

ManageEngine

ADManager Plus

Overview



In today's digital world, organizations face significant challenges in efficiently managing and securing identities. Challenges arise in several key areas, as indicated below

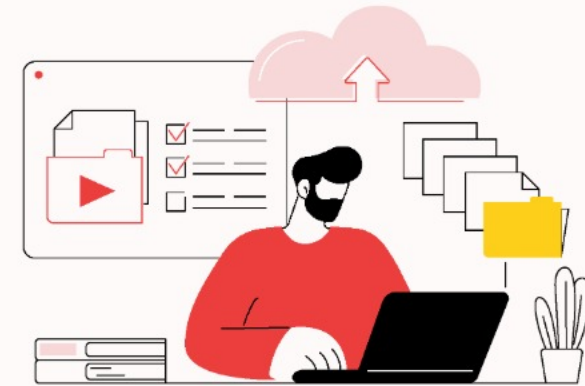
User lifecycle management



Security and compliance



Disaster recovery and backup



We provide the remedy for your issues with,







ManageEngine **ADManager Plus**

An identity governance and administration (IGA) solution that simplifies
identity management, ensures security, and improves compliance.

Why ADManager Plus?

- ✓ Streamlined identity life cycle management
- ✓ Compliance-oriented reporting
- ✓ Multi-level business workflows
- ✓ Granular access controls and delegation
- ✓ Entitlements management
- ✓ Inter-forest and intra-forest migration of AD objects
- ✓ Secure data backups and recovery
- ✓ Integration with popular SIEM, HCM, ITSM and help desk tools
- ✓ iOS and Android mobile apps
- ✓ Customizable dashboard

Agenda

-  **Management**
-  **Reporting**
-  **Delegation**
-  **Workflow**
-  **Automation**
-  **Backup and recovery**
-  **Risk and compliance**
-  **Integrations**



Management

This management solution empowers administrators to efficiently and securely handle users, computers, contacts, groups, and other resources across multiple platforms with ease.

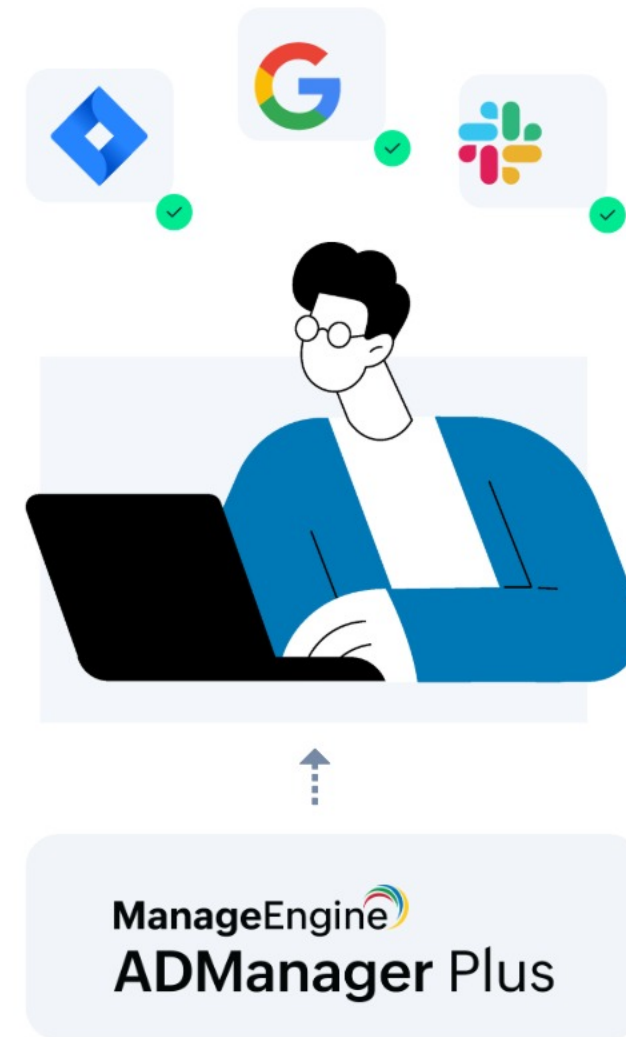
Management

Some important features under Management tab are shown below which will be explained in the upcoming slides:

- ✓ Streamlined life cycle management
- ✓ Customizable templates
- ✓ Bulk management
- ✓ File server management
- ✓ Migration
- ✓ Delete/Disable policy
- ✓ Real time notifications

Streamlined life cycle management

Provision user accounts across multiple platforms such as Active Directory (AD), Microsoft Exchange, Microsoft 365, MS Teams, and Google Workspace, simultaneously from a single console.



Customizable templates



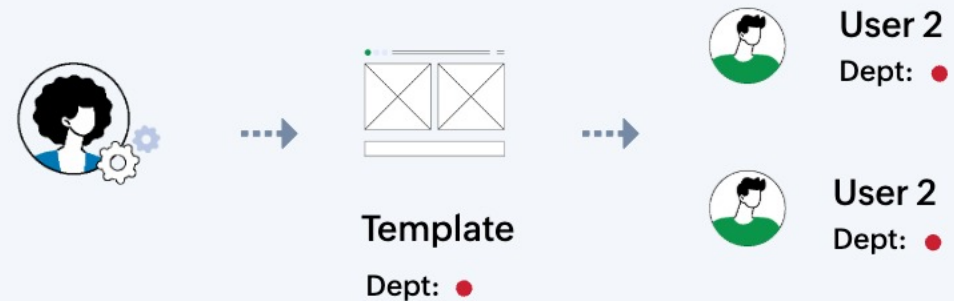
Streamline the management of AD objects like users, computers, groups, contacts, OUs, and GPOs using customizable templates with functionalities like condition-based management, duplication check, grouping creation, modification templates, and more.



Assign creation and modification templates to help desk technicians, enabling them to perform management actions with a specific set of templates.



Proactively identify and handle duplicates. Decide what action has to be taken in case duplication occurs.



Auto - configuring attributes based on condition

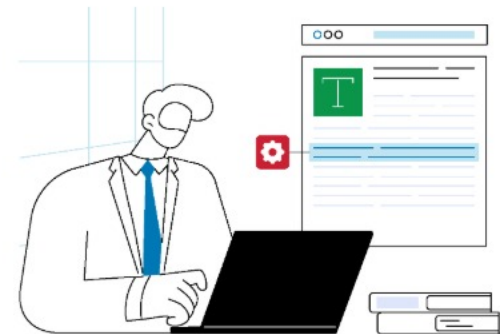
Customizable templates



Importing details
from a CSV

ManageEngine
ADManager Plus

Create or modify
objects



The bulk update tool simplifies all AD user management operations including tasks like resetting passwords for multiple user accounts, creating Microsoft 365 and Google Workspace accounts, enabling/ disabling/ and deleting inactive accounts, and more via CSV import.

File server management

Empowers administrators to manage users' NTFS and share permissions in bulk using below capabilities,

- ✓ Provide access to required resources without security risks.
- ✓ Perform bulk modification of permissions.
- ✓ Manage permissions on Active Directory, NetApp, and Isilon file servers.
- ✓ Carry out all these tasks from a simple, single, central window.
- ✓ Apply different types of permissions and limit the scope to particular folders and sub-folders.

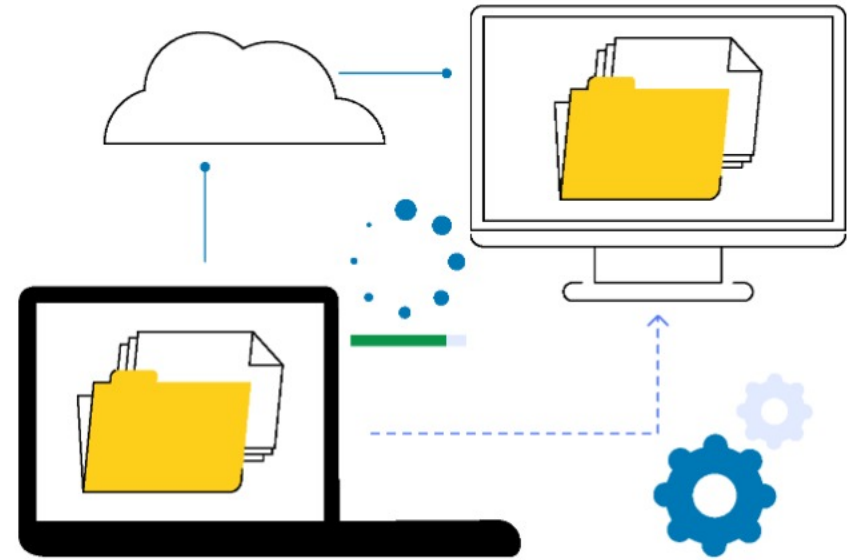


Migration

Active Directory (AD) migration is just an added task for an organization's already overburdened IT team, and the last thing administrators want is to struggle with the native Active Directory Migration Tool (ADMT). ADManager Plus' AD Migration feature lets administrators migrate users and groups across domains in their AD environment, with or without ADMT.

