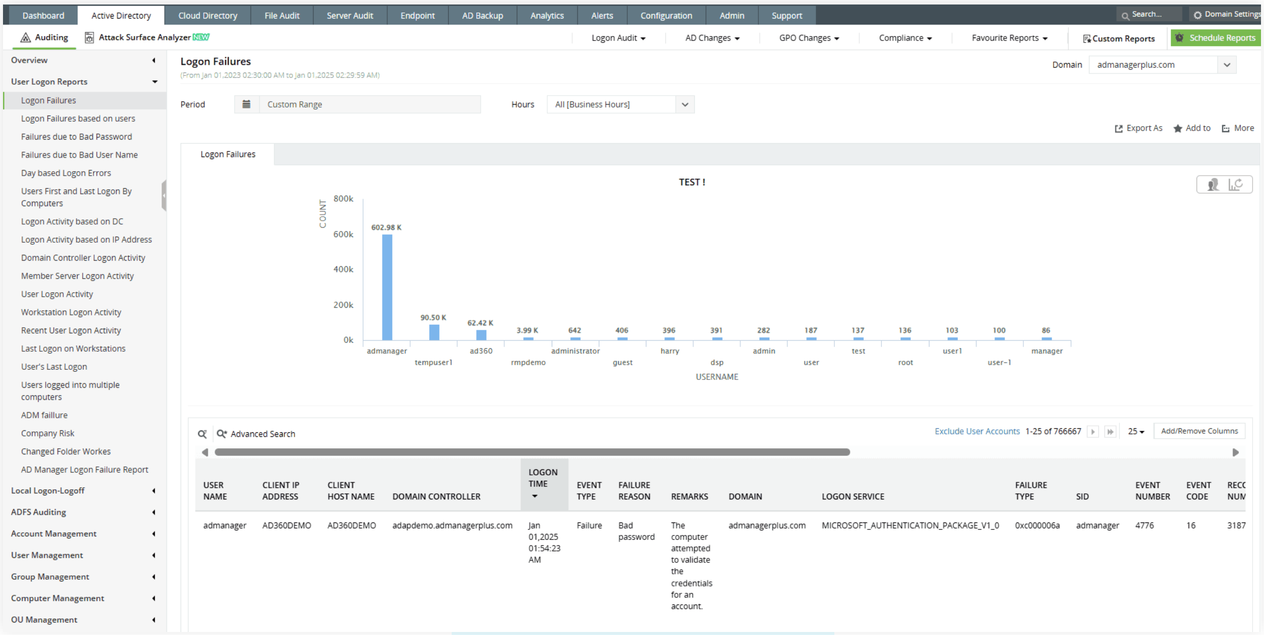
1-25 of 3609239 25

USER NAME	LOGON TIME	CLIENT IP ADDRESS	CLIENT HOST NAME	DOMAIN CONTROLLER	EVENT TYPE	FAILURE REASON	EVENT NUMBER	EVENT CODE	MESSAGE	FAILURE TYPE	USER DISTINGUISH NAME	USER OU GUID	LOGON SERVICE
adap	Jan 01,2025 02:22:54 AM	127.0.0.1	adapdemo.admanagerplus.com	adapdemo.admanagerplus.com	Success	-	4768	8	A Kerberos authentication ticket (TGT) was requested for adap from adapdemo.admanagerplus.com. Status : Success.	0x0	CN=adap,OU=ADAudit Users,DC=admanagerplus,DC=com	{0292460A-2203-49A8-AF5B-17B8A7636B61}	krbtgt
adap	Jan 01,2025 02:22:54 AM	127.0.0.1	adapdemo.admanagerplus.com	adapdemo.admanagerplus.com	Success	-	4768	8	A Kerberos authentication ticket (TGT) was requested for adap from adapdemo.admanagerplus.com. Status : Success.	0x0	CN=adap,OU=ADAudit Users,DC=admanagerplus,DC=com	{0292460A-2203-49A8-AF5B-17B8A7636B61}	krbtgt
adap	Jan 01,2025 02:22:54 AM	127.0.0.1	adapdemo.admanagerplus.com	adapdemo.admanagerplus.com	Success	-	4768	8	A Kerberos authentication ticket (TGT) was requested for adap from adapdemo.admanagerplus.com. Status : Success.	0x0	CN=adap,OU=ADAudit Users,DC=admanagerplus,DC=com	{0292460A-2203-49A8-AF5B-17B8A7636B61}	krbtgt

2. Account lockout and logon failure report

A surge in account lockouts can indicate either password fatigue or a brute-force attack in progress.

