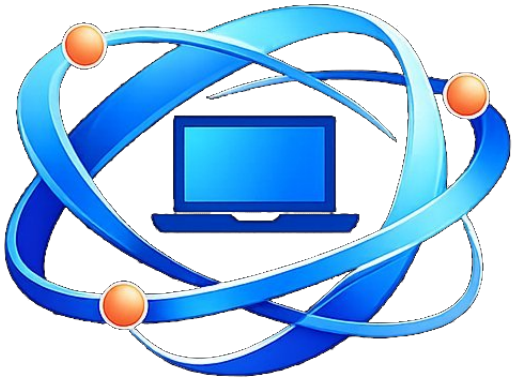

MFE-IT

Reference: INTUNE-MDM-MOB

Microsoft Intune Training Course

Mobile Device Management for Android and iOS

Duration: 3 Days | Hours: 21 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Mobile device management has become a strategic challenge for organisations of all sizes. From corporate-owned smartphones to BYOD scenarios, IT teams must control how devices access company data, enforce compliance and protect sensitive information across iOS, iPadOS and Android fleets.

This training course provides you with a comprehensive, hands-on understanding of Microsoft Intune for managing Android and iOS devices in an enterprise environment. You will learn to configure enrolment policies, enforce compliance, deploy applications, and integrate Apple Business Manager and Samsung Knox — covering the full MDM/MAM lifecycle from onboarding to troubleshooting.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Understand the key challenges of enterprise mobility management and the principles behind EMM/UEM solutions
- Master the Microsoft Intune architecture and its integration with Microsoft Entra ID and the Microsoft 365 ecosystem
- Configure and administer mobile device management (MDM) and mobile application management (MAM) policies
- Deploy and manage Android and Apple device enrolment using the available registration methods
- Implement compliance and security policies to protect corporate data and mobile endpoints
- Administer Android Enterprise and Samsung Knox environments, including automatic enrolment and firmware update management
- Integrate Apple Business Manager with Microsoft Intune to automate iOS and iPadOS device enrolment
- Deploy and manage mobile applications via Managed Google Play and Apple VPP
- Monitor device health and troubleshoot enrolment issues, compliance failures and platform synchronisation problems

PREREQUISITES

- Basic knowledge of Microsoft Entra ID (formerly Azure Active Directory)
- Familiarity with Windows client operating systems
- General understanding of mobile OS environments (Android, iOS/iPadOS)

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

- IT professionals responsible for deploying, managing and maintaining mobile devices and corporate applications
- System administrators and endpoint engineers working in mid-to-large organisations
- IT security engineers seeking to enforce mobile compliance and data protection policies
- Any IT professional looking to master Microsoft Intune for Android and iOS fleet management

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Day 1 – Intune Foundations, Architecture and Enrolment Policies

- Introduction and mobility overview: enterprise mobility challenges, EMM vs UEM concepts, Microsoft mobility stack
- Intune architecture: tenant setup, licensing, integration with Azure / Entra ID, RBAC configuration, dynamic groups
- Core concepts: device management (MDM) vs app management (MAM); compliance framework overview
- Workshop 1 – Intune hands-on: connect to the tenant, navigate the admin centre, create a dynamic group, assign a policy
- Enrolment methods: Android Work Profile, Fully Managed; Apple User Enrolment, Automated Device Enrolment
- Compliance and security: compliance policies, conditional access, device health attestation
- Workshops 2 & 3: create and assign a compliance policy; deploy a configuration profile to a group

Day 2 – Android Enterprise and Samsung Knox Management

- Android Enterprise: management modes (Work Profile, Fully Managed, Dedicated); security model and app management overview
- Samsung Knox: Knox architecture, enterprise advantages, zero-touch readiness
- Knox Mobile Enrollment (KME): auto-enrolment concepts, profile creation, association with Intune
- Workshop 4: create a KME profile, link to Intune, enrol a Samsung device
- Samsung EFOTA: controlling Android firmware versions, staging and freezing OS updates
- Workshop 5: create and assign an EFOTA policy
- Android app management: Managed Google Play, internal apps, deployment strategies
- Workshop 6: publish an app to Managed Google Play and deploy to a group

Day 3 – Apple iOS/iPadOS Management and Troubleshooting

- Apple enterprise platform: Apple Business Manager (ABM), device supervision, managed Apple IDs, Automated Device Enrolment
- ABM and Intune integration: APNS certificate, ABM token, enrolment programme token
- Workshop 7: connect Apple Business Manager to Microsoft Intune
- Automated Device Enrolment (ADE): full enrolment workflow from device purchase to automatic enrolment
- Workshop 8: enrol an iPhone using Automated Device Enrolment
- Apple app management (VPP): Volume Purchase Program, app licence management, user and device assignment
- Workshop 9: deploy an iOS application via VPP
- Troubleshooting and best practices: enrolment logs, compliance errors, ABM and Knox sync issues, diagnosing a non-compliant device
- Closing: group naming best practices, policy naming conventions, security architecture recommendations

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts