

A complete solution guide for

Automated user account provisioning in AD and cloud environments



Table of Contents

User provisioning - Introduction	1
The HR and IT disconnect	2
Aligning the HR and IT systems for streamlining user provisioning	3
User provisioning solution overview and architecture -	
ADManager Plus	3
• Templates	6
• Automation	6
• Workflow	7
• Delegation	8
• Orchestration and webhook	9
• Integrations and Rest API	10
• Hybrid provisioning	10
• Backup and recovery	10
ADManager Plus implementation for user provisioning -	
Use cases	11
• Education	11
• Government	18
• Banking	18
• NGO	19
Alleviating IT admin burnout with automated user provisioning	20
How ADManager Plus helps alleviate IT admin burnout	21
About ADManager Plus	22

User provisioning – An introduction

User account provisioning is an identity management process that involves creating, modifying, disabling, and deleting user accounts across the IT environment of an organization.

Manually managing user provisioning activities as and when events like hiring, transfers, promotions, and terminations happen can be a headache for the stakeholders involved. Therefore, organizations need an automated user provisioning process that makes identity management secure and error-free.













Manual Provisioning	Automated Provisioning
 Time consuming & complicated	 Fast & simple
 High chance of errors	 Practically zero errors
 Expensive	 Reduces costs & time taken
 Untimely updates	 Automatic updates
 No/low system insights	 High system visibility and insights
 No records for compliance	 Helps ensure compliance

Fig. 1: Manual vs automated provisioning

The HR and IT disconnect

User provisioning can be complex due to the two main stakeholders—the HR and IT teams—having different priorities. While the HR team focuses on activities like planning onboarding, collecting candidate data, releasing offer letters, and more, the IT team focuses on creating or modifying users in the backend systems and providing them with the necessary permissions based on their roles, while meeting compliance requirements. The ad-hoc workflows and inefficient manual processes involved in the exchange of employee data between these two teams result in challenges such as:

- 1 Incorrect user data getting propagated across the IT systems
- 2 Risk of data leakage as sensitive employee information is sent over email
- 3 Lower productivity due to delay in communication between the teams

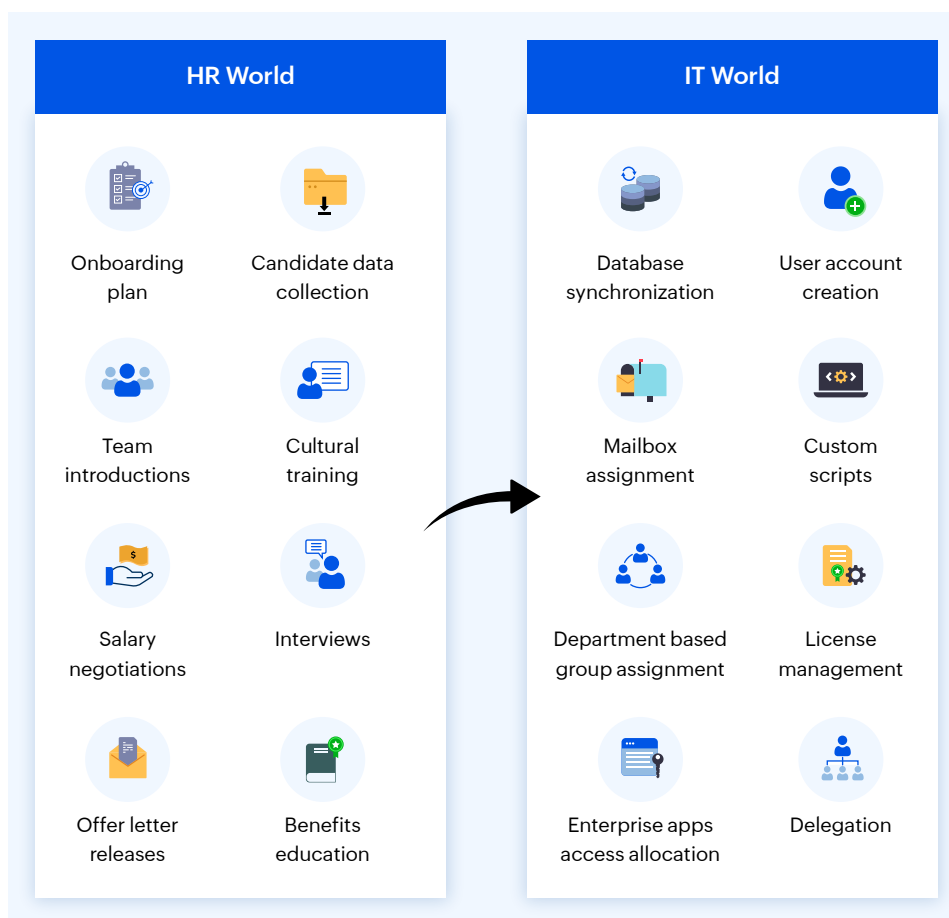


Fig. 2: The disconnect between HR world and IT world

Aligning the HR and IT systems for streamlined user provisioning

For most organizations, either an HR database or human capital management (HCM) software is the primary point of processing employee data.

Therefore, these can serve as a single source of truth when events such as the addition of new employees, changes in personal details, promotions, transfers, and terminations occur. Organizations can streamline the user provisioning process by integrating their HR and IT systems, and triggering automated workflows when changes are made to employee records in the HCM software. Automation in the IT system should detect identity-related changes and make the necessary modifications in directories such as Active Directory (AD), Microsoft 365, Google Workspace, and other enterprise applications.

User provisioning solution overview and architecture: ADManager Plus

With ManageEngine ADManagerPlus, organizations can take full control of their user provisioning process.

ADManager Plus' integrations with HCM solutions, HR databases, ITSM tools, and enterprise applications—as well as its automation capabilities—help replace the error-prone and time-consuming manual processes with an automated process that ensures productivity and data security.

