ManageEngine
AD360

A no-code guide to

AUTOMATE JML LIFE CYCLE MANAGEMENT

www.manageengine.com/active-directory-360/

Table of Contents

Introduction

In the digital era, efficiency and speed are paramount, yet many HR and IT departments rely on outdated onboarding and offboarding processes. Cumbersome paperwork, endless email chains, and repetitive tasks drain resources and hinder organizational productivity. Fortunately, there's a better way.

This e-book guides you through the benefits of automating joiners, movers, and leavers (JML) life cycle management, spotlighting how it can streamline operations and boost productivity. Let's explore how to make this transition.

Understanding user life cycle management

User life cycle management (ULM) is essential for HR and IT departments, facilitating smooth access management for all employees from onboarding to departure. It involves provisioning, updating, and revoking access rights to provide secure and appropriate access levels throughout an employee's tenure with the organization.

Exploring joiners, movers, and leavers

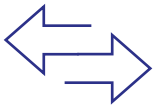
STAGE 1

JOINERS

(onboarding)

Initiates identity creation for new hires, ensuring they receive essential access to perform their roles effectively.

STAGE 2

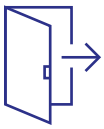


MOVERS

(transfers)

Updates access rights for employees transitioning to new roles, ensuring their access aligns with their current position.

STAGE 3



LEAVERS

(offboarding)

Removes access rights and disables or deletes accounts for employees exiting the organization.

Challenges of manual JML management

Manual management of the life cycle of joiners, movers, and leavers introduces considerable challenges and potential vulnerabilities for both IT and HR departments. This crucial process governing employee entry, internal transitions, and departure within an organization becomes increasingly complex and cumbersome without automated systems.

The 2022 Data Breach Investigations Report indicates that 82% of breaches are linked to human actions. However, human factors risks extend beyond common issues like phishing attacks or password mishandling.

Let's delve deeper into the key challenges associated with manual JML life cycle management:

CHALLENGE 1

Lengthy onboarding process

In organizations with more than 200 employees, manual user onboarding and offboarding are labor-intensive, averaging six hours to onboard an employee, and seven hours to offboard one. This inefficiency affects productivity levels and employees' overall experience and satisfaction.

CHALLENGE 2

A disconnect between HR and IT

Coordination of onboarding new employees often relies on outdated manual methods, like phone calls or emails. Even when organizations employ CSV files for this purpose, IT departments struggle with creating and managing user provisioning scripts and face challenges with constant API and data format changes.

CHALLENGE 3

Complexity in access provisioning

Assigning the right access levels to newly hired employees is a critical yet challenging task for IT staff. Finding the right balance is crucial; inadequate permissions hinder productivity, while excessive permissions pose security threats.

CHALLENGE 4

Ad hoc access management

While role-based access control (RBAC) and attribute-based access control (ABAC) systems can accommodate most access needs dynamically, exceptions might arise when employees require temporary or one-time access to resources for their role, necessitating manual overrides.

CHALLENGE 5

Management of external users

As organizations increasingly rely on external users, such as contractors and partners, manually managing their access introduces significant challenges. These users often fall outside the organization's HR systems, requiring manual account creation, which, if mishandled, can create security vulnerabilities.

CHALLENGE 6

Entitlement creep

Over time, employees may accumulate access permissions that are no longer necessary due to role changes or oversights. Manually tracking and updating these permissions increases the risk of entitlement creep, potentially leading to security breaches.

CHALLENGE 7

Timely access revocation

Promptly revoking access when an employee leaves the organization is crucial for preventing data breaches. Manual deprovisioning processes are prone to oversights and delays, leaving abandoned user accounts vulnerable to exploitation.

How do we fix these manual processes and security exposures for managing digital identities?

The answer is automation.

It's time to automate

While the previous section highlighted the challenges associated with manual JML life cycle management, let's delve deeper into why automating these processes is essential.

As employees progress through their life cycle within your organization, the focus shifts from enabling productivity to safeguarding your company's data. A poorly defined and executed joiner process not only delays new employees from reaching their potential value, but also increases the likelihood of them being dissatisfied due to a poor user experience. Research indicates that a strong onboarding process improved new hire retention by 82%.

Similarly, failing to execute the leaver process on time and consistently poses major security risks for your company, especially considering the prevalence of SaaS applications. Studies reveal that at least one in three former employees retain access to systems or data even after leaving their company.

Therefore, automation of JML processes is critical to mitigating access risks and ensuring seamless transitions for employees.

Securing the JML journey

Imagine a scenario where a newly hired employee joins a company. As soon as HR creates their record, automation begins. The employee's details, such as job title, department, and manager, are synchronized automatically with the IAM system. This triggers a series of automated actions based on predefined rules or mappings. Consequently, the new employee gains access to specific applications tailored to their role and department without manual intervention.

Now, consider the offboarding of an employee from the organization. As soon as HR marks them as a departing employee, automation kicks in again. Their account is promptly disabled, revoking all access granted during their tenure. This ensures that no lingering permissions pose a security risk to the company's data or systems.

But what about changes during an employee's tenure? Automation has that covered too. Whether an employee receives a promotion or undergoes a change in responsibilities, any updates made in the HR system propagate throughout the organization's infrastructure. Consequently, access rights are automatically adjusted to align with the employee's changed role. This ensures they possess the necessary tools and permissions to excel in their updated position.

The power of automation in the JML processes

Automating JML processes can significantly enhance organizational productivity by streamlining user identity and access privilege management. Utilizing an automated AD management solution simplifies the provisioning of new hires, revocation of access for departing employees, and modification of permissions. This streamlined approach saves time, minimizes errors, and enables organizations to effectively manage access to their resources.

Here are the top five advantages for implementing automation into JML life cycle management:

01

Saving time

Manually setting up user accounts can be time-consuming, particularly in organizations with many applications and roles that frequently onboard new employees or contractors. Automating the JML life cycle management process can save time and improve efficiency by streamlining the process of granting access to applications and resources.

02

Streamlines collaboration and communication

When a newly hired employee joins, the talent acquisition team typically notifies the IT department via email, a process that requires manual intervention by IT staff to create accounts and assign necessary access. An automated JML process enables the seamless importation of new hire information by IT teams, who can then efficiently create accounts on platforms such as Active Directory, Google Apps, or Microsoft 365. This automation streamlines new employee onboarding and lightens IT admin workloads.

03

Provides on-demand access with reduced complexity

In organizations where multiple teams have varying access needs to different applications and resources, managing access rights can become complex. Automating JML life cycle management centralizes access management, making it easier to grant and monitor access once IT teams are informed of each team's needs. This reduces the complexity involved in managing access for multiple users.

Secures provisioning

04

Automating the provisioning process can improve security by minimizing the risk of unauthorized access and potential data breaches. It enables better tracking and monitoring of user access, providing a detailed record of who has access to specific resources. It also ensures that users are deprovisioned from systems when they leave the company, so there are no zombie accounts or other security vulnerabilities.

Enables in-depth analysis

05

Automated JML life cycle management provides valuable insights for IT admins about user accounts. You receive information about users' accounts and access, including their access, when their accounts were created, when they need to be terminated, when their access was last updated, who started their accounts, and which apps they have access to.

Key phases of automated JML life cycle management

Let's explore each phase in detail to understand how ManageEngine AD360's AD management module, ADManager Plus, revolutionizes onboarding, transition, and offboarding experiences while strengthening security and compliance measures.

Automated onboarding (joiners)

Streamlined account creation

This phase automates the creation of user accounts across various systems and applications as soon as a newly hired employee joins the organization. By eliminating manual processes, new employees gain immediate access to the necessary tools and resources from their first day.

ADManager Plus streamlines the user creation process by integrating seamlessly with HCM solutions like UltiPro, WorkDay, BambooHR, and others with API support or CSV imports. By automating user creation across AD, Microsoft 365, and Google Workspace, users can be created quickly and easily. Utilizing user creation templates, ADManager Plus ensures a consistent and error-free setup by predefining essential user attributes such as usernames and email addresses. Organizations can also apply custom naming formats in the templates to create unique logon names and avoid duplication of names, which is a common problem in bulk user provisioning.

