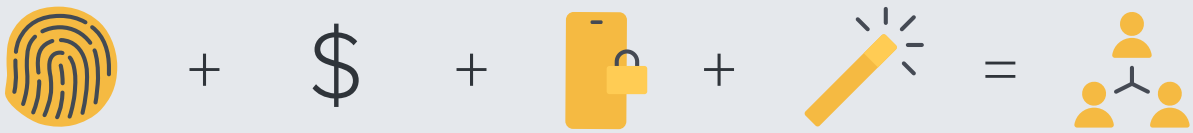
jamf

Jamf Mobile BYOD : **confidentialité** et **expérience utilisateur**

Encouragez l'adoption du BYOD mobile en équilibrant sécurité informatique et respect de la vie privée et de l'expérience utilisateur.

En s'affirmant comme les champions inégalés de la productivité personnelle, l'iPhone et l'iPad ont permis l'avènement d'une génération de professionnels modernes, mobiles et toujours connectés. Et cela représente un défi de taille pour la gestion informatique.

Les éléments clé du succès des solutions BYOD mobiles



Sécuriser les données de l'organisation

Réduire les coûts et la complexité des programmes

Garantir la confidentialité des utilisateurs

Offrir une expérience utilisateur familière

Augmenter l'adoption par les utilisateurs

Les appareils mobiles sont partout, et la plupart des employés apportent leur appareil personnel au travail. Mais les tentatives faites ces dernières années pour exploiter leur potentiel n'ont pas toujours été couronnées de succès. De nombreuses solutions BYOD (utilisation des appareils personnels en entreprise), excellentes dans leur conception, restent imparfaites dans leur mise en œuvre. Les employés fournissent le matériel, les organisations fournissent l'accès, mais cette pratique a deux écueils opposés : l'excès de gestion ou le manque de service aux utilisatuers.

En effet, le contrôle exercé par un cadre complet de gestion des appareils mobiles peut s'avérer trop invasif : le service informatique voit toutes les applications présentes sur l'appareil, qu'elles soient professionnelles ou personnelles. Il a également la capacité de verrouiller, déverrouiller ou effacer l'ensemble de l'appareil. Les propriétaires d'appareils mobiles n'aiment pas renoncer au contrôle de leur appareil, et encore moins que leur vie privée soit exposée – même si ce n'est qu'une impression.

Il existe une autre méthode de gestion des appareils mobiles BYOD : la gestion des applications mobiles (MAM). Elle permet à l'informatique d'appliquer des règles d'entreprise à des applications spécifiques fournies sur l'appareil. Cette technique sécurise uniquement les applications, et non la partie de l'appareil utilisée pour le travail. La MAM ne permet pas aux administrateurs de fournir des services d'entreprise, comme la configuration du Wi-Fi et de l'e-mail, ou l'installation automatique d'applications – pas même celles achetées en volume. Cet approche nécessite donc davantage d'interaction de la part des utilisateurs finaux. En l'absence de règles d'entreprise de base, ces employés se sentent mal servis et l'informatique craint les vulnérabilités de sécurité.

En réalité, pour être couronné de succès, un programme BYOD doit avoir une technologie utilisable, sécuriser les données et protéger la vie privée. **Cet article explique comment les solutions BYOD de Jamf et Apple atteignent cet équilibre délicat.**

Confidentialité avant tout

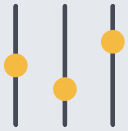
Nos appareils personnels contiennent les données les plus confidentielles : correspondance personnelle, photos, contacts, documents. Même le choix des apps installées sur l'appareil peut révéler des informations très privées sur nos passe-temps, nos habitudes et notre mode de vie. Tout le monde a peur de « Big Brother ». En inscrivant leur appareil personnel dans un système de gestion des appareils mobiles (MDM) contrôlé par le groupe informatique de leur organisation, la plupart des employés craignent de donner accès à ces informations. Et on comprend qu'ils soient réticents.

Ces réticences sont d'ailleurs une raison fréquente de l'échec des programmes BYOD. C'est un sujet crucial, et les utilisateurs sont de plus en plus sensibles à toute compromission de la confidentialité au nom du contrôle informatique.

La sécurité, une priorité pour l'informatique

Pour le responsable informatique, l'idée que des appareils mobiles personnels puissent accéder librement aux ressources internes, sans connaître leur configuration ni leurs réglages de sécurité, est un véritable cauchemar. **Les appareils mobiles sont couramment la cible d'attaques par logiciels malveillants ou par phishing**. Ils représentent un vecteur potentiel d'intrusion lorsqu'ils sont connectés au réseau d'une organisation.

