

Updated on 09/29/2026

Sign Up

Ivanti Endpoint Manager Mobile (EPMM) Certification Training

3 days (21 hours)

Overview

Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, enables you to manage, secure, and control mobile devices, applications, and business data from a centralized platform.

Our Ivanti Endpoint Manager Mobile (EPMM) Administrator Certification training will equip you with the skills needed to administer an EPMM environment and prepare you for the Administrator certification.

You will learn how to configure the platform, manage identities and certificates, and administer Android Enterprise and Apple devices. You will implement security and compliance policies as well as remediation mechanisms for non-compliant devices.

You'll also learn how to distribute and protect applications with AppConnect, secure access to resources with Standalone Sentry, and monitor, maintain, and troubleshoot your environment.

Upon completion of this training, you will be able to administer and secure Ivanti EPMM and will have the skills necessary to prepare for the Administrator-level certification.

Like all our training courses, this one will introduce you to **the latest stable version** of Ivanti MobileIron technology ([1.10.16](#)) and its new features.

Objectives

- Understand the Ivanti EPMM architecture

- Configure identities, roles, and certificates
- Administer Android Enterprise and Apple devices
- Implement security and compliance policies
- Administer AppConnect and Standalone Sentry
- Monitor, Maintain, and Troubleshoot EPMM
- Prepare for the Ivanti EPMM Administrator certification

Target Audience

- Ivanti EPMM Administrators
- Mobility and MDM/UEM Administrators
- System administrators
- Systems and Security Engineers

Prerequisites

- General knowledge of system and network administration
- Understanding of MDM/UEM principles
- Basic knowledge of LDAP, certificates, and authentication

Ivanti Endpoint Manager Mobile (EPMM) Training Curriculum

[Day 1 - Morning]

EPMM Architecture, Components, and Administration

- Understand the positioning of Ivanti Endpoint Manager Mobile (EPMM) and the platform's MDM, MAM, and MCM functions
- Identify the architecture and roles of the components: Admin Portal, System Manager, Enterprise Connector, CLI, and API
- Understand the communication flows between EPMM, endpoints, directories, and external services
- Navigate the administration interfaces and master the organization of users, devices, and configurations
- Understand administrative roles, permissions, and the principles of administrative delegation
- Hands-on workshop: Analyze an EPMM architecture, identify its components, and perform key operations using the administration interfaces.

[Day 1 – Afternoon]

Configure the platform, identities, and certificates

- Identify infrastructure prerequisites and configure key EPMM system settings
 - Connect enterprise directories using LDAP and manage the synchronization of users and groups
 - Configure administrative roles and control access rights to platform features
 - Understand the use of certificates in EPMM and configure certificate authorities
 - Distribute the certificates required for device authentication and access to corporate resources
 - Configure key integrations with internal services, email, and the company's
- Hands-on workshop: Integrate an LDAP directory, configure administrative roles, and set up certificate distribution for devices.

[Day 2 - Morning]

Administer device enrollment and lifecycle management

- Understand the device registration and enrollment processes in EPMM
- Administer Android Enterprise, work profiles, and fully managed devices
- Configure Managed Google Play, Android Zero Touch, and Samsung Knox Mobile Enrollment
- Manage Apple devices with Apple Business Manager, Device Enrollment, and User Enrollment
- Use Mobile@Work and select the appropriate enrollment mode for work and personal devices
- Manage the device lifecycle: lock, deactivate, wipe, delete, and re-enroll
- Hands-on workshop: Enroll and manage multiple device profiles, then perform key remote management actions.

[Day 2 - Afternoon]

Configure policies, compliance, and access control

- Create and deploy EPMM policies and configurations tailored to different device populations
- Configure restrictions, security settings, Wi-Fi, VPN, and work accounts
- Use labels and targeting criteria to control the assignment of configurations
- Define compliance rules and identify compromised, non-compliant, or high-risk devices
- Configure mechanisms for quarantining, restricting, and remediating non-compliant devices
- Link certificates, authentication, and compliance policies to control access to resources
- Hands-on Workshop: Developing a Comprehensive Compliance Policy, Tailoring It to a Specific Group set of devices, and addressing various non-compliance scenarios.

[Day 3 - Morning]

Manage applications, AppConnect, and secure access

- Deploy and manage public and internal apps from EPMM
- Manage Android Enterprise apps with Managed Google Play and Apple apps associated with the environment
- Understand the architecture and mechanisms of AppConnect to protect applications and work data
- Configure AppConnect policies and control data exchange between apps
- Understand the role of Standalone Sentry and secure access to internal resources and services
- Administer work content and maintain separation between personal and corporate data
- Hands-on workshop: Publish an app, apply an AppConnect policy, and configure secure access to a corporate resource via Sentry.

[Day 3 - Afternoon]

Maintain, monitor, and troubleshoot EPMM

- Monitor the status of EPMM devices, users, policies, configurations, and services
- Analyze events, logs, alerts, and compliance information to identify the root cause of an incident
- Diagnose issues with enrollment, LDAP, certificates, applications, and communication with endpoints
- Manage backups, restores, and major platform maintenance operations
- Prepare upgrades and verify the compatibility of components and integrations
- Use the CLI and understand the possibilities for automation and integration with EPMM APIs
- Hands-on workshop: Resolve several EPMM administration incidents, then review Administrator skills through practical questions and scenarios.

Strategies and Methods for Passing the Exam

- Identify the areas and skills required for the Ivanti EPMM Administrator certification
- Review key concepts related to architecture, configuration, enrollment, policies, security, and applications
- Analyze administration and troubleshooting scenarios that may be assessed
- Identify areas of weakness and organize your review before the exam

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Pre-training Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This

questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for the monitoring and smooth operation of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.