This report details failed logon attempts, lockout sources, and failure reasons, providing a quick overview of account-based risks. It allows CISOs to distinguish between misconfigurations and active threats, improving incident response and account hygiene.



Logon Failures
(From Jan 01,2023 02:30:00 AM to Jan 01,2025 02:29:59 AM)

Domain: admanagerplus.com

Period: Custom Range

Hours: All [Business Hours]

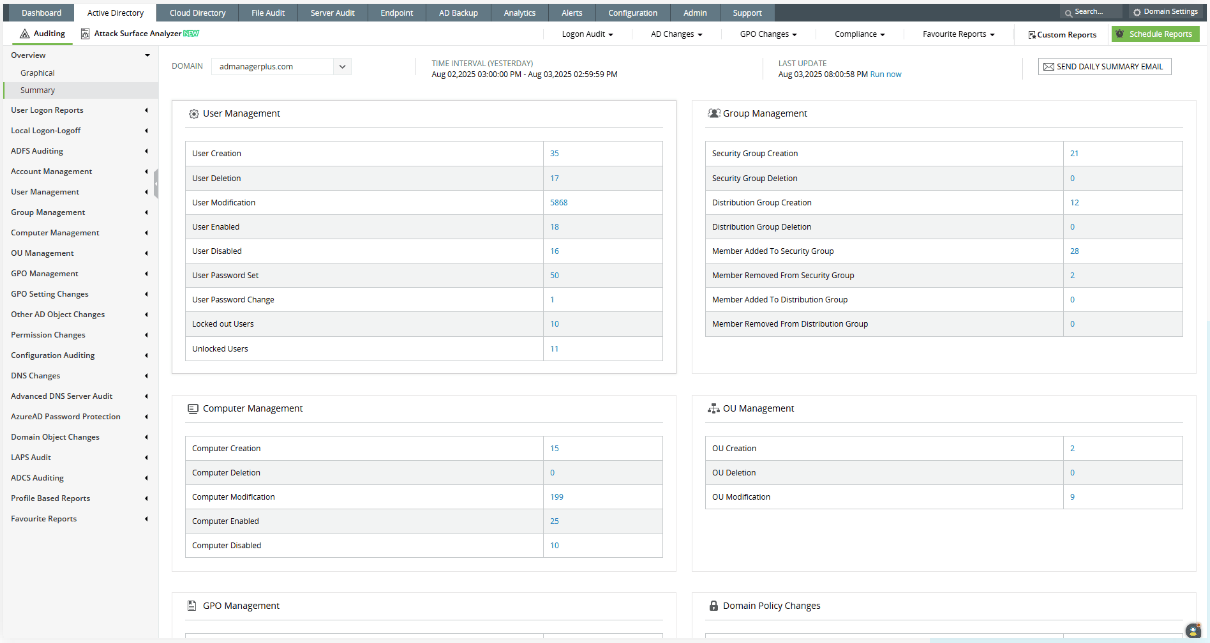
1-25 of 766667 25

USER NAME	CLIENT IP ADDRESS	CLIENT HOST NAME	DOMAIN CONTROLLER	LOGON TIME	EVENT TYPE	FAILURE REASON	REMARKS	DOMAIN	LOGON SERVICE	FAILURE TYPE	SID	EVENT NUMBER	EVENT CODE	RECC NUM
admanager	AD360DEMO	AD360DEMO	adapdemo.admanagerplus.com	Jan 01,2025 01:54:23 AM	Failure	Bad password	The computer attempted to validate the credentials for an account.	admanagerplus.com	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	0xc000006a	admanager	4776	16	3187

3. Active Directory change summary report

Unauthorized or undocumented changes to users, groups, OUs, and permissions can create serious security gaps.

This report summarizes AD changes by showing who made them, what was changed, and when the action occurred. CISOs can use it to detect privilege escalation, unapproved modifications, and policy violations across departments.



