ManageEngine
ADManager Plus

The ultimate guide to
Active Directory
automation

Introduction

Active Directory (AD) is a service that allows organizations to connect users, resources, and data. With it, administrators can easily manage multiple user accounts and devices within the organizational network. AD helps centralize resources and tighten security, and it allows for effective administrative control. Administrators typically perform functions such as user provisioning and de-provisioning, maintaining different user groups in the organization, and keeping an eye out for any suspicious activity, to name a few. Performing these repetitive tasks manually can be tiresome and time-consuming for the IT team. This is where automation comes in!

Why is automation crucial in AD?

An AD administrator's workload typically includes redundant tasks, such as user provisioning, de-provisioning, categorical group maintenance, security administration, and more. Automating repetitive actions can help organizations reduce the time and effort invested in maintaining their AD environment and makes administration more efficient and consistent.

Here are some of the tasks that, when automated, can ensure optimal utilization of resources:

- ⊘ **Employee onboarding and offboarding**
- ⊘ **Password reset**
- ⊘ **Account unlock**
- ⊘ **AD cleanup**
- ⊘ **Report generation for compliance audits**
- ⊘ **Complete AD backup**
- ⊘ **Group membership assignment**
- ⊘ **Folder access management for users**
- ⊘ **User properties modification**
- ⊘ **Password expiration reminders**

Employee onboarding and offboarding
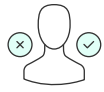
Most organizations are dynamic entities. They deal with employees that are joining and leaving the company, each change eliciting a series of data changes. Your admin team has to add and remove user accounts in addition to managing many other changes. From creating and deleting user accounts to assigning and removing licenses, there are quite a few AD operations to be performed during user provisioning and de-provisioning. Tracking this in an AD environment manually can be an arduous process.

Password reset
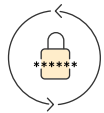
For various reasons, users across the organization might need to reset their passwords, including when they forget the password. Requesting permission to reset the password can be a taxing process for both your employees and the IT team. The time it takes to manually reset user passwords can increase your help desk costs while affecting the productivity of your employees due to due to lost passwords and account lockouts.

Account unlock
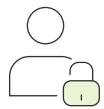
Employees can get locked out of their accounts for multiple reasons, which include entering an incorrect password or reaching a certain number of invalid logon attempts. AD administrators need to make sure they have a secure account lockout policy in place that ensures the organization's security posture while also reducing cyberthreats like brute-force attacks. But it can be difficult to identify users that have been locked out of their accounts using only native tools or PowerShell scripts. And manually unlocking the required user accounts will only add to this arduous process.

AD cleanup

Cleaning up your AD environment is necessary to keep it up-to-date and secure. It is important to keep an eye out for redundant user accounts of employees who have exited the company or changed their work roles. Such accounts pose a danger to the safety of the organization, as they can be used by potential hackers to infiltrate the network. By regularly cleaning your AD, you can avoid such situations. AD cleanup can include a number of tasks, such as removing the inactive or disabled accounts, revoking permissions that are no longer needed, and finding expired AD accounts. Manually performing these tasks can open opportunities for human error.

ManageEngine
ADManager Plus

Report generation

AD management requires you to keep a close eye on all the activities happening in your organizational network. While you can use PowerShell to gain knowledge about your on-premise AD environment, you will end up spending an unnecessary amount of time managing and reporting it on AD.

Complete AD backup

The AD environment is a key component of your organization's Microsoft Windows network. If your AD environment ever crashes, then your entire organization will come to a halt. Maintaining a backup of your AD is imperative for situations in which a domain controller (DC) experiences a failure or in case any other issues arise that could restrict your users from accessing their computers. That's why it is necessary to have a backup and recovery plan in case of any disaster. Manually backing up your AD can take up a lot of time for your IT team.

Group membership management

AD groups can organize users, computers, and even other groups into manageable units for easy administration and network maintenance. They are also used to streamline user and computer management across the organization by grouping them and granting them the required access privileges. By adding a user to a group, the administrator can easily give them access to all the shared resources and directory services associated with that group.

There are many situations where the dynamics of these groups should be changed. For example, when an employee changes departments, they might require new access permissions and will need to be added to a new group. Manually executing this task each time a modification to group memberships is needed can prove to be a time-consuming process for IT administrators.

