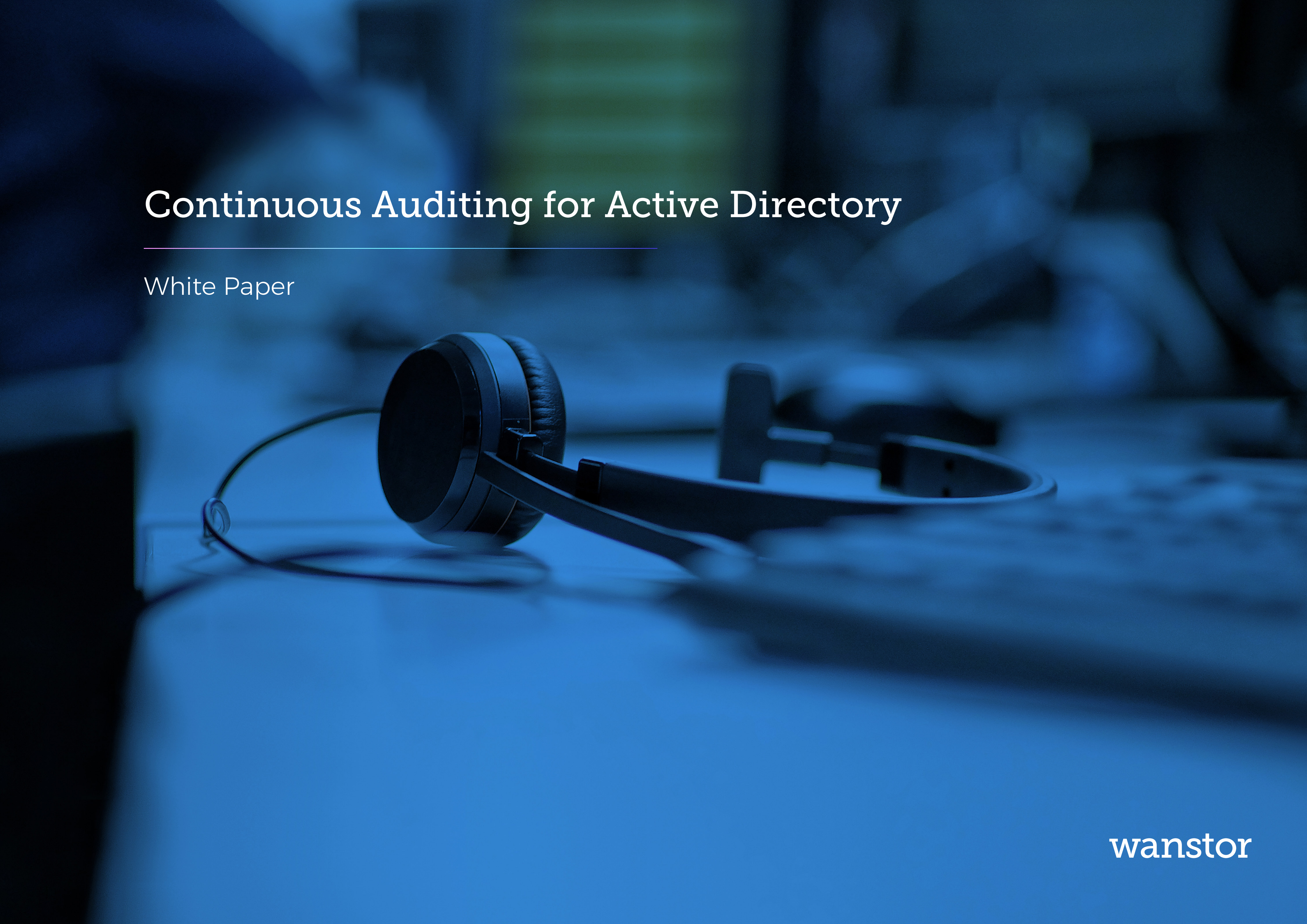


Continuous Auditing for Active Directory

White Paper

wanstor

True Continuous Auditing for Active Directory

Today, most auditors perform a standard audit on Active Directory. This standard audit is usually outdated, as it is a point-in-time solution that is only good for the day the reports were generated.

It should be noted that changes made to Active Directory can be made many times in between the standard audits, which are typically performed only once a year.

