Présentation des identifiants Apple gérés pour les entreprises

Lorsque vous utilisez des produits Apple au sein de votre organisation, il est important de comprendre le rôle des identifiants Apple gérés dans le cadre des services qui peuvent être utiles à vos employés. Les identifiants Apple gérés sont des comptes spécifiquement conçus pour les entreprises qui utilisent les principaux services d'Apple.

Les organisations peuvent tirer parti d'Apple Business Manager pour créer automatiquement des identifiants Apple gérés et permettre à leurs employés de collaborer dans les apps et les services Apple, ou encore d'accéder aux données de l'entreprise dans les apps gérées utilisant iCloud Drive. Avec l'authentification fédérée, ces comptes peuvent conserver les identifiants qu'ils utilisent déjà au sein de l'infrastructure existante, qui est détenue et gérée par l'entreprise.

Que sont les identifiants Apple gérés ?

Comme tous les identifiants Apple, les identifiants Apple gérés permettent de personnaliser un appareil. Ils donnent aussi accès aux apps et aux services Apple, et permettent aux équipes informatiques d'utiliser Apple Business Manager. Contrairement aux identifiants Apple, les identifiants Apple gérés sont détenus et gérés par l'organisation, qui assure notamment la réinitialisation des mots de passe et l'administration en fonction des rôles.

Avec Apple Business Manager, il est plus simple de créer un identifiant Apple géré unique pour chaque employé d'une organisation. Et grâce à l'intégration de Microsoft Azure Active Directory, les organisations peuvent utiliser les identifiants professionnels des employés pour leur fournir des identifiants Apple gérés.

Dans les entreprises ayant opté pour l'inscription des utilisateurs, les appareils iOS, iPadOS ou macOS Catalina appartenant aux utilisateurs peuvent utiliser à la fois un identifiant Apple géré et un identifiant Apple personnel. Un identifiant Apple géré peut aussi être utilisé sur n'importe quel appareil en tant qu'identifiant Apple principal et unique. Et après une première connexion à un appareil Apple, l'utilisateur pourra s'en servir pour accéder à iCloud sur le Web.

Il n'y a aucune obligation technique de déploiement d'appareils avec un identifiant Apple. Il est possible de gérer les appareils Apple et de distribuer les apps sans identifiant Apple. Étudiez les services que votre organisation compte utiliser et identifiez la meilleure stratégie pour passer aux identifiants Apple gérés. Ces derniers étant destinés aux entreprises uniquement, certaines fonctionnalités sont désactivées afin de protéger les organisations.

Fonctionnalités pour les entreprises

- **Accès aux services Apple.** Les employés peuvent utiliser les services Apple, notamment iCloud et la collaboration dans iWork et Notes. L'utilisation des e-mails est désactivée, tandis que FaceTime et iMessage sont uniquement disponibles lorsque l'identifiant Apple géré est l'unique identifiant Apple associé à l'appareil.
- **Recherche de comptes utilisateur.** Donnez aux employés la possibilité de rechercher les coordonnées d'autres utilisateurs dans leur organisation Apple Business Manager, pour collaborer plus facilement au sein de plusieurs apps.
- **Création de compte simplifiée.** Avec Apple Business Manager, les comptes des employés sont automatiquement créés lors de leur première connexion à un appareil Apple.
- **Authentification fédérée.** Les administrateurs peuvent lier Apple Business Manager à Microsoft Azure Active Directory pour que les employés puissent se connecter automatiquement en utilisant leurs identifiants professionnels existants.
- **Rôles et privilèges.** Les administrateurs peuvent créer et attribuer des rôles et des privilèges aux équipes informatiques pour leur donner différentes fonctions au sein d'Apple Business Manager.
- **Confidentialité et sécurité intégrées.** Les identifiants Apple gérés utilisent les mêmes protections par chiffrement de données que les identifiants Apple classiques. En outre, ils bénéficient d'un blocage empêchant le ciblage de la plateforme publicitaire d'Apple. Les fonctionnalités commerciales et l'accès aux services tels qu'Apple Pay et Wallet sont désactivés. L'app Localiser est aussi désactivée, car les entreprises disposent du mode Perdu via la solution de gestion des appareils mobiles (Mobile Device Management, MDM).

