Mobile device management

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Mobile_device_management#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Mobile_device_management#searchInput)

|  |  |
| --- | --- |
|  | This article **is written like a**[**personal reflection, personal essay, or argumentative essay**](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#Wikipedia_is_not_a_publisher_of_original_thought) that states a Wikipedia editor's personal feelings or presents an original argument about a topic. Please [help improve it](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit) by rewriting it in an [encyclopedic style](https://en.wikipedia.org/wiki/Wikipedia:Writing_better_articles#Information_style_and_tone). *(December 2013) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

**Mobile device management** (**MDM**) is an industry term for the administration of [mobile devices](https://en.wikipedia.org/wiki/Mobile_device), such as [smartphones](https://en.wikipedia.org/wiki/Smartphone), [tablet computers](https://en.wikipedia.org/wiki/Tablet_computer) and [laptops](https://en.wikipedia.org/wiki/Laptop). MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.



**Contents**

* [1Overview](https://en.wikipedia.org/wiki/Mobile_device_management#Overview)
* [2Implementation](https://en.wikipedia.org/wiki/Mobile_device_management#Implementation)
* [3Device management specifications](https://en.wikipedia.org/wiki/Mobile_device_management#Device_management_specifications)
* [4Use in enterprise](https://en.wikipedia.org/wiki/Mobile_device_management#Use_in_enterprise)
* [5For mobile security](https://en.wikipedia.org/wiki/Mobile_device_management#For_mobile_security)
* [6Additional MDM features](https://en.wikipedia.org/wiki/Mobile_device_management#Additional_MDM_features)
* [7SaaS versus on-premises solutions](https://en.wikipedia.org/wiki/Mobile_device_management#SaaS_versus_on-premises_solutions)
* [8Evolution of MDM](https://en.wikipedia.org/wiki/Mobile_device_management#Evolution_of_MDM)
* [9See also](https://en.wikipedia.org/wiki/Mobile_device_management#See_also)
* [10References](https://en.wikipedia.org/wiki/Mobile_device_management#References)
* [11External links](https://en.wikipedia.org/wiki/Mobile_device_management#External_links)

Overview[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=1)]

MDM is typically a deployment of a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure, for the purpose of simplifying and enhancing the IT management of end user devices. In modern corporate IT environments, the sheer number and diversity of managed devices (and user behavior) has motivated MDM solutions that allow the management of devices and users in a consistent and scalable way. The overall role of MDM is to increase device supportability, security, and corporate functionality while maintaining some user flexibility.

Many organizations administer devices and applications using MDM products/services. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on devices, enforcing corporate policies, and integrating and managing mobile devices including laptops and handhelds of various categories. MDM implementations may be either on-premises or cloud-based.

Some of the core functions of MDM include:

* Ensuring that diverse user equipment is configured to a consistent standard / supported set of applications, functions, or corporate policies
* Updating equipment, applications, functions, or policies in a scalable manner
* Ensuring that users use applications in a consistent and supportable manner
* Ensuring that equipment performs consistently
* Monitoring and tracking equipment (e.g. location, status, ownership, activity)
* Being able to efficiently diagnose and troubleshoot equipment remotely

MDM functionality can include [over-the-air](https://en.wikipedia.org/wiki/Over-the-air_programming) distribution of applications, data and configuration settings for all types of mobile devices, including [mobile phones](https://en.wikipedia.org/wiki/Mobile_phone), smartphones, tablet computers, [ruggedized](https://en.wikipedia.org/wiki/Rugged_computer) mobile computers, mobile printers, mobile [POS](https://en.wikipedia.org/wiki/Point_of_sale) devices, etc. Most recently laptops and desktops have been added to the list of systems supported as Mobile Device Management becomes more about basic device management and less about the mobile platform itself. MDM tools are leveraged for both company-owned and employee-owned ([BYOD](https://en.wikipedia.org/wiki/Bring_Your_Own_Device)) devices across the enterprise or mobile devices owned by consumers.[[1]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-2) Consumer Demand for BYOD is now requiring a greater effort for MDM and increased security for both the devices and the enterprise they connect to,[[3]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-3) especially since employers and employees have different expectations concerning the types of restrictions that should be applied to mobile devices.[[4]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-BYOD-4)

By controlling and protecting the data and configuration settings of all mobile devices in a network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and [security](https://en.wikipedia.org/wiki/Network_security) of a mobile communications network while minimizing cost and downtime.[[5]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-BYOD_Requires_Mobile_Device_Management-5)

With mobile devices becoming ubiquitous and applications [flooding the market](https://en.wikipedia.org/wiki/Flooding_the_market), mobile monitoring is growing in importance.[[6]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-A_Playbook_for_Fighting_Apple_and_Google-6) The use of mobile device management across continues to grow at a steady pace, and is likely to register a compound annual growth rate (CAGR) of nearly 23% through 2028. The US will continue to be the largest market for mobile device management globally.[[7]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-Japan_to_Hold_Notable_Market_Potential_in_Mobile_Device_Management_Landscape-7) Numerous vendors help mobile device manufacturers, content portals and developers test and monitor the delivery of their mobile content, applications and services. This testing of content is done in real time by simulating the actions of thousands of customers and detecting and correcting bugs in the applications.