These changes made to Active Directory are not tracked, not noticed, and put the entire organisation at risk.

There are, however, solutions that provide true continuous auditing of Active Directory and the changes that occur.

The ideal solution will have built-in reports that are easy to read, separate of roles, custom reporting, and alerting.

Standard Auditing of Active Directory

A standard audit of Active Directory is completed by gathering information of the existing infrastructure. This is called a “point-in-time audit” because the auditor asks the IT administrator to gather reports based on the current state of the servers.

This means that the IT administrators must use tools (built-in or third party) to discover and report on the controls that the auditor deems important for the audit.

Scoping the Audit

If you are the IT Administrator performing an internal audit or external audit of Active Directory, you must first establish the size of the Active Directory, including all of the details related to the infrastructure.

Here are the details you will need to gather to scope the audit as a minimum:

- Number of Active Directory forests
- Number of Active Directory domains
- Number of domain controllers per domain
- Number of trust relationships per domain
- NetBIOS and DNS names per domain
- Structure of the organizational units per domain

Most organisations also include Windows servers in their audits. In order to scope and choose the Windows servers, IT administrators will need to know the following information:

- Number of Windows servers per domain
- List of key applications per server (HR, finance, intellectual property, private information, etc.)
- List of operating systems per Windows server
- List of physical locations for company being audited
- Breakdown of IT structure per location
- Design implementation of security using group policy and organizational units, if any

Development of Audit Program

The development of the audit programme is usually based on four factors: scope, sampling, compliance requirements, and security controls. Changes to any of these factors can alter the audit programme completely.

Most audits are confined to both time and resources. Of course, both are tied to money, but the amount of time and number of people are the related physical issues that deliver an audit.

Most audits are driven primarily by compliance requirements. The end result must make sure the compliance requirements are met in order to avoid fines and additional time to meet the requirements.

There is little that can be done to reduce compliance requirements, as they are mandated and must be met. Ideally, there needs to be a good balance between the four factors.

The more servers that can be sampled, the better the overall confidence of the results.

If the scope is large, the overall audit time must be increased or the security controls will need to be reduced. If the scope is small and the sample is relatively small, the security controls can be increased to cover more areas of the Windows environment.

The end result of these four factors is the audit program. The audit program will consist of a list of reports needed for each server. Ideally, the audit program will include details such as:

- Tools being used to gather report
- Specifics regarding tools, such as command line example, location on server, menus and options to be selected, etc.
- Servers for which the tool should be run
- Report file format (.doc, .xls, .txt, etc)
- Report file name

Analysis and Audit Report

The analysis of the reports that an IT Administrator obtains will need to be evaluated based on many criteria. The criteria used for analysis could vary drastically from company to company.

The criteria could differ due to the fact that each company is willing to accept different levels of risk for each of the security controls that is being evaluated. In order to perform the analysis, IT administrators will need to obtain the following documentation:

+ Notes taken from interview with administrator
+ Company documentation regarding security configurations and controls
+ Server build documentation
+ Microsoft industry standards for security controls
+ All reports related to the audit programme

From these documents IT administrators will be able to perform your analysis. The outcome from the analysis will be a list of security controls that do not meet the security baselines and configurations that a company or not for profit organisation has set.

The security controls that are not correct are usually written up in the final report as exceptions. In that final report, each exception should have details regarding the control and what was expected and what was found.

This should be on a computer by computer basis, but in some cases when the exception is so widespread, the report could just indicate that.

Most reports will have a listing of the security control, the issue that was found, background information describing the security control, and suggested resolution.

Concerns with Standard Auditing of AD

Most Active Directory audits follow the same procedures and processes, so the majority of auditors are subject to the similar circumstances no matter what environment they are dealing with.

With this similarity in procedures and processes, most auditors have a ready made list of issues that concern them. Most of the issues and concerns are not warranted, but some are justified.

