Active Directory: Effective ways to manage the user lifecycle

White Paper

Contents

Introduction

Active Directory is a powerful and popular directory service which nearly all IT teams use.

However even though it is widely used, many IT teams are discovering or have discovered that there are significant gaps between user management features and IT administrators' needs.

The good news is many aspects of user lifecycle management can be addressed by ManageEngine Active Directory tools.

Provisioning, Managing, and De-Provisioning User Accounts Through a Life Cycle

Every business or not for profit organisation has to deal with employee turnover. When a new employee joins or an existing employee leaves, the user accounts for all employees who fit into these two categories must also be managed.

For example when employees are hired, new user accounts must be created, when employees leave their user accounts must be disabled and deleted.

When a single user is hired or leaves the company, (if the company is small) these tasks seem minor and quite simple for the IT team to undertake.

After all how difficult is it to create a new user in Active Directory and/or delete their details? The problems with Active Directory administration comes into play when businesses reach a certain size (usually 250 + employees).

Now, the turnover is not just one employee at a time. It's more like tens or even hundreds of employees at a time.

The management of user accounts must coincide with the management of groups, computers, domain controllers, services, security, applications, files, and everything else that must be managed on a typical corporate network.

> **Managing user accounts through the life of the account can prove to be extremely admin heavy**

However, some Active Directory solutions actually help IT teams as they can manage users from creation, through changes over their employment, to removal when the user account is no longer needed.

Such systems help comfort IT administrators that all user accounts will be correctly managed and the daily tasks of user life cycle management will be addressed.

User Account Life Cycle Overview

All IT administrators are aware of what it takes to take a user account from inception to elimination in Active Directory.

Figure 1 on the right illustrates what is required to manage a user account from the time it is created to the time it must be deleted from the system.

Each stage has many associated parts and details that can get lost in daily activities. This is what makes it vital that IT teams explore Active Directory user administration solutions to help take users from one stage to the next.

> What most IT administrators are not fully aware of is the user account life cycle management procedure as a whole

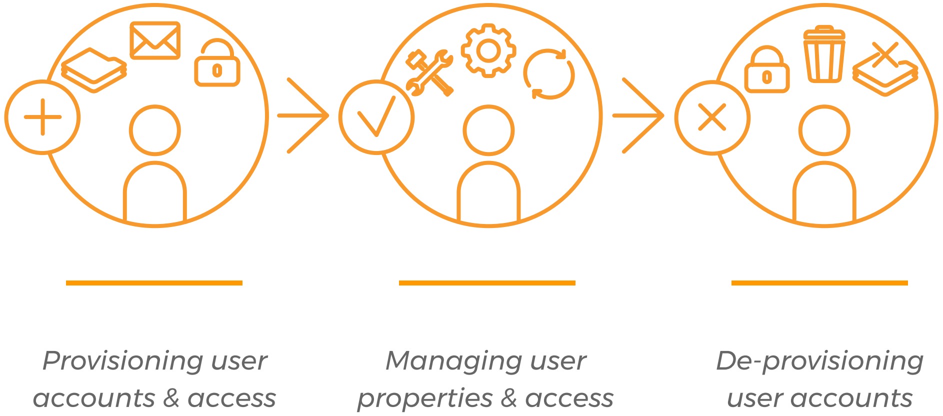

Provisioning user accounts & access
Managing user properties & access
De-provisioning user accounts

figure 1: User account creation to deletion lifecycle

Microsoft Active Directory Solutions for User Life Cycle Management

All IT teams are aware of the tools that Microsoft provides with an Active Directory solution. E.g. Active Directory Users and Computers, Active Directory Domains and Trusts, and tools that manage DNS, DHCP, and other network services.

Microsoft also offers tools that are not 100% Active Directory related, such as System Center and PowerShell, which can be leveraged to help manage the Active Directory environment.

But what about user account management? What does Microsoft provide to IT administrators to manage user accounts from creation through deletion?

