ManageEngine
ADManager Plus

Proof of Concept

Table of contents

Document overview

This document sheds light on the AD management and reporting challenges faced by IT departments. It details how ManageEngine ADManager Plus helps IT admins tackle all their AD management challenges, helping save time and simplify AD management.

ADManager Plus overview

ManageEngine ADManager Plus is a web-based Windows Active Directory management and reporting solution that helps Active Directory 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, like user account provisioning, stale account management, access management, and AD object backup and recovery. It also generates an exhaustive list of Active Directory reports, many of which are essential requirements for satisfying compliance audits. Adding to that, ADManager Plus helps administrators manage and report on their Exchange Server, Microsoft 365, Google Workspace, and Active Directory environments—all from a single console.

Automating user provisioning and deprovisioning securely across multiple applications

When new employees or contractors are onboarded, it can take days before they are given the appropriate access to the IT systems and applications needed to start their jobs. Similarly, when employees change roles or exit the organization, it often takes a lot of time before IT admins can reprovision access to resources or delete the obsolete user accounts.

Organizations need to be able to:

1. Provision users in AD and all connected applications at the same time.
2. Automate user provisioning and reduce manual work as much as possible.
3. Automate access management of users based on their roles.

How does ADManager Plus automate user provisioning and reduce manual labor?

ADManager Plus allows administrators to automate routine management tasks like creating users, moving users to different containers, and deleting or disabling inactive users to minimize the burden on IT administrators. ADManager Plus does this by allowing integration with any HCM solution with API support. With this powerful integration capability, IT teams can securely automate user management operations. Any changes made to users in the HCM solution, such as users being created or deleted, or roles being modified, are automatically synced to the AD environment.

Key benefits

Provision users across multiple platforms

ADManager Plus allows administrators to automate routine management tasks like creating users, moving users to different containers, and deleting or disabling inactive users to minimize the burden on IT administrators. ADManager Plus does this by allowing integration with any HCM solution with API support. With this powerful integration capability, IT teams can securely automate user management operations. Any changes made to users in the HCM solution, such as users being created or deleted, or roles being modified, are automatically synced to the AD environment.

Create automation policies to automatically provision users when new records are added in your HCM application.
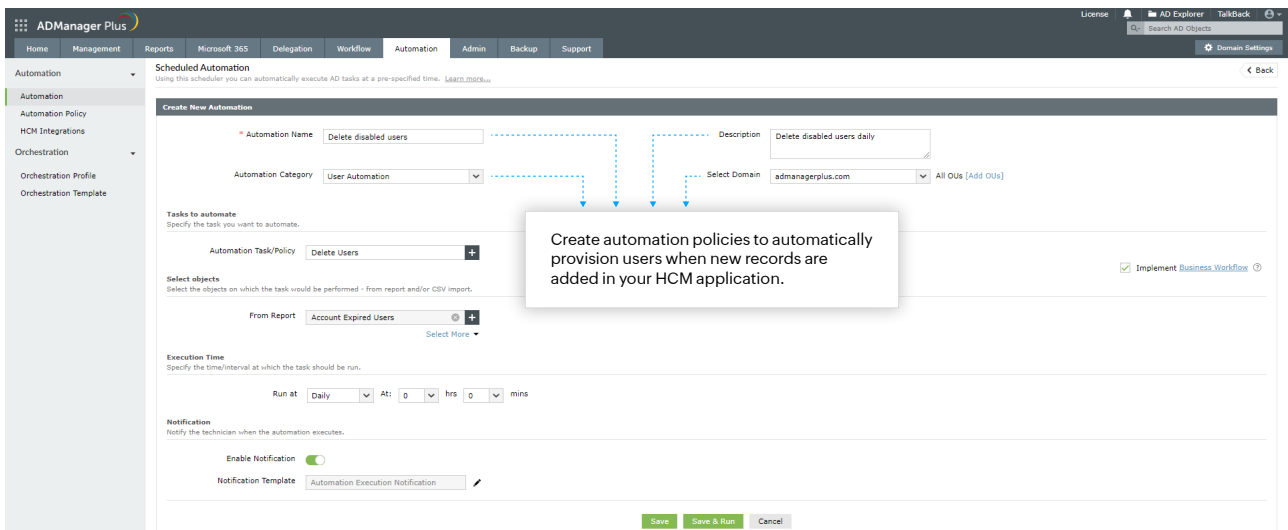
Synchronize any changes in the HCM software with AD

Automatically modify account properties, such as group memberships, OUs, and file server permissions, when employees change roles or teams to ensure that they have the right access to the right resources. With ADManager Plus' integration with HCM software, you can configure automation policies that will automatically synchronize any updates in the HCM system, like user creation or deletion, with AD.

Mitigate the security risks caused by obsolete user accounts

Automatically disable or delete users' AD accounts, remove their Microsoft 365 licenses, export their mailboxes, and more each time a user record is deleted in the HCM application. This reduces the window of time a hacker has to breach one of these accounts and access sensitive data.

