Active Directory Management
Automate compliance reporting

Quick start guide

wanstor

Automate compliance reporting

Regardless of the compliance requirements that your organisation are trying to fulfil, many current methods of gathering user data for generating reports are inefficient, ineffective, and fail to provide information that can confirm network security practices and protocols are in place.

Auditors, administrators, and security professionals need solutions that provide them with quality reports in a time frame that captures the correct security information.

> **One way to solve these concerns with compliance reporting is to use automation to generate reports.**

Automating report generation can solve not only the concerns around inefficiency and ineffectiveness, but can also make sure current security configurations are provided and reports are accessible.

More importantly, automating report generation makes sure your security compliance reports are accurate and available when you need them.

Inefficiency of current reporting methods

Nearly all audits for major compliance regulations, like SOX, HIPAA, PCI DSS, FISMA, GLBA, and ISO 27001, are performed once a year.

This means that auditors must request reports for each compliance regulation at the time of the audit. In some cases, reports from one audit can be used for another audit.

This does provide added value in making at least an area of the audit more efficient.

However, the current method for obtaining reports is not effcient for anyone involved in the process.

wanstor

Administrators must generate reports

Over the past 10+ years, performing audits has proven to be a frustrating process for everyone involved.

In general, auditors, administrators, and security professionals do not look forward to any audit. This is mainly due to the time required to gather reports, analyse them, and write up the results.

Just looking at the first two steps in the audit process exposes major concerns about efficiency in the collection of and reporting around data.

> **All of these factors result in auditors and administrators spending a significant amount of time on report generation and analysis.**

If these concepts could somehow be altered to make sure reports are generated the same way each time and are always available to the auditor, the overall audit process could be made more efficient.

A typical audit process

+ Auditors must request reports from administrators.
+ Administrators are required to take the time to generate auditor reports.
+ Quite often, one report doesn't correctly provide the information needed by the auditor, so administrators need to generate more reports.
+ There is no standard for report generation, forcing administrators to use different tools and report structures, as well as generate various file types.
+ Without consistent report structures and content, report analysis can take much longer than expected.

Auditors must wait for reports

Since auditors do not have the privileges required to generate security-based reports, they must follow procedures to request reports.

Unfortunately most auditors are not familiar with the operating system or application they need the report from, so they are left to describe the report content they are looking for.

> IT administrators, on the other hand, are generally seen as busy employees.

They do not have extra bandwidth to work full time with the auditor to make sure that the reports produced are 100% accurate.

This leaves IT administrators to decide which tools to use and what format they should use to produce the reports.

During this time, the auditor must wait for the IT administrator to send them the report.

In many cases, the report that the IT administrator produces does not meet the auditors' detailed requirements, so the entire process must be repeated, from describing what is needed to guessing which tool/format to use for each report.

Ideally, if everyone involved in the audit could determine which format is most efficient for analysis and select a tool to produce the correct content and format, the entire process could be automated.

If the reporting process was automated, auditors could have reports waiting for them when they need them.

The reports would also include the most recent security settings, and historical reports that indicate any changes over time.

Infectiveness of current reporting methods

Most of today's compliance audits are done as *"point-in-time"* audits. This means that once a year (usually) reports are generated on carefully selected security settings and configurations.

Then the auditor analyses these reports to determine if the organisation's security meets certain compliance requirements.

If the current settings do not meet compliance requirements, the final report will indicate that the administrator needs to alter their settings.

> The issue with this concept is the data the auditors are reviewing is only one snapshot in time.

The week, month, or year before the report was generated isn't included on reports; and there is no indication of what the security setting has been, only what it is at the time of the report.

Unfortunately this is not the only issue; there are other potential scenarios which make this type of audit process invalid.

For example:

- What if the administrator changes the security setting seconds before running the report, only to change it back after running the report?
- What if the security setting was incorrectly configured for a week, leaving the network exposed, but is correct at the time of running the report?
- What if the administrator alters the security setting from the final report from the auditor, only to change it a week after the auditor moves on to the next project?

The overarching goal of any compliance regulation and audit is to verify that the proper security standards are in place.

However, just analysing a single second during an entire year only verifies that one second, not the other 364 days, 23 hours, and 59 minutes.

In order for compliance to be useful, and security to be in place, auditors must be able to constantly receive reports proving that the security settings are not changing.

If auditors can receive constant reports and alerts for all changes to security settings, this can be considered true continuous auditing. True continuous auditing is the best form of security to ensure that a network is protected.

Auto-generating reports

Instead of performing audits that are inefficient and ineffective, let's consider another option - automation.

Using automation to generate reports solves the major issues which were highlighted in the previous section of this whitepaper, with a few added benefits:

+ Reports will always follow a standard format and structure from audit to audit
+ Reports can be generated once a day, week, month, etc
+ Auditors are not required to ask administrators to generate reports
+ Administrators will not need to take time and iterations to generate reports
+ Auditors will be able to analyse reports over time, instead of just at a single point in time
+ Auditors can easily view and analyse security changes.
+ All security setting and configuration reports can be customised for automation

Reports for each compliance regulation

Each compliance regulation has a unique set of requirements. This means each regulation has its own set of required reports.

Trying to decrypt these reports can be time-consuming, confusing, and frustrating. Once an organisation has decided what reports it needs for each of the compliance requirements, they can duplicate the reports for each cycle of the audit.

This is exactly what the ManageEngine suite of tools has done for each of the major compliance regulations. Log360 (which includes EventLog Analyzer and ADAudit Plus) provides reports for each compliance regulation, giving you a quick and easy way to automatically produce compliance reports.

As many IT administrators have seen, there are some reports that are required based on their company's needs, their operating systems and applications, or perhaps even the external auditor's interpretation of the regulations.

In order to meet these requirements, customised reports may be needed. It is essential that these custom reports be easy to design and implement, as well as automate.

ManageEngine's products are built to include custom reports that are very simple to create.

Since each organisation has different needs regarding reports for audits and analysis, all reports should have options for scheduling.

There should be a good balance between reports generated and reports being reviewed and analysed.

Too many reports can overwhelm the auditor; whilst too few reports will not give the auditors enough information for a decent analysis.

By default, compliance reports contain security-related information. If the wrong person can see the contents of compliance reports, it could result in a breach of some kind. This means it is imperative that these reports be secured.

Ideally, report automation will store the reports in a secure folder which is only accessible by approved IT, security, and auditors.

Again, ManageEngine allows IT administrators to store reports in a folder of their choosing, which can of course be locked down with security permissions.

Automate common reports

Each compliance regulation has a different sets of requirements for Windows security reports. This being said, there are some reports that are common across multiple compliance regulations.

Log360 provides reports which are separated by the compliance regulation that you are focusing on. For instance, Figure 1 illustrates reports for SOX compliance.

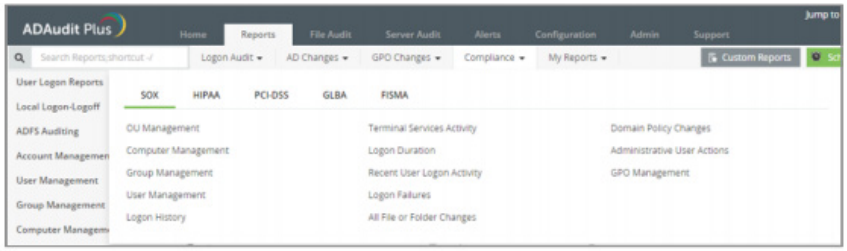


figure 1: Log360 supports all of the key compliance regulations

Automate custom reports

In many cases, a compliance regulation goes beyond the basic operating system installation and requires organisations to report on customised configurations. These requirements force administrators to produce reports that aren't available in any kind of reporting solution, as the objects being reported on are unique to each organisation.

Tools such as Log360 enable IT administrators to create custom reports, allowing them to meet these specific areas in compliance regulations. Figures 2 and 3 illustrate custom reports.

With Log360, any built-in report can be customized; administrators can also develop many custom reports using complex and detailed security requirements.

Automate and schedule report generation

As you can see, Log360's built-in and custom reporting capabilities are very powerful for IT teams and Auditors alike. Any and all reports that are available in Log360 can be automated and scheduled.

This provides a thorough view of all the changes for the compliance areas and settings that you need to report on. Creating automations for each and every report is easy using Log360.

Once an IT Administrator has opened a report in ADAudit Plus, they simply select the *"Add to"* button and select *"Schedule this report"*

Figure 2. A custom report using a built-in report as a foundation in Log360.

