With the compliments of Sybase® iAnywhere®

Mobile Device Management

FOR

DUMMIES®

Sybase iAnywhere Limited Edition

Securely manage your data, devices, and applications

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Mobile Device Management FOR DUMMIES®

By Mike Oliver, Sybase® iAnywhere®

John Wiley & Sons, Ltd

Mobile Device Management For Dummies®

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

E-mail (for orders and customer service enquires): cs-books@wiley.co.uk

Visit our Home Page on www.wiley.com

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-0-470-69472-5

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Contents at a Glance

Introduction

Welcome to *Mobile Device Management For Dummies*, your guide to the management and security of mobile computing equipment such as laptops and handheld devices.

About This Book

Every day, more and more of your enterprise – along with its data and transactions – is moving to the frontlines where you interact directly with your customers. The frontlines present a key opportunity for your business to gain a competitive advantage, by having the information and applications necessary to take decisive action when you need to. Technology is used at the frontlines in situations such as:

- A salesperson getting a customer to sign for the samples just received – using a handheld device.
- A police officer with a laptop in her vehicle, able to access a database of criminal information while on patrol.
- A field service engineer referring to a laptop that provides information on specific parts needed – so that he can fix the customer's problem the first time.
- A retail salesperson in a store checking stock levels and processing transactions with a handheld point-of-sale device.

- A health worker having up-to-date patient information – whether beside the bed in hospital or visiting the patient in her home.

This book gives you the lowdown on enterprise mobile device management and how Afaria®, the market leading solution, can help you.

Foolish Assumptions

In writing this book, we've made some assumptions about you. We assume that:

- You're in business and enjoy the benefits of being able to stay connected and informed while you're on the move.
- You're an IT manager who needs to keep on top of the multiple devices out and about in the field.

How to Use This Book

Mobile Device Management For Dummies is divided into five concise and information-packed parts:

- **Part I: Mobile Device Management: Why Bother?** We explore the reasons to go mobile, the challenges you'll face, and the need for effective management.
- **Part II: Managing Your Mobile Devices without Sweat or Tears.** We introduce the Sybase iAnywhere solutions, focusing on management.
- **Part III: Under Lock and Key: Enforcing Security.** We explain why securing your mobile data is absolutely vital.

- **Part IV: Looking to the Future.** Some crystal-ball gazing into the technologies you need to prepare for.
- **Part V: Top Ten Mobile Device Management Tips.** A small but perfectly formed chapter of tips for both the mobile user and systems administrator.

You can dip in and out of this book as you like, or read it from cover to cover – it shouldn't take you long!

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

The target draws your attention to time- or money-saving advice.

The knotted string highlights important information to bear in mind.

The Dummies man indicates real-life anecdotes to illustrate a point.

Where to Go from Here

As with all *For Dummies* books, you don't have to read this one from cover to cover if you don't want to. Use the headings to guide you to the information you need. If you require any more information, you can contact us at `contact_us@ianywhere.com`.

4

Part I

Mobile Device Management: Why Bother?

In This Part

- Considering security, visibility, and control
- Addressing the challenges of mobile device management

Did you know that up to 70 per cent of enterprise data exists in various frontline settings, from laptops to handheld devices, to shop and remote office environments? That's quite a statistic!

Your mobile staff might be employed for a variety of skills – to treat patients, dig up roads, repair malfunctioning equipment, or sell a product. They're rarely IT savvy and certainly not security experts. Yet more than 75 per cent of enterprises leave responsibility for security in the hands of the user – literally.

This part explores the challenges that mobility brings and why you need management and security to address these challenges.

Considering the Challenges of Mobility

Mobility brings numerous opportunities – but also challenges. Table 1-1 compares the advantages of networked computers with the challenges of mobile devices that you need to overcome.

