ManageEngine
M365 Manager Plus

Simplifying Microsoft 365 user life cycle management using automation

www.microsoft365managerplus.com

Introduction

User accounts go through various stages, including user creation, role assignment, addition to or deletion from groups, and account deletion. However, managing user accounts and their various life cycles is not without its share of challenges.

Admins need to quickly onboard new employees and provide them access to all the resources they need to do their job. On top of this, admins also have to keep up with employee role changes, promotions, transfers, etc., and modify user accounts accordingly.

Another important task for admins is ensuring their environment follows the principle of least privilege, i.e., employees should only have access to the resources they need for their roles. Whenever an employee's role changes or they leave the organization, their access permissions need to change or their account needs to be deprovisioned, respectively.

With native Microsoft 365 management tools, admins have to perform these tedious tasks manually. Not only is this time-consuming, but it also introduces the risk of human error including unintentional privilege escalation, denial of rightful access leading to loss of productivity, and more.

In this e-book, we'll discuss the challenges administrators face in user life cycle management, and how to address these challenges using M365 Manager Plus, ManageEngine's Microsoft 365 management, reporting, monitoring, auditing, and alerting solution.

User life cycle management challenges

1. Inefficient user onboarding

Providing proper permissions to new employees is a major challenge for IT admins, as they may not know what level of access is required for every role. Using native Microsoft 365 management tools, admins have to create accounts manually and provision the correct level of access, which is time-consuming and error-prone. Employees often end up not getting enough access, which hinders their work performance, or getting too much access, which creates a security risk for the organization.

2. Manual user offboarding

When an employee leaves an organization, their access to the organization's resources must be terminated immediately. If admins are managing user accounts manually, there's always the risk someone will forget to deprovision an account, or put the task off.

Over time, inactive user accounts will begin to collect in the Microsoft 365 environment, often without the knowledge of admins. These stale accounts are a huge security risk, as hackers can exploit these accounts to gain access to critical business information.

3. Entitlement creep

During the course of an employee's career, they may get promoted or transferred, which will likely change their role and responsibilities. This, in turn, may affect their group memberships, organizational units, and more.

Admins have to keep up with all role changes in the organization and modify users' account access permissions as needed. Unfortunately, admins often forget to remove permissions associated with an employee's previous role before granting permissions for their new role. This means that over the span of their careers, employees can accumulate access permissions that they no longer need. These accumulated access permissions, or entitlement creep, can prove disastrous for the organization's security.

4. Just-in-time access

There are some situations when users need temporary access to resources. For instance, a marketing analyst might require temporary access to the sales team's resources to gauge the results of a marketing campaign. Admins often grant temporary access to resources and forget to revoke the permission after access is no longer required.