Periodically check for disabled user accounts and delete them from your AD environment.
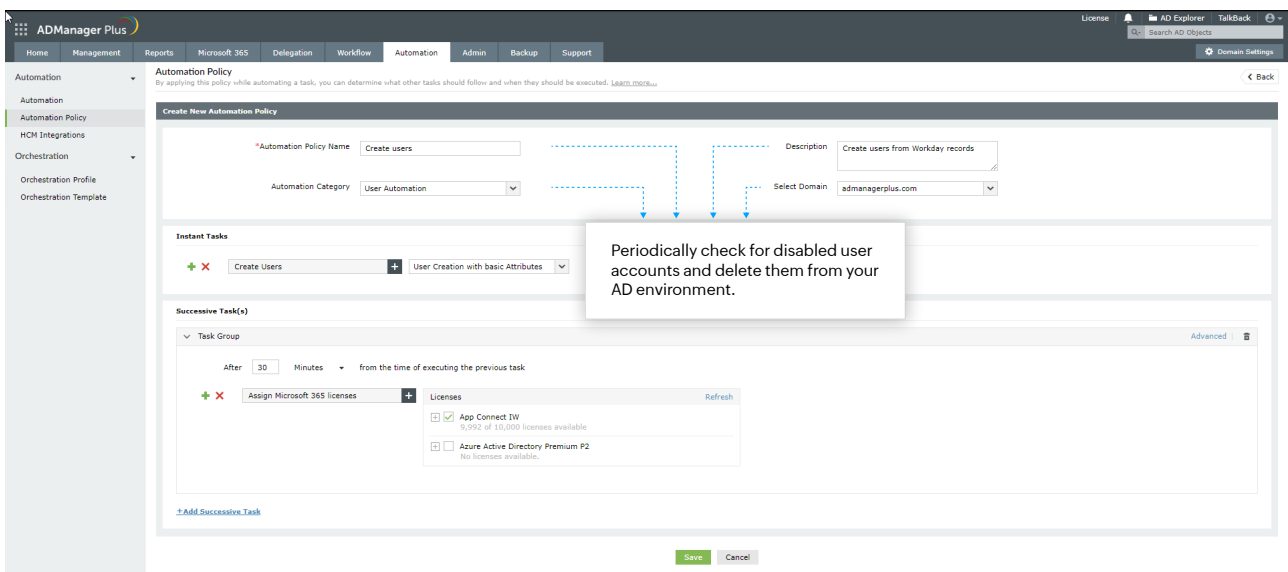
Simplifying AD reporting

IT administrators should be able to gather all the essential information about their AD infrastructure and objects at any time they choose. Administrators, at times, are required to generate reports at a moment's notice. Other times, they need reports that are automatically generated at fixed intervals. The native reporting tools available in AD are not equipped to perform all the tasks administrators need for their day-to-day activities. The native tools require complex PowerShell scripts to gather all the information required by an administrator, which can be time-consuming, error-prone, and requires in-depth knowledge of AD and scripting tools.

Organizations need to ensure their IAM solution can:

1. Generate reports without requiring scripts.
2. Generate reports for status of compliance automatically at fixed intervals.
3. Create reports for specific needs using a custom report builder.

How does ADManager Plus help administrators manage their AD environment?

Unlike the conventional Microsoft tools and PowerShell, ADManager Plus enables users with limited scripting knowledge and even non-IT users to generate AD reports on users, distribution lists, security groups, computers, and contacts. This purely GUI-based AD reporting software also helps you generate reports on Exchange Server mailboxes, Microsoft 365, Exchange Online, Google Workspace, Skype for Business, and more, all from a single console.

Key benefits

Script-free report generation

With ADManager Plus, administrators and help desk technicians can generate reports on all entities within AD using simple, GUI-based actions. ADManager Plus comes with over 200 preconfigured reports, and administrators can create custom reports as well based on their requirements. Administrators also have the option to export all generated reports to CSV, PDF, XLSX, HTML, and CSVDE formats.

Generate any report instantly in just a few, simple clicks.
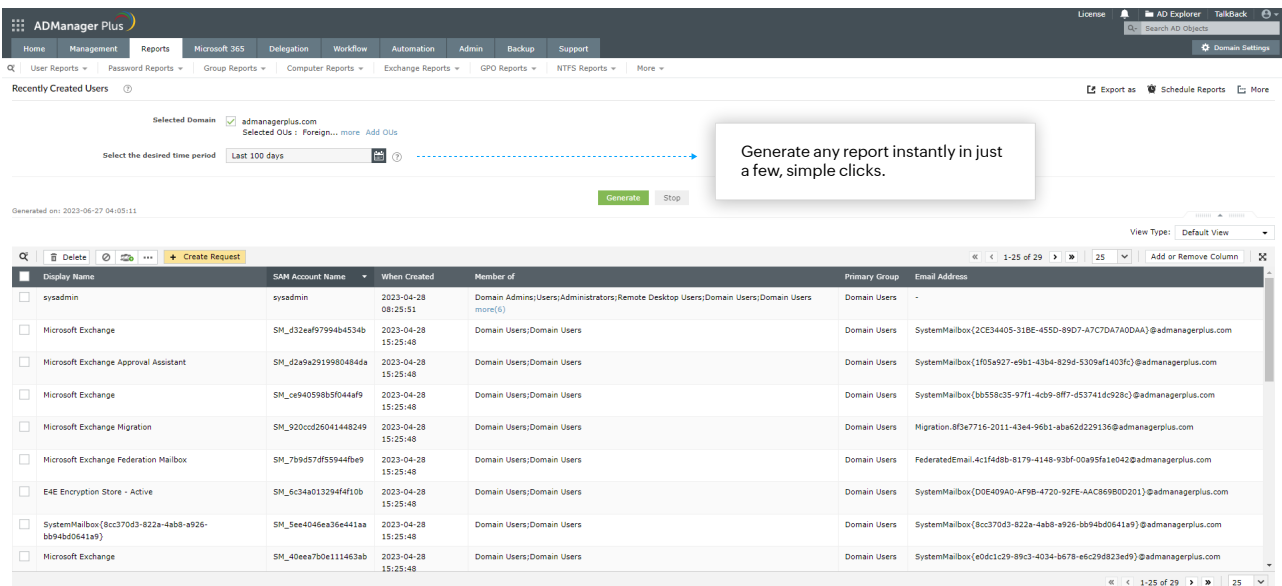
Automate compliance reporting

With ADManager Plus, administrators and help desk technicians can easily comply with various regulations such as SOX, HIPAA, the PCI DSS, the GLBA, and the GDPR. They can schedule the reports to be generated at fixed intervals and have them delivered to the email addresses of administrators or save the reports to a local repository in a format of their choice (PDF, HTML, XLSX, CSV, and CSDVE).