The following migrations can be performed using ADManager Plus:

- ✓ User migration
- ✓ Group migration
- ✓ Contact migration
- ✓ GPO migration



Delete/Disable policy

You can create domain-specific delete policies and disable policies with a specific set of preferences and instructions that must be executed whenever user accounts are disabled or deleted from the Active Directory.

You can automate the following actions whenever a user account is deleted, or disabled:

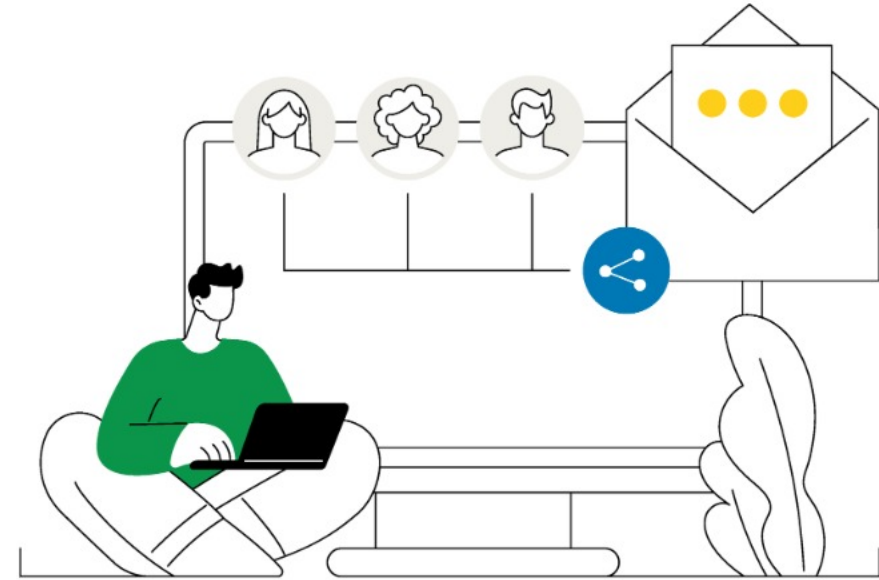
Delete, or disable the,

- ✓ Home folders
- ✓ Roaming profiles
- ✓ Microsoft 365, Google Workspace accounts, and more.



Real-time notifications

- ✓ Set up notifying administrators or technicians about any change made in AD through ADManager Plus via:
 - ↳ SMS
 - ↳ Email
- ✓ Create notification templates to configure the recipient, and the message that has to be sent.
- ✓ Create notification profiles to send custom notification messages.



Reporting

Generate and schedule more than 200 pre-configured, granular reports on AD, Exchange, Microsoft 365, and Google Workspace.

Reporting

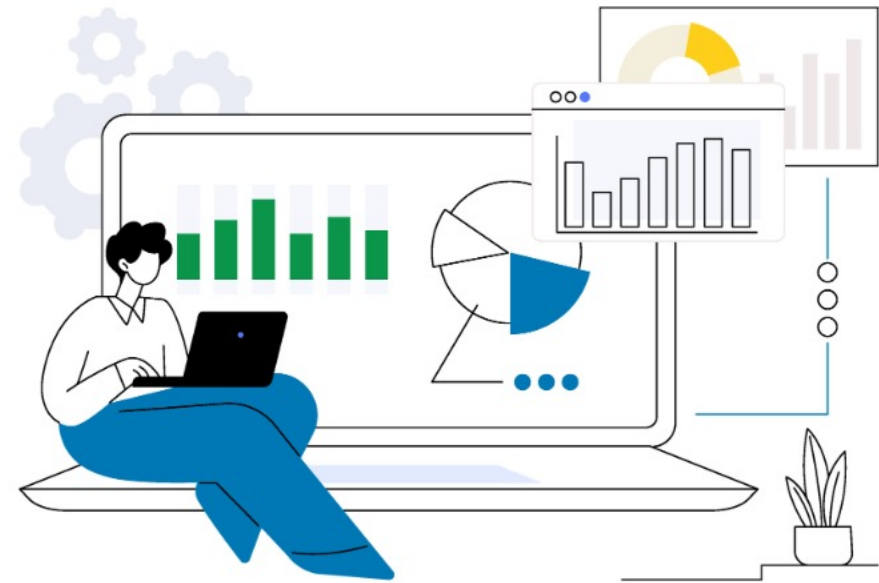
Some of the important features under Reporting tab are,

- ✓ Script-free reporting
- ✓ 200+ pre-packaged reports
- ✓ On-the-fly management
- ✓ Built-in report scheduler
- ✓ Custom reports
- ✓ Compliance reports for regulations like SOX, GLBA, HIPAA, PCI, GDPR and FISMA



Script-free reporting

While native AD tools leave you with no other choice except PowerShell and other scripting methods to build every report that you need from scratch, ADManager Plus offers a comprehensive list of pre-built reports, for efficient, trouble-free management and reporting.



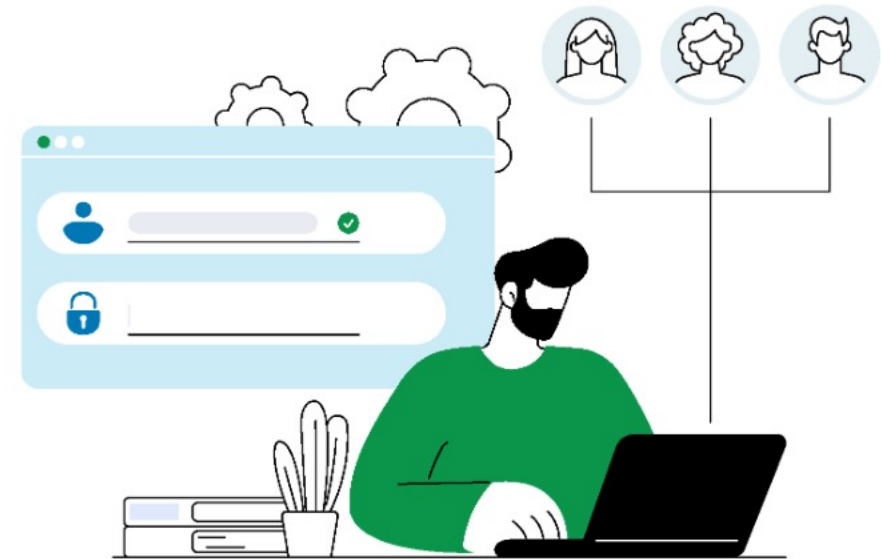
200+ pre-packaged reports

Generate reports such as Inactive users report, logon reports, disabled computers, and more. Also, export reports in multiple formats including HTML, PDF, XLS, XLSX, CSV, and CSVDE.



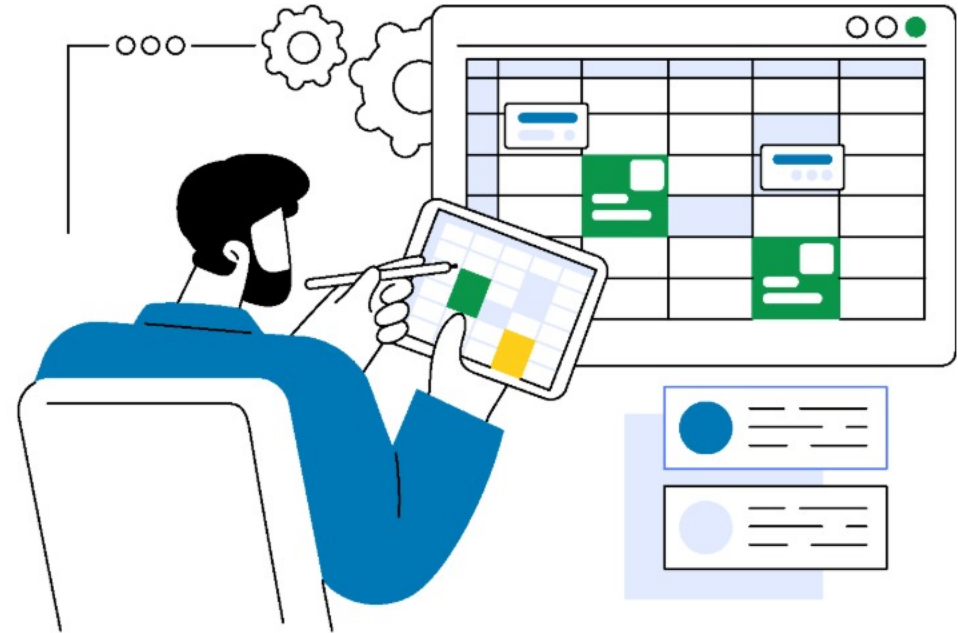
On-the-fly management

Perform management operations from within the reports like resetting password, unlocking user, enabling or disabling user, creating or archiving user mailboxes, and more.



