

DATASHEET



A unified platform for UBA-driven on-premises & cloud IT security

Reduce the attack surface of your hybrid IT ecosystem by proactively monitoring critical changes and identifying security gaps across on-premises and multi-cloud environments such as Active Directory (AD), Microsoft Entra ID (formerly Azure AD), file servers, Windows servers, and workstations with ManageEngine ADAudit Plus.

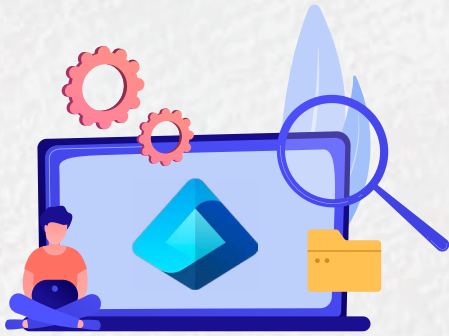


1. AD change auditing

- » **Audit AD changes:**
Track changes to organizational units (OUs), users, groups, computers, administrative groups, and other AD objects.
- » **Trace object change history:**
Receive detailed change audit reports with information on the old and new values of the changed attributes.
- » **Monitor DNS and schema changes:**
Gain visibility into the addition, modification, and deletion of DNS nodes and zones; monitor AD schema and configuration changes; and more.
- » **Track AD permission changes:**
View all changes in AD permissions, such as those made to domain-level permissions, OUs, schema, configuration, and DNS.
- » **Audit user account management:**
Track user creation, deletion, and modification; password resets; and other account management actions.
- » **Mitigate attacks:**
Detect 25+ AD attacks including Kerberoasting, Golden Ticket, DCSync, pass-the-hash, ransomware, and more.

License modules: Domain controllers

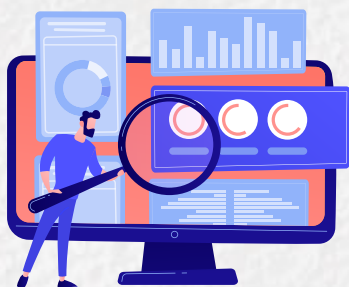
Supported platforms: Windows Server 2008 and above



2. Entra ID and cloud auditing

- » **Track sign-ins:**
Monitor all sign-ins and detect account lockouts, MFA failures, and more.
- » **Detect sign-in risks:**
Identify risky logon activity and gain insights into the risk level, risk state, and risk detail.
- » **Identify object changes:**
Audit user, device, and group management actions and get information on changes to user passwords, assignment and removal of roles, and more.
- » **Monitor Microsoft Intune admin center:**
Track device, policy, and app changes across Microsoft Intune with detailed audit trails.
- » **Monitor applications:**
Keep tabs on applications that have been added, updated, and deleted, and on consent given to APIs.
- » **Audit hybrid AD environments:**
Get a unified view of all activities happening across your AD and Entra ID environments.
- » **Detect risky configurations:**
Identify risky configurations and get step-by-step remediation guidance based on industry best practices like the NIST cybersecurity framework.
- » **Audit Microsoft 365:**
Gain visibility into Exchange Online mailbox and admin actions, OneDrive file activity, and SharePoint file operations.

License modules: Microsoft Entra ID tenants



3. File monitoring

- » **Monitor file and folder accesses:**
Track successful and failed file access attempts—including create, read, delete, modify, copy and paste, and move—in real time.
- » **Audit permission changes:**
Track NTFS and share permission changes along with details such as their old and new values.
- » **Monitor file integrity:**
Receive detailed reports on all changes made to critical system and program files, and trigger alerts when suspicious activity is detected.
- » **Report on file share changes:**
Track every access and change made to shared files and folders in your domain with details on who accessed what, when, and from where.
- » **Analyze files:**
Scan metadata and disk space to gain insights into file server security and storage.
- » **Audit across multiple platforms:**
View changes across Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx, QNAP, Azure, Nutanix, CTERA, and Qumulo file servers.

License modules: Windows file servers, NAS servers

Supported platforms: Windows Server 2008 and above; Dell VNX, VNXe, Celerra, Unity, and Isilon; Synology DSM 5.0 and above; NetApp ONTAP 7.2 and above for filers; NetApp ONTAP 8.2.1 and above for clusters; Hitachi NAS 13.2 and above; Huawei OceanStor V5 series, OceanStor 9000 V5 storage, OceanStor Dorado All-Flash Storage, and OceanStor Hybrid Flash Storage (V6 series); Amazon FSx for Windows; Amazon FSx for NetApp ONTAP-AWS; QNAP; Azure; CTERA Edge Filers series 7; Nutanix; and Qumulo Core version 6.2.2 and above.