Generate compliance reports for popular regulations such as SOX, HIPAA, PCI DSS, GLBA, and the GDPR.
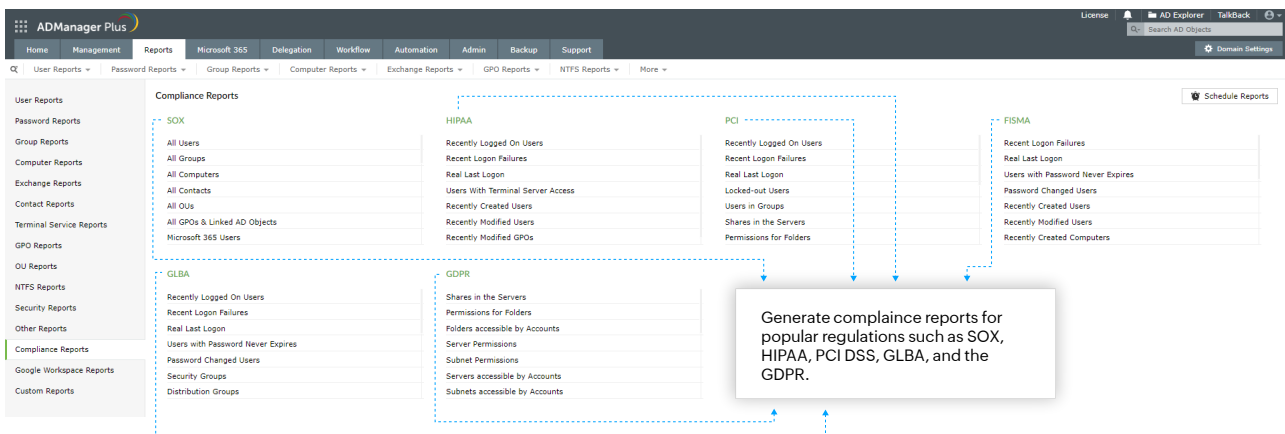
On-the-go management from reports

In addition to getting information from the reports, administrators can also perform management actions straight from the reports, simplifying AD administration. Administrators can perform actions like resetting passwords, managing user attributes and group memberships, and more directly from the reports.

Instantly perform management actions from the generated reports.
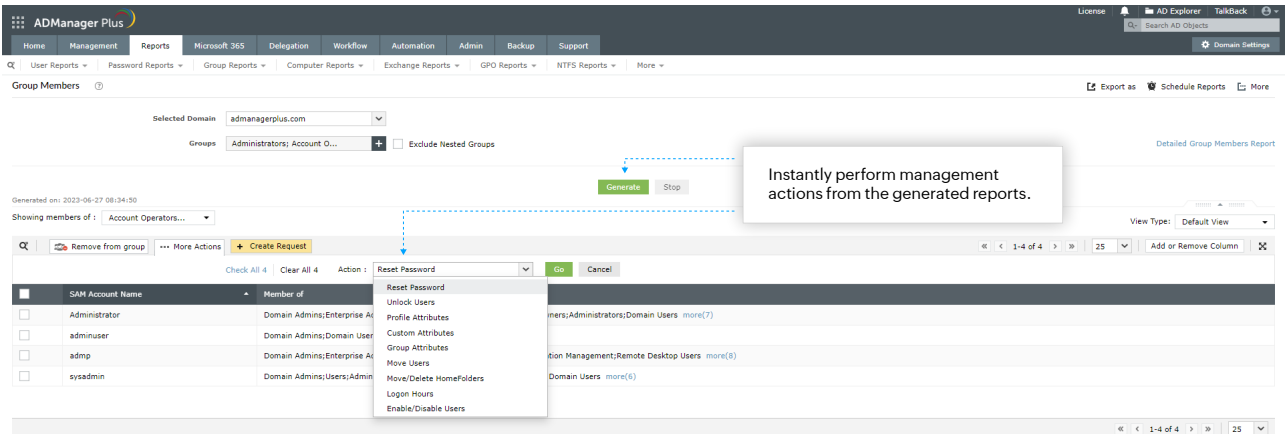
Improving efficiency with secure automation and orchestration

Employees of modern organizations use a variety of tools to perform day-to-day activities, and the onus is on the IT teams to provision, reprovision, and deprovision users across all these applications as and when needed. Making the changes across all applications individually is a time-consuming and mistake-prone task. It's important for organizations to ensure their IT teams are not held up creating and providing access to users and their accounts across various applications.

Organizations need to ensure their IAM solution can:

1. Manage user accounts across all applications simultaneously.
2. Provide a low-code, custom orchestration template builder.

How does ADManager Plus help administrators improve efficiency through identity automation?

ADManager Plus lets administrators automate a series of tasks at defined time intervals from a single console. ADManager Plus triggers a sequence of actions whenever a user or group management task is performed, not just in AD, but in other enterprise applications as well. Administrators can define the flow of actions to be performed using drag-and-drop actions. They can then define the conditions under which the actions will be executed.