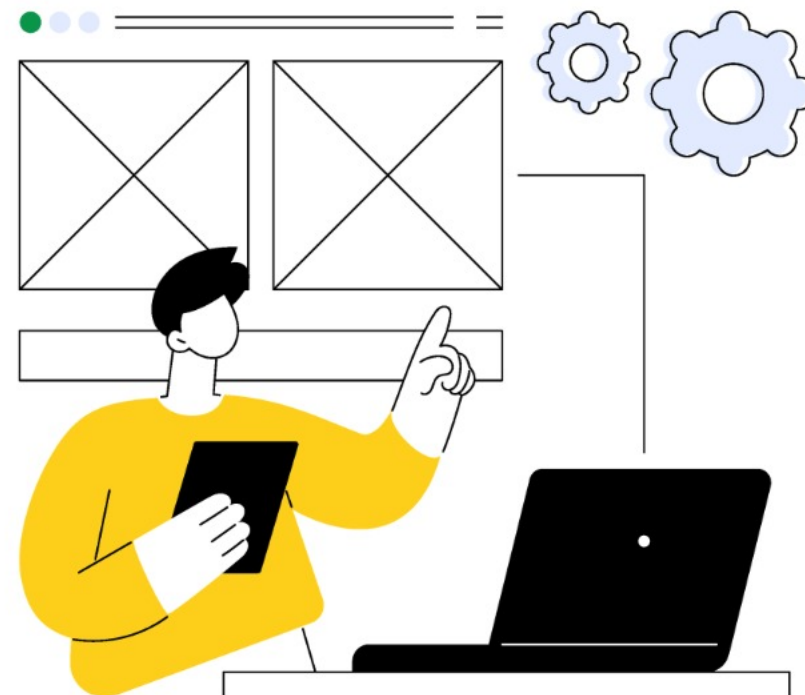
Built-in report scheduler

You can schedule reports to be generated at a specified time and configure sending the required reports to administrator/technicians automatically via email.



Custom reports

Apart from 200+ built-in reports, you can also create your own report that includes only the required attributes, and best suits the needs of your organization by customizing the LDAP Query, applying filter conditions, selecting columns and performing management actions simultaneously.



Compliance reports

Verify your compliance position with the help of predefined reports. If needed, take remedial actions within these reports to ensure your organization complies with PCI, HIPAA, SOX, GDPR, and more.

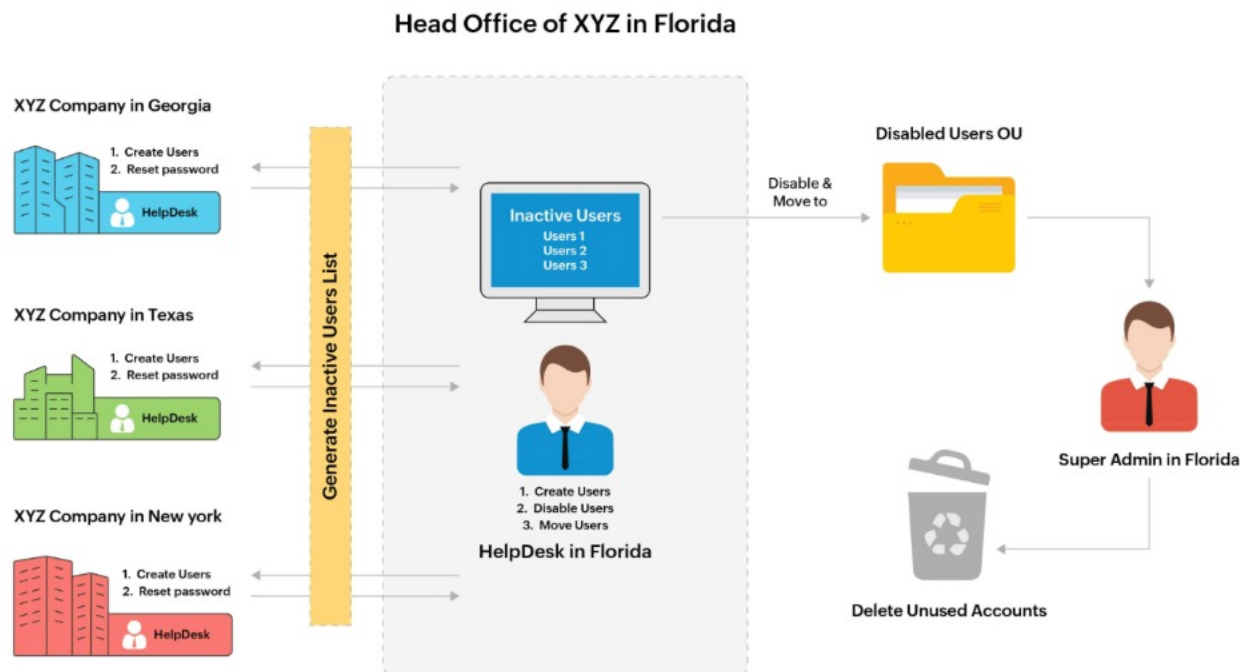


Delegation

Delegate tasks to help desk technicians in AD, Microsoft 365, and Google Workspace based on roles, OUs, groups or sites.

Delegation

With this feature, you can effectively set up help desk delegation in ADManager Plus, allowing your help desk staff to perform specific Active Directory tasks without granting them full administrative control. This helps improve efficiency, reduces the workload on IT administrators, and ensures that only authorized actions are taken within your Active Directory environment.



How delegation helps in ADManager Plus?

- ✓ **Non-invasive delegation**

Verify your compliance position with the help of predefined reports. If needed, take remedial actions within these reports to ensure your organization complies with PCI, HIPAA, SOX, GDPR, and more.

- ✓ **Conditional based access**

Create roles to granularly delegate management and reporting actions based on OU, role, group or site.

- ✓ **Audit reports**

Keep track of the activities performed by all the technicians in your AD environment

Workflow

Exercise control over automated tasks by setting up multi-level workflows to validate and prioritize user requests with efficient SLA management.

How workflow helps?


- ✓ Multilevel workflow that helps assign and prioritize tasks.
- ✓ Manager-based workflow that grants managers granular control over the properties of their team's objects.
- ✓ Track the status of delegated tasks. Monitor and review tasks including automated tasks.

Business Workflow
Define an order of execution for important administrative tasks. [Learn more...](#)


Workflow Name

Description


Workflow Stages


Requester
The one who raises a request for a particular action. [\[Configure\]](#)


→


Reviewer
The one who assesses the request, weighs its pros and cons, and offers recommendations. [\[Configure\]](#)
No. of Reviewers: 1 ▼

→


Approver
The one who possesses the authority to finalize an action. [\[Configure\]](#)
No. of Approvers: 1 ▼

→

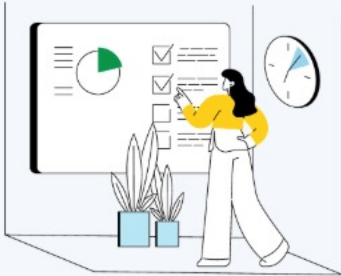

Executor
The one who executes the approved action. [\[Configure\]](#)

[Create Workflow](#) [Cancel](#)

Workflow SLA

Service-level agreements (SLA) in workflow help you take appropriate actions on pending and time sensitive requests in the most efficient manner.

Step 1



Setup conditions based on which the SLA must be executed

Step 2



Specify the time in days, hours or minutes, within which an action must be taken on the request.

Step 3

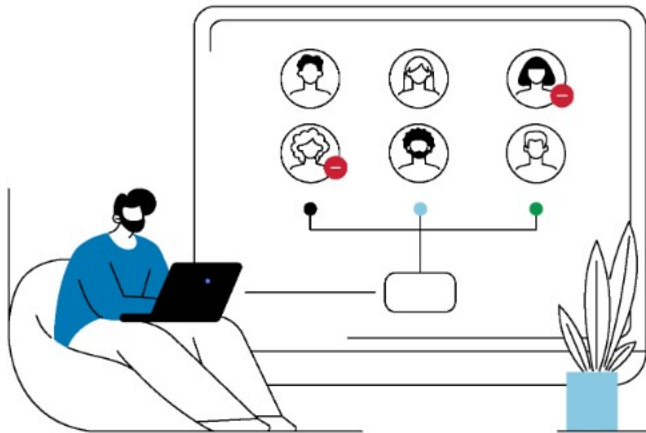
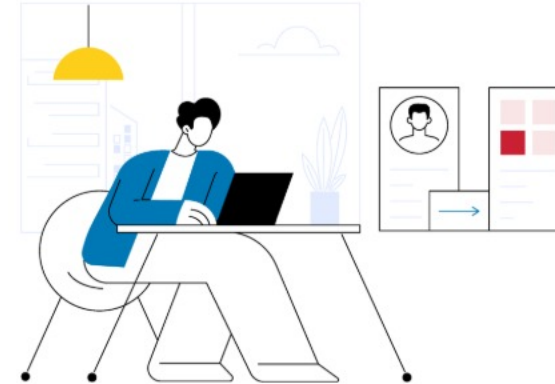


Configure what actions have to be taken when SLAs are violated. You can setup different levels of escalation.