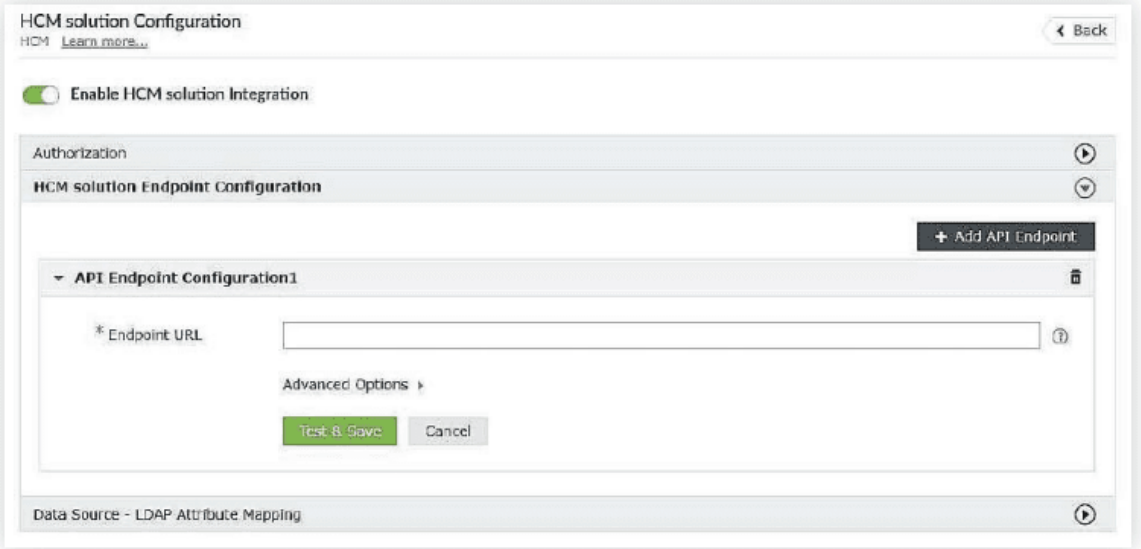


Figure 1. Custom HCM integration.

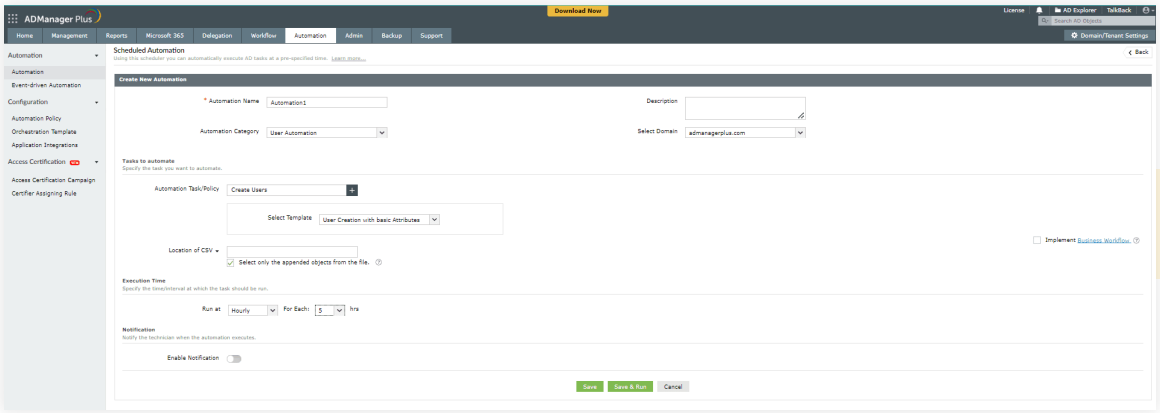


Figure 2. Automation for user onboarding.

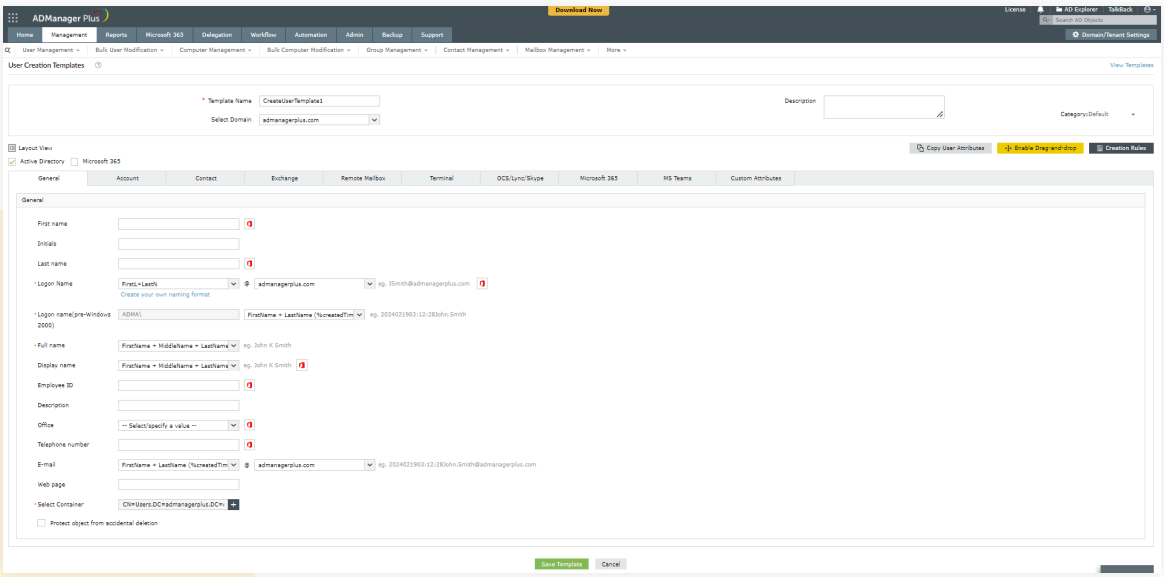


Figure 3. User creation template.