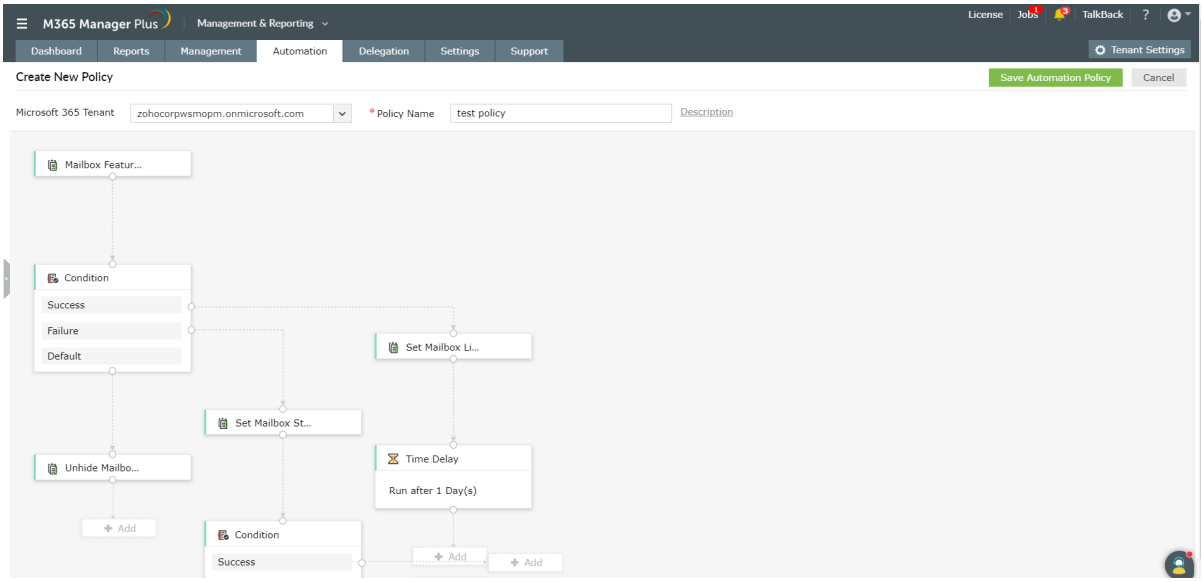
5. Repetitive tasks

One of the most repetitive and time-consuming identity management activities is resetting passwords. A Gartner study finds that 20-50 percent of all help desk calls are for password resets, thus taking up the lion's share of an admin's time. On top of this, research by Forrester shows that the average cost of a single password reset is $70.

Automating routine Microsoft 365 tasks with M365 Manager Plus

The Microsoft 365 Admin Center does not offer automations for user life cycle management tasks like user provisioning and deprovisioning, license management, and access permissions management. Even if admins use scripts to simplify some of these tasks, they have to constantly modify them, meaning scripts can't be used to completely automate any of these processes.

With M365 Manager Plus' graphical interface, admins can lay out a series of tasks to be carried out, and save these as automation policies. When a certain event occurs, these series of events will run automatically.



M365 Manager Plus's event-driven automation: User onboarding

With M365 Manager Plus' automation capabilities, admins can:

- **Schedule Microsoft 365 management tasks:** Admins can schedule individual user or mailbox management tasks to be executed at specific intervals.

- **Customize automation policies using flowcharts:** Admins can create automation policies using flowcharts to carry out chains of tasks at specific intervals.

- **Audit admin activities:** With detailed audit reports, the tool keeps track of the automation policies created, modified, delegated, and modified by admins and technicians.

- **Get input from multiple data sources:** For the automated tasks, the tool accepts CSV files, M365 Manager Plus reports, and shared locations are all accepted as input to automate tasks. Admins can use the appropriate M365 Manager Plus report as a data source for automated tasks instead of entering the data manually. For example, to reset user account passwords using M365 Manager Plus, the Password Expired Users report can be used as the data source.

How M365 Manager Plus solves Microsoft 365 life cycle management challenges

Using M365 Manager Plus, admins can automate routine user life cycle management tasks, enabling their organization to save on the costs and resources spent on user life cycle management.

1 Efficient user onboarding

An efficient IAM solution will help admins create user accounts automatically based on inputs from the HR team to provide users proper permissions without error or delay.

M365 Manager Plus lets admins configure event-driven automation policies that can be created in the form of condition-based flow charts. Admins can simply provide the list of users and the solution will create user accounts, assign licenses, enable mailboxes, configure multi-factor authentication (MFA), add users to appropriate groups as required by their roles, and more.

2 Automated user offboarding

A solid IAM solution lets admins automatically perform the necessary offboarding activities so that no orphan user accounts remain in the Microsoft 365 environment.

M365 Manager Plus helps admins streamline user deprovisioning by automating the removal of employees who are leaving the organization from all groups, deleting or removing their licenses, forwarding their emails to another employee or converting their mailboxes to shared mailboxes, removing mobile devices, disabling their accounts, and more. Admins only have to add the list of user accounts to be deprovisioned in a CSV file and schedule the necessary automations at required frequencies.

3 Principle of least privilege

Entitlement creep can be eliminated by using an IAM solution that allows admins to dynamically add or remove access rights when a user changes roles. M365 Manager Plus helps admins automate permission, license, and group membership changes when a user is promoted or transferred, helping to maintain up-to-date permissions for user accounts when there are role changes.

4 Just-in-time access

The challenge of providing temporary access to user accounts can be solved with time-based access permissions; admins can grant permissions for a specified time, and when that time expires, permissions will be automatically revoked.

Using time-based permissions for resources lets admins essentially set it and forget it; they can set the time for which users will gain temporary access, and forget about having to revoke it later without putting the organization at risk.

5 Password reset automation

M365 Manager Plus reduces the burden of repeat password reset requests by letting admins automate the process of resetting passwords of locked-out or expired user accounts by fetching the required details from prebuilt reports or CSV files.