ManageEngine
ADManager Plus

The JML automation blueprint:

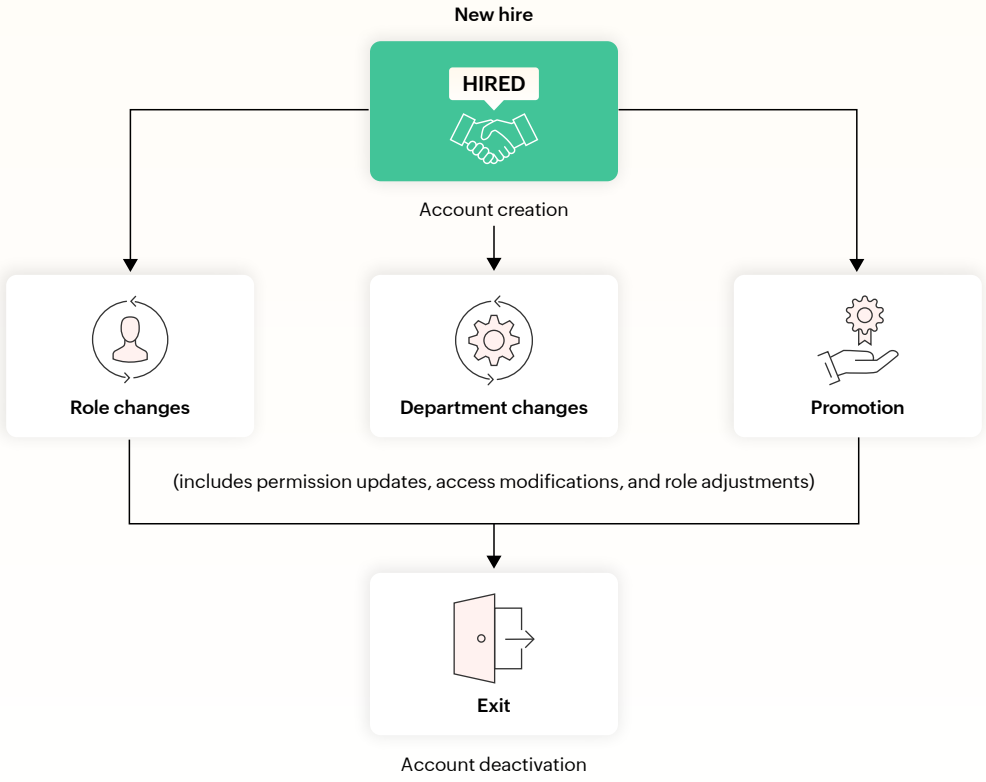
A complete guide to **joiners, movers,** and **leavers automation**

Applicable for enterprises of all industries

Table of **contents**

What is JML life cycle management?

Joiner-mover-leaver life cycle management (JML) defines the structured approach to managing user accounts and access rights throughout an employee's tenure within an organization. This critical IT process ensures security, compliance, and operational efficiency by automating the provisioning, modification, and deprovisioning of user accounts and associated resources. Effective JML management minimizes risks, streamlines IT operations, and enhances user productivity.



1. Joiners (onboarding)

When new employees join your organization, they need immediate access to systems, applications, and resources to be productive from day one. The onboarding process includes:

User account creation:
Establishing accounts across multiple systems (e.g., Active Directory, Microsoft 365, and Google Workspace).

Permission assignment:
Granting appropriate access rights and group memberships based on the employee's role, department, and location.

Resource provisioning:
Providing access to necessary files, shared folders, and applications.

Communication setup:
Setting up email accounts, distribution groups, and communication tools.

Security policy configuration:
Applying relevant security policies and baseline configurations.

2. **Movers** (internal changes)

Employee roles, departments, and responsibilities frequently change over time. The mover process involves adjusting access rights to align with new responsibilities, which include:

Role-based access updates:
Modifying permissions and group memberships to reflect new roles.

Department transfers:
Adjusting access based on changes in departmental affiliation.

Promotions and demotions:
Updating privilege levels according to changes in organizational hierarchy.

Temporary access grants:
Providing time-limited access for specific projects or roles, with automated revocation.

Periodic access reviews:
Conducting regular validations to ensure users retain only the necessary permissions, adhering to the principle of least privilege.

Location changes:
Updating access related to geographical or site-specific resources.

3. Leavers (Offboarding)

When employees leave the organization, proper and timely deprovisioning is crucial for maintaining security and compliance. The offboarding process includes:

Immediate access removal:
Revoking all system and application access to prevent unauthorized use.

Account disabling or deletion:
Securely disabling or deleting user accounts across all platforms.

Data backup and transfer:
Ensuring critical data is backed up and transferred to appropriate custodians.

Equipment recovery:
Managing the return of company assets.

Compliance documentation:
Generating and retaining records of the offboarding process for audit purposes.

The tangled wires of manual JML management

In today's hyper-digital world, where operational speed is paramount, many HR and IT teams still rely on manual processes for JML management. This often translates into excessive paperwork; convoluted email chains; and tedious, repetitive tasks that consume significant IT resources and introduce substantial risks. Each new hire, role change, or employee departure triggers a cascade of manual interventions by the IT team.

Imagine a different scenario. What if your JML life cycle could largely manage itself? With ADManager Plus, this vision becomes a reality. Instead of your IT team manually creating accounts across multiple systems, granting varied access, and configuring permissions for a new employee, these actions occur automatically.

ADManager Plus serves as a centralized command center for automating your employees' entire identity life cycle. This guide will illustrate how you can transition from JML chaos to orchestrated efficiency, detailing how ADManager Plus enables rapid employee onboarding; precise handling of role changes; and secure, gap-free offboarding. Whether you are an IT administrator seeking practical solutions, a potential customer evaluating options, or a partner aiming to understand the capabilities of ADManager Plus, this guide provides comprehensive insights.

The pain points of manual JML management

Reliance on manual JML processes incurs significant hidden costs and operational inefficiencies:

Time-consuming:
Manually creating and modifying accounts across various systems consumes valuable IT hours that could be dedicated to strategic initiatives.

Inconsistency:
Manual processes often result in inconsistent configurations and access privileges across users and systems, complicating management and auditing.

Error-prone:
Human error during data entry or permission assignment can lead to incorrect access rights, security vulnerabilities, or forgotten steps, potentially compromising data integrity.

Compliance challenges:
Achieving and demonstrating compliance with regulatory standards (e.g., the GDPR, HIPAA, and SOX) becomes difficult due to inconsistent, unaudited, and non-standardized processes.

Security risks:
Delayed or incomplete offboarding procedures can leave former employees with unauthorized access to sensitive company data, increasing the risk of data breaches and insider threats.

Poor user experience:
Delays in onboarding or access adjustments can negatively impact employee productivity and morale, hindering their ability to perform their duties effectively from the outset.

The blueprint for better identity management: JML automation

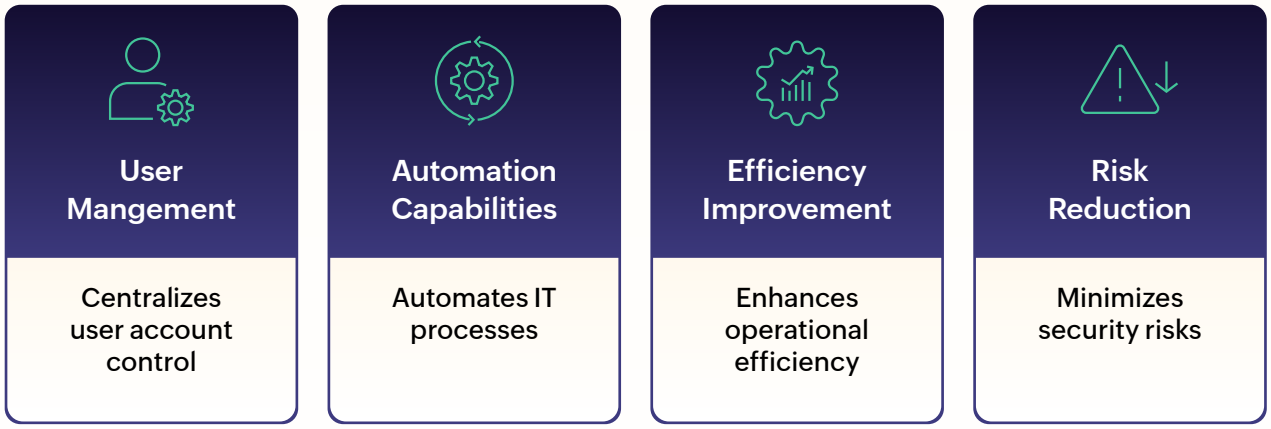
The JML life cycle is a continuous and dynamic process within any organization. Effectively managing each stage is paramount for operational efficiency, robust data security, and regulatory compliance. Without automation, this cycle can become a significant drain on IT resources, leading to the pain points described above.

