ManageEngine
ADAudit Plus

A UBA-driven change auditor

Keep your Active Directory, Windows servers, file servers, and workstations secure and compliant

www.adauditplus.com

What is ADAudit Plus?

ManageEngine ADAudit Plus is real-time change auditing and reporting software that can:

- Monitor your Active Directory (AD), Azure AD, Windows file servers, member servers, and workstations, and help you adhere to regulations such as HIPAA, GDPR, SOX, CCPA, GLBA, and more
- Transform raw and noisy event log data into actionable reports that show you who did what, when, and from where in your Windows ecosystem in just a few clicks
- Identify anomalous activity and detect potential threats to your enterprise using its user behavior analytics (UBA) capabilities

How ADAudit Plus can help your organization

With ManageEngine ADAudit Plus, you can:

1. View detailed reports on changes made to on-premises and Azure AD
2. Gain visibility into Windows user logon activity
3. Report on, analyze, and troubleshoot AD account lockouts
4. Closely monitor privileged user activities in your domain
5. Track logons/logoffs, changes to users, groups, etc.
6. Audit file activity in Windows, NetApp, EMC, Synology, Huawei, and Hitachi storage
7. Enhance threat detection with user behavior analytics (UBA)
8. Get prepackaged audit reports for SOX, HIPAA, PCI DSS, GDPR, and other regulations

Highlights of ADAudit Plus

1. AD and Azure AD change auditing and reporting
2. File server auditing (Windows, NetApp, EMC, Synology)
3. Group Policy settings change auditing
4. Windows server and member server auditing and reporting
5. Workstations auditing
6. User behavior analytics (UBA)
7. Privileged user monitoring

Active Directory auditing

Report on changes made to AD objects and GPOs; track user logon activity, analyze account lockouts, and more

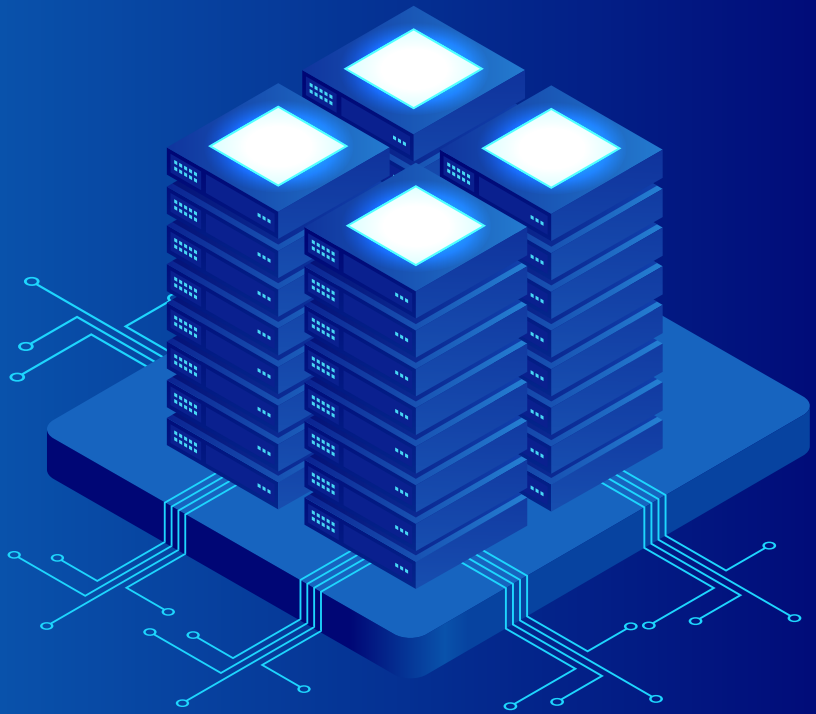
www.adauditplus.com

AD auditing

- **Audit all AD object changes:** Track changes made to OUs, users, groups, computers, and other AD objects with details such as the old and new values of the changed attributes
- **Track GPO setting changes:** Audit changes made to GPOs and their settings, including computer configuration changes, password and account lockout policy changes, etc.
- **Monitor user logon activity:** Get detailed reports on users' successful and failed logon attempts
- **Troubleshoot account lockouts:** Detect account lockouts quickly with alerts, and identify their source from an extensive list of Windows components
- **Gain visibility into privilege use:** Keep a close eye on privilege use in your enterprise by continuously auditing privileged user accounts and maintaining a detailed audit trail
- **Audit hybrid AD environment:** Get a single, correlated view of all activities happening across hybrid environments with alerts for critical events