Creating User Accounts

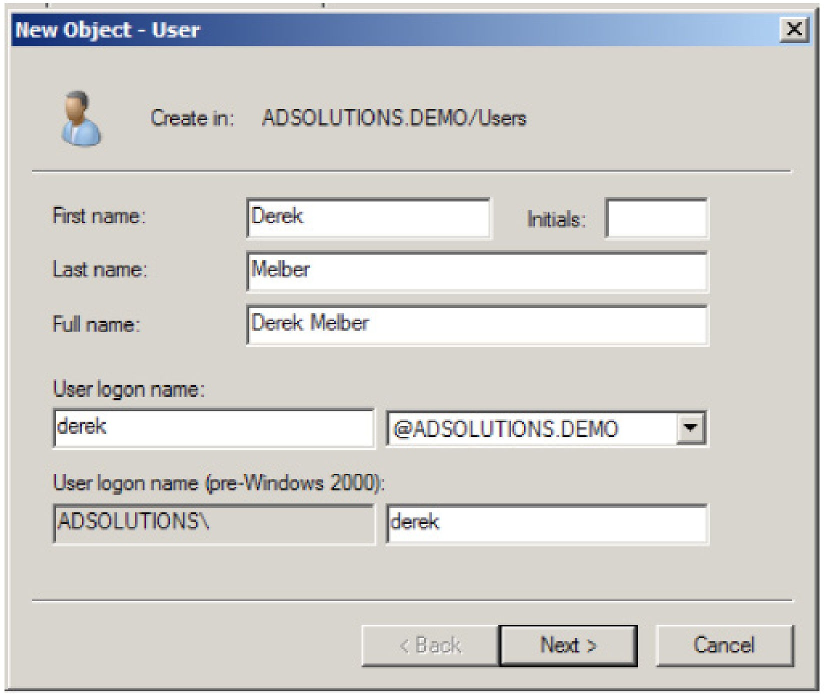
Microsoft provides Active Directory Users and Computers as the main tool for managing user accounts.

The tool is designed to be a single view of a single domain, so IT administrators can see how users are organised within each organisational unit.

When it comes to single user creation, Active Directory Users and Computers gets the job done - but not as quickly and easily as most IT administrators would like.

Due to the structure of the schema and the limitations of the user creation wizard, only a few of the most basic (and necessary) properties can be established during the creation of a user account.

These properties can be seen in figures 2 and 3, which show the options available during the creation of a user account using Active Directory Users and Computers.



Create in: ADSOLUTIONS.DEMO/Users

First name: Derek

Initials:

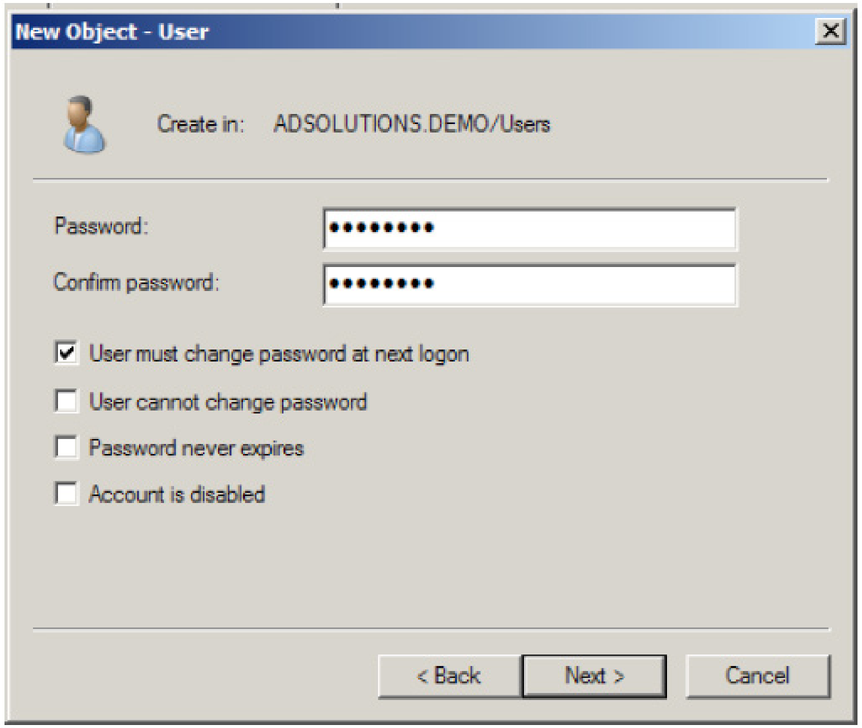
Last name: Melber

Full name: Derek Melber

User logon name: derek @ADSOLUTIONS.DEMO

User logon name (pre-Windows 2000): ADSOLUTIONS\ derek

figure 2 : Basic properties that need to be established while creating a user



Password: ●●●●●●●●

Confirm password: ●●●●●●●●

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

figure 3 : Other properties that need to be established while creating a user

All of the other properties for the user account must be configured "after" the user is created. This might not seem like a limitation, but it is when an IT administrator has to create multiple users. The iterations of creating users and then having to edit each user to configure the properties can be extremely time consuming.

