



# Managing Mobile Devices in a Device Agnostic World

WHITE PAPER



**Contents:**

Mobile Device Management 2.0 – or – The True Meaning of IT Consumerization ..... 2

Building an MDM Policy Framework that Makes Business Sense..... 3

    Policies that Help Make Business Operations More Efficient.....3

    Policies that Make Workers More Productive.....4

    Policies that Keep Company Information Assets Secure .....4

    Policies that Control Mobile IT Costs.....5

Implementing Policy: The Importance of an MDM Platform..... 7

Service Cycle Approach to Device Management ..... 8

Preparing for a New Age of Mobile Device Management ..... 9

    Notes .....10

# Mobile Device Management 2.0 – or – The True Meaning of IT Consumerization

Mobile Device Management (MDM) used to mean something.

Corporate IT reviewed and selected mobile devices for employees. Companies decided who should get devices, and how they would be used. IT managers configured the devices, issued them to employees, tracked them, and decommissioned them.

MDM was simpler in those days. It seems like just yesterday. In fact, for many companies it was just yesterday. But things are changing fast in business mobility, and one of the greatest areas of change is how workers go mobile.

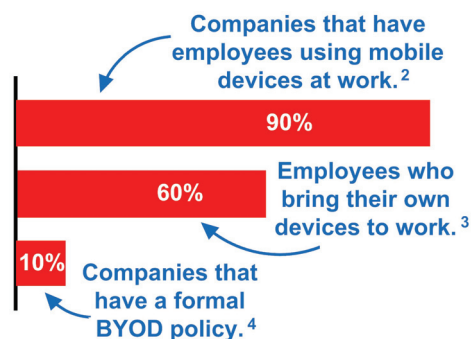
As soon as people figured out how to do email on their iPhones and Androids, personally owned devices started popping up all over the work place. Before long employees were pushing for other kinds of business applications, downloading apps from app stores, and buying out-of-the-box business solutions. Then tablets started showing up. It's no wonder the IT guy at the company BlackBerry dispensary started to feel left out.

This “bring your own device” (BYOD) trend can have big advantages. Some companies are experimenting with providing employees a budget and allowing them to buy the devices and service plans of their choice. Doing this has saved them over 20% in mobility costs.<sup>1</sup>

However BYOD presents a big management challenge for many companies. It changes who within an organization gets access to mobility and how they get it. It also affects the way a business operates, and it has implications that go way beyond the lonely guys in the IT department. BYOD raises new questions, like:

- How do you enforce security in a BYOD environment?
- How do you know who's mobile and what they are doing on their mobile devices?
- Is the company liable for what employees do if they do it on personal devices they use for work?
- Is there a practical limit to how many devices a company can support, and what does it cost to manage a great diversity of devices?
- Can one device actually support both personal and corporate needs?

These are fundamentally significant questions. They are also questions that have different answers for different organizations. Finding the answers and acting on them depends on two pieces of the mobility management equation: device management policy, and the technology you use to fulfill and enforce a policy. Let's first look at device management policy.



# Building an MDM Policy Framework that Makes Business Sense

You don't have to look far to find plenty of good mobility management guidance (see *The Enterprise Mobility Policy Guidebook* published in May, 2011 by the Enterprise Mobility Foundation). This guidance typically suggests policies that support essential mobility management tasks like asset inventory and management, expense management, security, operations management, and tech support.

Rather than replicate that device management advice here, we will take more of a business value approach to MDM policy development.

The value of a mobile device management framework is directly related to how effectively it serves your business mobility objectives. So what are your business mobility objectives? Most organizations would agree that by mobilizing certain business operations, they hope to realize the following benefits:

- Make business operations more efficient
- Make workers more productive
- Keep company information assets secure
- Control costs of mobile IT

Let's begin by breaking down MDM policies according to the business objectives they are intended to serve. The challenge in creating an MDM strategy for any organization is balancing operational benefits with risks and cost. Some policy objectives may conflict with others. However to have a successful mobility strategy, every organization needs to find the right balance.