File server auditing

Audit and report on file accesses and modifications across Windows, NetApp, EMC, and Synology storage devices



www.adauditplus.com

File server auditing

- **Monitor file and folder accesses:** Track all file activity—including read, delete, modify, copy-and-paste, move, and more—in real time
- **Detect failed file access attempts:** Receive reports on failed attempts to access files or folders
- **Audit permission changes:** Track NTFS and share permission changes along with details such as their old and new values
- **Monitor file integrity:** Easily detect critical events such as changes made to a specific file, by a particular user, or more with email and SMS alerts on these events
- **Audit file shares:** Track every access and change made to shared files and folders in your domain with details on who accessed what, when, and from where

Group Policy settings change auditing

Audit changes made to Group Policy settings, including password and account lockout policy changes, computer changes, etc.

Group Policy settings change auditing

- **Audit Group Policy Objects:** Audit and report on Group Policy Object (GPO) creation, deletion, modification, and more
- **Track changes to GPO settings:** Keep a close eye on who changes what GPO settings, when, and from where with comprehensive reports
- **Configure alerts for critical changes:** Receive instant email and SMS alerts for critical changes, such as computer configuration changes, password and account lockout policy changes, etc.
- **Maintain an audit trail:** Generate reports on the values of GPO settings before and after every change to instantly spot unwanted changes

Windows server auditing

Monitor member servers with real-time reports and alerts to keep a close eye on activity in your Windows network

www.adauditplus.com

Windows server auditing

- **Audit Windows servers:** Monitor changes to local administrative group memberships, local users, user rights, local policies, and more
- **Track scheduled tasks and processes:** Audit the creation, deletion, and modification of scheduled tasks and processes
- **Monitor removable device usage:** Identify USB plug-ins and file transfer activities to removable storage devices
- **Audit PowerShell processes:** Monitor PowerShell processes that run on your Windows servers along with the commands executed in them
- **Audit AD federation services (ADFS):** Report on successful and failed ADFS authentication attempts in real time

Workstation auditing

Track users' logon and logoff information, productive hours, logon history details, removable storage use, and more

www.adauditplus.com

Workstation auditing

- **Audit logon and logoff activity:** Track logon and logoff activity across your Windows network, record logon duration, and identify users who are currently logged on
- **Track user logon history:** Record every logon activity, identify users logged on to multiple machines, monitor RADIUS logons, and more
- **Identify logon failures:** Track all failed logon attempts with information on who attempted to log on, what machine they attempted to log on to, when, and the reason for the failure
- **Monitor file integrity:** Receive detailed reports on all changes made to system and program files
- **Measure employee productivity:** Track employees' idle time and actual work hours to ensure high productivity across your enterprise

User behavior analytics

Detect and mitigate threats like malicious logins, lateral movement, privilege abuse, data breaches, and malware

www.adauditplus.com

Threat hunting with UBA

- **Process logs from across your environment:** Collect and process logs from configured DCs, member servers, and workstations

- **Identify a safe baseline:** Processed log data is used to create a user-specific baseline of normal logon, file, user management, and process activities

- **Identify anomalies and alert admins:** Incoming log data and processed baselines are compared to detect anomalies and notify admins, so they can investigate further

- **Detect potential security threats:** Quickly spot potential cases of malicious logons, privilege abuse, privilege escalations, data exfiltration, malware attacks, and more

- **Automate incident responses:** Reduce the time it takes to mitigate damage by instantly shutting down devices, terminating user sessions, or more based on the security incident

Privileged user monitoring

Audit privileged user accounts across your domain and maintain an audit trail to quickly detect suspicious behavior

www.adauditplus.com

Privileged user monitoring

- **Audit administrator activity:** Track administrative user actions on Active Directory (AD) schema, configuration, users, groups, organizational units (OUs), Group Policy Objects (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 they are necessary for the user's role and duties

- **Spot behavioral anomalies:** Identify actions deviating from normal access patterns to find attackers using the stolen or shared credentials of privileged accounts

- **Receive alerts on suspicious activity:** Rapidly spot and respond to critical events, such as the clearing of audit logs or accessing critical data outside business hours, by configuring alerts

