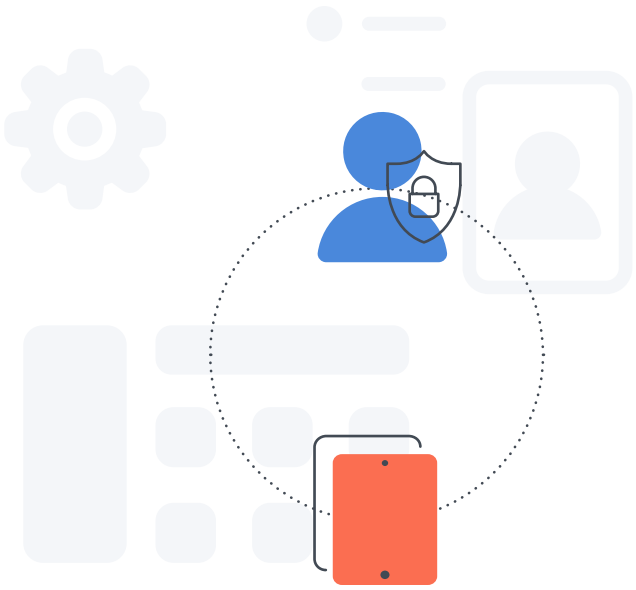
Parvenir à la conformité Microsoft Enterprise

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

Aujourd'hui, les utilisateurs travaillent, apprennent et soignent à distance : la sécurité des appareils mobiles est donc un enjeu majeur. Pour prodiguer des soins à des patients au bout du couloir ou pour soutenir des équipes réparties dans le monde entier, les appareils i sont essentiels à votre stratégie de productivité. Windows n'a plus l'exclusivité dans les environnements d'entreprise et les employés ont de plus en plus souvent le choix de leurs appareils. Pour toutes ces raisons, il est temps de mettre vos workflows de sécurité Apple au même niveau que ceux des autres environnements.
La conformité des appareils iOS et iPadOS (communément appelée conformité des appareils iOS), comme celle des appareils macOS, est un aspect essentiel du partenariat entre Jamf et Microsoft.



En savoir plus

Cette intégration Microsoft fait suite à la prise en charge de l'accès conditionnel sans proxy pour Mac, rendue possible par Jamf et Microsoft Enterprise Mobility + Security.

Tous les détails des workflows Mac de Microsoft et Jamf

Le partenariat dynamique entre Jamf et Microsoft

2017

Jamf et Microsoft annoncent un partenariat unique pour introduire l'accès conditionnel pour les Mac. Partenariat entre Jamf et Microsoft Enterprise Mobility + Security (EMS), qui fournit une solution de gestion automatisée de la conformité pour les appareils Mac accédant aux applications configurées avec l'authentification Entra ID. Cette collaboration s'appuie sur l'accès conditionnel pour garantir que seuls les utilisateurs de confiance peuvent accéder aux données de l'entreprise.

2018

Jamf étend son intégration pour permettre aux utilisateurs finaux de se connecter plus facilement. 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 Entra ID. Il n'est donc plus nécessaire de créer et de gérer un nom d'utilisateur local et un mot de passe sur le Mac de l'utilisateur final.

2020

Jamf poursuit l'extension de son partenariat avec Microsoft en proposant le premier accès conditionnel pour les appareils mobiles Apple. Les entreprises bénéficient déjà de l'accès conditionnel sur les appareils macOS, et partagent les données d'inventaire de Jamf avec Microsoft Endpoint Manager. L'approfondissement de la collaboration entre Jamf et Microsoft étend la prise en charge à iOS. Les équipes informatiques peuvent désormais empêcher un utilisateur autorisé d'utiliser un appareil macOS ou iOS non conforme aux règles de sécurité. Jamf Self Service facilite la correction des problèmes de conformité et leur permet de sécuriser et gérer l'ensemble du parc Apple.

2021

L'intégration de Microsoft Sentinel et de Jamf Protect marque une nouvelle étape clé pour le partenariat de sécurité. Les informations sur les menaces spécifiques à Apple sont directement envoyées à l'outil SIEM de l'équipe informatique et de sécurité dans un environnement Microsoft.

