ManageEngine
ADManager Plus

5 user provisioning challenges in healthcare and how to solve them

Table of Contents

Introduction

Healthcare is a highly dynamic industry due to the evolving changes in technology and an escalating employee turnover rate. On top of that, healthcare institutions must adhere to strict IT regulations that safeguard the interests of stakeholder data, such as HIPAA and HITECH. All this has made identity access management and user provisioning to be quite the challenge for IT admins in the healthcare industry. Manual methods can be tedious and prone to error, so organizations seek automated user provisioning solutions. But choosing the right solution that helps overcome IT challenges while meeting budget constraints is a tough task.

This e-book discusses some of the routine user provisioning challenges faced by IT admins in the healthcare industry and how to craft custom solutions that befit your healthcare institution with ADManager Plus.

User provisioning challenges in healthcare institutions

IT staff hours wasted on manual operations

The healthcare industry has one of the highest attrition rates compared to other industries. According to a 2022 retention and staffing report by NSI Nursing Solutions, over the past five years, the average US hospital experienced a 100.5% turnover in workforce. With such high turnover, IT admins have the task of frequently updating their identity management platform. They can spend hundreds of hours manually creating and modifying thousands of user accounts and copying user data in Human Capital Management (HCM) solutions, while managing AD and other cloud platforms, tracking and offboarding inactive accounts, and managing user permissions to critical clinical apps. From a healthcare professional's time of onboarding, they will be assigned certain privileges, and over time these privileges may change based on the nature of their role. This can make it even more difficult for the IT team to keep track of these accounts as they simultaneously make modifications in AD and other associated platforms.

Decreased interoperability of legacy applications with the increase in digitization

With the increased adoption of cloud platforms for employee and patient record management, healthcare institutions have undergone large-scale digitization over the past several years. This is a welcome change, as legacy systems are more vulnerable to modern security threats and have limited interoperability with other cloud applications.

Healthcare institutions that lack extensive resources and budgets will prompt their IT admins to rely on native AD tools and implement unsustainable methods such as coding complex PowerShell scripts. This process can be error prone and time-consuming enough to pull the IT admin team away from more critical matters.

Managing temporary medical contractors and consultant accounts

Healthcare institutions often employ contingent workers to address staff shortages or tackle short-term requirements. In organizations where manual provisioning is the norm, properly deprovisioning contingent users can be daunting. Failing to deprovision these temporary external users could pave way for data breaches resulting in the leak of sensitive information such as PHI, PII, financial records, etc., making the institution liable to huge fines and penalties due to compliance violations.

Struggling to produce audit trails for ensuring compliance

All healthcare institutions that store, process, or transmit PHI must strictly adhere to HIPAA and HITECH regulations. Depending on the degree of a HIPAA violation, the department of Health and Human Services (HHS) can impose fines ranging from $100 to $50,000 per violation, with an annual maximum of $1.5 million. But institutions that still rely on manual means of user provisioning and AD management will find it challenging to establish a supervised workflow for their staff. This makes it practically impossible to supervise or cross-check every activity carried out by technicians, resulting in lack of activity records for audits, and leading to compliance violations.

De-provisioning ex-employee accounts to secure patient data

Each organization will have their own policies for decommissioning inactive user accounts. Identity access management in health care institutions is dynamic—manually disabling all inactive accounts seamlessly can be daunting, and IT admins often find it impossible to track down all inactive users accurately for deprovisioning. The health care sector is at the most risk from stale accounts, with 79% of institutions having more than 1,000 orphaned accounts. The existence of stale accounts makes an organizations' network vulnerable, as they provide an opportunity for malicious actors to infiltrate and gain access to confidential internal resources.

