Digital Products and Services

White Paper
Mobile Device Management

ecom
A PEPPERL+FUCHS BRAND

Your automation, our passion.

PEPPERL+FUCHS

Contents

Introduction: The Modern Mobility Platform and Its Challenges

The use of smartphones and tablets as modern enterprise tools gives workers the flexibility to do their work in hazardous locations. In addition to enabling mobile work, they also enable safer work practices, increased productivity, and are a vital source of information for technicians responsible for completing even the most complex tasks.

While there are a wide range of benefits, the growing use of Windows® 10 and Android™ devices in plants presents IT managers with a range of challenges to overcome if the devices are to be integrated and managed effectively. In addition, working with smartphones and tablets creates a number of data security and protection challenges that need to be overcome.

Depending on the particular enterprise mobility strategy, enterprises can select from a large variety of device management models to equip their staff accordingly.

The Main Management Models

- **BYOD (Bring Your Own Device)**
  employees use their personal devices for work purposes—this is rarely seen in industrial environments
- **COPE (Corporate-Owned, Personally Enabled)**
  allows enterprise-owned equipment for personal use
- **COBO (Corporate-Owned, Business Only)**
  the company's own equipment is made available solely for work tasks
- **COSU (Corporately-Owned Single Use)**
  devices are locked down in a kiosk mode to perform only a single or small number of permitted tasks

Whether a company decides to allow BYOD, COPE, COBO, COSU, or even a mix of models, mobile devices must be intuitive for users and efficient for IT administrators. They must also ensure corporate security.

Mobile device management (MDM) is the standard way to securely and effectively enroll and integrate smartphones and tablets into corporate IT. MDM systems meet statutory provisions and compliance requirements when working with mobile devices. An example of MDM is Blackberry UEM, which is used internally by Pepperl+Fuchs.

1. Who Is This White Paper Suitable For?

This white paper is aimed at Pepperl+Fuchs employees who wish to gain basic knowledge about mobile device management systems. It shows how MDM software helps IT managers and administrators ensure security, visibility, and control over the use of smartphones and tablets within the enterprise. It is also designed to eliminate any misconceptions and help people understand the role of MDM in our customers' organizations. In our view, MDM systems do not have to be hard to set up or highly complex in order to perform efficiently and reliably. They are must-have solutions for customers' wishing to successfully execute enterprise mobility strategies.

2. What Is Mobile Device Management?

Mobile device management is the umbrella term for a suite of software-based solutions deployed to deliver centralized management and protection of mobile devices and applications in the corporate context. An efficient MDM system has intelligent functions for securely integrating terminal devices into a company's IT infrastructure, enabling productive, mobile work that complies with data protection regulations. Mobile device management solutions are available as subscription-based cloud services, such as Software as a Service (SaaS), or as on-premises software maintained on internal corporate servers.

3. What Is the Difference between EMM and MDM?

It's no longer just about smart devices. Enterprise mobility has evolved to focus more on secure information than on the device itself. This means that information is no longer primarily stored on the hardware; instead it is often uploaded to a remotely accessible server or a back-end cloud solution.

While solutions that are still considered MDM solutions by the newer interpretation of the term still exist, they are being phased out in favor of EMM solutions because of the simplicity and security that they offer.

Most EMM solutions also offer mobile app management, mobile content management, app wrapping, containerization, and other features. This provides an all-encompassing solution that works to cover every aspect of the device.

In this white paper, we have used the term MDM because we are currently focusing on hardware issues. Our solution eMDM can support a variety of EMM features as well.

4. Why Is Mobile Device Management Important?

MDM systems are used mainly for configuring, enrolling, and managing the mobile device estate and protecting corporate data and resources.

Easy mobile configuration and enrollment significantly reduces the workload of IT departments and is now widely expected within enterprises. Mobile device management makes it possible to execute models such as COPE through the MDM system, providing for the integration of the desired devices into the company's IT architecture.

The MDM system handles the staging/deployment of countless mobile devices, saving administrators from having to manually configure all settings and install necessary applications. Device staging is especially simple when the MDM system can be used with Android Zero-Touch. Apple's Device Enrollment Program (DEP) or Samsung Knox Mobile Enrollment (KME) are similar solutions.

If the MDM solution also has MAM (mobile application management), apps can be installed and fully configured from a management console on a wide variety of devices in just a few simple steps.

Employees must be able to use many types of mobile devices in various, and sometimes remote, parts of the world. Without MDM, it can be particularly challenging for our customers' IT departments to track versions of mobile operating systems, updates, and productivity apps and keep them up-to date.

MDM also allows access rights, configurations, network settings, and guidelines to be distributed and administered centrally.

5. Security Is Key

An MDM enables enterprise mobility and is also key to the protection of company data. Mobile device management allows terminal devices to be used securely and protects against data loss and theft in the event of device malfunction or misplacement. With MDM, companies can take emergency action, e.g., locating a lost device via location tracking and deleting company data remotely (remote wipe).