Sans aucune visibilité ni aucun contrôle des données d'entreprise sur ces terminaux, il est impossible de mettre en œuvre une sécurité informatique efficace. C'est cet impératif de sécurité qui incite les organisations à utiliser la MDM pour leur programme BYOD. Elles doivent donc demander à leurs employés d'enrôler leur appareil personnel avant de leur donner accès au réseau interne, à la messagerie, aux calendriers, au VPN et autres outils.



Les administrateurs informatique peuvent :

- Mettre en place des contrôles pour prévenir les pertes de données
- Proposer un catalogue d'applications Self-Service géré par l'utilisateur
- Appliquer les configurations de l'entreprise – Wi-Fi, VPN, VPN et codes d'accès
- Installer et supprimer les apps et livres de l'entreprise et les données associées
- Collecter des informations de sécurité à partir du compte professionnel
- Ajouter/supprimer des restrictions pour protéger les données de l'entreprise

Les administrateurs informatiques ne peuvent pas :

- Effacer les données personnelles – photos, courrier personnel, contacts, etc.
- Supprimer des apps personnelles
- Consulter des données privées (ce qui inclut le nom des apps personnelles)
- Limiter l'utilisation de l'appareil ou l'installation d'apps personnelles
- Suivre la localisation de l'appareil
- Supprimer ce qui a été installé par l'utilisateur
- Recueillir les informations de l'utilisateur à partir de l'appareil

Trouver le juste équilibre

Les préoccupations des employés sont aussi valables que celles de l'informatique. Les premiers ne veulent avoir qu'un seul appareil, mais sans donner ni accès ni contrôle sur leurs données privées. L'informatique veut réduire les coûts des appareils et améliorer l'expérience des employés, mais doit assurer les bases de sécurité de l'organisation. Dans de nombreuses entreprises, ces tiraillements ont signé l'échec du programme BYOD.

Pourtant, on peut répondre à ces deux préoccupations en repensant le rôle de la MDM dans le cadre du BYOD. Plutôt qu'une approche générique, les administrateurs peuvent choisir un outil conçu pour le BYOD. Cette solution protègera la vie privée des employés tout en fournissant des contrôles de sécurité solides pour répondre aux besoins des équipes de sécurité de l'information.

Le BYOD pour les équipes d'aujourd'hui

Les entreprises les plus en pointe choisissent un ensemble de fonctionnalités spécialement conçues pour le BYOD. L'objectif : répondre aux besoins des deux parties, sans complexités inutiles ni coûts supplémentaires. Il est important que l'informatique et l'utilisateur final comprennent bien les avantages d'un programme BYOD conçu pour eux. Assurer la réussite du programme exige également de communiquer les avantages d'un programme BYOD et de faire preuve de transparence auprès des employés : on apaisera ainsi toute tension liée à l'utilisation d'un appareil personnel au travail. Voici quelques avantages clés d'un programme BYOD bien pensé, pour l'entreprise comme pour ses employés.

Tout le monde doit y gagner

Avantages pour les employés

L'expérience native d'Apple pour les usages personnels comme professionnels, dans un seul appareil :

- Transparence des capacités de gestion informatique des appareils personnels avant l'enrôlement, pour garantir la protection des données personnelles de l'utilisateur.
- Accès sécurisé aux ressources d'entreprise – e-mails, calendriers, Wi-Fi et apps – pour favoriser la productivité.

Avantages pour l'organisation

Un équilibre entre sécurité et respect de la vie privée, dans un seul appareil :

- Sécurisation de l'appareil et de l'accès aux données et ressources de l'entreprise, pour préserver les employés et leur productivité
- Contrôle des coûts grâce à la baisse des acquisitions d'appareils

Comment Apple et Jamf garantissent la confidentialité des utilisateurs

Comme le souligne cet article, l'objectif est de trouver un juste milieu pour les appareils personnels. Sans tomber dans un excès de gestion, l'informatique doit avoir les moyens de bien servir ses utilisateurs et son organisation, en offrant un accès facile et sécurisé aux logiciels et aux apps utiles. C'est dans cette optique que Jamf prolonge les capacités et les atouts d'Apple pour optimiser les programmes BYOD.