JML automation transforms these complex, manual workflows into streamlined, policy-driven processes. By leveraging automation, organizations can ensure that user access is provisioned, modified, and deprovisioned accurately and promptly, aligning with business needs and security policies.

Introducing ADManager Plus: Your JML automation solution

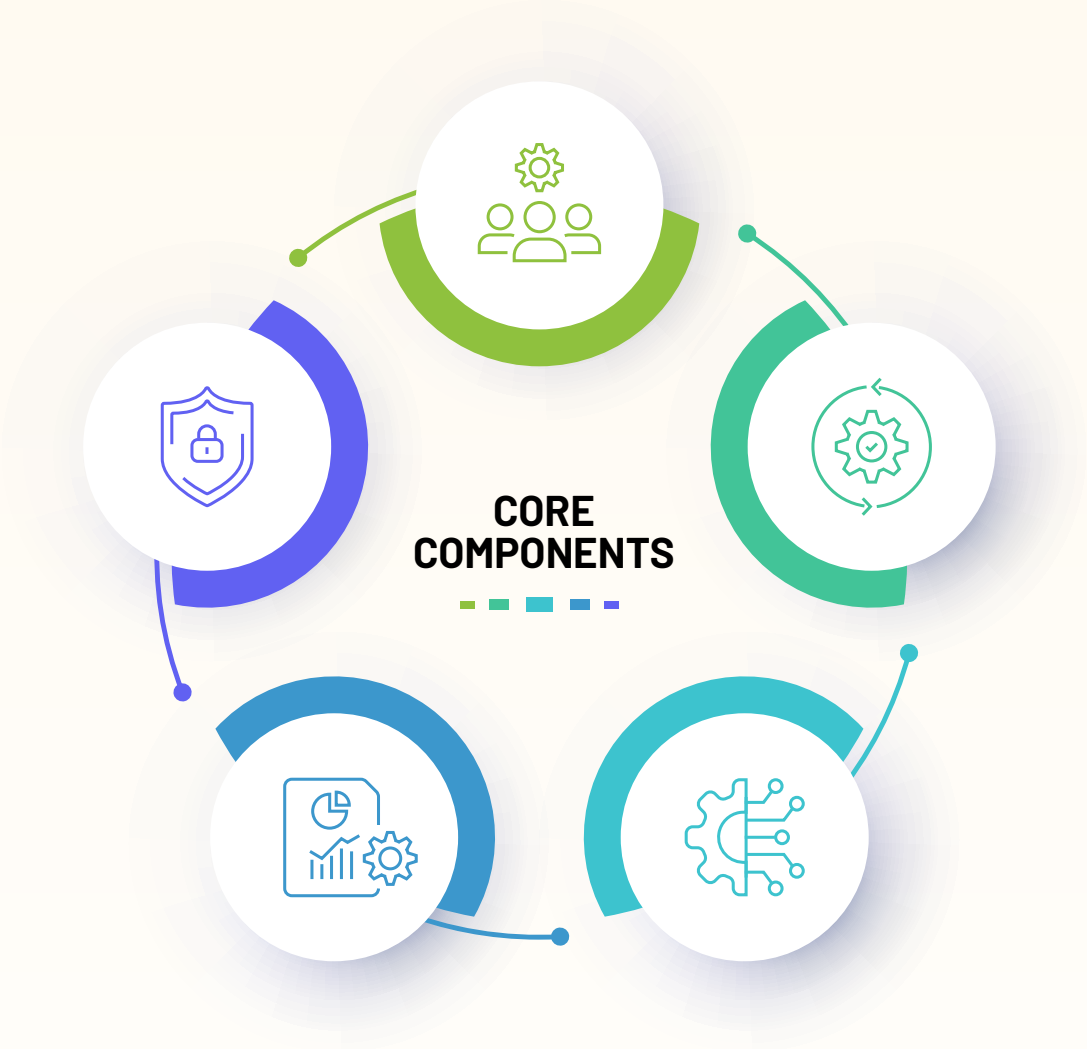
ADManager Plus is a comprehensive Active Directory and identity governance and access management solution specifically designed to empower organizations to automate every stage of the JML life cycle. By centralizing user management and providing powerful automation capabilities, ADManager Plus effectively eliminates the inefficiencies and risks associated with manual processes. It serves as a unified platform for managing user identities across on-premises Active Directory, Microsoft 365, Google Workspace, and other integrated systems.

Streamlining IT Management with ADManager Plus



Technical architecture

ADManager Plus operates through a secure, scalable, and robust architecture designed for high availability and performance in enterprise environments.



1. **Management console**
   Web-based interface configuration and monitoring

2. **Workflow engine**
   Processes automation rules and approval chanins

3. **Integration hub**
   Handies connections to external syatems

4. **Reporting engine**
   Generates insights and compliance documentation

5. **Security layer**
   Ensures secure communication and access control

Key features for JML automation

ADManager Plus provides a robust set of features specifically engineered to streamline and secure the entire JML life cycle.

1. Automated user provisioning

- **Template-based account creation:** Utilize predefined templates to ensure consistent, error-free user account setup across various systems, enforcing standardized naming conventions and attribute population.
- **Bulk operations:** Efficiently create, modify, or delete multiple user accounts simultaneously, significantly reducing manual effort for large-scale operations.
- **Seamless integration:** Integrate directly with HR applications (e.g., Workday, SAP, or BambooHR via API or CSV import) to automatically trigger user account creation upon new employee data entry.
- **Multi-domain and multi-tenant support:** Manage user accounts across multiple Active Directory domains, Microsoft 365 tenants, and Google Workspace instances from a single, centralized console.

2. Workflow automation

- **Intuitive workflow designer:** Create approval processes and task sequences without requiring any coding, enabling IT administrators to easily define JML workflows.
- **Multi-level approvals:** Implement hierarchical approval chains for sensitive JML actions, ensuring proper oversight and adherence to organizational policies.
- **Automated notifications:** Send customized messages to all technicians and users who need to be informed of status updates and required actions.

3. Role-based access control

- **Intelligent group membership:**
  Assign users to appropriate security and distribution groups based on their role, department, or other attributes with intelligent recommendations.

- **Temporary access granting:**
  Provide time-limited group memberships or permissions that automatically expire and revoke access after a specified duration, ideal for project-based roles or contractors.

- **Scheduled access reviews:**
  Perform periodic validation of user permissions through access certification campaigns, ensuring users maintain only the necessary access and adhering to the principle of least privilege.

4. Integration capabilities

- **HR systems:**
  Leverage direct integration with leading HCM platforms like SAP, Workday, BambooHR and support for custom HR solutions via APIs and webhooks.

- **Cloud platforms:**
  Seamlessly manage identities and licenses across Microsoft 365, Microsoft Entra ID, and Google Workspace.

- **Ticketing systems:**
  Integrate with ITSM platforms such as ServiceNow and Jira Service Management, allowing JML requests to be initiated and tracked through help desk tickets.

- **Security systems:**
  Integrate with SIEM tools like Splunk, Syslog, PowerBI, and EventLog Analyzer for enhanced security monitoring, auditing, and compliance reporting.