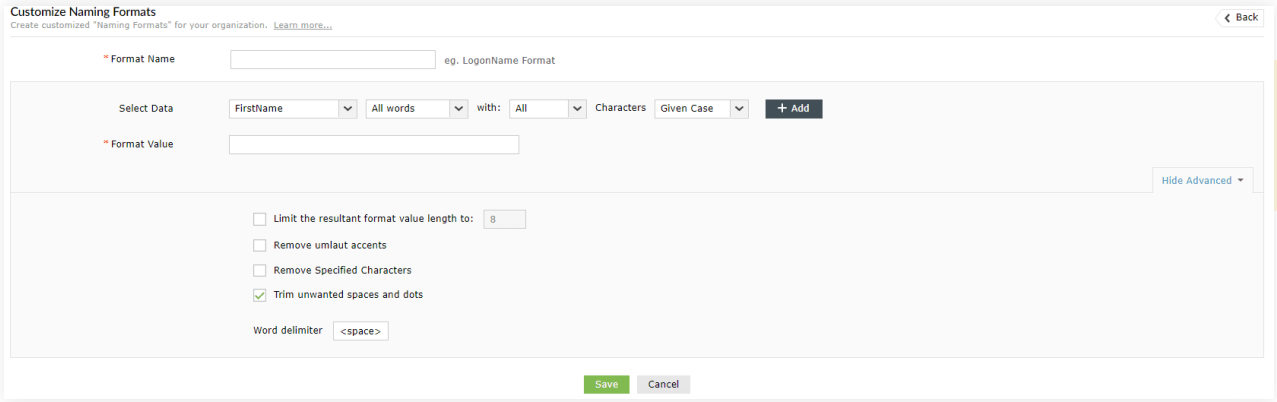


Figure 4. Custom naming format.

Role-based access control

An automated AD management solution assigns permissions and access rights based on the employee's role, department, or location. This ensures that employees only have access to resources relevant to their job responsibilities, enhancing security and data protection.

ADManager Plus gives IT admins the ability to provision users by applying the least privilege principle. This ensures that employees, consultants, contractors, and even temporary users can only access resources within their role. Organizations can manage access permissions to NTFS and shared folders by automatically assigning permissions based on factors like OUs and groups. Depending on the role, access to resources can be granted for a specific period of time.

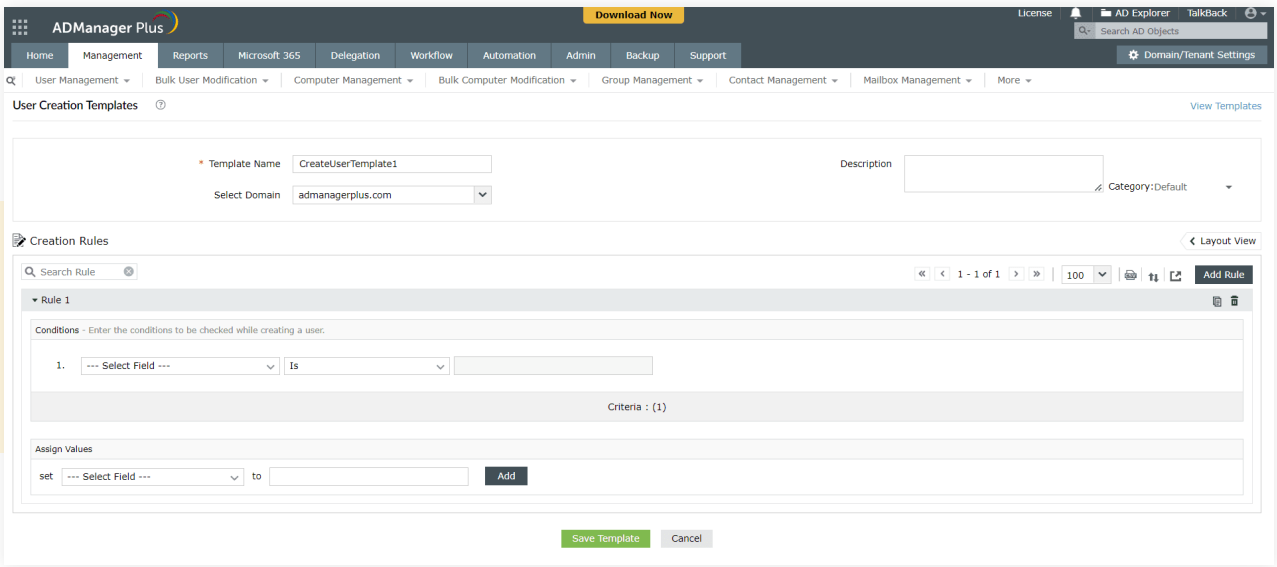


Figure 5. User creation rule.

