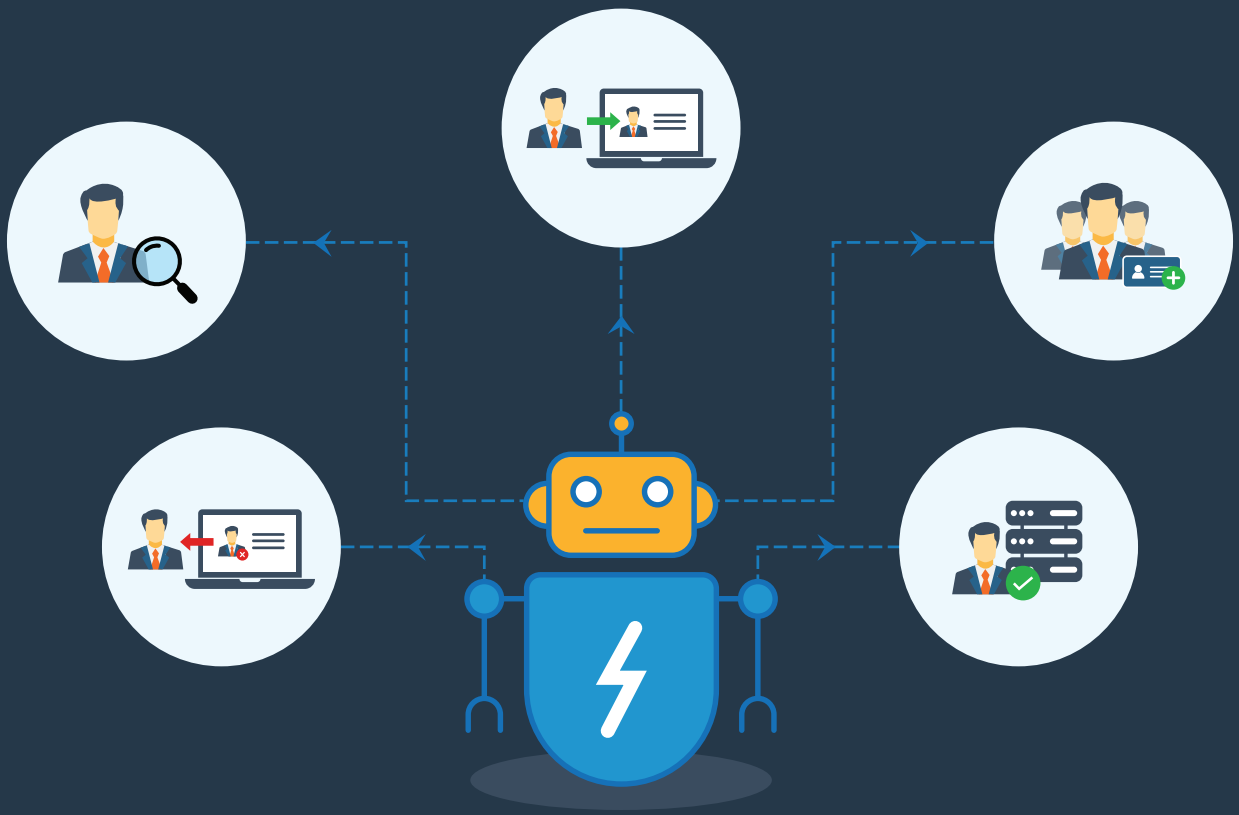
ManageEngine
ADManager Plus

5 reasons why you need to automate IAM process



www.admanagerplus.com

IAM is an essential framework for security and compliance as it defines user identities and privileges within an organization. However, even a simple IAM mistake can cause information security risks for an organization. Owing to the precarious nature of Active Directory (AD), IT technicians and administrators often manually perform painstaking user management actions using native AD tools, PowerShell, and other ineffective methods.

For organizations that grow each day, manually performing these user management tasks becomes cumbersome. On top of that, there are certain crucial AD tasks—such as user provisioning, deprovisioning, and managing Office 365 licenses—where there's no space for error. This guide exposes the most common identity management and access control blunders and discusses how automation is the best solution to prevent these mistakes.

1. High turnaround time during user onboarding.

How does the HR department notify IT administrators when new employees join the organization? In most cases, the HR manager exports the user details in a CSV file from their HRMS application and shares the file with the IT team via email. Creating user accounts in AD and defining access rights for each of them is time-consuming and could potentially lead to data entry errors, which could then lead to granting improper access rights to users. Automating user provisioning will eliminate repetitive onboarding tasks, freeing up plenty of time for IT administrators to deal with other important tasks.

ADManager Plus offers hands-free, bulk user account onboarding in AD, Office 365, Exchange, Skype for Business, and G Suite using customizable rule-based templates. You can also configure ADManager Plus to automatically fetch the latest user details and provision accounts from HRMS databases such as MS SQL, Oracle, and other popular HRMS applications.

2. Delayed response from too many user modification requests.

When the roles or responsibilities of employees change, the administrator has to modify properties of their accounts, add them to relevant groups, or move them to another OU. Administrators have to address group memberships and file server permissions immediately as these determine an employee's access to relevant resources. In addition, administrators are constantly bombarded with password resets, account unlocks, and other help desk requests. Any delay in processing such modification requests will hamper the productivity of the employees and the team. You can perform bulk management actions using native tools—but only via complex PowerShell scripts.

ADManager Plus offers a variety of automated user modification actions, including password resets and redistribution of Office 365 licenses. ADManager Plus also helps you notify relevant users via email or SMS every time a management action is carried out.

3. Buildup of stale accounts.

Orphaned accounts can go unnoticed for a long time, and getting rid of obsolete accounts is a sound security tactic. It's important to remove these accounts from systems as quickly as possible to eliminate potential attacks from aggravated ex-employees and malicious insiders. In a non-automated scenario, when an employee leaves the organization, HR or the employee's former manager notifies the admin to delete the account. However, there can often be a delay in the deprovisioning process, or in some instances, it may never even happen. By automating AD account cleanup, you're effectively closing the door on former employees who may want to access corporate data.

ADManager Plus simplifies account deprovisioning by automatically identifying obsolete accounts, stripping them of their group memberships, moving them to a different OU, and disabling or deleting the accounts based on your organization's policy.

4. Users have excessive rights.

Sometimes administrators grant additional privileges to users to access critical file servers for specific purposes like auditing and forget to revoke these privileges when the purpose is served. Users with excessive rights might have access to classified information, which could be stolen. Setting up a secure environment where trusted users are temporarily granted permissions to access certain files, folders, and groups can be a surefire way to guarantee users only have the required rights.

ADManager Plus redefines privileged access management with automated assignment of users to top-level security groups for a specific period of time. Aside from that, you can use predefined NTFS reports to identify which users are accessing critical resources in your environment.

5. No way to track management actions carried out using PowerShell or ADUC.

Administrators don't have visibility into user management actions carried out using traditional tools, since these tools do not provide the option to preview changes in AD or detect unauthorized modifications. You can improve visibility into AD management actions by implementing workflow in automation.

ADManager Plus offers controlled automation, which ensures that every automated task is reviewed and approved by a manager or an appropriate user before being executed.

ADManager Plus eliminates the risks, hassles, and costs of manually managing the user account life cycle in growing enterprises. Besides user management actions, the tool offers an array of automated prebuilt management actions for AD contacts, computers, and groups. Learn more.