MOBILE DEVICE MANAGEMENT (MDM) EXPLAINED

Mobile device management (MDM) refers to a set of functions and features that control the use of mobile devices in compliance with organizational policies. These functions include the management of software apps, inventory, policy, security, and services for mobile and electronic devices.

How mobile device management works

The devices are managed against these functions by administrators running a backend MDM platform that enables remote control over device functions. An overlay app or software is installed on the device to enable the MDM functionality and integrate with the backend services of the corporate network such as:

- Information access
- Data transfer
- Device log sharing
- Other capabilities as needed

The MDM solution effectively reduces the risks associated with conducting sensitive business tasks on mobile devices, including bring your own device (BYOD) and corporate-owned smartphones.

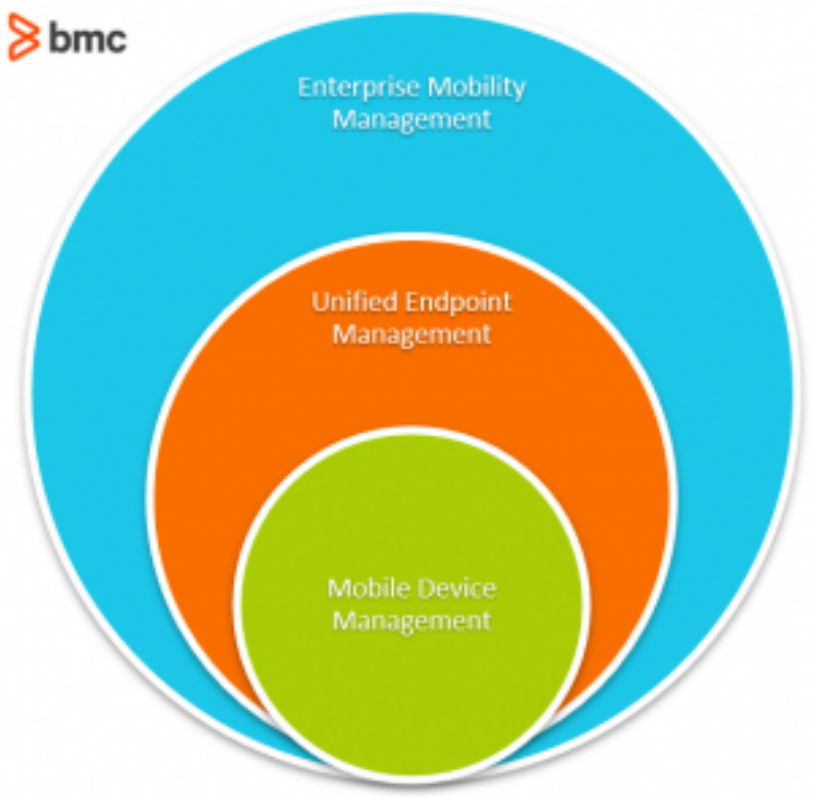
The importance of managing mobile devices

The proliferation of mobile devices and the growing BYOD trend fueled by the ongoing pandemic makes it crucial to adopt an MDM strategy. Take a look at some of the latest BYOD and enterprise mobility stats according to a recent research report:

- 67% of all employees use BYOD devices at the office.
- These devices enable users to spend an equivalent of an extra two hours daily for work related obligations.
- 87% of the employers are highly dependent on the workforce remotely accessing business information and apps on their devices.
- 69% of business decision makers support BYOD trends.
- 59% of businesses have already adopted BYOD strategies.
- The BYOD industry is expected to reach around $367 billion by the year 2022.

MDM is often a component of enterprise mobility management (EMM) solutions, which includes a collective set of tools to secure and manage mobile apps, company-provided and BYOD devices, content, data, and access. Components within an EMM solution may have overlapping features.

For instance, an MDM solution may also offer features to manage apps and data to complement what may be extensively offered only with mobile applications management solutions.



Mastering mobility: MDM vs EMM vs UEM

The mobility management space has received a lot of attention in recent years, with enterprise IT vendors entering the market with their own flavor of device management solutions. Phrases such as Mobile Device Management, Enterprise Mobility Management, and Unified Endpoint Management (UEM) are used commonly to sell overlapping and common features.

So, before we look at the key capabilities of an MDM solution, lets differentiate the terms MDM vs

EMM vs UEM:

- **Mobile device management** (MDM) is focused on managing smartphones and mobile devices connecting to a corporate network.
- **Enterprise mobility management** (EMM) is a superset of MDM and includes many components such as application management, mobile content management, mobile security management, mobile expense management, and identity and access management, among others.
- **Unified endpoint management** (UEM) consolidates the management of all endpoint devices including smartphones, IoT devices, sensors, wearables, and other endpoints. A single centralized platform unifies the management of all devices connecting to the network.