When it comes to creating users in bulk, using Active Directory Users and Computers is simply not an option.

For example if someone from HR hands the IT Administrator an excel file containing the latest batch of new employees. Does Microsoft provide any tools that the IT Administrator can take this list of employees and make user accounts for them?

Technically, the answer is "yes" - but with a number of stipulations and warnings. The longstanding tool, CSVDE, can take a CSV file containing employee names and other properties and create user accounts from it. The caveats? CSVDE offers no GUI, no confirmations of success, and no mechanism to identify failures or explain their cause.

Another tool, PowerShell, can also create users in bulk. This tool has the same limitations as CSVDE. Finally, what does Microsoft provide the IT administrator who wants to create users using a template? In short very little. For a single user, IT administrators can select an existing user account and "copy" it to create another single user account that will have the same group memberships as the copied user account.

When it comes to bulk user creation templates, Microsoft has literally nothing to offer. So in summary Microsoft tools only offer a partial solution that confines IT administrators to creating single users, one at a time. Bulk user creation, using either CSV files or templates, cannot be done efficiently using Microsoft tools.

Managing User Accounts

One of the more complex aspects of user account life cycle management is modifying user account properties to reflect changes in the user's job, role, responsibilities, and access privileges.

Group membership is simple at first viewing level but becomes complex as soon as group nesting, local groups, and access control list inclusion are involved.

Keeping group membership under control is vital to the overall security of Active Directory enterprise and asset management.

Another key user account management issue is making sure the correct location of each user account within the Active Directory structure.

If an account is put in the wrong place in an organisational unit, it could lock down the user and render them unproductive.

Incorrect placement could cause a security risk by giving users access to assets they should not be able to access.Unfortunately, Microsoft provides no tools to help manage user accounts during the life of the account.

When employees' roles, jobs, responsibilities, and access privileges change, Microsoft does not have any tools or processes to help make sure the correct group membership or organisational unit location is correct.

These corrections also include the properties related to a user account, which cannot be managed or altered based on an employee status.

> While a tool like PowerShell or VBScript could be used to perform such tasks, these tools do not come with these features by default.

An IT Administrator would need to customize these tools to perform these management tasks.

Even if successful, IT administrators still wouldn't have a GUI or any reporting associated with the management to inform them of any issues that might arise during the management of the user accounts.

De-provisioning of User Accounts

When an employee leaves the company, a good security practice is to immediately delete the user account associated with the employee.

This is often completed by disabling the user account and moving the user account to an organisational unit where it is locked down through group policy, which is controlling all of the user accounts in the organisational unit.

> For these scenarios, Microsoft tools do not provide any management of user accounts at this level.

The Microsoft tools are set up towards initial creation, manual management, and manual control of the user account upon the employee’s departure from the company.

What ManageEngine ADManager Plus Provides for User Life Cycle Management

For any IT Administrator who is responsible for managing Active Directory, ADManager Plus provides easy user account management, automated user account management, provisioning, de-provisioning, and user account recovery.

Any tool that goes beyond the Microsoft tools should be extremely easy to use, perform all of the actions in an area that an IT Administrator is addressing, and provide an immediate return to the budget line in terms of employee productivity and security.

