

Making Active Directory management more efficient

White Paper

wanstor

Contents

- + AD security is crucial to controlling risk and ensuring compliance
- + Perform regular account analysis
- + Link accounts to employee records
- + Monitor new accounts
- + Automate account maintenance
- + Handle departed users and role changes carefully
- + Understand your dormant accounts
- + Manage and maintain non-human accounts
- + Discover, Manage and Control exceptions
- + Control admin authority
- + Take advantage of workflow technology
- + Maintain a clean and secure Active Directory Application

AD security is crucial to controlling risk and ensuring compliance

Active Directory (AD) is the foundation of identity and access management (IAM) in most business and not for profit organisations today. At Wanstor we believe it should be viewed as the most crucial technology on the network. More and more systems and applications are depending on AD for authentication, policy, entitlements, and configuration management. If AD is secure, everything is secure.

Active Directory security is crucial to controlling risk and making sure of compliance within ever changing data management regulations. However maintaining AD in a clean, organised, and secure manner is still a major challenge for most IT teams.

The main problem area IT teams face with Active Directory is the creation, updating and deletion of user accounts. The management process of user accounts in AD is important for security reasons, but the sheer volume of potential changes can make AD difficult to maintain.

User accounts are probably the most important part to IT security as they are the basis for authentication and access to the network, systems, and applications.



They are difficult to maintain because they need to mirror the status and role of the user of the organisation that they represent during the lifecycle of the user and their user account. When an employee is hired, a user account is created.

As the user's job and assignments change, the AD account's identity information (such as job title, department, and phone number) is updated. The user is then made a member of different groups and hopefully removed from groups as appropriate. Eventually, when the user leaves the organisation, the account should be deleted.

This process may sound simple and straightforward. However the difference between fantasy and reality couldn't be starker. Wanstor's IT administrators have audited 100's of AD implementations over the past 15+ years and have yet to find one without a significant number of user accounts that were outdated, inappropriate, or out of compliance with good security practice and policy.

Problematic user accounts create an IT environment that is more difficult and time-consuming to manage. More importantly, they expose the business or not for profit organisation to security risks and compliance problems.

At the root cause of these problems is the fact that AD is not directly linked into the user account lifecycle events which were described earlier.

This means, organisations rely on end users, managers, and HR staff to recognise these events and inform or initiate requests to IT so that user accounts can be kept up to date.

In this whitepaper Wanstor's Active Directory experts have pooled their knowledge to bring together a set of practical actions IT administrators can take straight away.

These steps will help IT administrators to remediate user account problems in AD and to prevent them from occurring in the future. All the practical help identified in this whitepaper use native AD features and common workflow technology such as Microsoft SharePoint, so no significant requirements will stop the IT team from being able to implement the recommendations.

Perform regular account analysis

The first and probably easiest step to maintaining a clean and secure AD is to regularly review user accounts. If IT administrators take the time to extract and review a list of user accounts and their main properties before an audit, they will quickly find and remediate many points with which auditors take issue.

There shouldn't be any excuses from IT administrators, downloading a list of user accounts is easy. All they have to do is run a Windows PowerShell script and import the results to Microsoft Excel.

Once the script has been run the IT administrator should be able to filter the spreadsheet to find non-compliant accounts. This spreadsheet should then allow IT administrators to quickly filter on various user properties to find non-compliant accounts.

At Wanstor we recommend IT administrators begin by identifying accounts with easy-to-find problems, such as a password that never expires for example. Then include filtering criteria on other columns, such as SAM ID or description, to eliminate service, application, and other accounts that they know will be exceptions.



These are easy problems to fix before any auditor arrives and will reduce the number of risk findings on an audit. An obvious problem to look for is dormant accounts. IT administrators can usually find other problems, as well for example accounts that should never have been created in the first place or that were not provisioned according to naming standards or other account creation controls.

Without knowing or understanding naming conventions, account creation controls, and other standards, it is difficult to provide guidance. But if IT administrators start by filtering out all accounts beginning with specific prefixes to find the remaining questionable accounts that is a good starting point.

Once the obvious non compliant accounts have been deleted or amended, IT administrators may find that some of those remaining accounts might be legitimate exceptions. As mentioned earlier it is always important for IT teams to perform an account analysis prior to an audit.