Table 1-1 Comparing Networked Computers with Mobile Devices

Networked Computers	*Mobile Devices*
Unlimited bandwidth	Bandwidth is limited
Guaranteed, reliable connectivity	Intermittent, unreliable connectivity
Local support for users	No local technical support
IT can easily get to systems	IT may never see devices
The same platforms used	A variety of devices and platforms
Physical building security	Easily lost or stolen

The following sections consider other challenges you need to overcome when employing mobile devices.

Security

Mobile management and security are totally inter-dependent. An unsupported, unmanaged 'secure' system is invariably vulnerable the moment it leaves its cradle!

Mobile security is the need to control user access and protect your data on the device and storage, in transit, and if lost or stolen.

Without the appropriate security, mobile devices are extremely vulnerable to security gaps. As a result, the risk of intrusion is high and security controls are inconsistent at best and often unenforceable. Whether it's hackers, viruses, corrupted data, or lost or stolen devices, there's plenty to be concerned about.

Additionally, regulations regarding data privacy and encryption are becoming stricter and can even result in fines for noncompliance. IT and security experts must manage and protect sensitive information and enforce compliance centrally, rather than leaving the burden of security to the mobile device end-user.

Security will always be an issue – and the risk is even greater at the frontlines, on mobile devices.

User adoption

We all do whatever makes it easier for us to do our jobs. Your mobile workers are no different. Over the years, your office-based systems will have been honed by adopting best practices, and you'll face a challenge in asking your staff to abandon what they know and are comfortable with.

Introducing new systems for frontline workers always carries a risk that unless they see the benefits for themselves and 'buy in' to the systems, users will revert to their previous ways of working.

You need to ensure that electronic applications are intuitive and easier to use than the paper systems they replace. Ensure devices won't fail just when your workers need them most.

Engage your mobile workers early, train and listen to them, and they'll make the deployment a success!

Central visibility for IT

Central IT needs to see activity levels and user methodology in order to anticipate issues and continuously improve the system.

Being able to see what's actually going on at the frontlines is critical to success. Your IT folk need to know what activities are happening, and why, in order to make better decisions.

If your workers aren't utilising the systems you've deployed in the way you expected, you need to know why.

Control

Rather than trying to accommodate disparate systems and processes, you need to drive the project centrally to keep control.

You want to have mobile deployments linked for effective data sharing so your frontline workers have the information they need, when they need it, and so that the information they gather is automatically processed to everyone who requires it.

Food for thought

If you're not convinced about the benefits of mobile device management, here are some stats to chew over:

- Industry analysts rate 'mobile workforce enablement' and 'security' among the top enterprise IT priorities.
- It's estimated that over 300,000 mobile devices are lost or stolen in the US. In the UK, it's been reported that over 100 devices a month are lost at Heathrow Airport alone.
- Effectively mobilising existing paper-based systems almost always delivers significant business benefits. Numerous organisations have achieved improved conversion of prospects into active customers – by as much as 15 per cent.
- Effective device management can also bring communications costs under control, sometimes delivering as much as 60 per cent savings.

Each disparate system brings its own challenges. You might have a variety of devices with different user needs, connecting over significantly varying bandwidth, and they're often beyond direct, onsite IT support.

Having a management solution that gives you control over multiple devices and platforms, multiple user groups, and multiple processes is critical.

Business processes need to be consistently applied, and – as requirements change – executive leadership needs to be able to consistently drive changes to processes, actions, and behaviours.

Considering Why Enterprises Need Frontline Management

You may have already started venturing down the mobility path and have deployed devices and an application for a team within your organisation. However, without effective management, device reliability varies, applications aren't supported as well as those in the office, communication costs fluctuate, and security threats are significantly increased.

Effective mobile device management gives you secure control over your mobile data, devices, and applications, while giving your frontline workers the freedom to perform the job they were hired for, not struggle with technology.

Mobile workers are imperative to an organisation's success. Laptops and handheld devices that support workers at the frontlines are proliferating throughout corporations. With a mobile workforce comes the widespread distribution of sensitive, proprietary, and sometimes downright top-secret data outside the secure walls of HQ. It's critical for the success of a mobile deployment to put measures in place to control and protect mobile assets. By implementing a solution that

proactively manages and secures mobile data, devices, and applications, mobile projects can improve efficiency, customer service, and – ultimately – profitability.