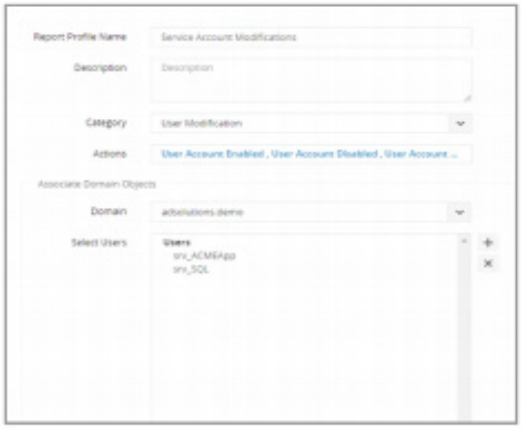


Figure 3. A custom report focusing on any changes to service accounts.

Figure 4. Scheduling a report in Log360.

Now all the IT Administrator has to do is select how often they would like to generate the report, along with the details shown in Figure 5. The IT Administrator can also make sure that an email is sent every time this report is automatically generated.

Once the IT Administrator has all of their compliance reports scheduled to automatically generate, it will free them up to concentrate on other administrative tasks.

Summary

Compliance can be a tedious and time consuming task. There are many compliance regulations out there, each requiring separate reports. Ideally, these reports would be automatically generated and emailed to the appropriate people in a chosen organisation when they're completed.

While Microsoft does not provide an efficient and effective solution for automatic report generation, ADAudit Plus from ManageEngine is the ideal solution to solve all of your reporting needs, and this is why Wanstor recommends this product to all of it's IT Support customers.

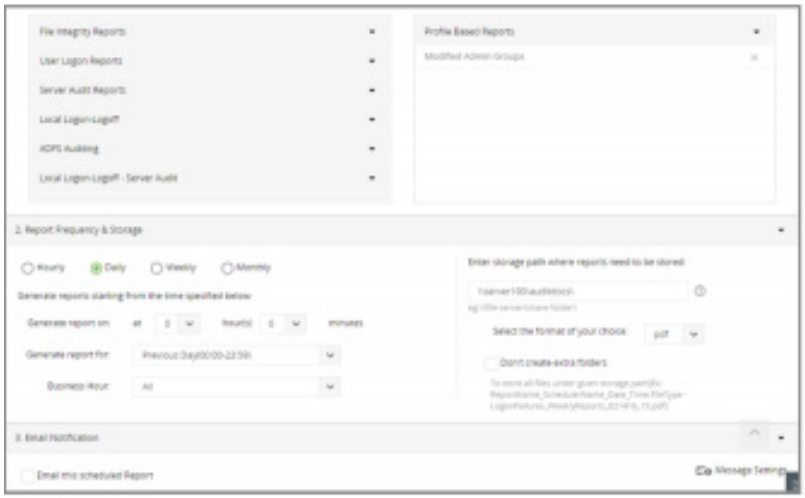


Figure 5. Report Scheduler in ADAudit Plus.

Solution Summary

Since its availability with Microsoft Windows 2000, business and not for profit organisations have used Active Directory to help administer and secure their Windows environments.

- Track information of users
- GPO
- Advanced GPO
- Groups
- Computer
- OU
- Configuration
- DNS
- Permission
- Schema changes

The tool gives IT administrators access to over 150+ detailed event specific reports and instant emails alerts so IT teams can understand what their users are up to and track every change in Windows AD, system, permission, configuration and file modifications by Admin, Users, Helpdesk, HR etc.

By having access to these reports IT administrators can preconfigure reports and set email alerting for changes to monitored folders / files.

This helps them to meet a range of compliance requirements for storing and managing data and user access rights.

ADAudit Plus falls into 4 category areas to help IT administrators. In this whitepaper we will explain what these 4 key areas are and give some examples of where the tool really adds business value for the IT Team.


