ManageEngine
M365 Manager Plus

Simplifier la gestion du cycle de vie des utilisateurs de Microsoft 365 grâce à l'automatisation

www.manageengine.fr/m365mp

Introduction

Les comptes utilisateurs passent par différentes étapes, notamment la création d'un utilisateur, l'attribution d'un rôle, l'ajout ou la suppression d'un groupe et la suppression d'un compte. Cependant, la gestion des comptes utilisateurs et de leurs différents cycles de vie n'est pas sans poser quelques problèmes.

Les administrateurs doivent rapidement intégrer les nouveaux employés et leur donner accès à toutes les ressources dont ils ont besoin pour faire leur travail. En outre, les administrateurs doivent également suivre les changements de rôle des employés, les promotions, les transferts et modifier les comptes utilisateurs en conséquence.

Une autre tâche importante des administrateurs est de s'assurer que leur environnement respecte le principe du moindre privilège, c'est-à-dire que les employés ne doivent avoir accès qu'aux ressources dont ils ont besoin pour leur rôle. Chaque fois que le rôle d'un employé change ou qu'il quitte l'entreprise, ses autorisations d'accès doivent être modifiées ou son compte doit être supprimé, selon le cas.

Avec les outils de gestion natifs Microsoft 365, les administrateurs doivent effectuer ces tâches fastidieuses manuellement. Non seulement cela prend du temps, mais cela introduit également un risque d'erreur humaine, notamment une élévation de privilèges involontaire, un refus d'accès légitime entraînant une perte de productivité, etc.

Dans cet e-book, nous aborderons les défis auxquels les administrateurs sont confrontés dans la gestion du cycle de vie des utilisateurs, et la façon de relever ces défis à l'aide de M365 Manager Plus, la solution de gestion, reporting, surveillance, audit, et alertes Microsoft 365 de ManageEngine.

Les défis de la gestion du cycle de vie des utilisateur

1. Intégration inefficace des utilisateurs

Fournir les autorisations appropriées aux nouveaux employés est un défi majeur pour les administrateurs informatiques, car ils ne savent pas toujours quel niveau d'accès est requis pour chaque rôle. En utilisant les outils de gestion natifs Microsoft 365, les administrateurs doivent créer des comptes manuellement et fournir le bon niveau d'accès, ce qui prend beaucoup de temps et entraîne des erreurs. Les employés finissent souvent par ne pas avoir un accès suffisant, ce qui entrave leurs performances professionnelles, ou par avoir un accès trop important, ce qui crée un risque de sécurité pour l'entreprise.

2. Sortie manuelle des utilisateurs

Lorsqu'un employé quitte une entreprise, son accès aux ressources de l'entreprise doit être désactivé immédiatement. Si les administrateurs gèrent les comptes utilisateurs manuellement, il y a toujours un risque que quelqu'un oublie de supprimer un compte ou repousse cette tâche à plus tard.

Au fil du temps, les comptes utilisateurs inactifs commencent à s'accumuler dans l'environnement Microsoft 365, souvent à l'insu des administrateurs. Ces comptes obsolètes représentent un énorme risque pour la sécurité, car les pirates peuvent les exploiter pour accéder à des informations professionnelles essentielles.

3. Dérive des droits

Au cours de sa carrière, un employé peut être promu ou muté, ce qui modifiera probablement son rôle et ses responsabilités. Cela peut également avoir une incidence sur leur appartenance à un groupe, à une unité d'organisation, etc.

Les administrateurs doivent se tenir au courant de tous les changements de rôle dans l'entreprise et modifier les autorisations d'accès aux comptes des utilisateurs si nécessaire. Malheureusement, les administrateurs oublient souvent de supprimer les autorisations associées au rôle précédent d'un employé avant d'accorder des autorisations pour son nouveau rôle. Cela signifie qu'au cours de leur carrière, les employés peuvent accumuler des autorisations d'accès dont ils n'ont plus besoin. Ces autorisations d'accès accumulées, ou dérive des droits, peuvent s'avérer désastreuses pour la sécurité de l'entreprise.