Folder access management for users
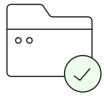
Administrators assign folder access permissions to users based on their roles, group membership, and what they are working on in the organization. The permissions that users require may also change now and then depending on various factors. For example, a user might start working on a special project that requires them to have access to a certain folder for a fixed period of time. Or, a change of roles in the workplace can also elicit a change in the resource access required. Performing this task manually can be a time-consuming process.

User account modification
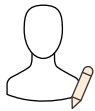
The workload of maintaining a user in your organizational AD environment does not stop with automating the creation of user objects. During their employment, various attributes of their user account can change. They could get a promotion or change departments, leading to a change in the user properties. Manually modifying these properties can be wearisome and exhausting.

Password expiration reminders

Security is of critical importance in any organization. Ensuring that your employees have strong and complex passwords is one of the simplest steps of cybersecurity. Not only do they need to have strong passwords that cannot be easily cracked, but users also need to be reminded of when their passwords are about to expire so that they can be changed effectively. Failure to do so can lead to account lockouts. It can be a taxing task for administrators to send out password expiration reminders manually to the respective users.

Automation using AD

AD does not allow you to automate any tasks except AD backup. Though you can schedule AD backup using the Windows Server Backup application, it is restricted to either full AD backup or volume-wise backup. It does not allow item-level backup and recovery nor does it have a system in place to automate password resets and account lockout for users.

The power of ADManager Plus

ManageEngine ADManager Plus is an enterprise solution for all your identity governance and administration needs. It offers powerful capabilities that can help you manage, administer, and report on your AD environment. With its automation feature, you can ensure efficient and easy AD management for your organization.

How ADManager Plus simplifies automation
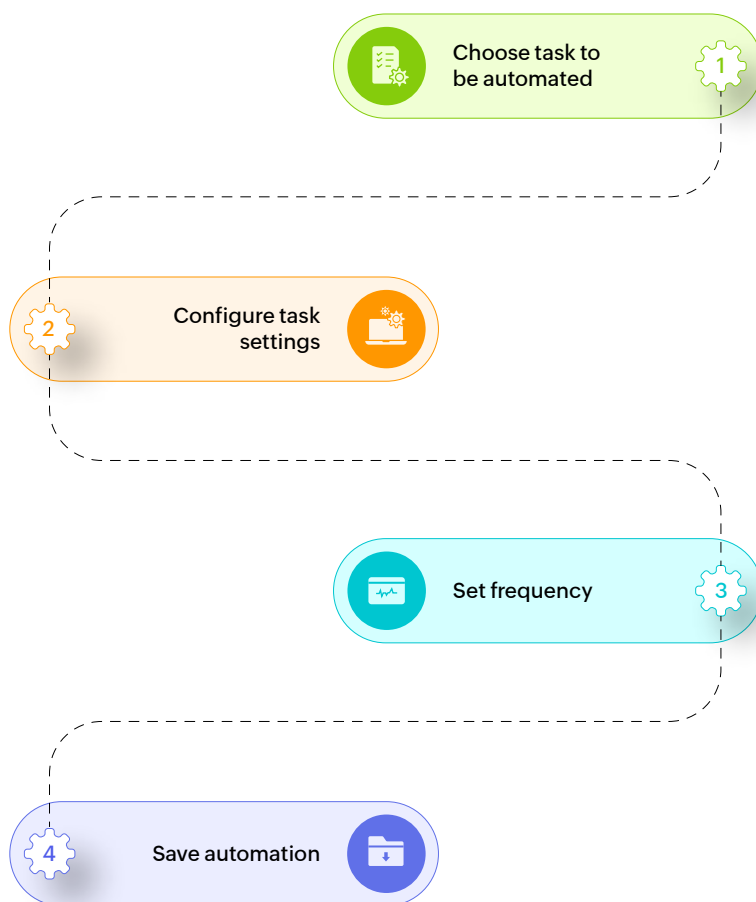
Due to their sensitive nature, most AD tasks are painstakingly and manually performed by IT administrators or achieved by using traditional methods like PowerShell. As organizations keep growing, these tasks can get extremely cumbersome. ADManager Plus's automation feature takes care of this burden by letting you automate repetitive and time-consuming AD tasks.