User Audit


Group changes


GPO settings changes


Logon failures


Membership changes


OU Management


Reports
View from the 150+ pre-configured audit reports with automatic periodic report generation - right to your inbox. 50+ Search Attributes I Schedule email reports Filter reports on business / non-business / all hours I Browser-based.
Alerts
Instant on-screen alerts and emailing of alerts to your inbox! User, time and volume based threshold alerts help identify the problem precisely. Email Notification I Web Based I In-Depth Event Analysis.
Active Directory
Administrators can track all domain events like Logon / Logoff, audit User, Group, Computer, GPO, OU changes with 150+ ready-to-view reports and email alerts. Exportable Reports | Archive Audit Data | Assign Operator roles (reports view only) for Compliance | Much, much more.
Workstations
Monitor every user logon / logoff and know the day-to-day user actions with detailed reports of every successful / failure logon event across workstations in the network.
File Server
Securely track File Server / FailOver Cluster for document changes to files (file creation /modification / deletion) and folders audit-access, shares and permissions.
Member Server
Monitor every Windows Member Server change with various detailed reports: Summary Report, Process Tracking, Policy Changes, System Events, Object Management and Scheduled Tasks.
File Integrity
Securely track File Server / FailOver Cluster for document changes to files (file creation /modification / deletion) and folders audit access, shares and permissions.
NetApp
Centrally audit, monitor and report with instant alerts on the NetApp Filer CIFS Shares changes. View reports on files created / modified / deleted, permission changes, failed attempt to file read / write.
Removable Storage
Monitor changes on every removable storage device with reports on all file or folderchanges, file read / modified / copy and paste. This feature is supported only inWindows Server 2012 & Windows 8.
Printers
Track all files printed over the Windows network, with thorough reports on the printerusage, recent print jobs, user / printer based reports for added security & SOX, HIPAACompliance.
Databases
Audit your Windows Server Environment from a choice of database formats: SQL Server, PostgreSQL and MySQL.
Other AD objects
Keep a track on other significant AD Objects: Containers, Contacts, Schema, Configuration, Site, DNS & Permission changes.
ManageEngine
ADAudit Plus
Admin
Administrator can audit and monitor with the 150+ pre-configured reports and instant email alerts for a clear view on the Windows Server environment changes.
Ease of use
Centrally operated, web based, detailed yet simple reports even for non-technical personnel with alerts help answer the four vital Ws: Who' did 'what' action, 'when' and from 'where'! Also, export the results to xls, html, pdf and csv formats for analysis.
Compliance
Get specific 'set of detailed graphical reports' for SOX, HIPAA, GLBA, PCI and FISMA to easily meet each compliance requirements.
Data archiving
To control the database growth, processed event log data older than what is required for immediate audit reporting can be cleared from the ADAudit Plus database and archived, saving on space. Unzip at ease for history reporting, compliance and forensic analysis.

Real-Time Windows Active Directory Auditing

IT administrators can have real time access to Active Directory files to make sure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes. The main areas this tool helps with include:

Insider Threats

Discover the signs of an insider attack. For any given account, extract a cosolidation of 3 audit trails - user actions in AD, access reports, and permission change reports.The audit trail offers a context which makes spotting the insider easier. IT teams can also learn instantly which computers a user compromised and the changes they made.

User Logon

Monitor user logon activity in real-time on Domain Controllers with pre-configured audit reports and email alerts. Audit reports make sure the IT administrator knows the reason behind user's logon failures, login history, terminal services activity, and users recent logon activities across the Windows server network.

Compliance

All business and not for profit organisations have to comply with industry specific Compliance Acts like SOX, HIPAA, GLBA, PCI-DSS, FISMA... With our Compliance specific pre-configured reports and real-time alerts, we make sure your Windows network can be audited 24/7 with periodic security reports and email alerts as standard procedure.

Reporting & Alerts

Choose from over 200+ pre-configured audit reports; create custom reports, set profile based reports and report from archived data for forensics. In real-time, track Windows AD object changes (Users, OU, Groups, GPO, Computer, Schema, DNS and System) and receive email alerts on unauthorized network access / modification events.

Data archiving

Run periodic archiving of audited events data to save on disk space. View reports from past events like Active Directory user logon history, password change history and more from the Active Directory archived audit data for computer forensics or compliance. The audited reports can be exported to xls, csv, pdf and excel formats.

GPO Settings

Audit and Report on the GPO changes to the Windows Active Directory and Windows Servers. AD Audit Plus provides in-depth advanced tracking of the Group Policy Objects new and old values, configuration, password policy and settings changes. This helps IT teams to meet IT network security compliance requirements.

Windows Log On/LogOff Auditing

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with email alerts for periodic analysis & quick response during security threats.

Logon/Logoff

Windows user workstations auditing reveals the exact logon and logoff time to quickly verify the user's status at the time of a unauthorized access attempt from the user's workstation. IT administrators can also gain access to the known logon terminal services activity with reports and instant email alerts.

Compliance

All organisations have to comply with industry specific Compliance Acts like SOX, HIPAA, GLBA, PCI-DSS, FISMA... With ADAudit Plus IT administrators can access compliance specifis pre-configured reports and alerts. We also make sure your network is fully auditable 24/7 and IT Administators have access to periodic security reports and email alerts as standard.