The need for mobile systems management is growing – fast!

Introducing Afaria, from Sybase iAnywhere

Afaria helps organisations succeed by delivering the right data to your mobile workers in the right place, at the right time. It gives IT the broadest cross-platform control and gives mobile workers the freedom to do their jobs rather than battle with baffling technology.

Afaria supports mobile workers, wherever they are, by:

- Maximising customer-facing time by minimising connection time, and delivering the right information at the right time, on a dependable device.
- Supporting the mobile workers' devices and applications as if they were in the office.

Afaria supports enterprise IT by:

- Delivering control over all mobile devices, data, and applications from a single console interface.
- Keeping the security responsibility away from your end-users and within your control.
- Automating business processes.

Sybase iAnywhere has the market-leading products that deliver the functionality enterprises demand. Afaria has been the acknowledged market-leading mobile device management (MDM) solution ever since the market's been measured! And, as Afaria is part of the Information Anywhere Suite, Sybase iAnywhere can help you easily add on email, collaboration, or extend other applications as your mobility needs grow. In Parts II and III we look at how Afaria securely manages devices, data, and applications at the frontlines of businesses.

Part II

Managing Your Mobile Devices without Sweat or Tears

In This Part

- Thinking about what makes a great MDM solution
- Seeing how Afaria fits the bill

Maintaining the reliability and security of data and devices at the frontlines can be very challenging. These environments are diverse, complex, and often beyond direct, onsite IT control. IT must be able to proactively manage all the devices, applications, data, and communications critical to the success of mobile workers.

Organisations need to take a centralised approach to management and security, providing IT with the control and visibility they need, while empowering mobile workers to be successful with the information and applications they need to do their jobs.

This part explains exactly what to look for in a mobile device management solution.

Defining the Elements of a Great Management Solution

It's time to think carefully about the components of a really effective management solution. This section explores the elements you need – that Afaria provides.

Naturally, you need mobile data and device security, but this subject is so important that Part III is dedicated to it.

Cross-platform device support

A good mobile device management solution supports a wide variety of client types – such as Symbian, Blackberry, Windows Mobile, Palm, and Windows XP – from a single web-based console. Your initial deployment may just be for a team of engineers all using the same tablet PCs, but you also need to plan for the future deployment of executive PDAs and smartphones, maybe some older Palm devices in the warehouse, or the sales team's laptops. Plan now for every platform you have in your enterprise today – and for the new platforms continually emerging!

Configuration management

Central control of mobile devices enables administrators to maintain a wide range of software and hardware settings including device identification, network settings, connection profiles, regional settings, and alerts. The settings are continually checked against centrally defined configurations and reset whenever necessary.

Protecting the insurers

A market-leading insurance provider needed to protect sensitive customer financial and medical information residing on the computers owned by 3,500 independent agents. Sybase iAnywhere's laptop hard disk encryption, software distribution, device management, and stolen device lockdown dramatically improved the ability to implement, monitor, and enforce stringent data security policies. The company's reputation as an industry leader in information security was enhanced and customer service improved by having the most up-to-date information on agents' laptops.

Device monitoring

Effective mobile device management enables the user to work offline, instead of being constantly reliant on a connection to HQ. A high-quality device management solution reacts to changes in the state of a device – monitoring memory, files, folders, and registry settings for changes – and can trigger processes such as backing up a device when the battery level drops or launching a particular application when a user signs on.

Monitoring also tracks application installation and usage policies through logging and reporting capabilities and can track when confidential files on mobile devices are written to external cards or sent to other devices.

License control

A valuable component of a mobile device management solution is tracking how software licenses are deployed and used. Automatically generated reports include information about the last time an application was accessed.

Software distribution

Applications can be electronically distributed, installed, and maintained – and all without the end-users' knowledge or involvement. Central administration controls software installations, including version management, rollback, and criteria checking.

