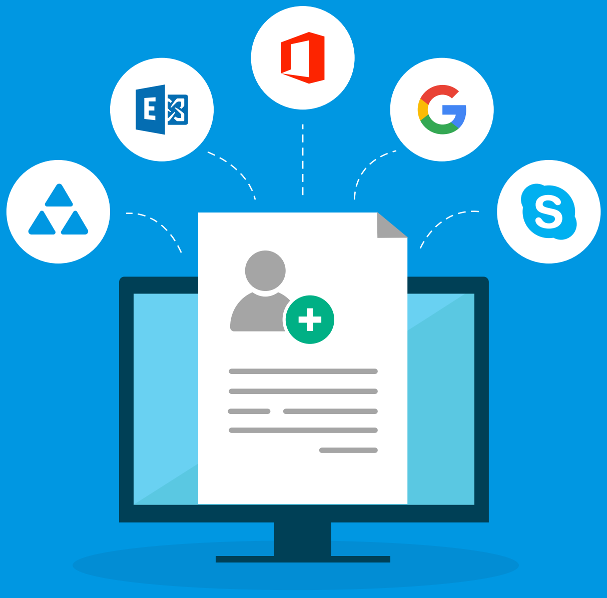
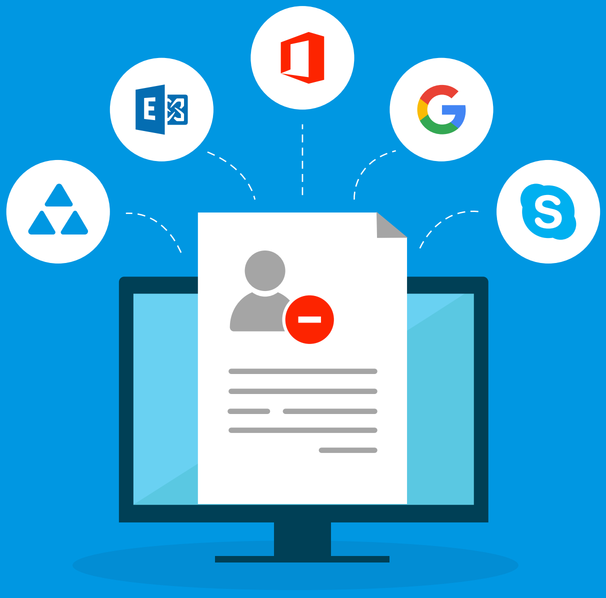
ManageEngine
ADManager Plus

Provisioning and deprovisioning users efficiently in hybrid Active Directory





www.admanagerplus.com

Introduction

For most organizations, the on-premises version of Windows Active Directory (AD) is a core component of their network infrastructure, controlling nearly all access to valuable data. As powerful and popular on-premises AD is, it's not uncommon for organizations to also leverage the cloud to harness new capabilities. The goal of hybrid Active Directory is a well-managed, well-integrated environment that consists of the traditional on-premises AD, as well as the cloud-based Azure AD.

In a hybrid Active Directory environment, you carry out routine, yet crucial tasks related to provisioning and deprovisoning users. However, the limited options of native tools to create AD user accounts, cloud app accounts, mailboxes, etc. for new users creates major challenges in terms of efficiency and security.

In this white paper, we'll take a look at the capabilities of native tools for user provisioning and deprovisioning in hybrid AD and discuss their drawbacks. We'll also look at solutions that can help you implement a better approach for the same tasks while ensuring consistency, security, and efficiency.

Native tools for bulk user account provisioning

In hybrid AD, user provisioning requires setting up user accounts in both on-premises and cloud environments and configuring user attributes, mailboxes, home folders, etc. See Figure 1 below. Active Directory Users and Computers (ADUC), the native tool for managing users' accounts in AD, is limited to single user account creation, with limited options for configuring properties.

Azure AD also offers no capabilities for bulk provisioning users, and while AD Connect helps with syncing user accounts across on-premises AD and Azure AD, the attributes are again limited to those of the native tools. While it's possible to create custom attributes in ADUC, it's impossible to do so in Azure AD.