At Wanstor we recommend IT teams undertake this type of audit every month to stay on top of Active Directory data. The ultimate goal after all is to keep AD secure and organised at all times. Be aware that this step is a detective or reactive control, not a preventive or proactive control. The IT teams goal should be to prevent the problems that have been described earlier in this document around user access and security.



Link accounts to employee records

The easiest way to keep Active Directory accounts clean and secure is to link all accounts to an actual human being or user. This includes non-human accounts such as those created for services and applications. First of all lets discuss accounts that are created for individual persons including end users, contractors, administrators, and others.

Firstly, any account that is assigned to an employee should be tagged in a way as to positively link that account to the employee's master record in the HR system. This link is crucial because employees' access to the network and entitlements within it must be tied to their status and role within the organisation.

The official record of this is the master record in HR, which also has the best chance of being up to date. When an employee's status or role changes, HR and IT teams must be able to find the employee's accounts and change the status or entitlements accordingly. Documenting the employee ID on AD accounts is the key to success as everything can then be managed from this record.

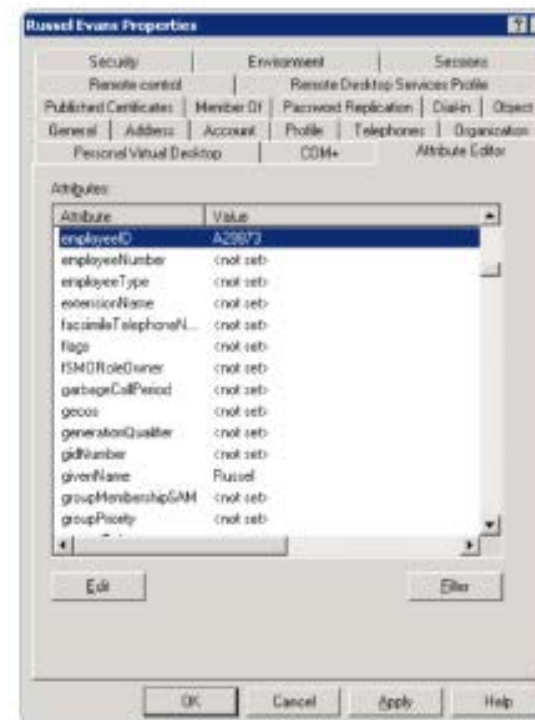


Figure 1 (right): There are many ways to link AD accounts to employee records: (1) Using the Employee ID or Employee Number attribute in AD; (2) Via the Attribute Editor tab, as shown in the figure above; (3) Entering the employee ID in the Description or Notes field; (4) Embedding the employee number in the logon name.

Monitor new accounts

When auditing Active Directory the Wanstor AD experts regularly discover a surprising number accounts that should never have been created or that were created without following the organisation's standards for naming convention or other policies. One of the major reasons this happens is because too many people in the IT department have authority to create accounts.

Successful intruders, both human and automated, often create backdoor accounts to make sure they have continued access and to hide their activity.

Flame, a recent weaponized malware, specifically attempted to create such an account whenever it discovered that it was running under the authority of a domain admin.

This means tracking down new accounts is crucial; but it is also seen as time-consuming and often inconclusive by many IT teams. At Wanstor we believe the best time to track down source of a new but non-compliant account is when it's first created as IT can:

- + Identity who created the account.
- + The account creator is still at your company.
- + The creator remembers why the account was created.



There are two ways to review and respond to new accounts:

- + Monitor AD domain controller security logs for event ID 4720 (you need to enable the User Account Management audit subcategory).
- + Run the Output-ADUsersAsCSV script and sort on the When Created column.

As the IT administrator reviews each account, they should be asking the following questions:

- + Is there a work ticket or other corroborating documentation for this account?
- + Does the account match established naming conventions?
- + Does the account comply with our organisation's other account-creation standards and policies?

If the account is unauthorized or non-compliant, the IT administrator will need to follow up with whoever created it. The advantage with using the first method is that the security log event 4720 tells the IT administrator who created the account.