ADManager Plus helps organizations perform user onboarding actions such as capturing new hire data from HCM systems; creating new users across AD, Microsoft 365, and Google Workspace; adding users to required groups; creating Exchange mailboxes; providing necessary permissions; provisioning users in enterprise applications; and more, all with ease.

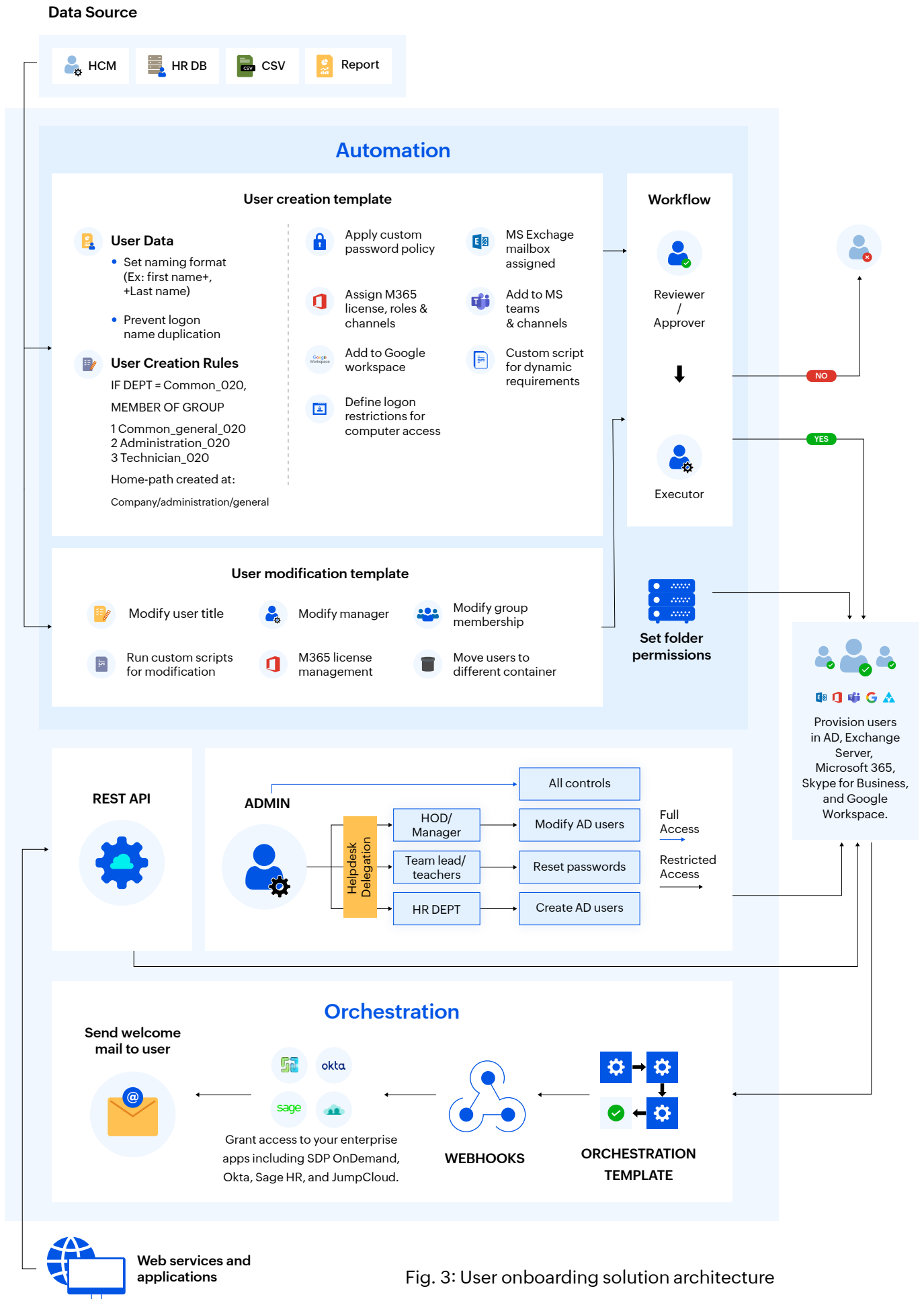


Fig. 3: User onboarding solution architecture

It also helps automate user offboarding activities, including disabling accounts of departing employees, revoking folder permissions, deleting group memberships, removing AD and M365 accounts, deleting Exchange mailboxes, removing permissions for enterprise apps, and much more.