Automated user provisioning solutions from ADManager Plus

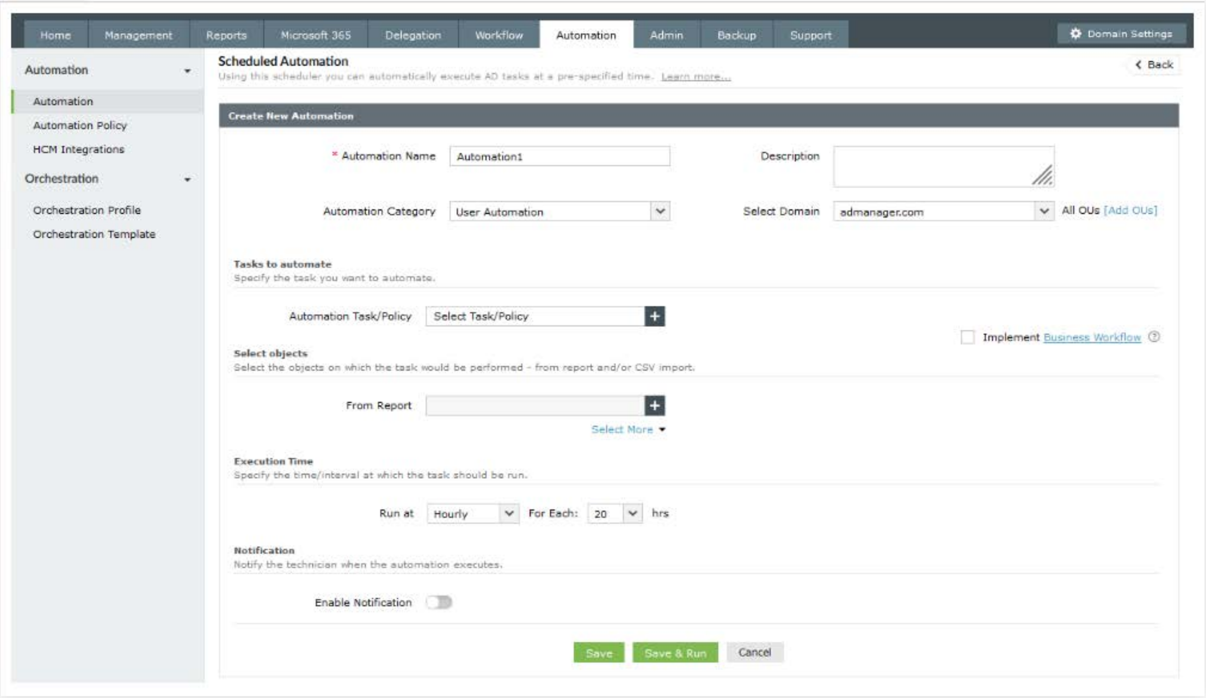
ManageEngine's AdManager Plus is a user-friendly, comprehensive solution that helps you automate AD management tasks like user provisioning and group policy management. Optimize user provisioning for your healthcare institution with automated solutions from ADManager Plus.

Automated lifecycle management

Healthcare institutions manage a diverse and fluid workforce ranging from clinicians, technicians, contingent workers, administrative staff, partners, and vendors. ADManager Plus helps you simplify challenging tasks that may cost your IT team operational efficiency. The solution offers a wide range of features for automated user provisioning, such as the ability to create and manage users and groups, resetting passwords, and managing permissions and access controls. Further, it allows IT admins and technicians via role-based access control (RBAC) to set up supervised workflows and implement orchestration for a sequence of routine automated tasks.

Bulk user management:

ADManager Plus allows IT admins to provision users accounts in bulk across AD, Microsoft 365, Google Workspace, and Exchange servers without having to rely on time-consuming, outdated legacy AD management tools or coding complex PowerShell scripts. With ADManager Plus, you can import user details via CSV files or based on inputs from your institution's HCM solutions and implement sequential follow-up tasks at predetermined intervals for routine bulk user management functions.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: admanager.com — All OUs [Add OUs]

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Select Task/Policy

□ Implement Business Workflow

Select objects

Select the objects on which the task would be performed - from report and/or CSV import.

From Report:

