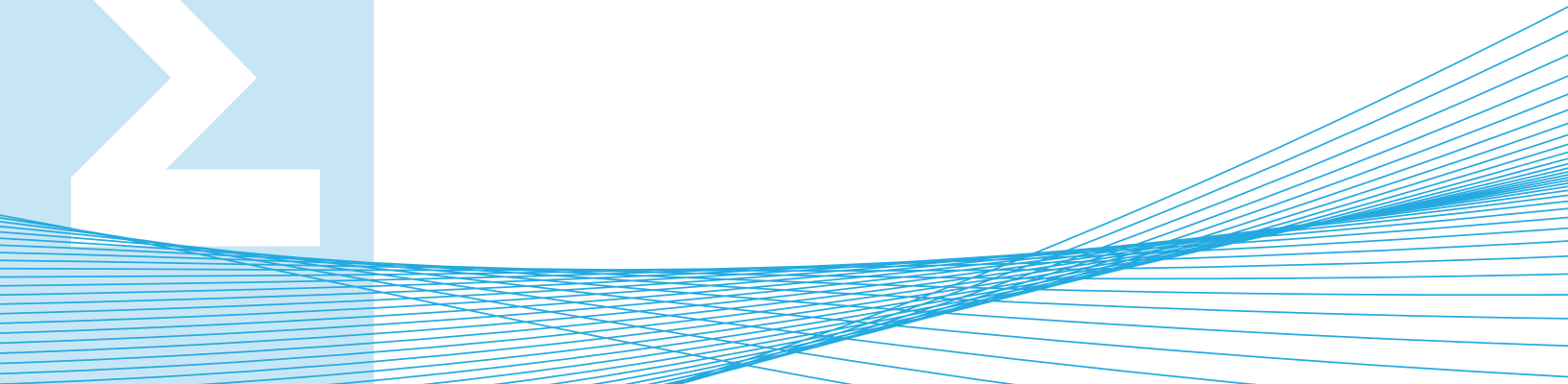
MDM

Mobile Device Management:

Your Guide to the Essentials and Beyond



Mobile Devices Are All Around You

More businesses than ever are confronting how to fully embrace mobile devices beyond their executive and sales teams. In a way, IT teams are being dragged into this. Many users have fully incorporated smartphones and tablets into their daily lives thanks to devices and operating systems from Apple and Google. They are choosing the personal user experience of Android and iPhone over the largely business-task-driven BlackBerry devices. They have also adopted application stores in their personal lives, blending activities like web browsing, games, and mobile payments with business uses such as corporate email.

So why is it taking so long for businesses to officially assimilate mobile devices into their organizations? It's usually because they want to put an IT strategy for management and operation in place first. We understand that IT would like to add a degree of rigor, but the solution doesn't have to be that difficult.

This guide describes twelve best practices for Mobile Device Management (MDM). The first eight principles are the essentials that every organization needs to adopt. The last four are advanced practices that will help take your organization to the next level.

The Essentials: Start with a Strong Foundation

Regardless of your business, industry or users, be sure to adopt the following practices:

1. Be Realistic with Your Policy
2. Gain Insight into Who's Mobile and What They're Doing
3. Cover the Basics: Passwords, Encryption, and Remote Wipe
4. It's as Easy as 1, 2, 3
5. Make it Simple to Get Up and Running
6. Let End Users Take Care of Device Management
7. Start Planning for Centralized Control
8. Spread the Word about Your Progress

Advanced Practices: Build Upon Your Foundation

Go a step further with advanced practices:

9. Get a Grip on Usage Costs
10. Automate Compliance Management
11. Manage Application Restrictions and Your Own Application Storefront
12. Provide a Backup & Recovery Service

1. Be Realistic with Your Policy

You need to:

1. Support multiple device platforms
2. Allow personal devices

Frankly, nearly all organizations are doing this now. They just don't know it. Chances are good that your business has a BlackBerry corporate standard, right? And that your business has at least one iPhone or iPad that syncs to your email infrastructure (most likely for the CEO or president) using Exchange ActiveSync® or Lotus Notes Traveler®.

If that's the case, you probably have a lot more personal iOS, Android and Windows Mobile devices inside your organization. After all, it's easy for any mobile device to integrate with mail infrastructure like Exchange using the Activesync functionality you turned on. Just Google *Setting up iPhone on Exchange* and see how your employees are doing it.

2. Gain Insight into Who's Mobile and What They're Doing

Making decisions and quantifying risks about mobile devices is hard without good data on the mobile devices in your environment. For instance, it's not uncommon for terminated employees to still be using corporate mobile devices—but you can't stop this unless you know about it.