Data Archiving

From within the AD Audit product, IT Administrators can run periodic archiving of audited events data to save on disk space. View reports from past events like Workstations user logon history, logon failures, terminal services history and more from the Workstations archived audit data for computer forensics or compliance needs. The audited reports can be exported to xls, csv, pdf and excel formats.

Reporting & Alerts

Choose from a number of pre-scheduled, pre-configured Workstations audit reports with many filter features. Create custom reports, set profile based reports and also, report from archived data for forensics. Track Windows Workstations activity and gain access to email alerts on unauthorized network access events.

All workstation reports

A complete set of workstation reports that help IT administrators and auditors to audit and monitor workstation events from every possible approach with numerous easy to understand graphical reports.

Windows File Server Auditing

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

With Windows File Server Auditing in a Microsoft Server Environment, IT administrators can securely monitor and view pre-configured reports / get instant email alerts for the modifications, document access, file/folder structure changes, shares and access permissions.

Access Permissions

IT administrators can audit the security settings to gain a full view on network shares in Windows. They can also keep track of every 'file/folder, shares & permission' modifications, and track the 'discretionary' and 'SACL' modifications with detailed new & original security descriptor values.

Failover Clusters

Audit and Monitor the Windows File Server Failover Clusters. Track user file server cluster share and access permissions. Additionally IT administrators can audit files and share security alonside the schedulable failover cluster reports and instant Email Alerts.

Netapp Filers

Auditing the NetApp Filer for Windows enables IT administrators to track every Windows and NetApp Filer CIFS Files / Folders create, modify, delete, settings and permissions change. They can also track with pre-configured reports and email alerts at times of network security breach and on critical objects access.

EMC Servers

Audit the EMC (VNX/ VNXe/Celerra) file shares with audit reports categorized by file, server, user, share based changes along with custom reporting, and document changes to files and folders. Additionally IT administrators can monitor the access, shares & permissions and export reports for security analysis and compliance audits.

All file server reports

View all the reports under the file server reports category. The reports help IT administrators / auditors to audit and monitor the Windows file server securely and access/modify events from every possible angle with access to a variety of easy to understand graphical reports.

Windows Server Auditing

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows servers

With Windows Member Server Auditing, track logon / logoff and monitor critical Terminal Services activity like policy changes with scheduled jobs, object management, system events and process tracking reports and email alerts.

Printer Auditing

IT administrators can centrally audit, monitor and track all files that are printed over the Windows Server network, with thorough reports on the printer usage, recent print jobs, user / printer based reports for added security & SOX, HIPAA Compliance.

File integrity Monitoring

File Integrity Monitoring helps monitor the changes to the Windows system, configuration, program files (Log, audit, text, exe, web, configuration, DB files), file attributes (dll, exe and other system files) and folders. IT administrators can also, schedule periodic email reports to XLS, HTML, PDF and CSV formats for better network analysis.

Compliance

All organizations have to comply with industry specific Compliance Act like SOX, HIPAA, GLBA, PCI-DSS, FISMA. With our Compliance specific pre-configured reports and alerts, we make sure your network is under 24/7 security audit as a standard procedure.

Reports & Alerts

Audit Windows servers by viewing the pre-configured audit reports with filter attributes; Track the Windows member server logon and logoff. Benefit from terminal services activity reports, process tracking on servers and monitor the schedule tasks activity with reports and alerts.

All Windows Server Reports

IT administrators can view all the reports under the Windows servers reporting category. The reports help IT administators / auditors to audit and monitor the Windows servers security, process tracking and system events with numerous easy to understand graphical reports.

Active Directory

Practical Management Solutions

What is ADManager Plus?

What is ADManager Plus?

ADManager Plus is a simple, easy-to-use Windows Active Directory Management and Reporting Solution that helps IT administrators and Help Desk Technicians with their day-to-day activities. With a centralized and intuitive web-based user interface, the software handles a variety of complex tasks like Bulk Management of User accounts and other AD objects, delegates Role-based access to Help Desk Technicians, and generates various AD Reports as an essential requirement in satisfying Compliance Audits. This tool also offers mobile AD apps empowering performance of important user management tasks right from mobile devices at any location with an internet connection.

What problems does ADManager Plus address?