MDM software also enables companies to define and enforce software and data policies as well as user rights according to the role of the worker. The appropriate MAM options also make it possible to restrict the use of certain apps on mobile devices via an app filter.

6. The Main Role of MDM

- 6.1 Quick and easy enrollment and integration of mobile devices into corporate IT:

  Time-saving integration of company-owned smartphones and tablets. With MDM, the devices can be completely configured in just a few easy steps. Apps and policies can be distributed and managed from a central location anywhere in the world.

- 6.2 Backup of company data and compliance with data protection:

  With important features such as the strict partition of private and enterprise-owned data, password requests, and remote data wiping, MDM ensures that employees operate the devices in compliance with the GDPR and that company data is fully protected.

7. Who Needs an MDM Solution?

The selection and use of MDM solutions has become standard practice for all enterprises wishing to ensure adequate data protection (GDPR compliance) and secure integration of the devices into their IT architecture. For companies who use smartphones and tablets, an MDM system is recommended when there are 20 or more mobile employees, even if they only use their devices to read business emails or connect to the internet.

8. What Criteria Is Expected from MDM Solutions?

To ensure the productivity of mobile workers, safeguard enterprise security, and ease the burden on IT departments, MDM systems should meet the following criteria:

- 8.1 Cross-platform solution

  An MDM solution should support multiple operating systems and hardware platforms. Ideally, it should be able to use the native functions of the respective device manufacturer—e.g., the separation of business and private contacts from iOS 11.3 on or work profiles on Android Enterprise.

- 8.2 Simple and intuitive

  Administrators should be able to configure the MDM platform with minimum effort. It should also integrate seamlessly into the company's existing IT infrastructure and active directory. This makes it easy to adopt roles and rights and minimize effort and expense.

- 8.3 Centralized device setup and configuration

  It should be possible to centrally configure device policies, profiles, and certificates and send them to the appropriate devices with the click of a mouse. Check whether the MDM system supports Android Zero-Touch or Samsung Knox Mobile Enrollment.

- 8.4 Comprehensive mobile security

  The MDM system must reliably protect company data, terminal devices, and the connections between the mobile devices and corporate resources. The MDM solution should have features for password security enforcement, data encryption, individual device blocking (e.g., file downloads or screen mirroring). In addition, the MDM system must enable device localization and blocking as well as a remote wipe of all data or company data should a device be lost or stolen.

- 8.5 Remote support and maintenance

  If multiple locations are to be managed centrally, it is practical if updates, data, apps and configurations can be carried out and delivered centrally via MDM console.

9. Adding MAM to the MDM Stack

It is also an advantage if an MDM solution has MAM functions. Mobile application management is about applying security and certain settings directly to apps. For example, MDM options can help ensure that an application can be encrypted and password-protected or deleted and uninstalled remotely. With MAM, administrators can distribute apps to mobile devices and fully configure them.

- 9.1 Data protection, security, and compliance with MDM

  Data protection requirements have been increasing for years. Since the enforcement of the EU General Data Protection Regulation (GDPR), data controllers must apply appropriate technical and organizational measures to comply with data protection principles. MDM solutions help companies meet the requirements of the GDPR and their own compliance guidelines.

- 9.2 Mobile data protection is a must

  Since company smartphones and tablets have access to the same data and resources as standard desktop PCs and servers, data protection also needs to be extended to mobile devices. It is imperative to securely integrate mobile devices into company networks and rule out security leaks and breaches.

- 9.3 Data protection through mobile device management

  The MDM system provides for GDPR-compliant separation of private and business data on mobile devices. Security measures and policies are uniformly enforced and monitored via the MDM console. For example, corporate password security policies become mandatory to protect systems against unauthorized access. User profile, email account, VPN, and Wi-Fi access are configured automatically.

- 9.4 Device allocation models need specific security measures

  In COBO (corporate-owned, business only) and COPE (corporate- owned, personally enabled) scenarios, devices must be operated in a fully managed mode, where Android devices separate work profiles from personal data. If a device is lost, the business-related content on the relevant terminal device can be deleted remotely.

10. What Does ECOM Instruments Offer?

Since summer the of 2019, ecom has offered a new product range called "Digital Products and Services." This includes the possibility for customers to apply for a service called "eMDM." Users can request that this service be preinstalled when ordering hardware. This way, customers can benefit from the MDM system immediately.

Customers who already have their own MDM system can apply for a service called eCSL, which enrolls the devices into the preexisting system. However, compatibility of the requested ecom hardware and the existing customer MDM solution needs to be tested and verified separately for each request.

All other services are available for a large range of ecom products. Please contact your local sales representative to get more info, or visit **www.ecom-ex.com/eDS.**

11. References

https://developers.google.com
https://www.samsungknox.com
https://www.cortado.com

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality
Download our latest policy here:

www.pepperl-fuchs.com/quality

PEPPERL+FUCHS

www.pepperl-fuchs.com
Subject to modifications · © Pepperl+Fuchs · 05/20
Author: Carl Henderson / Marco Kuhn