Event ID 4720 - A user account was created

Subject:

Security ID: ACME-FR\administrator

Account Name: administrator

Account Domain: ACME-FR

Logon ID: 0x20f9d

New Account:

Security ID: ACME-FR\John.Locke

Account Name: John.Locke

Account Domain: ACME-FR

Attributes:

SAM Account Name: John.Locke

Display Name: John.Locke

User Principal Name: John.Locke@acme-fr.local

Figure 2: Account log – Administrator view in Active Directory

Automate account maintenance

To help make sure that new accounts are created according to company/organisational standards, automate as much as possible of the account creation process. This will help to eliminate the potential for human error.

Creating a new account in AD should include the following steps:

- + Create the account in AD
- + Set identity attributes (job title, phone numbers, and so on)
- + Create the account's mailbox in Microsoft Exchange
- + Make the account a member of groups that are appropriate to the user's role
- + Register the AD account in other applications, as necessary
- + Automate the process with PowerShell scripts

Many of these steps can be automated through PowerShell scripts.

The following script performs steps one through four:

```
New-ADUser - Name "barrywilkinson" - SamAccountName  
barrywilkinson - AccountExpirationDate 01/01/2014 -  
GivenName "Barry" -Surname "Wilkinson"
```

```
-DisplayName "BarryWilkinson" - Path  
'CN=Users,DC=acme,DC=local' -EmployeeID "21001" -  
OfficePhone "3004" - Title "IT Director"
```

```
Enable - Mailbox - Identity acme\barrywilkinson -  
Database Database01
```

```
Add-ADGroupMember Group1 acme\barrywilkinson
```

```
Add-ADGroupMember Group2 acme\barrywilkinson
```

You can make a customized version of this script for roles in your organisation that have high turnover. Or you can enhance this script to accept input and build the account according to choices made at execution time.

Handle departed users and role changes carefully

Frequently a source of risk associated with Active Directory is user accounts that have not been disabled even though the person is no longer employed by the organisation. It is crucial that HR and/or line managers inform the IT team when employees are terminated or when other relationships (such as a contractor relationship) end.

IT staff responsible for account management also need to know when users change jobs or other roles so that the user's group memberships and other entitlements can be revised and updated as well.

As a general rule looking for dormant accounts does not address this problem. As simple as this might sound, businesses commonly fail to implement a working process to disable user accounts or to change entitlements when a user's status changes.

During IT audit interviews, when asked what the procedure is for disabling departed users, Wanstor's AD experts have observed staff answering that they regularly check for dormant user accounts and disable accounts that have not logged on recently. This is not an effective control for risks associated with live profiles once a user has left an organisation. If someone is still accessing the network after being terminated, their account will never show up as being dormant and will never be disabled.

The following are three ways that some IT teams fulfil this vital requirement, beginning with the easiest:

- + Most organisations have a clearly defined and strictly executed process for removing a user's physical access to the building; make account disabling part of this process.
- + If your HR application includes workflow, configure it to automatically send an email to account administrators when a user is terminated or when a user's job title or manager changes.
- + Most HR applications allow the automatic scheduling of report delivery; schedule a daily report of terminations and job changes to be delivered to account admins.

In summary, to comply with any regulation framework, IT teams must disable accounts and adjust entitlements whenever a user's status changes. Whichever process is selected, management should understand its importance and responsibility should be clearly defined.

Understand your dormant accounts

Given the difficulty that most organisations face with reliably disabling accounts of departed users, the next step in keeping Active Directory clean and secure is to regularly check for dormant accounts (i.e., user accounts that have not recently logged on).

Please note this is a separate piece of advice and should be used in conjunction with the advice we have given in the previous section of this document about the process to be followed when a user leaves.

The reason why many accounts were left “dormant” was because finding dormant accounts used to be hard for IT administrators. For example in Windows 2000, it was difficult to find a dormant user because the account’s last logon date and time was not replicated between domain controllers.

Therefore it was necessary, for each account, to query each domain controller for the last logon date and time on record for the account. The most recent date and time was then used to determine when the user had last authenticated.



However since Windows 2003 has been introduced, Microsoft have added a new last Logon Timestamp to Active Directory user accounts and this attribute is replicated every 7 days. This replication makes sure IT administrators can query any domain controller and get last logon times that are recent enough to identify dormant users.