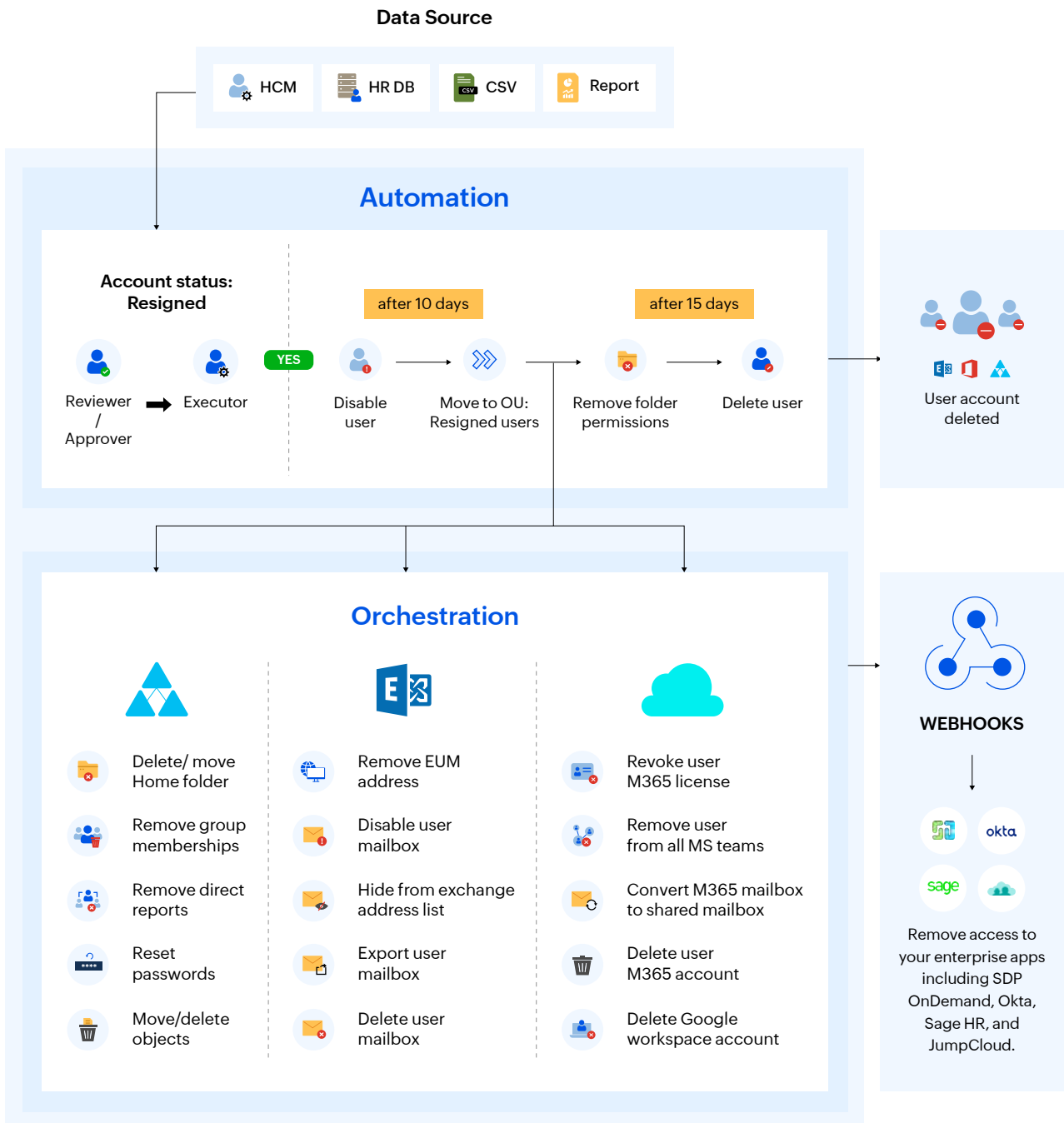


Fig. 4 : User offboarding solution architecture

ADManager Plus' user provisioning capability consists of the following components which come together to help implement a smooth user onboarding and offboarding process:

Templates

ADManager Plus provides creation and modification templates for users, computers, groups, contacts, mailboxes, and OUs. With templates, organizations can standardize the process of user creation and modification. They can use separate templates preconfigured with the necessary settings, permissions, and privileges specific to each role

User creation rules

User creation rules help admins to define the attributes that should automatically be updated with predefined values while creating a new user account. Using user creation rules, admins can also define how to reactively update specific attributes while creating the user accounts. They can set up conditions which, on being satisfied in the user account being created, shall trigger auto-population of the desired attributes.

Custom naming formats

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.

Automation

Routine tasks like bulk user creation, modification, and deletion can be configured and scheduled to run at specific times or intervals using ADManager Plus' automation capability. HCM solutions, HR databases, reports, or CSV files can be used as data source for these automations. Using the Automation Policy feature in ADManager Plus, organizations can define a set of follow-up tasks in a sequence after the main task, and specify time intervals for their execution.

Controlled automation according to organizational policies

A fully automated task can go completely wrong and produce devastating results if configured incorrectly. For instance, if a scheduled automation is configured to delete users who are on a long vacation instead of disabling them, the admins will have to spend a lot of time restoring these users. Instead, with ADManager Plus, organizations can configure controlled automation instead of full automation by incorporating workflows that introduce supervision from senior roles in the organization before executing any critical automated tasks.

Workflow

With ADManager Plus' workflow capabilities, organizations can ensure that all AD user management activities performed in their environment are supervised or verified. Using the Workflow feature, a hierarchy of approvals required to complete an automation can be defined, including who initiates the automation activity request, who reviews the process, who approves the process, and finally who executes it. Introducing supervision breaks like these while automating an activity helps eliminate errors and comply with IT regulations.

Review-approval workflow process

The workflow begins when a "requester" raises a request ticket for performing a task. This request is then reviewed by a "reviewer" who forwards this request to the next supervisory level, i.e., the "approver". Once the request is approved, the last level in the workflow, i.e., the "executor" can execute the requested task.

The workflow process not only reduces any margin for errors, but also helps create a ticket-based method for managing tasks. For compliance purposes, ADManager Plus also maintains a repository of all the requests and tickets created.

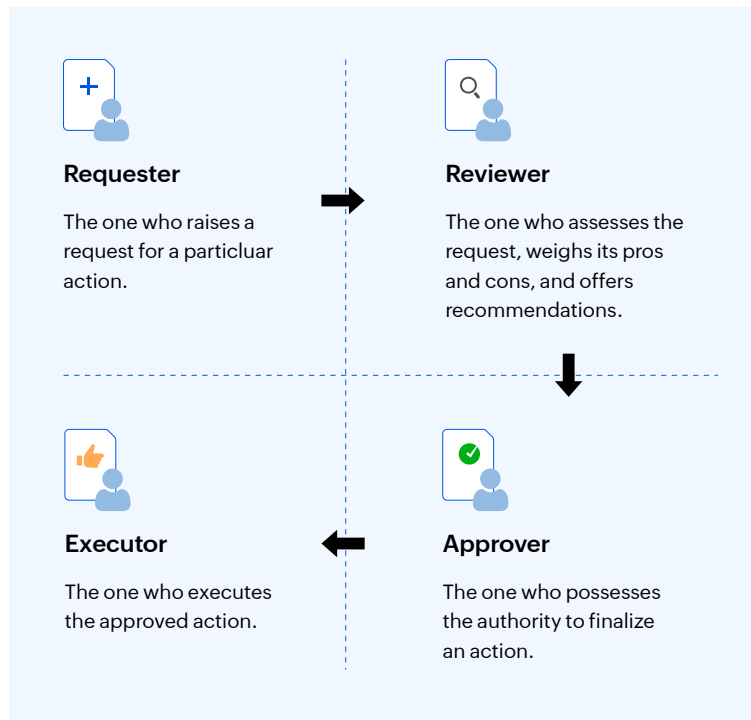


Fig 5: Review approval workflow

Delegation

If IT admins were to spend most of their time on routine provisioning activities like user modification, password reset, license assignment, folder access, etc., it would be a waste of their productive time. Provisioning tasks can be assigned to the HR or individual teams, thereby freeing up the IT admin team for more critical AD management tasks. ADManager Plus helps you create templates for user provisioning, which can be assigned to non-IT users—like HR, executives, teachers, principals, etc.—to delegate some of the user provisioning actions and offload the unnecessary burden from the IT team.