5. Comprehensive reporting and auditing

- **Real-time dashboard:**
  A customizable dashboard provides an at-a-glance overview of JML activities, request statuses, and key metrics, offering real-time operational insights.

- **Compliance reports:**
  Prebuilt reports tailored to common regulatory standards such as HIPAA, SOX, the GDPR, the PCI DSS, and the GLBA simplify the process of demonstrating compliance.

- **Custom reports:**
  Create specific reports to meet unique organizational requirements or internal audit needs.

- **Detailed audit trails:**
  Maintain a complete and immutable log of all JML activities, including who performed what action, when, and on which object. This ensures transparency and accountability, and provides irrefutable evidence for forensic analysis or compliance audits.

The joiner journey: Automated onboarding

Getting new employees productive quickly and securely is paramount for any organization. With ADManager Plus, the entire user provisioning process can be automated, ensuring a smooth, consistent, and secure experience from day one.

Streamlined account creation | Role-based access control

Streamlined account creation

ADManager Plus eliminates manual account setups by automating user account creation across various systems the moment a new hire joins. This ensures immediate access to necessary tools, significantly boosting productivity from day one.

ADManager Plus integrates seamlessly with your HR solutions such as UltiPro, Workday, BambooHR, and others (via APIs). This integration enables automatic user creation in Active Directory, Microsoft 365, and Google Workspace based on data from your HR system.

Furthermore, user creation templates ensure consistent, error-free setup by allowing you to predefine user attributes, naming conventions (e.g., for usernames and email addresses), and default group memberships. You can even apply custom naming formats to avoid duplicates during bulk provisioning, ensuring unique and standardized identity attributes.

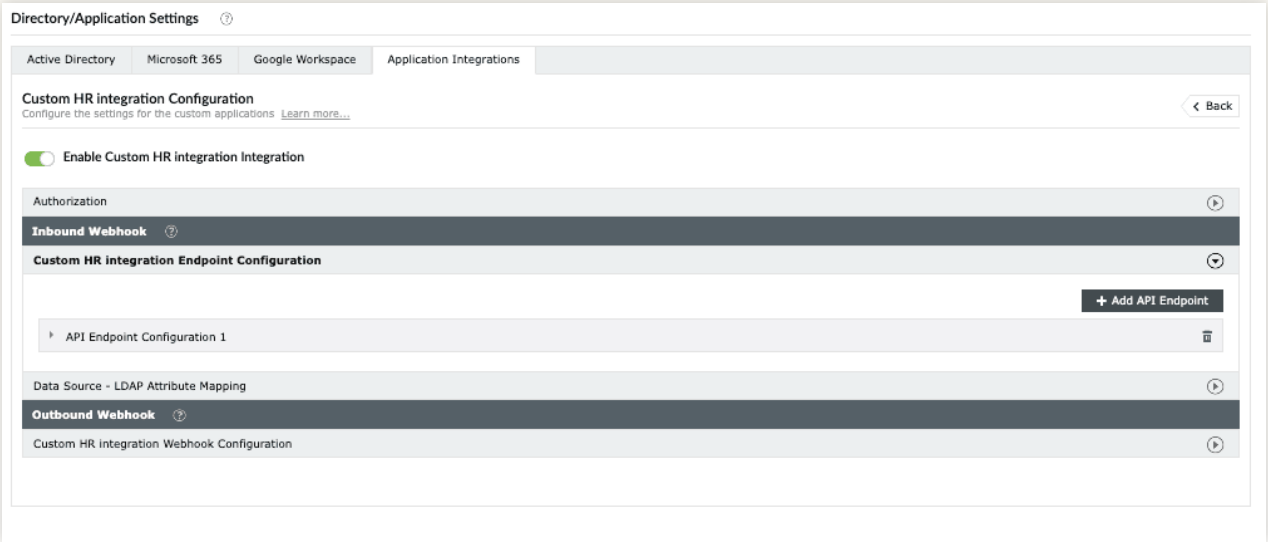


Figure 1: Custom HR application integration.

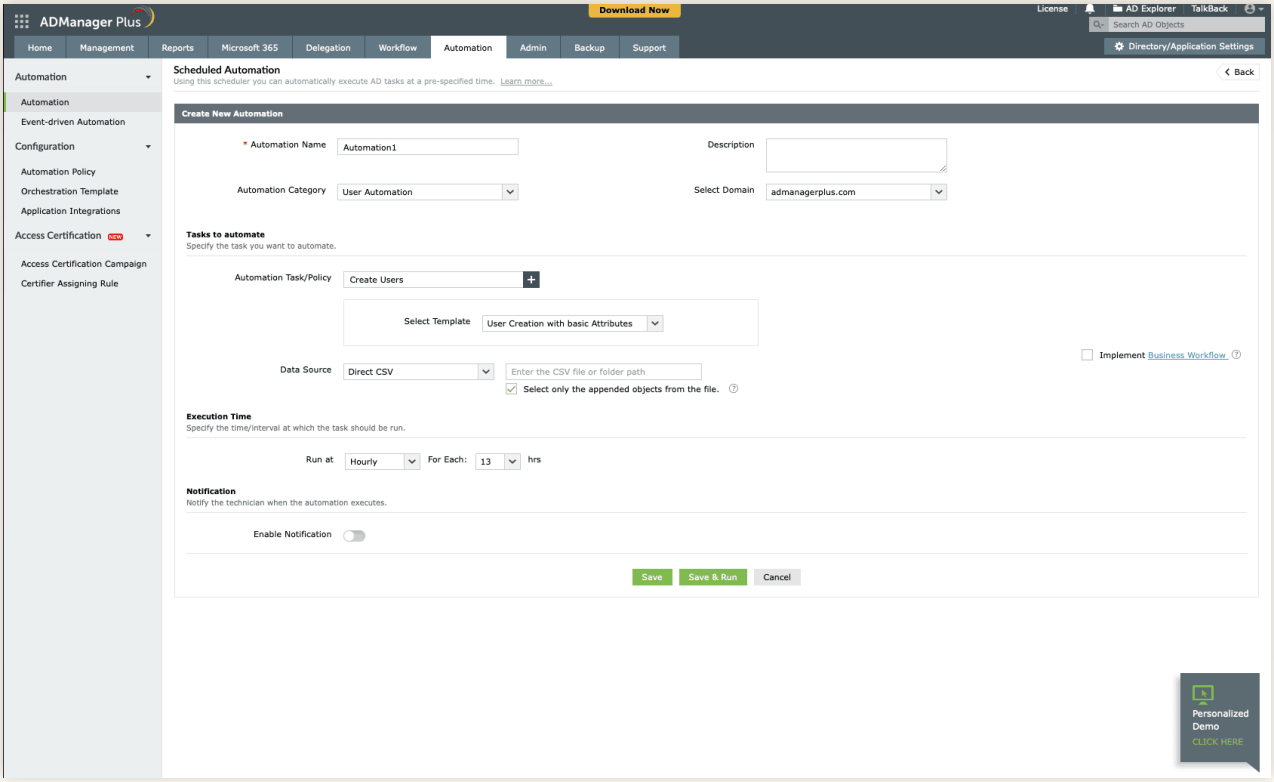


Figure 2: Automation for user onboarding.