The LastLogonTimestamp is exposed by Get-ADUser with the LastLogonDate property, With the appropriate CSV script, IT administrators simply need to sort on the Last Logon column in descending order to easily identify accounts that have not recently logged on.

IT Admins should also check for user accounts that have never logged on; these accounts are indicated by rows in which the Last Logon column is blank.

Manage and maintain non-human accounts

Not all accounts directly correspond to a person. For example, many applications require one or more accounts for services to log on. These accounts often have privileged access to servers and data and need to be secured. Generally highly privileged accounts are at risk. However, application and other non-human accounts are difficult to track. In IT audits, Wanstor's AD experts regularly find highly privileged accounts that are at risk for the following reasons:

- + No one is sure about the account's purpose or why it should continue to exist
- + The account password has not been changed, despite the departure of many administrators, for fear of breaking an application somewhere on the network
- + The account has authority to log on interactively. Note - Non-human accounts should be prohibited from logging on interactively at the console or via Remote Desktop to prevent administrators (who know the account's password) from logging on as that account to perform actions that can't be tied to their identity.

The first step in managing non-human accounts is to identify all of these accounts. IT administrators can do this by using a prefix in the

Logon Type	Logon Rights
Interactive	Allow log on locally Deny log on locally
Remote Desktop	Allow log on through Remote Desktop Services Deny log on through Remote Desktop Services
Service	Log on as a service Deny log on as a service
Scheduled Task	Log on as a service Deny log on as a service
Network (e.g. shared folder access)	Log on as a batch job Deny log on as a batch job
FIPS 140-2 RDP Transport encryption	Access this computer from the network Deny log on through Remote Desktop Services

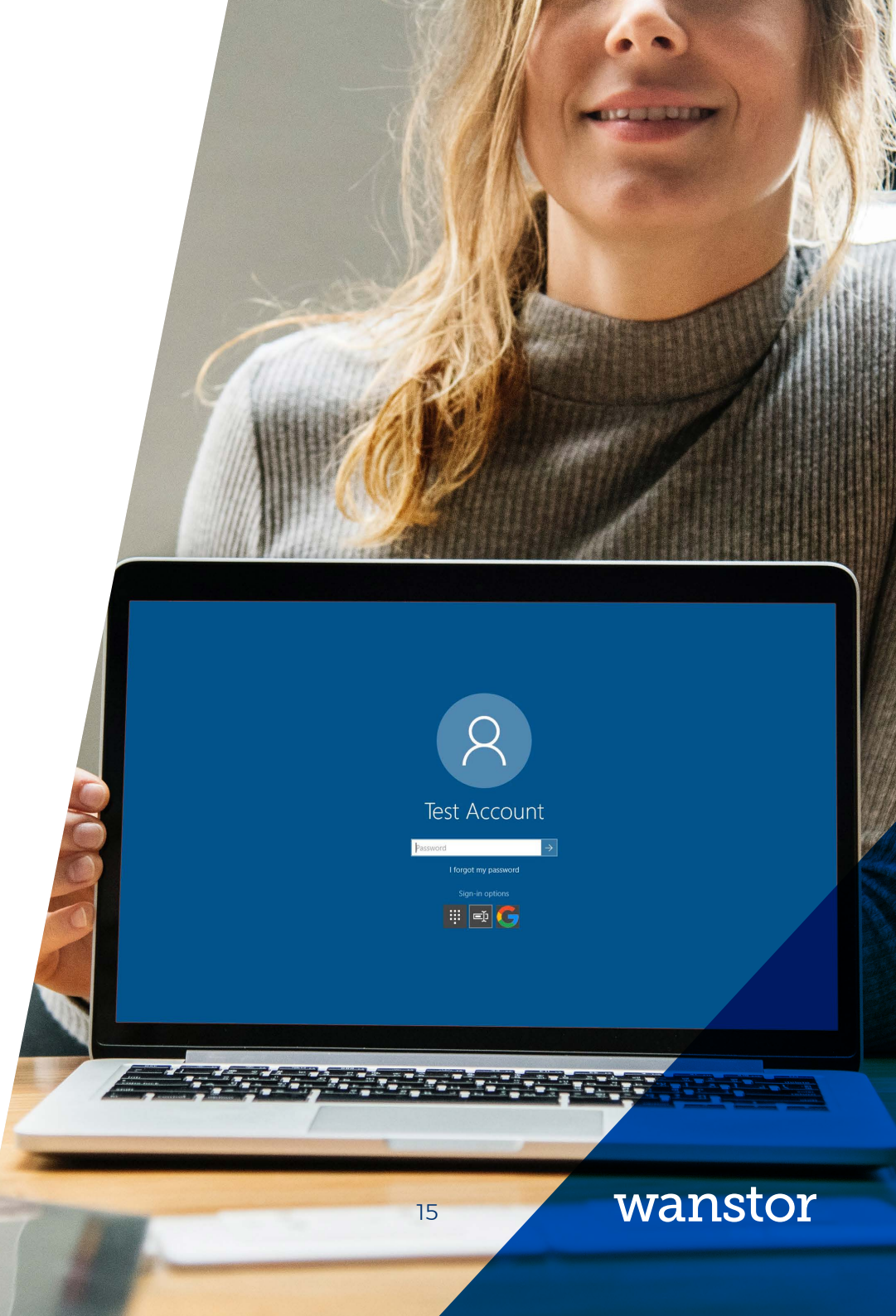
naming convention of the logon name, putting the accounts in a specific Non-Human Accounts organizational unit (OU), or tagging them as such via some other attribute in AD.

