Overcoming Active Directory Administration Challenges

White Paper

wanstor

Contents

Introduction

Active Directory's role in business and not-for-profit organisations has been elevated over the last five years.

The main reason why the role of Active Directory has become more prominent is because business and not-for-profit organisations have had increased pressure from the 'C-Level' within their organisation around the need to secure data it stores and to which it offers users access.

The lack of natural control measures makes the secure administration of Active Directory a challenging task for IT administrators.

As a result, business and not-for-profit organisations need help in creating repeatable, enforceable processes that will ultimately reduce administrative overhead, whilst helping to increase the availability and security of their systems.

Active Directory's Central Role in Business and Not-for-Profit Organisations

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.

Deployment of and reliance upon Active Directory is becoming more prevalent as it is seen as the central data store for sensitive user data and critical business information.

In summary, Active Directory can provide organisations with a consolidated, integrated and distributed directory service. It also enables the business to better manage user and administrative access to business applications and services.

In the past five years, Wanstor's IT Administration experts have seen Active Directory's role in business expand considerably. This is mainly because the need to secure data it stores and enables access to; has seen a considerable increase in interest, with new compliance regulations meaning that what was once just the preserve of IT is now on the 'C-Level' radar.

Unfortunately, native Active Directory administration tools provide little control over user and administrative permissions or access, meaning the secure administration of Active Directory is a challenging task for IT administrators.

The database also has a limited ability to report on activities performed, which means meeting audit requirements and securing Active Directory difficult. Many organisations require the creation of repeatable, enforceable processes that will reduce administrative overhead whilst helping to increase system availability and security.

At Wanstor, we believe Active Directory to be an essential part of the IT infrastructure mix. IT Administrators must both give thought to the application and be diligent in managing, controlling, securing and auditing it.With such a complex application there are challenges to address and resolve in reducing risk whilst deriving maximum value for IT teams.

In this paper, Wanstor's Active Directory experts explore some of the most challenging administrative tasks that IT teams currrently face.

Compliance Auditing & Reporting

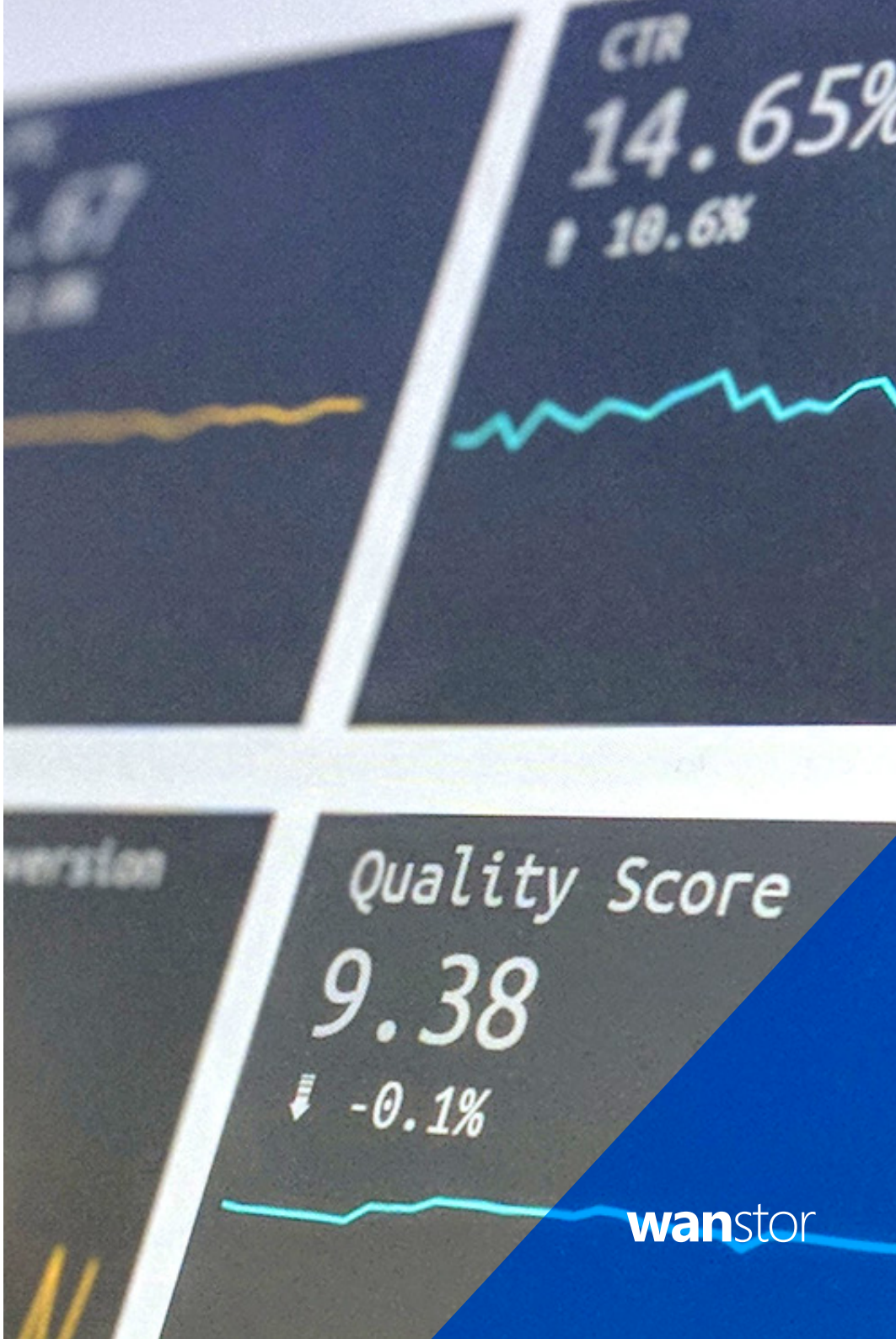
It is now taken as the norm that today's business and not-for-profit landscape is more heavily regulated than ever before, with new legislation released regularly with which organisations are obliged to comply - PCI–DSS, Sarbanes-Oxley and GDPR to name but a few.