Key benefits

Accelerate user onboarding

With ADManager Plus, IT administrators can create orchestration templates for user onboarding. When any user onboarding activity is initiated, a series of actions as defined in the template is automatically carried out in sequential order. User accounts are created in AD and other applications, such as Exchange, Microsoft 365, and other applications via webhooks, and are provided access based on the role assigned to the user. This speeds up the user onboarding process considerably and reduces the manual work of the IT team.
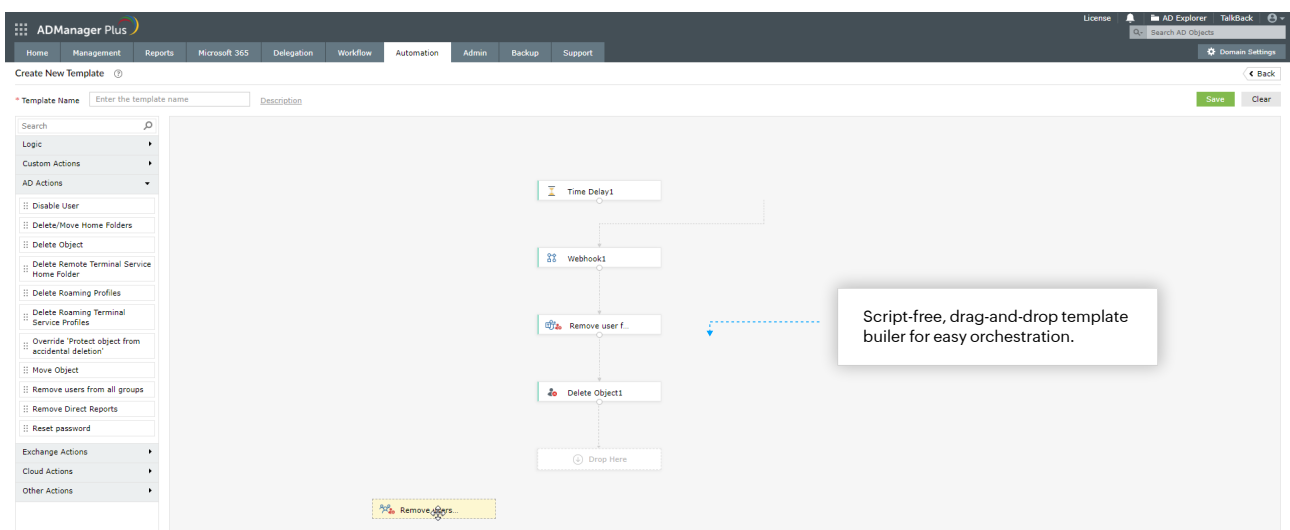
Employee Onboarding
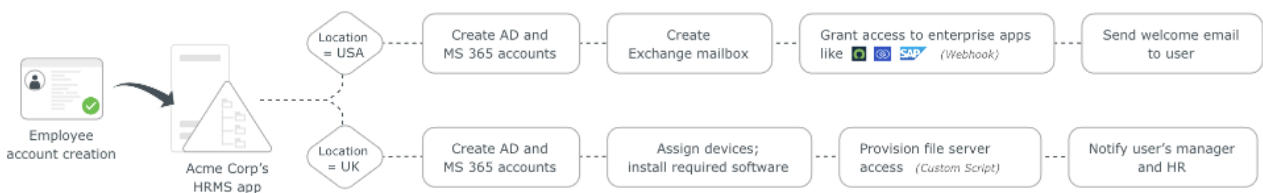
Employee Offboarding
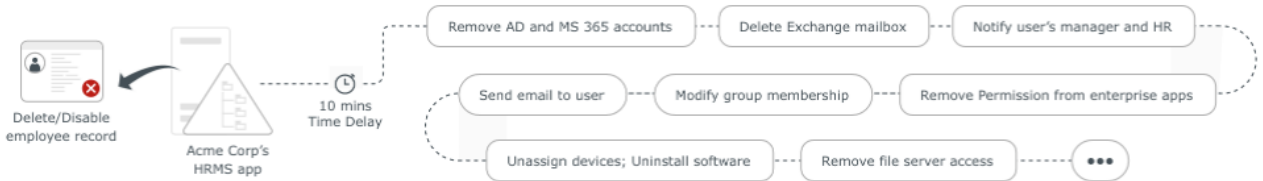
Drag-and-drop template builder

With ADManager Plus, administrators can create multiple orchestration templates for different use cases with zero code. Administrators can create new templates from scratch with simple drag-and-drop actions.

Script-free, drag-and-drop template builer for easy orchestration.

Custom notifications

With ADManager Plus, administrators can send automated emails to users and their managers when any action is completed through orchestration templates. Administrators can choose to send out notifications via email, SMS, or both depending on their preference. ADManager Plus also provides the ability to add macros and attachments to the content of the message.

Simplifying AD management

IT administrators are tasked with creating and managing multiple AD objects almost every day. Leveraging native AD tools like the Active Directory Users and Computers console and PowerShell scripts to execute these tasks is not ideal since admins have to toggle between multiple consoles. This can be time-consuming, error-prone, and requires in-depth knowledge of AD and scripting tools.

Organizations need to ensure their IAM solution can:

1. Manage AD objects in bulk.
2. Automate routine AD tasks.
3. Report on all changes in the AD environment.

How does ADManager Plus help administrators manage their AD environment?

ADManager Plus simplifies and automates AD administration. It allows IT administrators and technicians to manage AD objects easily and generate instant reports at the click of a button. The solution is loaded with more than 200 actionable reports that provide essential information about the AD infrastructure, allowing administrators the flexibility to perform management actions right from the reports.