DOMAIN admanagerplus.com

TIME INTERVAL (YESTERDAY)
Aug 02,2025 03:00:00 PM - Aug 03,2025 02:59:59 PM

LAST UPDATE
Aug 03,2025 08:00:58 PM Run now

User Management

User Creation	35
User Deletion	17
User Modification	5868
User Enabled	18
User Disabled	16
User Password Set	50
User Password Change	1
Locked out Users	10
Unlocked Users	11

Group Management

Security Group Creation	21
Security Group Deletion	0
Distribution Group Creation	12
Distribution Group Deletion	0
Member Added To Security Group	28
Member Removed From Security Group	2
Member Added To Distribution Group	0
Member Removed From Distribution Group	0

Computer Management

Computer Creation	15
Computer Deletion	0
Computer Modification	199
Computer Enabled	25
Computer Disabled	10

OU Management

OU Creation	2
OU Deletion	0
OU Modification	9

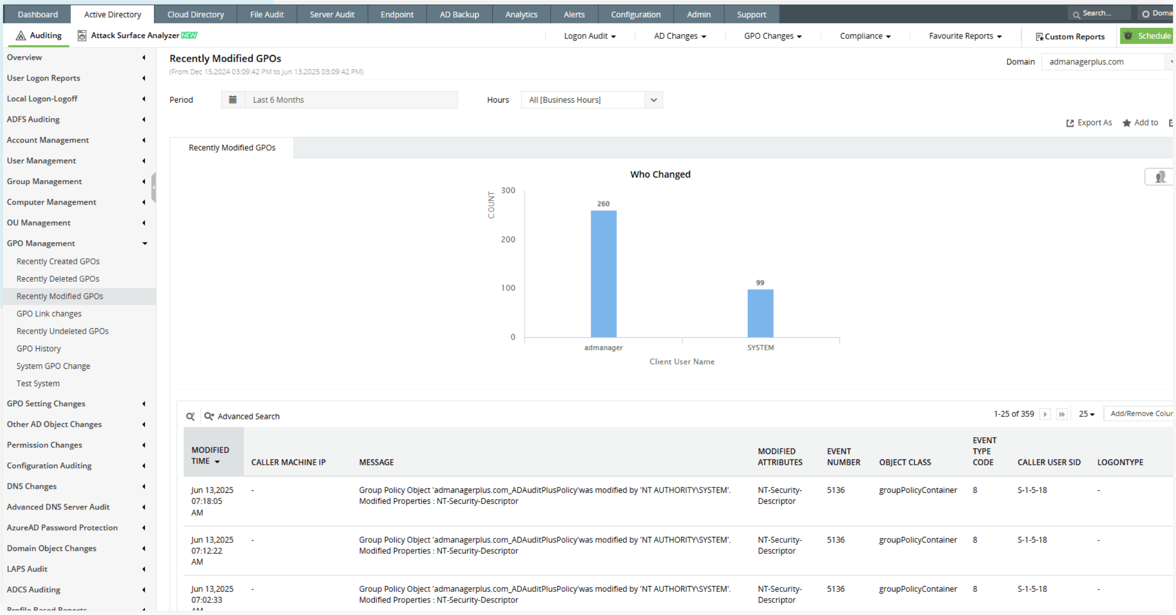
GPO Management

Domain Policy Changes

4. GPO modification report

Even small changes to Group Policy Objects (GPOs) can impact thousands of users or machines at once.

This report tracks every GPO creation, deletion, modification, and link change along with the responsible user. It helps CISOs enforce configuration baselines, detect risky GPO deployments, and prevent policy-based attacks.