- ⊘ Easily automate repetitive AD operations, like creating users, deleting inactive users, moving groups, scheduling password notification reminders, and more.

- ⊘ Track the status of the automated tasks.

- ⊘ Generate over 200 comprehensive and intuitive reports on various aspects of your AD environment.

- ⊘ Schedule reports for automated generation at a time that's convenient to you.

- ⊘ Automate a series of follow-up tasks linked to a primary task, arrange them in a specific order, and designate time intervals for their execution.

- ⊘ Tighten security by automating periodic password changes for users.

- ⊘ Set up an approval-based workflow for password reset requests, all with a single click.

- ⊘ Keep track of users that are locked out of their accounts and automate a system to unlock the locked-out AD accounts with zero stress.

Use case: AD cleanup

Let's say your organization has a system of moving all inactive user accounts to a separate OU at the end of every month, retaining them for a period of 100 days, and then deleting them permanently.
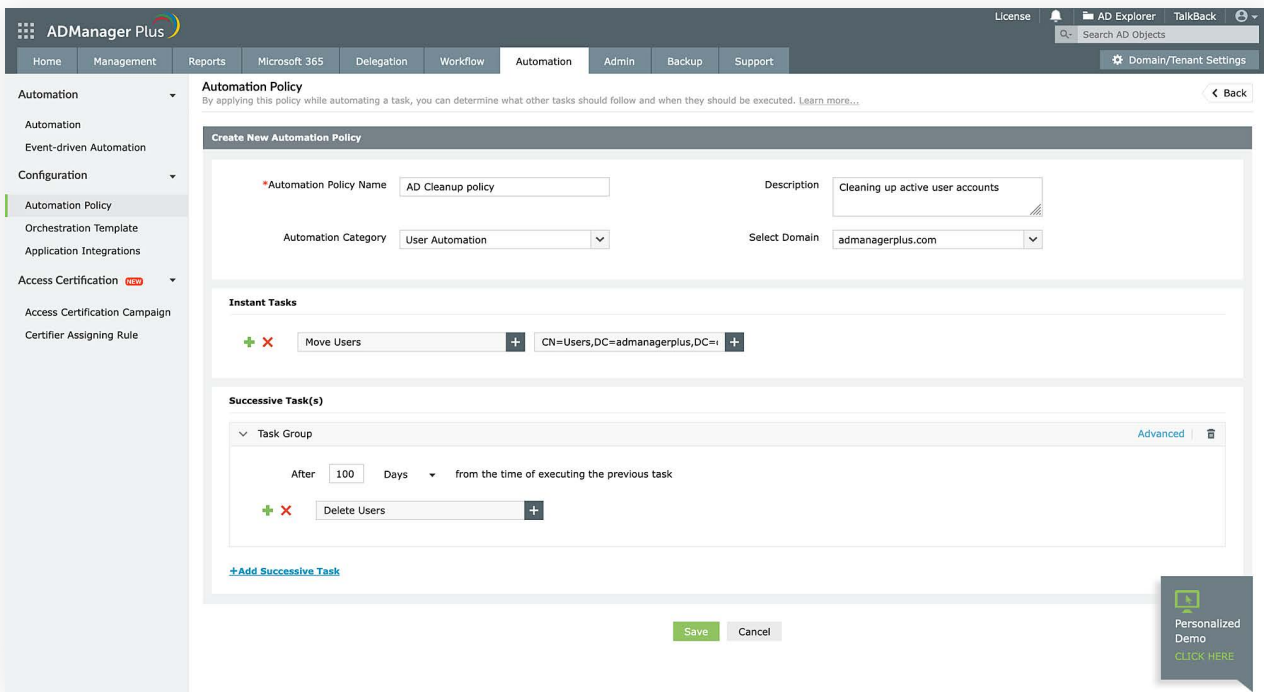
With ADManager Plus, you can streamline this monotonous task easily!