Achieving, demonstrating and maintaining compliance is a serious, ever changing challenge for IT teams. To satisfy audit requirements, business and not-for-profit organisations must demonstrate control over the security of sensitive and business-critical data.

However, without the right additional tools, demonstrating regulatory compliance with Active Directory is time-consuming, monotonous and complex.

Auditors and stakeholders require detailed information about user activities and, in particular, the activities of users with enhanced privileges.

This level of granular information allows interested parties to understand in greater detail where problems may originate, also providing information necessary to improving the performance and availability of Active Directory.



Auditing and reporting on Active Directory has always been challenging. Before the release of Windows Server 2008, there were no granular reporting capabilities.

There is now limited reporting on some of the details auditors require available in Windows Server 2008.

While this limited information is a step in the right direction, it is not robust enough to meet most auditing requirements or to support business change or decision making.

In pursuit of compliance, business and not-for-profit organisations should seek out solutions that provide robust reporting and auditing capabilities.

In Wanstor's opinion, Active Directory reporting should provide information on what, when and where changes happen, and on who made said changes.

Reporting capabilities should be flexible enough to provide information for business stakeholders, while also providing in-depth details necessary for IT administrators to improve Active Directory deployment.

The solution deployed should also securely store audit events for as long as is necessary in meeting data retention regulations, enabling people from across the organisation easy access via search for relevant events.

wanstor

Group Policy Management

It is well known that Microsoft recommends Group Policy as the foundation of Active Directory security. By leveraging the capabilities of Group Policy, IT teams can manage and configure user and asset settings, applications and operating systems from one central console. The Group Policy function in Active Directory should be viewed as an indispensable resource for managing user access, permissions and security settings in the Windows environment.

Maintaining a large number of Group Policy Objects or GPOs, which store policy settings, can be a tough task for IT administrators. For example, in large IT environments with many system administrators, care must be taken when making changes to GPOs, as the wrong change may affect every computer or user in a domain, in real time.

However, Group Policy lacks true change-management and version-control capabilities. Futher to this, limited built-in controls mean that completing something as simple as deploying a shortcut requires writing a script. Custom scripts are often complex to create and difficult to debug and test. If the script fails or causes disruption to the live environment, there is no way to go back to the last known setting or configuration.

Malicious or unintended changes to Group Policy can also have devastating and permanent effects on an IT environment and a business.

To prevent negative outcomes from Group Policy changes, IT teams often restrict admin privileges to a few highly-skilled IT administrators. This usually results in these staff members becoming overburdened with administering Group Policy rather than supporting the greater goals of the business.

