

HOW TO NAVIGATE THE ANDROID MDM LANDSCAPE

Do's and Don'ts – Best practices



Mobile devices are an essential part of the workflow in most businesses today. Android devices are trendy among employees, as they are affordable, easy to use, and available in various shapes and sizes.

However, with the popularity of mobile devices – including Android devices – comes challenges. As a business, it is essential to ensure that employee Android devices are secure and used in a way that complies with company policies. That's why you need **Android MDM** (Mobile Device Management).

Android MDM (Mobile Device Management) allows businesses to manage and secure their Android devices.

With Android MDM, you can, among other things:



Monitor devices and data



Enforce policies



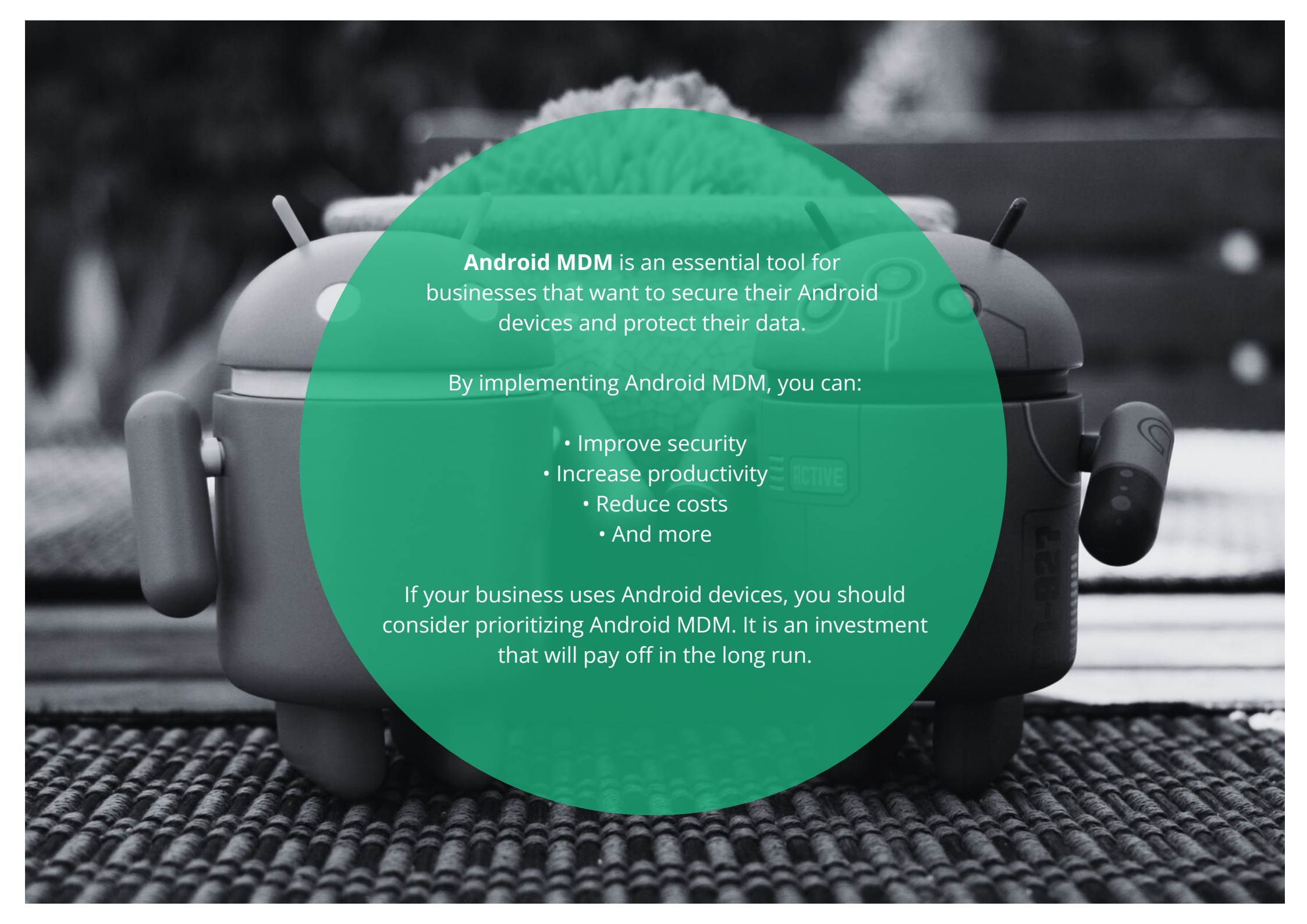
Back up and restore data



Remotely uninstall apps



Block access to specific websites and apps



Android MDM is an essential tool for businesses that want to secure their Android devices and protect their data.

