DATASHEET

ManageEngine
ADAudit Plus

A UBA-driven change auditor

Protect your enterprise from insider threats and cyberattacks by auditing your Active Directory (AD), file servers, Windows servers, and workstations with ManageEngine ADAudit Plus.

Active Directory and Azure 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.

- **Monitor hybrid AD environments:**
  Get a unified view of all activities happening across your on-premises and Azure AD environments with alerts for critical events.

License modules:
Domain Controllers, Azure AD Tenants

Supported platforms:
WWindows Server 2003 and above

File Change 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.
- **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.
- **Audit permission changes:** Track NTFS and share permission changes along with details such as their old and new values.
- **Streamline compliance audits:** Receive out-of-the-box reports for HIPAA, GDPR, FISMA, PCI DSS, SOX, GLBA, ISO 27001, and more.
- **Monitor file integrity:** Receive detailed reports on all changes made to critical system and program files, and trigger alerts when suspicious activity is detected.
- **Audit across multiple platforms:** View changes across Windows file servers, failover clusters, NetApp filers, Synology NAS, Hitachi NAS, EMC VNX, VNXe, Isilon, Celerra, and Unity from one console.

License modules:
Windows File Servers, NAS Servers

Supported platforms:
• Windows Server 2003 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 and OceanStor 9000 V5 storage systems

Group Policy settings change auditing

- **Audit Group Policy Objects:** Keep an eye on Group Policy Object (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.

License modules:
Domain Controllers

Supported platforms:
Windows Server 2003 and above

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.

License modules:
Member Servers

Supported platforms:
Windows Server 2003 and above

Logon and logoff auditing

- **Audit logons and logoffs:** Track logon and logoff activity and logon duration across your domain controllers (DCs), Windows servers, and 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 machine learning to rapidly spot and respond to unusual volumes of logon failures, unusual logon times, and more.

License modules:
Domain Controllers, Member Servers, Workstations

Supported platforms:
• Windows Server 2003 and above • Windows XP and above

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 logins, 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 user behavior analytics (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, Member Servers, Workstations

Supported platforms:
• Windows Server 2003 and above • Windows XP and above

Employee activity monitoring

- **Measure employee productivity:**
  Know how employees spend their work hours with computer startup and shutdown times, logon history details, file activity, and more.

- **Track employee attendance:**
  Maintain accurate time sheets for your employees with their clock-in and clock-out times, and analyze their logon duration.

- **Calculate actual working hours:**
  Find the list of users currently logged in and calculate their actual work hours with details on when they were active and idle.

- **Monitor remote workers:**
  Track remote desktop gateway and RADIUS logons, and know who attempted to log on remotely, when, whether they were successful, and how long their session lasted.

- **Monitor employees' computer activity:**
  Find recent startup and shutdown times for a computer, along with details on who initiated it, the shutdown type, and more.

- **Identify risky logon activity:**
  Spot and analyze repeated failed attempts to log on to workstations, remote machines, and critical servers with instant email and SMS alerts.

License modules:
Workstations

Supported platforms:
Windows XP and above

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, Member Servers

Supported platforms:
Windows Server 2003 and above

Malware and insider threat detection

- **UBA-powered threat hunting:**
  Quickly spot repeated logon failures, user activity anomalies, privilege escalations, data exfiltration, and more with UBA.

- **Detect ransomware intrusions:**
  Spot telltale indicators of ransomware intrusions such as unusual spikes in file renaming, deletion, or permission change events.

- **Respond to threats instantly:**
  Automatically execute scripts to shut down machines, end user sessions, or carry out other tailor-made responses to mitigate threats.

- **Identify file activity anomalies:**
  Trigger alerts for suspicious activities such as the deletion of critical files, sudden surges in file access, or file activities at unusual times.

- **Detect lateral movement:**
  Spot indicators of lateral movement like out-of-the-ordinary remote desktop activity or the execution of new processes.

License modules:
Domain Controllers, Member Servers, Windows File Servers, NAS Servers, Workstations

Supported platforms:
• Windows Server 2003 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 and OceanStor 9000 V5 storage systems • Windows XP and above

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, 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, Member Servers, Windows File Servers, NAS Servers, Workstations

Supported platforms:
• Windows Server 2003 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 Version 13.2 and above • Huawei OceanStor V5 series and OceanStor 9000 V5 storage systems • Windows XP and above

System requirements

For the complete system requirements, see the Quick Start Guide.

Supported browsers:
Internet Explorer 8 and above, Mozilla Firefox 3.6 and above, Google Chrome, Microsoft Edge

Processor: 2.4GHz

RAM: 8GB

Disk space: 50GB

Supported platforms

DC and member server auditing	File auditing	Other components
Windows Server versions: 2003/2003 R2 2008/2008 R2 2012/2012 R2 2016/2016 R2 2019	**Windows file server auditing:** Windows File Server 2003 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:** OceanStor V5 series and 9000 V5	**ADFS auditing:** ADFS 2.0 and above **Workstation auditing:** Windows XP and above **PowerShell auditing:** PowerShell 4.0 or 5.0

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	
Azure AD Tenants	Starts at $595
Windows File Servers	Starts at $495
NAS Servers (EMC, NetApp, Synology, Hitachi, Huawei)	Starts at $595
Member Servers	Starts at $595
Workstations	Starts at $245

ManageEngine ADAudit Plus

A UBA-driven change auditor that keeps your AD, 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