Select More

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly — For Each: 20 hrs

Notification

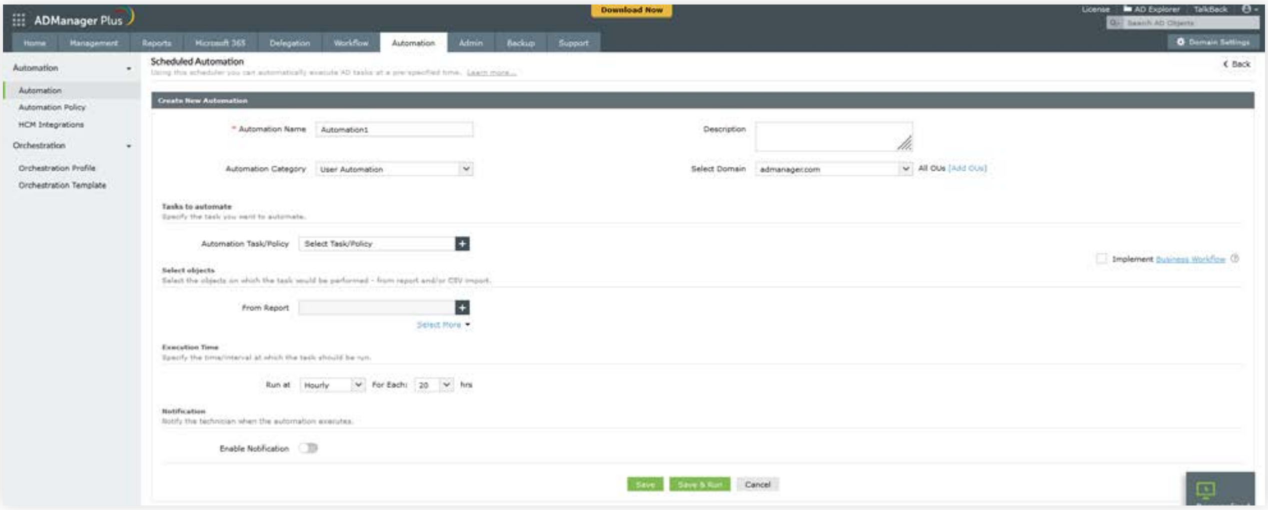
Notify the technician when the automation executes.

Enable Notification

Templates:

Healthcare institutions can use rule-based user provisioning templates by setting up predetermined attributes for each role based on every department, both medical and non-medical, and adhering to organizational policies.

ADManager Plus' templates help you create reactive provisioning measures for every situation. Set up user creation rules for every scenario like creation and modification templates for users, computers, groups, contacts, mailboxes, and OUs to help IT admins save time and effort.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: admanager.com All OUs [Add OUs]

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Select Task/Policy

□ Implement Business Workflow

Select objects

Select the objects on which the task would be performed - from report and/or CSV import.

From Report:

Select More

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly For Each: 20 hrs

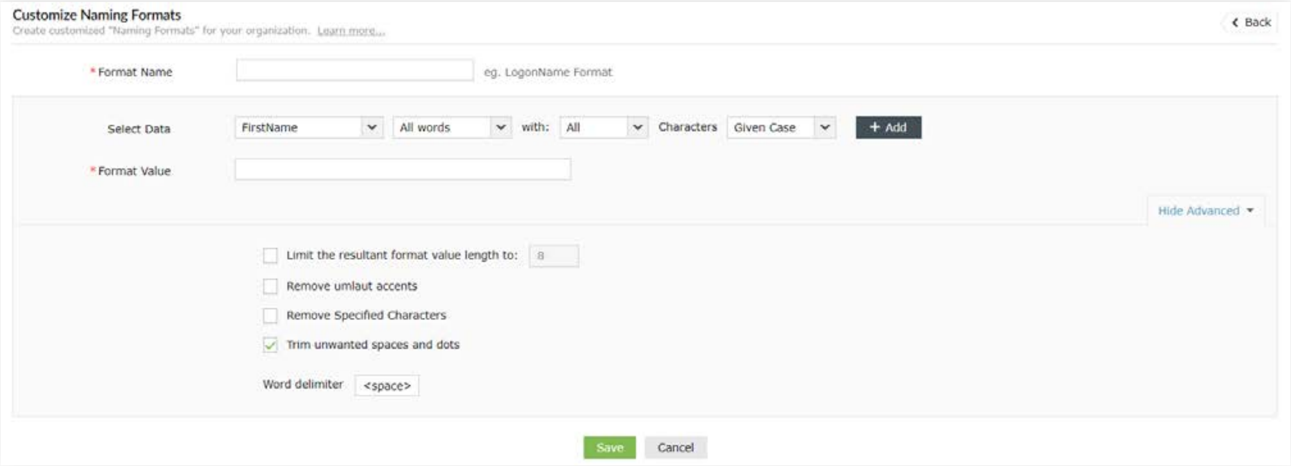
Notification

Notify the technician when the automation executes.

Enable Notification

Custom naming formats:

ADManager Plus' custom naming format templates let you create unique logon names using a custom naming format to avoid duplication during bulk user creation.



Customize Naming Formats

Create customized "Naming Formats" for your organization. Learn more...