Non-invasive helpdesk delegation

While admins grant non-admin users the ability to perform AD management tasks, it doesn't come at the cost of security. Admins can create the technician role for delegating tasks only for those users already created in Active Directory. The technician role is not created in AD itself, but only in the tool, which enhances AD security because they're not granted any privileges in AD. These technicians can only view those tasks that are delegated, preventing them from making any other changes.

Auditing actions performed by technicians

With critical actions delegated to the helpdesk and HR department, it is critical to have an accurate record of the activities performed by the technicians. ADManager Plus provides Help Desk Audit Reports, which gives admins a detailed view of the changes effected by technicians.

Challenges	ADManager Plus solution
Risk of elevating AD rights	No need to elevate user rights in AD as the user access will be proxied via the ADManager Plus service account.
Ensuring that a technician does only what's required of them	Grant technicians access only to those features required to carry out the delegated tasks.
Monitoring the execution of delegated tasks	Workflow feature helps set up 4 levels of review system, which lets the admins keep track of the progress of the delegated tasks.
Lack of granular control over delegated tasks	Delegate different set of roles for different OUs to any technician

Fig 6: Helpdesk delegation - challenges and solution

Orchestration and webhook

With ADManager Plus' Orchestration capability, multiple tasks can be configured to execute in a sequence to complete a large process automatically. This will help organizations streamline routine and repeatable processes like user onboarding or offboarding, which are comprised of multiple tasks like permission management, mailbox management, group membership management, and more.

ADManager Plus also allows organizations to configure webhooks that can pass data between ADManager Plus and a target enterprise application in their environment to perform the desired user management actions. Once an ADManager Plus webhook integration is set up with an application, organizations can automate the creation or removal of users in the application whenever the webhook POST to a specific URL.

Integrations and Rest API

Most organizations rely on HCM systems such as Zoho People, UKGpro, BambooHR, and Workday or databases like Oracle and MS SQL to maintain a record of their employee information. ADManager Plus provides out-of-the-box integrations with these tools to make user account management easy for organizations.

Custom HCM integrations provided by ADManager Plus can help organizations setup user data collection from an HCM tool of their choice for user provisioning.

ADManager Plus allows for the integration of its AD management functions—such as user creation, password reset, disable user, delete user, and more—with other applications using REST API. These APIs allow organizations to access ADManager Plus from the web services or applications they use, and perform the necessary AD user account management functions.

Hybrid provisioning

For organizations with a hybrid environment, onboarding user accounts separately in AD, Microsoft 365, and Google Workspace can result in unnecessary delays. With ADManager Plus, organizations that have M365 and Google Workspace configured can sync the new user information from their AD to the cloud. They can automatically create mailboxes, perform M365 license management, and do much more for these users.

For users who are already present in the AD environment, Microsoft 365 accounts can be created instantaneously using reports or CSV files. Organizations can also provision users only in Microsoft 365 by simply selecting the Microsoft 365 option alone during user creation.

Backup and recovery

Unwanted and accidental changes in your AD can sometimes result in a disaster for organizations. With ADManager Plus' backup and recovery capability, organizations can create full and incremental backups of AD objects, including users, computers, contacts, groups, OUs, GPOs, and dynamic distribution groups. These AD objects can also be restored down to the attribute level. Thus, in the event of any mishaps in their AD, organizations can restore access for employees to their IT applications without much downtime and ensure productivity is not affected.

ADManager Plus implementation for user provisioning: Use cases



Education

Here's the case of one of the schools where we recently implemented ADManager Plus for user provisioning.

IT environment details:

The school has around 3,000 users and 250 groups. They use a third-party student information system and HCM solution for onboarding their staff and students.

The users in the school have the following user codes:

- 01 Student
- 02 Teacher
- 03 Principal
- 04 Admin staff

The codes for the buildings where these users are assigned are as follows:

- ES Elementary school
- MS Middle school
- HS High school
- AD Administration

Requirements:

1. Automating the routine user onboarding tasks
2. Integrating the school HR system with their IT system to avoid duplicate data entry
3. Ensuring new users have all the necessary access from day one

Implementation:

The entire user provisioning process was automated using ADManager Plus as follows:

Integrating the school's HR system with ADManager Plus

For this description, let's assume we are provisioning a user account for a teacher in the middle school. The department code for this user is MS-02, where MS stands for middle school and 02 is the user code for teacher.

The HR team creates a record for the new user in the HCM solution with basic details such as first name, last name, and department.

To automatically capture this data from the HCM solution every time a user record is created or modified, the HCM solution was integrated with ADManager Plus using the Custom HCM Integration feature (as seen in Fig. 7).