Workflow use-cases

Workflow based User creation

When a new employee joins the organization, there is a series of processes that gets executed like, the HR recruits the employee, requests admin to create an user account. The manager reviews & approves the request and finally, the admin creates the user account in AD. We can automate this whole process using workflow and schedule to repeat it every time an employee joins.



Workflow based disabling of inactive users

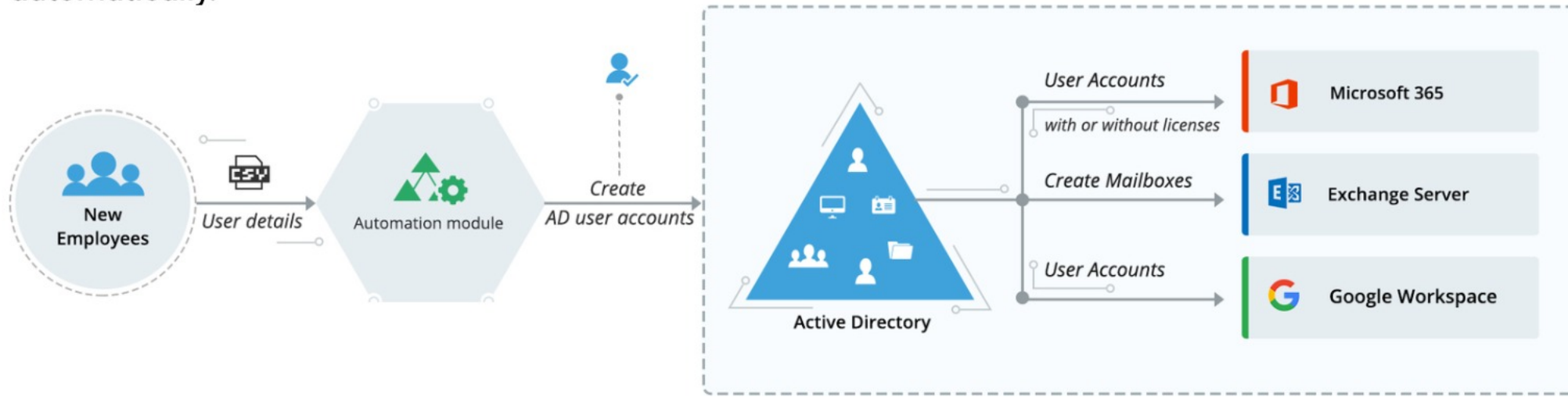
Say a administration wants to disable the accounts of employees who have been absent for a very long time. First, the HR identifies the users who haven't logged in for a while, raises request to disable their accounts which is reviewed by employees' managers and finally disabled by admins. This flow of work can be automated using workflow and made to repeat itself every time an employee's account has to be disabled.

Automation

Using the Automation feature you can configure a task or sequence of tasks and schedule it to be executed at a pre-specified time or interval.

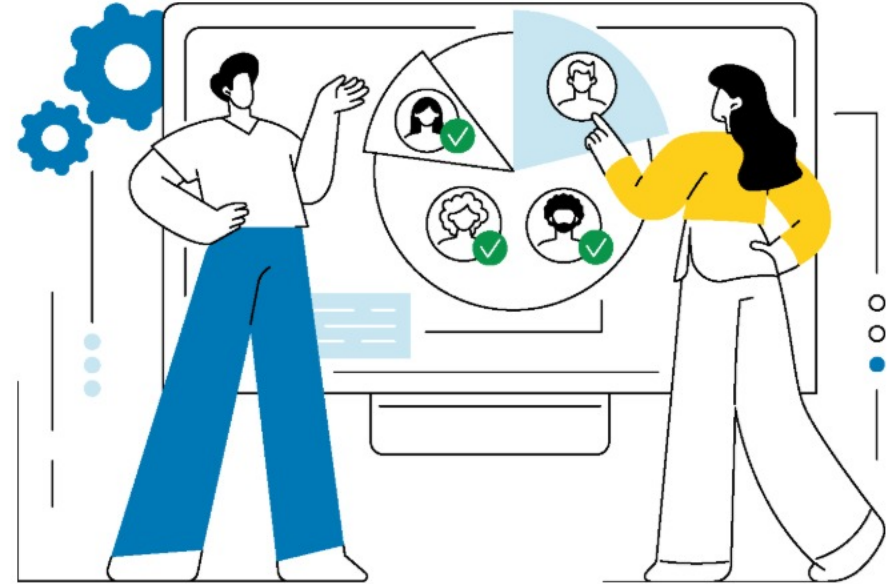
Automation

- ✓ Script-free automation to run crucial standalone tasks such as user creation, password resets, moving computers, and more at specific time intervals.
- ✓ Enforce workflow for controlled automation
- ✓ Automated AD object management with the help of pre-built actions
- ✓ Option of importing user details from a CSV, or external databases or HRMS, for creating AD users automatically.



Orchestration

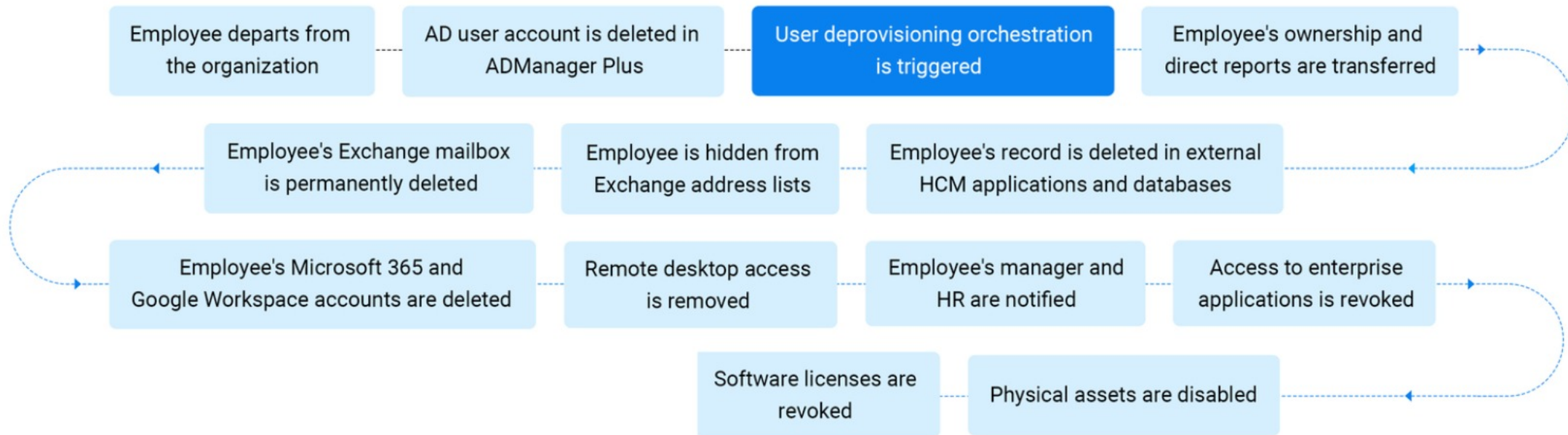
- ✓ Automate a series of user provisioning and deprovisioning tasks in succession at defined time intervals whenever a user or group management task is carried out in ADManager Plus
- ✓ Create, update, and delete users, groups, and their attributes in external applications using webhook templates
- ✓ Build templates easily with drag-and-drop actions



What makes up orchestration?

- ✓ Webhook templates
- ✓ Logic blocks
- ✓ Custom scripts
- ✓ Predefined AD, Exchange, Microsoft 365, and Google Workspace actions
- ✓ Orchestration profile

User deprovisioning using orchestration is one of the major use cases



Risk and compliance

Management of identity and access-related risks and the adherence to compliance requirements with features like identity risk assessment and access certification.