Dynamic access management (movers)

Seamless role transitions

As employees change roles within the organization, an automated AD management solution updates their permissions and access rights accordingly. This ensures that employees have the correct access privileges for their newly assigned positions without delays or manual interventions.

IT admins can efficiently adjust AD groups for users using user modification templates in ADManager Plus. This functionality proves particularly useful when employees transfer between teams, as it allows admins to modify folder permissions and group memberships using the predefined templates. ADManager Plus also provides workflow capabilities, ensuring all AD user management activities are supervised and verified. Through the workflow feature, organizations can establish a hierarchical approval process for automations, specifying who can initiate, review, approve, and execute automation activity requests. By incorporating supervision steps into the automation process, errors are minimized and IT regulations are followed.

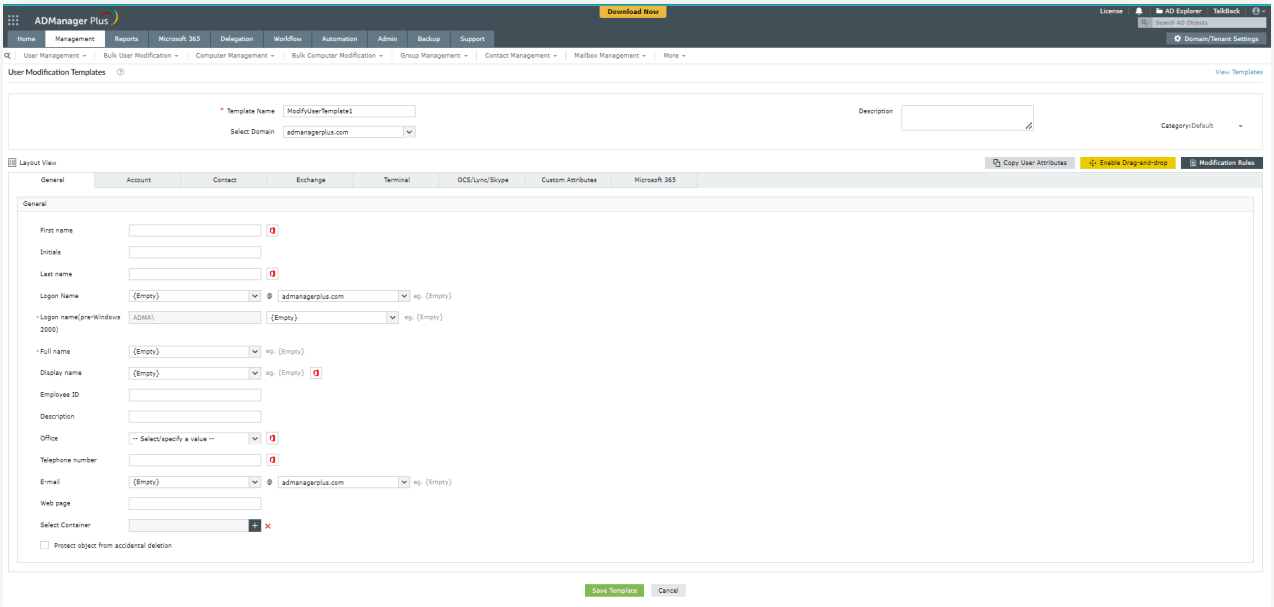


Figure 6. User modification template.

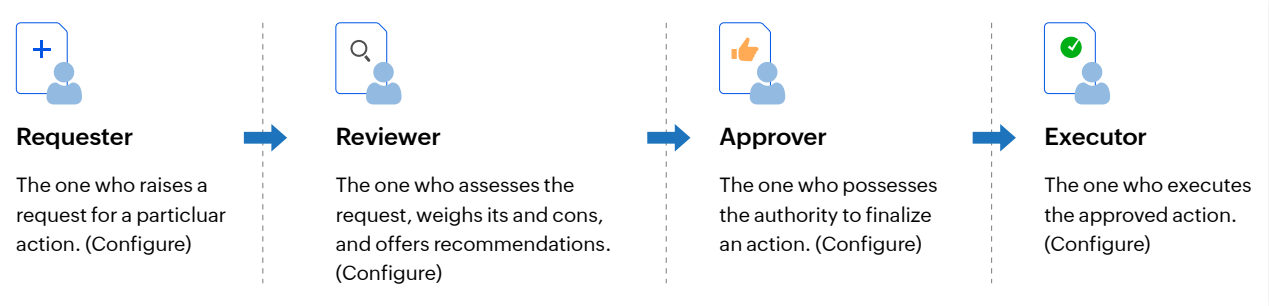


Figure 7. Review approval workflow.