To leverage the capabilities of Group Policy, it is necessary to have a solution in place that provides a secure offline repository to model and predict the impact of Group Policy changes before they go live.

The ability to plan, control and detect errors in Group Policy changes (along with an approved change and release-management process) enables IT teams to improve security and compliance around Windows environments without making administrative errors.

IT teams should also employ a solution for managing Group Policy, enabling easy and flexible reporting to demonstrate that they have met audit requirements.

User Provisioning, Re-Provisioning and De-Provisioning

The majority of employees require access to several systems and applications. Each application usually has its own account and login information.

Even with today's more advanced processes and systems, employees often find themselves waiting days for access to the systems they need.

Keeping employees waiting to undertake work can seriously cost a business in terms of lost productivity and employee downtime.

To decrease workloads and speed up the provisioning process, many organisations look to Active Directory as the main data store for managing user account information and access rights to both IT resource and assets.

Provisioning, re-provisioning and de-provisioning access via Active Directory is often a manual process.

wanstor

In a large business, maintaining appropriate user permissions and access can be a time-consuming activity, especially when there is significant personnel turnover.

In a large, complex business manual provisioning can take days. There are no automation or policy enforcement capabilities inherent to Active Directory.

With little control in place, there is no way to make sure that users will receive the access they need when they need it. Additionally, there is no system of checks and balances.

Administrative errors may result in elevated user privileges leading to security breaches, malicious activity or other unintended errors

Administrative errors may easily result in elevated user privileges leading to security breaches, malicious activity or unintended errors that can expose the business to significant risk.

Business and not-for-profit organisations should, thus, investigate automated solutions in executing these provisioning activities.

Implementing an automated solution with approval capabilities can significantly reduce the burden on IT administrators, improve adherence to security policies, reinforce standardization, and decreases waiting time for user access.

It can also expedite user access removal, minimizing the ability of those with malicious intent to access sensitive data.

Secure Allocation of User Privilege

Reducing the number of users with executive administrative privileges is a constant challenge for those administering Active Directory.

Many user and helpdesk requests require dealings with Active Directory, but these common interactions often result in elevated access for users who do not need it in their job roles.

Because there are only two levels of administrative access in Active Directory (Domain Administrator or Enterprise Administrator), it is difficult to control what users can access and manipulate once they gain administrative privileges.

Once a user has access to administrative capabilities, they can easily access sensitive business and user information, elevate their privileges further, or even make changes within Active Directory.

Elevated administrative access, especially when granted to someone with malicious intent, dramatically increases the risk of exposure for Active Directory and the applications, users and systems reliant upon it.

At Wanstor, we have found that it is not uncommon for a business or not-for-profit organisation to discover that thousands of users may have unintended elevated administrative privileges. Each of these presents a threat to the security of both IT infrastructure and business.

This, alongside Active Directory's vulnerabilities, means it is very easy for someone to make administrative changes capable of bringing business grinding to a halt. When this occurs, finding and dealing with the issues can become a nightmare for IT teams, as auditing and reporting limitations make it extremely difficult to gather a clear picture of the problem.

To reduce risks associated with elevated user privilege and make sure that users only have access to the information they require, IT teams should investigate solutions that can securely delegate entitlements.

This is a requirement to meet mandates covering separation of duties, as well as a way to share the administrative load by securely delegating privileges to subordinates.

Change Auditing & Monitoring

To achieve and maintain a secure and compliant environment, IT administrators must both control change and monitor for unauthorized changes that may negatively impact upon the business or not-for-profit organisation.

Active Directory change auditing is an important procedure for identifying and limiting errors and unauthorized changes to Active Directory configuration.

One single change can put an entire business or not-for-profit organisation at risk, introducing security breaches and compliance issues.

In Wanstor's experience, built-in Active Directory tools fail to proactively track, audit, report and alert administrators to vital configuration changes.

Additionally, real-time auditing and reporting on configuration changes (including GPOs), day-to-day operational changes and critical group changes does not exist.

wanstor

This exposes the organisation to risk, as the IT Team's ability to limit and repair damage is heavily dependent on their ability to detect and troubleshoot a change once it has occurred.

