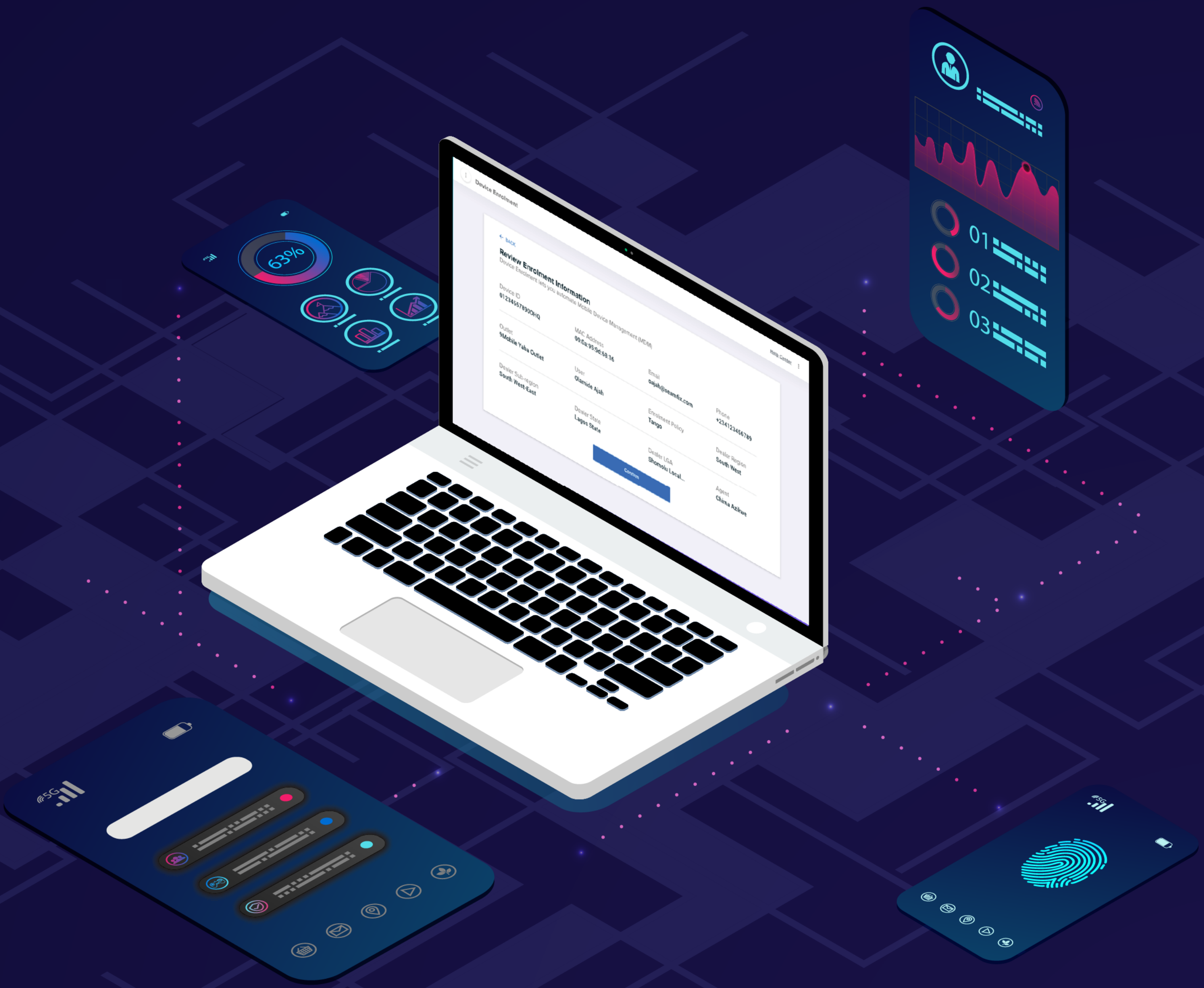
SmartMDM

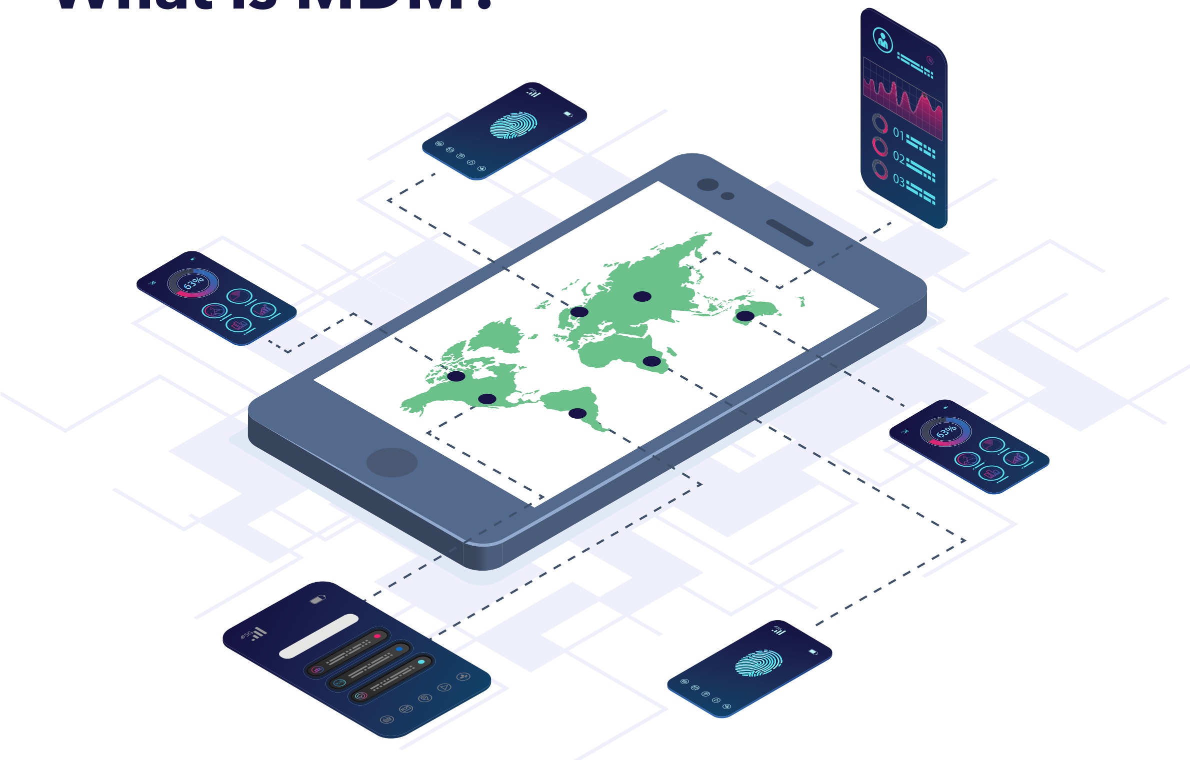
Complete Guide to Mobile Device Management (MDM)



www.seamfix.com/smartmdm/

A Product of SEAMFIX

What is MDM?



Mobile Device Management (MDM) helps you increase the security level of corporate data and mobile devices.This is achieved through the MDM software by monitoring, managing the mobile devices.

Why MDM?

Critical business data are shared across different mobile devices during work hours. This means that, if the device is hacked, stolen or lost, not only would the device be missing but the data on that device can be accessed by an authorised party.

Since the use of mobile devices can't be wiped off, there's a need to come up with a plan to protect business information and devices to reduce loss of property and breach of confidentiality of information.

How does MDM work

Mobile Device Management solution uses software that can run on cloud or on-site(premise). Through the console, admins can get role based access to the mobile devices. MDM can grant the admin access to data valuable for the organization, email, a secure VPN, GPS tracking, password-protected applications, and any other software needed to secure the data of your organization.

This doesn't encroach on the privacy of the user, as access is role based, meaning the admin can only access the softwares they've been given leverage to access.

Incase of theft, since the MDM has access to GPs tracking, the location of the phone can be tracked, and if given access to softwares where relevant company data are stored, the data can be wiped off from the device via the admin console area, to prevent information theft.

MDM ensures that the devices are kept safe from cyberthreats and malware.

Benefits of MDM

Regulatory Compliance

Compliance can be tracked and monitored through one centralized platform when you use Mobile Device Management tools. For some organizations, complying with a regulatory standard is very necessary. So having software in place with reporting is valuable.

Remote Management