Key benefits

Bulk AD objects management

With ADManager Plus, administrators can create and manage AD users, computers, groups, contacts, OUs, GPOs, file servers, and more using simple GUI-based actions. They can also perform bulk password resets, automate periodic password changes, and configure unique passwords for different users instantly. They can manage users, groups, contacts, calendars, licenses, teams, sites, and more either individually or in bulk with built-in bulk management templates.
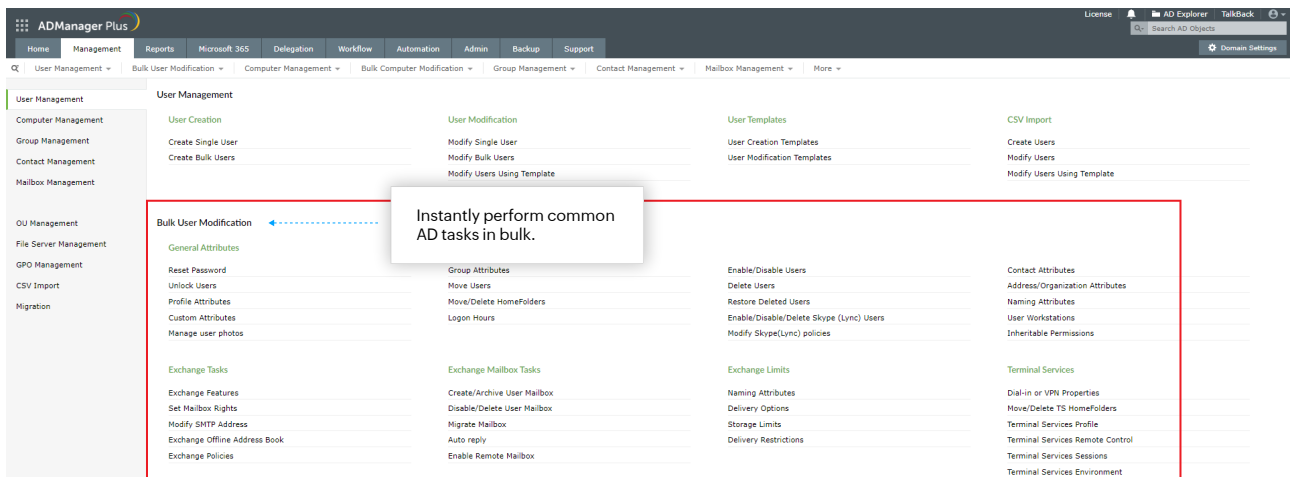
Automate routine AD tasks

With ADManager Plus, administrators can automate time-consuming, routine AD tasks such as provisioning and deprovisioning users, resetting passwords, creating and modifying AD groups, and revoking Microsoft 365 licenses. They can configure Automation Policies to define and execute subsequent tasks at predefined intervals and enumerate a set of tasks to be executed sequentially after a specified task is performed. Administrators can even maintain complete control over all automated tasks by implementing approval-based business workflows to get an overview of tasks before they are executed.

Comprehensive AD reporting

Administrators can generate detailed reports to fetch vital information on AD and Azure AD, such as users' accounts, logons, and password statuses; group types; GPO scopes; and accesses to objects and mailboxes, all without writing a single PowerShell script. They can leverage the custom report builder to create reports that include custom AD attributes and LDAP queries. All reports generated by ADManager Plus can be exported to multiple formats, such as PDF, XLS, CSV, or HTML, can be scheduled to run at specific times, and can be delivered to the email addresses of administrators once the report has been generated. The reports can be filtered to fetch the exact information needed, and administrators can perform on-the-fly management actions directly from the generated reports.

Administrators can view important information from multiple, business-critical reports directly from a customizable dashboard and monitor the data from each AD domain in separate tabs.
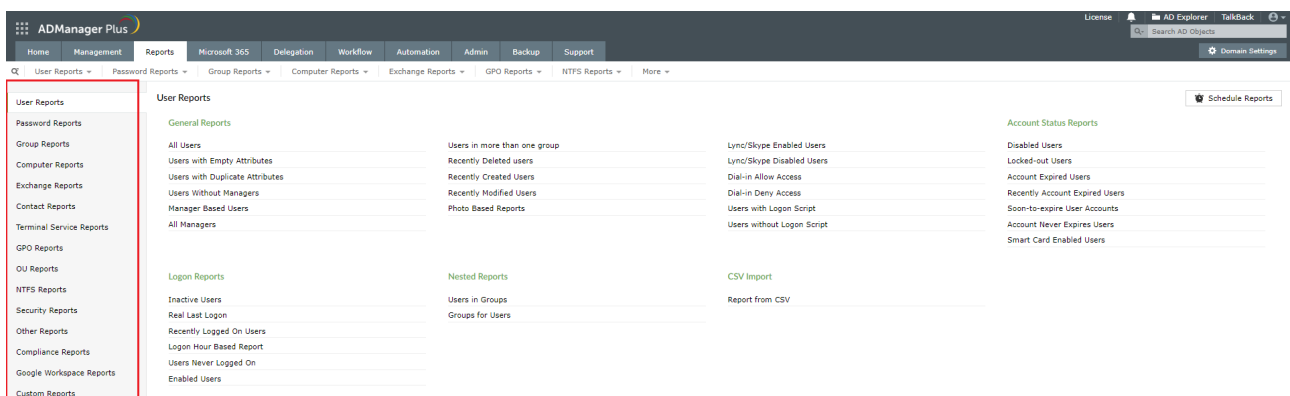
Challenge 5:

Streamlining access management

One of the major challenges administrators face is managing access for all users in the organization. Providing excess access can cause security issues while insufficient access can disrupt regular work activities for employees. Administrators need to ensure all employees are provided just enough access to carry out their tasks and access must be revoked when their work is accomplished.

Organizations need to ensure their IAM solution can:

1. Provision users with access when their accounts are created.
2. Revoke access automatically when it's no longer needed.
3. Manage file server permissions.

How does ADManager Plus help administrators manage their users' access?

ManageEngine ADManager Plus simplifies and streamlines user access management with its ability to provision users with all the required access rights when user accounts are created. Administrators can also modify individual users or bulk modify multiple users' access with a few simple clicks. The solution also allows you to automate access permissions of end users with time-bound access.