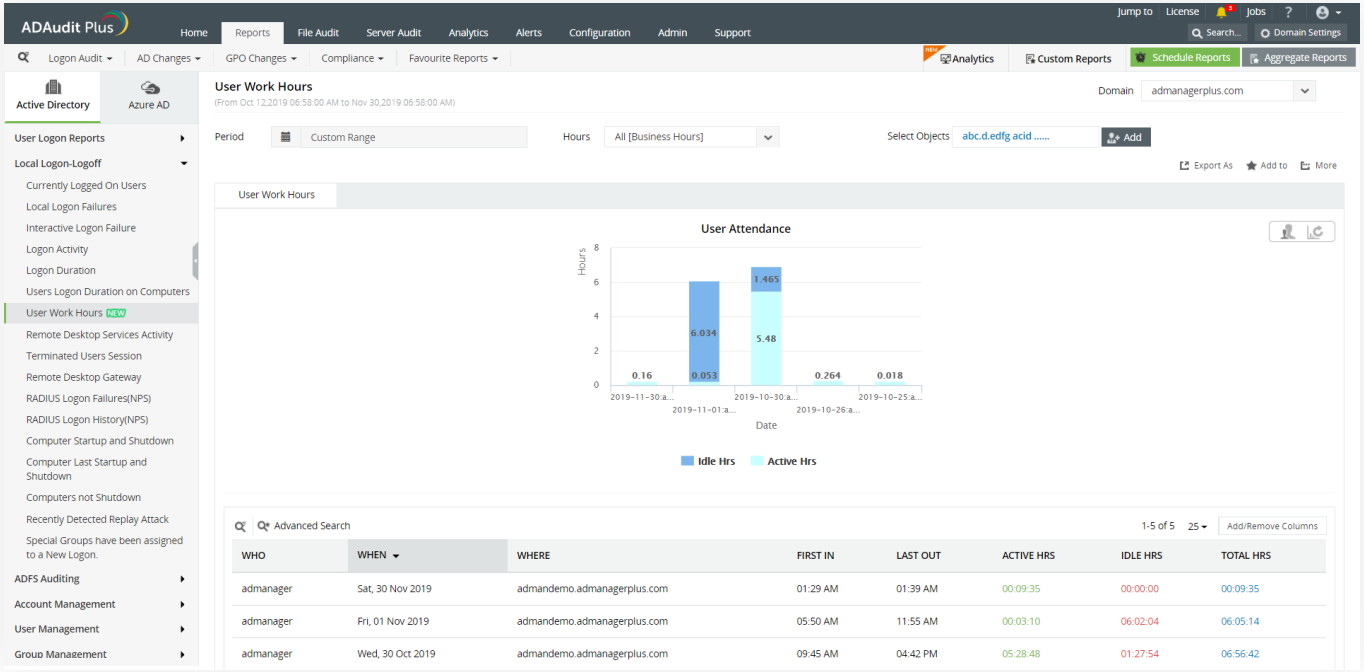
Most popular features

A birds-eye view of the features that our customers love

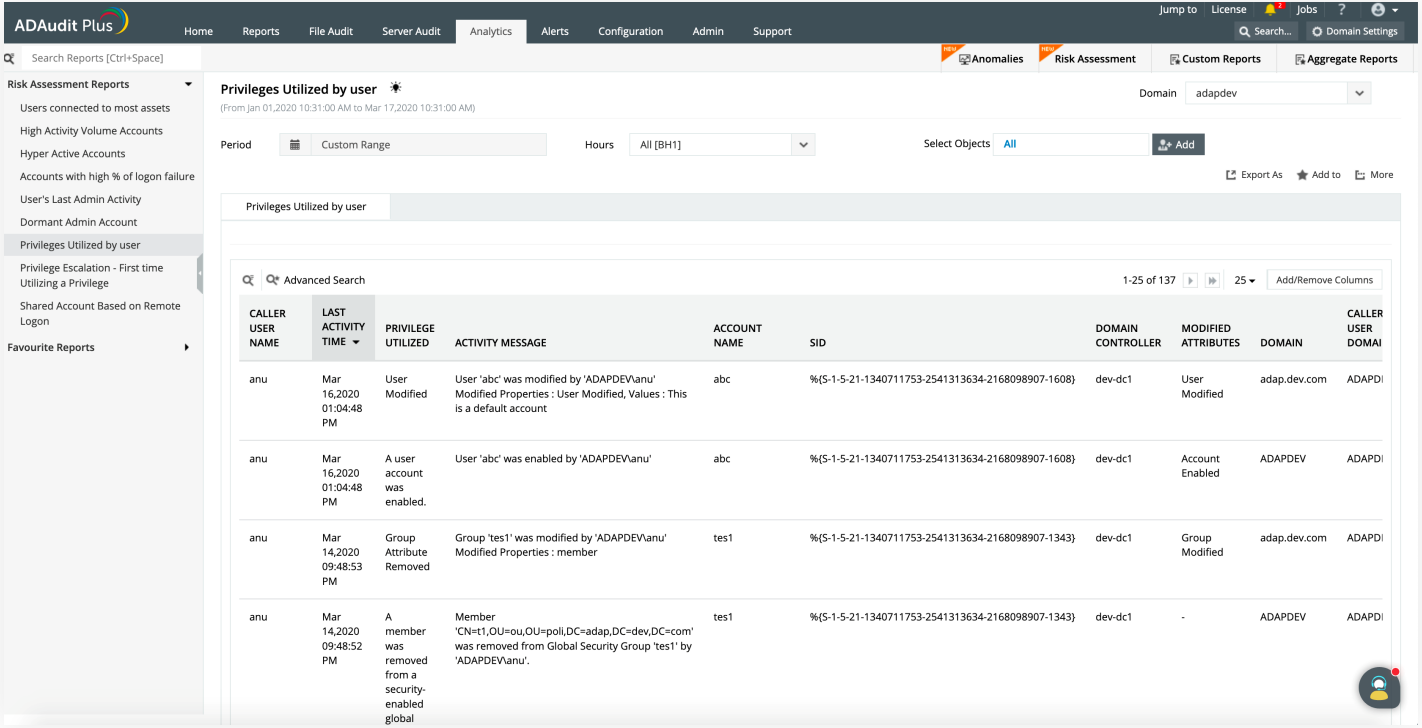
www.adauditplus.com

More features our customers love