4. Group Policy settings change auditing

- » **Audit GPO:**
Keep an eye on GPO creation, deletion, modification, and more.
- » **Track GPO setting changes:**
Track changes made to GPO settings and see who changed what setting, when, from where, and the setting's values before and after the change.
- » **Trace GPO change history:**
View the change history of one or multiple GPOs in a domain to detect unwarranted activities.
- » **Configure alerts for critical changes:**
Trigger instant email and SMS alerts for critical changes, such as computer configuration changes and password and account lockout policy changes.
- » **Schedule GPO change reports:**
Send scheduled reports on important GPO or GPO settings changes to specified recipients.
- » **Detect GPO misconfigurations:**
Identify critical security misconfigurations across Windows servers and workstations, by evaluating system settings against CIS benchmarks.

License modules: Domain controllers

Supported platforms: Windows Server 2008 and above



5. Windows server auditing and reporting

- » **Audit Windows servers:**
Monitor changes to local administrative group memberships, local users, user rights, local policies, and more.
- » **Track scheduled tasks and processes:**
Report on the creation, deletion, and modification of scheduled tasks and processes.
- » **Monitor USB and printer usage:**
Track USB usage and file transfers to removable storage devices. Also track which file was printed, when, by whom, the number of pages and copies printed, and much more.
- » **Audit PowerShell processes:**
Monitor PowerShell processes that run on your Windows servers, along with the commands executed in them.
- » **Monitor ADFS, LAPS, and ADLDS:**
Track ADFS authentication attempts, users who have viewed local administrator passwords, changes made to a password's expiration time or date, and more.
- » **Detect high-risk misconfigurations:**
Identify critical security misconfigurations like weak lockout and password policies, insecure remote access settings, and disabled audit logging configurations by evaluating system settings against CIS benchmarks.

License modules: Windows servers

Supported platforms: Windows Server 2008 and above



6. File security and exposure analysis

- » **Expose dormant file security risks:**
Detect files with excessive permissions, broken inheritance, or full control access granted to inappropriate users, and reduce exposure.
- » **Control uncontrolled data growth:**
Locate redundant, obsolete, and trivial (ROT) data, duplicate, hidden, and non-business files that consumes critical storage.
- » **Prevent misuse of abandoned and orphaned files:**
Locate files owned by inactive or former users, abandoned folders, and outdated files that can be misused long after their original business relevance has ended.
- » **Uncover permission and ownership gaps:**
Analyze how permissions and ownership are distributed across files to identify over-privileged users, unmanaged files, and weak controls that increase insider risks.

License modules: Windows servers by data size

Supported platforms: Windows Server 2008 R2 and above



7. Logon and logoff auditing

- » **Audit logons and logoffs:**
Track logon and logoff activity across your domain controllers, Windows servers, and Windows and Mac workstations.
- » **Track user logon history:**
Record every user's logon activity, identify users who are currently logged on, list users logged on to multiple machines, and more.
- » **Audit RADIUS logons:**
Gain visibility into logons on your RADIUS servers with reports on RADIUS logons, logon failures, and RADIUS (NPS) logon history.
- » **Analyze logon failures:**
Track all failed logon attempts with details on who attempted to log on, what machine they attempted to log on to, when, and the reason for the failure.
- » **Respond to malicious logon activity:**
Leverage ML to spot and respond to unusual volumes of logon failures, unusual logon times, and more.

License modules: Domain controllers, Windows servers, workstations

Supported platforms: Windows Server 2008 and above; Windows XP and above; MacOS Catalina 10.15 and above



8. Account lockout analysis

- » **Receive account lockout notifications:**
Detect AD user account lockouts in real time with email and SMS alerts, and reduce account lockout duration.
- » **Find the account lockout source:**
Analyze mobile phone logons, RDP sessions, services, scheduled tasks, and more for stale credentials, and identify the source of account lockouts.
- » **Check the account lockout status:**
Pull up reports on the status of every locked-out account, the time at which the lockout occurred, and more.
- » **Examine account lockouts with UBA:**
Identify negligent users and malicious insiders by spotting abnormal lockout activities with UBA.
- » **Improve help desk efficiency:**
View reports with all the information required by help desk personnel to resolve account lockout issues faster and minimize service downtime.
- » **Analyze the root cause:**
Maintain a clear audit trail of password resets, password changes, and account lockout sources to streamline forensic analysis.