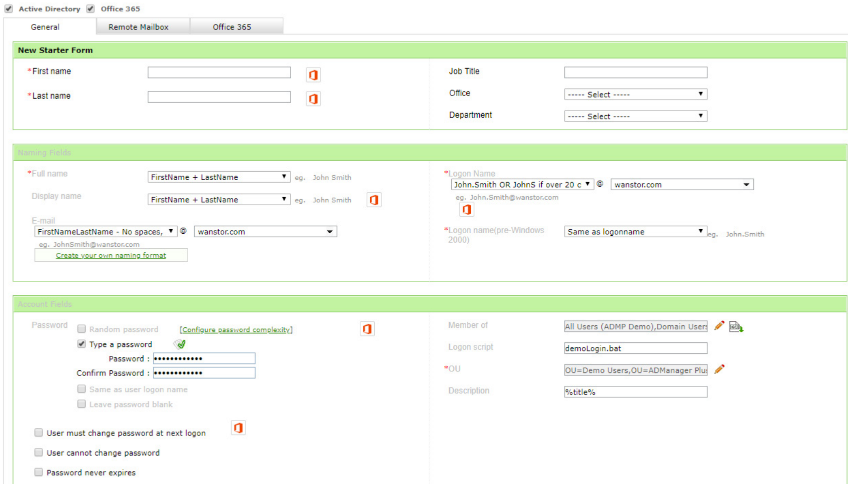
Creating User Accounts

The creation of a single user or even bulk users should be a streamlined, efficient, and an easy process for an IT Adminstrator. ManageEngine's ADManager Plus tool provides a simple-to-use interface for both single user and bulk user account creation.

The Microsoft solution to creating user accounts relies heavily on the Active Directory schematic and the mandatory attributes of the user object. This reliance is a reason why the standard Microsoft solution fails, and one which ADManager Plus avoids.

When creating a single user or bulk users, ADManager Plus gives IT administrators the opportunity to configure all of the user attributes, eliminating the need to iterate back and forth, per user, to configure all of the user properties.

Figure 4 demonstrates the breadth of the user object properties that can be configured at user account creation.



☑ Active Directory ☑ Office 365

New Starter Form

*First name
*Last name
Job Title
Office: ----- Select -----
Department: ----- Select -----

Naming Fields

*Full name: FirstName + LastName eg. John Smith
Display name: FirstName + LastName eg. John Smith
E-mail: FirstNameLastName - No spaces, @ wanstor.com
eg. JohnSmith@wanstor.com
Create your own naming format
*Logon Name: John.Smith OR JohnS if over 20 c @ wanstor.com
eg. John.Smith@wanstor.com
*Logon name(pre-Windows 2000): Same as logonname eg. John.Smith

Account Fields

Password
□ Random password [Configure password complexity]
☑ Type a password
Password : ••••••••••••
Confirm Password : ••••••••••••
□ Same as user logon name
□ Leave password blank
□ User must change password at next logon
□ User cannot change password
□ Password never expires

Member of: All Users (ADMP Demo),Domain Users
Logon script: demoLogin.bat
*OU: OU=Demo Users,OU=ADManager Plus
Description: %title%

figure 4 : All user account properties can be configured during creation

A more complete list of user profile properties that are configurable at user creation include:

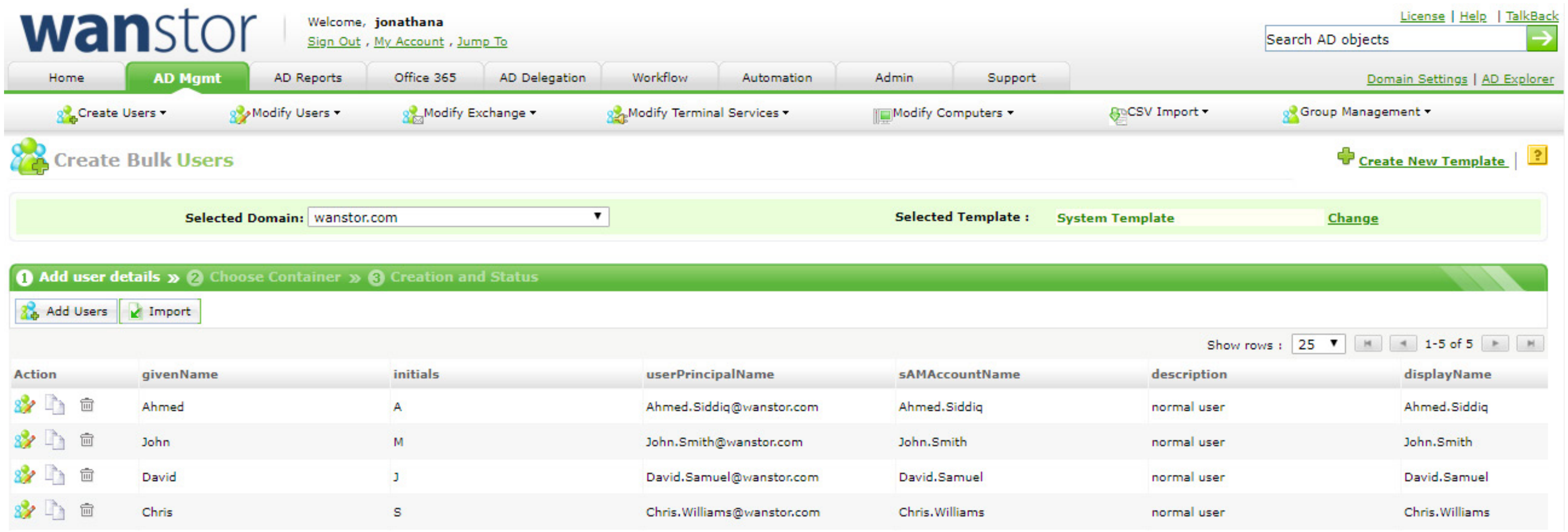
- First name, last name, initials
- Logon names
- Display name
- Employee ID
- Office information
- Logon script
- User profile path
- Delegations
- Group memberships
- Account expirations
- Telephones, addresses, organisation info
- Exchange server details
- Terminal server details
- Custom attributes