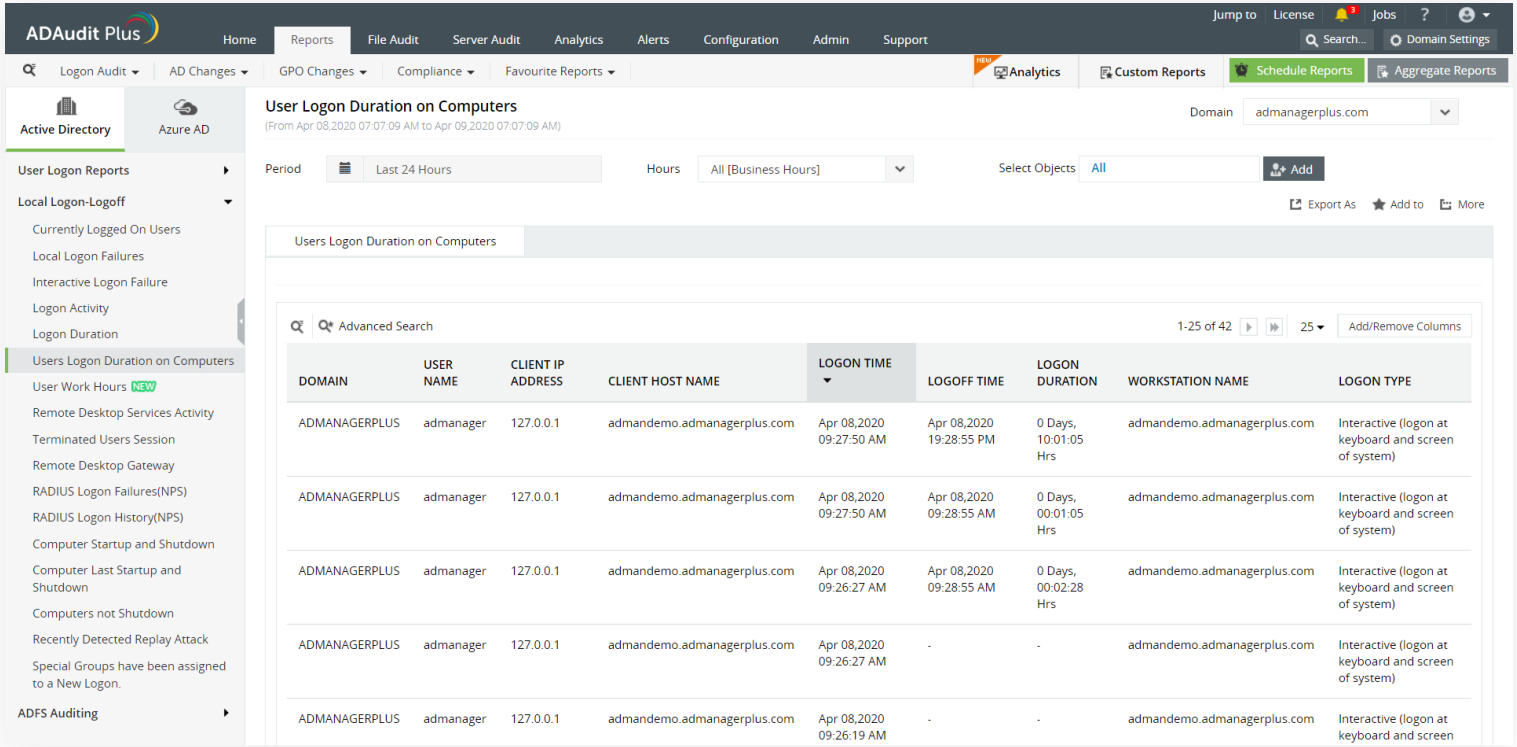
- **User work hours monitoring:** Track attendance, active hours, idle hours, and productive hours of employees using any computer within your environment