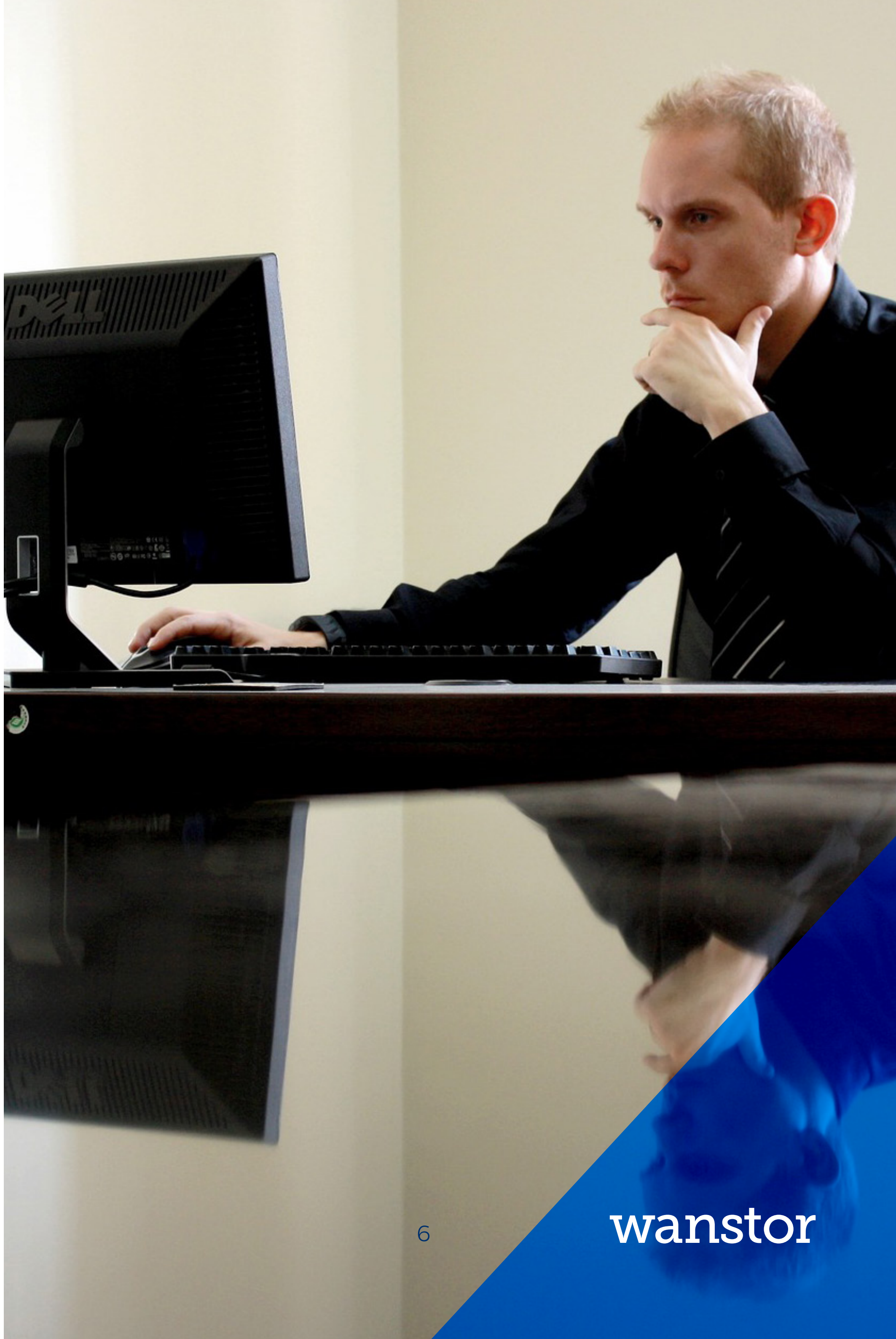
Security Controls Being Altered for Report Only

This concern is usually not justified, but there are malicious IT administrators who would do something like this. There is little that can be done in order to overcome this issue.

Even if you "observe" the administrator generating the report, there is no certainty that the change was made before you started your observation. The only true way to verify that this is not occurring is to perform continuous auditing on the controls to make sure that no changes have been made over time.

Text Documents are Not Reliable

This is a valid worry, but the premise is not valid. The premise is that, compared to a screen capture, a text file can "easily" be changed. This is wildly incorrect. Screen captures can just as easily be changed. If you are only receiving screen captures, your time to analyse information can be nearly doubled compared to obtaining text files, which can be searched.