2023

Jamf devient membre de la Microsoft Intelligent Security Association (MISA), un écosystème d'éditeurs de logiciels indépendants et de fournisseurs de services de sécurité gérés dont les solutions s'intègrent à Microsoft Security pour protéger leurs clients contre les menaces de cybersécurité. Partageant la même vision de la sécurité Apple, Jamf a été invité à faire partie de la MISA pour la qualité de ses intégrations. Nos produits permettent une gestion efficace des appareils, sécurisent l'accès aux ressources de l'entreprise et protègent les terminaux Apple au travail.

Qui a besoin de la conformité des appareils iOS

La conformité des appareils iOS est utile à tous. La conformité des appareils iOS est intéressante pour les entreprises qui exploitent des environnements hybrides, celles dont les services informatique et de sécurité sont séparés, et celles qui utilisent à la fois des appareils Apple et Microsoft.
Les entreprises bénéficient déjà de l'accès conditionnel sur les appareils macOS, et partagent les données d'inventaire de Jamf avec Microsoft Intune. Les équipes informatiques peuvent désormais empêcher un utilisateur autorisé d'utiliser un appareil iOS non conforme aux règles de sécurité de leur organisation, et corriger les problèmes avec Jamf Self Service.

Le principe :

Définissez des critères de conformité :
Avec la conformité des appareils, les administrateurs informatiques tels que vous peuvent désormais définir des critères de conformité pour garantir que les appareils iOS et macOS répondent aux normes de sécurité avant d'accéder aux ressources de l'organisation.

Appliquez les critères de conformité :
En s'appuyant sur des groupes intelligents brevetés pour appliquer sélectivement les critères, Jamf Pro vérifie la conformité des appareils et envoie ensuite un statut « conforme/non conforme » à Microsoft Entra AD.

Produisez des rapports de conformité :
Les informations sur l'appareil recueillies par Jamf sont ensuite envoyées à Entra ID. Comme Entra ID 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.

Corrigez :
Si un appareil est « non conforme », l'accès est refusé et des corrections doivent être appliquées pour que l'utilisateur final soit autorisé à continuer. Il est donc redirigé vers Jamf Self Service pour lancer le processus de correction et remettre l'appareil en conformité.

Que faut-il pour commencer

- Jamf Pro intégré à Microsoft Intune
- Un groupe intelligent qui contient les appareils dont vous voulez contrôler la conformité
- Un compte utilisateur Jamf Pro avec des privilèges d'accès conditionnel
- Une règle d'accès conditionnel qui exige que les appareils aient le statut « conforme » pour accéder aux ressources de votre organisation
- Microsoft Enterprise Mobility + Security (en particulier Microsoft AAD Premium et Microsoft Intune)

Pour superviser la conformité des appareils, ceux-ci doivent être équipés de :

- Jamf Pro 10.29.0 ou une version ultérieure hébergée dans Jamf Cloud
- Un compte d'utilisateur Jamf Pro avec des privilèges de conformité des appareils.
- iOS 11 ou version ultérieure, iPadOS 13 ou version ultérieure ou macOS 10.11 ou version ultérieure.
- L'application Microsoft Authenticator (disponible dans l'App Store) pour iOS et iPadOS.
- Jamf Self Service pour iOS 10.10.3 ou version ultérieure
- Dernière version de l'application Microsoft Intune Company Portal pour macOS

À vos marques, prêts, en conformité

Les organisations du monde entier voient la conformité zéro-trust des appareils comme une nécessité, et la généralisation du télétravail a encore accentué l'importance de la conformité et de la sécurité.

La conformité des appareils iOS avec Apple et Microsoft – les deux standards en entreprise – vous permet de sécuriser et de gérer vos appareils iOS pour garantir leur conformité et protéger votre flotte Apple.

Lancez-vous !

Pour les clients qui utilisent déjà Jamf Cloud, cette nouvelle intégration apparaîtra dans Jamf Pro sous l'intitulé 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 distributeur Apple pour commencer.

Demander une version d'essai