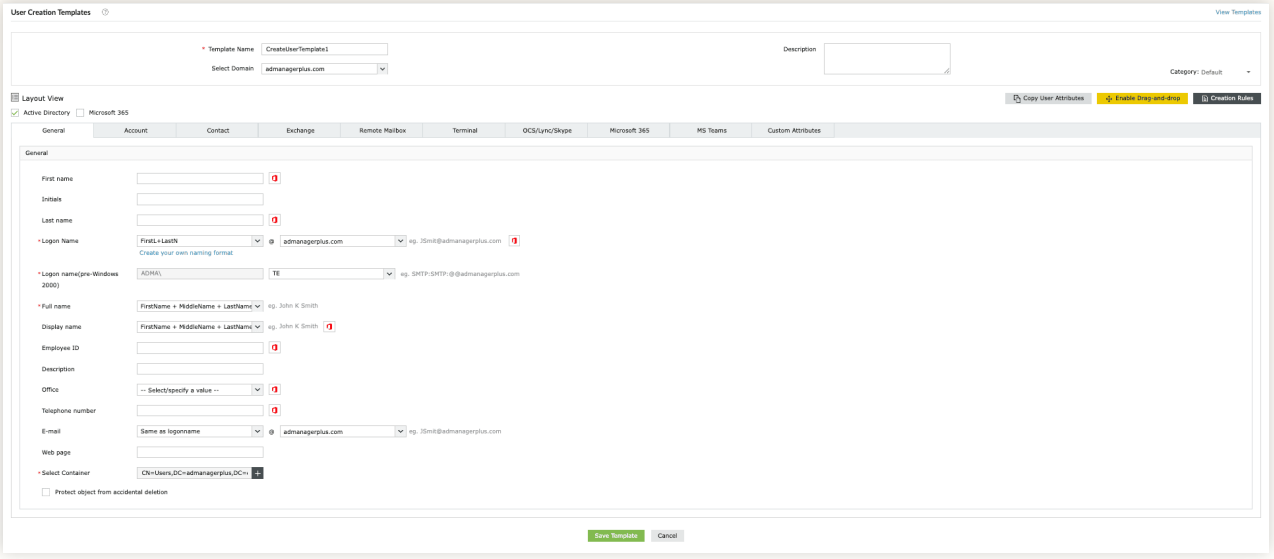


Figure 3: User creation template configuration.

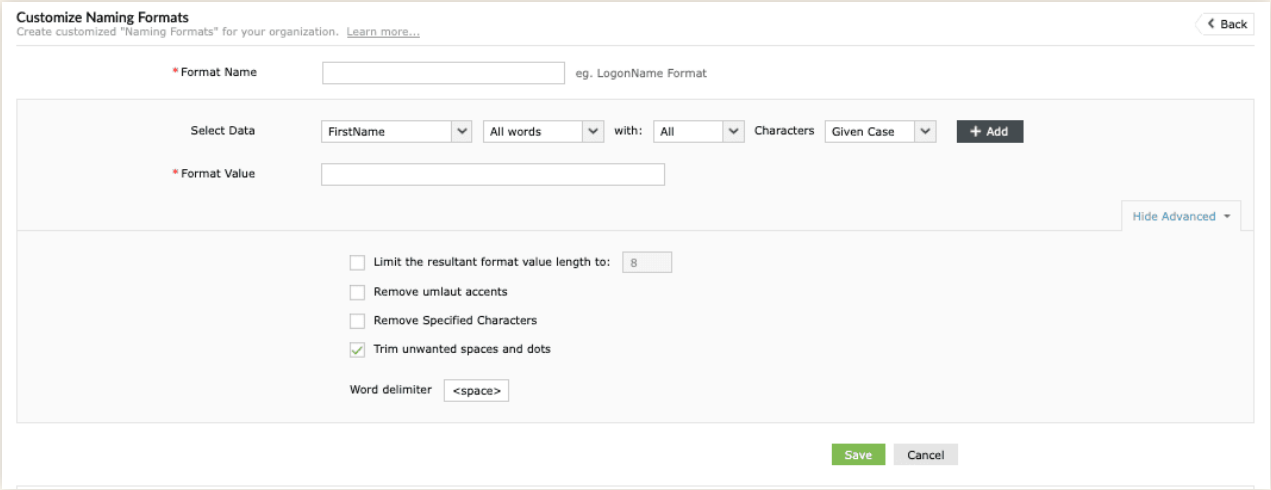


Figure 4: Custom naming formats setup.

Role-based access control

Once accounts are created, ADManager Plus automates the assignment of permissions based on an employee's role, department, or location. This ensures users are granted only the necessary access to relevant resources, significantly enhancing security and data protection by enforcing the principle of least privilege.

ADManager Plus empowers IT administrators to provision users with the minimum required access. You can manage NTFS and shared folder permissions by automatically assigning access based on organizational units (OUs) and group memberships. For temporary roles or project-based assignments, access can even be granted for a specific period, with automatic revocation upon expiration, minimizing the risk of stale or excessive permissions.

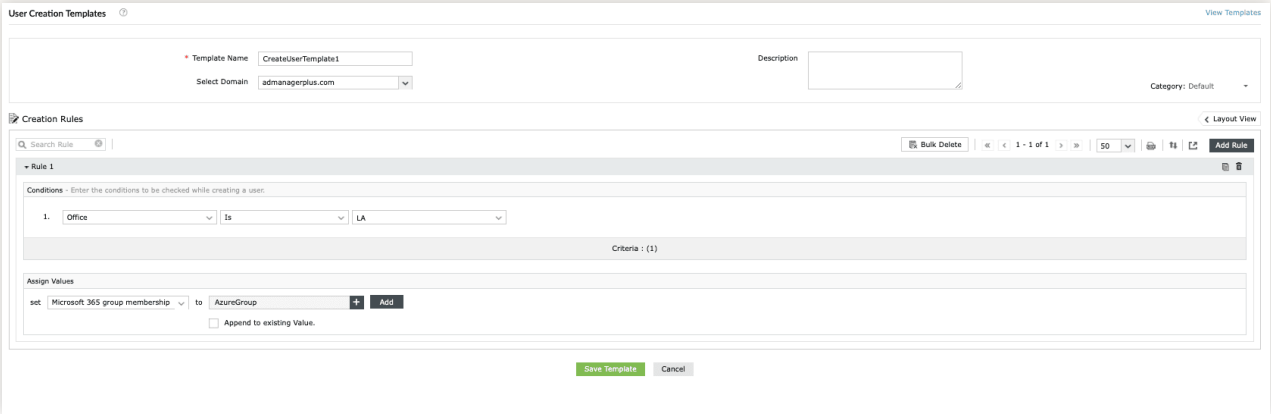


Figure 5: User creation rule.

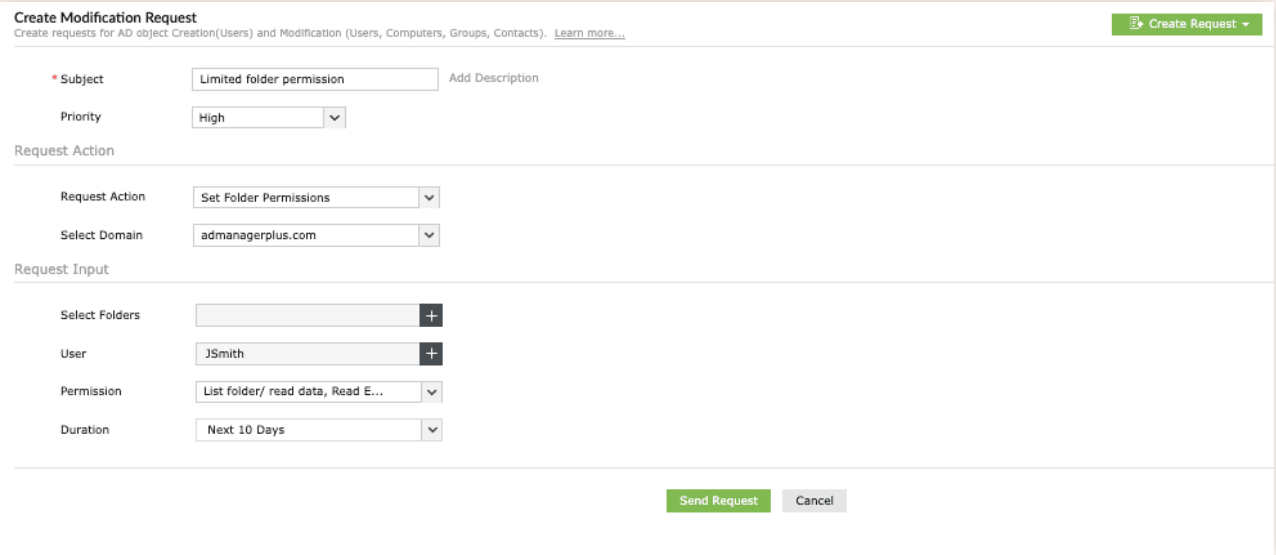


Figure 6: Assigning time-limited permissions.