By implementing Android MDM, you can:

- Improve security
- Increase productivity
- Reduce costs
- And more

If your business uses Android devices, you should consider prioritizing Android MDM. It is an investment that will pay off in the long run.

Security, security, and security

If your company has a focus on security, there are some things you should consider when choosing an Android MDM:

- Ensure the MDM solution offers robust security features like encryption and app control.
- Ensure the MDM solution is compatible with your company's Android devices.
- Make sure the MDM solution is easy to implement and use.
- Make sure the MDM solution is affordable for your company.



Considering these factors, you can choose an Android MDM that will help you protect your Android devices and data.

We have briefly listed some additional details about some of the security features you should also look for in an Android MDM:

- **Encryption:** Encryption protects your data from unauthorized access, even if the device is lost or stolen.
- **App control:** App control allows you to block or allow certain apps on your Android devices.

Choosing an Android MDM with solid security features can help protect your Android devices and data from hackers and other cyber threats.

WHEN CHOOSING **ANDROID MDM**

Do's



Consider your needs: What are your most essential requirements for an Android MDM solution? Do you need to be able to manage devices, monitor data, enforce policies, or do something else? Once you know what you need, you can narrow your options.



Research different solutions: There are many other Android MDM solutions on the market, so it's essential to research your options thoroughly before deciding. Compare prices, features, and user-friendliness to find the best solution.



Try it out: Most Android MDM providers offer [free trials](#), so you can try a solution before buying it. That is an excellent way to see if the solution meets your needs and is easy to use.



Talk to other businesses: Ask other organizations that use an Android MDM solution for their recommendations. They can share their experiences and give you insight into what is essential to consider when choosing a solution.

Don'ts



Don't choose a solution that doesn't meet your needs: It's essential to select an Android MDM solution that meets your needs. It would be best if you chose a solution that is powerful enough to be able to protect your data and manage your devices effectively.



Don't forget to consider your users' needs: An Android MDM solution should be easy for your users. If the solution is too complex, your users won't use it, and you won't be able to achieve the desired results.



Don't forget to implement the solution correctly: Once you have chosen an Android MDM solution, you must implement it correctly. That includes configuring the solution to meet your needs and training your users on how to use it.



Don't forget to monitor the solution: After implementing an Android MDM solution, you must watch it to ensure it works properly. That includes monitoring devices, data, and policies.

By following these do's and don'ts, you can choose the best Android MDM solution for your needs and ensure that it is implemented and monitored correctly.



CapaSystems is a Danish software and consulting company that has been dedicated to creating software solutions since 1996. Our goal is to provide a better overview, lower costs, higher end-user satisfaction, and greater flexibility for our customers. We achieve this by delivering expertise and smart technology that can leverage the potential of our customers' IT systems. At CapaSystems, you are guaranteed a solution that meets your needs.

CapaSystems is behind the development of two on-premise software solutions, **CapaInstaller** and **PerformanceGuard**, as well as the cloud solution **CapaOne**, which supports all deployment tools. We are constantly developing new products for CapaOne, including **Android** (management of the company's Android devices), **AdminOnDemand** (Privileged Access Management), **Drivers** (automatic driver updates), **Reliability** (providing a comprehensive overview and finding solutions to the company's IT challenges), and **Updater** (streamlined updating of third-party programs). Today, CapaSystems employs over 30 employees located in Taastrup and Skanderborg. CapaSystems' solutions are used by a wide range of Danish and international companies, with over 25% of Danish municipalities choosing to use CapaSystems software.

Book a meeting

Call us to book a presentation of our products that can save you and your organization vital time.

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup
Tel. (+45) 70 10 70 55
www.capasystems.com