



Mobile Management Checklist: 6 Essential Steps

According to IDC, over 82 million converged mobile devices will be shipped by 2011. As more and more businesses invest in workforce mobility, IT departments will be required to assert tighter control over these devices. In fact, a well-thought-out mobile device management strategy is a key ingredient for any successful deployment. In this Expert E-Guide, we arm those responsible for managing smart phones and PDAs with strategies that can and should be applied now to reduce risk, contain cost, and increase productivity.

Sponsored By:



Mobile Management Checklist: 6 Essential Steps

Table of Contents:

[Mobile device management checklist](#)

[Making mobile device management fit](#)

[Managing mobile device diversity](#)

[Resources from Sybase iAnywhere](#)

About the author: *Lisa Phifer is vice president of Core Competence Inc., a consulting firm specializing in network security and management technology. Phifer has been involved in the design, implementation, and evaluation of data communications, internetworking, security, and network management products for nearly 20 years. She teaches about wireless LANs and virtual private networking at industry conferences and has written extensively about network infrastructure and security technologies for numerous publications. She is also a site expert to SearchMobileComputing.com and SearchNetworking.com.*

Mobile device management checklist

According to Forrester, employee handheld use expanded at 69% of North American businesses last year, but most still lack a cohesive plan to handle this fast-growing tidal wave. Ideally, IT should be managing those new smartphones and PDAs throughout their entire lifecycle, from activation to retirement. In this checklist, we highlight business needs that you should consider when developing your own mobile device management strategy.

Out of sight, out of mind

For the past decade, IT departments turned a blind eye to mobile handhelds, believing that cell phones were too limited and PDAs saw too little use to warrant attention. But today's increasingly powerful converged mobile devices have blown past both barriers, leaving IT in the hot seat. After all, you cannot secure what you don't manage, and you cannot manage what you don't see.

Mobile device management (MDM) can help your business plug this gaping hole by enabling remote visibility and control over smartphones and other handheld devices carried by your workforce. But MDM can also be a frustratingly vague term, applied to a diverse collection of products. The first step is to define precisely what you want MDM to do for your mobile workforce. The following checklist can help you identify your needs and common MDM capabilities that could address them.

Mobile asset inventory

Clearly, your MDM must maintain a list of devices to be managed—that is, your mobile asset inventory. But what should your inventory include, and how will it be maintained?

- **Device inventory:** What physical details do you need to track? Beyond the basics (device ID, hardware model, firmware version), an MDM can help you record and report on related assets like wireless adapters and removable memory.
- **Inventory classification:** How do you want to group those mobile devices? For example, an MDM might auto-classify your devices by mobile OS/version or state (e.g., unknown, authorized, provisioned, decommissioned).
- **Inventory maintenance:** How do you want to update your inventory to reflect adds, changes and deletes? An MDM might be used to periodically poll devices, check for changes at network connect, or carry out admin-initiated audits.
- **Physical tracking:** Do you need to know not just who carries each handheld but precisely where that device is located? With many smartphones now supporting GPS, location-based MDM features become feasible.
- **Database integration:** Do you already have inventory systems that manage other assets (e.g., desktops, phones)? If so, you may want to integrate managed mobile device records into a common database using inventory exports or reports.

Mobile device provisioning

Managing a device through its lifecycle begins with activation and provisioning. How will each new device become an authorized, capable member of your handheld fleet?

- **Supported platforms:** Device management depends on characteristics like operating system and vendor/model/version. What platforms (e.g., Windows Mobile, Symbian, BlackBerry) and minimum models/versions (e.g., Symbian 9+ on Series 60) must you support? Target a few devices that satisfy your needs, while making device-independent choices wherever possible and practical.
- **Device registration:** How will you enroll mobiles to be managed? MDMs can help administrators register company handhelds (e.g., directory add) or let users register their own devices (e.g., enrollment portals), or some combination thereof.
- **Agent activation:** How will the MDM agent get installed on each new device? Alternatives include manual IT install, desktop sync, mail gateway sync, and over-the-air installation (user visits URL from email or SMS).
- **Device configuration:** How will you override factory/carrier defaults? For example, you might want to require passwords, add registry keys, or rewrite menus to eliminate non-business applications. MDMs can apply your "standard config" to each device after initial activation or hard reset.

Mobile software distribution

Many MDMs go beyond device inventory and configuration, providing tools that deliver and update mobile applications. This may not be Job 1, but it should be a close second.