The mover journey: Effortless role changes

ADManager Plus simplifies internal transfers and role changes, minimizing downtime and ensuring employees consistently have the appropriate access as their responsibilities evolve. This phase is critical for maintaining productivity and security.

Seamless role transitions | Access review campaigns

Seamless role transitions

When employees change roles, their access needs inherently change. ADManager Plus automates the update of permissions and access rights, ensuring employees instantly have the correct privileges for their new positions, free from delays or manual intervention.

IT administrators can easily adjust Active Directory group memberships and other permissions using user modification templates in ADManager Plus. This is particularly effective for team transfers, as admins can modify folder permissions and group memberships with predefined templates that align with new roles.

ADManager Plus also offers robust workflow capabilities to supervise and verify all Active Directory user management activities. Through this feature, you can set up a hierarchical approval process for automations, defining who can initiate, review, approve, and execute automation requests. Adding these supervision steps minimizes errors and helps maintain compliance with internal IT policies and external regulations.

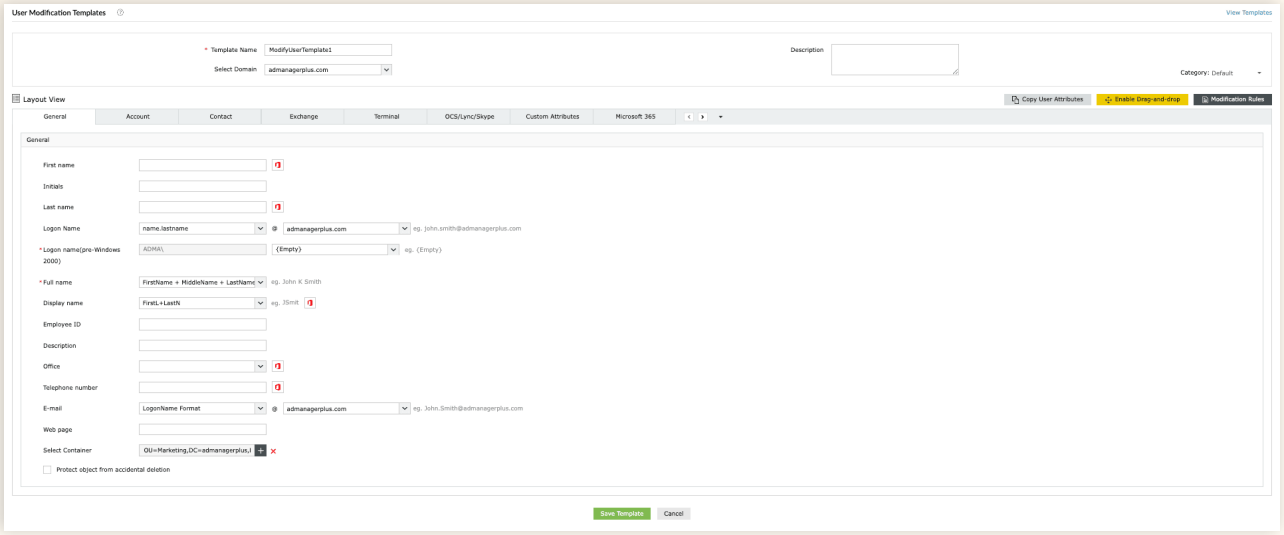


Figure 7: User modification template for role changes.

Figure 8: Multi-level approval workflow.

Access review campaigns

To bolster security and compliance, ADManager Plus facilitates regular access review campaigns to validate and adjust access rights to match a user's current role. This proactive approach minimizes the risk of excessive privileges, strengthens your security posture, and ensures ongoing alignment with internal policies and regulatory requirements.

ADManager Plus provides access certification capabilities to streamline your access control methods. Access certification campaigns allow you to assign, recertify, and revoke user access rights based on a periodic review by data owners or managers. This promotes the principles of least privilege, segregation of duties, and role-based access control, thereby helping organizations prevent privilege abuse attacks and enhance network security. With ADManager Plus, these campaigns allow bulk validation of user access rights, significantly improving operational efficiency for security and compliance teams.

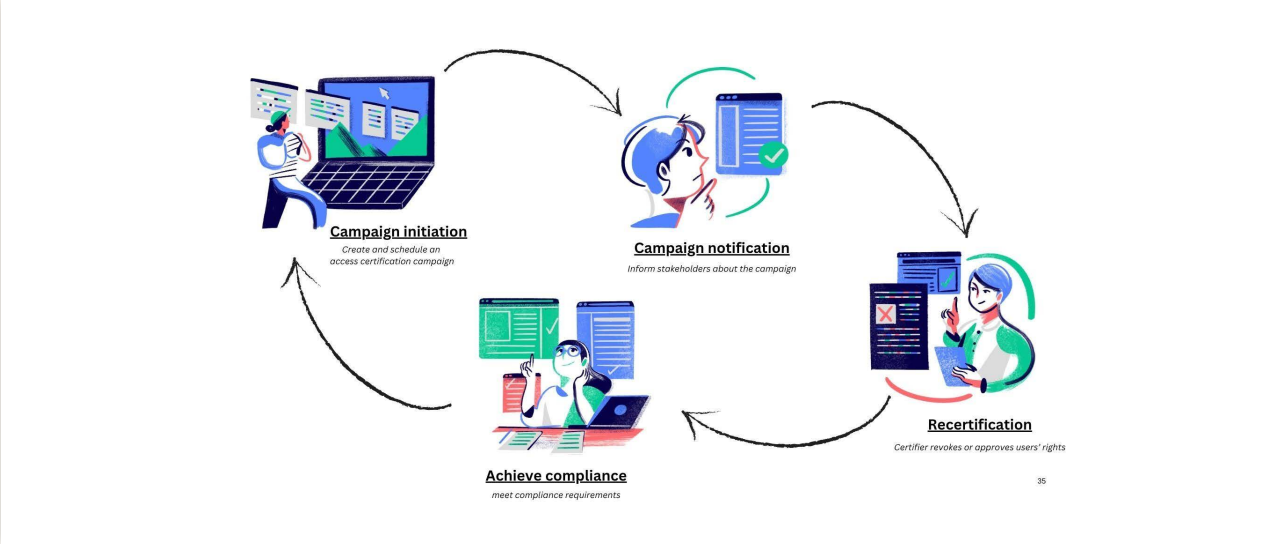


Figure 9: Access reviewer process.

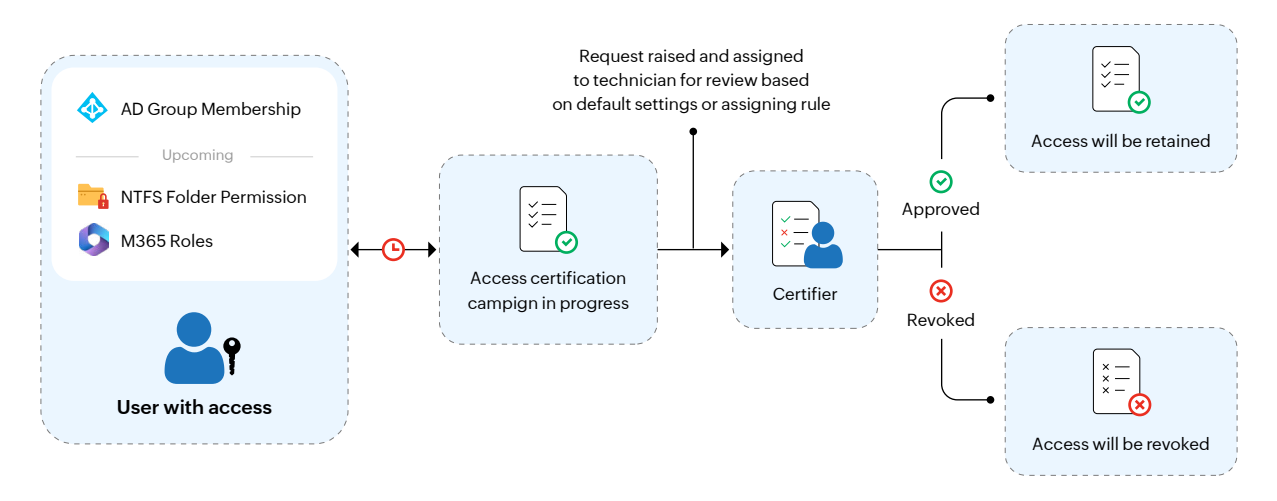


Figure 10: Access certification campaign.