## ***Policies that Help Make Business Operations More Efficient***

One of the greatest benefits of mobility is that it enables real-time access to people and information. This accelerates business activity, improves the quality and accuracy of decision making, and enables a more collaborative business process. Collaborative access to information and people is only possible if the business environment is "transparent" to everyone in it.

Note that transparency does not mean everyone has equal access to all information and all other people. It means there are not arbitrary technical barriers that prevent this kind of access. Collaboration and access need to be governed by business process needs, workflows, and security. They should not be arbitrarily restricted by technology induced business process silos.

What kind of MDM policies ensure mobile transparency that is manageable and flexible enough to change with business over time?

Policy Objectives	Policy Rules
<input type="checkbox"/> <b>Policies that ensure the greatest acceptance, and therefore penetration, of mobility use in the enterprise.</b>	Whether mobile devices used at work are employee or company owned, policies should permit a wide choice in device types and carriers. Tips: <ul style="list-style-type: none"> <li>• The more prescriptive you make your list of acceptable devices, the more resources you will use managing the list.</li> <li>• Some job roles and work functions will require different device types than others.</li> <li>• Support dual-use (personal and work) devices. This BYOD approach has economic and user productivity advantages.</li> </ul>
<input type="checkbox"/> <b>Policies that ensure the portability of data and applications.</b>	Require that internally developed mobile applications, including hybrid web applications, be built on a common mobile enterprise application platform (MEAP). This simplifies porting applications to different devices, and it ensures data compatibility between applications and devices, thus

	<p>avoiding isolated “silos” of mobile business activity. Tip:</p> <ul style="list-style-type: none"> <li>• Mandate that third party contractors who develop mobile applications for you leverage your MEAP platform.</li> </ul>
<p>❑ <b>Policies should limit the use of third party mobile applications that rely on proprietary data sets incompatible with existing corporate databases.</b></p>	<p>Mobile operations often begin as extensions of conventional operations. Rules should encourage the extension of existing data to mobile devices rather than adopting new applications with new data form factors to fulfill mobility needs. This ensures data compatibility between mobile and conventional operations. Tips:</p> <ul style="list-style-type: none"> <li>• Employees can be the best source of information about new third party applications. Establish a process whereby employees submit “free” or commercial third party mobile apps for business use review.</li> <li>• Prohibit downloads of unapproved business apps.</li> </ul>

***Policies that Make Workers More Productive***

More efficient business operations go hand in hand with more productive workers. Recent studies continue to show significant increases in productivity of mobile workers over their less mobile colleagues.<sup>5</sup> It is not difficult to see why. Workers become more productive when they use their time more effectively. Mobility allows them to communicate and find information more quickly, answer email and perform workflow tasks on the run, and generally accomplish more in smaller time bites. People know this, which is a major reason why up to now the driving force behind enterprise mobility has been the employees themselves.

What MDM policies maximize worker productivity?

Policy Objectives	Policy Rules
<p>❑ <b>Policies that ensure workers use mobility to their greatest professional advantage.</b></p>	<p>Workers are inventive when it comes to finding better ways to do their work. MDM rules can encourage productive use of business mobility in these ways:</p> <ul style="list-style-type: none"> <li>• Rules allowing employees to choose the devices they want, or to bring their own devices to work, result in higher levels of employee adoption and use.</li> <li>• Rules that enable employees to participate in mobile application acquisition and development result in higher levels of employee engagement.</li> <li>• Initiatives to mobilize business workflows that enable “any time” work makes workers more productive.</li> </ul>

Note that many device management policies relate to managing the applications users run on their devices. For more information about mobile application management, see the Sybase paper “Mobile Applications May Be Running the Business, but Who’s Running the Apps?”

***Policies that Keep Company Information Assets Secure***

Some IT managers worry that policies encouraging wide use of mobility in the enterprise are a threat to information security. They have plenty of reason for concern. Data shows that 36% of consumers have either lost a phone or had one stolen.<sup>6</sup> Other research shows companies continue to be lax in their implementation of mobile security, or where they have policies, employees are largely unaware of them.<sup>7</sup>

One approach to mobile security is to limit risk by limiting mobility in the company. From a security perspective, that works. However this strategy also puts the company at a massive competitive disadvantage, and in the long run could actually drive the company out of business. Companies that turn

their backs on mobility are not realizing the operational efficiencies and worker productivity gains achieved by more mobile organizations (including their competition).