Capabilities of mobile device management

Switching back to MDM, we can identify the key elements of an MDM solution:

- **Asset management**, which includes multi-platform support for companies to apply custom organizational policies to enterprise mobility and BYO device use in the corporate network. Asset management might monitor and control how the devices can be used as well as enforce company policy across all enrolled devices, multiple platforms, and operating system versions.
- **Configurations management**, which can identify, control, and manage hardware and software settings based on geographic regions, user profiles, and identity.
- **Risk management**, audits, and reporting, which monitors device activity and reports anomalous behavior to limit issues such as unauthorized access of corporate networks or data transfers.
- **Software updates and distribution**, which can remotely control applications, software and OS updates, and licenses across multiple devices.
- **Profile management**, which allows management of policies and settings to specific groups of end users based on specific profiles.
- **Identity and access management**, which ensures that the device, data, network connection, and services are provided to appropriate authorized users.
- **Applications management,** which distributes, manages settings, and blocks or allows apps and software functionality.
- **Enterprise app stores**, which maintain a library of apps and services dedicated for corporate use that are available to authorized end-users.
- **Bandwidth optimization**, which manages bandwidth usage at the device and application level.
- **Data security**, which ensures that data is accessed, transferred, and utilized in accordance with organizational policies. For instance, in the event of device theft or loss, data stored on the device can be wiped out remotely.
- **Content management**, which synchronizes and secures business information across multiple devices.
- **Tech support**, which includes dedicated remote technology support can be provided remotely.

Best practices for mobile device management

The mobile device ecosystem is fragmented. Organizations constantly finding ways to enhance user productivity acknowledge the importance of BYOD devices for work, but struggle to translate

enterprise mobility into a productive workforce.

The following key best practices can help organizations adopt a risk-averse enterprise mobility strategy that also maximizes workforce productivity within the defined information security policies of your organization:

1. **Implement policies before deploying an MDM solution.** Establish the right set of policies to meet the unique technical and business needs of the organization before deploying an MDM solution.
2. **Make device enrollment to MDM solutions easy and convenient.** Ensure that no BYOD device goes under the radar, especially because of difficult or insufficient enrollment procedures or platform support.
3. **Establish self-service capabilities.** End user self-service is crucial in maintaining compliance with MDM solutions. Self-service capabilities can include remote data wipe-out, password reset, and lost device tracking.
4. **Ensure up-to-date MDM versions**. Push configuration changes, patch installations, and install software updates as soon as required and made available. A BYOD device running vulnerable outdated software is a security incident waiting to happen.
5. **Protect end-user privacy**. This will become key to ensuring end users continue compliance. Protect employee privacy by restricting data collection to a bare minimum and establishing procedures to eliminate misuse of personal employee information while still aligning with the company's technical and business needs.
6. **Deploy containment technologies**. These can separate corporate apps, data, and MDM controls from the personal use of a BYO device. With such containment in place, the MDM rules and features will only apply when the BYO device engages in corporate use.
7. **Monitor devices for specific activities or situations.** Monitor devices for anomalous activities or underoptimized data usage.

Top vendors for MDM technologies

The MDM solutions space is growing exponentially, and no individual vendor offers a one-size-fits-all solution for the enterprise market. The features span across the wide spectrum of Enterprise Mobility Management solutions, some of which may be more important to your enterprise than others.

- IBM MaaS360: An end-to-end AI-driven MDM solution. Additional capabilities include Unified Endpoint Management (UEM) that uses AI capabilities to analyze threats and manage security of mobile devices across all fronts.
- Cisco Meraki: A simplified platform that integrates well with the existing IT network. Granular BYOD management features that are easy to administer in a large enterprise. The attractive price point makes it a viable starting point for MDM at small and midsize business organizations.
- Citrix Endpoint Management: A powerful UEM technology that includes a feature-rich MDM solution. Citrix is one of the leading mobile cybersecurity solutions providers and is known for its popular and unintrusive BYOD device management capabilities.

More solutions listed here.

Related reading

- BMC Business of IT Blog
- BMC Service Management Blog
- ITSM vs ITOM: Service Management & Operations Management Explained
- Top IT Trends Today
- What Is the Internet of Behaviors? IoB Explained
- 5G for Companies: Hype, Reality & Potential