Recently Modified GPOs
(From Dec 15,2024 03:09:42 PM to Jun 13,2025 03:09:42 PM)

Domain admanagerplus.com

Period Last 6 Months

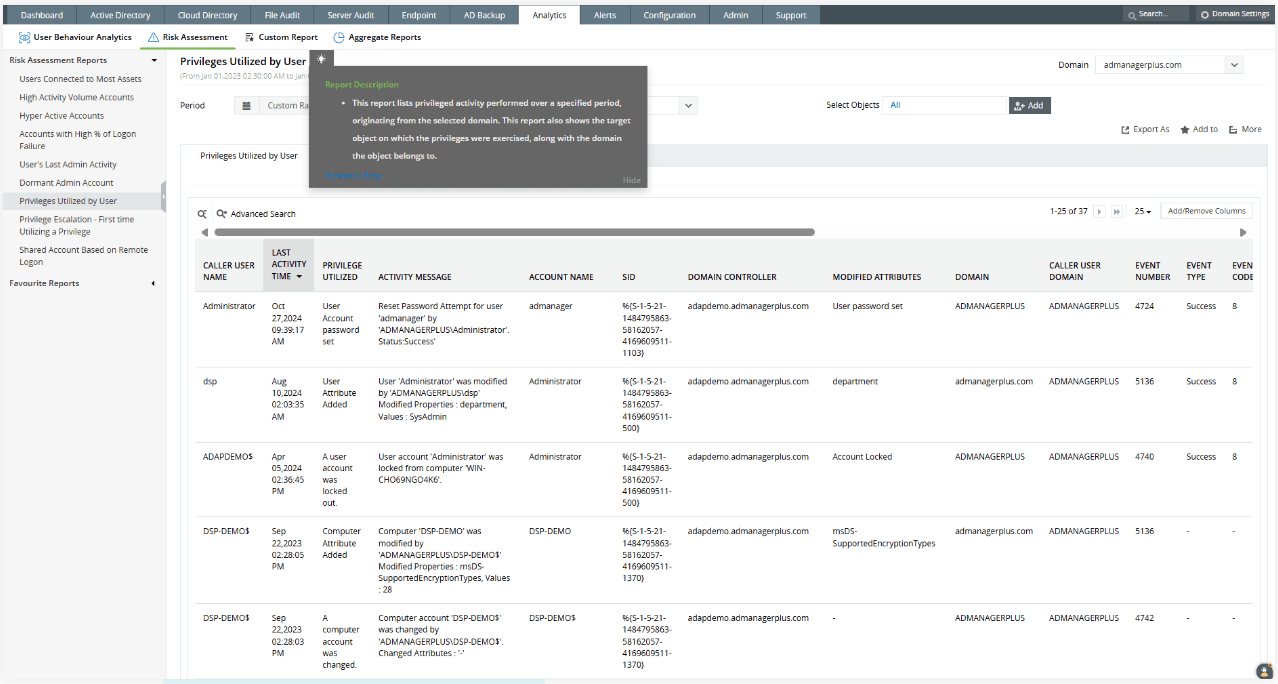
Hours All [Business Hours]

MODIFIED TIME	CALLER MACHINE IP	MESSAGE	MODIFIED ATTRIBUTES	EVENT NUMBER	OBJECT CLASS	EVENT TYPE CODE	CALLER USER SID	LOGONTYPE
Jun 13,2025 07:18:05 AM	-	Group Policy Object 'admanagerplus.com_ADAuditPlusPolicy'was modified by 'NT AUTHORITY\SYSTEM'. Modified Properties : NT-Security-Descriptor	NT-Security-Descriptor	5136	groupPolicyContainer	8	S-1-5-18	-
Jun 13,2025 07:12:22 AM	-	Group Policy Object 'admanagerplus.com_ADAuditPlusPolicy'was modified by 'NT AUTHORITY\SYSTEM'. Modified Properties : NT-Security-Descriptor	NT-Security-Descriptor	5136	groupPolicyContainer	8	S-1-5-18	-
Jun 13,2025 07:02:33	-	Group Policy Object 'admanagerplus.com_ADAuditPlusPolicy'was modified by 'NT AUTHORITY\SYSTEM'. Modified Properties : NT-Security-Descriptor	NT-Security-Descriptor	5136	groupPolicyContainer	8	S-1-5-18	-

5. Privileged user activity report

Privileged accounts are often exploited in breaches, making monitoring them a top executive priority.

This report provides insight into administrator logons and permission escalations. By regularly reviewing this report, CISOs can stay on top of privileged access trends and identify potential insider threats.



Privileges Utilized by User
(From Jan 01,2023 02:30:00 AM to Jan

Report Description

- This report lists privileged activity performed over a specified period, originating from the selected domain. This report also shows the target object on which the privileges were exercised, along with the domain the object belongs to.