Key benefits

Secure access provisioning during user creation

With ADManager Plus, administrators can create accounts for users not only in AD, but across multiple applications at the same time using its Orchestration functionality. When accounts are created for users across different enterprise applications, ADManager Plus can also provision all necessary access to each of these accounts based on the created users' roles. This ensure new users will be ready to begin work as soon as they log in instead of having to wait for IT teams to manually provide them with required access across each individual application.
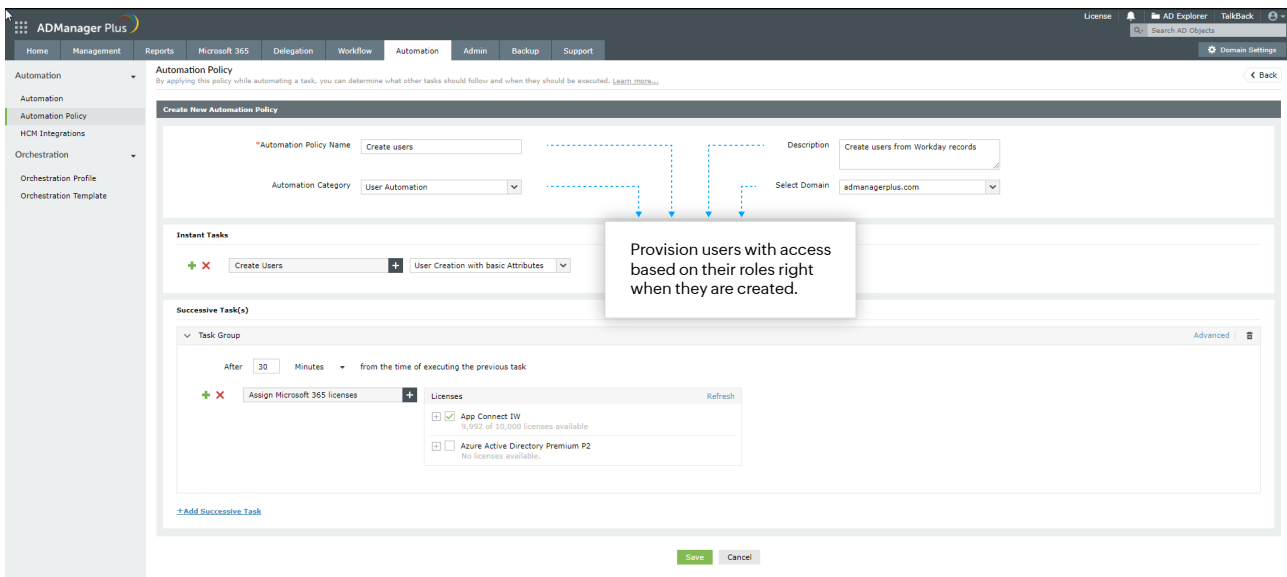
Automate access provisioning and revocation

With ADManager Plus, administrators can automate access provisioning and revocation. ADManager Plus also allows administrators to automate security group memberships for all users. In addition to that, ADManager Plus can automate membership modification based on any users' role changes in the organization's HCM solution, ensuring users are equipped with all required permissions whenever their role within the organization is modified.

Manage file server permissions

With ADManager Plus' file server management feature, administrators can manage (i.e., assign, modify, and revoke) users' NTFS and share permissions either individually or in bulk. All administrators have to do is choose the shared resource and then scrutinize and define the access controls of users based on their needs. Administrators can also provide just-in-time access and just enough permissions in only a few mouse clicks, and delegate AD file server permissions management to technicians securely.
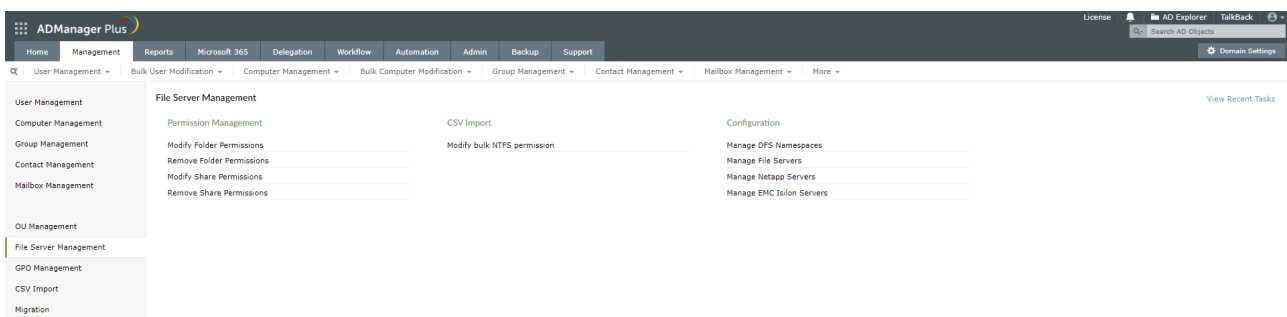
Detecting identity and access-based risks in AD, such as stale accounts and elevated privileges

As organizations grow and evolve, user roles and permissions frequently change, resulting in a high degree of variability in identity-related risks. This increased variability can elevate the risk of data breaches, unauthorized data access, and other security incidents.

Organizations should follow a structured process aimed at evaluating and mitigating security risks associated with user identities within an organizational framework. Adopting a proactive strategy to mitigate the potential impact of unauthorized access bolsters the organization's resilience against security threats.

Organizations need to ensure that their IAM solution can:

1. Effectively address security misconfigurations
2. Securely manage the organization's identities
3. Ensure compliance with relevant regulations

How does ADManager Plus provide a comprehensive view of your AD threat landscape?

Identity risk assessment in ADManager Plus involves a systematic evaluation of potential security risks associated with user identities in the AD environment. ADManager Plus provides essential tools and features for administrators to analyze user identities, audit actions, and enforce security controls, ensuring a proactive approach to identity and access management. By conducting identity risk assessment, organizations can enhance their security posture, address compliance requirements, and safeguard against potential threats to their digital assets.

Key benefits

Proactively secure AD against potential threats

With ADManager Plus, administrators are alerted so they can easily recognize and address potential risks before they escalate into security threats. This is crucial for preventing Active Directory-related attacks, security breaches, and ransomware incidents. This proactive approach not only safeguards your organization's sensitive data and assets, but it also prevents financial implications that may arise from addressing and recovering from such security incidents.

