



MDM vs. MDM

What's the Difference Between
Mobile Device Management and
Modern Device Management?



Table of Contents

What “mobile device management” and “modern device management” each mean	3
The differences and similarities between the two platforms	4
Why so many people confuse the two – it’s more than just the shared “MDM” acronym	5
About Ivanti	7

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit [ivanti.com](https://www.ivanti.com)

When it comes to mobile device management versus modern device management, they may sound similar, but there's a significant degree of difference between them. The explosive growth in these devices within enterprises makes it crucial for organizations to choose the right platform for overseeing them.

What's mobile device management?

Mobile device management — we'll call it "mobile MDM" in this post — can be defined this way:

Mobile device management is a technology that helps an organization's IT and security teams to manage and secure their enterprise's mobile devices, such as smartphones, laptops and tablets, across different locations, formats and operating systems (OS).

Mobile MDM solutions help sysadmins efficiently configure, monitor and update the hardware and software settings on multiple mobile devices from one dashboard.

In this way, mobile MDMs ensure that an end user's device usage — whether directly managed or permitted to access organizational apps through bring-your-own-device (BYOD) policies — complies

with company policies and protects any confidential data stored or accessed through the endpoint.

Mobile MDM solutions typically include features such as:

- Policy enforcement.
- Software installation/update management.
- Remote wipe capabilities.
- Device tracking/monitoring.
- User authentication/authorization controls.
- Asset inventory management.

By allowing administrators to remotely manage these settings on all their organization's mobile devices from a single console or dashboard — regardless of the device type or operating system — mobile MDM solutions make it much easier for organizations to maintain consistent security policies across all of their connected assets.

Plus, most mobile MDM solutions provide robust support for enterprise mobility management (EMM). EMM provides additional layers of security for mobile endpoints by allowing administrators to enforce granular access controls over which applications can be installed or accessed by specific end users.

This granularity ensures that specific employee user profiles only have access to approved applications through an organization-approved app store, while also providing detailed visibility into each user's application usage and data sharing activities.

In addition to these security features, many mobile device management solutions also provide advanced analytics capabilities that allow organizations to gain valuable insights into endpoint device and data usage trends across their connected device base.

These endpoint analytics help organizations:

- Identify potential problem areas so they can proactively address issues before they become serious threats.
- Optimize IT and technology resources while improving user experience.

Overall, mobile MDM solutions represent a powerful tool for organizations looking to streamline the process of managing multiple mobile devices while maintaining a high level of security for their confidential data assets.

Mobile device management

is a technology that helps an organization's IT and security teams to manage and secure their enterprise's mobile devices.

Comparing MDM to MDM: what's the difference between mobile and modern device management?

There are two primary areas of difference between modern device management and mobile device management:

1. The kinds of devices covered by each MDM.
2. Each MDM's primary focus.

The differences and similarities between the two platforms

MDM difference #1: Modern device management solutions cover more types of endpoints than mobile device management

When comparing mobile device management versus modern device management (MDM), the first and most obvious difference between the two lies in their scope of coverage.

- *Mobile* device management covers traditional mobile devices such as smartphones, tablets and laptops.
- *Modern* device management reaches a wider range of connected network devices, including but not limited to:
 - IoT sensors.
 - Wearables (e.g., smart watches).
 - Medical equipment.
 - Industrial machinery.
 - Desktops.

MDM difference #2: Mobile device management focuses on controlling configurations; modern device management primarily collects and gathers usage data

Additionally, while both mobile device management and modern device management platforms are designed to manage corporate-owned mobile or connected devices within an organization's environment, the scope of control that each type of management provides varies greatly.

- *Mobile* device management provides IT administrators with comprehensive control over the configuration settings of each mobile device they manage, including access restrictions on applications or certain features.
- In contrast, *modern* device management is focused on monitoring user activity and providing insights into usage trends across all managed devices. It also allows for remote wiping of any sensitive data stored on the device if required.

Comparing MDMs: what do both mobile and modern device management have in common?

Despite these fundamental differences in scope and focus, these two types of device management solutions share some commonalities. Both:

- Offer enterprise-level security capabilities through encryption and authentication techniques.
- Allow for quick application patching.
- Provide device location tracking.
- Support geofencing capabilities.
- Enable software distribution.
- Have inventory management capabilities.
- Provide detailed reporting insights about each managed device.
- Enable automated backups.
- Ensure compliance with industry privacy standards, such as HIPAA or GDPR regulations.
- Reduce costs associated with managing a large fleet of devices by automating manual tasks.
- Increase productivity by streamlining processes related to device management operations, among other features.

Clearing up confusion over mobile device management versus modern device management

The similarities between the two MDM platforms offer quite a bit of room for confusion — even if *modern* device management solutions clearly cover a wider range of possible endpoint devices.

For example, both systems offer encryption technology for data security. However:

- *Mobile* MDM focuses more on authentication techniques.
- *Modern* MDM offers more detailed monitoring of user activity.

Similarly, both systems provide location tracking capabilities, but:

- *Mobile* MDM is better suited for managing fleets of devices or assets in remote locations.
- *Modern* MDM is better suited for tracking individual user device behavior.

Another area where confusion arises is software distribution. Both systems can deploy application updates and patches to devices remotely. However:

- *Mobile* MDM focuses only on over-the-air deployments.
- *Modern* MDM provides more comprehensive control over configuration settings.

	Encryption and security	Location tracking	Software distribution
Mobile device management	Focuses more on authentication techniques.	Better suited for managing fleets of devices or assets in remote locations.	Focuses only on over-the-air deployments.
Modern device management	Offers more detailed monitoring of user activity.	Better suited for tracking individual user device behavior.	Provides more comprehensive control over configuration settings

Finally, there are also differences in terms of reporting insights and automated backups. While both systems provide these features to varying degrees, depending on device type and usage requirements, it's important for customers to understand which system best meets their needs before making any decisions.

	Mobile device management	Modern device management
Primary devices focus	Phones, tablets, PDAs, COSU, etc.	Same as mobile, but with additional device types including servers, desktops, laptops, IoT, etc.
Management scope	Mobile device focus	User focus
Application deployment	Yes – via MAM	Yes – via in-house apps store
Endpoint configuration and policies	Mobile only	Yes
Device tracking	Mobile only	Yes
Reporting and trends	Limited	Yes
OS and application updates	Over-the-air	Comprehensive patching and management



Which MDM is right for you?

There are clear differences when contrasting mobile device management versus modern device management. And both offer extensive benefits to organizations looking for ways to optimize their IT infrastructure while ensuring their assets remain secure at all times.

The best practice in picking between the two? An organization should select an MDM system based on its individual requirements. For example, while both mobile and modern device management systems offer similar features like encryption technology or authentication techniques, they vary significantly in terms of scope and focus.

Make sure you select the solution that matches best with your current security protocols and desired feature set — because while they may share an acronym, their differences may make all the difference for your enterprise.


About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive.

We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

ivanti®

A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

For more information, or to contact Ivanti, please visit [ivanti.com](https://www.ivanti.com).