Microsoft Intune et macOS : Platform SSO, Conformité et Accès conditionnel

Référence Agnosys	SS/IPCA
Durée	2 jours
Certification	Non
Support de cours	En français

Description

Cette formation explore le déploiement de Platform SSO, de la conformité et de l'accès conditionnel sur macOS via Microsoft Intune. Elle détaille la mise en œuvre des méthodes d'authentification Mot de passe et Enclave sécurisée, cette dernière étant également abordée dans le cadre d'un parcours Passwordless initié par un Pass d'accès temporaire (TAP). Ces trois scénarios font l'objet d'une démonstration de leur implémentation dans le cadre du Simplified Setup for Platform SSO, qui permet de réaliser la jonction Entra ID directement depuis l'assistant de configuration initiale, avant même la création du compte utilisateur local. L'ensemble se conclut par la configuration de stratégies de conformité rigoureuses et l'application de l'accès conditionnel afin d'interdire l'accès aux ressources critiques par des Mac non conformes.

Objectifs

• Comprendre comment la technologie Platform SSO renforce la sécurité des accès en combinant une expérience utilisateur fluidifiée et une authentification forte
• Maîtriser la mise en œuvre de Platform SSO, en distinguant les méthodes d'authentification Mot de passe et Enclave sécurisée
• Acquérir les bases du Passwordless en utilisant des Pass d'accès temporaire (TAP) et des clés d'accès (Passkeys) pour s'affranchir de l'usage des mots de passe
• Implémenter Simplified Setup for Platform SSO afin de réaliser la jonction Entra ID depuis l'assistant de configuration initiale dans le contexte de l'inscription automatisée des appareils
• Savoir définir des règles de conformité strictes pour évaluer l'intégrité et le niveau de sécurité du Mac
• Mettre en œuvre l'accès conditionnel pour garantir que seul un appareil conforme puisse accéder aux ressources critiques

Qui peut s’inscrire ?

Cette formation s'adresse aux administrateurs système dans les organisations de toutes tailles (entreprise et éducation) disposant déjà de Microsoft Intune et souhaitant implémenter la technologie Platform SSO ainsi que des stratégies de conformité et d'accès conditionnel.

Pré-requis

Pour suivre cette formation, vous devez :
- avoir suivi la formation "Administrer les Mac et les appareils iOS avec Microsoft Intune" (Réf. SS/MSIT)
- ou bien déployer et gérer des Mac au quotidien dans des environnements Microsoft intégrant Microsoft Entra et Microsoft Intune.

Nous insistons sur le fait que cette formation intensive est spécifiquement centrée sur l'implémentation de la technologie Platform SSO avec les méthodes d'authentification Mot de passe et Enclave sécurisée, et sur la mise en œuvre des stratégies de conformité et d'accès conditionnel.

Elle vise à compléter les compétences acquises suite au suivi de la formation "Administrer les Mac et les appareils iOS avec Microsoft Intune" (Réf. SS/MSIT), ou à une expérience d'administration des Mac avec Microsoft Intune.

Participants et matériels sous la responsabilité d'Agnosys

Cette formation est limitée à six participants maximum.

La classe sera équipée d'un accès aux centres d'administration Microsoft Entra et Microsoft Intune, ainsi que des Mac et des appareils iOS nécessaires pour les démonstrations réalisées par le formateur.

Les participants disposeront des droits d’administrateur sur Microsoft Entra et Microsoft Intune pour réaliser des travaux pratiques et apprendre à utiliser ces services sans risquer d’impacter un environnement de production.

Matériels sous la responsabilité exclusive des participants

Chacun des participants devra être équipé sous sa responsabilité :
- d'un Mac Apple silicon de test équipé de la version la plus récente disponible du système d’exploitation macOS et d'un capteur Touch ID, sur l'assistant de configuration initiale
- d'un iPhone ou d'un iPad de test équipé de la version la plus récente disponible du système d’exploitation iOS ou iPadOS, sur l'assistant de configuration initiale
- d'un réseau Wi-Fi basique avec authentification WPA/WPA2/WPA3
- d'un compte Apple personnel fonctionnel (authentification à deux facteurs activée).

En raison des contraintes matérielles inhérentes à l'inscription automatisée des appareils, l'implémentation du Simplified Setup for Platform SSO sera abordée sous forme de démonstrations détaillées par le formateur.