Inventory and asset control

Administrators can perform comprehensive inventory scans of hardware and software, automatically receiving alerts of changes. A prime example is help desk personnel quickly capturing the state of a device to hasten the fixing of any problems.

Remote control

Laptop or handheld device systems are remotely controlled to diagnose and correct faults, enabling mobile workers to focus on their jobs, not their IT systems.

Connection management

A strong MDM solution uses an intelligent architecture design that optimises the ability to make the appropriate decisions about which tools to use when managing a frontline deployment. Additionally, connection management functions are fully deployable over-the-air,

Getting the medical database fit and well

A leading medical database management organisation needed a solution to better manage data retransmitted by business services. With Sybase iAnywhere technology, its staff can update software and remotely diagnose laptop computers out in the field, eliminating the time-consuming method of physically shipping computers back to headquarters to be updated or repaired. This significantly reduces time spent on back-office tasks and improves productivity.

eliminating the need for remote devices to be manually configured by IT.

Scheduling and prioritisation

Comprehensive scheduling enables work to be completed at the most efficient times, and prioritisation of different tasks ensures quick completion of the most important activities. System administrators control the content, timing, parameters, and method of communication.

Bandwidth optimisation

Comprehensive bandwidth management supports applications across all network types. On-the-fly data compression, restarting connections at the point of interruption, file segmentation, and file-level and byte-level differencing minimise data volume for both large and small transfers.

Protecting corporate security

With more than 25,000 mobile workers, a leading global financial services company wanted to enforce corporate security and perform inventory control on thousands of newly deployed handheld devices. It turned to Sybase iAnywhere technology to secure information when devices are lost or stolen, provide proactive technical support by contacting users with solutions to potential problems, and increase productivity because employees are always connected. A spokesperson said: 'Even when a device was out of coverage, the Sybase iAnywhere software gave us the audit trail to ensure that the device was password protected.'

Dynamic Bandwidth Throttling releases bandwidth to other applications when activity levels increase and then reclaims it when they grow idle. Combining the ability to dynamically react to throughput conditions, dynamically change throttling schemes, and dynamically configure and monitor these schemes provides you with a powerful means to reduce costs and minimise your end-user pain. Clever stuff.

Software and inventory management

A leading mobile device management solution provides visibility into frontline devices so IT know exactly what devices are deployed, where they're located, and what software is installed. This provides IT with the ability to better manage and control future software deployments.

Speeding up fast food

A fast food chain of 1,300 restaurants needed to improve its remote PC management capabilities, specifically sending and receiving large files over the course of several transmissions, with the ability to re-start a file transmission without the entire file having to be re-sent. It wanted specific stores to connect at specified times, silent software installations, inventory monitoring, and security patches applied throughout its estate. Using Sybase iAnywhere software, the chain improved bi-directional communication – both scheduled and ad hoc – significantly improving patch management, and simplifying IT infrastructure. Transmission of daily reports has been reduced from 45 minutes to seconds, leaving store operators now able to focus more time on running their restaurants!

Application support

Significant management capabilities can be added to third-party or custom applications such as initial deployment, updating, and continual over-the-air maintenance. This functionality can even be fully integrated into your application via published APIs.

Document and content distribution

A good mobile device management solution goes beyond device management and gives IT the ability to control applications and data too. Document files are securely delivered to frontline workers using a forced or subscription model. Document owners have control over content and can easily add, delete, and update

content so that out-of-date documents in the field are automatically replaced.

File-based information can be updated from any source and format, including HTML, database files, documents, and other electronic content. Technologies such as *byte-level differencing*, which means replacing or updating a segment of a file (rather than the entire file), can deliver significant savings.

Process automation

Important tasks can be personalised and automated to make them faster and easier for the IT administrator and user.

Wizard-driven point-and-click scripting allows infinitely customisable activities on server or client systems, automating tasks and removing onerous responsibility from mobile workers. These processes can be scheduled or initiated manually, or they can be triggered by the monitoring of a third-party application.