4. Accès ponctuel

Dans certaines situations, les utilisateurs ont besoin d'un accès temporaire aux ressources. Par exemple, un analyste marketing peut avoir besoin d'un accès temporaire aux ressources de l'équipe commerciale pour évaluer les résultats d'une campagne marketing. Les administrateurs accordent souvent un accès temporaire aux ressources et oublient de retirer l'autorisation lorsque l'accès n'est plus nécessaire.

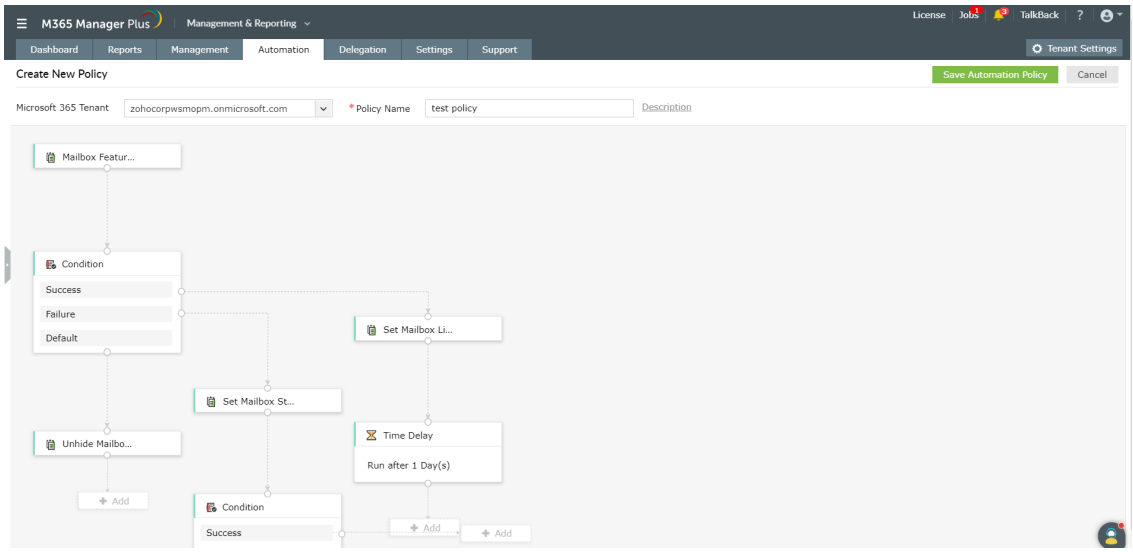
5. Tâches répétitives

L'une des activités de gestion des identités les plus répétitives et les plus chronophages est la réinitialisation de mot de passe. Selon une étude Gartner, 20 à 50 % de tous les appels au helpdesk concernent la réinitialisation de mot de passe, ce qui représente la majeure partie du temps d'un administrateur. En outre, une étude de Forrester montre que le coût moyen d'une seule réinitialisation de mot de passe est de 63 euros.

Automatisation des tâches courantes Microsoft 365 avec M365 Manager Plus

Le centre d'administration Microsoft 365 n'offre pas d'automatisation pour les tâches de gestion du cycle de vie des utilisateurs, comme la création et la suppression des utilisateurs, la gestion des licences et la gestion des autorisations d'accès. Même si les administrateurs utilisent des scripts pour simplifier certaines de ces tâches, ils doivent constamment les modifier, ce qui signifie que les scripts ne peuvent pas être utilisés pour automatiser complètement l'un de ces processus.

Grâce à l'interface graphique M365 Manager Plus, les administrateurs peuvent définir une série de tâches à exécuter et les enregistrer en tant que stratégies d'automatisation. Lorsqu'un certain événement se produit, ces séries d'événements s'exécutent automatiquement.



L'automatisation pilotée par les événements M365 Manager Plus : Intégration des utilisateurs

Grâce aux capacités d'automatisation de M365 Manager Plus, les administrateurs peuvent :

- **Planifier les tâches de gestion Microsoft 365 :** Les administrateurs peuvent planifier des tâches de gestion utilisateurs ou de boîtes aux lettres individuelles à exécuter à des intervalles spécifiques.

- **Personnaliser les stratégies d'automatisation à l'aide d'organigrammes :** Les administrateurs peuvent créer des stratégies d'automatisation à l'aide d'organigrammes pour exécuter des chaînes de tâches à des intervalles spécifiques.