Implementation[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=2)]

Typically solutions include a server component, which sends out the management commands to the mobile devices, and a client component, which runs on the managed device and receives and implements the management commands. In some cases, a single vendor provides both the client and the server, while in other cases the client and server come from different sources.

The management of mobile devices has evolved over time. At first it was necessary to either connect to the handset or install a [SIM](https://en.wikipedia.org/wiki/Subscriber_identity_module) in order to make changes and updates; [scalability](https://en.wikipedia.org/wiki/Scalability) was a problem.

One of the next steps was to allow a client-initiated update, similar to when a user requests a [Windows Update](https://en.wikipedia.org/wiki/Windows_Update).

Central remote management, using commands sent over the air, is the next step. An administrator at the mobile operator, an enterprise IT data center or a handset OEM can use an administrative console to update or configure any one handset, group or groups of handsets. This provides scalability benefits particularly useful when the fleet of managed devices is large in size.

Device management software platforms ensure that end-users benefit from plug and play data services for whatever device they are using.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Such a platform can automatically detect devices in the network, sending them settings for immediate and continued usability. The process is fully automated, keeps a history of used devices and sends settings only to subscriber devices which were not previously set, sometimes at speeds reaching 50 over-the-air settings update files per second.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Device management systems can deliver this function by filtering [IMEI](https://en.wikipedia.org/wiki/IMEI)/[IMSI](https://en.wikipedia.org/wiki/International_mobile_subscriber_identity) pairs.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Device management specifications[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=3)]

* The [Open Mobile Alliance](https://en.wikipedia.org/wiki/Open_Mobile_Alliance) (OMA) specified a [platform-independent](https://en.wikipedia.org/wiki/Platform-independent) device management protocol called [OMA Device Management](https://en.wikipedia.org/wiki/OMA_Device_Management). The specification meets the common definitions of an [open standard](https://en.wikipedia.org/wiki/Open_standard), meaning the specification is freely available and implementable. It is supported by several mobile devices, such as PDAs and mobile phones.[[8]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-OMA_DM-8)
* [Smart message](https://en.wikipedia.org/wiki/Smart_message) is text SMS-based provisioning protocol (ringtones, calendar entries but service settings also supported like: ftp, telnet, SMSC number, email settings, etc...)
* [OMA Client Provisioning](https://en.wikipedia.org/wiki/OMA_Client_Provisioning) is a binary SMS-based service settings provisioning protocol.
* Nokia-Ericsson OTA is binary SMS-based service settings provisioning protocol, designed mainly for older Nokia and Ericsson mobile phones.

[Over-the-air programming](https://en.wikipedia.org/wiki/Over-the-air_programming) (OTA) capabilities are considered a main component of mobile network operator and enterprise-grade mobile device management software. These include the ability to remotely configure a single mobile device, an entire fleet of mobile devices or any IT-defined set of mobile devices; send software and OS updates; remotely lock and wipe a device, which protects the data stored on the device when it is lost or stolen; and remote troubleshooting. OTA commands are sent as a binary [SMS](https://en.wikipedia.org/wiki/SMS) message. Binary SMS is a message including binary data.[[9]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-9)

Mobile device management software enables corporate IT departments to manage the many mobile devices used across the enterprise; consequently, over-the-air capabilities are in high demand. Enterprises using OTA SMS as part of their MDM infrastructure demand high quality in the sending of OTA messages, which imposes on SMS gateway providers a requirement to offer a high level of quality and reliability.

Use in enterprise[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=4)]

As the [bring your own device](https://en.wikipedia.org/wiki/Bring_your_own_device) (BYOD) approach becomes increasingly popular across mobile service providers, MDM lets corporations provide employees with access to the internal networks using a device of their choice, whilst these devices are managed remotely with minimal disruption to employees' schedules.

For mobile security[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=5)]

All MDM products are built with an idea of Containerization. The MDM Container is secured using the latest cryptographic techniques (AES-256 or more preferred[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]). Corporate data such as email, documents, and enterprise applications are encrypted and processed inside the container. This ensures that corporate data is separated from user's personal data on the device. Additionally, encryption for the entire device and/or SD Card can be enforced depending on MDM product capability.

