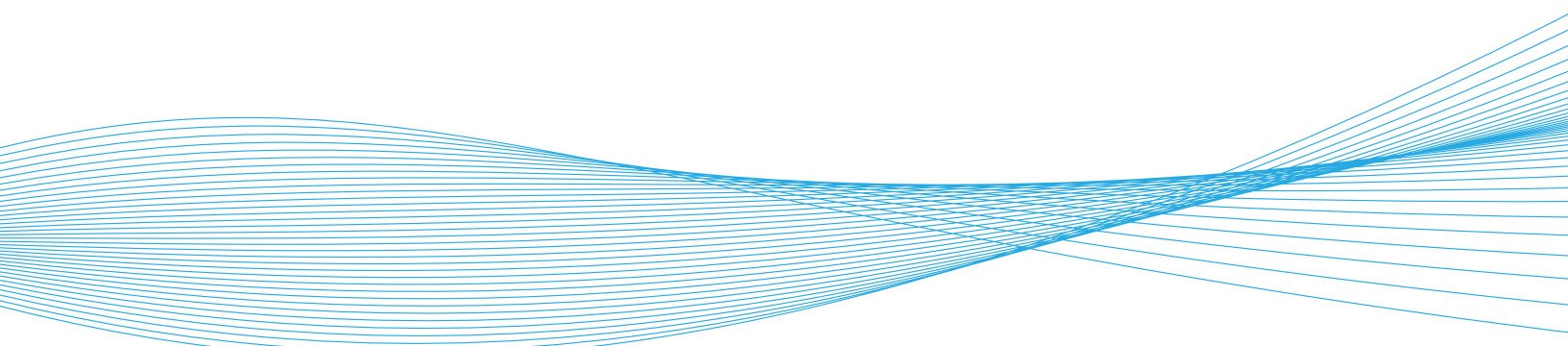
MaaS360® by Fiberlink

# 11 Best Practices for Mobile Device Management (MDM)



# 11 Best Practices for MDM

## Table of Contents



## Introduction

Businesses and employees are now using mobile devices in ways not envisioned as recently as a year ago. Personal device ownership and usage in the enterprise is growing rapidly, and more businesses than ever before are facing the challenge of how to fully provision, manage and secure mobile devices in their corporate environments. Desktops, laptops, smartphones and tablets are coming together and need a single platform to manage every device, both personal and corporate owned.

So what's slowing businesses down? It's the exercise of putting in place an IT strategy for management and operation. While it's understandable that IT would like to add a degree of rigor, it doesn't have to be that difficult to combine security with rapid enrollment.

This document describes 11 best practices for Mobile Device Management (MDM).

## Start With a Strong Foundation

These are the general requirements that all businesses should put into place.

### 1. HAVE A POLICY THAT'S REALISTIC

This means that you acknowledge the following two requirements:

1. 1. You have to support multiple device platforms in a single window
2. 2. You need to allow personal devices along with corporate owned ones

Nearly all organizations are doing this now—even if they don't know it. Chances are that your business has a BlackBerry corporate standard already in place. And your business has at least a few iPhones that sync to your Microsoft Exchange Server or Lotus Notes by enabling an Activesync protocol.

If that's the case, you probably have a lot more personal iPhones, Androids and Windows Mobile devices inside your organization, since it is easy for a mobile device to use ActiveSync functionality to integrate with corporate mail. Just Google "Setting up iPhone on Exchange" and see how your employees are doing it.

Need more reasons to consider allowing personal devices? The $199 phone purchase and $30/month data plans being paid by the employees will add up quickly to cost savings for your business.

## 2. TAKE STOCK USING A MULTI-PLATFORM REPORTING AND INVENTORY TOOL

Making decisions and quantifying risks regarding mobile devices is hard because businesses don't have good data on their mobile devices. For instance, it's not uncommon to uncover terminated employees with corporate mobile devices that are still functioning.

This can be solved with a lightweight reporting and inventory tool. Make sure your solution:

- Provides detailed visibility into what is out there.
- Works for help desk troubleshooting.
- Is accessible outside of IT (for instance, HR should have read-only access during exit interviews to avoid the previously mentioned issue).
- Has strong application inventory and search capabilities, because those will become increasingly more important.

It is imperative that you acquire this tool as quickly as possible, and that it be easy to implement.

## 3. ENFORCE BASIC SECURITY: PASSWORD, ENCRYPTION, AND REMOTE WIPE

Be sure to do the following:

- Require a strong password.
- Set up devices to automatically lock after a specified period of inactivity.
- Be able to remotely wipe devices after a certain number of failed login attempts, or if devices are reported lost.
- Enforce local data encryption.

Some organizations may want to consider more protection. But before you do that, ask yourself one question: can you do these things on your laptops? If you can't, you will need to make an honest assessment on how important it is initially?

Also, you may be worried that to get started on the items above you'll need a new solution. That isn't necessarily the case. If you have a BlackBerry Enterprise Server, then you are covered on that platform. And even now, if you have Exchange or Lotus Notes, you can enforce your PIN policy and remote wipe your iPhones, iPads, Androids and Windows Mobile devices.

