ManageEngine
ADManager Plus

# 5 Pain points in AD user account management

www.admanagerplus.com

# Table of contents

# Introduction

Active Directory (AD) is a crucial identity and access management (IAM) component for many enterprises as it enables the creation, maintenance, and use of digital identities.

The strength of your organization's security posture is directly proportional to how secure your AD infrastructure is. Since user accounts act as the basis of authentication and initial access to your network, ensuring that they are managed effectively could go a long way in optimizing the IT operations and securing your AD infrastructure, thereby reducing the risk of security breaches.

From the moment an employee is onboarded until they leave the organization, the IT administrator is responsible for managing the user's account. The administrator has to create an AD user account, modify its properties when required assign sufficient access rights, and hopefully delete the user account when the employee is offboarded.

Although all these activities look fairly uncomplicated, using just the native AD tools to accomplish them is time-consuming and tedious.

Here are five common AD user management pain points IT administrators can overcome using ADManager Plus, a web-based Active Directory (AD) management and reporting solution.

Pain Point - 1

# User account creation

Provisioning user accounts in bulk using native Active Directory (AD) tools or Windows PowerShell scripts have always been irksome and time consuming, as it requires in-depth scripting knowledge. Further, as IT administrators have to often toggle between multiple consoles while provisioning access rights to new employees, there is plenty of room for error.

With the help of CSV-based user provisioning techniques, ADManager Plus simplifies bulk user provisioning for IT administrators. For instance, if the group of employees sharing the same set of permissions are to be onboarded, the IT administrator can create a user template by specifying the required permissions, then create a CSV file with the names of the employees. The IT administrator can simply import the CSV file, and apply the created template to create the users in bulk.

Pain Point - 2

# Account access management

Often, employees' access permissions to resources depends on their job title. Over time, these permissions might vary based on the project they are currently working on.

Due to the overlap of access permissions between different job titles, it becomes challenging for IT administrators to keep track of all the access permissions applicable to every user account. Users might have access permissions to top-level security groups or confidential data, which they don't need, for example. Hence, it is a recommended best practice to employ the principle of least privilege—providing only the bare minimum access required by an employee to do a specific task. To reduce risks further, administrators should be able to assign time-bound access to business-critical data.

ADManager Plus empowers administrators to grant only the minimal amount of privileges required by an employee. Further, using ADManager Plus' automated time-bound group permissions management feature IT admins can assign users to specific groups and revoke remove them automatically after a specified period. In addition to this, with the help of the predefined NTFS reports, you can identify which user accounts have access to your organization's critical folders.

Pain Point - 3

# Password reset for multiple users

Say there have been signs of a few account compromise attempts. The administrator would want to quickly reset all the passwords on their site to avoid unauthorized access of critical resource or data. However, you do not have any option in native AD to reset the passwords of multiple users at once without using complex PowerShell scripts.

With ADManager Plus' built-in password reset feature, you can reset the passwords of multiple user accounts in just a few clicks. You can choose from the available options to reset the passwords. You can generate a random password, type a new password, use the logon name as the password, or leave the password blank, forcing users to change their passwords immediately on their first logon.

To specify the users whose passwords you want to reset, all you have to do is import a CSV file with the required list of users, or you can use the built-in search feature to search for the required list of users.

Pain Point - 4

# Stale accounts cleanup

When employees leave your organization, their user accounts often remain in Active Directory (AD) unnoticed. The passwords of these accounts remain unchanged, which can lead to potential account compromises. It gets worse if one of these accounts belonged to a privileged user.

This is why it's crucial to identify inactive accounts and immediately purge them. However, the only way to ensure all inactive accounts are removed immediately is by automating the process. While native AD has provisions to track down and eliminate inactive user accounts, it can't remove them in bulk or automate the process.

ADManager Plus lets you effortlessly generate a list of all the inactive user accounts, disabled user accounts, and the expired user accounts in the form of reports. Right from these reports, you can delete or disable these accounts in bulk instantly. If required, you can also move them to a separate OU, quarantine them for a desired period of time, and then delete them eventually. Best of all, you can automate these tasks and specify how often you want this automation to run.

Pain Point - 5

# Group membership management

When employees are transferred from one department to another within their organization, the access privileges they had earlier need to be revoked, and their group membership needs to be updated. This forces IT admins to again resort to using complex PowerShell scripts or native AD tools, which aren't very user-friendly. What you need is a GUI-based group membership management solution that lets you effortlessly manage the group membership of your users in bulk.

ADManager Plus helps manage the group membership of users with the help of automation and user modification templates. Using these templates, IT administrators can set up rules to automate the process of updating users' group memberships based on specific conditions. For example, the user will automatically be added to the group "Finance" if the user's title is "Accounts Manager." You can also update or manage the group membership for users in bulk by importing a CSV file containing the list of user accounts to be modified.

ManageEngine
ADManager Plus

ManageEngine
ADManager Plus

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates an exhaustive list of AD reports, some of which are essential requirements to satisfy compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, and G Suite environments, in addition to AD, all from a single console.

For more information about ADManager Plus, visit www.manageengine.com/products/ad-manager/

$ Get Quote

⤓ Download