A better approach is to effectively implement a mobile security policy. What kinds of policies will keep corporate information assets secure without stifling capabilities that make workers more productive and business operations more efficient?

Policy Objectives	Policy Rules
<input type="checkbox"/> <b>Policies that protect data.</b>	<ul style="list-style-type: none"> <li>• Require encryption of all business related data (both transmitted and stored).</li> <li>• Implement an MDM platform that enables you to remotely lock and wipe devices, and remotely monitor data activity for purposes of breach detection.</li> <li>• In dual-use devices, use application and device management to segregate business and personal use functions on the devices.</li> </ul>
<input type="checkbox"/> <b>Policies that manage access.</b>	<ul style="list-style-type: none"> <li>• Require password authentication before users can launch business applications.</li> <li>• Use mobile application functionality to manage data access, and use group policies to manage which devices and job roles are able to run which applications.</li> </ul>
<input type="checkbox"/> <b>Policies that sustain a culture of security best practices in a business ecosystem.</b>	<ul style="list-style-type: none"> <li>• Develop a life cycle or service cycle strategy that includes a process to enable a device for business use.</li> <li>• The “enablement” process should include standard steps like encrypting data, setting a password, and installing anti-virus and anti-malware software.</li> <li>• Require immediate reporting of a lost or stolen device.</li> <li>• Promote safe mobility practices.</li> </ul>

The key to implementing and enforcing security policies is an enterprise grade MDM platform. We’ll talk more about MDM platform capabilities below. For a more detailed discussion of developing and implementing a mobile security strategy, see the Sybase paper “Mobility Advantage: Why Secure Your Mobile Devices?”

### ***Policies that Control Mobile IT Costs***

When people think of the costs of mobility, they often think of direct costs of devices, service plans, data plans, and exceptional charges that traveling workers might incur.

Beyond these direct costs, there are many indirect, or let us say “less visible,” costs associated with business mobility. These less visible costs can be far greater than the direct costs. Less visible mobility costs include:

- **Costs associated with the mobility infrastructure** – These are costs of systems needed to manage devices and security, and provide back-end support for proprietary mobile business applications and data access.
- **Mobile application development and management** – Costs associated with building, acquiring, customizing, distributing, and maintaining mobile applications can be significant. If your company has BYOD device policies such that you are supporting multiple device types, this can have a huge multiplier effect on the costs of application development and support. As companies become more mobile over time, they will be supporting ever larger numbers of mobile applications. Costs associated with mobile

application management (MAM) can vary tremendously depending on how you implement a MAM strategy.

One way to limit mobility costs is to standardize around one device type and a standard rate plan. This approach limits the benefits of mobility in these ways:

- Employees are less likely to use the company issued device for anything more than bare necessities;
- In this world of rapidly changing mobile technology, companies will be stuck with old technology and will find themselves at a disadvantage compared to their more mobile competitors.

The reality is that there are more mobile devices coming to market, more ways to adapt them to different aspects of the business process, and more companies are shifting to BYOD policies for knowledge workers. As companies develop policies to control mobility costs, they will need to support a variety of devices. What kinds of policies work to control costs in such a dynamic mobility environment?

Policy Objectives	Policy Rules
<input type="checkbox"/> <b>Policies that regulate direct costs.</b>	<ul style="list-style-type: none"> <li>• Establish an approved list of carriers</li> <li>• Define permitted rate plans that are appropriate for different job functions (some employees may have larger data requirements than others)</li> <li>• Define rules for plans and plan adjustments that cover the needs of international travelers; define rules of usage when traveling internationally.</li> <li>• Define rules around allowances and expense reimbursements.</li> </ul>
<input type="checkbox"/> <b>Policies that reduce less visible costs.</b>	<ul style="list-style-type: none"> <li>• Adopt a device and application management platform with a common set of management tools for all applications and devices. Investing in an enterprise grade platform vastly reduces long term costs of managing a dynamic device and application portfolio.</li> <li>• Develop a life cycle or service cycle approach to device management that includes a process to enable a device for business use.</li> <li>• Adopt an application development platform standard that enables all business applications to share common back-end data.</li> <li>• Use a hybrid web-app strategy to reduce the cost of developing and maintaining custom business applications.</li> </ul>

