Modern Desktop and Mobile Device Management with Microsoft Intune Training

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Duration: **4 Day**

88% of learners would recommend this course.

- **Learn to deploy, configure and manage Windows, Android and Apple devices with Microsoft Intune.**
- **Designed for IT administrators and technical professionals responsible for modern device management.**
- **Build practical experience through expert-led instruction and hands-on labs using real enrolled devices.**

Modern Desktop and Mobile Device Management with Microsoft Intune is a **four-day, hands-on training course** designed for IT professionals who need to manage desktop and mobile devices through a centralised management solution.

The programme explores modern endpoint management using **Microsoft Intune** and **Microsoft Endpoint Manager**, introducing the core technologies and processes involved in administering devices across different platforms.

Throughout the course, participants learn how to **enrol, configure, manage and secure Windows, Android and Apple devices** within an organisational environment.

Training combines **instructor-led sessions** with **practical laboratory exercises**. Learners configure the Microsoft Endpoint management environment and gain experience enrolling and managing devices running different operating systems.

The course covers essential areas such as **device enrolment**, **compliance policies**, **conditional access**, **application deployment**, **data protection**, **endpoint security**, and **monitoring and reporting**.

Prerequisites

This course involves several technology areas associated with Microsoft platforms and enterprise device management.

Participants should have a good level of technical competence in at least one of the following operating systems:

- **Windows 10**
- **Windows 11**
- **Windows Server 2016**

Although no additional detailed technical prerequisites are required, knowledge or experience in some of the following areas would be beneficial:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Active Directory**
- **Cloud Services (SaaS)**
- **Windows operating systems**
- **Mobile device operating systems**
- **Application deployment**
- **Networking**
- **Public Key Infrastructure (PKI)**

Important: Multi-Factor Authentication (MFA) Requirements

For security purposes, Microsoft may require**Multi-Factor Authentication (MFA)** when accessing the **Microsoft 365 or Dynamics 365 tenants** used during the training.

Participants may therefore need to have a mobile device available to install and configure the free **Microsoft Authenticator** application before attending.

The application and setup instructions are available through the following resources:

- Microsoft Authenticator app
- Microsoft 365 MFA sign-in setup instructions

Who Should Attend

This training is intended for:

- **IT administrators** taking responsibility for modern device management.
- **Microsoft 365, Endpoint Manager and Intune administrators** who manage Windows, Android and Apple devices.
- **Desktop Support, Infrastructure and Workplace Technology professionals** moving from traditional device administration to **cloud-based device management**.
- Technical professionals with **Windows administration experience** who want to implement and manage **Microsoft Intune**.

Modern Desktop and Mobile Device Management with Microsoft Intune Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By completing the **Modern Desktop and Mobile Device Management with Microsoft Intune Training**, participants will develop the knowledge and practical skills needed to manage enterprise devices across multiple platforms.

By the end of the course, learners will be able to:

- Understand the **architecture and capabilities of Microsoft Intune and Microsoft Endpoint Management**.
- Configure and manage **device enrolment for Windows, Android and Apple devices**.
- Deploy and administer **device compliance and configuration policies** across different platforms.
- Implement **application deployment and management** using Microsoft Intune.
- Manage **security settings and device protection features** for modern endpoints.
- Apply practical skills through **hands-on labs**, configuring Microsoft Endpoint Manager and working with realistic device management scenarios.

This course helps participants strengthen their capabilities in**cloud-based device management**, **cross-platform endpoint security** and **enterprise application administration** using Microsoft Intune.

Training Outline

1. Introduction to Endpoint Management

The course begins by exploring why organisations need a **Unified Endpoint Management (UEM)** solution in today's IT environments.

Participants examine the requirements of modern device administration and the role of centralised management in supporting different device types.

2. Microsoft Endpoint Manager Options and Licensing

This module introduces the position of **Microsoft Endpoint Manager within the Microsoft ecosystem** and reviews the available licensing approaches.

Key topics include:

- **Microsoft Endpoint Manager components**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

- **Integration within the Microsoft ecosystem**
- **Available licensing options**
- **Selecting a suitable licensing approach**

3. Role-Based Access Control

After enabling Microsoft Endpoint Manager, participants explore how to establish an effective administration and support structure.

The module focuses on using **Role-Based Access Control (RBAC)** to provide detailed control over administrative permissions.

- **Configuring RBAC**
- **Defining administrative roles and permissions**
- **Implementing granular access control**
- **Establishing a structured support environment**

4. Hybrid Environments

This module examines the use of Microsoft Endpoint Manager within **hybrid IT environments**.

Participants explore how **Azure Active Directory** and **Active Directory Domain Services** can be connected, together with the **co-management capabilities of Configuration Manager** for administering Windows devices.

- **Hybrid endpoint management**
- **Azure Active Directory and Active Directory Domain Services integration**
- **Configuration Manager Co-management**
- **Concurrent management of Windows 10 and Windows 11 devices**

5. Device Enrolment and Management

Once the endpoint management environment has been configured, participants learn how to enrol and administer devices across different platforms.

The module introduces automated enrolment technologies and explains how to apply organisational compliance requirements.

Key topics include:

- **Microsoft Autopilot V2** for automated device enrolment
- **Apple Business Manager** integration
- **Google Zero-touch** enrolment

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- **Device Compliance Policies**
- **Conditional Access** configuration

Participants also learn how to ensure that devices can access organisational services only when they satisfy the required **security and compliance conditions**.

6. Application Deployment and Control

After devices have been enrolled and brought under management, the course explores how to**deploy, configure and protect applications**.

Participants learn how Microsoft Endpoint Manager can be connected to different application stores, enabling applications to be acquired and distributed at an organisational level.

Topics covered include:

- **Microsoft's business application store**
- **Apple App Store**
- **Google Play Store**
- **Corporate application acquisition and distribution**
- **App Protection Policies**
- **App Configuration Policies**

The module also explains how to protect **corporate data within applications** and configure applications before they are used for the first time.

7. Security in Microsoft Intune

This module focuses on the security capabilities of**Microsoft Intune** and their practical use in protecting enterprise devices.

Participants learn the distinction between **Endpoint Security**, which is used to configure device security policies, and **Microsoft Defender for Endpoint**, which provides advanced threat detection and response capabilities.

The module covers:

- **Endpoint Security** for managing device security policies
- **Microsoft Defender for Endpoint** for advanced threat detection and response
- **BitLocker drive encryption** on Windows devices
- **FileVault encryption** on macOS devices
- **Windows Security Baselines** for implementing recommended security practices

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- **Windows Defender Antivirus** integration
- **Activation Lock** for securing Apple devices
- Intune device management actions: **Wipe, Retire and Delete**

By the end of this module, participants will understand how to use**Microsoft Intune security features** to help protect organisational data and endpoint devices.

8. Monitoring and Reporting

The final module introduces the**monitoring and reporting tools** available within Microsoft Endpoint Manager.

Participants explore how these tools can be used to dynamically monitor the**health, activity and operational status of managed endpoint devices**.

- **Endpoint Manager reporting tools**
- **Monitoring device health**
- **Tracking endpoint activity**
- **Dynamic monitoring and reporting**