The leaver journey: Secure and swift offboarding

Inconsistent or delayed offboarding procedures pose significant security risks to an organization. ADManager Plus ensures a streamlined and secure departure process, preventing unauthorized access, protecting sensitive company data, and maintaining compliance.

Automated account deactivation | Comprehensive audit trails

Automated account deactivation

When an employee leaves, ADManager Plus promptly deactivates or deletes their accounts across all systems and applications. This critical step prevents unauthorized access, significantly reducing the risk of data breaches and security incidents.

A user offboarding automation policy in ADManager Plus can be triggered by specific events, such as an account being disabled or a date-based trigger. This comprehensive automation policy can include several vital steps:

1. **Group membership removal:**
   All group memberships are systematically removed, safeguarding resources and ensuring former employees lose unnecessary permissions.

2. **OU segregation:**
   Departing user accounts are moved to a dedicated OU for better organization and streamlined management throughout the offboarding process.

3. **User account deletion:**
   Disabled user accounts can be automatically deleted after a predefined quarantine period, preventing any unauthorized activity and mitigating long-term security risks.

4. **License revocation:**
   Automatically remove associated licenses in cloud platforms like Microsoft 365.

Furthermore, event-driven automation can be configured in ADManager Plus to seamlessly execute additional offboarding actions. This includes tasks like removing Microsoft 365 licenses, disabling user mailboxes, archiving data, and revoking access to other applications, ensuring a clean and secure IT environment upon an employee's departure.

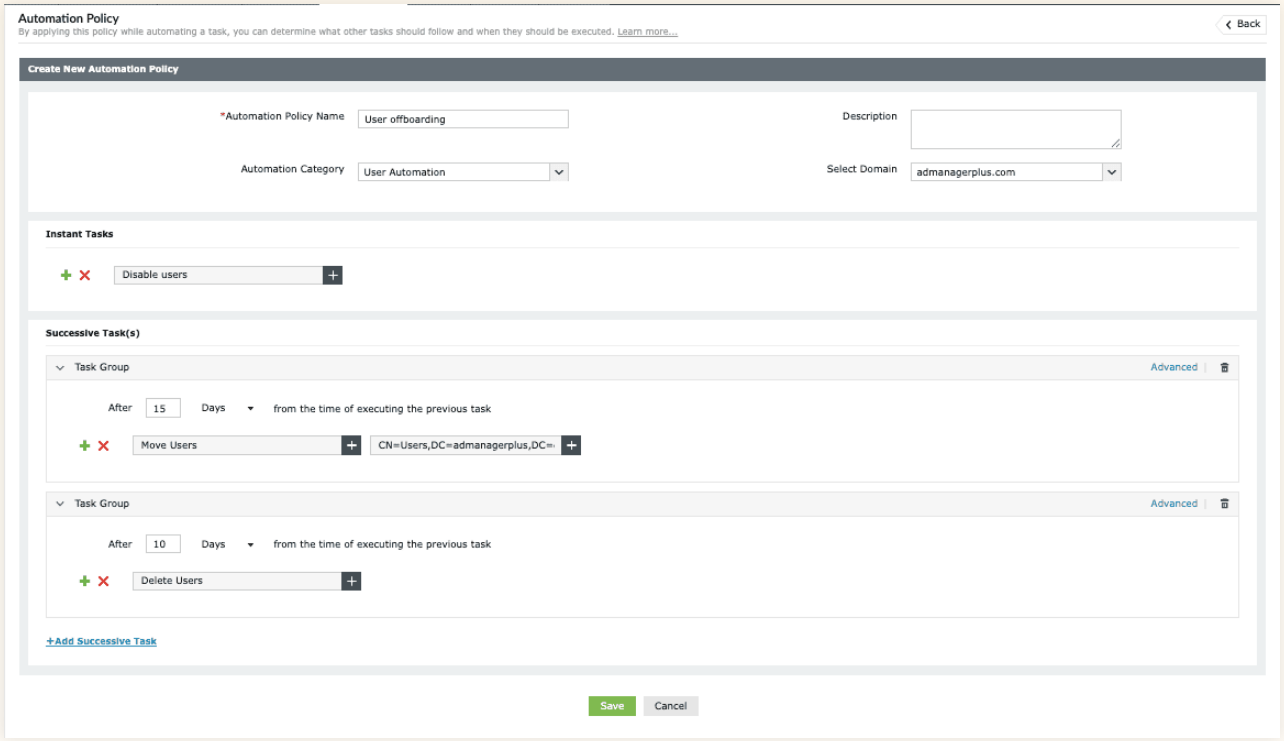


Figure 11: Automation policy for user offboarding.

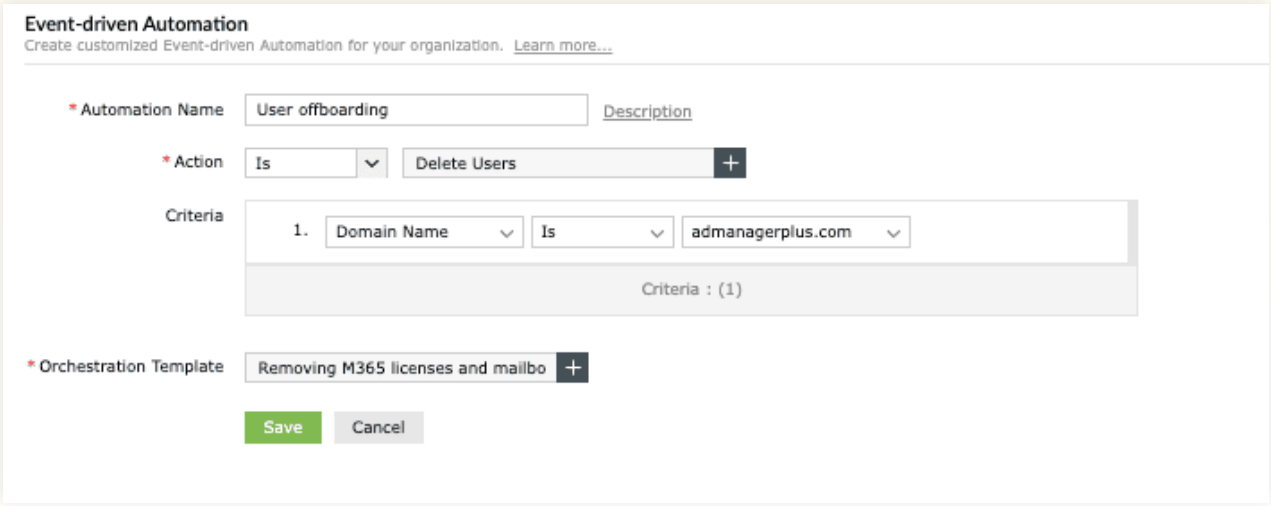


Figure 12: Event-driven automation trigger setup.

Comprehensive audit trails

Every employee life cycle event—from onboarding and role changes to offboarding—generates comprehensive audit trails within ADManager Plus. These detailed records of user activities, access permissions, and administrative actions enhance transparency, enable accountability, and critically support compliance efforts.

With critical actions often delegated to help desk technicians and HR personnel, accurate records of their activities are vital. ADManager Plus provides help desk audit reports, offering administrators a detailed view of all changes made by technicians. These reports track task status, object names, action categories (e.g., password resets or user deletions, creations, or modifications), allowing close monitoring of all events and adherence to the principle of least privilege in delegated administration.