- **Audit des activités des administrateurs :** Grâce à des rapports d'audit détaillés, l'outil assure le suivi des stratégies d'automatisation créées, modifiées, déléguées et modifiées par les administrateurs et les techniciens.

- **Obtenir des entrées à partir de plusieurs sources de données :** Pour les tâches automatisées, l'outil accepte les fichiers CSV, les rapports M365 Manager Plus, et les emplacements partagés sont tous acceptés comme entrée pour automatiser les tâches. Les administrateurs peuvent utiliser le rapport M365 Manager Plus approprié comme source de données pour les tâches automatisées au lieu de saisir les données manuellement. Par exemple, pour réinitialiser les mots de passe des comptes utilisateurs à l'aide de M365 Manager Plus, le rapport "Password Expired Users" peut être utilisé comme source de données.

Comment M365 Manager Plus résout les problèmes de gestion du cycle de vie Microsoft 365

Grâce à M365 Manager Plus, les administrateurs peuvent automatiser les tâches courantes de gestion du cycle de vie des utilisateurs, ce qui permet à leur entreprise de réduire les coûts et les ressources consacrés à la gestion du cycle de vie des utilisateurs.

1 Intégration efficace des utilisateurs

Une solution IAM efficace aidera les administrateurs à créer automatiquement des comptes utilisateurs sur la base des données fournies par l'équipe RH, afin de fournir aux utilisateurs les autorisations appropriées sans erreur ni retard.

M365 Manager Plus permet aux administrateurs de configurer des stratégies d'automatisation en fonction des événements, qui peuvent être créées sous la forme d'organigrammes basés sur des conditions. Les administrateurs peuvent simplement fournir la liste des utilisateurs et la solution créera les comptes utilisateurs, attribuera les licences, activera les boîtes aux lettres, configurera l'authentification multifacteur (MFA), ajoutera les utilisateurs aux groupes appropriés en fonction de leurs rôles, etc.

2 Sortie automatisée des utilisateurs

Une solution IAM solide permet aux administrateurs d'effectuer automatiquement les activités d'exclusion nécessaires afin qu'aucun compte utilisateur orphelin ne subsiste dans l'environnement Microsoft 365.

M365 Manager Plus aide les administrateurs à optimiser le déprovisionnement des utilisateurs en automatisant la suppression des employés qui quittent l'entreprise de tous les groupes, en supprimant ou en retirant leurs licences, en transférant leurs e-mails à un autre employé ou en convertissant leurs boîtes aux lettres en boîtes aux lettres partagées, en supprimant les appareils mobiles, en désactivant leurs comptes, etc. Les administrateurs n'ont qu'à ajouter la liste des comptes utilisateurs à supprimer dans un fichier CSV et à planifier les automatisations nécessaires aux fréquences requises.

3 Principe du moindre privilège

La dérive des droits peut être éliminée en utilisant une solution IAM qui permet aux administrateurs d'ajouter ou de supprimer dynamiquement des droits d'accès lorsqu'un utilisateur change de rôle. M365 Manager Plus aide les administrateurs à automatiser les changements d'autorisation, de licence et d'appartenance à un groupe lorsqu'un utilisateur est promu ou transféré, ce qui permet de maintenir les autorisations à jour pour les comptes utilisateurs en cas de changement de rôle.

4 Accès ponctuel

Le défi de fournir un accès temporaire aux comptes utilisateurs peut être résolu avec des autorisations d'accès basées sur le temps ; les administrateurs peuvent accorder des autorisations pour une période déterminée, et lorsque cette période expire, les autorisations seront automatiquement retirées.

L'utilisation d'autorisations temporelles pour les ressources permet aux administrateurs de définir et d'oublier l'accès ; ils peuvent fixer la durée pendant laquelle les utilisateurs obtiendront un accès temporaire et ne pas avoir à le retirer plus tard sans mettre l'entreprise en danger.

5 Automatisation de la réinitialisation de mot de passe

M365 Manager Plus réduit la charge des demandes répétées de réinitialisation de mot de passe en permettant aux administrateurs d'automatiser le processus de réinitialisation de mots de passe des comptes utilisateurs verrouillés ou expirés en récupérant les détails requis à partir de rapports prédéfinis ou de fichiers CSV.