- **Insider threat detection:** Instantly spot insider threat indicators like malicious logins, privilege abuse, lateral movement, data mishandling, and more



- **Logon/logoff tracking:** Get user-specific information on logon and logoff actions, see which users are logged on to multiple computers, and view the IP addresses and logon times



Why ADAudit Plus stands out

- **Instant alerts:** Receive instant email and SMS notifications about critical events or activities by a critical user
- **Threat detection and response:** The UBA engine quickly detects privilege abuse, insider attacks, malware, and other threats, and executes tailor-made responses
- **Over 250 reports:** Streamline compliance with multiple regulations, including PCI DSS, HIPAA, SOX, GDPR, GLBA, ISO 27001, and more with audit-ready reports
- **Log archiving and forensic analysis:** Archive audit data at a user-defined location, and generate reports based on it when needed
- **Top-notch customer support team:** Our efficient support team is only an email, phone call, or chat away

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 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 auditing: Huawei OceanStor V5 series and OceanStor 9000 V5 storage systems	• AD FS auditing: AD FS 2.0 and above • Workstation auditing: Windows 10, 8, 7, Vista, and XP • PowerShell auditing: PowerShell version 4.0, 5.0

Available editions

Standard	Professional	Free
Download 30-day trial	Download 30-day trial	Download Free edition
Reports and alerts on event log data collected from the below licensed components: • Domain controllers • Azure AD tenants • Windows servers • Workstations • Windows file servers • Synology NAS servers • NetApp filers • EMC file servers	Includes all the features of the standard edition, along with: • Account lockout analysis • Group Policy setting change tracking • Before and after values of AD object/attribute changes • AD permission change auditing • DNS change tracking • AD schema and configuration change tracking, etc.	Includes all the features of the professional edition for 30 days from the date of installation. It also: • Never expires • Provides audit reports for up to 25 workstations • Allows report generation for event log data collected during the evaluation/ license period

Licensing details

ADAudit Plus' licensing for the Active Directory Auditing component is based on the number of domain controllers.

Other add-ons are based on the number of:

- Azure AD tenants
- File servers
- EMC file servers/NetApp Filers/Synology NAS servers/Huawei NAS servers/ Hitachi NAS servers
- Member servers
- Workstations

Evaluation assistance

There are a number of ways we can help you during your evaluation of ADAudit Plus. These include:

- A fully-functional 30-day free trial
- Extension of evaluation license, if needed
- 24x5 technical support and guided demo options
- A live demo hosted at demo.adauditplus.com
- Detailed installation and configuration guides
- An extensive knowledge base

Nine of every ten Fortune 100 companies trust us to manage their IT

And we have the credentials to prove it

ADAudit Plus was named a 2019 Gartner Peer Insights Customer's Choice for SIEM

ManageEngine
ADAudit Plus

In their own words

A good web based and cost effective solution. We like the auditing option on NetApp Filer. Also, it has partially to do with our satisfaction with other products that ManageEngine has excelled in.

Ricky Chand
Systems Engineer, Bank of South Pacific, Fiji

Prior to ADAudit Plus, we had no visibility into our AD infrastructure. Now we're able to monitor all AD transactions as far as group changes, User creation, security, authentication logs and much more.

Callixtus Muanya,
Windows administrator, Harvard Medical School

Read more of our customers' testimonials here.

Contact details

Telephone

+1-925-924-9500

Email the support team

support@adauditplus.com

Visit our website

www.adauditplus.com

Mailing address

ZOHO Corporation 4141 Hacienda Drive, Pleasanton, CA 94588, USA

Get a fully-functional, 30-day free trial

Download now