If multiple users need to be created, they will often be created through a CSV file provided by another functional business unit.

ADManager Plus consumes CSV files with ease. Before generating the user accounts, ADManager Plus will give an IT administrator a summary of the user accounts that will be created and all of the properties that the CSV file includes.

This information enables a more efficient method of creating user accounts, as there will be fewer errors and failures during the user creation process.

The IT Administator simply has to import the CSV file into ADManager Plus, so you can review the contents before the user accounts are created as shown in Figure 5.



Selected Domain: wanstor.com

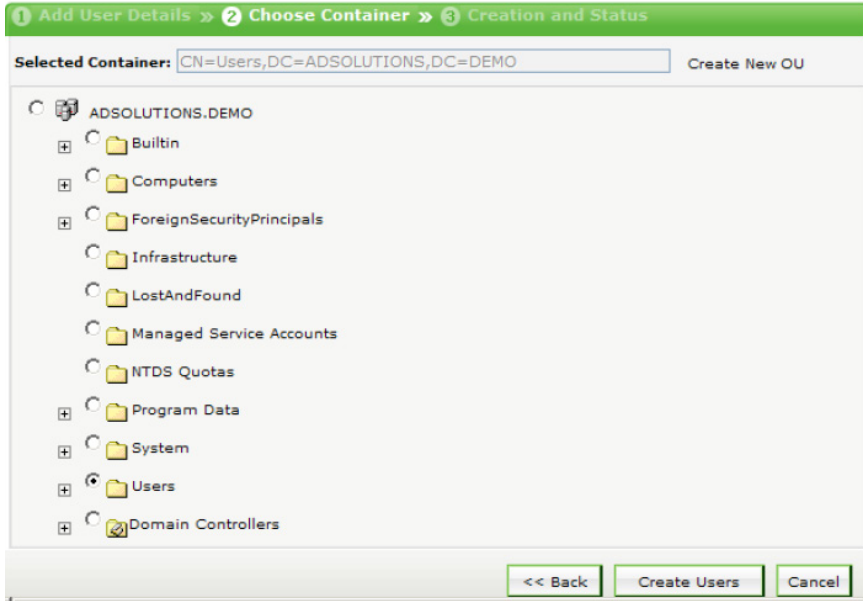
Selected Template : System Template Change

Action	givenName	initials	userPrincipalName	sAMAccountName	description	displayName
	Ahmed	A	Ahmed.Siddiq@wanstor.com	Ahmed.Siddiq	normal user	Ahmed.Siddiq
	John	M	John.Smith@wanstor.com	John.Smith	normal user	John.Smith
	David	J	David.Samuel@wanstor.com	David.Samuel	normal user	David.Samuel
	Chris	S	Chris.Williams@wanstor.com	Chris.Williams	normal user	Chris.Williams

figure 5 : AD Manager Plus - Importing CSV files is easy and gives error reviewing options

Each row contains approximately 20 properties in this example, which can all be seen by scrolling across the table output. This allows for verification before the next step, which is to define which container the user accounts will be created in.