License modules: Domain controllers, Windows servers, workstations

Supported platforms: Windows Server 2008 and above; Windows XP and above



9. Privileged user monitoring

- » **Audit administrator activity:**
Track administrative user actions on AD schema, configuration, users, groups, OUs, GPOs, and more.
- » **Review privileged user activity:**
Comply with various IT regulations by maintaining an audit trail of activities performed by privileged users in your domain.
- » **Detect privilege escalation:**
Identify privilege escalation with reports documenting users' first-time use of privileges, and verify if a user's privileges are necessary for their role.
- » **Spot behavioral anomalies:**
Identify actions deviating from normal access patterns to find attackers using stolen or shared credentials of privileged accounts.
- » **Receive alerts on suspicious activity:**
Rapidly spot and respond to high-risk events, such as the clearing of audit logs or accessing critical data outside business hours, with instant alerts.

License modules: Domain controllers, Windows servers

Supported platforms: Windows Server 2008 and above



10. Identity threat detection and response

- » **Detect changes in real time:**
Get instantly alerted on who performed what change, when it was made, and from where, in AD and Microsoft Entra ID environments.
- » **Mitigate attacks:**
Detect 25+ AD attacks including Kerberoasting, Golden Ticket, DCSync, pass-the-hash, ransomware, and more.
- » **Remediate risky cloud configurations:**
Identify risky configurations in Azure, AWS, and GCP, and receive remediation guidance based on industry best practices.
- » **Automate AD backup and recovery:**
Automate backup and recovery for AD objects (including GPOs, group memberships, and more) and rollback unwanted changes.
- » **Detect anomalous activities:**
Quickly spot repeated logon failures, user activity anomalies, privilege escalations, data exfiltration, and more with UBA.
- » **Respond to threats instantly:**
Automatically execute scripts to shut down machines, end user sessions, or carry out other tailor-made responses to mitigate threats.
- » **Integrate with IT helpdesk ticketing tools:**
Automatically generate support tickets in ServiceNow, Zendesk, and other tools for critical AD events to streamline incident management.

License modules: Domain controllers, Microsoft Entra ID tenants, Windows servers, Windows file servers, NAS servers, workstations

Supported platforms: Windows Server 2008 and above; Windows Server 2008 and above; Dell VNX, VNXe, Celerra, Unity, and Isilon; Synology DSM 5.0 and above; NetApp ONTAP 7.2 and above for filers; NetApp ONTAP 8.2.1 and above for clusters; Hitachi NAS 13.2 and above; Huawei OceanStor V5 series, OceanStor 9000 V5 storage, OceanStor Dorado All-Flash Storage, and OceanStor Hybrid Flash Storage (V6 series); Amazon FSx for Windows; Amazon FSx for NetApp ONTAP-AWS; QNAP; Azure Files; CTERA Edge Filers series 7; Nutanix; and Qumulo Core version 6.2.2 and above; Windows XP and above



11. Compliance reporting

- » **Leverage over 250 reports:**
Ace compliance audits easily with detailed reports on changes across AD, file servers, Windows servers, and workstations.
- » **Receive out-of-the-box audit reports:**
Schedule periodic, ready-made reports for HIPAA, PCI DSS, the GDPR, ISO 27001, GLBA, FISMA, and SOX, and customize reports for other regulations.
- » **Perform root cause analysis:**
In the event of a breach, analyze the incident thoroughly, identify the source of leaks or intrusions with accurate forensic data, and share your findings with custom reports.
- » **Monitor file integrity:**
Track every access to operating system, database, and software files; archived audit logs and reports; and other critical files.
- » **Configure instant alerts:**
Detect security incidents quickly using email and SMS alerts specific to files, users, time periods, or events. Reduce false positives with UBA.
- » **Mitigate damage with automated responses:**
Save crucial time with automated responses, such as running custom scripts to disable accounts or shut down devices.

