Updated on 14/08/2025

Sign up

Ivanti Neurons Mobile Device Management (MDM) Training

2 days (14 hours)

Overview

Ivanti Neurons for MDM is a modern UEM cloud solution that enables you to manage and secure all your mobile devices and desktops (iOS, Android, Windows, macOS, ChromeOS) from a unified platform.

This course will teach you how to integrate Entra ID (Azure AD), Apple Business Manager and Android Enterprise, configure Sentry/AppTunnel for secure access, and automate your operations via rules and APIs.

You'll orchestrate enrolment, policies and application distribution, while protecting business data and ensuring compliance.

At the end of the course, you'll know how to design, deploy and operate a robust, secure MDM architecture optimized for Data challenges. As with all our training courses, this one covers the latest documented stable release of Ivanti Neurons for MDM.

Objectives

- Define a secure and scalable UEM architecture
- Implement app enrolment, policies and distribution
- Secure access (Sentry/AppTunnel) and compliance
- Industrialize with rules and REST APIs
- Supervise, diagnose and maintain QoS

Target audience

- System administrator
- Data-oriented mobility managers
- Production engineers/mobility ops

Prerequisites

- Knowledge of networks, IAM/SSO and security
- Knowledge of Azure/Entra ID, Apple and Google for the enterprise

Ivanti Neurons Mobile Device Management (MDM) training program

UEM fundamentals & Neurons architecture

- The role of Ivanti Neurons for MDM in a data-driven UEM strategy
- Platform scope: iOS/iPadOS, Android, Windows, macOS, ChromeOS
- Enrollment models: COPE/COBO/COBYO, ABM/ASM, Android Zero Touch, Knox
- Governance: RBAC, tenants, dynamic groups, traceability and Audit Trail
- Core IS integrations: Entra ID, PKI, IdP/SSO, SCIM
- Workshop: mapping your UEM architecture and defining the data perimeter

Enrolment & identity

- Preparing to hold: domain names, certificates, Apple/Google junction
- Apple Business Manager: VPP/ABM tokens, DEP/Automated Device Enrollment
- Android Enterprise: Work Profile, Fully Managed, COSU
- Identity security: MFA, Conditional Access, password strategies
- Best practices in onboarding and user communication
- Workshop: setting up an end-to-end iOS and Android enrolment process

Applications, configurations & compliance

- App Catalog, distribution channels (Public/VPP/Private/In?House)
- AppConfig, Managed App Config, KSP (Knox Service Plugin)
- Policies: Wi?Fi, VPN, certificates, restrictions, DDM (Apple)
- Compliance: rules, actions, remediation, Conditional Access integration

- Monitoring: inventory, tagging, reports, CSV/Elastic exports
- Workshop: publishing a managed app with configuration and compliance rules

Secure access & data protection

- Sentry / AppTunnel: gateways, profiles, certificates and high availability
- Professional data: containers, Data Loss Prevention, Managed Open?in
- Mobile Threat Defense (Zimperium): integration and risk policies
- Device posture: Device Compliance ? resource access
- Logging, Audit Trail, secure storage and export
- Workshop: securing internal e-mail access via Sentry + MTD

Automation, API & operations

- Attribute-based rules and workflows, Account/Rule Groups
- REST APIs: principles, pagination/limits, authentication, Swagger
- Recurring tasks: assignment models, lifecycles, labels
- Supervision: dashboards, alerts, advanced search, scheduled reports
- Change management, validation, security review
- Workshop: automating the addition of a device to the right group + app/policy deployment

Troubleshooting, performance & best practices

- Diagnostics: Device Details, logs, App/Device Timeline
- Performance: impact of rules, inventory volumes, latency, capacity planning
- Continuity: backups, token/certificate rotations, HA Sentry
- Compliance & audit: proofs, RBAC, separation of environments
- Deployment kits and Run/Operate checklists
- Workshop: enrolment incident resolution runbook + go?live checklist

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as enrolment is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, his or her expectations and personal objectives with regard to the forthcoming training course, and his or her level of proficiency in the various technologies.

expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.