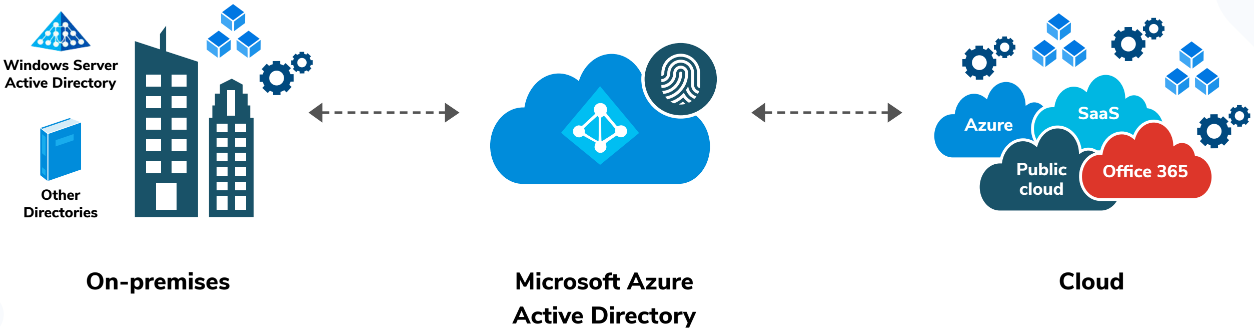


Figure 1. A hybrid AD environment.

Microsoft does provide a solution to create users in bulk, which is PowerShell. Using PowerShell, you can create users in bulk by leveraging a CSV file. This solution also allows you to configure user attributes, generate random passwords, define least privileges, set up user emails, and implement workflows and automations in hybrid AD environments.

While PowerShell can effectively perform the above actions, it requires expertise in scripting, can be complex, and doesn't allow complete automation of user account creation. Additionally, the lack of a GUI, no confirmation of success, and no mechanism to identify failures or explain their cause are common challenges PowerShell users encounter.

Native solutions for bulk user account deprovisioning

Disabling and deleting user accounts, as well as revoking licenses and access to all cloud apps, are tasks that you perform as part of deprovisioning at the end of a user account's life cycle. When employees leave the organization, it's important to secure their user account, but also provide access to their data and email for a short period of time.

Ideally the user account is moved to a secured organizational unit (OU), and the account is disabled until access is required. When it comes to deleting the user account, native tools fail to clean up the associated settings and data. Although the process is simple, it's not uncommon for administrators to forget to perform these actions.

Automation is one way you can easily solve these issues and simplify the process of deprovisioning user accounts. However, it is only through complex PowerShell scripts that you can configure automations in hybrid AD, as native tools in on-premises AD and Azure AD don't offer such capabilities.

Simplifying user provisioning and deprovisioning with the right solution

The ideal solution to overcome the challenges of managing user provisioning and deprovisioning in a hybrid AD environment is to opt for a tool that seamlessly operates between on-premises and cloud environments. This will not only plug security holes but drive consistency and efficiency in any hybrid AD environment. This is where ADManager Plus comes into play.

Bulk user provisioning

ADManager Plus is web-based software that lets you simultaneously create and manage multiple users in AD, Office 365, Exchange, G Suite, and Skype for Business, all from a single console, as seen in Figure 2. This ensures secure and consistent configuration with limited input from CSV files by the use of user creation templates, which play a key role in the automation of user account provisioning. See Figure 3 below.