Organizations can protect employee data and maintain compliance with regulations like SOX, HIPAA, the PCI DSS, the GLBA, and the GDPR with exclusive, prebuilt compliance reports. These reports provide verifiable evidence for auditors, demonstrating that appropriate JML processes and controls are in place and being followed.

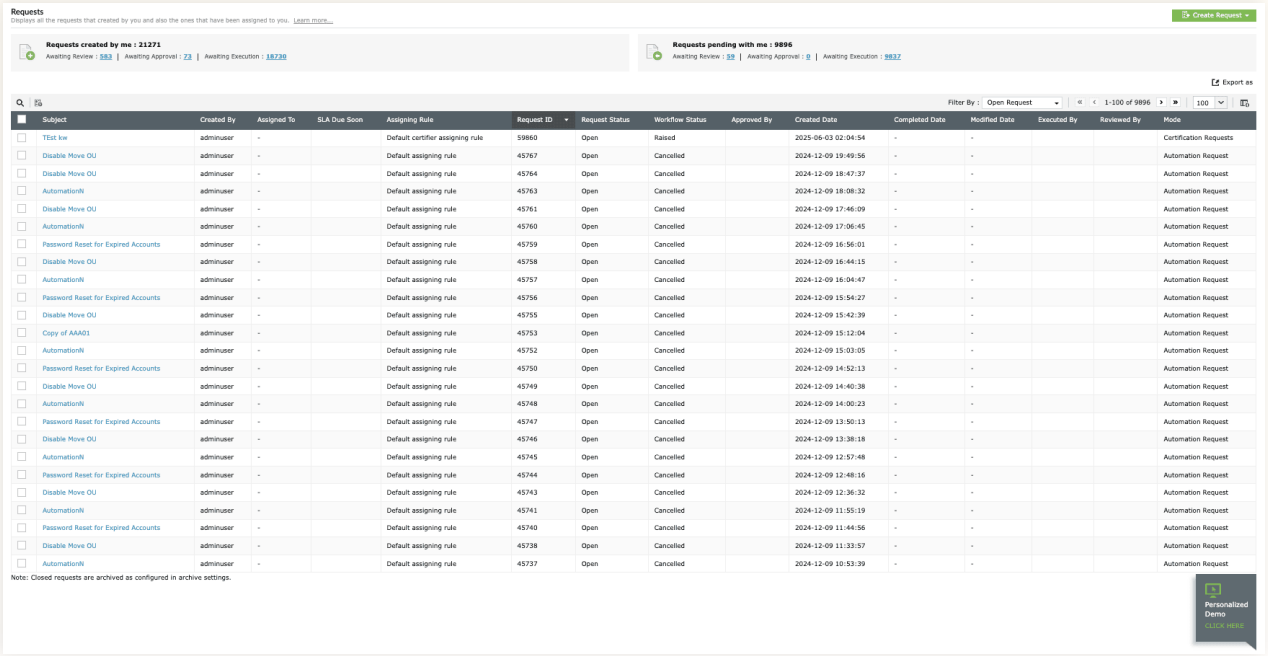


Figure 13: Logs of access requests.

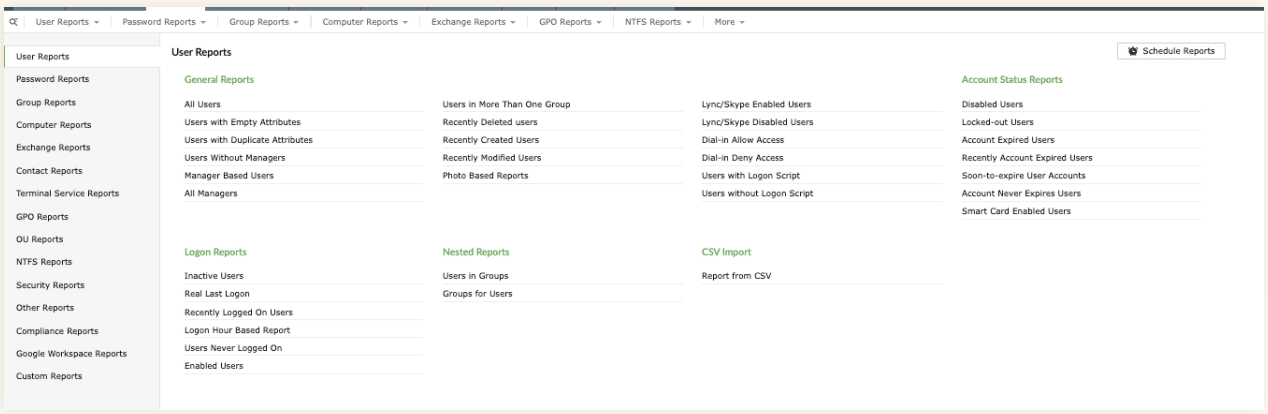


Figure 14: Over 200 reports to track all user activities.

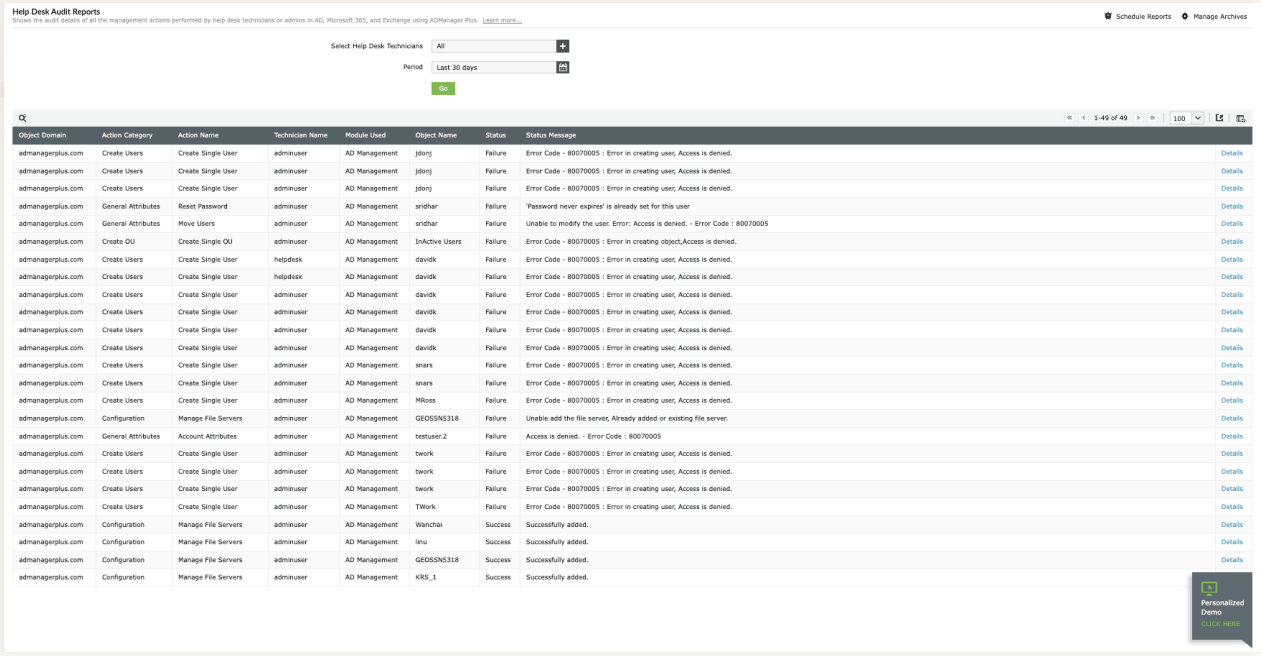


Figure 15: Help desk audit reports.

