

Gestion moderne des postes de travail et mobiles avec Microsoft Intune

Programme *(Mis à jour le 25/08/2026)*

Module 1 — Architecture Intune & Entra ID

- Concepts Modern Management
- Architecture Intune : services, rôles, flux, endpoints
- Licences : M365, EMS, Intune Suite
- Entra ID : identités, devices, RBAC, groupes dynamiques
- Modèles d'inscription : BYOD, COPE, Corporate
- Différences Entra Join / Hybrid Join / Workgroup

Travaux pratiques – Module 1

- Création de groupes dynamiques (règles avancées)
- Mise en place d'un rôle RBAC Intune personnalisé
- Analyse d'un device Entra ID (état, compliance, logs)

Module 2 — Enregistrement des appareils

- Méthodes d'enregistrement Windows
- Inscription iOS / iPadOS (ADE, Company Portal)
- Inscription Android Enterprise (Work Profile, Fully Managed)
- Inscription macOS (ADE, Company Portal)
- Gestion des inventaires : hardware, apps, compliance, logs

Travaux pratiques – Module 2

- Enregistrement d'un poste Windows (Entra Join)
- Enregistrement d'un smartphone Android (Work Profile)
- Enregistrement d'un iPhone (Company Portal)
- Vérification de l'inventaire et des attributs de conformité

Module 3 — Windows Autopilot

- Concepts Autopilot
- Profils de déploiement
- Scénarios : User-Driven, Self-Deploying, Pre-Provisioning (WhiteGlove)
- Hybrid Join vs Azure AD Join
- Gestion des devices Autopilot
- Dépannage Autopilot (logs, MDM diagnostics)

Travaux pratiques – Module 3

- Import d'un device Autopilot
- Création d'un profil Autopilot complet
- Déploiement d'un poste en mode User-Driven
- Simulation d'un scénario Pre-Provisioning
- Analyse des logs Autopilot

Module 4 — Configuration & Mises à jour

- Settings Catalog : approche moderne
- Templates : Device Restrictions, Security Baselines
- Scripts PowerShell (Windows)
- Gestion des mises à jour : Windows Update for Business
- Rings

Référence

THIS3693

Durée

5 jours / 35 heures

Prix HT / stagiaire

3250€

Objectifs pédagogiques

Niveau requis

- Connaissances de base de Windows 10/11
- Notions sur Azure AD / Entra ID (identités, groupes, MFA)
- Connaissances générales sur Microsoft 365
- Notions PowerShell recommandées (mais pas obligatoires)
- Avoir déjà administré un parc informatique (AD, GPO, M365, etc.)

Public concerné

- Administrateurs systèmes et réseaux
- Ingénieurs postes de travail / Modern Workplace
- Responsables sécurité / SOC / SecOps
- Chefs de projet IT en charge de la modernisation du poste de travail
- Consultants Microsoft 365 / Intune
- Toute personne impliquée dans la gestion, la sécurisation ou l'automatisation du parc Windows / mobile
- Public intermédiaire ? avancé, déjà exposé à Microsoft 365

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD

Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices

Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'exécution de

- Feature Updates
- Quality Updates
- Gestion des paramètres macOS / iOS / Android

Travaux pratiques – Module 4

- Création d'un profil Settings Catalog (BitLocker, Firewall)
- Déploiement d'un script PowerShell (configuration avancée)
- Mise en place d'un ring WUfB
- Déploiement d'une Feature Update ciblée

Module 5 — Déploiement d'applications

- Applications Win32 : packaging, detection rules, requirements
- Applications MSI
- Applications Microsoft Store
- Applications mobiles (iOS / Android)
- Filtres d'appareils (Device Filters)
- Cycle de vie des applications

Travaux pratiques – Module 5

- Packaging d'une application Win32 (IntuneWinAppUtil)
- Création des règles de détection
- Déploiement d'une application mobile iOS
- Déploiement d'une application Store Windows
- Test de mise à jour applicative

Module 6 — MAM / App Protection Policies

- Protection des données (DLP mobile)
- Scénarios BYOD
- Restrictions d'accès aux apps
- Gestion des sessions, chiffrement, sauvegarde
- Intégration avec Conditional Access

Travaux pratiques – Module 6

- Création d'une App Protection Policy (BYOD)
- Test sur un smartphone personnel
- Mise en place d'une restriction d'accès (CA + MAM)
- Validation du comportement (copier/coller, sauvegarde)

Module 7 — Conformité & Conditional Access

- Compliance Policies
- Device Health
- Actions de non-conformité
- Conditional Access : MFA
- Device filters
- App filters
- Scénarios Zero Trust
- Intégration conformité ? CA

Travaux pratiques – Module 7

- Création d'une stratégie de conformité complète
- Mise en place d'une politique CA "compliance required"
- Test d'accès bloqué / autorisé
- Analyse des logs CA

Module 8 — Endpoint Security & Defender

- Antivirus (Defender)
- Firewall avancé
- Attack Surface Reduction (ASR)
- BitLocker (Device Encryption)
- Account Protection
- Device Control

- Intune Suite : EPM (Endpoint Privilege Management)
- Remediations
- Microsoft Defender for Endpoint : onboarding, investigation

Travaux pratiques – Module 8

- Déploiement d'une stratégie ASR
- Activation BitLocker via Intune
- Onboarding d'un poste dans MDE
- Analyse d'une alerte MDE
- Création d'une remediation automatique

Module 9 — Supervision & Troubleshooting

- Monitoring Intune
- Rapports Intune
- Log Analytics Workbooks
- Diagnostic des appareils
- Troubleshooting avancé (MDM logs, Event Viewer)

Travaux pratiques – Module 9

- Création d'un Workbook personnalisé
- Analyse d'un poste via les logs Intune
- Diagnostic d'un échec de déploiement
- Mise en place d'une alerte Log Analytics

Module 10 — Automatisation & Design

- PowerShell Intune
- Graph API
- Automatisation des déploiements
- Remediations avancées
- Bonnes pratiques de design Intune
- Modèles d'architecture entreprise

Travaux pratiques – Module 10

- Appel Graph API pour récupérer les devices
- Script PowerShell pour automatiser un déploiement
- Création d'une remediation personnalisée
- Atelier final : Conception d'une architecture Intune complète
- Présentation du design par les participants