Reports Are Incorrect

Auditors often are concerned that the information that they are provided is not correct. The concern could be that the administrator changed the information before generating the report (addressed above) or that the information provided is not the correct information.

For example, in less than 5% of reports do auditors gather the incorrect information regarding the domain users' password policy. Not obtaining the correct information is a complete waste of time. Making sure the information that is received is correct and accurate is essential. It is essential that the reports that are being generated and provided are giving you the correct information.

Changes Made Between Audits are Not Captured

A standard audit is a point in time only. This means that changes made before the report is run or after the report is run are not captured.

In reality, changes can be made many times between audits, and the security controls for these changes would never be captured.

This leaves the company and entire network at risk for attack.

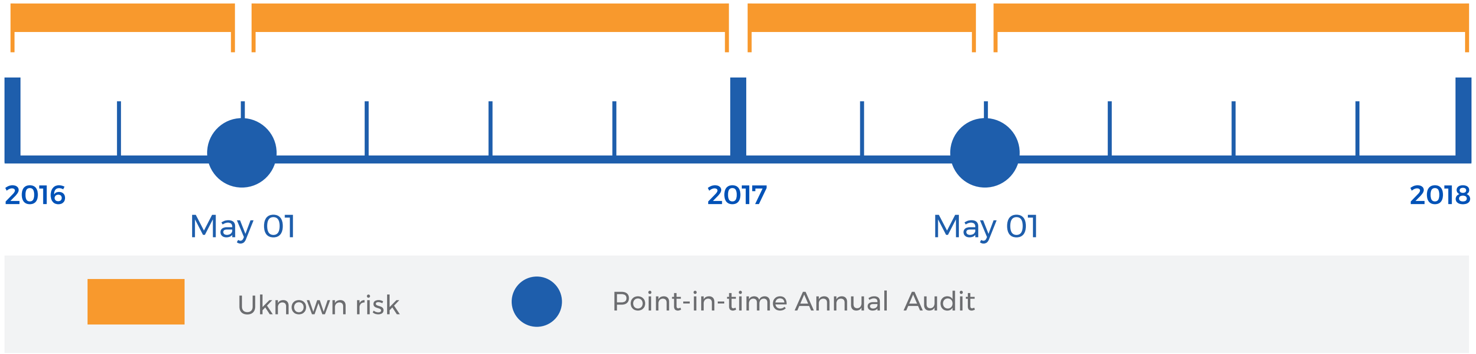


figure 1: Point in time audit to timeline

Continuous Auditing

As a solution to the shortcomings of point-in-time audits, the auditing community came up with the concept of continuous auditing. This concept is great in theory, but the typical implementation is not.

Often, continuous auditing is accomplished by using existing, point-in-time tools that are simply run more often or scheduled to run periodically. The end result is close to continuous auditing, as multiple reports are run for the same security controls. Figure 2 illustrates typically continuous auditing on a timeline. However, the disparate results must be manually compared to the other reports to determine if there are any changes from one report to the other.

There are quite a few tools that can be used to generate periodic or schedule reports. These tools are typically free or very inexpensive, including:

Active Directory Users and Computers: Saved Queries, Dumpsec (both GUI and command line options), Powershell (basic PowerShell and the Active Directory Module for PowerShell), PowerGUI (A Dell/Quest tool based on their ActiveRoles Management Shell for Active Directory), Scheduled tasks (built into every Windows computer)

