

Mobile Device Management (MDM)

H2: Mobile Device Management · Microsoft Intune MDM & MAM Framework



MDM vs MAM — Two Pillars of Intune Mobile Management

Mobile Device Management (MDM)

Full device enrolment and management. Organisation controls the entire device — ideal for corporate-owned devices.

What Intune delivers:

- Full device enrolment & control
- Security policy enforcement
- Remote wipe & lock capability
- Device compliance monitoring
- Config profiles: VPN, Wi-Fi, email
- Certificate deployment
- BitLocker / FileVault encryption
- Windows Update management

Corporate-Owned Devices

All 4 Platforms

Full Policy Control

Remote Wipe Ready

Mobile Application Management (MAM)

App-level management without device enrolment. Protects corporate data inside apps — BYOD without compromising privacy.

What Intune delivers:

- App protection policies (no enrolment)
- Corporate data separation in apps
- Selective app wipe on departure
- Approved app catalogue deployment
- Per-app VPN configuration
- Copy/paste restrictions
- Data encryption within apps
- Works on personal devices

BYOD Friendly

No Enrolment Needed

Data Isolated

App-Level Control

BYOD (Bring Your Own Device) Security Framework

01

Device Registration

Employee registers personal device in Intune. Device checks for basic compliance — OS version, PIN, encryption.

- Self-service enrolment portal
- Automated compliance check
- Entra ID identity verified
- Device health attestation

02

Policy Application

MAM policies applied at app level — corporate data is encrypted and isolated from personal data on the device.

- App protection policies applied
- Corporate data encrypted in apps
- Personal data stays untouched
- Copy/paste between apps restricted

03

Secure Access Granted

Conditional access verifies device compliance + user identity before granting access to corporate resources.

- Entra ID conditional access check
- MFA verification enforced
- Compliant device = full access
- Non-compliant = blocked or limited

04

Ongoing Compliance

Intune continuously monitors device health. Non-compliance triggers automatic alerts and remediation actions.

- Real-time compliance monitoring
- Auto-alert on policy breach
- Selective wipe on non-compliance
- Quarterly policy review cadence

MDM+MAM

Dual Management

BYOD

Fully Supported

4-Step

BYOD Framework

8 Weeks

MDM Deployed

Zero Enrolment

MAM Option