Administrer les Mac et les appareils iOS avec Microsoft Intune

Référence Agnosys	SS/MSIT
Durée	4 jours
Certification	Non
Support de cours	En français

Description

Cette formation vous apportera des bases solides pour administrer des Mac et des appareils iOS avec Microsoft Intune. Vous apprendrez à inscrire les appareils, à les gérer via des profils de configuration et des commandes MDM, à déployer des applications, ainsi qu'à appliquer des stratégies de sécurité basées sur les technologies Apple et Microsoft Defender. Enfin, vous verrez comment optimiser l'expérience utilisateur des services Microsoft 365 grâce à l'authentification unique (SSO).

Objectifs

• Savoir inscrire des Mac, des iPhone et des iPad dans Microsoft Intune
• Savoir déployer des applications de l'App Store et d'autres sources
• Savoir gérer les appareils avec des profils de configuration et des commandes MDM
• Savoir sécuriser les appareils inscrits avec les technologies Apple et Microsoft Defender
• Savoir mettre en œuvre l'authentification unique (SSO)

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 ayant pour objectif d'étendre la flotte gérée aux Mac et aux appareils iOS.

Pré-requis

Pour suivre cette formation, vous devez avoir déjà travaillé avec des environnements Microsoft intégrant Microsoft Entra et Microsoft 365, et idéalement avec Microsoft Intune pour la gestion des appareils autres qu'Apple.

Cela implique, par exemple, de connaître le rôle de ces solutions, de savoir s'authentifier sur leurs centres d'administration (MFA), d'être en mesure de manipuler rapidement leur interface graphique en anglais en suivant des instructions écrites en français, et d'avoir déjà travaillé avec les applications Microsoft Portail d'entreprise, Authenticator, Teams, Outlook et Edge.

Par ailleurs, vous devez disposer des connaissances attendues pour un technicien assurant le support au quotidien des Mac et des appareils iOS équipés de versions de macOS et d'iOS sorties voici moins de trois ans. Pour vous assurer de disposer de ces connaissances, nous vous invitons à consulter les contenus des deux formations suivantes et au besoin, à vous y inscrire :
- Support macOS : les clés d'une assistance aux utilisateurs réussie (SE/SUPMOS)
- Support iOS : prise en main et assistance aux utilisateurs (IPD/SUPIOS).

Nous insistons sur le fait que cette formation intensive est centrée sur l'administration des appareils Apple avec Microsoft Intune et qu'elle n'inclut pas la configuration initiale d'un environnement Microsoft intégrant Microsoft Entra et Microsoft 365, supposé déjà exister dans votre organisation, ni la découverte des systèmes d'exploitation macOS et iOS.

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, Microsoft Intune et Microsoft Defender, 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 Intune pour réaliser des travaux pratiques et apprendre à utiliser la solution 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 de test équipé de la version la plus récente disponible du système d'exploitation macOS, 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).

Les processus d'inscription automatisée des appareils Apple (Automated Device Enrollment) seront traités par le formateur sous la forme de démonstrations.

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

Infrastructure

– Modèle de déploiement moderne
– Composants rendant possible un déploiement moderne
– Présentation de Microsoft Intune
– Présentation du programme de déploiement Apple Business Manager
– Présentation du cadre de gestion des Mac et des appareils iOS
– Flux requis
– Fonctionnement du Push via APNs
– Configuration initiale et renouvellement du certificat Push
– Configuration d'une identité de supervision dans Apple Configurator 2

Travaux pratiques :
– Préparation du Mac et de l'appareil iOS pour les exercices
– Connexion à Microsoft Intune
– Supervision manuelle d’un appareil iOS avec Apple Configurator 2

Inscription des appareils

– Modèle de déploiement One to One (1 appareil, 1 utilisateur régulier)
– Inscription des appareils et inscription automatisée des appareils
– Activation de l'inscription des appareils iOS depuis le portail Web
– Configuration de Microsoft Intune pour l'inscription automatisée des appareils
– Ajout d'un appareil à Apple Business Manager avec Apple Configurator pour iPhone
– Synchronisation des appareils entre Apple Business Manager et Microsoft Intune
– Gestion des profils d'inscription automatisée des appareils
– Inscription d’un Mac et d'un appareil iOS en inscription automatisée des appareils