Ensure adherence to audit and compliance standards

With ADManager Plus, administrators can ensure compliance with mandates such as the GDPR and PCI DSS. ADManager Plus adheres to NIST SP 800-30 guidelines to assess the probability and impact of risk indicators, generating a comprehensive risk score. Administrators can efficiently streamline the process by identifying risk indicators and producing exportable, comprehensive reports for compliance auditing purposes.


Reinforce the risk posture with advanced security measures

With ADManager Plus, elevate the robustness of your cybersecurity approach by proactively identifying potential risk indicators using the Identity Risk Assessment dashboard. The Risk Score provided by the dashboard serves as an indicator of your organization's overall risk posture, categorized as low, medium, high, or critical. ADManager Plus ensures you can take action based on the mitigation measures and remediation techniques provided by the solution to eliminate and avoid the identified risk indicators.
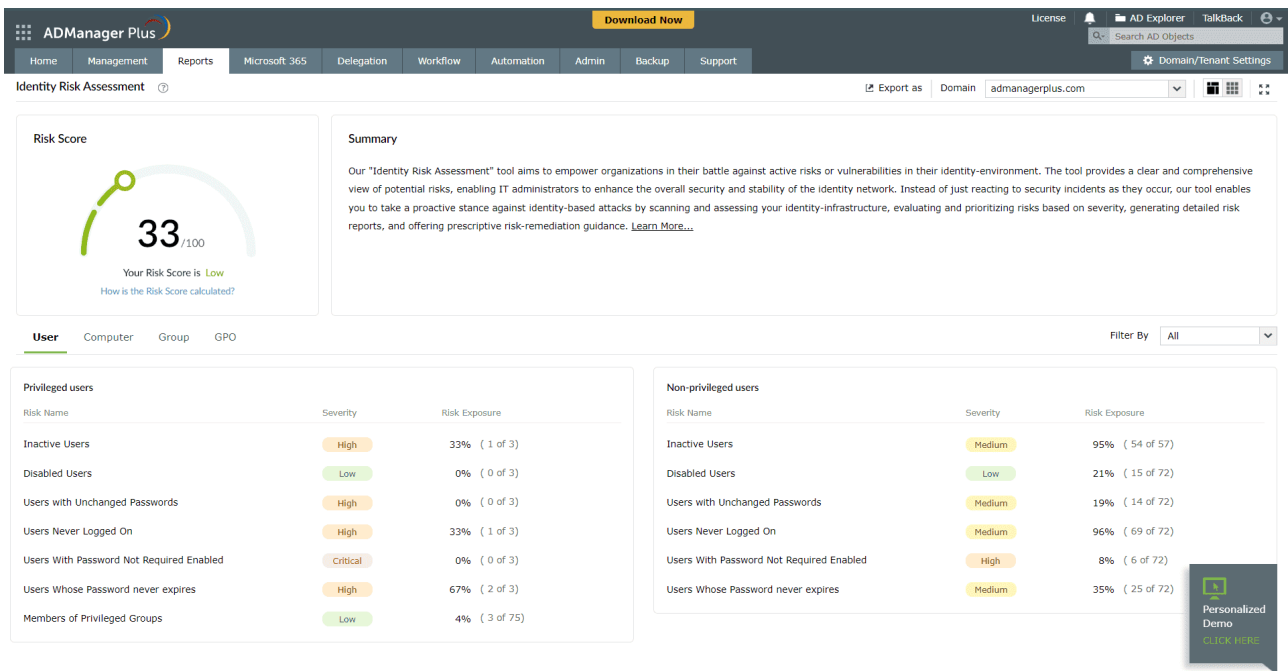
Challenge 7:

Executing access certification campaigns

An access certification campaign involves reviewing and validating the access rights and privileges granted to users. Regularly conducting these campaigns enables organizations to maintain control over access management, reduce the risk of unauthorized access or data breaches, and meet regulatory requirements for data privacy and security.

Organizations need to ensure that their IAM solution can:

1. Align with compliance policies
2. Supports certification campaigns
3. Mitigate risks of unauthorized access or data breaches

### How does ADManager Plus validate access rights and privileges?

ADManager Plus, as an identity governance and administration (IGA) solution, provides organizations with access certification capabilities, streamlining their access control methods. During an access certification campaign, certifiers receive notifications and reminders, prompting them to review and verify the access rights assigned to the users. Options are available to either select a default certifier for certifying the access request, or designating multiple technicians as certifiers using an assigning rule. The certifier has the authority to revoke permissions if any access rights are deemed unnecessary.

