



# Connexion unique

Approvisionnez, personnalisez et réinitialisez les appareils partagés.

**Les organisations ont de plus en plus besoin d'appareils mobiles polyvalents, équipés d'applications clés permettant à leurs différents utilisateurs d'effectuer des tâches spécifiques. Mais mettre en place une telle approche peut être complexe pour les utilisateurs finaux, l'informatique et les opérations.**

Imaginez qu'un vendeur soit déconnecté de force d'un appareil alors qu'il sert un client. Il doit se reconnecter, retrouver l'application et reprendre la transaction – autant d'épreuves pour la patience de l'employé et du client.

Pour optimiser leur productivité, les entreprises ont besoin d'un processus de transfert simple, pour approvisionner et réapprovisionner les appareils à distance, en toute sécurité et sans intervention de l'informatique.

## Les environnements d'appareils partagés ont des besoins spécifiques :

- Identité utilisateur et approvisionnement basé sur le rôle
- Workflows plus efficaces
- Élimination de l'étape de connexion avec mot de passe
- Temps d'arrêt minimal
- Simplification de l'expérience de l'employé et du client
- Utilisation optimale de l'appareil
- Suivi de l'inventaire à des fins de gestion
- Personnalisation des appareils partagés

En répondant à ces exigences, vous allégez la charge du service informatique et vous instaurez une cohérence à l'échelle des appareils et des applications. Vous évitez également aux utilisateurs d'attendre les personnalisations dont ils ont besoin. Ils approvisionnent et personnalisent leurs expériences comme ils le souhaitent, sans délai.



# La connexion unique, un workflow optimisé par Jamf Setup et Jamf Reset, permet d'offrir davantage d'autonomie aux utilisateurs d'appareils iOS et iPadOS partagés.

## Simplifier le workflow de l'utilisateur final

L'authentification réseau basée sur l'identité cloud permet à la fois l'approvisionnement basé sur le rôle et le contrôle d'accès. Le personnel accède automatiquement à un appareil mobile qui possède tous les paramètres requis dès la connexion.

## Renforcer la sécurité et la gestion

Grâce à la visibilité sur l'affectation des appareils et des utilisateurs, le service informatique a facilement accès à des rapports. Nous avons également amélioré l'activation et l'effacement des codes d'accès à chaque service.

## Authentification unique (SSO) multi-applications

Jamf Setup et Jamf Reset s'appuient sur le cadre SSO d'entreprise d'Apple. Plus précisément, ces applications utilisent l'implémentation par Apple d'un plug-in Microsoft SSO pour prendre en charge l'authentification unique multi-applications.

## Simplifier les transferts d'appareils

Au moment de la déconnexion, Jamf Reset efface les identifiants et le rôle sélectionné sans procéder à un effacement complet de l'appareil.

Voici comment cela fonctionne :

1.

Une connexion ponctuelle dans Jamf Setup permet d'approvisionner, d'attribuer et de sécuriser un appareil iOS, sur la base de l'identité et du rôle d'un utilisateur dans Azure Active Directory.

2.

La connexion est automatique : les utilisateurs n'ont pas besoin de saisir un identifiant ou un mot de passe. Un écran d'accueil personnalisé, avec un fond d'écran aux couleurs de l'organisation, informe les utilisateurs de l'état de l'appareil.

3.

Pendant la pause ou en fin de service, les utilisateurs se déconnectent très simplement de l'application Jamf Reset. Leurs traces et leurs applications sont supprimées de l'appareil.

*Ces technologies sont actuellement en version anticipée : veuillez à soupeser les éventuels problèmes de prise en charge et autres risques avant de les utiliser. Les technologies Microsoft en accès anticipé sont soumises aux conditions générales de Microsoft et ne doivent pas être utilisées dans un environnement de production.*



www.jamf.com/fr

© 2002–2023 Jamf, LLC. Tous droits réservés.

Pour en savoir plus sur la connexion unique, rendez-vous sur [jamf.com](https://www.jamf.com)

Contactez votre représentant Jamf ou votre revendeur préféré