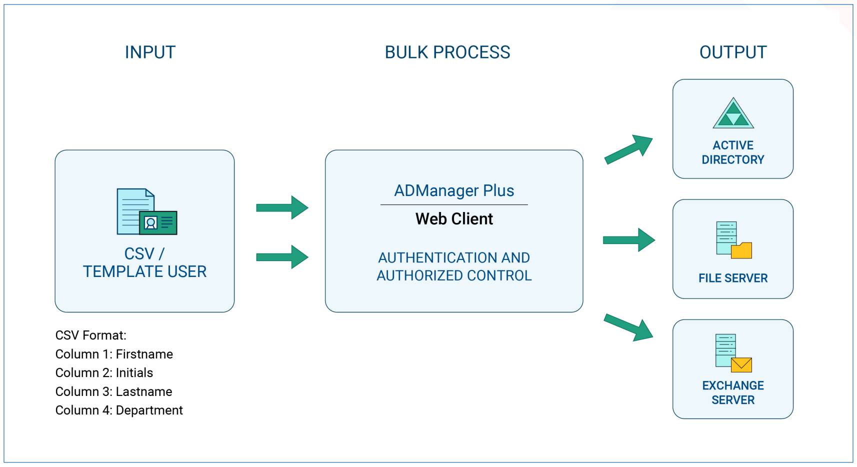
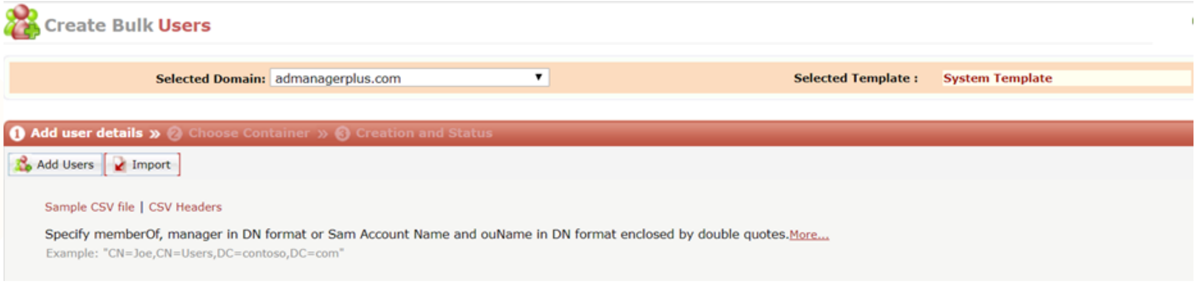


Figure 2. Bulk user creation flow in ADManager Plus.

When you create user accounts in AD using ADManager Plus, you can also create Exchange mailboxes and new user accounts in Office 365, G Suite, and Skype for Business. Aside from making user creation more efficient, automating user provisioning with ADManager Plus offers error-free user onboarding. See Figures 3 and 4. Furthermore, you no longer have to work with complex PowerShell scripts or multi-step processes involving native tools


Create Bulk Users

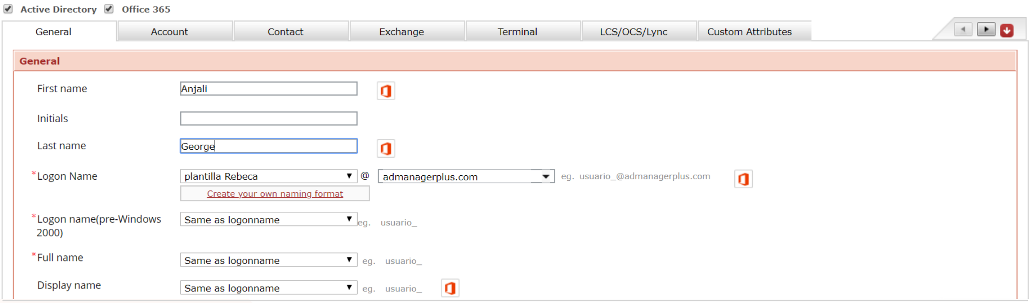
Selected Domain: admanagerplus.com ▼ Selected Template : System Template

1 Add user details » 2 Choose Container » 3 Creation and Status
Add Users
Import

Sample CSV file | CSV Headers

Specify memberOf, manager in DN format or Sam Account Name and ouName in DN format enclosed by double quotes.More...
Example: "CN=Joe,CN=Users,DC=contoso,DC=com"

Figure 3. Bulk user provisioning in ADManager Plus through CSV file import.


☑ Active Directory ☑ Office 365

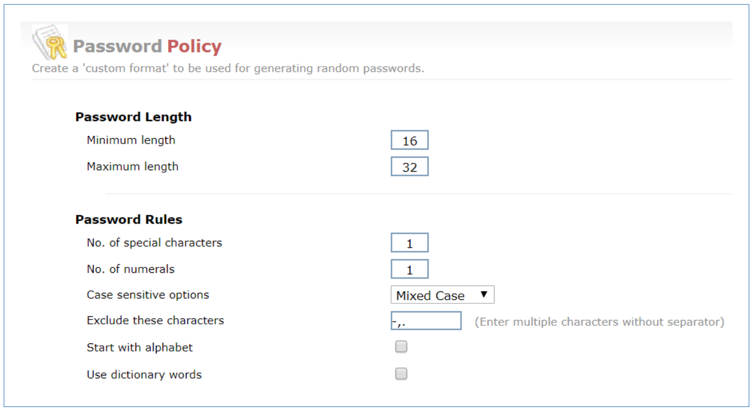
General

First name	Anjali	
Initials		
Last name	George	
*Logon Name	plantilla Rebeca ▼ @ admanagerplus.com ▼ Create your own naming format	eg. usuario_@admanagerplus.com
*Logon name(pre-Windows 2000)	Same as logonname ▼	eg. usuario_
*Full name	Same as logonname ▼	eg. usuario_
Display name	Same as logonname ▼	eg. usuario_

Figure 4. Simultaneous user provisioning in AD and Office 365 using ADManager Plus.