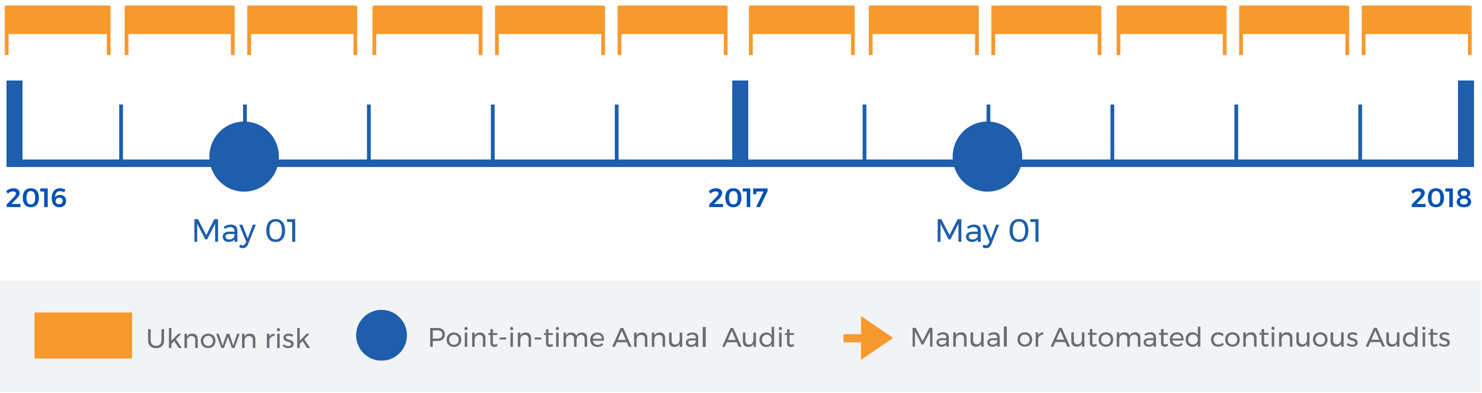

2016
May 01
2017
May 01
2018
Uknown risk
Point-in-time Annual Audit
Manual or Automated continuous Audits

figure 2: Continuous auditing on a timeline

True Continuous Auditing

As you can see from the standard auditing and continuous auditing approaches, there are too many chances for changes to occur to Active Directory without those changes being tracked, reported, or analysed. This lack of reporting for changes that occur between audits and reports being generated exposes the environment to potentially high and devastating risks.

In reality, any *"point-in-time"* audit, whether standard or generated periodically, is only as good as that point in time. Point-in-time reports fail to generate constant changes that might occur to security controls. In an ideal continuous auditing world, point-in-time audits would be replaced with constant tracking and reporting on security controls.

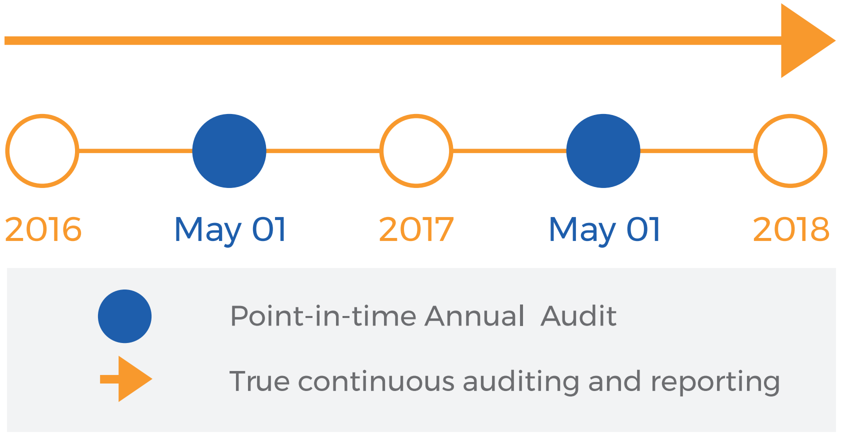

2016
May 01
2017
May 01
2018
● Point-in-time Annual Audit
➔ True continuous auditing and reporting

figure 3: Continuous auditing on a timeline

The features of such a solution would include:

- Every change made in Active Directory would be tracked
- Reports would clearly indicate if and when security controls were changed, including details regarding date, time, user making modification, modifications made, etc.
- Read only access would be granted, so auditors could generate reports at will
- Customized reports could be created to monitor and report on specific users, computers, and groups
- Alerts could be generated when key security controls change