With a lightweight reporting and inventory tool, you can keep tabs on how mobile devices are being used and by whom. Make sure the solution:

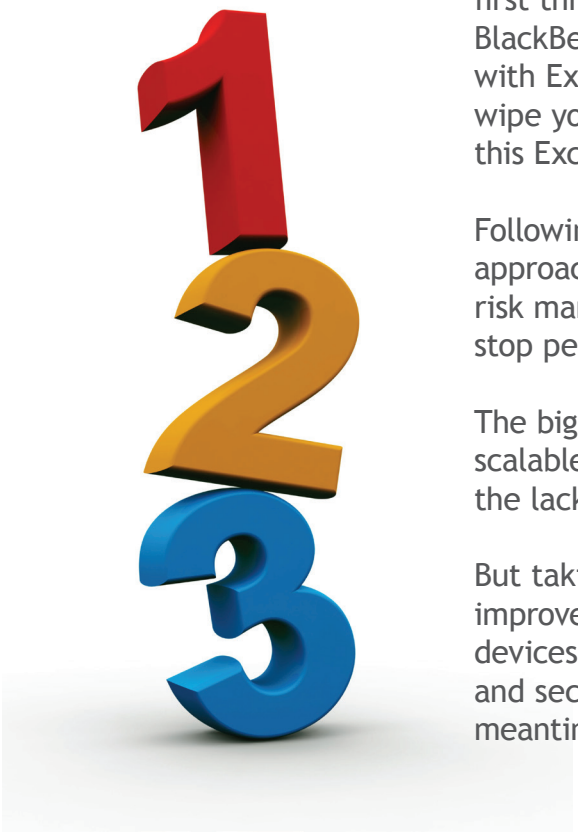
- Empowers the helpdesk to troubleshoot devices
- Is accessible outside of IT (for example, HR should have access during exit interviews to turn off devices for employees who are leaving the company)
- Includes strong application inventory and search capabilities

3. Cover the Basics: Passwords, Encryption, and Remote Wipe

Be sure to do the following:

- Require a strong password of at least four characters
- Set up devices to automatically lock after 5-15 minutes of inactivity
- Configure devices to automatically wipe after 10 failed login attempts or if they are reported lost
- Enable local encryption

Some organizations may want to consider more protection. But before you put yourself in that category, ask yourself one question: Do we enforce this level of security on our laptops?



4. It's as Easy as 1, 2, 3

You may be worried that you'll need a new solution to implement the first three best practices. That isn't necessarily the case. If you have a BlackBerry Enterprise Server, then you are covered on that platform. And with Exchange or Lotus Notes, you can enforce your PIN policy and remote wipe your iPhones, iPad®s, and Windows Mobile devices. (Android™ added this Exchange-based security control in version 2.2.)

Following the three principles we've already outlined is a responsible approach that takes advantage of existing infrastructure for device and risk management. And it's a smart one considering that you really can't stop people in your environment from using mobile devices.

The biggest issue with this approach is that reporting is limited and not scalable—you'll need to develop and run reports manually, and deal with the lack of a centralized view into all devices.

But taking the first step with reporting and inventorying can dramatically improve your current posture on the uber-popular iPhone and Android devices. Then you can plan a more scalable and robust management and security solution (as described in the next best practices). In the meantime, click here for our free ActiveSync reporting tool.

5. Make it Simple to Get Up and Running

Don't make IT responsible for reviewing each request for device and system access. Instead, empower users to enroll their own devices by visiting a single URL. Set up a default policy that approves the users' devices and pushes down their e-mail and corporate Wi-Fi profiles.

In addition to making the process easy for end users, simplify things for IT. For example, your policy could specify that any Android device with OS 2.2.4 or above is automatically granted access to corporate systems, while any Android device on an earlier OS version is automatically blocked.

6. Let End Users Take Care of Device Management

With employees relying on mobile devices to get their jobs done, you don't want basic device management issues to get in the way of productivity. You also don't want users calling the helpdesk with issues they can resolve themselves. Empower end users with a self-service portal that allows them to:

- Enroll their devices
- Lock and wipe their devices if think they've been stolen
- Reset their own passcodes
- Locate their lost devices

7. Start Planning for Centralized Control

Your BlackBerry Enterprise Server is probably well entrenched, both operationally and economically. But it is not multi-platform, and a multi-platform solution is needed to support the variety of devices in your environment.

Consider these four emerging—and economically sound—best practices:

1. Adopt an MDM platform that can also manage PCs and Macs as well as mobile devices. The lines between laptops, tablets, and smartphones will continue to blur in both user functionality and IT operations. A versatile MDM solution 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 your reporting and inventory tool consolidates both your existing BlackBerry and your multi-platform MDM solutions. You'll rely on your data and reports daily, and you'll want to avoid any manual processes to access your business intelligence on mobile devices.

3. Take a look at cloud-based MDM services. When you account for full Total Cost of Ownership (TCO), a LAN-oriented management solution can be costly. Why use a more expensive—and wired—solution to manage remote mobile devices?

