Aperçu des identifiants Apple gérés pour les entreprises

Pour bien utiliser les produits Apple en entreprise, il est important de comprendre comment les identifiants Apple gérés soutiennent les services dont vos employés ont besoin. Ces identifiants sont des comptes qui donnent accès aux services clés d'Apple – et ils sont conçus spécialement pour les entreprises.

Dans Apple Business Manager, les entreprises peuvent créer automatiquement des identifiants Apple gérés pour leurs employés. Ceux-ci peuvent alors collaborer avec les apps et les services d'Apple et accéder aux données de l'entreprise dans des apps gérées compatibles avec iCloud Drive. Et grâce à l'authentification fédérée, les comptes tirent parti des identifiants existants de l'infrastructure détenue et gérée par l'entreprise.

Que sont les identifiants Apple gérés?

À l'instar de l'identifiant Apple grand public, l'identifiant Apple géré sert à personnaliser un appareil. Il donne aussi accès aux apps et aux services d'Apple, et permet aux équipes de TI d'accéder à Apple Business Manager. Toutefois, contrairement à l'identifiant Apple grand public, l'identifiant Apple géré est détenu et géré par l'entreprise, qui s'occupe de la réinitialisation des mots de passe et de l'administration des rôles.

Dans Apple Business Manager, il est facile de créer un identifiant Apple géré unique pour chaque employé. Et grâce à l'intégration de Microsoft Azure Active Directory, les entreprises peuvent fournir des identifiants Apple gérés aux employés au moyen des identifiants existants.

L'identifiant Apple géré peut être utilisé conjointement avec un identifiant Apple personnel sur l'appareil d'un employé grâce à l'inscription par l'utilisateur sous iOS, iPadOS et macOS Catalina. Il est également possible d'utiliser un identifiant Apple géré sur n'importe quel appareil en tant qu'identifiant Apple principal et unique. L'identifiant Apple géré donne aussi accès à iCloud en ligne dès la première ouverture de session sur un appareil Apple.

L'utilisation d'identifiants Apple n'est pas essentielle au déploiement. Il est possible de gérer des appareils Apple et d'y distribuer des apps sans identifiant Apple. Familiarisez-vous avec les services que votre entreprise a l'intention d'utiliser et évaluez la meilleure stratégie de transition vers l'adoption des identifiants Apple gérés. Puisque l'identifiant Apple géré est réservé aux activités commerciales, certaines fonctionnalités sont désactivées pour protéger les entreprises.

Fonctionnalités pour les entreprises

- **Accès aux services d'Apple –** Les employés ont accès aux services d'Apple comme iCloud et la collaboration dans iWork et Notes. Les courriels sont désactivés, tandis que FaceTime et iMessage sont accessibles seulement lorsqu'un identifiant Apple géré est le seul identifiant Apple d'un appareil.
- **Recherche de comptes d'utilisateur –** Permet aux employés de rechercher les coordonnées d'autres utilisateurs dans le répertoire Apple Business Manager de l'entreprise pour simplifier la collaboration dans diverses apps.
- **Création de compte simplifiée –** Dans Apple Business Manager, un compte est créé automatiquement lorsqu'un employé ouvre une session sur un appareil Apple pour la première fois.
- **Authentification fédérée –** Les administrateurs peuvent lier Apple Business Manager à Microsoft Azure Active Directory, de manière à ce que la configuration des comptes d'employés se fasse automatiquement à partir des identifiants d'entreprise existants.
- **Rôles et privilèges –** Les administrateurs peuvent créer et attribuer des rôles et des privilèges pour permettre aux équipes de TI d'utiliser les diverses fonctionnalités d'Apple Business Manager.
- **Confidentialité et sécurité intégrées –** L'identifiant Apple géré emploie les mêmes techniques de chiffrement de données que l'identifiant Apple grand public. Il bloque également les publicités ciblées de la plateforme publicitaire d'Apple. Les opérations commerciales sont désactivées, de même que l'accès aux services Apple Pay et Wallet. L'app Localiser est désactivée, puisque les entreprises ont accès au mode Perdu de la solution de GAM.