This is a key aspect of the user account creation (single or bulk) as moving objects after creation can be difficult and can cause incorrect configurations if the objects are not located properly.


1 Add User Details » 2 Choose Container » 3 Creation and Status

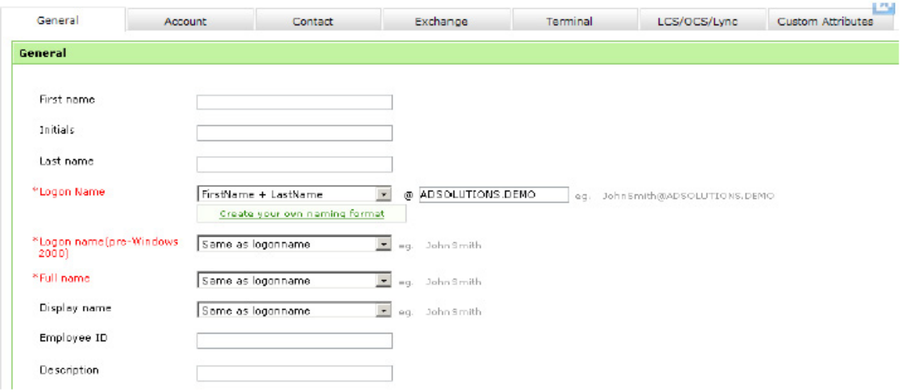
Selected Container: CN=Users,DC=ADSOLUTIONS,DC=DEMO

figure 6 : During user account creation, user accounts are located in the correct AD container

The selection of the container is easy to make as a view of the Active Directory structure is presented, allowing IT administrators to choose the container as you can see in Figure 6.

As identified in the example we have talked through, the creation of bulk user accounts using ADManager Plus is easy and efficient.

If IT administrators were to use the user template option, they could also use wildcards and variables to generate the majority of the user properties, eliminating the need to have those fields in the CSV file or to fill out in the user creation GUI as seen in Figure 7.



First name

Initials

Last name

*Logon Name: FirstName + LastName @ ADSOLUTIONS.DEMO eg. JohnSmith@ADSOLUTIONS.DEMO

Create your own naming format

*Logon name(pre-Windows 2000): Same as logonname eg. JohnSmith

*Full name: Same as logonname eg. JohnSmith

Display name: Same as logonname eg. JohnSmith

Employee ID

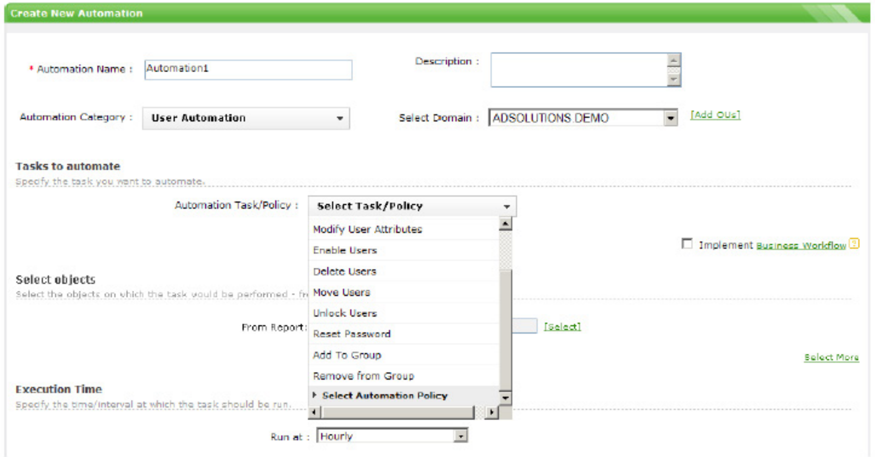
Description

figure 7 : Templates allow for variables and wildcards for quick and efficient user account creation

Managing User Accounts

Often, a user will move from one stage to another in their career. For example, an intern becomes a full-time employee, a full-time employee becomes a contractor, a student advances from 1st grade to 2nd grade, and many other scenarios.

In these situations, the user account must be modified to meet new employee responsibilities, access demands, and other environment requirements. Without some reminder or existing workflow process, the IT Administrator will need to remember to perform these actions on the date of the change to the employee.