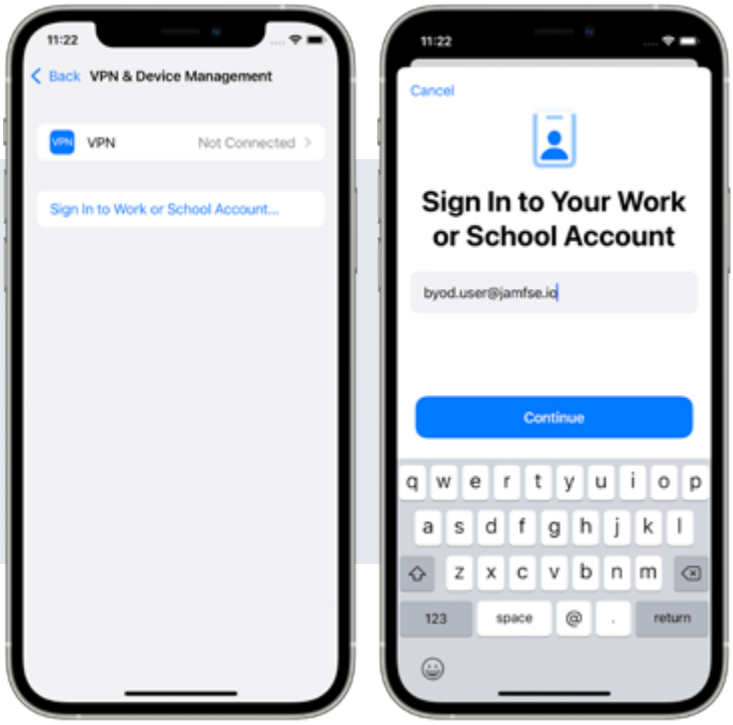
L'**inscription des utilisateurs basée sur le compte** d'Apple met l'accent sur la sécurité et la confidentialité. Cette méthode BYOD, axée sur les appareils iOS et iPadOS, rationalise le processus d'inscription des utilisateurs pour leur donner un accès entreprise, tout en préservant le caractère confidentiel de leur appareil personnel. Grâce à ce nouveau workflow, les entreprises peuvent enrôler les appareils mobiles de leurs employés exploitant iOS ou iPadOS 15 et plus avec Jamf Pro (à partir de la version 10.33). Jamf Pro utilise les workflows d'**inscription utilisateur** natifs d'Apple pour configurer un compte professionnel et un compte personnel distincts, et ainsi protéger la vie privée des employés. Il existe deux méthodes d'inscription : l'inscription de l'utilisateur basée sur le compte et l'inscription basée sur le profil. Jamf préfère l'inscription basée sur le compte : l'employé s'inscrit lui-même à l'aide de l'application Réglages.

L'inscription de l'utilisateur sépare les données personnelles des données institutionnelles en leur associant deux identifiants différents : un Apple ID personnel pour les premières, et un Apple ID géré pour les secondes. Jamf Pro a adopté la fonction de découverte des services d'Apple : elle permet d'exploiter différentes configurations qui associent la gestion à l'employé et son usage professionnel de l'appareil plutôt qu'à l'appareil proprement dit. L'employé accède ainsi à ses données d'entreprise de manière sécurisée, sans que l'informatique n'ait à toucher l'appareil ni à lui envoyer un lien d'inscription, ce qui réduit les risques d'attaques de phishing. L'employé bénéficie même du Jamf Self Service pour installer des applications d'entreprise. Cette expérience d'inscription a l'avantage d'inspirer confiance à l'employé. Elle se rapproche également du déploiement zero-touch pour les administrateurs, en assurant un accès sécurisé aux ressources de l'organisation.

Comment se passe l'inscription de l'employé ?