Configure an automation policy

1. In ADManager Plus, navigate to the **Automation** tab and choose **Automation Policy** from the left pane.

2. Click **Create New Automation Policy.**
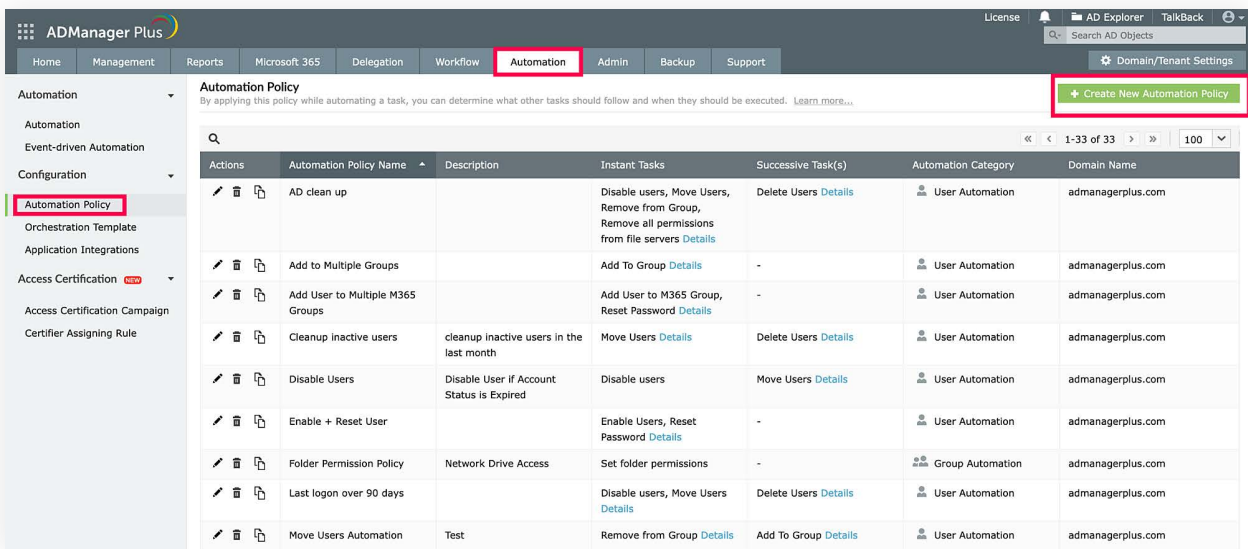
3. In the page that appears, configure the **Automation Policy Name, Description**, and **Domain Name.**

4. In the *Automation Category* drop-down, choose **User Automation.**

5. Under *Instant Tasks*, choose **Move Users** and select the required OU.

6. Click **Add Successive Tasks** and choose the time (e.g., 100 days) after which the successive tasks will be carried out.