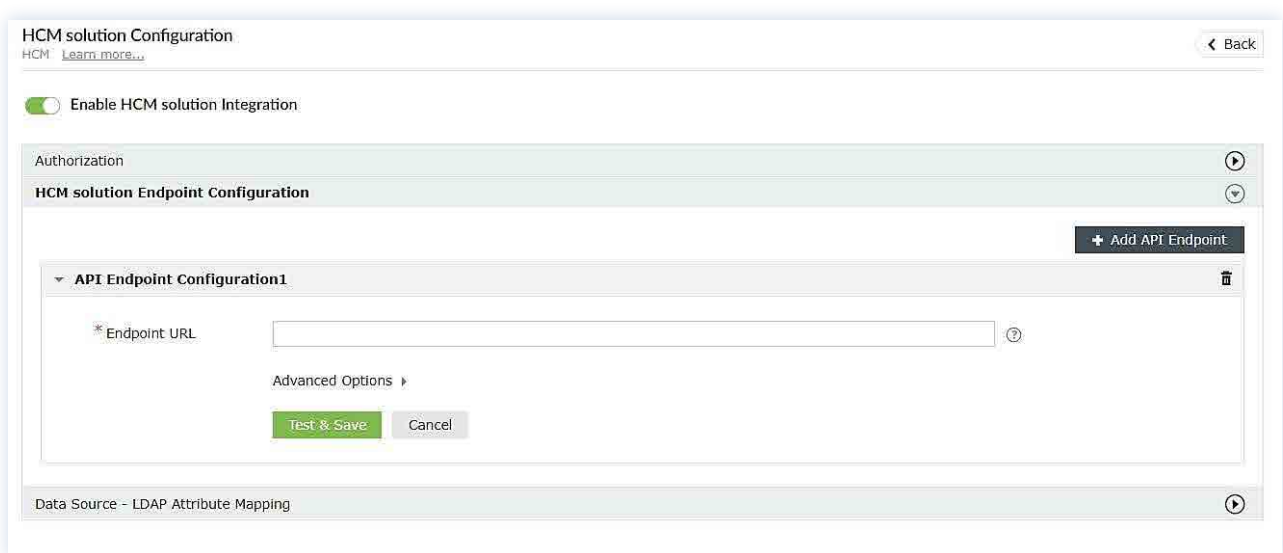


Fig. 7: Custom HCM integration

How to enable custom HCM integration in ADManager Plus

[▶ Watch now](#)

Setting up user creation templates

The user account attributes required for a middle school teacher were configured in a single step using user creation templates.

Using the customizable naming formats, a unique logon name format was created (as shown in Fig. 8) and applied in the template to standardize logon names.

Customize Naming Formats
Create customized "Naming Formats" for your organization. [Learn more...](#) ← Back

*Format Name: eg. LogonName Format

Select Data: All words with: All Characters: Given Case + Add

*Format Value:

Hide Advanced ▾

Limit the resultant format value length to:

Remove umlaut accents

Remove Specified Characters

Trim unwanted spaces and dots

Word delimiter:

Save Cancel

Fig. 8: Customizable Naming Formats

How to create a customized naming format with ADManager Plus [▶ Watch now](#)

The Prevent Duplication feature in the template was enabled to ensure that no two users are created with the same logon name.

Edit Logon Name

Field Name:

Field Type:

Enter the Default Value:

* Logon Name: @ eg. John Smith@admanager.com

[Create your own naming format](#)

Options

Security: Mandatory ReadOnly None

Appearance:

Prevent Duplication: Check for duplicates at level

Done Cancel

Fig. 9: Prevent Duplication check

Using the Creation Rules option, the user attributes—like office, address, container, group membership, home folder, and M365 licenses—were defined to be reactively-populated for department MS-02 (as shown in Fig 10).

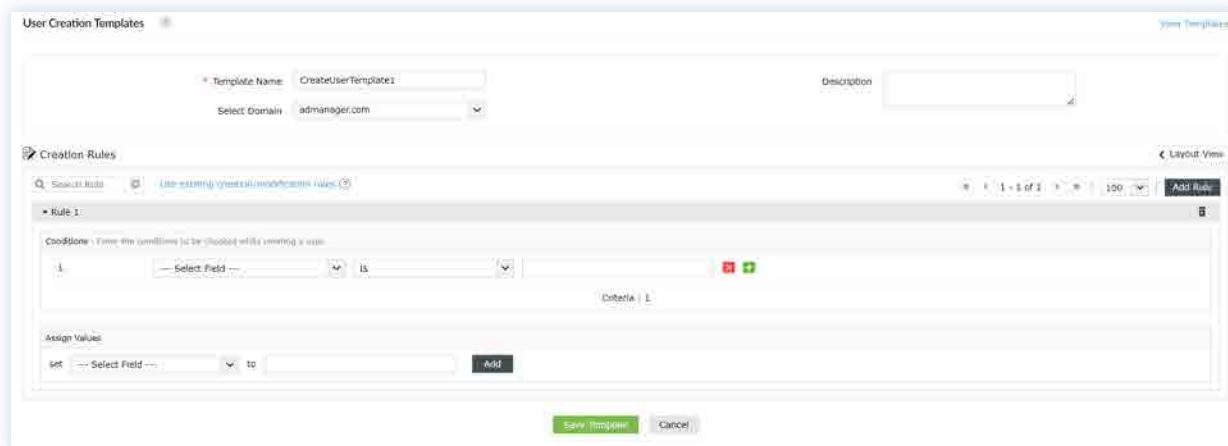


Fig. 10: User creation rules

How to set rule-based actions using templates with ADManager Plus [▶ Watch now](#)

Creating user provisioning automation with workflow

The next step was to create a user provisioning automation with a workflow. A new automation was created (as shown in Fig 11), which uses the user creation template created above to onboard new users after collecting new user information from the HCM solution. The automation fetches the details of the new teacher with the department marked as MS-02 from the user records in the HCM solution.