License modules: Domain controllers, Windows servers, Windows file servers, NAS servers, workstations

Supported platforms: Windows Server 2008 and above; Windows Server 2008 and above; Dell VNX, VNXe, Celerra, Unity, and Isilon; Synology DSM 5.0 and above; NetApp ONTAP 7.2 and above for filers; NetApp ONTAP 8.2.1 and above for clusters; Hitachi NAS 13.2 and above; Huawei OceanStor V5 series, OceanStor 9000 V5 storage, OceanStor Dorado All-Flash Storage, and OceanStor Hybrid Flash Storage (V6 series); Amazon FSx for Windows; Amazon FSx for NetApp ONTAP-AWS; QNAP; Azure Files; CTERA Edge Filers series 7; Nutanix; and Qumulo Core version 6.2.2 and above; Windows XP and above

System Requirements

For the complete system requirements, [see the Quick Start Guide](#).

Supported browsers:

Mozilla Firefox 3.6 and above, Google Chrome, Microsoft Edge

Processor: 2.4GHz

RAM: 8GB

Disk space: 50GB

Supported platforms

DC and Windows Server auditing	File auditing	Other components
Windows Server versions: ✓ 2008/2008 R2 ✓ 2012/2012 R2 ✓ 2016/2016 R2 ✓ 2019	Windows file server auditing: Windows File Server 2008 and above EMC auditing: VNX, VNXe, Celerra, Unity, Isilon Synology auditing: DSM 5.0 and above NetApp filer auditing: Data ONTAP 7.2 and above NetApp cluster auditing: Data ONTAP 8.2.1 and above Hitachi NAS auditing: Hitachi NAS 13.2 and above Huawei OceanStor auditing: Huawei OceanStor V5 series, OceanStor 9000 V5 storage, OceanStor Dorado All-Flash Storage, and OceanStor Hybrid Flash Storage (V6 series) Amazon FSx for Windows Amazon FSx for NetApp ONTAP-AWS QNAP Azure Files CTERA Edge Filers series 7 Nutanix Qumulo Core version 6.2.2 and above	AWS Managed Microsoft AD Entra ID tenants Azure, AWS, and GCP (Attack Surface Analyzer only) ADFS auditing: ADFS 2.0 and above AD Certification Service Workstation auditing: Windows XP and above MacOS Catalina 10.15 and above PowerShell auditing: PowerShell 4.0 or 5.0 File Analysis: Windows Server 2008 R2 and above

Available editions



FREE EDITION

\$00

Never expires

Audit and collect data across 25 workstations

Generate reports using log data collected during evaluation

[Try now](#)



STANDARD EDITION

Starts at **\$595** annually

All features of the Free edition

+

Reports and alerts on event log data collected from these licensed components:

- ✓ DCs
- ✓ Azure AD tenants
- ✓ Windows servers
- ✓ Workstations
- ✓ Windows file servers
- ✓ NAS devices

[Try now](#)



PROFESSIONAL EDITION

Starts at **\$945** annually

All features of the Standard edition

+

Account lockout analysis

AD permission change auditing

GPO settings change auditing

DNS and AD schema change auditing

Old and new values of AD object attribute changes

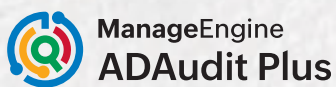
Support for MS SQL database

And much more

[Try now](#)

Licensing and pricing details

License module	Annual subscription price
Domain controllers	Starts at \$595
Add-ons	
Entra ID Tenants	Starts at \$995
Windows file servers	Starts at \$495
NAS servers (NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx, QNAP, Azure Files, CTERA, Nutanix, and Qumulo file servers)	Starts at \$595
Windows servers	Starts at \$345
Workstations	Starts at \$245
User count (for AD backup and recovery)	Starts at \$195
Data size in TB (for File analysis)	Starts at \$145



A UBA-driven change auditor that keeps your AD, Microsoft Entra ID, Windows servers, file servers, and workstations secure and compliant.

Download now

Free, 30-day trial

Contact details

Website:

www.adauditplus.com

Personalized demo:

www.manageengine.com/products/active-directory-audit/demo-form.html

Get a quote:

www.manageengine.com/products/active-directory-audit/get-quote.html

Live online demo:

www.demo.adauditplus.com

Email tech support:

support@adauditplus.com

Sales inquiries:

sales@manageengine.com

Toll-free call:

+1.408.916.9891