We acknowledge that this isn't fail-safe. For instance, iPhones have a password vulnerability based on mounting the device to an Ubuntu machine. But, this approach is a responsible approach leveraging existing infrastructure for device and risk management today, especially if you believe, as discussed previously, that you really can't stop users today.

The biggest issue with this approach is that reporting is limited and not scalable. But this first step can dramatically improve your current posture on the uber-popular iPhone and Android devices while you are planning a more scalable and robust management and security solution (as described below).

## 4. MAKE BLUETOOTH HIDDEN OR NON-DISCOVERABLE

It seems to be the most used, but still highly infrequent, security risk. This is tricky in practice. Users will need to put it into discover mode to pair with their car or new headset, for instance, but your policy must require them to turn it back to non-discoverable when they're finished with that one-time action to be qualified to have the device for corporate use.

### 5. START PLANNING FOR A SINGLE CONSOLE, MULTI-PLATFORM MDM SOLUTION

Your BlackBerry Enterprise Server is probably well entrenched, both operationally and economically. But it is not multi-platform, and you will need to implement a multi-platform solution.

Here are four emerging best practices to consider that map to our economically frugal times:

1. The lines between laptops, tablets, and smartphones will continue to blur in both user functionality and IT operations. Your MDM platform should also be able to manage PC/Mac form factor and OS devices. This will cut down on infrastructure costs, improve operational efficiency, and create a single user view into devices and data for operations and security.
2. Be sure that your reporting and inventory tool consolidates both your existing BlackBerry solution and your multi-platform MDM platform. You will rely on your data and reports daily, and you should avoid any manual processes to access your business intelligence on mobile devices.
3. Consider web- or cloud-based MDM services. Why use a more expensive (when you add in full TCO) solution that is LAN-oriented to manage remote mobile devices? Manage the cloud from the cloud.
4. Go the agent route with caution. If you can meet your needs with server-side management controls, that will prove to be the better solution for the long haul, given the proliferation of hardware/OS/carrier combinations that an agent-based solution has to keep up with across the mobile landscape.

### 6. INCLUDE YOUR MOBILE DEVICE INVENTORY AND POLICY STATUS IN OPERATIONS REVIEWS

Report on and discuss your mobile device inventory and policy status in your IT operations reviews. Be sure to include personal devices. It's a good way to gain exposure to the benefits for your organization and future resource needs. Your inventory and reporting tool should make this simple.

The practices we've discussed above should meet most organizations' needs. For instance, the healthcare industry has some of the most stringent security and privacy regulations as dictated by the HIPAA Act and HITECH. But those regulations only require, in practice, encrypting your data and having the ability to destroy the data on a lost device. The practices we've already discussed cover that and more.

## Consider These Advances, Once You Have the Foundation in Place

Most organizations can benefit from the following practices, although they certainly are not required for an effective mobile IT operation in the near term.

### 7. ENABLE COST MANAGEMENT FOR NETWORK USAGE

Multi-national businesses need to be able to monitor and limit international data roaming, since those costs can quickly reach thousands of dollars per trip. Also, with US pricing plans introduced by AT&T® for iPhones and iPads, usage tracking and restriction will become a requirement for domestic connectivity. Verizon also has iPhone and Androids so, anything other than flat rate unlimited could lead to high costs.

### 8. MANAGE APPLICATION RESTRICTIONS AND YOUR OWN APP STORE™

Today, most handset vendors do a good job of limiting applications to certified and approved applications. Some would argue too good of a job restricting access to the phone by developers. That said, certain organizations or industries may have the need to restrict the type of application allowed on a corporate approved device. Most MDM solutions provide this functionality.

On a more proactive front, businesses can set up their own enterprise app stores to restrict the set and to ease the delivery of applications to your mobile devices. This is not a requirement, but certainly is something to explore after your foundation is in place.

### 9. PROVIDE A BACKUP & RECOVERY SERVICE

If you have a user segment that has critical and unique data, beyond email, you may want to consider using a backup and recovery solution. Now, that's not very critical for iPhone users, since iTunes has taken care of this already, or for BlackBerry users, but Android smartphones might require this additional functionality.

## If You Need a Fortress

Very few organizations should find themselves in this group currently (and for what looks like the foreseeable future). If you think you are, then you are probably involved in highly sensitive and classified information.

### 10. LIMIT DATA TRANSFERS, AND SEPARATE CORPORATE AND PERSONAL INFORMATION

Some businesses find it valuable to restrict downloading attachments or prevent the copying of data to removable media. Implementing these solutions is very difficult, and the data classification exercise is nearly intractable. An alternative is to create separate virtual containers for business and personal data and applications.

### 11. INSTALL FIREWALL, ANTI-VIRUS AND INTRUSION PREVENTION SOLUTIONS

There are effective applications in the market that apply these PC-like approaches to device security. Home Wi-Fi access does raise some concerns that devices are not always protected by carrier networks. But for the time being, mobile devices enjoy the same company as Macintosh and Linux platforms and have the benefit of much less complexity as the attack-prone Windows PCs. So these solutions are primarily targeted to highly sensitive environments where "good enough" just isn't.