Authentification fédérée

Avec l'authentification fédérée, vous pouvez lier Apple Business Manager à Microsoft Azure Active Directory (Azure AD) et donner aux utilisateurs la possibilité d'utiliser leur nom d'utilisateur et mot de passe existants en tant qu'identifiant Apple géré.

Microsoft Azure AD est le fournisseur d'identités où sont stockés les noms d'utilisateur et mots de passe des comptes que vous souhaitez utiliser avec Apple Business Manager.

Les identifiants Apple gérés intégrés à Microsoft Azure AD étant fédérés avec des identifiants existants, ils respectent les mêmes règles de sécurité de mot de passe.

Les identifiants Apple gérés sont créés automatiquement lorsque les utilisateurs se connectent à leur appareil Apple. Ainsi, les administrateurs informatiques n'ont pas besoin de passer du temps à tout mettre en place à l'avance.

Les employés peuvent utiliser leur identifiant Azure AD pour accéder aux services Apple, notamment iCloud Drive, Notes, Rappels et les fonctionnalités de collaboration.

L'organisation assurant déjà la gestion de l'identité, toutes les règles de mot de passe et de réinitialisation sont également gérées par l'organisation, ou par l'utilisateur, dans Microsoft Azure AD.

Configuration requise pour l'authentification fédérée

- **Microsoft Azure Active Directory.** Si ce service a déjà été mis en œuvre, vous pouvez d'ores et déjà commencer à utiliser l'authentification fédérée.
- **Active Directory déployé sur site.** Vous devez suivre des étapes de configuration supplémentaires pour vous synchroniser avec Azure AD. Microsoft propose de la documentation et un outil de synchronisation que vous trouverez ci-dessous.

Configuration de l'authentification fédérée

1. **Vérifier votre domaine auprès d'Apple**. Connectez-vous à Apple Business Manager en tant qu'Administrateur ou Gestionnaire de personnes et ajoutez le ou les domaines que vous souhaitez fédérer.
2. **Se connecter à Microsoft Azure Active Directory et accorder les autorisations d'accès à Apple Business Manager.** Utilisez un compte d'administrateur général ou d'administrateur d'application pour vous connecter à Azure AD et accorder à Apple Business Manager l'autorisation de lire les profils des utilisateurs.
3. **Vérifier la propriété du domaine avec Microsoft Azure Active Directory.** Une fois le lien de confiance établi, poursuivez le processus pour vérifier la disponibilité du ou des domaines. Allez dans Apple Business Manager, puis connectez-vous à Microsoft Azure AD avec un compte se terminant par le nom de domaine que vous souhaitez fédérer. Cette étape permet de vérifier la configuration du domaine et prouve que vous en êtes le propriétaire.
4. **Identifier les éventuels conflits au sein de votre domaine.** Apple Business Manager effectue ensuite une recherche dans votre ou vos domaines pour y détecter d'éventuels conflits parmi les identifiants Apple existants. Il peut s'agir d'identifiants Apple personnels ou d'identifiants Apple gérés configurés par une autre organisation utilisant le même domaine.
5. **Lancer la résolution des conflits identifiés dans votre domaine**. Si Apple Business Manager détecte des identifiants Apple personnels dans les domaines que vous essayez de fédérer, les utilisateurs concernés recevront une notification et devront modifier les adresses e-mail associées à leur identifiant Apple. Tous les achats et les données resteront associés à l'identifiant Apple personnel de chaque utilisateur.
6. **Effectuer la migration de comptes pré-existants.** Si votre entreprise a déjà créé des identifiants Apple gérés, vous pouvez procéder à leur migration de sorte qu'ils puissent tirer parti de l'authentification fédérée. Pour ce faire, les utilisateurs devront modifier leurs informations de manière à ce qu'elles correspondent au domaine et au nom d'utilisateur fédérés.

Ressources

- Guide de démarrage 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 dans Apple Business Manager
- En savoir plus sur les conflits avec les identifiants Apple existants
- En savoir plus sur l'intégration de domaines AD sur site avec Azure AD

© 2019 Apple Inc. Tous droits réservés. Apple, le logo Apple, Apple Music, Apple Pay, FaceTime, iPad, iTunes, iTunes U, iWork et Safari sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays. App Store, iCloud et iCloud Drive sont des marques de service d'Apple Inc., déposées aux États-Unis et dans d'autres pays. Les autres noms de produits et de sociétés mentionnés dans ce document appartiennent à leurs propriétaires respectifs.