* Format Name: eg. LogonName Format

Select Data: FirstName All words with: All Characters Given Case

* Format Value:

□ Limit the resultant format value length to: 8

□ Remove umlaut accents

□ Remove Specified Characters

☑ Trim unwanted spaces and dots

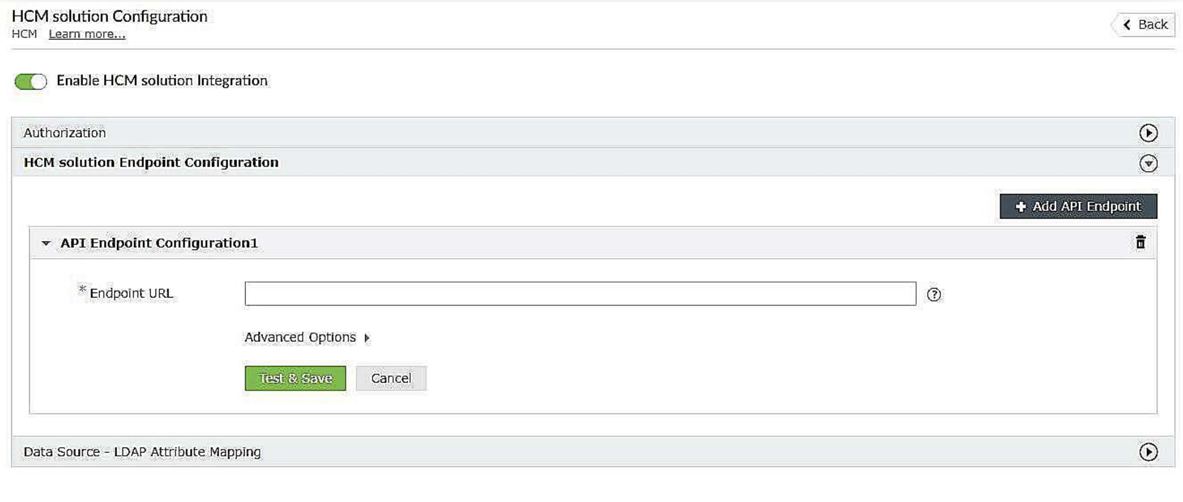
Word delimiter: <space>

Enterprise-ready integrations

According to a survey from HIMSS, more than 83% of healthcare institutions now make use of cloud platforms. With ADManager Plus, IT administrators can integrate user data across various cloud applications and HR management solutions with API support.

i. Custom HCM integrations:

Your healthcare institution can use ADManager Plus to seamlessly integrate HCM applications like UKG Pro, BambooHR, and Workday with API support, and databases like Microsoft SQL or Oracle to automatically reflect user provisioning changes in your AD accounts and other associated cloud platforms.



HCM solution Configuration

HCM Learn more...

Enable HCM solution Integration: on

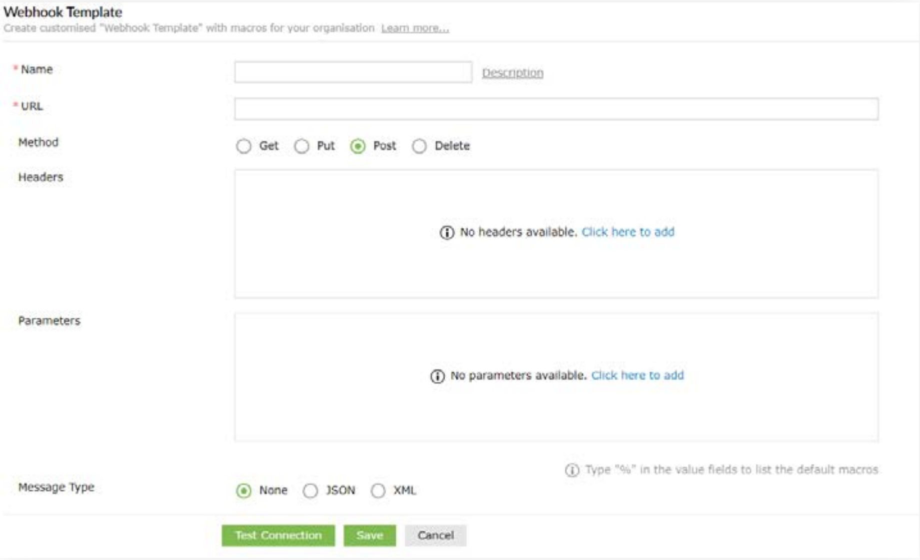
API Endpoint Configuration1

* Endpoint URL:

Back
Authorization
HCM solution Endpoint Configuration
Add API Endpoint
Advanced Options
Test & Save
Cancel
Data Source - LDAP Attribute Mapping

ii. Webhooks:

ADManager Plus' webhook integration with your target application lets you automate user creation, modification, and deletion whenever the webhook POSTs to a specific URL.