Domain: admanagerplus.com

Period: Custom Ra

Select Objects: All

Privileges Utilized by User

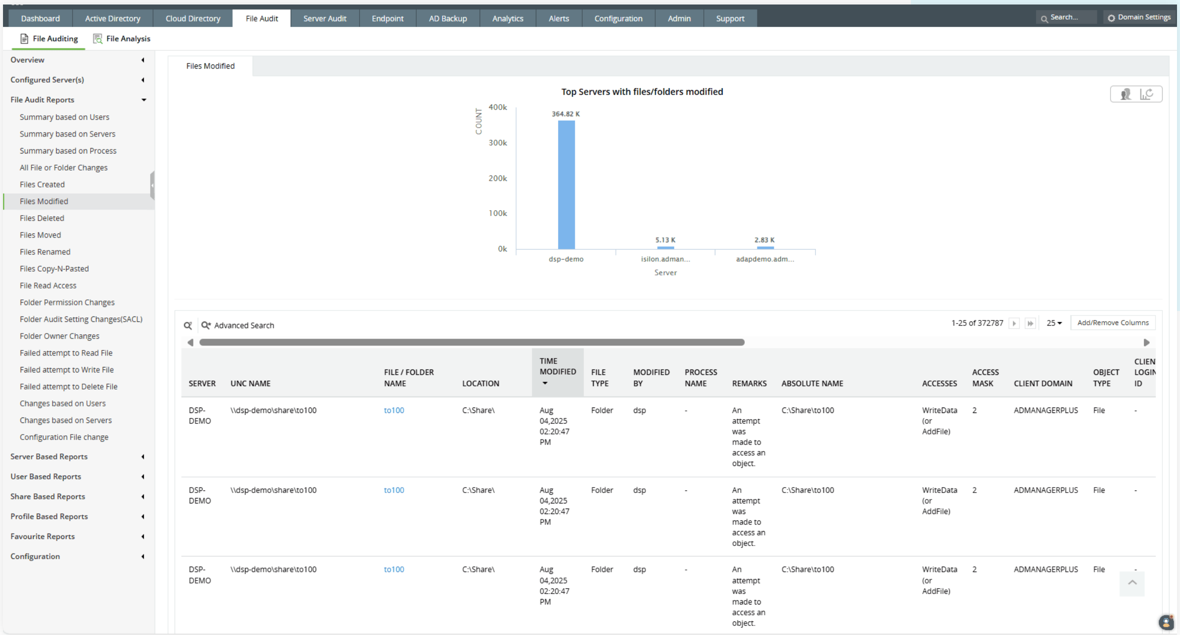
1-25 of 37 | 25

CALLER USER NAME	LAST ACTIVITY TIME	PRIVILEGE UTILIZED	ACTIVITY MESSAGE	ACCOUNT NAME	SID	DOMAIN CONTROLLER	MODIFIED ATTRIBUTES	DOMAIN	CALLER USER DOMAIN	EVENT NUMBER	EVENT TYPE	EVEN CODE
Administrator	Oct 27,2024 09:39:17 AM	User Account password set	Reset Password Attempt for user 'admanager' by 'ADMANAGERPLUS\Administrator'. Status:Success'	admanager	%{S-1-5-21-1484795863-58162057-4169609511-1103}	adapdemo.admanagerplus.com	User password set	ADMANAGERPLUS	ADMANAGERPLUS	4724	Success	8
dsp	Aug 10,2024 02:03:35 AM	User Attribute Added	User 'Administrator' was modified by 'ADMANAGERPLUS\dsp' Modified Properties : department, Values : SysAdmin	Administrator	%{S-1-5-21-1484795863-58162057-4169609511-500}	adapdemo.admanagerplus.com	department	admanagerplus.com	ADMANAGERPLUS	5136	Success	8
ADAPDEMO$	Apr 05,2024 02:36:45 PM	A user account was locked out.	User account 'Administrator' was locked from computer 'WIN-CHO69NGO4K6'.	Administrator	%{S-1-5-21-1484795863-58162057-4169609511-500}	adapdemo.admanagerplus.com	Account Locked	ADMANAGERPLUS	ADMANAGERPLUS	4740	Success	8
DSP-DEMO$	Sep 22,2023 02:28:05 PM	Computer Attribute Added	Computer 'DSP-DEMO' was modified by 'ADMANAGERPLUS\DSP-DEMO$' Modified Properties : msDS-SupportedEncryptionTypes, Values : 28	DSP-DEMO	%{S-1-5-21-1484795863-58162057-4169609511-1370}	adapdemo.admanagerplus.com	msDS-SupportedEncryptionTypes	admanagerplus.com	ADMANAGERPLUS	5136	-	-
DSP-DEMO$	Sep 22,2023 02:28:03 PM	A computer account was changed.	Computer account 'DSP-DEMO$' was changed by 'ADMANAGERPLUS\DSP-DEMO$'. Changed Attributes : '-'	DSP-DEMO$	%{S-1-5-21-1484795863-58162057-4169609511-1370}	adapdemo.admanagerplus.com	-	ADMANAGERPLUS	ADMANAGERPLUS	4742	-	-