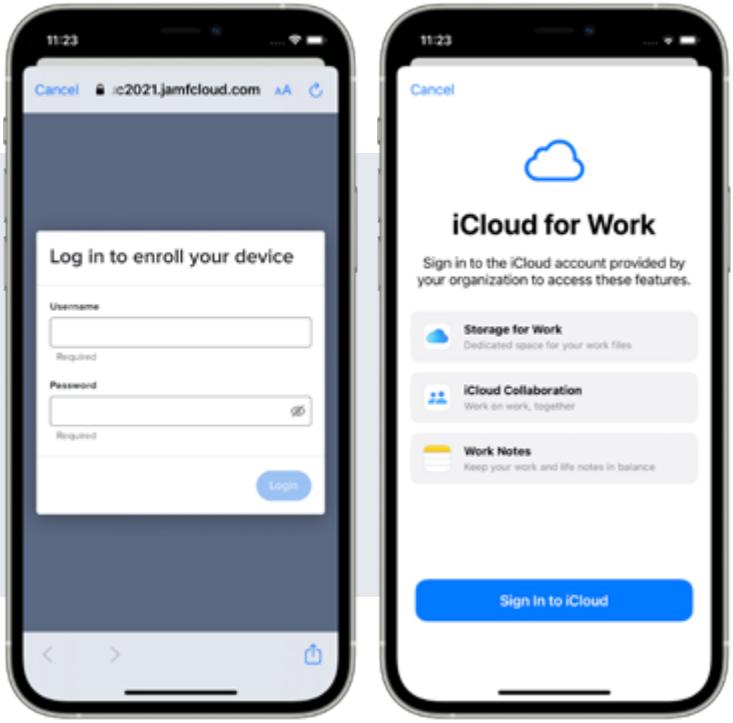
1

L'utilisateur s'authentifie sur l'appareil à l'aide d'un identifiant Apple géré en accédant à Réglages > Général > VPN et gestion des appareils, puis se connecte à son compte professionnel ou scolaire avec son identifiant Apple géré. Après avoir saisi l'Apple ID géré, i l appuie sur Continuer.



2

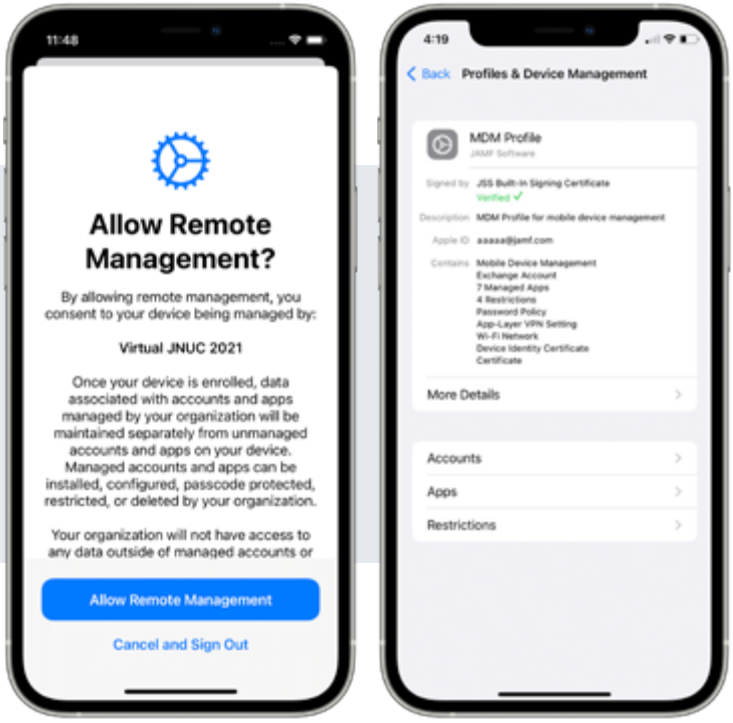
Le portail d'enrôlement s'affiche et invite l'utilisateur à saisir son compte utilisateur Jamf Pro ou ses identifiants d'annuaire (LDAP ou Azure AD, par exemple). Il appuie ensuite sur Connexion. L'utilisateur se connecte alors à iCloud avec l'adresse e-mail de son identifiant Apple géré et son mot de passe lorsqu'il y est invité.



3

Il est ensuite invité à autoriser la gestion à distance et le téléchargement du profil MDM sur l'appareil.

Et c'est tout ! C'est une expérience simple pour l'utilisateur final, mais elle assure à l'organisation une sécurité de niveau entreprise.



Solutions d'accès et de sécurité pour le BYOD

Jamf Connect et Jamf Protect offrent des solutions supplémentaires de gestion et de sécurité.

Avec l'accès réseau zero-trust (ZTNA) fourni par Jamf Connect, seuls les utilisateurs de confiance munis d'appareils approuvés et sûrs sont autorisés à accéder aux applications et aux données professionnelles. Jamf Protect renforce le cadre de sécurité déjà solide d'Apple pour protéger les données de l'entreprise.

Pour mettre en œuvre Jamf Connect et Jamf Protect, les administrateurs déploient Jamf Trust sur les appareils des employés. C'est cette application unique qui délivre les fonctionnalités d'accès et de sécurité de Jamf Connect et Jamf Protect sur les appareils mobiles. Jamf Trust ne fonctionne que sur le compte professionnel de l'appareil, préservant ainsi la confidentialité du compte personnel.

Conclusion

Un programme BYOD réussi est un avantage pour les employés comme pour les administrateurs informatiques. Avec la bonne solution, l'informatique peut se consacrer aux besoins critiques de l'entreprise sans subir les frictions de la technologie ou des utilisateurs. Les utilisateurs bénéficient d'une expérience confortable et familière sur leur appareil personnel, sans ressentir l'intrusion de l'informatique.

Découvrez-en plus sur l'**enrôlement des utilisateurs BYOD** et voyez comment Jamf avec Apple peut donner vie à vos plans BYOD en **demandant une version d'essai.**