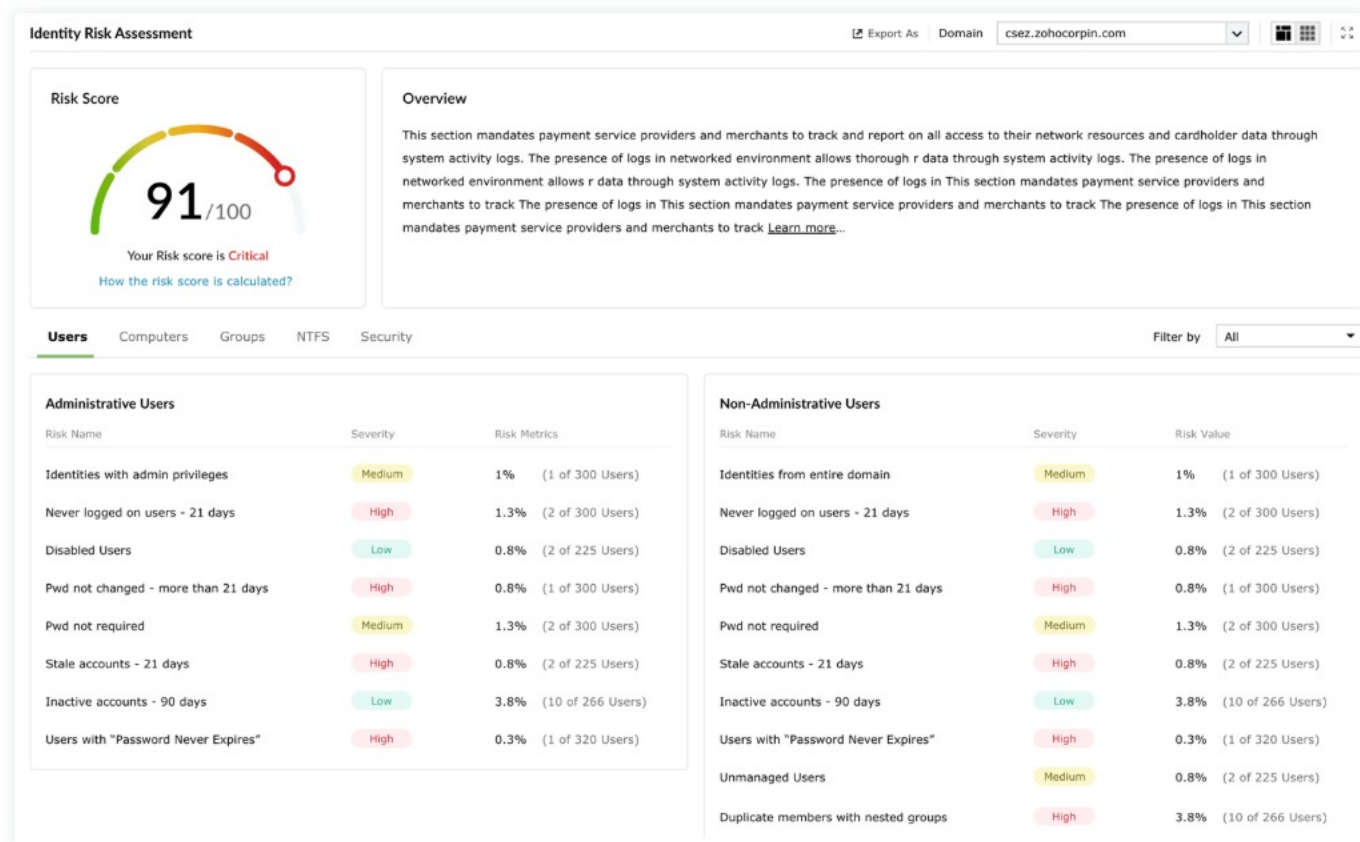
Identity risk assessment

The Identity Risk Assessment report provided by ADManager Plus helps to identify potential risks within your organization and delivers insights into the potential risks lurking in your AD and Microsoft 365.



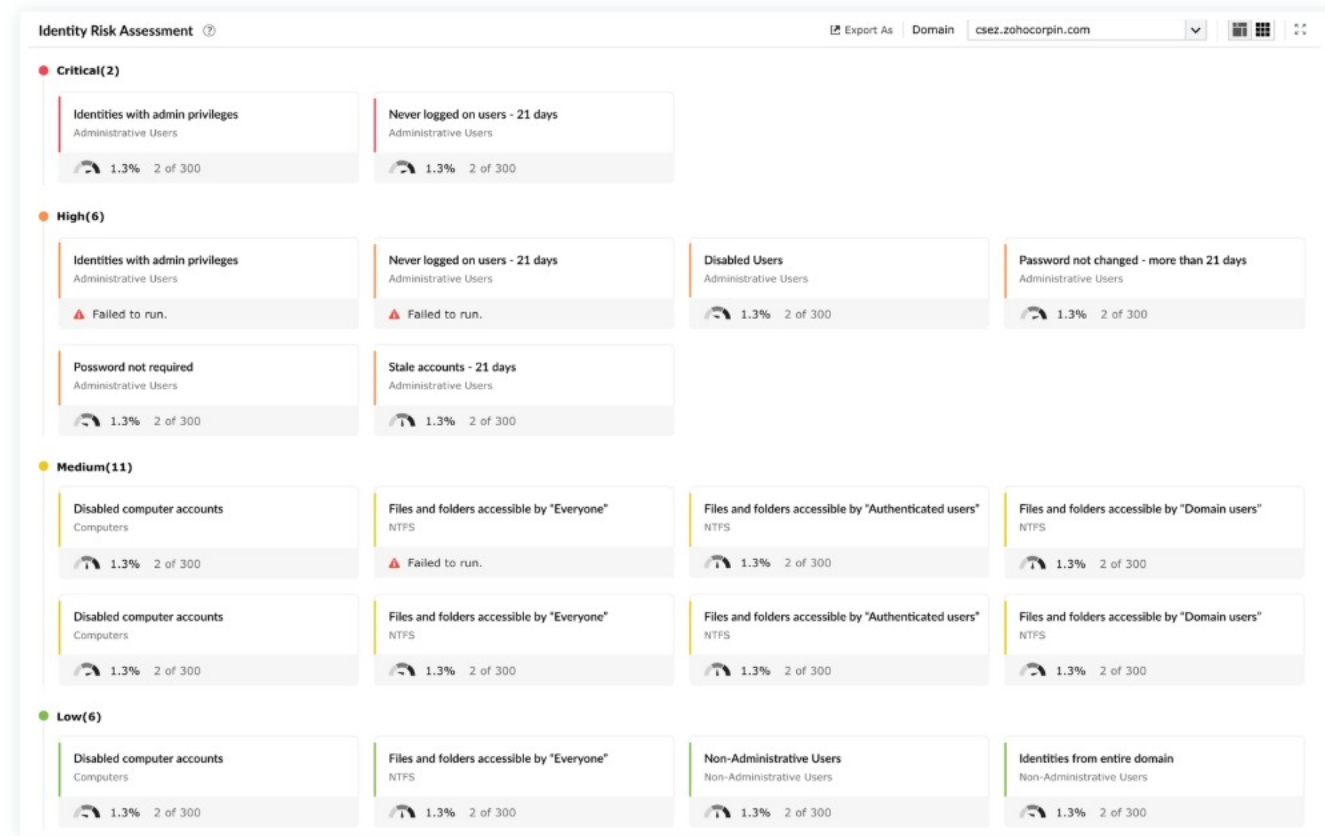
Key highlights identity of risk assessment

- ✓ **Risk score dashboard:** Graphical dashboard provides security settings risk score with insights on risk indicators categorized by severity.



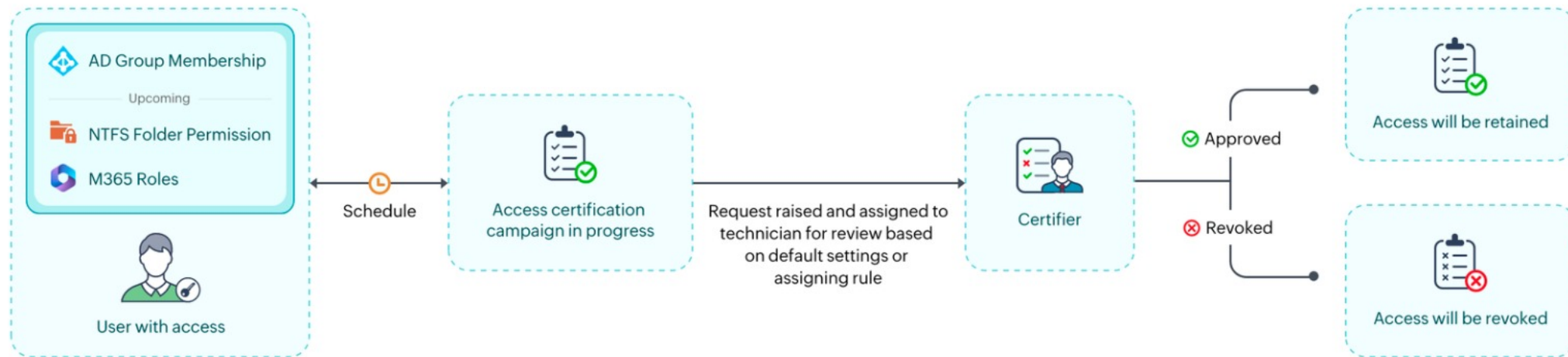
Key highlights identity of risk assessment

- ✓ **Incident management:** Utilize reports on risk indicators, providing details on impact & remediation actions. Proactively take necessary actions from the tool.