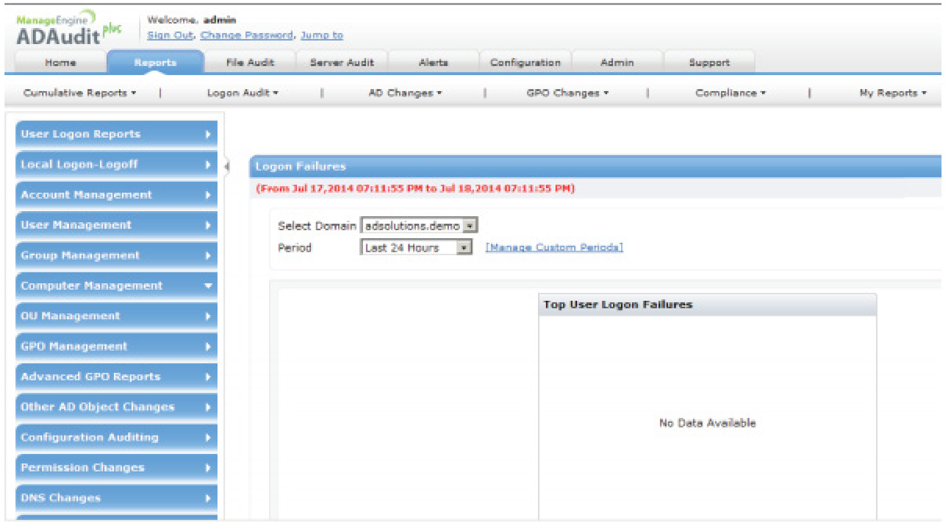
ADAudit Plus

True continuous auditing has not been obtainable until now. ManageEngine ADAudit Plus is the tool that makes true continuous auditing a reality. ADAudit Plus is powerful, comprehensive, easy to use, developed with reporting in mind, and completely integrated with alerting for key security controls

Every Change to Active Directory Tracked

Every Windows domain controller provides extremely verbose auditing of every change that occurs to every object in Active Directory. ADAudit Plus looks at these logs and captures the information in a database before the Windows log is overwritten.

The captured information is then organised for quick and efficient reporting. ADAudit Plus provides over 125 reports. The reports give IT administrators insight into changes to users, groups, organisational units, group policy, and more.



Logon Failures

(From Jul 17,2014 07:11:55 PM to Jul 18,2014 07:11:55 PM)

Select Domain: adsolutions.demo

Period: Last 24 Hours

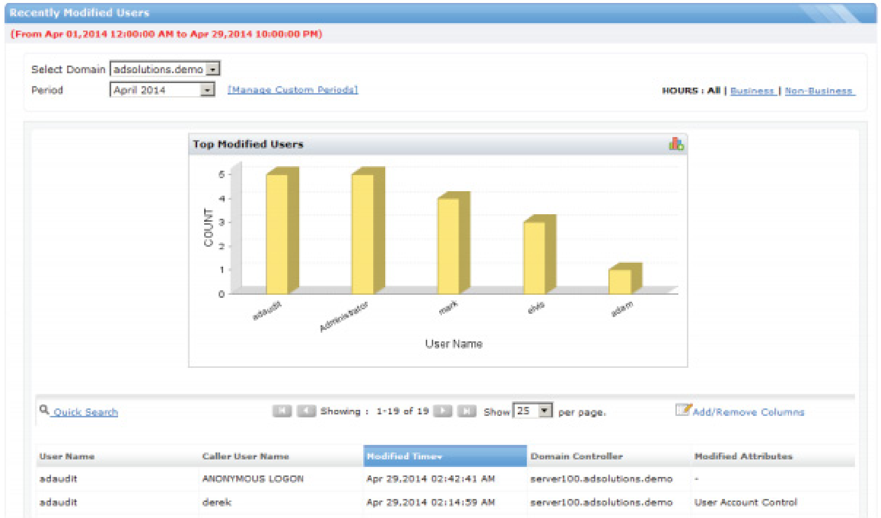
Top User Logon Failures

No Data Available

figure 4: ADAudit provides over 125 default reports

Reports Are Lengthy

Each report provides detailed information that can be used to determine exactly what was changed in Active Directory. Depending on the report, information will be provided as to who made the change, when the change was made, what change was made, as well as the old and new configurations where applicable. Figure 5 shows you a sample of such a report.