- **Software packages:** How will you bundle related applications for purposes of configuration and delivery? MDMs can help you define and deploy those packages, helping to resolve platform, memory, and application dependencies.
- **Package distribution:** Do you want software to be pushed to devices (on schedule) or pulled by periodic device polls? Push can propagate updates faster but requires more frequent communication that drains handheld battery life.
- **Mobile optimizations:** Must your strategy accommodate unreliable or limited WANs? Some MDMs offer compression, incremental updates, and bandwidth management (attempting or resuming installation only over fast, low-cost links).
- **Change control:** How often will your mobile applications need patching or update? Define how deployed packages will be maintained so that changes are applied without resulting in user pain or weeks of effort to fix failed updates.

Mobile security management

On handhelds, device and security management tend to converge. Many MDMs offer basic security features that are missing from mobile OSs or related to device tasks.

- **User authentication:** How will you authenticate users before granting access to mobile devices? Some MDMs can be integrated with enterprise directories while addressing mobile needs like network-disconnected authentication.
- **Password policy enforcement:** How many login attempts will you allow before requiring reset? Can emergency calls bypass authentication? Many MDM agents can enforce these and other password policies that go beyond OS-provided PINs.
- **Remote device wipe:** Do you need the ability to wipe clean a remote mobile device? For example, an MDM can often delete data or hard-reset a lost smartphone on next server connect or upon receipt of an SMS "kill pill."
- **White/black lists:** An MDM involved in software management may require certain business applications and ban other applications. Similarly, an MDM that controls device settings can help you disable risky interfaces and wireless options.
- **Secure communication:** How will sensitive MDM traffic (e.g., configuration changes, software packages) be protected? Some MDMs provide their own secure channels rather than relying on OS or third-party protocols.

Mobile data protection

Data just might be the most sensitive corporate asset on any mobile handheld. MDMs can help you preserve and protect that mobile data.

- **Data encryption:** Do you want to enforce policies that prevent unauthorized access to data stored on mobile devices? A few MDMs provide this capability; others can enforce your policies by installing or activating third-party encryption.
- **Backup/restore:** How will you prevent data loss when a mobile is damaged or stolen? Most MDMs support scheduled over-the-air backup from remote handhelds to a central archive and restoration by authorized users or admins.
- **Data tracking:** Do you need to maintain an audit trail of corporate data copied to and from mobile devices? Some MDMs can control and report on sensitive files transferred during over-the-air synchronization or onto removable media.

Monitoring and help desk support

Mobile device total cost of ownership can far exceed hardware/software purchase. Over time, MDM should pay for itself by reducing maintenance and support costs. How?

- **Self-help:** Can some admin tasks be cost-effectively shifted away from IT? Some MDMs offer self-help portals for user-initiated device enrollment, password reset or recovery, optional package download, and data restoration from backup.
- **Diagnostics:** When problems arise, what will your help desk need to see? MDMs can play a big role by providing not just intended settings but real-time status and health information (e.g., memory, battery, network connectivity).
- **Remote control:** When remote users need assistance, what can your help desk really do? Many MDMs include remote-control features (e.g., screen sharing) that let support staff interact with an off-site handheld in real time.
- **Audit and compliance:** Do you need to prove that mobile devices comply with your stated policies and/or industry privacy regulations? MDMs can help you automate remote assessment, remediation, and compliance reporting.
- **Activity reports:** How much insight will you need into mobile user activities, including interaction with business servers and networks? Most MDMs provide historical reports – but look closely to see whether they capture what you need to know.

Conclusion

Your company probably does not need everything on this checklist, and any single MDM product is unlikely to cover all of these bases. Instead, treat this checklist as though it were a menu, introducing you to a foreign cuisine. Some considerations are simply variations on traditional desktop management needs, while others may be new and unfamiliar. Trial a few MDMs to gain field experience with mobile user and device requirements before settling on a management strategy for your mobile workforce.

Making mobile device management fit

For many enterprises, mobile device management (MDM) is an afterthought—a band-aid to mend the operational and security gaps created by workforce mobility. Loosely coupled systems can address near-term challenges, but long-term success will require some degree of integration between MDM and the rest of your IT infrastructure and processes. Here, we consider several “touch points” where MDM must (eventually) dovetail with past and future IT investments.

On edge: Joining the corporate network

Integration with your corporate network—usually at the perimeter—is required for nearly all mobility initiatives. Most MDM servers are deployed in the network’s demilitarized zone (DMZ). Some MDMs can use a proxy server that sits in the DMZ, interacting with a main server inside the trusted network, providing an added layer of defense.

In either case, you must permit selected network protocols and ports between the MDM server/proxy and mobile devices, directly or through your wireless carrier’s gateway. In most cases, you will also need to allow narrow communication between the MDM and other trusted servers (e.g., email, directory). Typically, this integration requires firewall rule changes, but it can also have an impact on your threat management policies—for example, if your firewall scans for viruses, will it do so before/after the MDM server?