The capacity to remotely manage users and the devices they are using is valuable. This helps to guarantee the security and health of all mobile devices connected to the network. Remote device access provides organizations with the option to disable any users or applications that are unauthorized. Thereby blocking specific access to important data. This can also reduce the risk of device misuse and data breaches.

Device Tracking

With some mobile device management solutions, you may have the option to track devices. This ensures that they remain within a specified safe location. Also, MDM solutions can help organizations to keep devices and data secure by setting and activating geo-locks.

Some companies have workers who are field-based and work within a specific, well-defined geographical area. In situations like this, geo-fencing can be highly useful for blocking access to stolen or lost devices. Also, geo-fencing limits your activity to your geographical radius.

Security Improvement

Organization-wide protocols and security procedures that apply to on-premises PCs can extend to all mobile devices. This means no loop in security protocols will be created. As things like identity management, access limitations, password regulation, and blacklists will extend to include mobile devices.

While mobile devices help increase efficiency and flexibility, a large number of devices and their use outside the office can sometimes cause challenges for the IT team – especially when employees are using various operating systems and device models.

No matter what size of the company you have, MDM provides indisputable benefits, including reduced support costs, increased employee productivity, and data security.

Therefore, many organizations rely on MDM tools that bring flexibility to both the IT department and end-users. With MDM, IT admins can securely manage all devices from a single portal, while employees can choose the devices they prefer to use.
No matter what size of the company you have, MDM provides indisputable benefits, including reduced support costs, increased employee productivity, and data security.