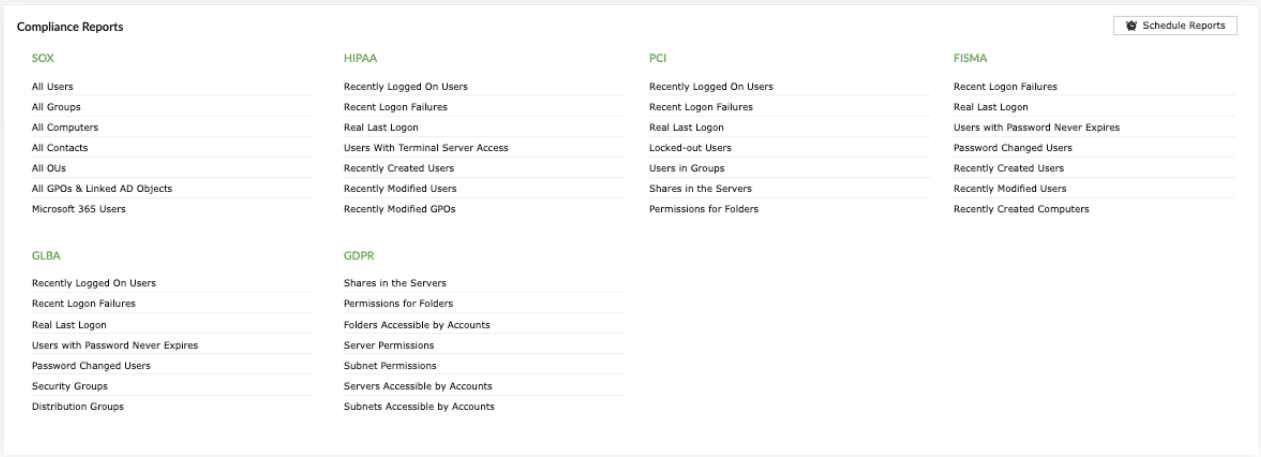


Figure 16: Prebuilt compliance reports.

Key features that drive JML automation in ADManager Plus

Feature	Description	Benefit
Automation	Design automations and automation policies that automatically trigger JML actions (e.g., user creation, disable user, or group modification) based on predefined conditions, data changes in integrated HR systems, or scheduled events.	Significantly reduces manual effort, ensures process consistency, and enforces organizational policies.
Onboarding and offboarding templates	Create custom templates with predefined user attributes, security settings, and permissions for different roles and departments, ensuring standardized and error-free provisioning and deprovisioning.	Speeds up the JML process, minimizes human errors, and ensures consistent application of security and compliance policies.
Role-based access control	Define granular access permissions based on user roles, automatically granting or revoking access as users join, move, or leave. Includes capabilities for periodic access reviews via certification campaigns.	Enhances security by enforcing the principle of least privilege and simplifies complex access management.
Integration with HR systems	Connect directly with your HR applications (e.g., Workday, SAP, or BambooHR) via APIs and webhooks, allowing automatic data flow to trigger user account and mailbox creation, permission assignment, and more.	Eliminates the need for manual data entry, ensures timely execution of JML processes, and improves data consistency.
Multi-system management	Manage user accounts and access rights across on-premises Active Directory, Exchange, Microsoft 365, Microsoft Entra ID, Google Workspace, and other critical applications from a single, centralized console.	Provides a single point of control, simplifies administration, and improves cross-platform operational efficiency.
Comprehensive reporting	Generate detailed reports on user accounts, group memberships, access privileges, and all JML process activities. Provides robust audit trails of administrative and delegated actions for accountability and compliance.	Offers valuable insights into user management, facilitates proactive security monitoring, and helps meet regulatory requirements.

Why choose ADManager Plus for JML automation?

ADManager Plus offers a powerful, user-friendly, and secure solution for automating your JML life cycle, helping you save time, enhance security, and improve overall IT efficiency.

Comprehensive feature set:
A complete management and reporting solution for Active Directory and broader IT infrastructure management, including robust, end-to-end JML automation capabilities.

User-friendly interface:
An intuitive, web-based, and easy-to-navigate interface that requires minimal training, accelerating adoption and reducing the learning curve for IT teams.

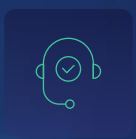
Seamless integrations:
Integrates seamlessly with leading HR systems, identity management solutions, ITSM platforms, and other business applications to create a truly automated identity life cycle.

Scalability:
Designed to handle the user management needs of organizations of all sizes, from small businesses to large enterprises with complex, multi-domain environments.

Granular access control:
Enables you to review and manage the access rights of users with periodic and automated access certification campaigns, ensuring the principle of least privilege is continuously enforced.

Robust security architecture:
Built with security as a core principle, helping you protect sensitive data, prevent unauthorized access, and maintain compliance with industry standards.

Proactive risk management:
Identifies potential security risks in your Active Directory and Microsoft 365 environments, allowing for proactive remediation.



Excellent support:
Backed by a dedicated and responsive support team to assist you with implementation, configuration, and ongoing management, ensuring a smooth operational experience.

Implementation planning and best practices

Implementing JML automation effectively requires careful planning and adherence to best practices to ensure a smooth transition and maximize benefits.

1. Phased rollout strategy

a. Pilot program:
Start with a small, contained pilot group (e.g., one department or a specific role) to test workflows, identify issues, and refine processes before a broader rollout.

b. Gradual expansion:
Expand automation incrementally, phase by phase, allowing your team to gain experience and adapt to the new automated workflows.

2. Data cleansing and standardization

a. HR data accuracy:
Ensure your HR system is the authoritative source of truth for employee data. Inaccurate or inconsistent data in your HR information system will directly impact the effectiveness of JML automation.

b. Standardized naming conventions:
Implement consistent naming conventions for users, groups, and OUs to simplify management and automation.

3. Define clear workflows and policies

a. Map existing processes:
Document your current manual JML processes to identify bottlenecks and areas for automation.

b. Define automation policies:
Clearly define the rules, triggers, and actions for each JML automation policy within ADManager Plus.

c. Approval hierarchies:
Establish clear approval hierarchies for sensitive actions, ensuring the right individuals have oversight.

4. Security best practices

a. Principle of least privilege:
Continuously apply the principle of least privilege to ADManager Plus service accounts and delegated administrators.

b. Regular access reviews:
Utilize ADManager Plus' access certification campaigns to regularly review and validate user access rights, especially for privileged accounts.

c. Audit logging and monitoring:
Leverage comprehensive audit trails and reporting capabilities to monitor all JML activities and identify suspicious patterns. Integrate with SIEM solutions for centralized logging and alerts.

d. Secure integrations:
Ensure all integrations (e.g., HR, cloud platforms, and ticketing) are configured using secure protocols (e.g., OAuth or API keys) and strong authentication.

5. Training and documentation

a. Administrator training:
Provide thorough training for IT administrators and delegated help desk personnel on how to configure, monitor, and troubleshoot JML automation workflows in ADManager Plus.

b. User guides:
Create clear documentation for common scenarios and troubleshooting steps.

6. Performance and scalability considerations

a. System sizing:
Ensure the ADManager Plus server and database resources are adequately sized for your organization's user volume and anticipated workload.

b. Monitoring:
Regularly monitor server performance, database health, and automation task statuses to ensure optimal operation.

Data inconsistencies
Solution: Implement robust data validation rules in ADManager Plus and enforce data quality standards in your HR system.

Complex custom workflows
Solution: Leverage ADManager Plus' flexible workflow designer, breaking down complex processes into smaller, manageable sub-workflows.

User resistance to change
Solution: Communicate the benefits of automation clearly to all stakeholders. Involve end users and department heads in testing phases to foster buy-in.

COMMON CHALLENGES AND SOLUTIONS

Integration failures
Solution: Utilize ADManager Plus' logging and notification features to quickly identify and troubleshoot integration issues. Ensure API connectivity and credentials are correct.

Getting started with JML automation

Ready to transform your user management with ADManager Plus? Take the next step towards a more efficient, secure, and compliant JML life cycle.

Request a free demo | Download a free trial | Explore our resources

ManageEngine
ADManager Plus

Our Products

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

About 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 Entra ID management.

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

$ Get Quote Download