Over the air: WLAN infrastructure

Many mobile devices spend their lives interacting with the corporate network from afar, but some devices—particularly those with Wi-Fi interfaces—can also be local. In this case, your MDM may need to interface with your wireless LAN infrastructure.

Your MDM may supply its device inventory database to your WLAN switch or wireless IPS for access control or intrusion detection. In return, your WLAN may supply your MDM with valuable insight into connection status and historical activity. Today, these systems tend to interact through file import/export and alerts, but converged devices with multiple wireless interfaces will lead to tighter integration.

Who goes there? Authentication and identity

MDMs can have their own user databases, but most enterprises want to reuse existing authentication services and identity stores (e.g., Active Directory, LDAP, eDirectory). This creates two integration points: authentication and policy storage.

When a user tries to activate a new device or access services (e.g., password reset), your MDM must validate that user’s credentials. For example, your MDM might use Active Directory to log a mobile user into your Windows domain, retrieving policy attributes that dictate what that user can and cannot do. You may also want to use that directory to store MDM-generated attributes—for example, binding mobile device IDs to users.

All together now: Desktop management

If your company already uses a desktop management system like LANDesk or Microsoft System Center, it could make sense for you to tap those products (directly or using plug-in extensions) to configure and maintain your mobile devices too.

But a single device management system may not be a good fit for your mobile workforce. Perhaps you need to support more diverse mobile devices, or perhaps you have already invested in a pure-play MDM that focuses on mobile needs. In those situations, you may still find opportunities to reuse policies, practices and staff to simplify maintenance and promote consistency, for both administrators and end users.

Layer defenses: Mobile security solutions

Many MDM solutions incorporate a few security features—for example, some present their own login screen to authenticate device access and enforce policies regarding password length, complexity, update and recovery. However, MDMs do not necessarily provide all the security measures you may need to deploy on a given mobile device.

For example, a growing number of businesses want to encrypt data stored on mobile devices. Although some MDMs do this, many do not. Furthermore, you may want to use third-party data encryption that delivers cross-platform support for smartphones, PDAs and laptops. Even so, there may be opportunities for integration, like using your MDM to install the encryption program and verify correct configuration and operation. Similar possibilities exist for other third-party security solutions (e.g., VPN, antivirus).

Keep your eye on the ball: Event monitoring

Most MDMs collect a wealth of information about mobile devices and their activities for purposes of reporting, alerting and auditing. Of course, you probably already have numerous event sources throughout your corporate network—and perhaps even a central event management system to analyze them.

MDMs can fit into that “big picture” by supplying real-time alerts (e.g., traps, email) and historical logs describing mobile devices and their activities. This integration point may eventually leverage standards—for example, the Open Mobile Alliance (OMA) Device Management (DM) standard specifies a Generic Alert to convey client- or server-initiated management alerts.

Means to an end: Mobile applications

A well-oiled MDM can help you meet your business goals, but ultimately what really matters is whether mobile users can reach business applications. For example, your users may need to reach your Microsoft Exchange or Communicator server; and your MDM can play an important role in making that application accessible to mobile users.

For starters, your MDM may deploy packages, settings and policies required for mobile devices to access those servers. Some MDMs also play an active role by serving as a gateway to connect mobile users to back-office

enterprise servers, applications and data. Others can be paired with mobile application offerings from the same vendor to provide value-added features (e.g., push email delivery).

Conclusion

Over time, mobile devices will become an integral part of enterprise networks. Although close-knit integration of management services, policies and IT practices will not be achieved overnight, it will be necessary as more workers replace desktops with laptops and then leave their laptops behind in favor of handheld devices. The sooner you start thinking about potential MDM integration points, the faster you will accomplish unification and the less you may be forced to rework along the way.

Managing mobile device diversity

In a perfect world, your entire workforce would carry a standard mobile device that could be managed easily and effectively through one platform. Alas, few IT managers enjoy this luxury—most must deal with increasingly diverse employee and employer-owned devices, spanning multiple operating systems and product generations. How can you manage this handheld potpourri without going crazy or breaking the bank?

Different strokes for different folks

In a recent InformationWeek Analytics study of business technology managers, 59% said they specify and procure standard mobile devices, while another 13% specify standard devices that employees can purchase on their own. However, popular new devices like the Apple iPhone are making enforcement of standards difficult.