Here are a few reasons why you should invest in MDM:

Essential elements of MDM

MDM should provide security for your mobile devices

The primary purpose of MDM is security. Security is the most essential element of MDM. Your MDM should be able to protect your mobile device and the data in it, from a single management system. Key security features you need to look out for data encryption security configuration, and access monitoring.

MDM must have features for access control

MDM should have an access control feature that ensures only the right people have access to the right data. For this to occur, MDM needs to have a feature that carries out authentication and identity verification processes. If this is in place, you can be sure that only authorized users would have access to certain data.

Over-the-air (OTA) distribution

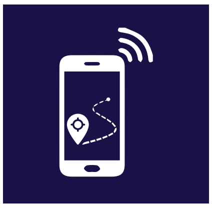
Your MDM software should not be dependent on physical connections to communicate to a device. An ideal MDM software should be able to push out information to devices connected to it wirelessly.

Remote Device troubleshooting

Your MDM software should be able to troubleshoot and fix devices connected to it, remotely. You don't need to be in the same location with your team members to troubleshoot their devices. Your MDM software should enable you to discover business-critical mobile devices and fix them remotely.

Remote wiping

A good MDM solution should be able to wipe off data from any device connected to it, in the event of a security breach, when the device is missing or any other situation that calls for clearing of data remotely. Your MDM solutions should be able to clear off all data even when the device isn't in the same location with the IT admin.



Device location tracking

In addition to remote data wiping, your enterprise should also be able to track a mobile device's location through an MDM system. ENsure one of its feature is GPS tracking , before selecting that MDM solution.

MDM and BYOD

BYOD is the acronym for bringing your own device. One common question people ask is, can MDM be used for personal devices. The answer is yes! It can be used, all you need to do is register the device with your MDM solution and you're good to go.

If your organization runs a BYOD system, here are some policies you may find helpful.

A BYOD policy may include all or some of the following:

- What constitutes acceptable use of personal devices for business activities;
- Types of mobile devices approved for use by IT;
- Software that must be installed to help secure the device, for instance mobile device management (MDM) or mobile application management (MAM) tools;
- Security measures such as password requirements;
- User responsibilities around the device and its access to the network;

- Any incentives or cost reimbursement for using personal data plans for work-related activities;
- A clear definition of the termination policy; and
- An exit plan when employees no longer wish to use their personal devices for work.

What devices work best with MDM?

MDM can be used to manage printers, laptops, desktops, phones, POS devices etc from the same portal.

Supported operating systems vary between MDM solutions. Some MDM solutions support just APPle or Android devices while some support a mix of different devices and operating systems. Enterprise Mobile Management supports multiple platforms like phone, laptops and POS etc. at the same time.

MDM Case Studies

TeleHealthcare

Mobile devices are used as a means for storage of client details for telehealth organizations. MDM helps healthcare organizations secure their devices and data and comply with industry regulations. It's easier to take devices into use and configure them according to company policies.

Transportation and logistics

Phones, laptops and tablets are used when carrying out tasks in the supply chain.Task like; accessing custom applications, scanning barcodes, locating deliveries, sending notifications, and making quality controls.

There's a need for them to be working at all times seeing as they are used for a crucial aspect of the business, hence MDM can help in troubleshooting quickly. Also, because supply chain is a crucial aspect, sensitive information like a client's address etc would be in it. MDM can help to ensure the security of these critical data, so that there would be no unauthorized access, endearing the lives of your clients, and breaching client's trust.

Education

Schools and other educational institutions are gradually adopting tablet-based teaching methods to facilitate teaching and learning. Tablets and laptops need to be correctly configured and have all the essential apps installed before they can be used in teaching. With Mobile Device Management, IT can configure the entire device fleet remotely and set restrictions for device usage, such as blacklist harmful applications or block access to specific websites.

Service industry

In service industries like restaurants, tablets are used for ordering food. MDM solutions can be used to turn the device into a single-app kiosk, since they would have multiple users.

A single-app kiosk uses the Assigned Access feature to run a single app above the lock screen. Once a user signs into the kiosk account, the app is launched and no other activity can be carried out on the device. This is needed to improve productivity among workers and prevent mixing of orders.

Government

Public sector organizations and governments handle sensitive data often. Hence the need to protect the devices to handle them. Governments must often comply with even stricter security standards than big corporations and securing devices and sensitive data is paramount. MDM helps public-sector organizations comply with regulations and increase operational efficiency with automation tools.

Managed Service Providers

Mobile Device Management helps Managed Service Providers (MSPs) IT service providers view all their customers' devices and manage them proactively. Your customers would be happier because they get to spend less time with the IT team.

Ready to MONITOR, TRACK, SECURE;MANAGE MULTIPLE MOBILE DEVICES ON ONE PLATFORM?

Visit: www.seamfix.com/smartmdm/ **or**
Call: +44 7756 238056 **or** +234-1-342-9192