4. Go the agent route with caution. If you can meet your needs with server-side management controls, all the better. You'll find this is the better solution for the long haul, given the proliferation of hardware/OS/carrier combinations. If you opt for an agent-based solution, you'll spend lots of time installing and maintaining it across the mobile landscape.

8. Spread the Word about Your Progress

Report on and discuss your mobile device inventory and policy status—including personal devices—in your IT operations reviews. It's a good way to broaden the discussion beyond those responsible for managing devices in your environment. It's also an opportunity to raise the visibility of the benefits for your organization, as well as for future resource requirements such as needed involvement from those responsible for security and other areas of IT. Your inventory and reporting tool should make it simple to produce the reports to start conversations in these meetings.

Designed for Any Environment

The practices we've discussed so far should meet most organizations' needs. In fact, they satisfy the most stringent security and privacy regulations, such as those dictated by the HIPAA, FINRA, and PCI DSS. These regulations only require, in practice, that organizations encrypt their data and are able to destroy data on a lost device. The essential practices cover that and more.

Build Upon Your Foundation with Advanced Practices

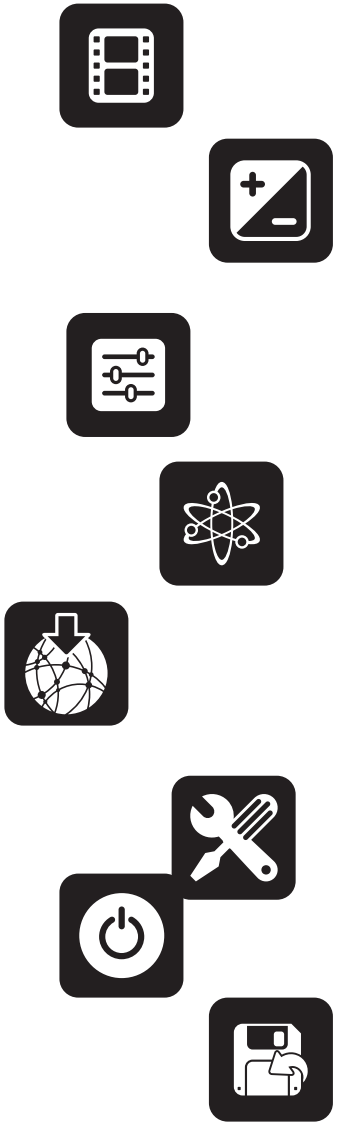
With the essentials in place, your organization is primed for an effective mobile IT operation in the near term. Now you need to determine whether or not your organization needs to go a step further with advanced practices.

9. Get a Grip on Usage Costs

You need to be able to track, monitor, and restrict network usage. After all, the costs for international data roaming can reach thousands of dollars per trip. Even domestic usage can quickly add up, especially considering the pricing plans introduced by AT&T for iPhones and iPads in 2010.

10. Automate Compliance Management

IT needs a way to automatically detect devices out of compliance with policy—and automatically respond. For example, your policy may specify that jailbroken or rooted devices are not allowed in the corporate environment and if one is detected, you will immediately revoke access to corporate systems. Ideally, the detection and revocation should happen automatically. At the same time, you want to automatically notify the user of the action being taken and what's needed to come into compliance and regain access to corporate resources. Once the device is in compliance, access should be automatically reinstated.



11. Manage Application Restrictions and Your Own Application Storefront

Today, most smartphone and tablet vendors do a good job of limiting usage to certified and approved applications. Some would argue they do too good of a job restricting access. Other vendors maintain a very open policy for creating applications, with no formal process for certifying apps. That said, certain organizations or industries may need to restrict the type of application allowed on a corporate-approved device.

If you want to be proactive about it, set up your own enterprise application storefront. This allows you to present a list of approved applications and ease their delivery to mobile devices. Plus, your users will know where to go for these applications and for updates. Some MDM-solution providers can even help you deliver documents such as PDFs to devices.

12. Provide a Backup & Recovery Service

If any of your users work with critical and unique data beyond email, you may want to consider using a backup and recovery solution. Those using an iPhone or an iPad can rely on iTunes to take care of this. Just make sure your policies are set to force an encrypted backup. For those not using iTunes for backup, you'll probably need to address specific use cases.

Mobility Can't Wait

Mobile devices in the corporate environment are here to stay. Your organization can either drag its feet while renegade devices access corporate resources, or employ best practices that will satisfy end users and IT. Whether you need to cover the basics or need to step up mobile device management to a higher level, this guide will start you on your way.

Interested in a free evaluation of a leading mobile device management solution? Click here to take advantage of a quick and easy trial.

Or, check out these resources to learn more about mobile device management software from Fiberlink.

- www.maas360.com
- Mobile Device Management
- MaaSters Center


MaaS360®
by Fiberlink, an IBM company