One scenario may see a bad actor elevate privileges and assign their identity to senior personnel in, for example, HR; this would, in turn, allow access to employee records, granting the aforementioned access to amend personal details - manipulating pay rules or restricting access to business critical software or tools.

Employing a solution encompassing each of these elements will enable IT Administrators to identify unauthorised changes, find their source and resolve issues before these negatively impact upon the business.

To reduce risk and help prevent security breaches, organisations should employ a solution that provides comprehensive change monitoring.

This solution should include:

- ***Real-time change detection***
- ***Intelligent notification***
- ***Human-readable events***
- ***Centralised auditing and detailed reporting***

Preserving Data Integrity

It is important for IT teams to make sure that the data which is stored within Active Directory supports the needs of the organisation, especially as other applications rely on Active Directory for content and information. Data integrity involves both the consistency of data and the completeness of information.

For example, there are multiple ways to enter a phone number:

44.7713.418.3232

07713 418-3232

77134183232

Entering data in inconsistent formats creates data pollution. Data pollution stops the organisation from efficiently organising and accessing important information.

If there are inconsistencies in Active Directory's data, there are currently no ways to make sure that an IT administrator can group all the members of a group together.

Another vital aspect of data integrity when working with Active Directory is the completeness of information.

For example, if an employee is transferred to a new department, the organisation's HR system would use Active Directory to update benefits and payroll information. However, the HR system would not know where to send the employee's pay slip if the IT administrator did not enter the correct postcode.

Active Directory does not provide control over content that is entered manually. If little or no controls are in place, IT administrators can enter information in any format and leave fields that the business relies upon blank.

To support and provide trustworthy information to all aspects of the organisation that rely on Active Directory, IT teams should employ a solution that controls both the format and completeness of data entered into Active Directory.

By putting these controls in place, IT Administrators can significantly reduce data pollution and improve the consistency and completeness of content in Active Directory.

Self-Service Administration

The majority of requests made by the business or by users require access to and administration of Active Directory. Usually an access request involves manual work by nature, and there are few controls in place to prevent administrative errors.

Active Directory's inherent complexity means many of these errors are common and re-occur. You may be thinking '*yes, but if they are common then they should be easy to eradicate, and if they are that common, then what is the actual impact*?'

The answer is that administrative errors in Active Directory mean just one mistake could damage the entire security infrastructure. With the lack of controls, the business or not-for-profit organisation cannot have random users administering Active Directory.

While it may be practical to employ engineers and consultants to install and maintain Active Directory, the reality is many organisations cannot afford to have their highly-skilled and valuable IT employees spending the majority of their time responding to trivial user requests.

This is where self-service administration and automation are logical solutions when looking to streamline Active Directory operations in pursuit of greater efficiency and improved compliance.

At Wanstor, we believe this is achieved by placing controls around common administrative tasks and enabling the system to perform user requests without tasking highly-skilled administrators.

IT teams should take the time to identify processes that are routine yet hands-on, and consider solutions that provide user self-service and process automation. Doing so reduces the workload on highly-skilled IT administrators and improves compliance with policies, since automation does not allow users to skip steps in the process.

> **Identify processes that are routine yet hands-on and consider solutions that provide user self-service and process automation**

IT Teams should, where possible, identify opportunities for self-service and automation solutions that allow for approval, and provide a comprehensive audit trail of events to help demonstrate policy compliance.

Reasons why you need to invest in Active Directory Management Tools

Active Directory is a mission-critical component of the IT infrastructure. As businesses continue to use its powerful capabilities as a commanding repository, it should be understood that Active Directory is in fact a vital part of enterprise security.

This means IT administrators must be able to control, monitor, administer and protect the information held therein with the same degree of discipline currently applied to other high-profile information, such as credit card data and customer data.

Because the built-in tools within Active Directory do not enable or support the secure and disciplined administration required, many IT teams means they must find solutions that enable its controlled and efficient administration.

These solutions help to ensure that business information located within Active Directory is secure in a format that serves the requirements of the business or not-for-profit organisation.

This paper has explored some of the most challenging aspects of securely administering Active Directory.

Wanstor provides Active Directory management and security solutions that help IT Teams to increase control over AD administration, improving their ability to achieve and maintain compliance.

Additionally, many of the Active Directory solutions we deploy decrease the cost and complexity associated with administering this vital component of IT infrastructure.

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

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

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

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

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

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

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

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.

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

wanstor