Generating random passwords

Generating random passwords for new users is a crucial task for organizations. This prevents the reuse of the same password for every newly created user account, which leaves these accounts vulnerable to cyberattacks. ADManager Plus' GUI-based features help you generate random, secure passwords that are compliant with your domain's password policy requirements. See Figure 5. Generating random passwords is key to securing existing users accounts that use weak passwords, as well as user accounts that have not been logged into, and retain the initially set password. You can choose to send users these passwords manually or automatically via SMS.



Password Policy

Create a 'custom format' to be used for generating random passwords.

Password Length

Minimum length	16
Maximum length	32

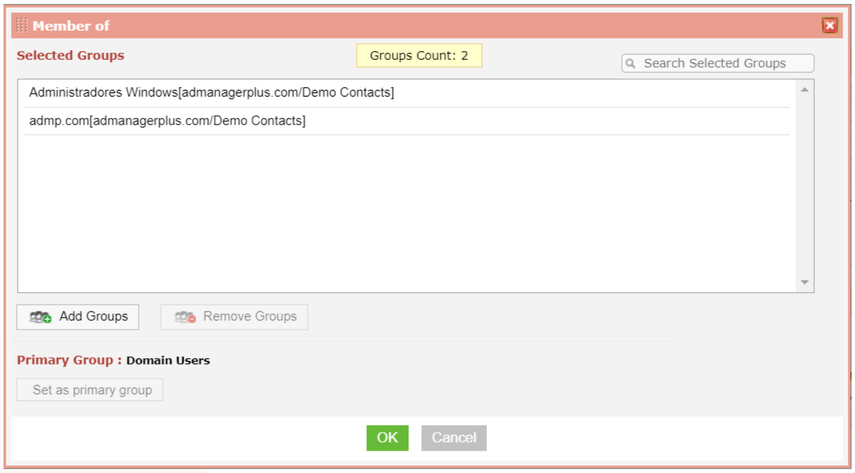
Password Rules

No. of special characters	1
No. of numerals	1
Case sensitive options	Mixed Case ▼
Exclude these characters	-,. (Enter multiple characters without separator)
Start with alphabet	□
Use dictionary words	□

Figure 5. Configuring random passwords for user accounts.

Enforcing the concept of least privilege

ADManager Plus helps you easily employ the principle of least privileges by granting only the minimal amount of privileges that each user needs. See Figure 6.



Member of

Selected Groups — Groups Count: 2

Administradores Windows[admanagerplus.com/Demo Contacts]
admp.com[admanagerplus.com/Demo Contacts]