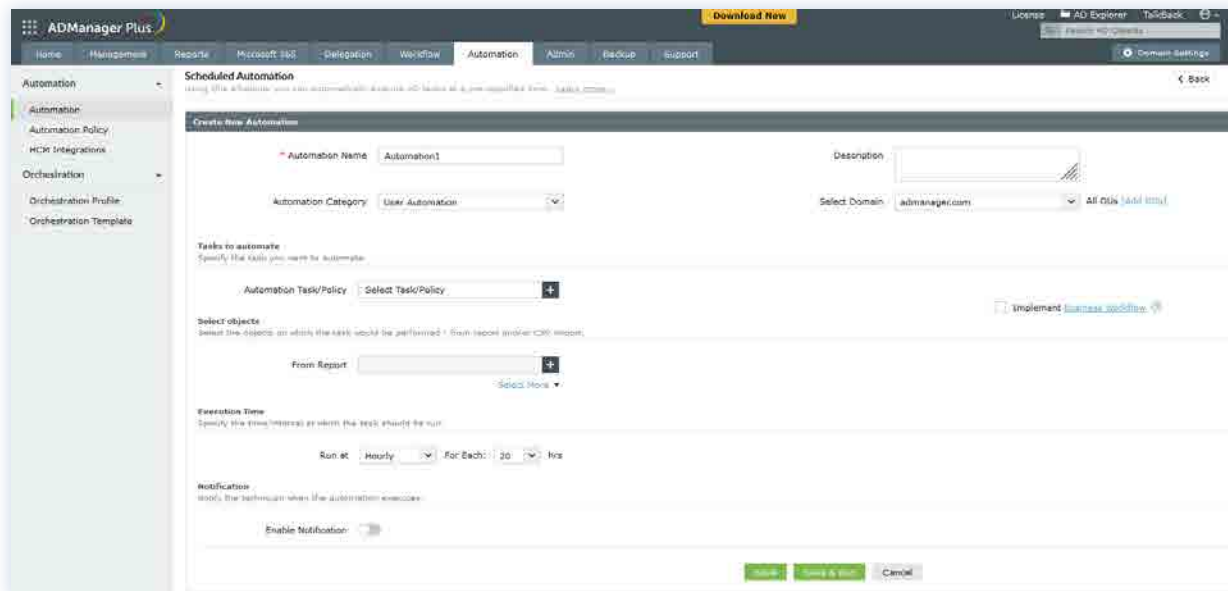


Fig. 11: Automation for new user onboarding

How to automate AD user creation using ADManager Plus [▶ Watch now](#)

A workflow was added to ensure that new user the data was verified by the Principal before the IT admin executed the task. The automation is raised as a ticket to the Principal. Once the request is reviewed and approved by the Principal, the automation request will be moved to the IT admin for execution.

The screenshot shows the 'Business Workflow' configuration page. At the top, there's a title 'Business Workflow' and a subtitle 'Define an order of execution for important administrative tasks. [Learn more...](#)'. A green 'Create Request' button is in the top right. Below the title, there are two input fields: 'Workflow Name' with the placeholder 'Enter a name' and 'Description' with the placeholder 'Enter a description'. The main section is 'Workflow Stages', which displays a horizontal flow of four stages: 1. 'Requester' (icon: person with plus) with description 'The one who raises a request for a particular action. [\[Configure\]](#)'. 2. 'Reviewer' (icon: person with magnifying glass) with description 'The one who assesses the request, weighs its pros and cons, and offers recommendations. [\[Configure\]](#)' and a dropdown 'No. of Reviewers: 1'. 3. 'Approver' (icon: person with checkmark) with description 'The one who possesses the authority to finalize an action. [\[Configure\]](#)' and a dropdown 'No. of Approvers: 1'. 4. 'Executor' (icon: person with checkmark) with description 'The one who executes the approved action. [\[Configure\]](#)'. Arrows connect the stages from left to right. At the bottom, there are 'Create Workflow' and 'Cancel' buttons.

Fig. 12: Workflow

Configuring orchestration for provisioning enterprise apps

A webhook was configured for the exchange of data between ADManager Plus and various applications used in middle school for interactive learning, assignments, grading, and more.

The screenshot shows the 'Webhook Template' configuration page. At the top, there's a title 'Webhook Template' and a subtitle 'Create customised "Webhook Template" with macros for your organisation. [Learn more...](#)'. Below the title, there are several fields: 'Name' (required) and 'Description' (optional) input fields; 'URL' (required) input field; 'Method' with radio buttons for 'Get', 'Put', 'Post' (selected), and 'Delete'; 'Headers' section with a message 'No headers available. [Click here to add](#)'; 'Parameters' section with a message 'No parameters available. [Click here to add](#)'; and 'Message Type' with radio buttons for 'None' (selected), 'JSON', and 'XML'. A note at the bottom right says 'Type "%s" in the value fields to list the default macros'. At the bottom, there are 'Test Connection', 'Save', and 'Cancel' buttons.

Fig. 13: Configuring webhooks for access to the school's apps

An orchestration profile was then created, which used the above webhook configuration to grant the teacher access to the configured apps when the user was created in the Middle School OU.