Scripting delivers numerous possibilities: file transfers, hard disk checks and changes, configuration changes, and even 'IF/THEN' logic processes for complex tasking.

System management extensions

Within the confines of HQ, systems management is a relatively routine task. However, this task becomes complicated with remote devices because these devices aren't always connected to the network. A top-notch mobile device management system simplifies these routine management tasks by enabling regular monitoring of devices to ensure compliance with corporate policies.

Saving time and money

A large broadband communications company with over 3,500 field service representatives increased mobile worker and IT productivity, reduced repair time, and reaped about $500,000 in annual savings – much attributable to automated device management and application updates through Sybase iAnywhere technology.

Support for Microsoft SMS and other LAN systems management tools

A comprehensive MDM solution is Microsoft .Net-based and you can integrate it with LAN-based systems management tools (such as Microsoft SMS) to expand the range of devices that can be managed from the console. You can use it to manage all the latest Windows platforms, as well as extend management of other existing mobile operating systems including RIM, Palm, Symbian, and Windows handheld devices.

Finding the Solution with Afaria, from Sybase iAnywhere

You know the challenges and requirements of a really effective mobile device management solution, and the great news is that Afaria meets every one of these unique challenges of frontline environments. Afaria provides comprehensive management capabilities to

Counting the savings

A leading provider of cleaning services found that manually moving large business-critical IT files to remote devices was costly. It deployed Sybase iAnywhere mobile device management technology to manage its mobile devices and the flow of data. Staff time spent updating software decreased by 93 per cent, travel reduced by 80 per cent, and shipping costs dropped by 100 per cent!

proactively manage and secure all the devices, applications, data, and communications critical to frontline success, regardless of the bandwidth you have available.

Afaria is an enterprise-grade, highly scalable solution with a central web-based console that enables IT to control a host of key functions from a standard browser. And as Afaria is part of the Information Anywhere Suite, you can easily add other key functionality as your mobility needs evolve.

With Afaria's ability to tie into enterprise directories, these functions provide everything necessary to extend your organisation's management and security capabilities to any device, in any location.

Part III

Under Lock and Key: Enforcing Security

In This Part

- Thinking about your security needs
- Reading case studies

Laptops, handheld devices, and other mobile devices are, by their very nature, easy to lose and rarely within the grasp of your IT department. They're usually loaded with sensitive customer information, the risk of intrusion is high, and security controls are often inconsistent or non-existent. Mobile devices represent one of the most challenging battlegrounds in your campaign against data loss and theft.

You employ your mobile workers for a variety of skills – to sell, fix, treat things, and so on. They're not always comfortable with IT and certainly not security experts. Yet, more than 75 per cent of enterprises leave responsibility for security in the hands of the user.

This part delves into the security issues and, more importantly, the solutions you need to consider.

Safe as Houses: Considering Your Requirements

When thinking about security, remember that security is three-pronged and includes:

- **Availability:** Systems work promptly and service isn't denied to authorised users.
- **Integrity:** Data isn't changed in an unauthorised manner and the system itself isn't manipulated.
- **Confidentiality:** Information isn't disclosed to unauthorised individuals during storage, processing, or in transit.

Consider the relevance of the following list when developing the policies for your organisation:

- Protection for small, easily lost devices carrying sensitive information, rarely under the direct control of IT tech support.
- Centralised control from a single console over all your devices and user groups – whatever the device type, platform, or location.
- Security policies that meet legislative regulations.
- Reliable user authentication to control access to the device and subsequently your corporate data store.
- Protection for the data during transit and when it's stored on the device – whatever the platform or device type.

- The ability to protect the device even if you can't communicate with it, utilising data fading or 'kill-pill' functionality.
- Future-proof solutions for new platforms and emerging threats.

Stating the Requirements of Your Security Solution

An effective mobile security solution, like Afaria, combines security and systems management functionality from a single console. IT can transparently manage security requirements centrally, while supporting the application and device as if the mobile worker were attached to the office LAN. All necessary tasks can occur during a single connection.