- **Eliminates repetitive, mundane and complex tasks associated with AD Management**
- **Automates routine AD Management and Reporting activities for AD Administrators**
- **Facilitates Creation, Management and Deletion of AD objects in Bulk**
- **Provides 'on the move' AD user management capability through its mobile apps**
- **Acts as an essential resource during Compliance Audits like PCI, GDPR and ISO**

What features does it offer?

+ Single and bulk user management	+ Group Computer Management	+ Help Desk Delegation
+ O365 Management & Reporting	+ Active Directory Automation	+ Active Directory Cleanup
+ Active Directory Reports	+ Real Last Logon Reports	+ Exchange Management

Key Features of AD Manager Plus

Every IT administrator faces the challenge of managing Active Directory objects including users, groups, computers, OUs and more daily. Manually performing complex tasks such as configuring user properties is extremely time consuming, tiresome and prone to error. AD Manager Plus enables automation and simplification of many of these tasks, with key features including:

MANAGEMENT

+ Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step
+ Create or modify AD objects (users, groups, contacts, OUs, computers) in bulk via CSV import
+ Perform tasks like password reset, account unlock, clean up and more
+ Streamline management of AD objects such as users and OUs with customizable templates
+ Assign, replace, or revoke Office 365 licenses in bulk
+ Manage shared, remote, room, equipment mailboxes

OU & ROLE-BASED HELP DESK DELEGATION

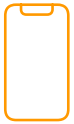
+ Delegate AD tasks to help desk technicians granularly within specific OUs
+ Delegate tasks like password reset and user creation
+ Delegate without elevating technicians' AD privileges

AD AUTOMATION & WORKFLOW

+ Automate routine tasks such as AD clean up
+ Manipulate automated tasks via workflow with automation
+ Configure review-approval workflows to execute AD tasks with a structured flow

REPORTING

+ Generate and schedule more than 150 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps
+ View inactive users, locked out users, disabled computers, and more in just few clicks
+ Perform management tasks for specific users within reports
+ Export to various formats: HTML, PDF, XLS, XLSX, CSV, CSVDE
+ Mention specific users or computers in a CSV file for generating their important details
+ Generate compliance reports to meet regulatory standards such as PCI, GDPR, ISO and more



iOS & ANDROID APPS

+ Manage users from anywhere - reset passwords; unlock, enable, disable and delete accounts
+ Report on locked out, disabled, password, expired, inactive users
+ View, manage, and execute AD workflow requests

Other Active Directory Tools by Wanstor & ManageEngine

		Features & Benefits
ManageEngine ADSelfService Plus	ADSelfService Plus is an IT self-service solution designed for Windows environments. It is a feature rich IT self service solution which can be implemented independently or integrated seamlessly with company websites.	+ Self-service password management for on-premises Active Directory and cloud applications + Notify users (email & SMS) on impending password & account expiration + Enforces granular password policies across AD and connected on-premises and cloud applications + Automatically syncs Active Directory password in real-time across multiple applications + Offers Active Directory-based single sign-on (SSO) for cloud applications
ManageEngine ADAudit Plus	In real-time, IT administrators can ensure critical resources in the network like Domain Controllers are audited, monitored and reported on with information on Users, Groups, GPO, Computer and OU changes, with 200+ detailed event specific reports and instant email alerts.	+ Web-based, Active Directory tool to track all domain events, including user, group computer, GPO, and OU changes + Audits Windows files servers, failover clusters, NetApp for doc changes to files and folders, audit access + Monitors every user logon and logoff, including every successful and failed logon event across network workstations + Tracks Windows member servers, FIM, printers, and USB changes with events summary; tracks application, policy, and system events + Brings 150+ ready-to use audit reports with instant email alerts to ensure security and meet IT Compliance requirements
ManageEngine Exchange Reporter Plus	ManageEngine Exchange Reporter Plus is a comprehensive web-based analysis & reporting solution for Microsoft Exchange, providing over 100 different reports on every aspect of the Microsoft Exchange Server environment.	+ Web-based change auditing / reporting solution for MS Exchange environments + Track / monitor enterprise ActiveSync infrastructure & inventory of related smart devices + Report on Outlook Web Access usage, mailbox traffic, mailbox growth + Supports customized reports that use data filters, automatic scheduling, and multi-format report generation + Provides audit feature to enable investigation of unauthorized mailbox logons and other critical changes
ManageEngine RecoveryManager Plus	Empowers IT teams to back up changes made to AD objects as separate versions, providing an Exchange Online backup solution for numerous Exchange functions & data	+ Automated incremental backup of Active Directory objects + Simple and granular restoration down to the attribute level + Change tracking to undo changes + Detailed version management of each attribute change + Provision to roll back Active Directory to an earlier state