Webhook Template

Create customised "Webhook Template" with macros for your organisation Learn more...

* Name:

* URL:

Method: ○ Get ○ Put ● Post ○ Delete

Headers: No headers available. Click here to add

Parameters: No parameters available. Click here to add

Type "%" in the value fields to list the default macros

Message Type: ● None ○ JSON ○ XML

iii. REST APIs:

Integrate ADManager Plus with other applications using REST APIs. Carry out AD management activities such as user creation, user modification, user deletion, password reset, and more by integrating with other applications using REST APIs.

Role-based access control

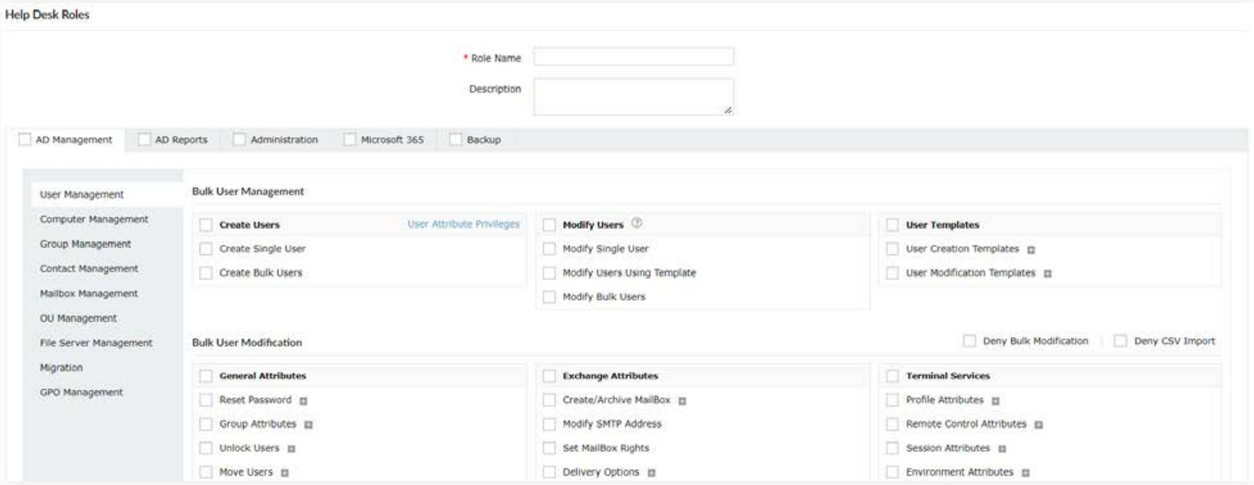
ADManager Plus lets you manage user access privileges for your stakeholders by the principle of least privilege (PoLP). Provide doctors, nurses, operational staff, and contingent users access to resources based on their roles.

IT admins can reduce their burden by automating processes like managing group memberships and access to files or folders by providing birthright access for every staff that joins the healthcare institution from their date of joining. Limit a user's access scope based on their OUs and groups to reduce chances for unauthorized access to sensitive information like PHI and PII.

Delegated administration

Using ADManager Plus reduces the burden on your IT admin staff by delegating routine user provisioning functions to non-technicians without the risk of elevating the user's AD rights. Delegate repetitive tasks like managing group memberships, OU changes, folder permissions, password reset, and account unlocking to technicians with non-admin rights.

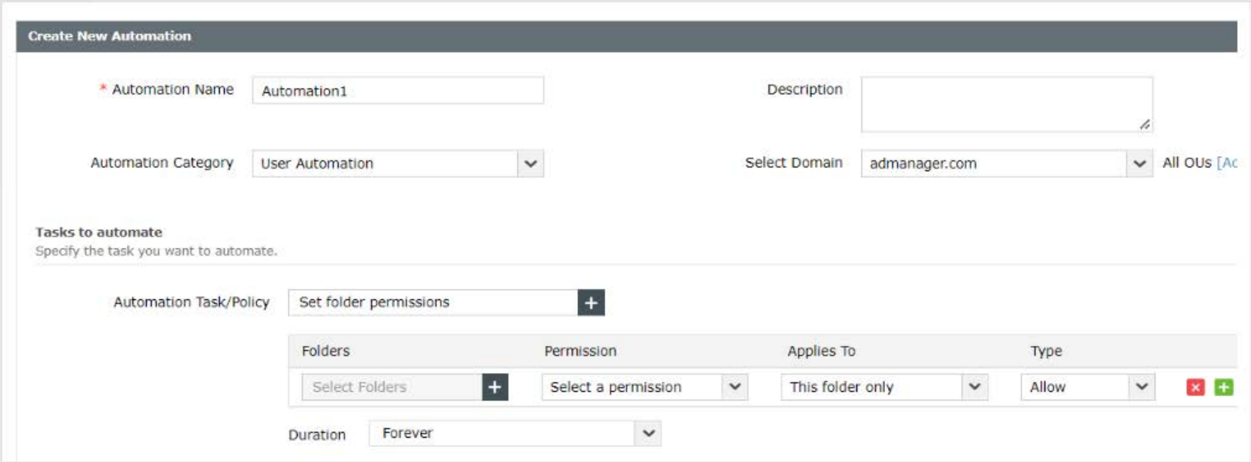
Authorize key personnel such as physicians, department heads, and senior operational staff with delegated administrative rights to take care of repetitive routine functions such as modifying permissions and allocating and removing group members. This reduces dependencies on the IT admin staff, leaving them more time to address critical aspects of AD management.



