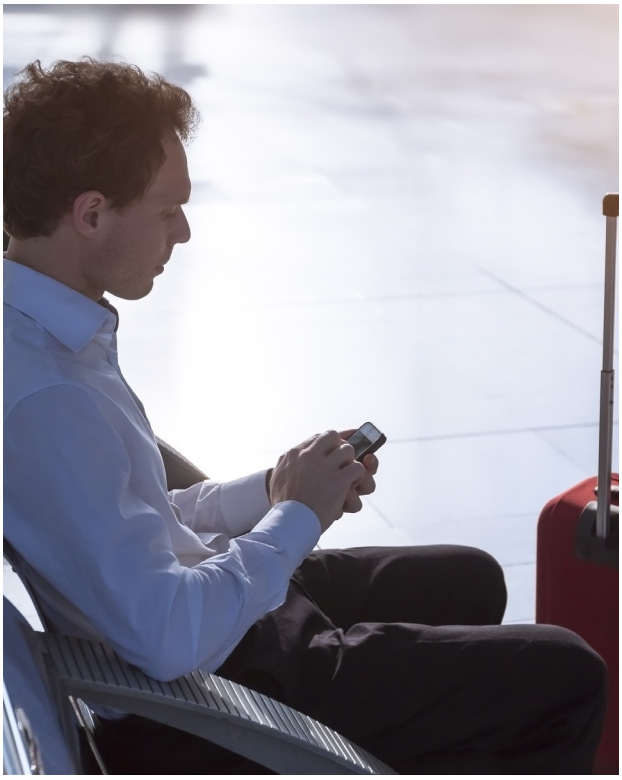
Employing a Mobile Device Management Solution: What You Need to Know to Get Started



Mobile devices used for business can drive productivity skyward, but they can also expose businesses to additional risk and liability. If managed incorrectly, they may even lead to decreased productivity due to lack of oversight. As more businesses incorporate various types of mobile devices, remote work and Bring Your Own Device (BYOD) policies, most need a way to manage employee device usage effectively.

Mobile device management (MDM) is software that monitors, manages and secures data and applications on employee- and company-owned devices within an organization. MDM helps prevent problems associated with mobile devices in the workplace, whether from lack of supervision of employee app usage, threats from unsecured networks or unenforced policies.

As with any new technology or process, getting your business and your employees ready to adopt MDM in advance will make for an even smoother transition. Taking the time to consider what MDM solution is right for you will help you enact policies that make your business safer and more productive.

Decide the Scope of Device Management

What level of MDM will you implement? Determine how much protection your business needs before proceeding. Each level adds more functionality while retaining all the features of the lower levels.

1. Basic Policy Management
Full device wipes and password protections.

2. Basic Device Management
Full and partial device wipes, application and inventory management, basic OS support and volume purchasing for apps.

3. Advanced Device Management
Comprehensive OS support, desktop support, user monitoring, role-based user administration and self-service portal and analytics.

4. Enterprise Mobility Management
Mobile application wrapping, custom software development kit, Personal Information Manager (PIM), secure web browser, mobile content synchronization, SSO authentication and location/network-based restrictions.

Create a Clear Policy

Once you decide on the MDM features that are right for your business, you need to create a policy that will cover the new procedures. Draft a written policy that explains MDM, your rules for accessing company information via mobile devices, and the ramifications for violating the policy.

Topics to address in your policy might include:

- **Devices**: What mobile devices will be supported? ?
- **Data plans**: Will the organization pay for the data plan?
- **Compliance**: What regulations govern the data your organization needs to protect?
- **Security**: What security measures are needed on mobile devices?
- **Applications**: What apps are permitted for work?
- **Agreements**: Is there an Acceptable Usage Agreement (AUA) for employee devices with corporate data?
- **Services**: What kinds of resources can employees access for training, troubleshooting and policy questions?
- **Privacy**: What data is collected from employees' devices and how will their privacy be protected?

A well planned MDM solution can help your business incorporate mobile devices and workflows while avoiding pitfalls down the road.

Prepare Your Employees

Preparing your workforce for a new policy is a key part of MDM adoption. If they have all the information in advance, they will be ready to install work software on their devices and adhere to new BYOD guidelines. To build trust around MDM, you should communicate clearly and transparently with your employees. Update them on decisions that could affect their personal devices or data. Allow them to ask questions before asking them to sign an MDM policy, and consider creating a FAQ that explains the benefits of MDM and how it will protect their devices.

Additionally, complexity breeds non-compliance. Poor usability stands in the way of MDM buy-in for 57% of employees.[1] Once your employees are on board with the policy, ensure they have clear instructions and a simple way to enroll their devices. Taking the time to walk through the newly-created policy will also help secure quick employee adoption and full policy adherence. If employees feel that they were included in the process and have clear instructions to follow, your business can transition smoothly to a full MDM solution.

To learn more about MDM solutions for your business, visit U.S. Cellular®.

Sources:

1. Hamblen, Matt. One-fifth of IT pros say their company had mobile data breach. Computer World, 2016. https://www.computerworld.com/article/3048799/mobile-wireless/one-fifth-of-it-pros-say-their-companies-had-mobile-data-breach.html