Seek a security solution that delivers the following functionality.

Password protection

Password protection is the first step toward securing data on mobile devices. You need a solution that offers the ability to centrally define, control, and enforce end-user password policies.

It's handy for central IT to be able to remotely retrieve the password if your mobile worker forgets it. But if it's an unauthorised attack, you need *power-on password* enforcement, requiring a user to enter a password each time the device is turned on. If your pre-determined threshold of failed attempts is breached,

device lock-down policies automatically reset the device or delete specified or encrypted data.

On-device data encryption

Data on devices and removable storage must be encrypted and decrypted with minimal user inconvenience. In the case of a lost or stolen device, data is protected through strong encryption and other device disabling policies. Through the management console, you can select what data to encrypt and when. You can also encrypt removable storage media, such as compact flash cards and SD cards. Full-disk encryption protects the hard drives of laptops and tablet PCs, where the entire hard disk is encrypted, not just the

May the force be strong!

A police force needed a single solution that would send up-to-date information wirelessly through the network to laptops fitted within its patrol cars. It chose Sybase iAnywhere because it had so many features above and beyond what other providers offered: document management, hardware management, software management, and a script-writing feature. The wireless solution automatically starts working every time a patrol car enters the coverage area – updating information and software in 30 to 60 seconds, marking and restarting the update if the car leaves the coverage area before the download is complete. HQ is able to send out large files to the cars including wanted posters, missing persons information, crime statistics – and is able to update those files automatically.

Following the five-point plan to security

Remember the five key elements of enterprise mobile security:

- Set and centrally enforce your policies
- Authenticate the user
- Protect the data during transit and when it's stored on the device
- Secure your data if the device is lost or stolen
- Don't rely on your mobile workers for security!

user data. This is a more secure approach and doesn't require the user to make judgements about what files to encrypt.

Data-fading

Data-fading is the capability for an IT administrator to automatically lock, wipe, or reset a device that hasn't communicated with the corporate email or management server after a predetermined number of days, in case a device is lost or stolen. Similar protection can be initiated by sending a *kill-pill* to the device: a message 'pinged' to the device by the system administrator that immediately initiates data deletion or device reset.

Over-the-air data encryption

Over-the-air encryption ensures data is protected between the device and data centre. This also helps ensure that you comply with any enforced security legislation.

Helping an electricity provider shine brighter

An electricity provider needed a solution to manage its field-force asset inspection team. Previously, this field collection was completed in different regions using either paper or knowledge-based systems. Going mobile, utilising Sybase iAnywhere technology, enables distribution of work orders to inspectors in the field to capture and synchronise the asset information back to head office, automates previously manual processes, and provides secure data transfer between head office and field inspectors. More importantly, it increases flexibility for the field inspection team, giving them GPS location information for each asset and a full maintenance history – at their fingertips!

Patch management

Patches are automatically downloaded and deployed appropriately on an individual or group basis. Usually detailed logs and reports are kept to show the current patch levels and the protection levels employed.

The Security Checklist

Consider the following security measures in this handy checklist when you're planning a mobile security deployment:

- ✓ **Secure the device:**
  - Enforce strong power-on password protection that users can't bypass or turn off.

- Remotely lock devices that are lost or stolen.
- Proactively wipe data from devices when you need to.
- Reprovision devices in the field (automatically configuring devices for new usage, or building a new device with the configuration, applications, data, and security policies of a lost device it replaces).
- Encrypt sensitive data stored on mobile devices.
- Manage, distribute, and install security patches transparently via an administrator.
- Regularly back up key data from mobile devices to the corporate network.
- Inform users about the importance of and the means of protecting their information.

✔ **Guard against malicious code:**

- Distribute and install antivirus updates and software patches immediately and transparently.
- Prepare to tackle future threats – such as the increase in viruses that target handheld devices.
- Monitor and enforce system and application settings each time a device connects to the LAN, keeping track of who's accessed information.
- Block unprotected devices from accessing corporate systems such as email.

