



LIVRE BLANC

Microsoft Enterprise Compliance : comment assurer la conformité de son parc Apple



La mise en conformité des appareils iOS étend le partenariat entre Jamf et Microsoft pour prendre en charge l'ensemble de la flotte Apple en entreprise.

Le travail, l'apprentissage et les soins à distance ont rendu la sécurité des appareils mobiles plus importante que jamais. Que votre organisation prodigue des soins aux patients proches ou qu'elle soutienne son personnel dans le monde entier, les appareils iOS et iPadOS jouent souvent un rôle clé dans votre stratégie pour accroître la productivité. L'entreprise ne fonctionnant plus exclusivement sous Windows et les employés ayant de plus en plus souvent le choix de leurs appareils, il est temps de faire passer vos workflows de sécurité Apple au même niveau que ceux des autres environnements.

La mise en conformité des appareils iOS et iPadOS (communément appelée Mise en conformité des appareils iOS) est une extension importante du partenariat de Jamf avec Microsoft.

En savoir plus :

Cette intégration Microsoft fait suite à l'accès conditionnel sans proxy pour Mac rendu possible par Jamf et Microsoft Enterprise Mobility + Security.

[Tous les détails des workflows Mac de Microsoft et Jamf](#)

Jamf et Microsoft : un partenariat en pleine évolution

2017

Jamf et Microsoft ont annoncé un partenariat unique en son genre pour introduire l'accès conditionnel sur Mac.

Le partenariat conclu entre Jamf et Microsoft Enterprise Mobility + Security (EMS) a donné naissance à une solution automatisée de gestion de la conformité pour les appareils Mac qui accèdent aux applications configurées avec l'authentification Azure AD. Cette collaboration s'appuie sur l'accès conditionnel pour garantir que seuls les utilisateurs de confiance puissent accéder aux données de l'entreprise.

2018

Jamf a étendu son intégration pour faciliter la connexion des utilisateurs finaux.

L'intégration des technologies Jamf et Microsoft permet aux utilisateurs finaux de se connecter plus facilement. Avec Jamf Pro, Jamf Connect et Microsoft Enterprise Mobility + Security (EMS), les utilisateurs peuvent se connecter à un nouveau Mac avec des identifiants Microsoft Azure Active Directory. Il n'est donc plus nécessaire de créer et de gérer un nom d'utilisateur et un mot de passe locaux sur le Mac de l'utilisateur final.

2020

Jamf a poursuivi l'extension de son partenariat avec Microsoft en proposant le premier accès conditionnel pour les appareils mobiles Apple.

Les entreprises peuvent déjà tirer parti de l'accès conditionnel sur les appareils macOS, en partageant les données d'inventaire de Jamf avec Microsoft Endpoint Manager. La collaboration étendue entre Jamf et Microsoft permet de prendre également en charge iOS. Les équipes informatiques peuvent désormais empêcher un utilisateur autorisé d'utiliser tout appareil macOS ou iOS non conforme aux règles de sécurité. Elles peuvent aussi utiliser Jamf Self Service pour appliquer des mesures correctives, et ainsi sécuriser et prendre en charge l'ensemble de leur parc d'appareils Apple.

À qui s'adresse la conformité des appareils iOS ?

La mise en conformité des appareils iOS est utile à tous. Les entreprises dotées d'environnements hybrides, celles qui ont des responsables différents pour l'équipe informatique et l'équipe de sécurité de l'information, et celles possédant des appareils Apple et Microsoft bénéficient de la conformité des appareils iOS.

Les entreprises bénéficient déjà de l'accès conditionnel sur macOS, en partageant les données d'inventaire Jamf avec Microsoft Endpoint Manager. Désormais, les équipes informatiques peuvent empêcher un utilisateur autorisé d'utiliser tout appareil iOS non conforme aux règles de sécurité de leur organisation et tirer parti du Jamf Self Service pour appliquer des mesures correctives.



Fonctionnement

Définir des critères de conformité :

Grâce à la mise en conformité des appareils iOS, les administrateurs peuvent établir des critères de conformité pour garantir que les appareils iOS répondent aux normes de sécurité avant d'accéder aux ressources de l'organisation.

Passer en revue les critères de conformité :

En s'appuyant sur des groupes intelligents brevetés pour passer en revue les critères de conformité, Jamf Pro vérifie la conformité des appareils et envoie ensuite un statut « conforme/non conforme » à Microsoft Azure AD.

Établir un rapport de conformité :

Les informations sur l'appareil recueillies par Jamf sont ensuite envoyées à Azure AD. Comme Azure AD conserve les informations transmises par Jamf Pro dans le dossier de l'appareil et vérifie son statut à chaque connexion avant d'accorder l'accès aux ressources de l'entreprise (OneDrive, Outlook, etc.), les actifs, les données et les ressources de l'entreprise sont mieux protégés et plus sécurisés.

Appliquer des mesures correctives :

Si un appareil est marqué « non conforme », l'accès est refusé et des mesures correctives doivent être appliquées pour que l'utilisateur final puisse continuer. L'utilisateur est dirigé vers le Jamf Self Service afin d'entamer le processus de remédiation pour remettre l'appareil en conformité.

Ce dont vous avez besoin pour commencer

- Jamf Pro intégré à Microsoft Endpoint Manager
- Un groupe intelligent qui contient les appareils dont vous voulez contrôler la conformité
- Un compte utilisateur Jamf Pro avec des droits d'accès conditionnel
- Une règle d'accès conditionnel exigeant que les appareils soient marqués comme conformes afin d'accéder aux ressources de votre organisation
- Microsoft Enterprise Mobility + Security (en particulier Microsoft AAD Premium et Microsoft Intune)



Afin que la conformité des appareils puisse être contrôlée, ceux-ci doivent être munis de :

- iOS 11 ou version ultérieure, ou iPadOS 13 ou version ultérieure avec Safari défini comme navigateur par défaut
- L'application Microsoft Authenticator (disponible dans l'App Store)
- Jamf Self Service pour iOS 10.10.3 ou version ultérieure

À vos marques, prêts, en conformité

Les organisations du monde entier constatent la nécessité d'une conformité Zero-Trust des appareils. Et cette expérience utilisateur étant la seule que connaît les employés à distance, on ne saurait trop insister sur l'importance de la conformité et de la sécurité.

La mise en conformité des appareils iOS avec Apple et Microsoft (les solutions de référence dans le monde de l'entreprise) vous permet de sécuriser et de gérer vos appareils iOS, de garantir leur conformité et de prendre en charge votre flotte Apple.

Commencez dès aujourd'hui

Pour les clients actuels utilisant Jamf Cloud, cette nouvelle intégration apparaîtra dans Jamf Pro en tant que Conformité de l'appareil iOS sous le menu Gestion globale. Pour plus d'informations et d'aide sur cette nouvelle fonctionnalité, veuillez consulter notre [guide technique](#).

Si vous n'avez pas encore rejoint Jamf, demandez une version d'essai gratuite ou contactez votre revendeur Apple pour commencer.

[Demandez une version d'essai](#)