		Features & Benefits
ManageEngine **SharePoint Manager Plus**	ManageEngine SharePoint Manager Plus is a tool that helps IT administrators to manage, audit and report on both on-premises and Office 365 SharePoint environments. It also allows monitoring, tracking and analysis of all activities in a SharePoint infrastructure, which facilitates informed, timely and accurate decision-making and management.	+ Web-based tool to manage and audit SharePoint on-premise servers and Office 365 configurations + Provides complete infrastructure visibility into both on-premise and online SharePoint server components + Includes out-of-the-box reports for monitoring SharePoint components such as farms, content databases, web applications, site collections, sites, lists and document libraries + Performs component level and security level auditing. Tracks permission changes, group changes and new role changes instantly with alerts + Meet compliance requirements by archiving audit log data for flexible time period
ManageEngine **DataSecurity Plus**	ManageEngine DataSecurity Plus is agent-based, real-time file auditing & reporting software that delivers complete visibility into Windows file server environments, showing IT administrators the 'who, what, where and when' behind every access event while also perform storage analysis. This helps to improve organisational Windows file server data security and information management, in a simple yet efficient and cost-effective way.	+ Web-based, real-time Windows file server access auditing & storage analysis tool helping meet data security, information management & compliance needs + Track & analyze access to files & folders by inspecting anomalies, recording access patterns & examining share & NTFS permissions + Optimize storage space by isolating old, stale & non-business files, gain insight into disk space usage & viewing file and folder properties + Actively respond to security breaches with instant email alerts. Detect & counter ransomware with mass access alerts & response automation + Stay compliant with SOX, HIPAA, FISMA, PCI, GLBA, GDPR, and other regulatory mandates
ManageEngine **O365 Manager Plus**	Providing exhaustive preconfigured reports on Office 365 & helping IT administrators perform complex tasks including bulk user & mailbox management, secure delegation and more. Monitor Office 365 services 24/7 and receive instant email notifications about service outages. 0365 Manager Plus eases compliance management with built-in reports, offering advanced auditing & alert features to keep Office 365 setups secure.	+ An Office 365 reporting, monitoring, management and auditing tool + Utilize out-of-the-box reports Exchange Online, Azure Active Directory, OneDrive for Business and Skype for Business, as well as reports on security, compliance management and licences for Office 365 + Monitor Office 365 service health around the clock, and receive instant email notifications on service outages + Effortlessly oversee your Office 365 setup with a wide range of Exchange Online and Azure Active Directory management features + Track even the most granular user activities in Exchange Online, Azure Active Directory, OneDrive for Business, Sway, and other services + Audit critical activities and changes in your Office 365 environment with custom alerts for each Offices 365 service + Delegate Office 365 administration tasks granularly to help desk staff and other non-IT users through role-based delegation

Wanstor's ManageEngine Customers

Final Thoughts

Every IT Administrator faces a number of Active Directory management challenges, which include managing user accounts in Active Directory almost every day.

Configuring user properties manually is extremely time consuming, tiresome, and error-prone, especially in a large, complex Windows network.

A solution that can automate cumbersome, boring, repetitive tasks, simplify AD management and provide exhaustive reports on tasks completed is now a must-have for all proactive IT departments, no matter what the size of their organisation.

Wanstor is ManageEngine's largest European partner. We work with ManageEngine to plan, deploy and manage Active Directory tools such as ADManager Plus in helping IT administrators overcome their Active Directory management challenges.

Our Active Directory management tools are designed to offer IT professionals absolute control over their Active Directory environment, with the main toolset that we recommend being ADManager Plus.

ADManager Plus is comprehensive web-based Microsoft Windows Active Directory management software that simplifies user provisioning and Active Directory administration with complete security and authentication, allowing only authorized users to perform management actions.

It also provides a complete set of management tools to IT administrators for efficient management of Active Directory.

For more information about Wanstor and ManageEngine's Active Directory management solutions, call us on **0333 123 0360**, email us at **info@wanstor.com** or visit our website at **www.wanstor.com** and one of our Active Directory experts will be in touch.

Wanstor | 124-126 Borough High Street | London | SE1 1LB | info@wanstor.com

wanstor