Create New Automation

* Automation Name : Automation1

Description :

Automation Category : User Automation

Select Domain : ADSOLUTIONS.DEMO

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy : Select Task/Policy

Select objects

Select the objects on which the task would be performed - fr

From Report:

Execution Time

Specify the time/interval at which the task should be run.

Run at : Hourly

figure 8 : Automation policies automatically perform actions to user accounts

This work is usually forgotten as IT administrators are called to help out with other programmes of work at short notice. It means the IT administrator will either forget to perform the action, or if many user accounts are affected, one or more user accounts will not be configured correctly.

Instead of having a human responsible for such configurations, Wanstor believes it is better to have a computer perform the action on the required day.

Building in an automated schedule for how user accounts will be managed is extremely easy to do with ADManager Plus.

As figure 8 demonstrates, IT administrators can create one or more actions that will be performed on the user account as the user account ages and as milestones are hit. Now, they can create an elaborate or simple set of rules that will apply to specific user accounts.

The rules will have a schedule associated with them, which automatically performs the actions, so the IT Administrator is not required to remember to perform the action. This will create a stable, secure, and compliant environment for all user accounts.

De-Provisioning User Accounts

In a similar way to managing a user account when the employee changes roles and responsibilities, user accounts need to be de-provisioned at certain times as well. Generally there are at least two scenarios in which user de-provisioning is viable.

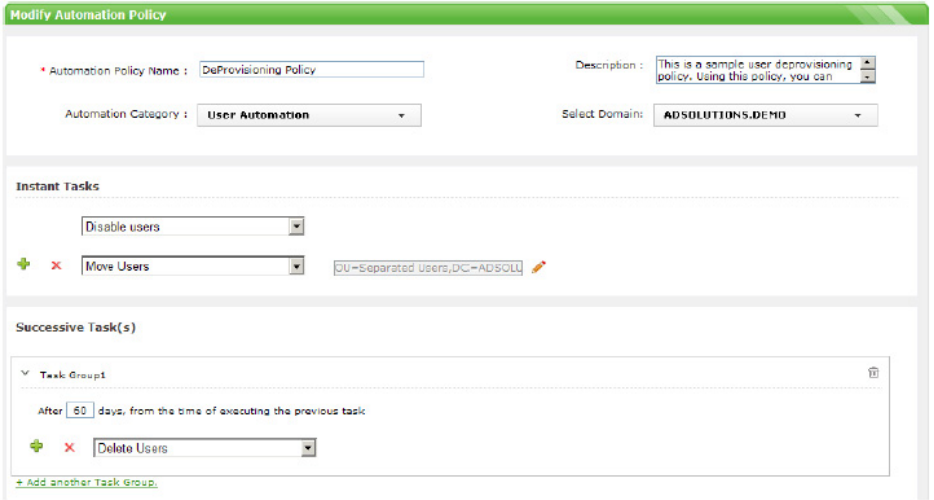
The first is when IT administrators know that a user account needs to be disabled, based on the employee contract or other factors related to the user.

This could be the last step in the automated management of the user account in the section above. Another scenario is when an employee is separated from the organisation and their account is disabled.

Upon disabling the user account, the automated rule could place the user account into a different organisational unit. This would help keep the user account secured and locked down.

Then, another rule in the automation policy could delete the user account after a certain period of time, per the corporate policy.

That automation policy would look like Figure 9 in ADManager Plus. With ADManager Plus, user accounts will no longer be orphaned, left enabled after separation, or retained in the Active Directory after the corporate policy's purge time frame.



Modify Automation Policy

* Automation Policy Name : DeProvisioning Policy

Description : This is a sample user deprovisioning policy. Using this policy, you can

Automation Category : User Automation

Select Domain: ADSOLUTIONS.DEMO

Instant Tasks

Disable users

Move Users OU=Separated Users,DC=ADSOLU

Successive Task(s)

Task Group1

After 60 days, from the time of executing the previous task

Delete Users

figure 9 : De-provisioning of user accounts is automatic to ensure security of the enterprise

User account life cycle management looks like a simple process upon first glance, but the details and requirements for the creation, management, and de-provisioning of user accounts can be complex.

The Microsoft tools in Active Directory are far from complete when it comes to user account life cycle management.