Just-in-time (JIT) access

Considering the nature of sensitive data in health care institutions, it is essential to ensure that there is no unrestricted or arbitrary access for anyone in the organization. With ADManager Plus templates, manage user permission to files and folders by providing JIT access for your guest users for a specified, limited duration.

During unprecedented events like pandemics or natural calamities, it is likely for healthcare institutions to onboard temporary medical staff for additional support. Seamlessly manage ad hoc requests from your contingent users, granting them access to the required resources for a specific duration without causing any delays, while safeguarding data security.



Create New Automation

* Automation Name: Automation1
Description:
Automation Category: User Automation
Select Domain: admanager.com — All OUs [Ac

Tasks to automate
Specify the task you want to automate.

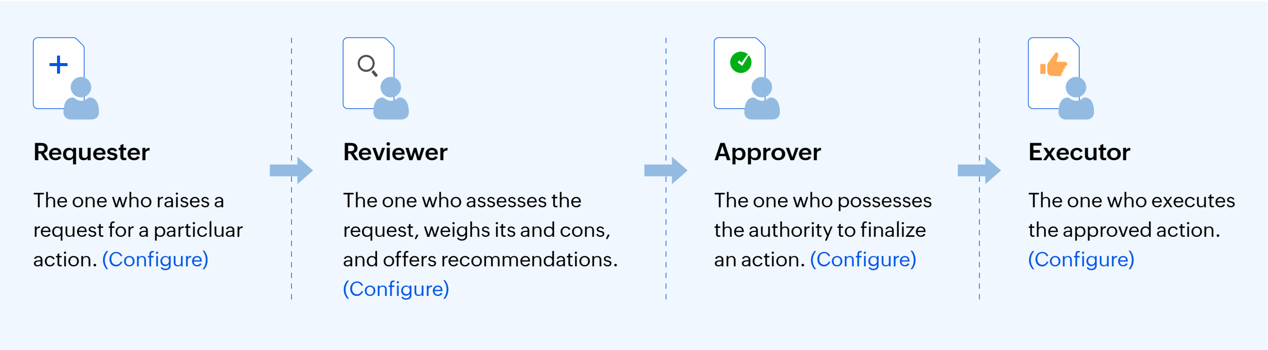
Automation Task/Policy: Set folder permissions

Folders	Permission	Applies To	Type
Select Folders	Select a permission	This folder only	Allow

Duration: Forever

Enhance security and compliance

Using ADManager Plus, create a workflow that enables controlled automation with adequate supervision from key personnel like department heads and managers for every activity carried out by technicians and non-technicians. Introducing a supervised workflow will reduce the risk of errors and create a ticket-based system for every AD management activity. Having an audit trail record for every AD activity will help healthcare institutions adhere to compliance measures such as HIPAA and HITECH.



Requester

The one who raises a request for a particluar action. (Configure)

Reviewer

The one who assesses the request, weighs its and cons, and offers recommendations. (Configure)

Approver

The one who possesses the authority to finalize an action. (Configure)

Executor

The one who executes the approved action. (Configure)

About ManageEngine ADManager Plus

ManageEngine ADManager Plus is a web-based Windows Active Directory management and reporting solution that helps Active Directory administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks, like AD object backup and recovery, and generates an exhaustive list of Active Directory reports, many of which are essential requirements for satisfying compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, G Suite, and Active Directory environments—all from a single console.

$ Get Quote

⤓ Download