6. File access and modification report

Unauthorized access to sensitive files can signal insider threats or potential data exfiltration.

This report captures file creation, modification, deletion, and read actions across monitored Windows file servers and NAS devices. It helps CISOs monitor critical data activity, spot unusual access patterns, and ensure that sensitive information isn't being mishandled or exposed.

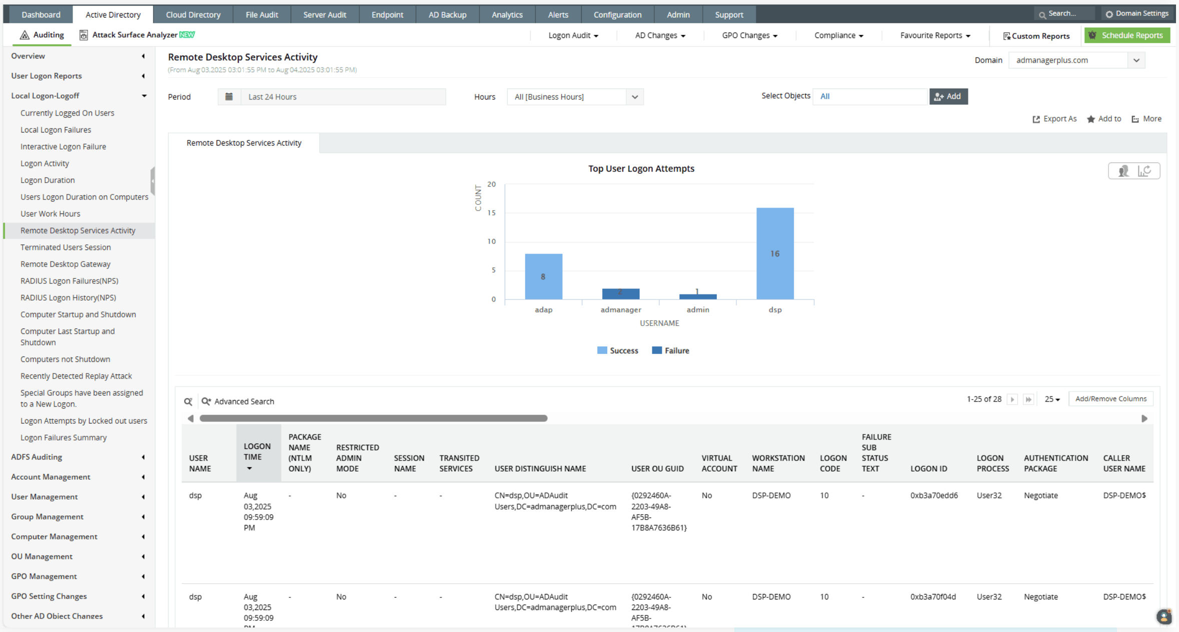


SERVER	UNC NAME	FILE / FOLDER NAME	LOCATION	TIME MODIFIED	FILE TYPE	MODIFIED BY	PROCESS NAME	REMARKS	ABSOLUTE NAME	ACCESSES	ACCESS MASK	CLIENT DOMAIN	OBJECT TYPE	CLIEN LOGIN ID
DSP-DEMO	\\dsp-demo\share\to100	to100	C:\Share\	Aug 04,2025 02:20:47 PM	Folder	dsp	-	An attempt was made to access an object.	C:\Share\to100	WriteData (or AddFile)	2	ADMANAGERPLUS	File	-
DSP-DEMO	\\dsp-demo\share\to100	to100	C:\Share\	Aug 04,2025 02:20:47 PM	Folder	dsp	-	An attempt was made to access an object.	C:\Share\to100	WriteData (or AddFile)	2	ADMANAGERPLUS	File	-
DSP-DEMO	\\dsp-demo\share\to100	to100	C:\Share\	Aug 04,2025 02:20:47 PM	Folder	dsp	-	An attempt was made to access an object.	C:\Share\to100	WriteData (or AddFile)	2	ADMANAGERPLUS	File	-

7. Remote desktop session report

Remote Desktop Protocol is a popular target for attackers looking to gain internal access.

This report logs session start and end times, accessed machines, and the users behind each connection. CISOs can use it to detect suspicious remote access, monitor after-hours activity, and validate secure remote work practices across the environment.



Remote Desktop Services Activity
(From Aug 03,2025 03:01:55 PM to Aug 04,2025 03:01:55 PM)

Domain: admanagerplus.com

Period: Last 24 Hours

Hours: All [Business Hours]