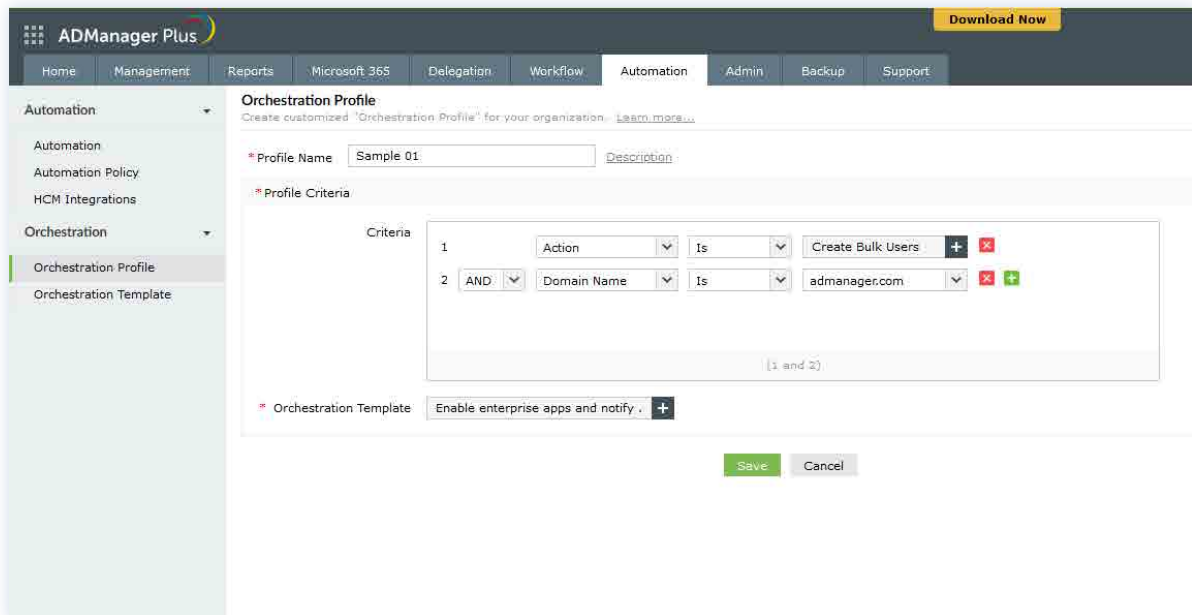


Fig. 14: Orchestration profile

Delegating user modification tasks to teachers and the principal

A help desk role was created to let teachers and the principal perform tasks such as resetting passwords or managing group memberships and folder permissions for users in their respective OUs.

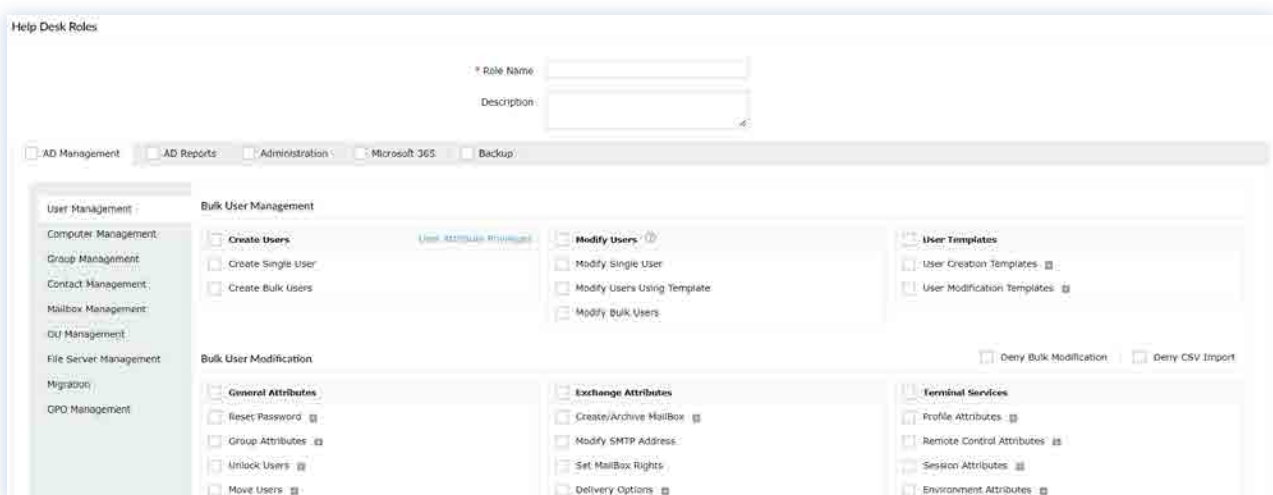


Fig. 15: Help Desk Role creation

Configuring user offboarding automation with workflow

A user offboarding automation policy was created to deprovision users who have left the school. The automation is triggered for users in the HCM system with status as "Resigned". The automation proceeds to:

- Remove all group memberships for these accounts.
- Disable the user accounts.
- Move them to a separate OU for departing user AD accounts.

A workflow was also implemented in this automation to ensure that no user would be deleted by mistake.

An orchestration profile was also configured to perform a sequence of user offboarding actions like removing M365 licenses, disabling the users mailbox, removing group memberships, and more.

With this automation, the user accounts that are no longer necessary will be removed from the school's IT environment within a specific time of the user's departure.