Authentification fédérée

Grâce à l'authentification fédérée, vous pouvez lier Apple Business Manager à Microsoft Azure Active Directory (Azure AD) pour permettre aux employés d'employer leur nom d'utilisateur et leur mot de passe existants à titre d'identifiant Apple géré.

Microsoft Azure AD est le fournisseur d'identités, qui stocke les noms d'utilisateur et les mots de passe des comptes que vous voulez utiliser dans Apple Business Manager.

Une fois le lien établi avec Microsoft Azure AD, les identifiants Apple gérés sont soumis aux mêmes politiques régissant les mots de passe, parce qu'ils sont fédérés au moyen d'identifiants existants.

L'identifiant Apple géré est généré automatiquement dès que l'utilisateur ouvre une session sur son appareil Apple. L'équipe des TI n'a donc pas besoin d'en créer un au préalable.

Les employés peuvent utiliser leurs identifiants Azure AD pour accéder à iCloud Drive, Notes, Rappels et d'autres services de collaboration d'Apple.

Parce que l'entreprise gère déjà les identités, toutes les politiques et les réinitialisations de mots de passe sont traitées par un administrateur ou par l'utilisateur dans Microsoft Azure AD.

Exigences pour l'authentification fédérée

- **Microsoft Azure Active Directory –** Si vous avez déjà cet outil, vous n'aurez aucune difficulté à utiliser l'authentification fédérée.
- **Répertoire Active Directory local –** D'autres opérations de configuration sont nécessaires pour synchroniser le répertoire avec Azure AD. Microsoft met à votre disposition de la documentation et un outil de synchronisation (voir les liens ci-après).

Configurer l'authentification fédérée

1. **Vérifiez le nom de domaine auprès d'Apple.** Dans Apple Business Manager, connectez-vous avec un compte d'administrateur ou de gestionnaire de comptes, et ajoutez le ou les domaines que vous voulez fédérer.
2. **Connectez-vous à Microsoft Azure Active Directory et accordez l'accès à Apple Business Manager.** Ouvrez une session dans Azure AD avec un compte d'administrateur global ou d'administrateur d'applications pour accorder les permissions qui permettront à Apple Business Manager d'accéder au profil des utilisateurs.
3. **Vérifiez à qui appartient le domaine dans Microsoft Azure Active Directory.** Une fois le lien de confiance établi, continuez de suivre le processus pour vérifier le ou les domaines. Dans Apple Business Manager, ouvrez une session dans Microsoft Azure AD avec un compte dont le nom se termine par le domaine que vous souhaitez fédérer. Cette étape vous permet de vérifier la configuration du domaine et de prouver l'appartenance.
4. **Vérifiez l'existence d'éventuels conflits dans les domaines.** Apple Business Manager vérifie la possibilité de conflits avec les identifiants Apple actuels dans votre ou vos domaines, ou encore avec des identifiants Apple gérés configurés par une autre organisation utilisant le même domaine.
5. **Entamez la résolution des conflits de domaines.** Si Apple Business Manager découvre qu'un identifiant Apple personnel utilise le nom de domaine que vous voulez fédérer, l'utilisateur sera avisé et devra changer l'adresse courriel associée à son identifiant Apple. Toutes les données et tous les achats restent toutefois associés à l'identifiant Apple personnel de l'utilisateur.
6. **Transférez les comptes existants.** Si vous avez déjà des identifiants Apple gérés, vous pouvez les transférer dans le système d'authentification fédérée en modifiant les données pour qu'elles correspondent à celles du nom de domaine fédéré et au nom d'utilisateur.

Ressources

- Guide de démarrage d'Apple Business Manager
- Guide de l'utilisateur d'Apple Business Manager
- En savoir plus sur la création d'identifiants Apple gérés dans Apple Business Manager
- Introduction à l'authentification fédérée des appareils dans Apple Business Manager
- En savoir plus sur les conflits avec les identifiants Apple existants
- En savoir plus sur l'intégration d'un répertoire AD local avec Azure AD