Access certification campaign

With access certification, you can create audit campaigns to regularly review the access permissions, including NTFS permissions, of AD and Microsoft users and groups. You can also review Exchange mailbox access and Microsoft Teams channel memberships. Assign certifiers to approve or revoke access as required and track the progress of access certification campaigns.



Key highlights of access certification campaign

- ✓ Mitigate privilege abuse
- ✓ Simplify the auditing process
- ✓ Prevent privilege creep
- ✓ Streamle access management
- ✓ Enhancing your adherence to compliance

Compliance management

With the the risk assessment and access certification campaign features in place, compliance to mandates like GDPR, PCI DSS, SOX. HIPAA and other is made easier, as an effective incident management technique mandated them.



Risk exposure management

The Risk Exposure Management report in ADManager Plus offers a real-time, graph-based view of how privilege escalation can occur within your AD environment. By mapping potential attack paths leading to highly privileged built-in and custom groups, it reveals exploitable relationships that traditional tools or manual audits often miss.

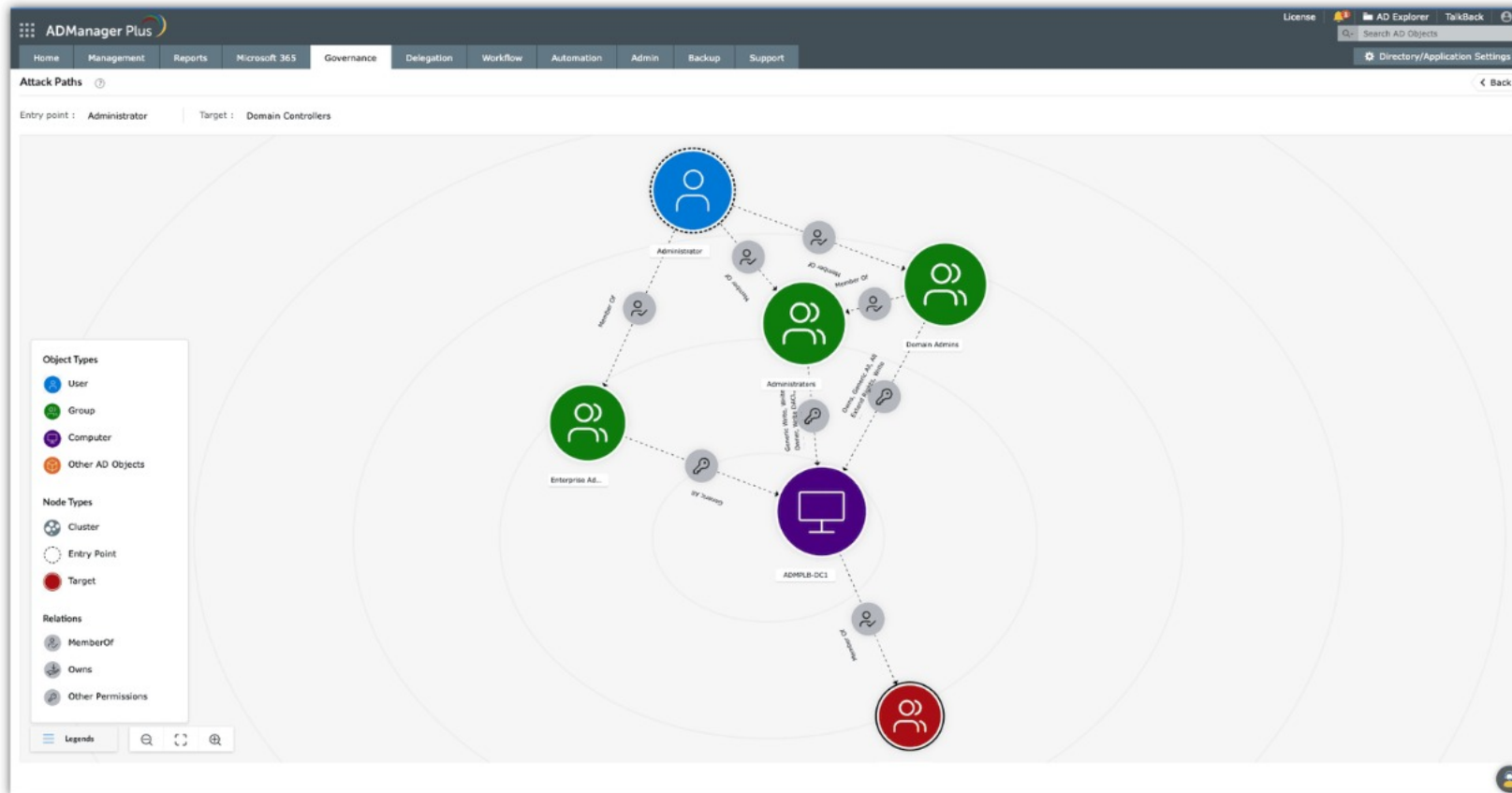
Key highlights of risk exposure management

- ✓ **Continuous monitoring:** Track the exposure of privileged groups and identify new threat paths as access changes occur in your AD environment, ensuring that your visibility into privilege risks stays current.

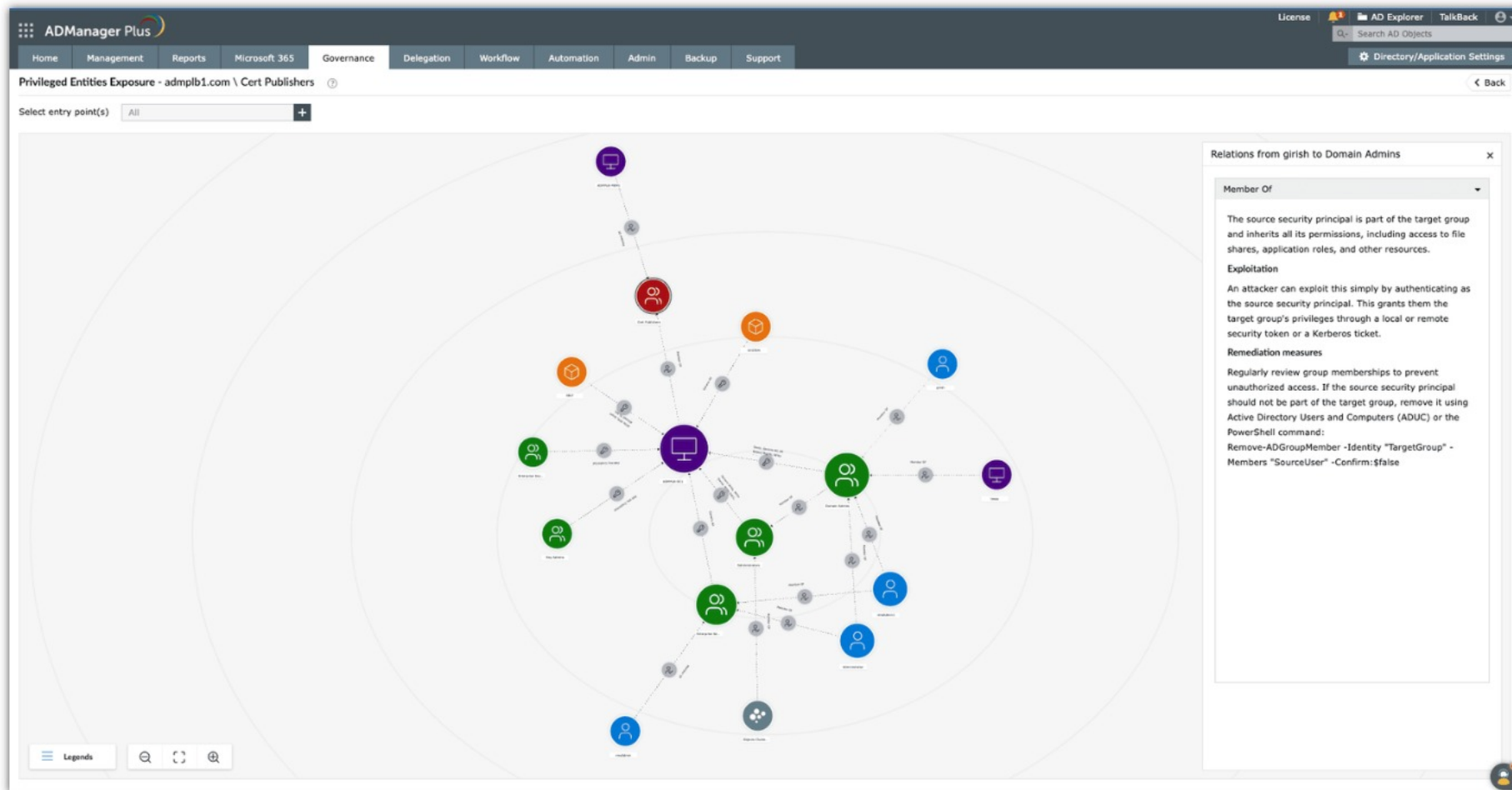
The screenshot displays the ADManager Plus Risk Exposure Management dashboard. At the top, there's a navigation bar with tabs like Home, Management, Reports, Microsoft 365, Governance, Delegation, Workflow, Automation, Admin, Backup, and Support. The main header shows 'Risk Exposure Management' with a search bar and a 'Select Domain' dropdown set to 'admplb1.com'. Below this, two summary cards are visible: 'Privileged Entities' with a count of 14 and 'Attack Paths' with a count of 75. An 'Overview' section provides a brief description of the tool's purpose. The main content area is titled 'Attack Paths' and includes a sub-tab 'Privileged Entities Exposure'. A table below this tab lists various attack paths, showing the entry point, parent, target, relation, and attack flow. The table is paginated to show 1-25 of 75 items.