- Retrieve client-scan log files to analyse who's accessing data and applications on the frontlines.

- **Secure connections to corporate networks:**
  - Authenticate users and devices during each connection to the corporate network.
  - Encrypt data to ensure safe transfer over the network.
  - Automate an inspection that verifies compliance with security standards for antivirus software, patch levels, and personal firewall settings before allowing a connection.
- **Block network-based intrusion:**
  - Distribute, install, and maintain personal firewalls transparently via an administrator.
  - Enforce software settings.
  - Monitor intrusion attempts at every connection from the frontlines and block unauthorised access or unprotected devices.
  - Use exception reporting and alerts via an administrator to identify and correct network weak points to limit intrusion.
- **Centralise control of policies and corporate directories:**
  - Implement centrally managed security policies complete with established written policies.
  - Audit security policies and ensure that they're enforced by consistent reporting.

The PDA prescription

A leading hospital delivering care to nearly 700,000 patients every year deployed handheld devices to much of its medical staff. They selected Sybase iAnywhere technology to ensure that the most accurate information and applications are available to their users. The data transfer process is so easy and quick that the users can stay up-to-date all the time. Their IT department uses the technology to know who has which device, which software is licensed to each device, and how much memory remains. One of the great benefits of these features is that the IT department can keep track of inventory and can diagnose and treat IT problems. By examining logs via a web browser, helpdesk personnel can proactively troubleshoot a variety of problems.

Part IV

Looking to the Future

In This Part

- Seeking multiple components from a single vendor
- Guarding against handheld virus attacks

Especially in the 'mobile' space, technology changes faster than you can deploy! In this part we peer into the crystal ball at what you're likely to need to consider in the near future.

Integrating Mobile Deployment Components

As mobility becomes adopted more strategically in the future, organisations will seek to have more components from a single vendor. Having integrated components – such as management + security; security + email; email + messaging; application + messaging + management – reduces the risk of technological conflicts, not to mention the challenge of working with multiple contracts and multiple vendors when you just want your system to work.

Afaria, from Sybase iAnywhere, is part of the Information Anywhere Suite, a secure, scalable mobile device platform that addresses these converging IT requirements. By combining mobile email, collaboration, device management, enterprise-to-edge security, and back-office application extension, the Information Anywhere Suite enables your organisation to empower employees to do their work anywhere, at any time, on any device.

MAGnificent Multichannel Access Gateways

Currently, mobile deployments consist of a mix of mobile solutions from multiple vendors – each with separate software stacks for data transport. This leads to direct conflicts with network connections, as well as battery drain, complexities with testing, higher support costs, and an inability to effectively secure or manage your systems.

IT staff are moving towards combining the currently clashing data transport communications within a single access gateway called a multichannel access gateway (MAG).

Make sure that your mobile management and security solution is capable of communicating within your multichannel access gateway.

Keeping Up with a Changing World

New devices and even new platforms constantly challenge corporate IT. As soon you try to standardise on a device or platform, it's out of date, or your staff demand support for their own shiny gadgets!

The line between personal and work devices is becoming increasingly indistinct. There's a mix of enterprise operating systems and devices, with no single clear winner. And suddenly an emerging class of consumer devices will make their way into the enterprise.

You need to select a vendor who's committed to supporting the entire mixed device needs of your company – not just a sub-set.

Avoiding Viruses Like the Plague

Viruses are predominantly the curse of the laptop and desktop world, but handheld virus attacks are becoming increasingly prevalent since the first PDA virus was reported way back in 2004. As the devices become more popular, expect threats to your business to increase too! Choose a management and security solution that counters this risk.

Hotting things up for the fire brigade

One of the largest fire brigades in Europe selected Sybase iAnywhere to provide its mobile systems management solution to update and distribute risk information and building plans to over 150 fire appliances. The solution ensures all fire appliances are equipped with an up-to-date plan of all major risk buildings in their locality, to facilitate a fast and efficient emergency service, as well as to satisfy regulatory legislation. Probably the most important feature of the deployment is that it ensures data is standardised throughout the force so that if an emergency is large enough for more than one station to be involved, attending appliances are working from the same information.