Access rights reconciliation

An automated AD management solution regularly reviews and adjusts access rights to align them with the user's current role. By minimizing the risk of excessive privileges, organizations enhance security and compliance with internal policies and regulatory requirements.

ADManager Plus provides access certification capabilities to help organizations streamline access control methods. Access certification campaigns enable the assignment, recertification, and revocation of user access rights. They promote the principles of least privilege, segregation of duties, and role-based access control. By implementing these principles, organizations can mitigate privilege abuse attacks and enhance network security. With ADManager Plus, access certification campaigns validate user access rights in bulk, improving operational efficiency.

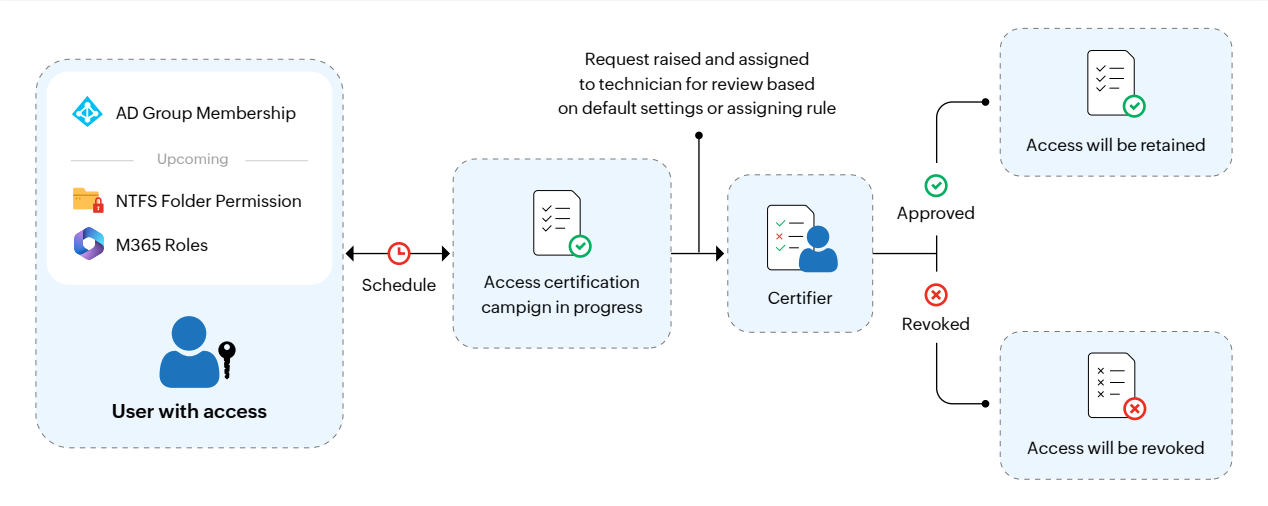


Figure 8. Access certification campaign.

Secure offboarding (leavers)

Automated account deactivation

When an employee leaves the organization, an automated AD management solution promptly deactivates their accounts across all systems and applications. This prevents unauthorized access and reduces the risk of data breaches or security incidents.

With ADManager Plus, a user offboarding automation policy is created to efficiently deprovision users who have exited the organization. This automation is triggered for users in the HCM system with a "Resigned" status. The automation process encompasses several crucial steps to ensure comprehensive user offboarding:

- **Group membership removal:**
  The automation systematically removes all group memberships associated with the departing user accounts. This step helps safeguard against unauthorized access to resources and ensures that former employees no longer retain unnecessary permissions.

- **User accounts disabled:**
  To prevent unauthorized access or activity, departing employees' user accounts are promptly removed. By disabling these accounts, organizations mitigate the risk of security breaches and unauthorized access to sensitive information.

- **OU segregation:**
  ADManager Plus facilitates the smooth transition of departing user accounts by moving them to a dedicated OU specifically designated for departing user accounts. This segregation ensures better organization and management of user accounts throughout the offboarding process.

Additionally, a workflow is integrated into the automation to provide an added layer of security and accuracy. This workflow serves as a safeguard, ensuring that no user is mistakenly deleted during the offboarding process.