A large part of developing mobility management policies suitable for any operation is balancing potential policy conflicts. For instance a highly restrictive mobile device policy may be easier to secure, but it will cost in worker productivity. In fact there is no one right set of policies. Different organizations with different security and operational constraints will have vastly different mobility policies.

The principle objective of mobility policies should be to establish mobility as a secure, cost effective business enabler in an organization. However developing mobility policies is only one part of the equation. The other is implementing and enforcing those policies.

The heart of any MDM policy enforcement is a mobile device management platform. What exactly is that?

# Implementing Policy: The Importance of an MDM Platform

Whether you are relying on a service provider to manage your corporate mobility, or you are building in-house IT infrastructure to do this, effective mobile management depends on a mobility management platform. Why?

A platform provides essential controls mobility managers need to enforce policy. It is the combination of mobility policy and a robust device management platform that enables an organization to build a mobile business strategy.

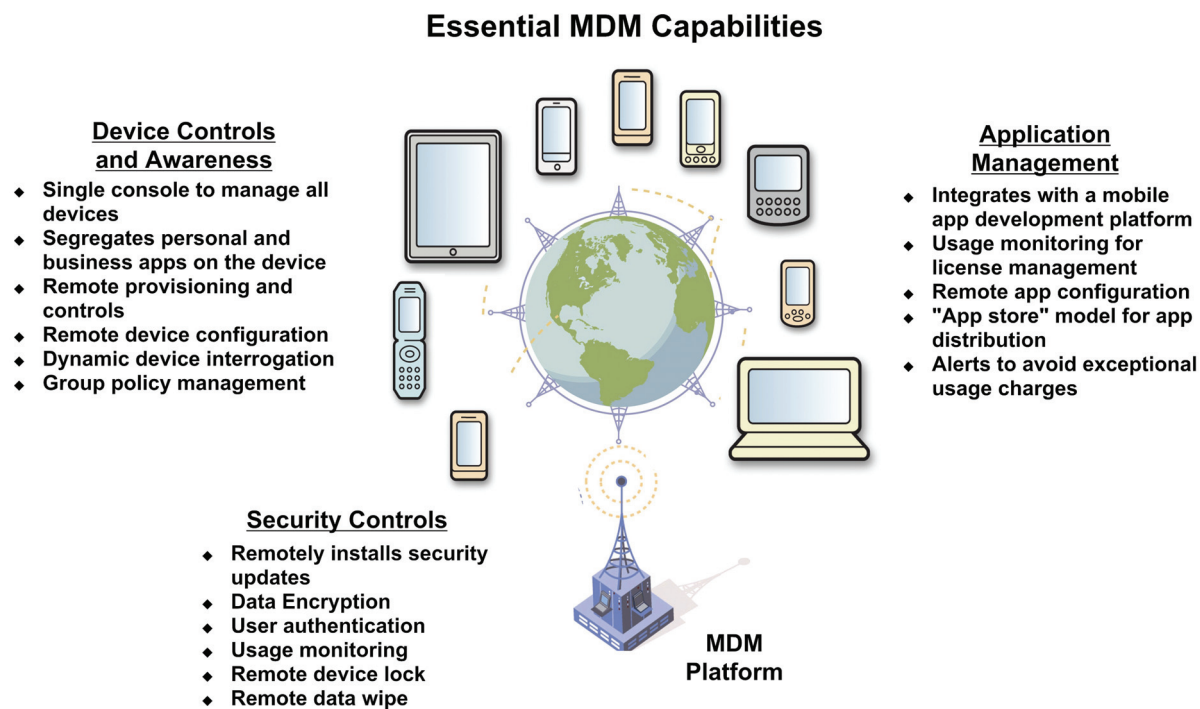
The illustration on this page shows essential capabilities of an enterprise grade MDM platform. These include:

**Compatibility with the widest selection of device types and mobile operating systems:** This is critical in that it enables an organization to support the most up-to-date mobile devices. It also gives an organization greater flexibility when creating a BYOD policy for employees.