**Secure email**: MDM products allow organizations to integrate their existing email setup to be easily integrated with the MDM environment. Almost all MDM products support easy integration with Exchange Server (2003/2007/2010), Office365, Lotus Notes, [BlackBerry Enterprise Server](https://en.wikipedia.org/wiki/BlackBerry_Enterprise_Server) (BES) and others. This provides the flexibility of configuring email over the air.

**Secure docs**: Employees frequently copy attachments downloaded from corporate email to their personal devices and then misuse it. MDM can restrict or disable clipboard usage into or out of the secure container, restrict forwarding of attachments to external domains, or prevent saving attachments on SD card. This ensures corporate data is secure.

**Secure browser**: Using a secure browser can avoid many potential security risks. Every MDM solution comes with built-in custom browser. An administrator can disable native browsers to force users to use the secure browser inside the MDM container. URL filtering can be enforced to add additional security measures.

**Secure app catalog**: Organizations can distribute, manage, and upgrade applications on an employee's device using an App Catalogue. This allows applications to be pushed onto the user's device directly from the App Store or push an enterprise developed private application through the App Catalogue. This provides an option for the organization to deploy devices in Kiosk Mode or Lock-Down Mode.

Additional MDM features[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=6)]

There are plenty of other features depending on which MDM product is chosen:

* Policy Enforcing: There are multiple types of policies which can be enforced on MDM users.
  1. Personal Policy: According to corporate environment, highly customizable
  2. Device Platform specific: policies for advanced management of Android, iOS, Windows and Blackberry devices.
  3. Compliance Policies/Rules
* VPN configuration
* Application Catalogue
* Pre-defined Wi-Fi and Hotspot settings
* [Jailbreak](https://en.wikipedia.org/wiki/Jailbreak_(computer_science))/Root detection
* Remote Wipe of corporate data
* Remote Wipe of entire device
* Device remote locking
* Remote messaging/buzz
* Disabling native apps on device
* Some [Kiosk software](https://en.wikipedia.org/wiki/Kiosk_software) features[[10]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-10)

SaaS versus on-premises solutions[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=7)]

Present day MDM solutions offer both [software as a service](https://en.wikipedia.org/wiki/Software_as_a_service) (SaaS) and on-premises models. In the rapidly evolving industry such as mobile, SaaS (cloud-based) systems are sometimes quicker to set up, offer easier updates with lower capital costs compared to on-premises solutions which require hardware or virtual machines, need regular software maintenance, and might incur higher capital costs.

For security in [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing), the US Government has compliance audits such as [Federal Information Security Management Act of 2002](https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002) (FISMA) which cloud providers can go through to meet security standards.

The primary policy approach taken by Federal agencies to build relationships with cloud service providers is [Federal Risk and Authorization Management Program](https://en.wikipedia.org/wiki/Federal_Risk_and_Authorization_Management_Program) (FedRAMP) accreditation and certification, designed in part to protect FISMA Low, Moderate, High and Li-SaaS systems.[[11]](https://en.wikipedia.org/wiki/Mobile_device_management#cite_note-11)

Evolution of MDM[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=8)]

MDM is also about managing the device features, but its coupled with mobile content management (MCM) and Mobile Identity Management (MIM), Application management (MAM) it called as Enterprise Mobility Management (EMM). As EMM was specifically about managing the apps and content on mobile devices it was not able to manage older devices such as [Windows](https://en.wikipedia.org/wiki/Windows) laptops/desktops and new Macs, so EMM evolved into UEM ([Unified Endpoint Management](https://en.wikipedia.org/wiki/Unified_Endpoint_Management)) with additional functionality to manage both mobile and traditional devices such as desktops and laptops.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Mobile_device_management&action=edit&section=9)]

* [The SyncML Initiative](https://en.wikipedia.org/wiki/The_SyncML_Initiative)
* [OMA Device Management](https://en.wikipedia.org/wiki/OMA_Device_Management)
* [Open Mobile Alliance](https://en.wikipedia.org/wiki/Open_Mobile_Alliance)
* [Device Management Forum](https://en.wikipedia.org/wiki/Device_Management_Forum)
* [Over-the-air programming](https://en.wikipedia.org/wiki/Over-the-air_programming)
* [Mobile application management](https://en.wikipedia.org/wiki/Mobile_application_management)
* [Mobile content management system](https://en.wikipedia.org/wiki/Mobile_content_management_system)
* [Mobile security](https://en.wikipedia.org/wiki/Mobile_security)
* [Enterprise mobility management](https://en.wikipedia.org/wiki/Enterprise_mobility_management)
* [BlackBerry Enterprise Server](https://en.wikipedia.org/wiki/BlackBerry_Enterprise_Server)
* [List of Mobile Device Management software](https://en.wikipedia.org/wiki/List_of_Mobile_Device_Management_software)
* [Unified Endpoint Management](https://en.wikipedia.org/wiki/Unified_Endpoint_Management)