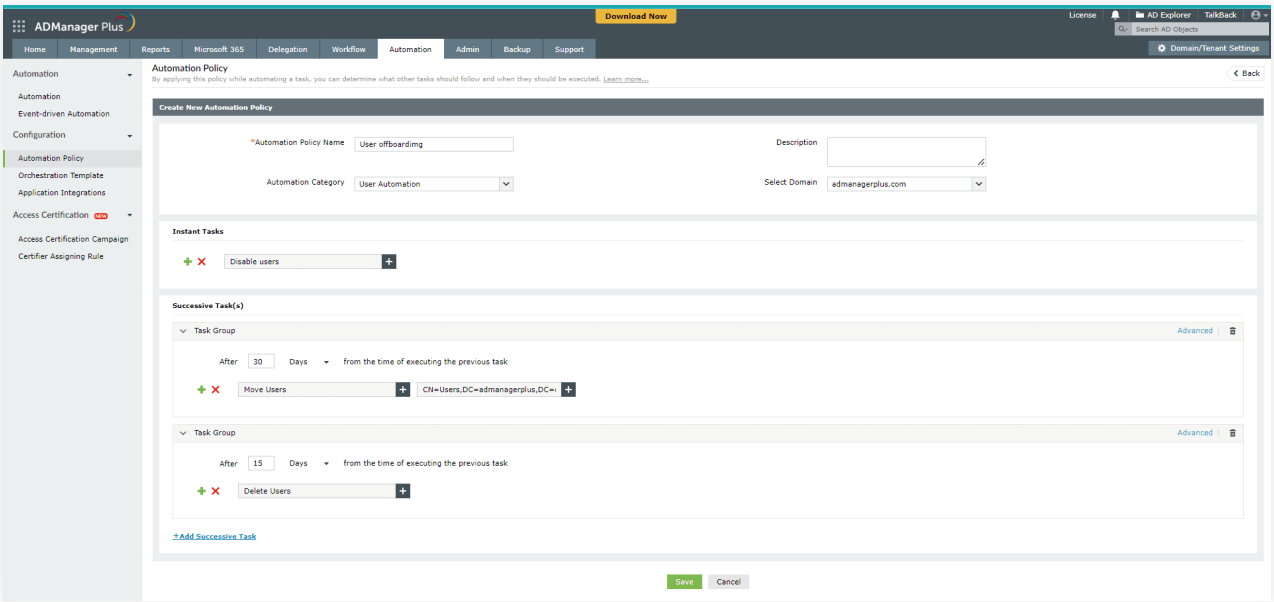


Figure 9. Automation for user offboarding.

Furthermore, event-driven automation is configured within ADManager Plus to execute user offboarding actions seamlessly. This profile includes tasks such as removing Microsoft 365 licenses, disabling user mailboxes, and removing additional group memberships, among others. By orchestrating these actions, organizations can streamline user offboarding and maintain IT environment hygiene.

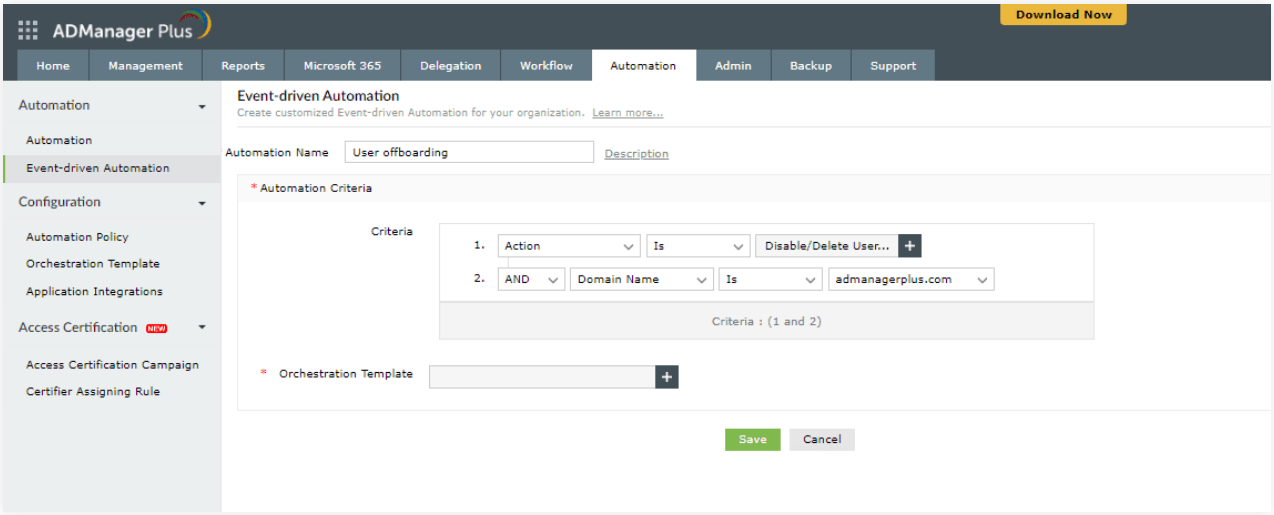


Figure 10. Event-driven automation.