**Remote provisioning and control:** This enables managers to remotely configure devices, and it provides remote and automated security controls used to secure data on lost, stolen, or decommissioned devices. It also enables companies to push applications to remote devices over the phone service network.

**Dynamic device interrogation:** This gives real-time visibility into mobile systems, providing information like device types, version of operating system a device is running, software licenses in use, and other essential information about mobile systems.

**Group policy management:** An MDM platform should support remote device control based on group policies. For instance, you might want to distribute three different versions of an application, one for all iPad users, one for all Android phone users, and one for all BlackBerry users. Or, you might want to distribute a particular application or software update just to account managers.



Using these MDM platform capabilities to enforce mobility policies enables organizations to manage mobility in a strategic way, much like they already manage other IT assets. Let's see how policy and platform combine to produce an operational mobility management strategy.

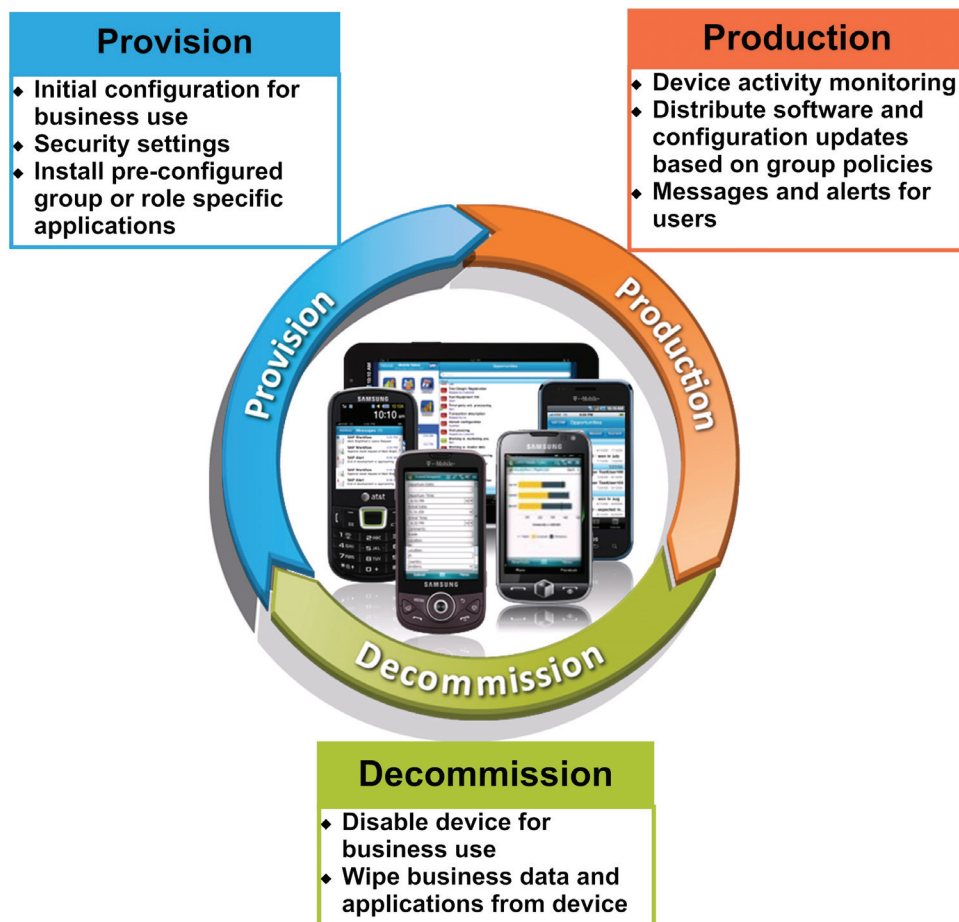
# Service Cycle Approach to Device Management

One approach to mobility management is to enforce policies in the context of a device's life cycle or service cycle. A service cycle is the period of time when a device is in active service with the company.