Entry point	Parent	Target	Relation	Attack Flow
Administrator	Enterprise Admins	Enterprise Admins	Member Of	View
Administrator	Domain Admins	Domain Controllers	Member Of	View
Administrator	Administrators	Administrators	Member Of	View
Administrator	Domain Admins	Administrators	Member Of	View
Administrator	Enterprise Admins	Cert Publishers	Member Of	View
Administrator	Administrators	Cert Publishers	Member Of	View
Administrator	Enterprise Admins	Domain Controllers	Member Of	View
Administrator	Schema Admins	Schema Admins	Member Of	View
Administrator	Domain Admins	Cert Publishers	Member Of	View
Administrator	Administrators	Domain Controllers	Member Of	View
Administrator	Domain Admins	Domain Admins	Member Of	View
Administrators	ADMPLB-DC1	Cert Publishers	Generic Write, Write Owner, Write DACL, All Extend Rights	View
Administrators	ADMPLB-DC1	Domain Controllers	Generic Write, Write Owner, Write DACL, All Extend Rights	View
ADMPLB-DC1	Domain Controllers	Domain Controllers	Member Of	View
ADMPLB-DC1	Cert Publishers	Cert Publishers	Member Of	View
ADMPLB-MEM1	Cert Publishers	Cert Publishers	Member Of	View
CN=srvAcc2,CN=Managed Service Accounts,DC=admplb1,DC=com	Administrators	Domain Controllers	Member Of	View
CN=srvAcc2,CN=Managed Service Accounts,DC=admplb1,DC=com	Administrators	Cert Publishers	Member Of	View

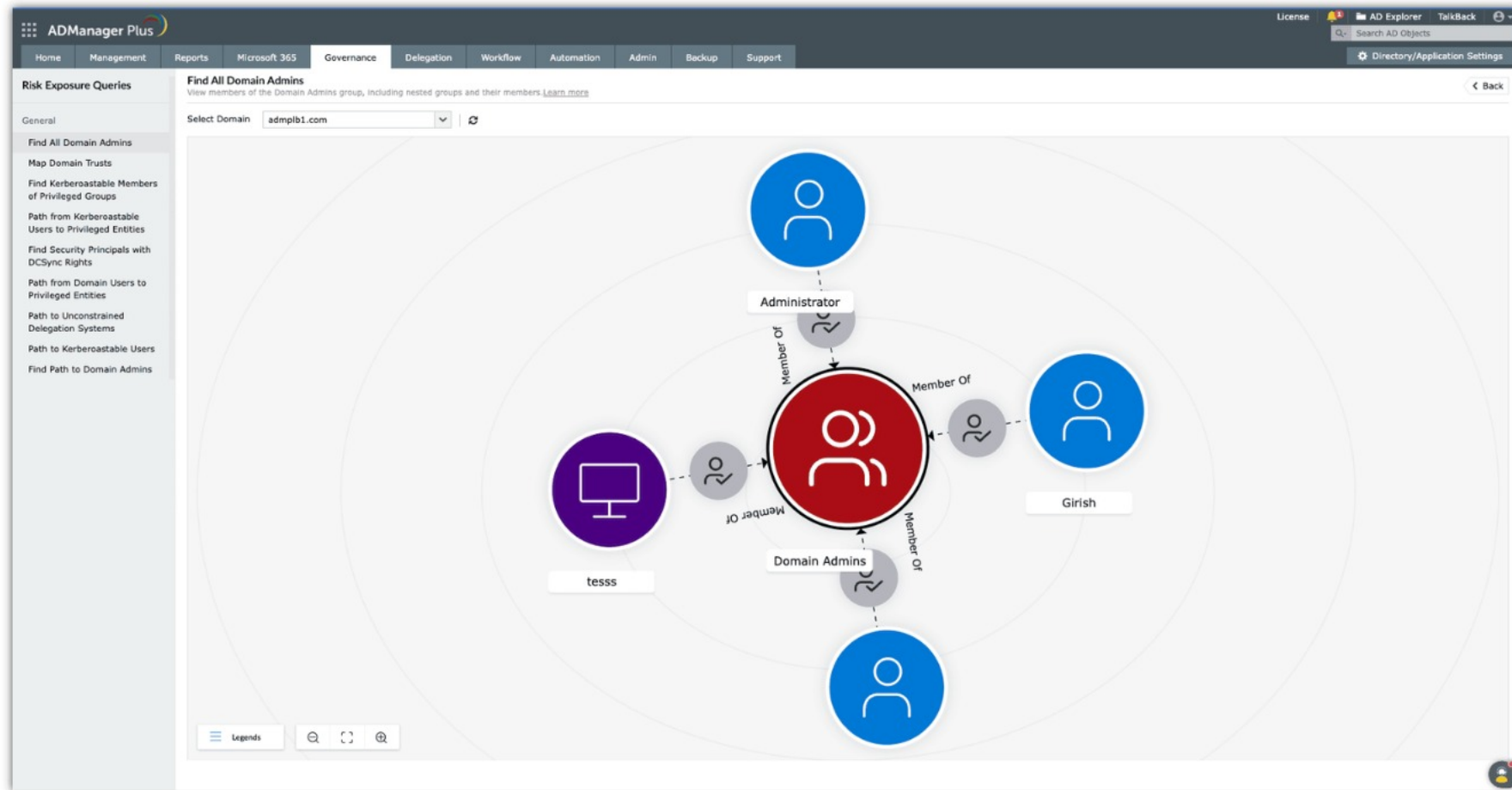
- ✓ **Comprehensive risk mapping:** Focus your mitigation efforts where they matter most; ADManager Plus maps and surfaces the most critical privilege escalation paths, helping you prioritize high-impact remediation without digging through raw data dumps
- ✓ **Attack path visualization:** Clearly see and understand how attackers could possibly leverage the access to reach Domain Admins, Account Operators, and other high-value groups



- ✓ **Remediation measures:** ADManager Plus doesn't just identify vulnerabilities; it also provides clear, actionable remediation measures and suggestions that help organizations implement targeted solutions to mitigate the identified risks effectively



- ✓ **A built-in privileged queries library:** Accelerate your analysis with prebuilt queries to detect Kerberoastable users, DCSync rights, domain trust paths, and other critical AD privilege risk indicators



Integrations

ADManager Plus provides out-of-the-box integrations with third-party applications. Webhook feature is also available to establish communication between applications and services effortlessly.