Audit trails

Comprehensive audit trails are generated for each employee's life cycle event, including onboarding, role changes, and offboarding. These audit trails enhance transparency, enable accountability, and support compliance efforts by providing a detailed record of user activities and access permissions.

With critical actions delegated to the help desk and HR department, it is critical to have an accurate record of technicians' activities. ADManager Plus provides help desk audit reports, which give admins a detailed view of technicians' changes. Using audit reports, you can track the status of each technician's task or operation, the object name, the category of the action, etc., that help you closely monitor events like password resets, users deletions, users creation/modification etc.

Audit reports display the module that was used by the help desk technicians, such as automation or AD management, while performing the assigned actions. This enables the organization to protect its employees' data and be compliant with SOX, HIPAA, PCI DSS, GLBA, and the GDPR.

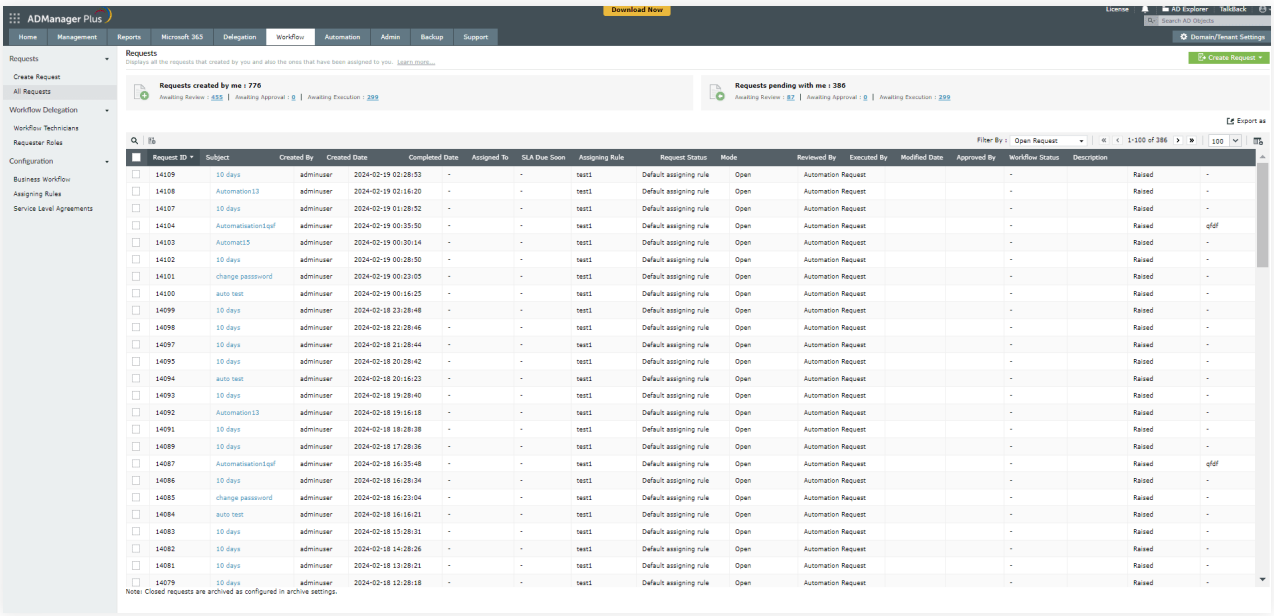


Figure 11. Help desk audit reports.

Conclusion

As people play a major role in business operations, it's critical to manage their access and associated risks throughout their journey. A robust strategy comprising well-defined processes is paramount for maintaining security and data integrity without micromanagement.

Automated provisioning and deprovisioning of users plays a pivotal role in refining ULM. By transitioning from manual, error-prone methods to streamlined, automated processes, organizations can significantly boost operational efficiency and reduce IT burden. ADManager Plus provides ULM functionalities that not only simplify the tasks for IT staff but also provide a seamless experience for newly hired employees navigating access setup.

By adhering to the guidelines outlined in this e-book, organizations can initiate their automation journey and harness the transformative potential of automated JML life cycle management. Embracing automation optimizes processes and empowers organizations to adapt swiftly to evolving demands while maintaining robust security measures.

If you'd like to automate and streamline user management processes, check out our unified AD, Exchange, and Microsoft 365 management and reporting solution.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
Exchange Reporter Plus | RecoveryManager Plus

About AD360

ManageEngine AD360 is a unified identity and access management (IAM) solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, access certification, risk assessment, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports of AD, Exchange Server and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for your IAM needs, including fostering a Zero Trust environment. For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download