In a service cycle approach to device management, the service cycle breaks down into three phases:

- **Provisioning Phase** – This is the process of preparing a device for use in the business environment by installing essential security and business applications, segregating business and personal use functions if this is an employee owned device, and performing initial security and user configuration.
- **Production Phase** – During the production phase, a device is being actively used for work purposes. Applications will be installed or updated during this time, and companies will remotely monitor device activity to detect security breaches or violations of use policies. In addition to normal flows of business data to and from devices, workers may receive operational messages and alerts. For instance a user might receive notification of data usage that exceeds the data plan for that device. IT managers will use group policies to automate some device management tasks.
- **Decommissioning Phase** – When a device comes to the end of its service life (either naturally, or by being lost or stolen), it will go through a decommissioning process that removes all business applications and data. A device management platform enables IT management to perform decommissioning functions over-the-air when they do not have physical possession of a device.

With a device management platform in place and a comprehensive set of mobility policies, it becomes possible to build and enforce a service cycle management strategy that looks something like this:



# Preparing for a New Age of Mobile Device Management

For many organizations, mobility today means managing and enabling workers who use smartphones at work. However mobile technology is moving very quickly.

Industry analysts are forecasting that by 2013, 80% of business will be supporting workforces that use tablets.<sup>8</sup> These workers will not be throwing away their smartphones. This means that in the near future, typical knowledge workers will be equipped with two mobile devices, each with its own device and application management requirements. Many organizations already support multiple mobile devices for their workers.

As mobile technology evolves and companies mobilize more of their operations, the greatest business advantage will go to organizations that most effectively manage their business mobility. This means:

- Establishing mobility policies that make business operations more efficient, make workers more productive, keep company information assets secure, and effectively control mobile IT costs;
- Implementing a device and application management platform that is capable of managing and enforcing mobility policies for all devices in the organization.

Companies that have the best mobility implementations will be the ones that win in a world of real time business engagement. For more information about developing and managing mobile applications that are core to your business operations, click [here](#), or contact a Sybase or SAP representative.

## Notes

1. "2011 Winner profile: Foley and Lardner." *CIO Magazine*, Spring 2011.
2. "The Enterprise Mobility Policy Guidebook." *Enterprise Mobility Foundation*, May 2011.
3. Reardon, Marguerite. "Motorola turns up the heat on RIM." *CNET News*, June 9, 2011.
4. Herrema, John. "Personal Mobile Devices in the Enterprise: What IT Needs to Know." *Digital Discourse*, May 17, 2011.
5. "Research Reveals the Business Value of Managed Content—30 Percent Productivity Gains, 25 Percent in Efficiency Improvements." *PR Newswire*, March 24, 2011; *Cognizant*, "Enterprise Mobile Apps: How Role-Based Apps Will Drive Productivity and Transformation in Manufacturing Companies." July, 2011.
6. Maurer, Allan. "More than a third of consumers have had cell phones lost or stolen." *TechJournal South*, February 8th, 2011.
7. Moscaritolo, Angela. "Risky mobile behaviors routine in business." *SC Magazine*, May 25, 2011
8. Gartner. "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond." *Gartner Newsroom*, November 30, 2010

SYBASE, INC.  
WORLDWIDE HEADQUARTERS  
ONE SYBASE DRIVE  
DUBLIN, CA 94568-7902 USA  
Tel: 1 800 8 SYBASE

[www.sybase.com](http://www.sybase.com)

Copyright © 2011 Sybase, Inc. All rights reserved. Unpublished rights reserved under U.S. copyright laws. Sybase, and the Sybase logo are trademarks of Sybase, Inc. or its subsidiaries. ® indicates registration in the United States. SAP and the SAP logo are the trademarks or registered trademarks of SAP AG in Germany and in several other countries. All other trademarks are the property of their respective owners. 05/11.

iPhone and iPad are registered trademarks of Apple, Inc.

BlackBerry®, RIM®, Research in Motion®, SureType®, SurePress®, BBM® and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license from Research In Motion Limited.