Part V

Top Ten Mobile Device Management Tips

This part is small but packs a punch! Here are our top tips for both the systems administrator and the mobile worker.

For the corporate systems administrator:

- **Centrally enforce security policies on mobile devices.** Don't leave it up to the end-user to turn on password software, encrypt data, or keep anti-virus software up-to-date.
- **Implement a back-up system to protect corporate data.** Don't expect mobile workers to back up their own systems regularly. The back-up system needs to work even over slow dial-up connections and be completely unobtrusive to the user.
- **Utilise software that enables remote configuration of all your mobile systems.** You can then maintain browser and security settings centrally.
- **Keep an up-to-date hardware and software inventory along with a back-up of all users' data.** Doing so helps you get the user up and running faster if the worst does happen.

- **Provide your mobile workers with top levels of support.** Your mobile workers need that support – they're on their own and they're generating revenue for the business.

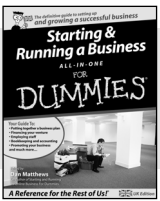
For the mobile worker:

- **Push your IT people to provide an automatic back-up system for your data.** This relieves you of the burden of remembering to back up your system every day.
- **Change your passwords regularly.** Don't use ones that others could easily guess such as your spouse's, child's, or pet's name.
- **Be wary about where you browse on the Internet.** Set your security settings to maximum within your web browser. Some unscrupulous websites could be spying on you and your data.
- **Be careful about who you open emails from.** Don't open a message from someone whose name you don't recognise, particularly if it has an attachment.
- **Don't abuse the system by loading software that could impact its use for your job.** Remember that the system is a tool to help you work efficiently.

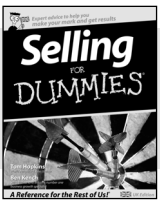
FOR DUMMIES®

A Reference for the Rest of Us!™

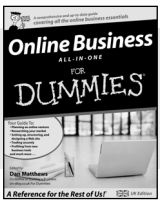
BUSINESS



978-0-470-51648-5



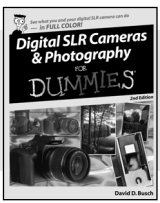
978-0-470-51259-3



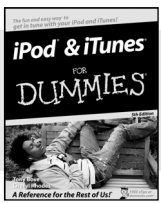
978-0-470-51646-1

DIGITAL LIFESTYLE

978-0-470-17469-2

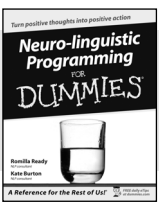


978-0-470-14927-0

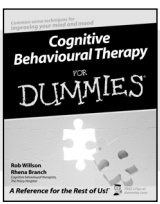


978-0-470-17474-6

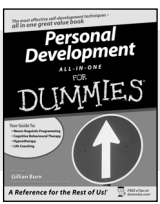
SELF HELP



978-0-7645-7028-5



978-0-470-01838-5



978-0-470-51501-3

Available wherever books are sold

WILEY

Secure and manage all your mobile devices

Choose the right mobile deployment solution

In order to do their job, your field personnel need the right information at the right time, on reliable devices. And, of course, security is vital. This minibook makes it easy for IT administrators to successfully mobilise their organisation – showing how to secure mobile data, manage devices and applications, and unleash the potential of the mobile workforce.

Discover how to:

- *Manage your mobile devices and applications*
- *Secure your mobile data*
- *Unleash your mobile workforce's potential*

THE DUMMIES WAY®

- *Explanations in plain English*
- *'Get in, get out' information*
- *Icons and other navigational aids*
- *A dash of humour and fun*

Get smart! @www.dummies.com

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Browse our free articles*

ISBN: 978-0-470-69472-5

Not for resale

For Dummies®
A Branded Imprint of
WILEY