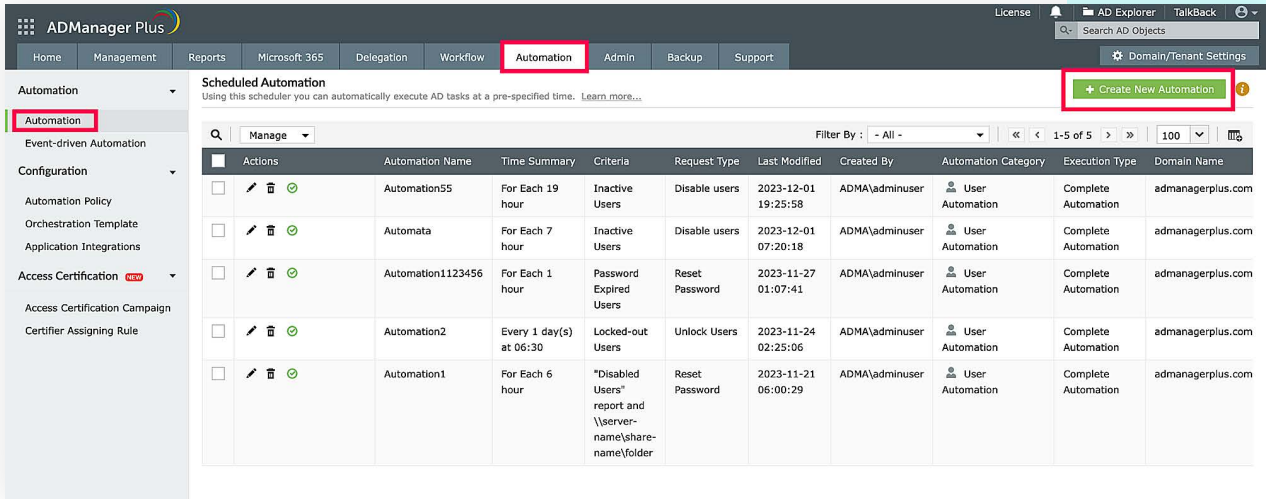7. In this case, select **Delete Users** as the successive task.
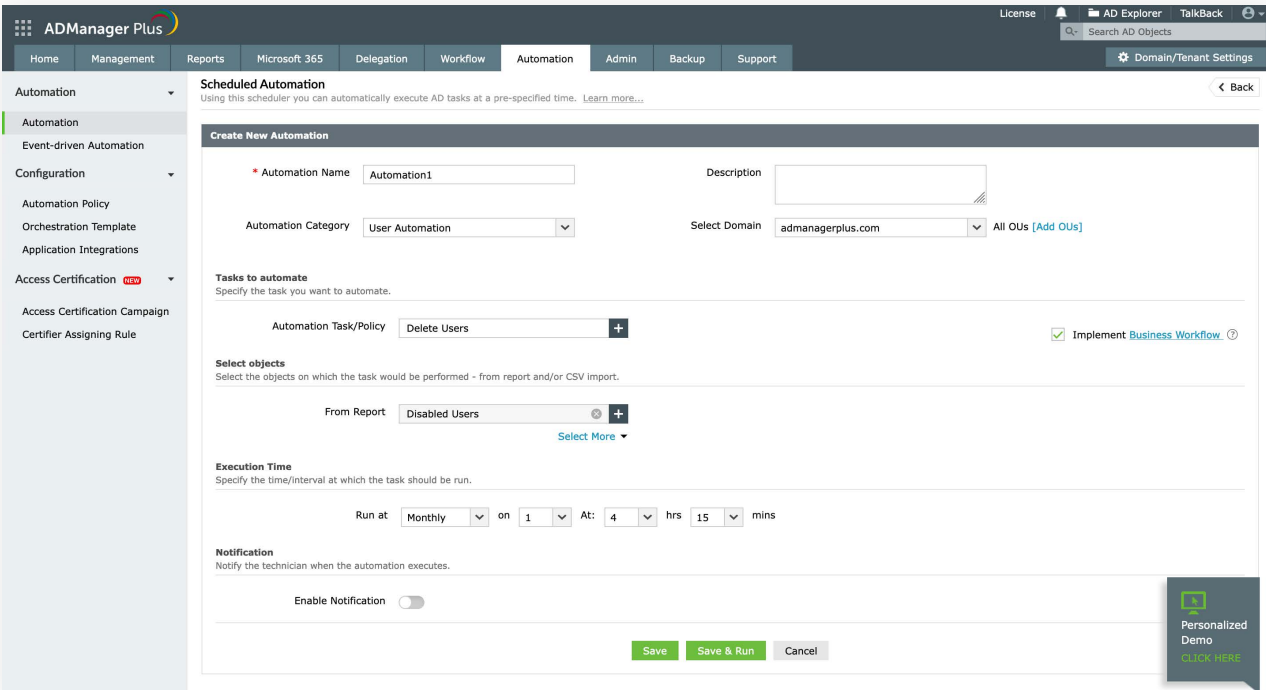

8. Save the automation policy.

Now, you can create an automation to implement this policy automatically.

1. In ADManager Plus, navigate to the **Automation** tab and choose **Automation** from the left pane.

2. Click **Create New Automation.**

3. In the page that appears, configure the **Automation Policy Name, Description**, and **Domain Name.**

4. In the *Automation Category* drop-down, choose **User Automation.**

5. Under *Automation Task/Policy*, choose the automation policy you created.

6. Under *From Reports*, choose the **Inactive Users** report.

7. Select an execution time for the automation. For example, you can choose to run the task on the first of every month, at 2 hours and 0 minutes.

8. Save the automation.

After this automation is configured and saved, the inactive users will be automatically moved to a separate OU on the first of every month, and follow-up tasks will be scheduled.

Ready to revolutionize your AD management with ADManager Plus? Get started with a 30-day, free trial of ADManager Plus or schedule a free demo session with one of our product experts today!

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine
ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management. For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote   ± Download