Travaux pratiques :
– Inscription d’un Mac en inscription des appareils depuis Microsoft Portail d'entreprise
– Inscription d’un appareil iOS en inscription des appareils depuis le portail Web
– Déclaration des appareils inscrits comme appartenant à l'entreprise
– Association des appareils inscrits à des groupes d’appareils dynamiques
– Association des appareils inscrits à des utilisateurs membres de groupes

Distribution d'applications

– Acquisition en masse de licences d’apps
– Sites et jetons par site
– Transfert de licences entre sites
– Délégation
– Moyens de paiement et crédit VPP
– Distribution multinationale
– Configuration de Microsoft Intune pour la distribution gérée

Travaux pratiques :
– Synchronisation des licences entre Apple Business Manager et Microsoft Intune
– Assignation des apps pour un déploiement requis ou à la demande
– Distribution d’une app de l’App Store
– Installation d'applications Line-of-business et PKG
– Installation initiale et mise à jour d'une application DMG
– Configuration des apps iOS déployées (AppConfig)

Gestion des appareils

– Inventaire des appareils
– Bénéfices de la supervision
– Profils de configuration
– Gestion déclarative des appareils (Declarative Device Management)
– Commandes MDM
– Exécution d'un script Shell
– Déclaration d'un attribut personnalisé

Travaux pratiques :
– Distribution d’une configuration Wi-Fi
– Application de restrictions et de réglages
– Distribution de signets dans Microsoft Edge et Google Chrome pour Mac
– Configuration des mises à jour macOS et iOS via la gestion déclarative des appareils

Sécurité et confidentialité

– Puce Apple silicon, Secure Boot
– Sécurité du matériel, du système, des données et des apps
– Verrouillage d’activation
– Règles de mot de passe et de code de verrouillage
– FileVault, SecureToken et Bootstrap Token
– Activation de FileVault depuis l'assistant de configuration initiale
– Firewall applicatif
– Gatekeeper
– Approbation des System Extensions
– Réglages de confidentialité et Privacy Preferences Policy Control (TCC)
– Séparation transparente des données professionnelles et personnelles
– Gestion de l’ouverture des sources gérées dans des destinations non gérées
– Gestion de l’ouverture des sources non gérées dans des destinations gérées
– Domaines gérés
– Mode perdu
– Intégration de Microsoft Intune avec Microsoft Defender

Travaux pratiques :
– Activation de FileVault et du Firewall applicatif
– Configuration de Gatekeeper
– Configuration d’un code de verrouillage
– Configuration de l'enregistrement de l'écran pour Microsoft Teams (TCC)
– Gestion des flux de données (sources gérées vers destinations non gérées)
– Mode perdu et géolocalisation
– Vérification du fonctionnement de Microsoft Defender

Authentification unique (SSO)

– Authentification unique de plateforme (Platform SSO) pour les Mac
– Extension SSO d'application (Single sign-on app extension) pour les appareils iOS
– Création dynamique de comptes locaux depuis des comptes Entra ID
– Ouverture de session avec un compte Entra ID
– Création d'un compte administrateur LAPS avec EasyLAPS
– Gestion du statut administrateur ou standard des comptes existants et nouveaux

Travaux pratiques :
– Implémentation de l'authentification unique de plateforme pour les Mac
– Implémentation de l'extension SSO d'application pour les appareils iOS
– Configuration de Google Chrome pour l'authentification unique de plateforme
– Vérification du fonctionnement des configurations SSO

Réinitialisation locale et à distance

– Méthodes de réinitialisation locale d’un Mac et d’un appareil iOS
– Méthodes de réinitialisation à distance d’un Mac et d’un appareil iOS

Travaux pratiques :
– Réinitialisation à distance d’un appareil iOS
– Réinitialisation locale d’un Mac

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