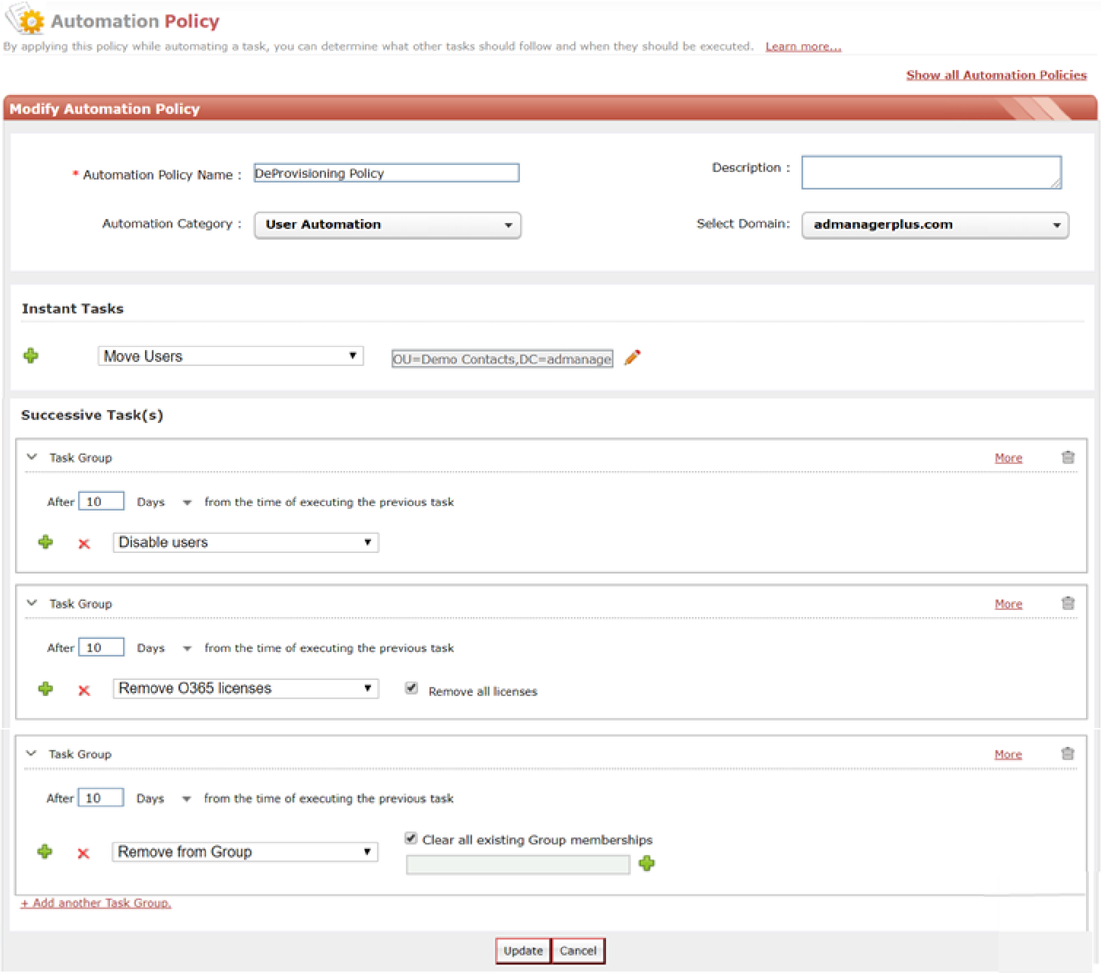
Primary Group : Domain Users

Figure 6. Adding members to groups using ADManager Plus.

Automated user deprovisioning

ADManager Plus can be configured to automatically deprovision user accounts, delete mailboxes, remove licenses, and revoke access to cloud apps all at once when an employee leaves the organization. You can set up a disable/delete policy to automate the identification and clean up of inactive, disabled, and expired user accounts, as well as groups without members.

With the help of customizable templates in ADManager Plus, you can import data from a CSV file, and bulk disable or delete accounts based on the organization's policy. See Figure 7. Not only does this improve the efficiency of user deprovisioning, but also the security posture by preventing unauthorized access to the corporate network by terminated employees and attackers.



Automation Policy

By applying this policy while automating a task, you can determine what other tasks should follow and when they should be executed. Learn more...

Show all Automation Policies

Modify Automation Policy

* Automation Policy Name : DeProvisioning Policy

Description :

Automation Category : User Automation

Select Domain: admanagerplus.com

Instant Tasks

Move Users — OU=Demo Contacts,DC=admanage

Successive Task(s)

Task Group

After 10 Days from the time of executing the previous task

Disable users

Task Group

After 10 Days from the time of executing the previous task

Remove O365 licenses ☑ Remove all licenses

Task Group

After 10 Days from the time of executing the previous task

Remove from Group ☑ Clear all existing Group memberships

Figure 7. Automating user deprovisoning in hybrid AD.

Summary

Considering the details and requirements for the provisioning and deprovisioning of user accounts in hybrid AD environments, user account management can be a complicated affair for IT administrators and organizations alike. Microsoft's native tools are far from complete when it comes to user account life cycle management; in turn, administrators must perform more actions to complete mundane tasks or develop scripts to manage users as they move through their life cycles.

ADManager Plus solves these issues quickly, efficiently, and cost effectively. The tool is designed for every aspect of user account life cycle management, as well as for other Active Directory objects. With its easy-to-use GUI configurations, automations, and comprehensive reporting, ADManager Plus adds value to businesses by streamlining user account management in hybrid Active Directory environments.