Recently Modified Users

(From Apr 01,2014 12:00:00 AM to Apr 29,2014 10:00:00 PM)

Select Domain: adsolutions.demo

Period: April 2014

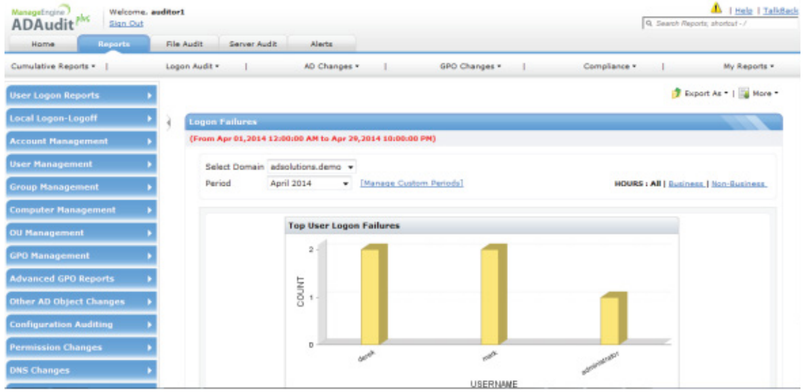
User Name	Caller User Name	Modified Time	Domain Controller	Modified Attributes
adaudit	ANONYMOUS LOGON	Apr 29,2014 02:42:41 AM	server100.adsolutions.demo	-
adaudit	derek	Apr 29,2014 02:14:59 AM	server100.adsolutions.demo	User Account Control

figure 5: ADAudit Plus provides verbose reporting to give you insight into what was changed in Active Directory

Read-only Access to All Reports

One of the most important aspects of auditing is the ability to separate the different roles and responsibilities of those involved with the security configuration, reporting, and auditing.

Ideally, these different roles should be controlled through both Windows permissions and the tool being used to generate the true continuous auditing reporting. ADAudit Plus provides this separation with seamless effort. ADAudit Plus does not require any installation for the auditor, only that the auditors user account is granted “Operator” access, which allows for read-only access to every report as seen in Figure 6.



Welcome, auditor1

Logon Failures

(From Apr 01,2014 12:00:00 AM to Apr 29,2014 10:00:00 PM)

Select Domain adsolutions.demo

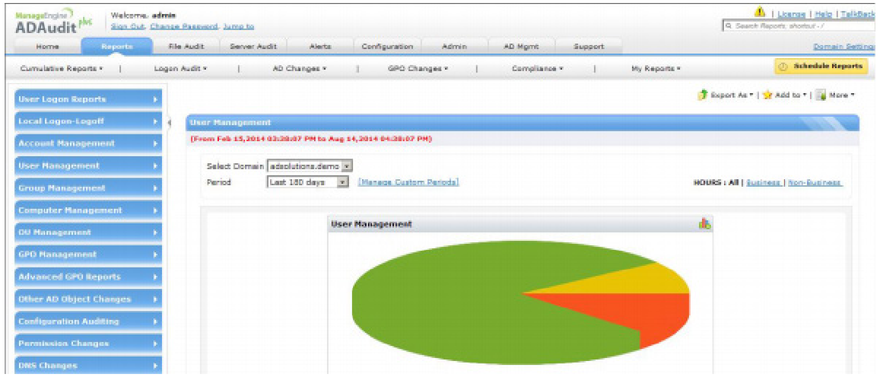
Period April 2014

figure 6: ADAudit Plus provides read-only access to reports

Customised Reports are Easy to Create

Every Active Directory installation has custom users, groups, service accounts, and more. These accounts need to be monitored just like every other built-in user and group. ADAudit Plus provides customization of these custom users and groups, so special reports can be created to report on just what you want to see.

For example, custom groups are created for many applications that are installed. These groups are granted elevated privileges and need to be monitored. Figure 7 shows you what a custom report for custom groups might look like.



User Management

(From Feb 15,2014 03:28:07 PM to Aug 14,2014 04:28:07 PM)