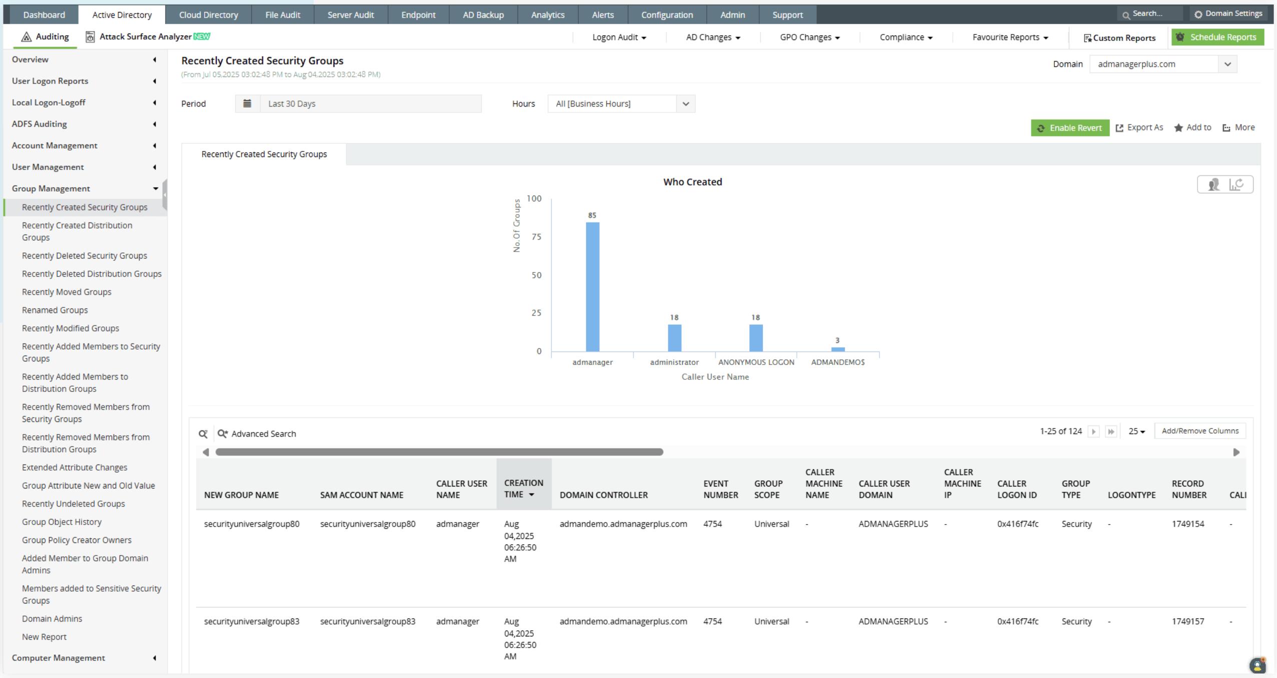
Select Objects: All

USER NAME	LOGON TIME	PACKAGE NAME (NTLM ONLY)	RESTRICTED ADMIN MODE	SESSION NAME	TRANSITED SERVICES	USER DISTINGUISH NAME	USER OU GUID	VIRTUAL ACCOUNT	WORKSTATION NAME	LOGON CODE	FAILURE SUB STATUS TEXT	LOGON ID	LOGON PROCESS	AUTHENTICATION PACKAGE	CALLER USER NAME
dsp	Aug 03,2025 09:59:09 PM	-	No	-	-	CN=dsp,OU=ADAudit Users,DC=admanagerplus,DC=com	{0292460A-2203-49A8-AF5B-17B8A7636B61}	No	DSP-DEMO	10	-	0xb3a70edd6	User32	Negotiate	DSP-DEMO$
dsp	Aug 03,2025 09:59:09	-	No	-	-	CN=dsp,OU=ADAudit Users,DC=admanagerplus,DC=com	{0292460A-2203-49A8-AF5B-	No	DSP-DEMO	10	-	0xb3a70f04d	User32	Negotiate	DSP-DEMO$

8. Security group change report

Security groups control which users and admins have access to critical systems, applications, and data. Unauthorized changes to these groups can open the door to privilege misuse and data exposure.

This report tracks security group creation, modification, deletion, restoration, renaming, and membership changes, such as users or admins being added or removed. CISOs can use it to validate access policies, monitor elevated privileges, and prevent unauthorized access across the organization.



Recently Created Security Groups
(From Jul 05,2025 03:02:48 PM to Aug 04,2025 03:02:48 PM)

Domain admanagerplus.com

Period Last 30 Days

Hours All [Business Hours]

NEW GROUP NAME	SAM ACCOUNT NAME	CALLER USER NAME	CREATION TIME	DOMAIN CONTROLLER	EVENT NUMBER	GROUP SCOPE	CALLER MACHINE NAME	CALLER USER DOMAIN	CALLER MACHINE IP	CALLER LOGON ID	GROUP TYPE	LOGONTYPE	RECORD NUMBER	CALI
securityuniversalgroup80	securityuniversalgroup80	admanager	Aug 04,2025 06:26:50 AM	admandemo.admanagerplus.com	4754	Universal	-	ADMANAGERPLUS	-	0x416f74fc	Security	-	1749154	-
securityuniversalgroup83	securityuniversalgroup83	admanager	Aug 04,2025 06:26:50 AM	admandemo.admanagerplus.com	4754	Universal	-	ADMANAGERPLUS	-	0x416f74fc	Security	-	1749157	-