According to Gartner analyst Ken Dulaney, ergonomics and emphatic personal preferences for specific mobile device features instigate this mutiny, exacerbated by the broad spectrum of low-cost consumer-based mobile devices now available. “It is too easy for a user to purchase a smartphone with a personal credit card and then use it to access sensitive corporate data,” Dulaney said. In this increasingly diverse world, the only way IT can reasonably expect to maintain control is by categorizing mobile computing devices into three distinct classes: trusted, tolerated and despised.

Rather than telling your mobile workforce that they must assimilate (resistance is futile!), give them choices—accompanied by service-level consequences and enforceable access boundaries.

Managing diversity

Start by specifying a few well-chosen profiles for “trusted devices” that garner full IT support. Gartner recommends adopting no more than four to seven trusted device profiles that reflect your mobile workforce’s application/communication requirements, locations and work styles. Those profiles will serve as your primary target for hardware procurements, standard software images, mobile device management services, and mobile application development. If you do this right, users who depend on having access to many business applications will be encouraged to carry trusted devices.

But don’t stop there. Develop a second category composed of “tolerated devices”—the essential middle ground in your three-tiered strategy for managed diversity. Carefully define the applications and corporate network/data access levels that you can safely and effectively support for a reasonably broad range of mobile devices—including those commonly purchased by consumers.

For example, you might support only telephony features and browser-based access to enterprise Web portals. Or you might permit access to enterprise email only under certain conditions (e.g., over secured connections, from recognized devices registered with your mobile device manager). When defining this tier, aim to empower your workforce with personal choice while clearly limiting your support responsibilities and risk exposure.

Deal with exceptions

Last but certainly not least, define processes associated with that third tier of “despised” devices—devices over which you have so little control that officially supporting them would be cost-prohibitive or even dangerous. This should probably include so-called “closed” devices – smartphones with factory- or carrier-installed images that you cannot reconfigure because the APIs required to do so are not exposed to third-party developers.

It is tempting to forbid business use of these unmanaged, uncontrolled devices. But as soon as you adopt this policy, a C-level executive will receive one of these sexy little handhelds as a gift and complain to your CIO that your device management strategy is broken.

One solution, according to Gartner, is to offer “concierge services” for devices that deviate from your trusted/tolerated criteria. If supporting your CEO’s iPhone becomes a business necessity, determine what doing so will cost and a process for acquiring those funds. This policy in a nutshell: “We’ll meet your needs—for the right price.”

Minimize your personal footprint

Note that all of the mobile devices in tier 3—and many of those in tier 2—are employee-owned handhelds used for both business and pleasure. The tools and software used to deliver full support for tier 1 devices may be too intrusive for personal devices. A less heavy-handed approach will probably be necessary to balance business risk and cost on personal devices.

For example, you might use a mobile device manager to provision trusted devices with a standard set of software packages and configurations, including security programs like VPN clients. You might install policies that require those trusted devices to synchronize only with your corporate server and block personal email (POP account) access. But employees might chafe at having these programs and policies installed on their personal handhelds, for reasons of usability and privacy.

To avoid workforce mutiny—and to encourage corporate policy compliance—find opportunities to limit your footprint on tier 2 personal devices. Use available tools to defend your business against device loss or compromise, without trying to shoulder full responsibility for those devices themselves. This can run the gamut from allowing read-only browser access to using temporary Java agents to prevent session data from being stored on the handheld. Inside your network, use techniques like network-based virus scanning and email spam filters to reduce risk, independent of those mobile devices you cannot fully control anyway.

Conclusion

Gartner predicts that more than 70% of enterprises will implement converged management and security policies for corporate-owned and non-corporate mobile devices by 2012. Mobile devices are already proliferating at a rapid pace, both in terms of platform and ownership. The sooner you develop a mobile device management strategy to deal with this daunting but inevitable scenario, the better life will be for both your employees and your IT staff.

Resources from Sybase iAnywhere



[Video Webcast: How to Future-proof for Mobility: An Integrated Management and Security Strategy, with featured analyst firm Gartner, Inc.](#)

[Introduction to Device Management and Security with Afaria \(Flash Webcast\)](#)

[Customer Success Video: U.S. Foodservice Benefits from Sybase iAnywhere Mobility Solutions](#)

[Learn more about Mobile Device Management and Security solutions from Sybase iAnywhere](#)

About Sybase iAnywhere

Sybase iAnywhere enables success at the front lines of business. The company holds worldwide market leadership positions in mobile and embedded databases, mobile management and security, mobile middleware and synchronization, and Bluetooth® and infrared protocol technologies. Tens of millions of mobile devices and 20,000 customers and partners rely on the company's "Always Available" technologies, including SQL Anywhere and the Information Anywhere Suite.

www.sybase.com