The next step should be to define the purpose of the account and the systems on which it is used should be documented in the Description or Notes fields of the account. An owner should be designated for each non-human account and the information needs to be documented in Active Directory. The owner can be an individual human user account, but it is usually better to select a group that corresponds to the team that is responsible for the application or other technology that uses the account. The owner can also be documented in the Description or Notes field.

Password maintenance

At Wanstor we understand that one of the most difficult risks associated with non-human accounts is password maintenance. The password of a non-human account needs to be changed whenever an administrator (who knows the password) leaves the business or not for profit organisation. Unless accounts are documented correctly, determining to which non-human accounts a given administrator had access is difficult.

But changing an account password means risk: any services, scheduled tasks running as that account, or applications that store that account's password must be updated or they will break the next time they start or attempt to log on.



Define which systems an account is being used on

If an IT administrator is attempting to clean up an existing set of non-human accounts, they can determine which systems an account is being used on by consulting the Windows security log.

Assuming that you have enabled the Service Ticket Operations audit subcategory in your Default Domain Controller Policy Group Policy Object (GPO), your domain controllers will log event ID 4769 whenever a user account requests a service ticket to any system in the domain.

By searching domain controller security logs for all occurrences of 4769 where Account Name is the service account in question, IT administrators can obtain a list of all computers on which that account is being used; look at the Service Name field in those events. The Service Name field in event ID 4769 identifies the computer for which the user account is requesting authentication.

Limit the logon rights of non-human accounts

One final step for securing non-human accounts is to limit their logon rights on computers throughout the domain. This helps to prevent non-human accounts from being accessed or abused by someone logging on with the account interactively at a computer's console or via Remote Desktop. This step also serves as a defence in case password changes are missed when an administrator leaves.

Logon types in Windows have both allow and deny rights

To log on in a given way, you must have the corresponding allow logon right. Even then, if you have also been assigned the deny logon right, you will not be allowed to log on; the deny logon right overrides the allow right. You can find these rights in a GPO under Computer Settings\Windows Settings\Security Settings\Local Policies\User Right Assignments.

Usually, non-human accounts should have only the “Log on as a service” right. It would be advisable to explicitly deny Interactive and Remote Desktop logon rights to prevent the account from being misused.

If IT administrators add all non-human accounts to a specific group for that purpose, they can then assign that group the “Deny log on locally” and “Deny log on through Remote Desktop Services” rights in a GPO such as Default Domain Policy, which is applied to all domain computers.

Be careful about denying the Network logon right. The application using the account might need to access resources on other networks.

Discover, Manage & Control exceptions

Quite often you will hear people in IT saying that “rules are made to be broken.” There are definitely legitimate exceptions to every rule and in this case standards for user accounts. For instance, you might have an application that requires a user account with a specific name that violates normal naming conventions.