Integrations

ADManager Plus supports integrations with:



ITSM/HelpDesk tools



HCM applications



SIEM applications

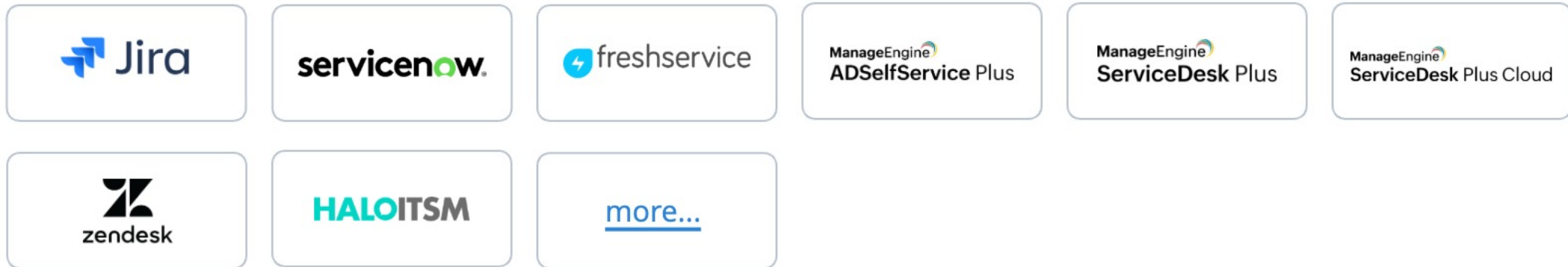


Databases

Integration with ITSM and help desk softwares

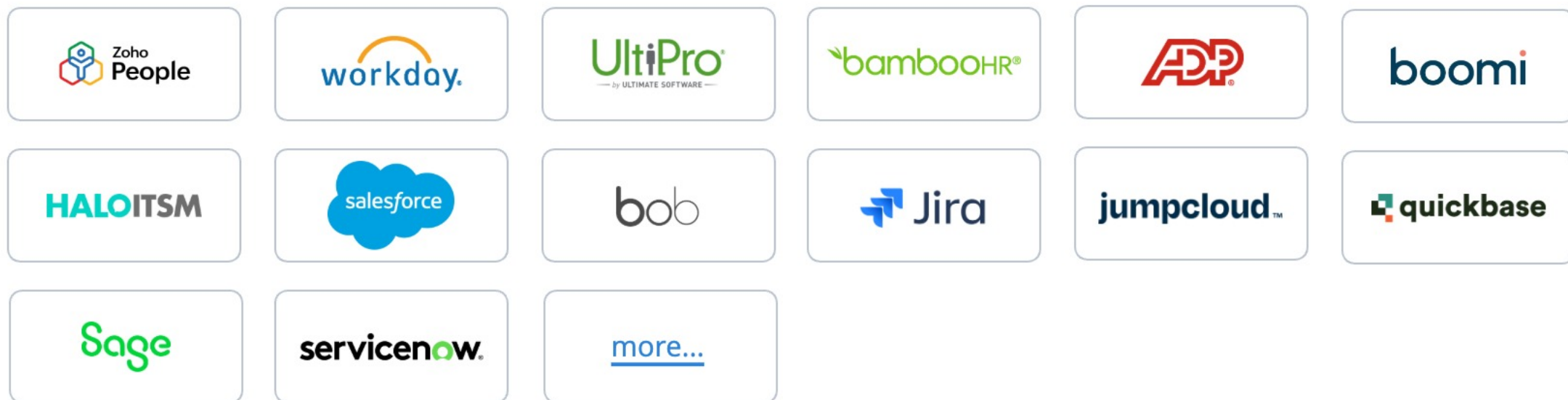
ADManager Plus integration with help desk tools assists AD administrators and technicians with carrying out AD management actions without using multiple tools. ADManager Plus currently integrates with below applications,

ITSM and help desk applications that can be integrated with ADManager Plus:



Integration with HCM applications

ADManager Plus helps integrate with popular HCM tools listed below, making AD account management easy for administrators and HR managers alike, with complete hands-free user provisioning, management, and deprovisioning. You can also custom integrate any other HCM application.



Integration with SIEM applications

ADManager Plus integrates with SIEM applications to automatically send all logs of AD operations in ADManager Plus to a SIEM tool. SIEM software uses AD log data to identify and prevent potential attacks, and analyze security breaches.

SIM applications that can be integrated with ADManager Plus:

The Splunk logo, featuring the word "splunk" in a bold, lowercase, sans-serif font, followed by a right-pointing chevron symbol.The RAPID7 logo, with "RAPID" in bold black uppercase letters and "7" in a stylized orange font.The Freshservice logo, featuring a blue circular icon with a white lightning bolt, followed by the word "freshservice" in a lowercase, sans-serif font.The Syslog Server logo, with the words "Syslog Server" in a bold, black, sans-serif font.The ManageEngine Log360 logo, with "ManageEngine" in a small black font above "Log360" in a larger black font, and a small rainbow-colored circular icon to the right.A blue, underlined text link that says "more...".

Integration with external databases

ADManager Plus' integration with MS SQL and Oracle databases makes AD account management easy for IT administrators and HR managers alike, with complete hands-free user provisioning, management, and deprovisioning.

Database



MS SQL



Oracle



Azure SQL



AWS SQL

Backup and recovery

Back up your AD, Azure Active Directory, and Google Workspace environments from a single console and restore any object whenever you need it.



Backup and recovery



Azure AD

Backup and restore Azure AD objects including users, groups, devices, applications, directory roles and domains.



Backup and recovery

Take backups and perform restorations of Google Workspace mailboxes, contacts, user drives, and calendar items



AD

Back up and restore important AD objects, such as users, computers, contacts, groups, OUs, and GPOs, without directly accessing the DC.

Backup

You can use the below functionalities while performing backup,

- ✓ **Incremental backup:** Expedite the backup process and minimize the utilization of storage space by only backing up the changes made since the last backup. Subsequent backups are stored as versions.
- ✓ **Full backup:** Regularly perform complete backups of all the objects present in your domain.
- ✓ **Scheduled backup:** Schedule backups for a specific date, day, and time



Recovery

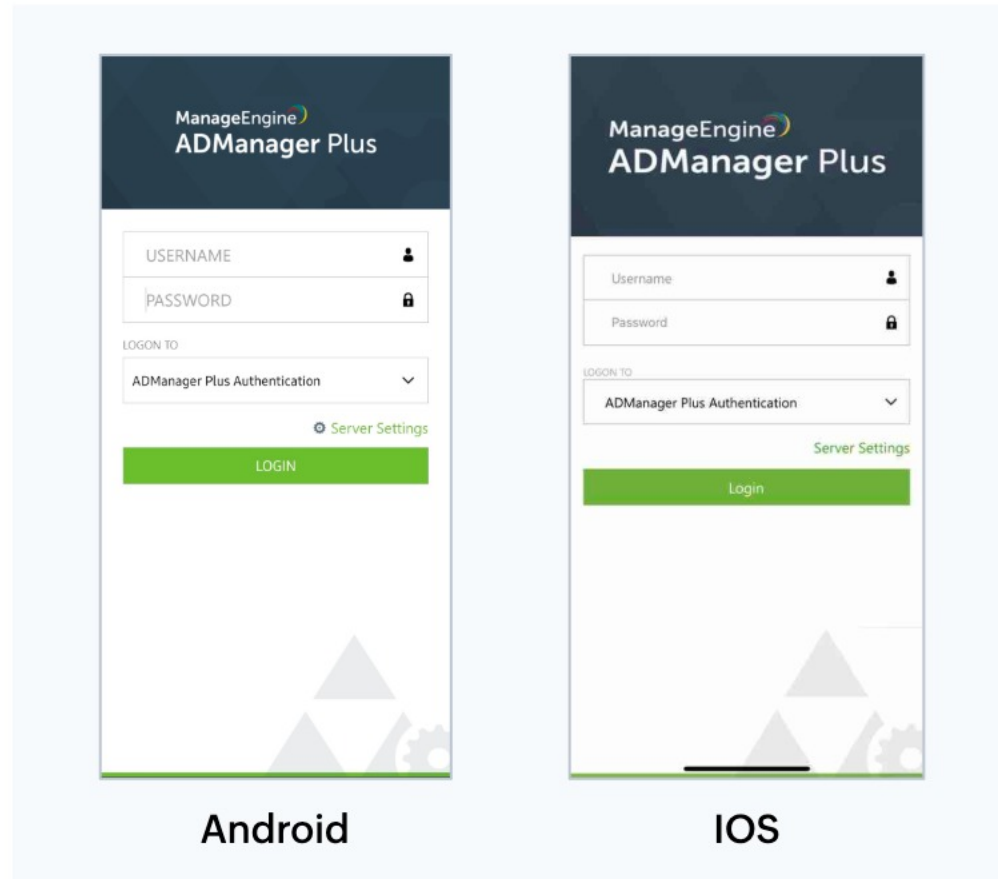
You can use the below functionalities while recovering data from backup,

- ✓ **Object and attribute-level restoration:** Restore only the required objects or individual attributes of particular objects.
- ✓ **Restart-free recovery:** Recover objects completely or granularly without having to restart your DCs.



Android & iOS support

ADManager Plus Mobile offers on the go Active Directory management and reporting with support for both Android and iOS platforms.



How ADManager Plus helps enterprises solve business challenges?

Ensurem, an insurance marketplace, had trouble streamlining onboarding and offboarding of AD users

Solution: ADManager Plus' ability to integrate with custom HCM solutions helped Ensurem automate user onboarding and offboarding without any hassles

Al Ahli Bank of Kuwait (ABK) found it difficult to identify and manage inactive accounts in its AD network

Solution: ADManager Plus' reports provided visibility into dormant accounts and helped ABK declutter its network in one swift action

ADManager Plus' licensing

ADManager Plus is licensed based on the number of domain and help desk technicians and the edition purchased

Standard	Professional	Add-ons
Starts at \$595	Starts at \$795	Backup and Recovery Governance, Risk and Compliance

For more details on pricing, please visit our [store](#) or [pricing](#) page