This means IT administrators must perform more actions to complete mundane tasks or develop scripts to manage users as they move through their life cycle.

ADManager Plus from ManageEngine solves those issues quickly, efficiently, and cost effectively. The tool is designed for every aspect of life cycle management for user accounts, as well as for other Active Directory objects.

With its easy-to-use GUI configurations and its reporting and error information, ADManager Plus will make user account management simple in the future.

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

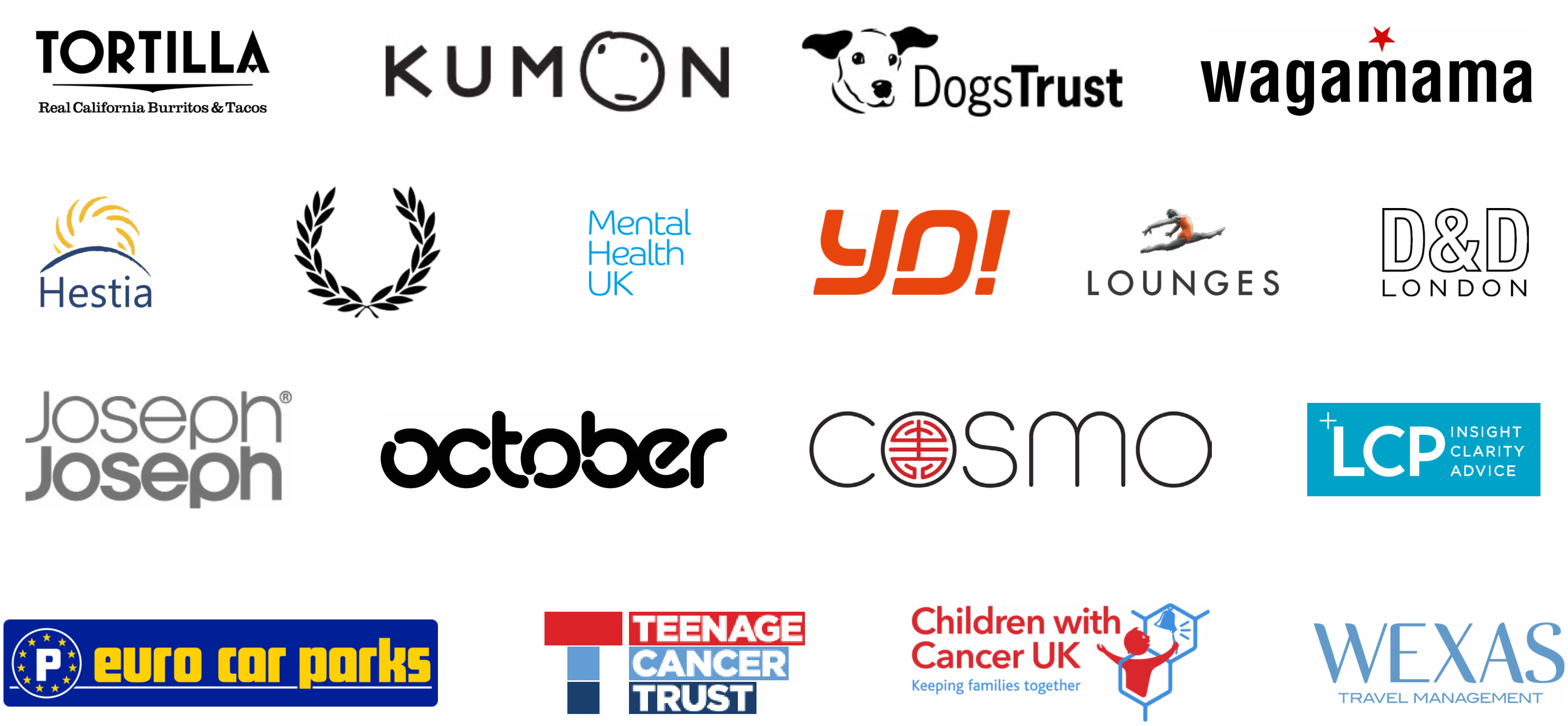
- Manage users from anywhere - reset passwords; unlock, enable, disable and delete accounts
- Report on locked out, disabled, password, expired, inactive users
- View, manage, and execute AD workflow requests

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



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.