Attention — Le Mac et l'iPad seront effacés pendant la formation et ne doivent donc pas contenir de données. Ils ne doivent pas être inscrits dans une solution MDM. Ils peuvent appartenir à un programme de déploiement Apple mais ne doivent pas être associés à un profil d'inscription automatisée des appareils. Le Mac de test ne doit pas être une machine virtuelle (le formateur ne gèrera pas cette spécificité).

Recommandation — Pour fluidifier la réalisation des travaux pratiques, notamment lors des tâches requérant un changement de compte utilisateur, nous recommandons aux participants de suivre la formation depuis un autre ordinateur Mac ou PC ou une tablette, équipé d'une caméra et d'un micro, qui servira uniquement à l'utilisation du logiciel Zoom et à l'affichage des ressources du cours.

Sujets traités

Socle technique

– Présentation des services Entra ID et Microsoft Intune pour la formation
– Device Enrollment et Automated Device Enrollment
– Gestion à distance et certificat Push
– Enclave sécurisée, Face ID, Touch ID
– FileVault

Travaux pratiques :
– Préparation du Mac et de l'appareil iOS de test pour les exercices
– Détails de la configuration initiale du Tenant Microsoft
– Accès aux centres d'administration du Tenant Microsoft
– Vérification du certificat Push dans Intune
– Inscription du Mac en Device Enrollment

Platform SSO avec la méthode d'authentification Mot de passe

– De la jonction traditionnelle avec Active Directory à Platform SSO avec Entra ID
– Fonctionnement, bénéfices et pré-requis de Platform SSO
– Verrouillage du nom du compte local dans l'assistant de configuration initiale
– Application d'une règle de complexité sur les mots de passe des comptes locaux
– Synchronisation des mots de passe du compte local et du compte Entra ID
– Utilisation de la commande app-sso pour vérifier le statut de fonctionnement
– Gestion du changement ou de la réinitialisation d'un mot de passe synchronisé
– Utilisation de la clé de secours FileVault dans le contexte d'une réinitialisation

Travaux pratiques :
– Configuration de l'extension Microsoft Enterprise SSO
– Jonction du Mac avec Entra ID
– Gestion du changement d'un mot de passe synchronisé
– Gestion de la réinitialisation d'un mot de passe synchronisé
– Création de comptes locaux depuis la fenêtre d'ouverture de session
– Création de comptes locaux temporaires depuis la fenêtre d'ouverture de session
– Suppression de la demande de connexion SSO pour le compte administrateur local
– Implémentation de Simplified Setup for Platform SSO dans ce scénario

Platform SSO avec la méthode d'authentification Enclave sécurisée

– Bénéfices de la méthode d'authentification Enclave sécurisée
– Lien entre l'identité Entra ID et la puce de sécurité Apple (Hardware-bound)
– Gestion du changement d'un mot de passe

Travaux pratiques :
– Reconfiguration de l'extension Microsoft Enterprise SSO
– Jonction du Mac avec Entra ID
– Gestion du changement d'un mot de passe de compte local
– Implémentation de Simplified Setup for Platform SSO dans ce scénario

Platform SSO et expérience Passwordless

– Pass d'accès temporaire (TAP) et clé d'accès (Passkey)
– Une expérience utilisateur sans connaissance du mot de passe Entra ID
– Utilisation d'un appareil iOS comme authentificateur physique FIDO2

Travaux pratiques :
– Génération d'un Pass d'accès temporaire (TAP)
– Enregistrement de l'appareil iOS et création d'une clé d'accès (Passkey)
– Inscription d'un Mac en Device Enrollment via l'appareil iOS
– Jonction du Mac avec Entra ID
– Implémentation de Simplified Setup for Platform SSO dans ce scénario

Conformité

– Présentation des stratégies de conformité dans Microsoft Intune
– Évaluation de la posture de sécurité du Mac

Travaux pratiques :
– Stratégie : Protection de l'intégrité du système, version minimale de macOS et FileVault
– Stratégie : Pare-feu et Gatekeeper
– Analyse de la conformité

Accès conditionnel

– Présentation des stratégies d'accès conditionnel dans Microsoft Entra ID
– Le principe du Zero Trust (utilisateur, appareil, application)
– Corrélation entre l'état de conformité et le droit d'accès aux services Microsoft 365
– Communication auprès de l'utilisateur et processus de remédiation

Travaux pratiques :
– Déclaration de la stratégie de verrouillage
– Vérification du fonctionnement de la stratégie avec un Mac conforme et non conforme

AGNOSYS
Conseil - Audit - Formation
Consultants Network
jamf SERVICES Partner
01 64 53 25 25 **www.agnosys.com** **contact@agnosys.fr**