For situations like this IT administrators need a way to document legitimate, approved exceptions. The best way is with an OU named Exceptions or by flagging exception accounts as such in the Description or Notes fields. But simply labelling an account as an exception is not enough; the account’s purpose and owner should be documented.

At Wanstor, we always advise IT administrators that exceptions to many rule should be just that and they should not become commonplace.



A word of caution

At Wanstor, we have witnessed AD implementations in which a large percentage of accounts were exceptions.

Staff had simply moved into the habit of flagging an account as an exception whenever it was inconvenient to follow account maintenance standards and procedures.

The provision for exceptions should not be abused.

Control admin authority

First of all: Limit the number of people who can create accounts

Earlier in this document we highlighted one reason Active Directory tends to become littered with unneeded or mystery accounts is because organisations frequently give too many people authority to create user accounts.

To enforce new account creation controls that are crucial for security and compliance, IT administrators must limit the number of people who can create accounts to just a few people who are trained and responsible for new-account policy compliance.

Active Directory supports least privilege by allowing domain admins to delegate selected permission over specific OUs. When properly implemented, AD's delegation of control ability allows people to do their jobs without giving them more authority than needed.

For example, rather than making the help desk members of Domain Admins, the IT administrator may grant the Help Desk group the Reset password permission on the OU that contains your end-user accounts. To begin the Delegation of Control Wizard, simply right-click the desired OU and select "Delegate Control." The following figure on the right hand side shows password reset authority being delegated to the Help Desk group.



Take advantage of workflow technology

At Wanstor we find many organisations trying to handle new account requests, job terminations, job changes, and various approvals using only email as their primary tool. This makes it difficult to follow account management standards or to prove compliance.

Workflow technology, such as lists in SharePoint, will never be a full automation option for account management, but it is an improvement over email alone.

SharePoint, as an example of workflow technology, allows IT administrators to give announcement lists an email address that turns incoming emails into new list items and carries any attached documents over to list item attachments. IT Admins can then customise the list with Status fields to track the processing steps of the list item.

Example: Using SharePoint to manage termination-related account changes

IT administrators can use an email-enabled SharePoint list to organise job termination notifications and to document compliance with a departed user procedure.

Simply configure the HR application to send its emails to a SharePoint list, and add Status and Notes columns to the list. As new job termination notifications or reports are delivered to the list, IT Admins can disable the associated accounts in Active Directory and edit the list item to document that it was processed and which accounts were disabled in response.

IT Admins can even subscribe to alerts on the list so they know as soon as an item is created. Similar lists can be created for new account requests and job change notifications.

The point here is that IT administrators need to leverage workflow technology to reduce the clerical and documentation burden while improving compliance standards.

Maintain a clean and secure Active Directory Application

At Wanstor we have found many organisations using “native tools”. In short, native tools alone leave a lot of manual work – and the risk of human error. The recommendations in this document will help IT administrators clean up the user accounts in their Active Directory and prevent problems from being repeated in the future.

However, if IT teams simply follow the recommendations without investing in additional tools, much of the clerical and manual confirmation burden on IT staff will remain, along with the reliance on end users, managers, and HR staff for notification of and information about important user lifecycle events.

Within IT, most organisations spend far too much time creating and terminating user accounts in Active Directory. Native tools are inefficient and time-consuming, and the manual processes that they require can introduce human error that compromises both the security and stability of the environment.

Additionally, many IT organisations have equally inefficient but completely separate processes for creating accounts in their non-Windows systems, adding to administrative overhead and introducing even more security risks.

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	<p>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.</p>	<ul style="list-style-type: none"> + 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	<p>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.</p>	<ul style="list-style-type: none"> + 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	<p>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.</p>	<ul style="list-style-type: none"> + 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	<p>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</p>	<ul style="list-style-type: none"> + 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		
<div> <div>ManageEngine</div> <div>SharePoint Manager Plus</div> </div>	<p>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.</p>	<ul style="list-style-type: none"> + 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
<div> <div>ManageEngine</div> <div>DataSecurity Plus</div> </div>	<p>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.</p>	<ul style="list-style-type: none"> + 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
<div> <div>ManageEngine</div> <div>O365 Manager Plus</div> </div>	<p>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.</p>	<ul style="list-style-type: none"> + 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.