Key benefits

Enhance the security of privileged accounts

With ADManager Plus, administrators can conduct a personalized certification campaign designed to meticulously manage the privileges associated with accounts that have access to sensitive information. This process involves thoroughly scrutinizing and validating the permissions assigned to these accounts.
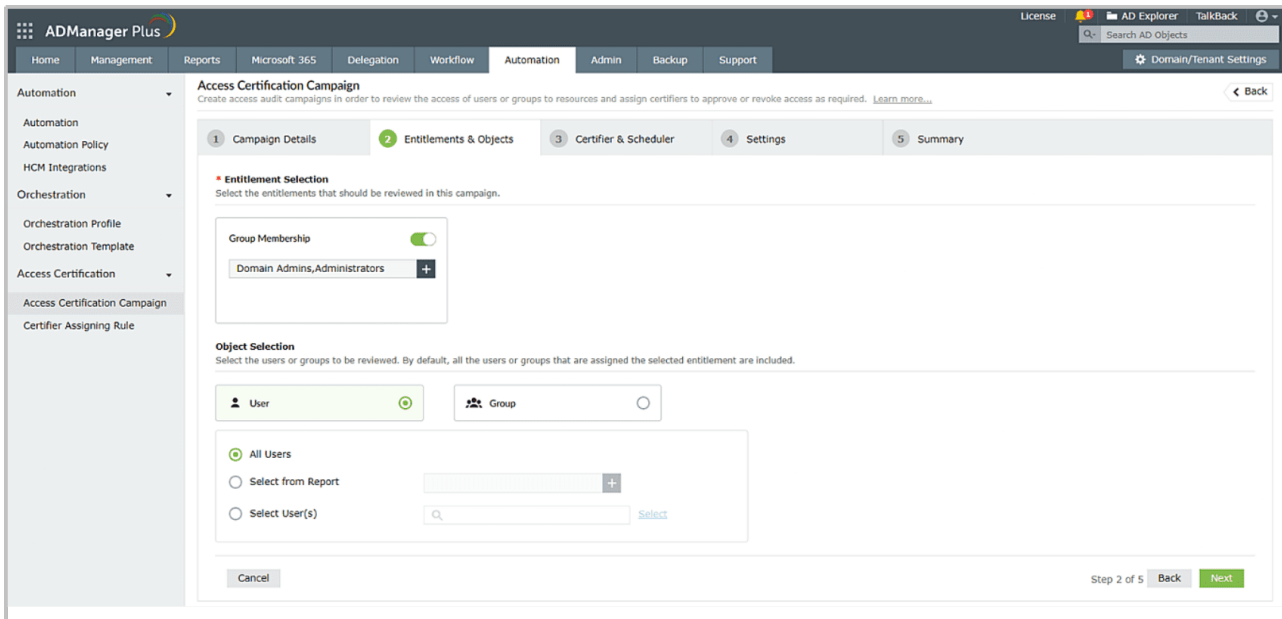
Ensuring alignment with compliance and audit requirements

Every certification campaign conducted in ADManager Plus is archived and accessible to stakeholders. A comprehensive campaign history, encompassing certifier details, actions taken, certifier comments, and additional information, is meticulously recorded. This repository of certification activities serves as a valuable resource for auditors and compliance personnel during audit trials.
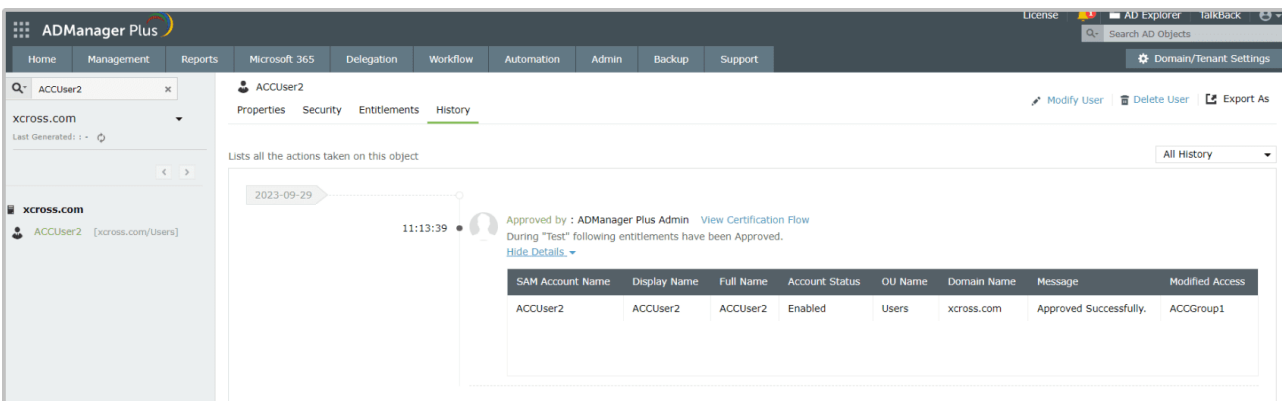
Mitigated risks from insider threats

Managing what data employees can access might seem easy, but it's actually quite difficult. Administrators should conduct regular reviews of users' access rights and proactively revoke unnecessary privileges with regularly scheduled but automated access certification campaigns. Utilizing a dependable solution is vital, as it safeguards against threats posed by malicious insiders.

Challenge 8:

Protecting the data in all enterprise applications

Data is invaluable, and organizations today have a lot of data across various enterprise applications. Ransomware has been a major threat the past few years and shows no signs of slowing down, so organizations need to ensure they have a reliable way to protect their data. The native tools in enterprise applications are not equipped to ensure complete data protection.

Organizations need to ensure their IT teams can:

1. Back up all data in AD, Azure AD, and Google Workspace.
2. Restore the entire application or just a part of it in an instant.
3. Satisfy rigorous recovery point objective (RPO) requirements.

How does ADManager Plus help administrators protect their critical data?

ADManager Plus simplifies data backup and restoration for enterprises with its ability to back up multiple enterprise applications such as AD, Azure AD, and Google Workspace from a single console. ADManager Plus allows administrators to back up all parts of their environment and restore an entire application or just a single object to any of its backed up states in a matter of minutes.

Key benefits

Incremental backups and versioning

With ADManager Plus, administrators can back up all changes made to their enterprise application data as separate versions. This allows them to restore any object or item to any of its past versions instantly. Moreover, since only the changes are backed up since the last backup cycle, the time taken to complete the backups is minimal, ensuring administrators can back up a recent version of the environment quickly.

One-click recycle bin

All native tools have a retention period for items in the recycle bin, post which the object will be purged forever from the system. With ADManager Plus, administrators can restore any deleted item, be it a user object or a mailbox item, no matter when it was deleted.

Flexible RPOs and storage options

ADManager Plus allows administrators to define distinct RPOs for each data class depending on its criticality. It also allows administrators to store backups within their premises in network-attached storage devices or in the cloud (i.e., Azure Blob storage and file shares).

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