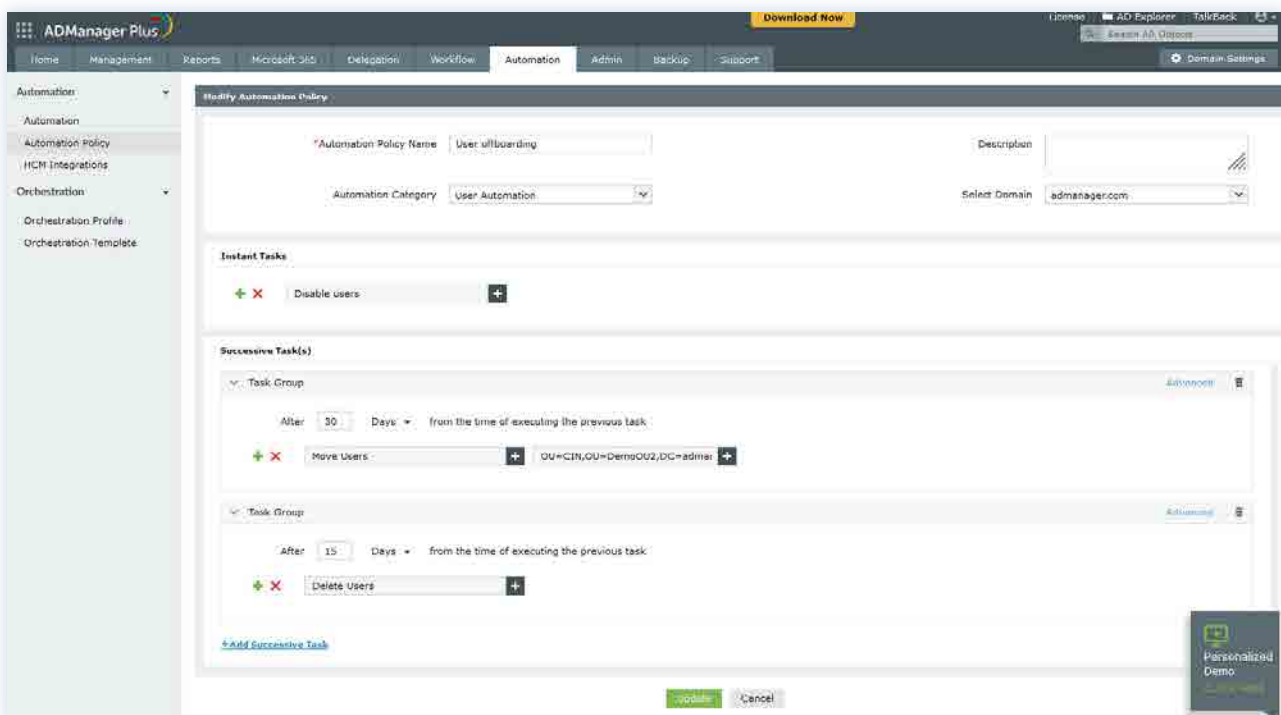


Fig. 16: Automation policy for user offboarding

How to automate AD user deprovisioning using ADManager Plus

▶ Watch now



Government

The ADManager Plus team helped the IT department of a government organization automate their provisioning process.

IT environment details:

The government agency's network spans over 2 sites and has approximately 1,800 groups. It currently uses Microsoft Forms where managers gather user data and CSV files for user provisioning. The IT admin was manually onboarding employees, resulting in a waste of productive time.

Requirements:

1. CSV-based bulk user onboarding
2. Creating a naming convention for user logon name using the following rules:
 - First 4 letters of first name
 - Then an underscore
 - Followed by the first 2 letters of last name
 - For duplicate user names, add a number at the end of it, such as: adam_go1, adam_go2, etc.

Implementation:

1. User provisioning and modification templates
2. Custom naming formats
3. Automation with workflows
4. Delegation of non-admin tasks to managers



Banking

ManageEngine helped a state-chartered bank with their user provisioning needs.

IT environment details:

The bank had over 550 employees and 50 groups. They used UKGPro as their HR management software.

Requirements:

1. Integration with UKGPro
2. Exchange mailbox creation for new users
3. User creation template that will create users with SAM Account Name in H+Employee ID format
4. Automate last working day process for exiting employees

Implementation:

1. Out-of-the-box HCM integration with UKGPro
2. User creation templates with Exchange Server mailbox creation and custom naming formats
3. User offboarding automation



NGO

The ManageEngine team was approached by an NGO for their user provisioning requirement.

IT environment details:

The NGO has a network consisting of 600 user objects and 60 group objects. It uses Paycom HRMS solution and iSupport as their IT help desk tool. They wanted a solution to automate their user provisioning process as they faced high turnover of employees.

Requirements:

1. Automating user creation and termination process due to high turnover
2. Delegating user management tasks to non-admins to reduce IT admins' workload

Implementation:

1. Custom HCM integration
2. User creation templates
3. Automation for user onboarding and offboarding with workflow
4. Help desk delegation

Alleviating IT admin burnout with automated user provisioning

Organizations are reeling under the pressure of an escalating number of cybersecurity issues, record levels of employee turnover, and a tight job market for experienced IT staff. IT teams are under tremendous pressure on a daily basis to keep their IT infrastructure running smoothly. Due to this excessive workload, IT teams suffer from burnout, low morale, and high churn, each of which could be detrimental for an organization on their own, but combine to make a potentially disastrous scenario.

Some of the major causes of distress for the IT admins in their routine work are:

Repetitive manual tasks

Many organizations have not adopted the latest IT management tools. Most of their routine tasks like user provisioning are therefore executed manually by the IT team. This means that the IT staff have to allocate a great share of their work time on mundane time-intensive tasks like user creation, modification, deletion, permissions management, and more, all while having to deal with other time-critical work, like resolving network issues, which adds to their stress.

Code-heavy operations

As mentioned above, a lot of mundane tasks are executed manually in many organizations. This requires the IT staff to do a lot of PowerShell scripting and coding in other programming languages for any user management tasks to be performed in their environment. Writing code for even small tasks can be mentally draining and time-consuming for IT administrators.

Misaligned technology

Despite having the technology, in some organizations, IT admins are likely to be fast-tracked to burnout. This is due to the out-of-sync technology stack used for their IT management. Besides the lack of sync in the tech stack, the different priorities of various teams and lack of collaboration between them can also accelerate burnout.

How ADManager Plus helps alleviate IT admin burnout

ADManager Plus helps overcome the above challenges by helping organizations replace redundant manual user account provisioning processes with an end-to-end automated provisioning process. It also helps reduce the IT team's burden with provisions for delegating some of the routine tasks to non-admin staff. Some of the important capabilities of ADManager Plus that help reduce IT admin burnout are:

Codeless or no-code automation

ADManager Plus helps IT teams automate routine AD tasks completely or in a controlled manner using workflows according to their organization's requirements. An IT admin can configure this automation just with a few clicks using an intuitive UI and it doesn't require them to write practically any code. This simplifies the job of an IT admin and takes out a great deal of stress from their routine.

Enhanced interoperability

The integration feature in ADManager Plus helps organizations operate multiple applications such as HCM solutions, databases, enterprise apps, etc. in conjunction with the user provisioning tool. This helps IT teams align the applications in their IT environment towards a common purpose rather than each application working in silos. This also improves the harmony between the various stakeholders involved in the provisioning process.

Delegation of tasks

ADManager Plus' help desk delegation capability allows IT teams to empower non-admin staff with the ability to perform routine AD tasks. This lets the IT team focus on more important administrative tasks, while reducing fatigue and the chances of them committing any critical errors.

About ADManager Plus

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians efficiently accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates a comprehensive list of AD reports, some of which are essential requirements to satisfy compliance audits. The solution also helps administrators manage and report on their Exchange Server, Microsoft 365, and Google Workspace environments, all from a single console.

[\\$ Get Quote](#)[↓ Download](#)