Select Domain: adsolutions.demo

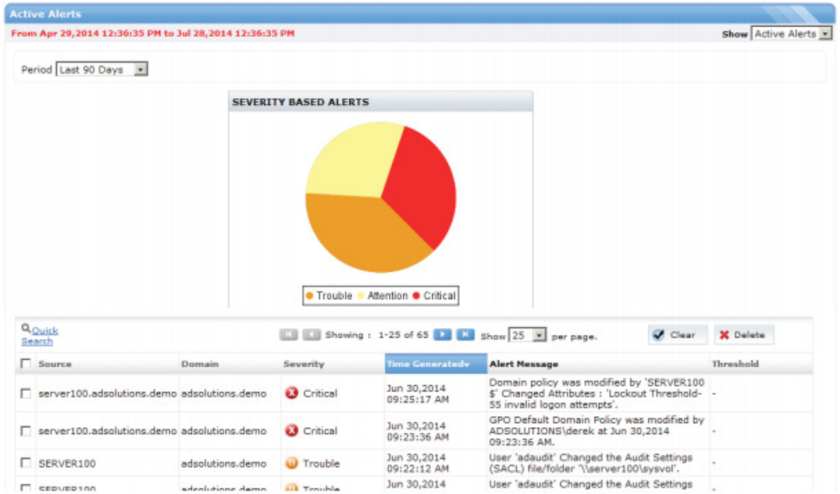
Period: Last 180 days

figure 7: ADAudit Plus provides customization for your Active Directory enterprise of users and groups.

Alerts are Easy to Create

The key to true continuous auditing is not only the ability to track every change made to Active Directory and make it reportable but also to have an immediate alert generated when a key security control is changed.

Alerts can be created to match every built-in and custom report, with the outcome being an event being generated, the ADAudit Plus interface indicating the alert, and an email being sent to your inbox. Figure 8 shows you how the alerts look in the interface.



Active Alerts

From Apr 29,2014 12:36:35 PM to Jul 28,2014 12:36:35 PM

Show: Active Alerts

Period: Last 90 Days

Show: 25 per page.

□	Source	Domain	Severity	Time Generated	Alert Message	Threshold
□	server100.adsolutions.demo	adsolutions.demo	Critical	Jun 30,2014 09:25:17 AM	Domain policy was modified by 'SERVER100 $' Changed Attributes : 'Lockout Threshold-55 invalid logon attempts'.	-
□	server100.adsolutions.demo	adsolutions.demo	Critical	Jun 30,2014 09:23:36 AM	GPO Default Domain Policy was modified by ADSOLUTIONS\derek at Jun 30,2014 09:23:36 AM.	-
□	SERVER100	adsolutions.demo	Trouble	Jun 30,2014 09:22:12 AM	User 'adaudit' Changed the Audit Settings (SACL) file/folder '\\server100\sysvol'.	-
□	SERVER100	adsolutions.demo	Trouble	Jun 30,2014	User 'adaudit' Changed the Audit Settings	-

figure 8: Alerts give you insight into changes made in real time to Active Directory

Standard auditing is outdated, inefficient, and insufficient to provide enough information needed to truly audit and secure your Active Directory enterprise.

ADAudit Plus from ManageEngine provides a true continuous auditing solution that is revolutionary, efficient, and complete.

Reports are plentiful, insightful, and comprehensive; and they can be set for read-only mode. Custom reports can give IT Administartors insight into specific Active Directory installation. Alerts can be created to immediately IT Admins of key security control changes that occur.

In summary, ADAudit Plus is an IT security and compliance solution designed for Windows-based organisations. It provides in-depth knowledge about changes effected to both the content and configuration of Active Directory and servers.

Additionally, it provides thorough access intelligence for desktops and file access in servers (including NetApp filers), enabling you to protect organisational data.

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

ManageEngine
ADAudit Plus

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.

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.

File Server

Securely track File Server / FailOver Cluster for document changes to files (file creation /modification / deletion) and folders audit-access, shares and permissions.

File Integrity

Securely track File Server / FailOver Cluster for document changes to files (file creation /modification / deletion) and folders audit access, shares and permissions.

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.

Databases

Audit your Windows Server Environment from a choice of database formats: SQL Server, PostgreSQL and MySQL.

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.

Compliance

Get specific 'set of detailed graphical reports' for SOX, HIPAA, GLBA, PCI and FISMA to easily meet each compliance requirements.

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.

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.

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.

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.

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.

Other AD objects

Keep a track on other significant AD Objects: Containers, Contacts, Schema, Configuration, Site, DNS & Permission 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.

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. O365 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

TORTILLA
Real California Burritos & Tacos
KUMON
DogsTrust
wagamama
Hestia
Mental Health UK
YO!
LOUNGES
D&D LONDON
Joseph Joseph®
october
COSMO
LCP INSIGHT CLARITY ADVICE
P euro car parks
TEENAGE CANCER TRUST
Children with Cancer UK
Keeping families together
WEXAS
TRAVEL MANAGEMENT

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.