## MaaS360 for Mobile Devices

MaaS360 for Mobile Devices helps IT administrators provision, manage, and secure today's expanding suite of mobile devices.

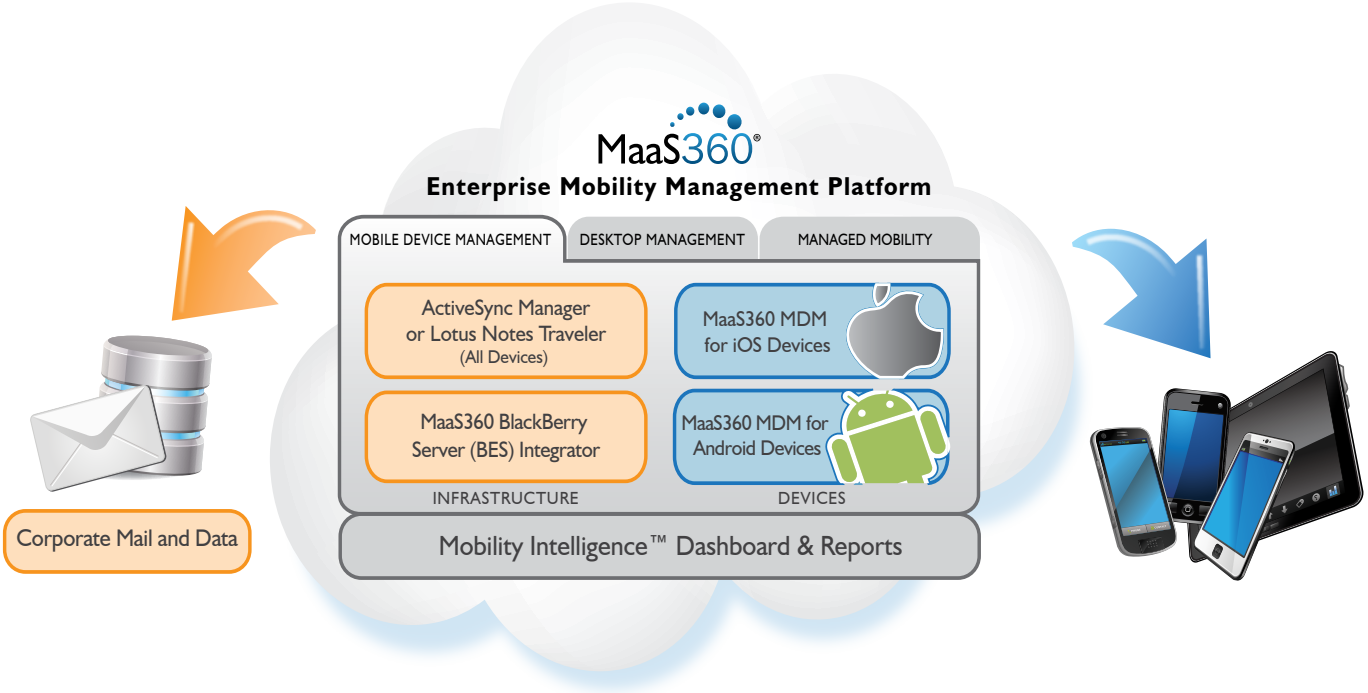
- MaaS360 supports all major smartphone and tablet platforms including iOS, Android, Windows Phone, BlackBerry, Symbian, Windows Mobile, and Palm WebOS.
- MaaS360 provides workflows to discover, enroll, manage, and report on personally owned devices as part of your mobile device operations.
- MaaS360 provides auto-quarantine and alerts for IT personnel to approve all new devices, and additionally provides for user self-enrollment into your mobile device management program.

MaaS360 by Fiberlink

# 11 Best Practices for MDM

## MaaS360 for Mobile Devices Product Line

MaaS360 offers the key components of Mobile Device Management (MDM) as a set of flexible entitlements providing comprehensive and flexible security and management for mobile devices.




## About MaaS360

MaaS360, the leader in mobile device management, is the creator and developer of cloud-based Mobility as a Service (MaaS) solutions. The company's MaaS360 platform enables IT to manage laptops, desktops and smartphones in one window, one system. The company's MaaS360 mobility infrastructure and subscription services have revolutionized how enterprises and business users share and secure information over the Internet.

The MaaS360 platform ensures reliable, secure and compliant mobile working for employees, while delivering unprecedented Mobility Intelligence™ to senior management and IT operations. MaaS360 is a recognized leader in mobile device management, helping both Global 2000 companies and smaller businesses cost-effectively support expanding mobile workforces and use mobile devices to remain competitive in today's economy. Additional information about MaaS360 is available at http://www.maas360.com.



For More Information
To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | Fax 215.664.1601 | sales@fiberlink.com

WP_201107_0001