Delivering the right reports with the right tool

Manually aggregating raw log data and formatting it into audit-ready reports using native tools is time-consuming and often incomplete. That's where a dedicated AD auditing solution like ManageEngine ADAudit Plus makes a difference.

See how these key auditing tasks differ when done natively versus using a purpose-built solution like ADAudit Plus:

1. Identify locked-out user accounts
2. Track changes to FSMO roles
3. Audit who deleted user accounts and when
4. Monitor computer activity across the Active Directory environment

ADAudit Plus provides over 200 prebuilt AD reports that can be scheduled, customized, and sent directly to security leaders in formats like PDF, XLS, or HTML.

This solution helps streamline compliance efforts, strengthen executive visibility, and reduce response times across the board.

> “We are a 2 billion dollar bank. ADAudit Plus gives us a wealth of information about what is occurring within our AD infrastructure, which we couldn't know earlier. Our auditors are more than happy with the audit reports.
>
> Chris Schum
> *Information security officer, Central Bank*

About ADAudit Plus

ManageEngine ADAudit Plus is a unified auditing solution that provides full visibility into activities across Active Directory (AD), Entra ID, Windows file servers and NAS devices, Windows servers, and workstations—all in just a few clicks.

ADAudit Plus helps organizations streamline auditing, demonstrate compliance, and enhance their identity threat detection and response with capabilities like real-time change auditing, user logon tracking, account lockout analysis, privileged user monitoring, file auditing, compliance reporting, attack surface analysis for AD and Azure AD, response automation, and AD backup and recovery.

For more information about ADAudit Plus, visit www.manageengine.com/products/active-directory-audit/.

$ Get Quote   ⤓ Download