+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 14/08/2025

S'inscrire

# Formation Ivanti Neurons Mobile Device Management (MDM)

2 jours (14 heures)

## Présentation

Ivanti Neurons for MDM est une solution UEM cloud moderne qui permet d'administrer et sécuriser l'ensemble de vos terminaux mobiles et postes (iOS, Android, Windows, macOS, ChromeOS) depuis une plateforme unifiée.

Cette formation vous apprendra à intégrer Entra ID (Azure AD), Apple Business Manager et Android Enterprise, à configurer Sentry/AppTunnel pour l'accès sécurisé, et à automatiser vos opérations via règles et APIs.

Vous orchestrez l'enrôlement, les politiques et la distribution d'applications, tout en protégeant les données métiers et en assurant la conformité.

À l'issue, vous saurez concevoir, déployer et exploiter une architecture MDM robuste, sécurisée et optimisée pour les enjeux Data. Comme toutes nos formations, celle?ci couvre la dernière version stable documentée d'Ivanti Neurons for MDM

## Objectifs

- Définir une architecture UEM sécurisée et scalable
- Mettre en œuvre enrôlement, politiques et distribution d'apps
- Sécuriser l'accès (Sentry/AppTunnel) et la conformité
- Industrialiser avec règles et APIs REST
- Superviser, diagnostiquer et maintenir la QoS

## Public visé

- Administrateur système
- Responsable mobilité orientés data
- Ingénieurs production/ops mobilité

## Pré?requis

- Connaissances en réseau, IAM/SSO et sécurité
- Notions Azure/Entra ID, Apple et Google pour l’entreprise

# Programme de formation Ivanti Neurons Mobile Device Management (MDM)

## Fondamentaux UEM & architecture Neurons

- Rôle d’Ivanti Neurons for MDM dans une stratégie UEM orientée Data
- Périmètre plateformes : iOS/iPadOS, Android, Windows, macOS, ChromeOS
- Modèles d’enrôlement : COPE/COBO/COBYO, ABM/ASM, Android Zero?Touch, Knox
- Gouvernance : RBAC, tenants, groupes dynamiques, traçabilité et Audit Trail
- Intégrations cœur SI : Entra ID, PKI, IdP/SSO, SCIM
- Atelier : cartographier votre architecture UEM et définir le périmètre de données

## Enrôlement & identité

- Préparation tenant : noms de domaine, certificats, jonction Apple/Google
- Apple Business Manager : tokens VPP/ABM, DEP/Automated Device Enrollment
- Android Enterprise : profils Work Profile, Fully Managed, COSU
- Sécurité identité : MFA, Conditional Access, stratégies de mot de passe
- Bonnes pratiques d’onboarding et communication utilisateurs
- Atelier : mettre en place un parcours d’enrôlement iOS et Android de bout en bout

## Applications, configurations & conformité

- App Catalog, canaux de distribution (Public/VPP/Private/In?House)
- AppConfig, Managed App Config, KSP (Knox Service Plugin)
- Politiques : Wi?Fi, VPN, certificats, restrictions, DDM (Apple)
- Compliance : règles, actions, remédiations, intégration Conditional Access

- Pilotage : inventaire, étiquetage, rapports, exports CSV/Elastic
- Atelier : publier une app gérée avec configuration et règles de conformité

### Accès sécurisé & protection des données

- Sentry / AppTunnel : passerelles, profils, certificats et haute dispo
- Données professionnelles : conteneurs, Data Loss Prevention, Managed Open?in
- Mobile Threat Defense (Zimperium) : intégration et politiques de risque
- Posture de l’appareil : Device Compliance ? accès ressources
- Journalisation, Audit Trail, conservation et export sécurisés
- Atelier : sécuriser l’accès e?mail interne via Sentry + MTD

### Automatisation, API & opérations

- Règles et Workflows basés sur attributs, Account/Rule Groups
- APIs REST : principes, pagination/limites, authentification, Swagger
- Tâches récurrentes : modèles d’assignation, cycles de vie, labels
- Supervision : dashboards, alertes, recherche avancée, rapports programmés
- Gestion des changements, validations, revue de sécurité
- Atelier : automatiser l’ajout d’un device au bon groupe + déploiement app/politiques

### Dépannage, performance & bonnes pratiques

- Diagnostics : Device Details, logs, App/Device Timeline
- Performance : impact des règles, volumes d'inventaire, latence, capacity planning
- Continuité : sauvegardes, rotations de tokens/certificats, HA Sentry
- Conformité & audit : preuves, RBAC, séparation des environnements
- Kits de déploiement et check?list Run/Operate
- Atelier : runbook de résolution d’un incident d’enrôlement + checklist go?live

## Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs

personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.