

5 Steps: Successfully Supporting a Mobile Initiative

XCELLENET™

Table of Contents

Introduction	3
Getting Started.....	3
Step 1: Security.....	3
It's 2:00 a.m. Do you know where your devices are? Securing mobile data and devices from unauthorized use.....	3
Safety starts with a solid plan.....	4
Out of sight shouldn't mean out of mind.....	4
Step 2: The Devices.....	5
From Chaos To Control: How to inventory, manage and maintain a growing number of mobile devices.....	5
Visibility without having to have the device	5
A smart first step	5
Step 3: The Applications	6
Version X.Anything: How to standardize mobile applications and keep them current.	6
Control at your fingertips	6
Overcoming the mobile software distribution challenge	7
Step 4: The Data.....	7
Rock Solid Sync: How to keep critical data accurate and accessible for a growing mobile workforce.....	7
The benefits of a secure, reliable infrastructure.	8
Anticipating changes	8
Step 5: The Network	9
Ending The Mobile Network Nightmare: How to optimize bandwidth usage and ensure connectivity.....	9
Prioritizing is the first priority	9
Preparing for tomorrow, today.....	9
About XcelleNet	10

Introduction

While working with more than 2,500 customers across a wide range of industries, XcelleNet has seen many of the challenges companies face when implementing mobile solutions. With this insight, we decided to pull together a brief white paper that outlines common challenges and addresses how some companies are attempting to solve them. We'll take you through five steps that every major mobile project must consider: Security, Devices, Applications, Data, and Networks.

While this is not a technical document, our hope is that this level of detail is enough to help you start thinking about your mobile game plan. For a more technical solution we offer a free XcelleNet Starter Kit that includes software, documentation, technical support and online training. We've found that since each technical challenge is unique, providing this type of starter kit is the best way to educate the technical group on the requirements for a robust mobile infrastructure.

Getting Started

The cost of inaction is hard to calculate. After all, how important is the security of your corporate data? Or the sanity of your IT staff? A Gartner Group analysis shows that technical support, asset tracking and synchronization activities have already increased the total cost of ownership for the average PDA to more than \$2,500 per year. What happens as your handheld user base increases? What happens when your company decides to roll out more complex applications? Will you be able to cost-effectively support these devices? Will your infrastructure scale to meet new demands?

These are challenging questions that demand answers and often it's difficult to determine where to start. We offer this white paper and the XcelleNet Starter Kit as tools to help you understand the complexities in any mobile project.

Step 1: Security

It's 2:00 a.m. Do you know where your devices are? Securing mobile data and devices from unauthorized use.

It's 2:00 a.m. In the rush to catch a red-eye, your V.P. of Marketing just left his PDA in the airport lounge. On the hard-drive: Product roll-out dates and strategic pricing info. Quick . . . What do you do?

If you think this scenario is far-fetched, think again. Millions of mobile devices already store sensitive corporate data, most without even password protection to keep data safe. Gartner Research estimates that 250,000 devices were left in airports last year alone, an alarming trend considering that more than 40% of corporate data will reside on handhelds by 2005.

So, how safe is your data? For future peace of mind, now is the time to extend corporate LAN security to the wireless world.

Safety Starts with a Solid Plan

A handheld device that falls into the wrong hands can result in as much damage as a PC commandeered by a hacker. Therefore, it's critical to treat mobile devices with the same care as a PC/LAN environment. This includes focusing on three key security areas:

- ◆ *Preventing damage caused by malicious code.* As handheld usage grows, code is being written to damage, corrupt and just plain steal your mobile data. Be prepared.
- ◆ *Protecting data while in transit over wireless networks.* Whether over wires or airwaves, data in transit is vulnerable to attack. Adhering to standards including (SSL) encryption and digital certificates is a key step to keeping data secure.
- ◆ *Protecting data resident on mobile devices.* Ensuring data integrity requires password enforcement, the centralized ability to lock or delete data on devices, and the power to update software security patches.

Out of Sight Shouldn't Mean Out of Mind

Unfortunately, while you may see the need for mobile data security, others may not. After all, mobile devices aren't physically tied to the corporate LAN, so why should corporate dollars be spent to secure them? Adding to the nay-sayers are users themselves. The "I've got a password, I'm covered" mentality simply won't fly. Password features are easily turned off (and busy executives are notorious for doing so to save time) and seasoned hackers can bypass a standard password without blinking. It's simply not enough protection.

A mobile infrastructure should provide centralized control over critical security functions including: user authentication, data encryption, anti-virus administration, software version control, data syncing, automatic backups, and (in the case of our forgetful Marketing VP at the airport) emergency data lock-downs.

Step 2: The Devices

From Chaos To Control: How to inventory, manage and maintain a growing number of mobile devices.

A quick peek around the office will confirm it: mobile devices are everywhere. And if it hasn't happened already, the task of supporting these devices will inevitably end up in the lap of the IT department. Of course, effective support begins by bringing these devices under centralized control. But how can you gain control when the technology is changing so rapidly? You can't even get an accurate inventory of what's already out there, much less get corporate data to these devices.

Believe it or not, there's a way to control the chaos. And it's a lot less painful than you might think.

Visibility... Without Needing to Have the Device

Imagine a world where you could log onto any Web browser and gain instant visibility into your mobile devices; you would know who owns what type of device, and what type of hardware and what version of software is loaded on it. Now imagine being able to automatically monitor and repair these devices without ever needing physical contact with them. You don't have to pinch yourself. This can be your reality. By adding a level of software intelligence, you can easily manage the chaos, and ensure that end-users always have the right software, that it's working properly, and that the IT department isn't overwhelmed trying to manage and support it all.

A Smart First Step

You can quickly experience centralized management of mobile devices with features that allow you to:

- ◆ *Keep track of valuable assets:* automatically scan and retrieve detailed data on software licensing, processor type, amount of memory and operating system installed. This information gives you the clear picture you need prior to performing hardware and software updates, troubleshooting or other administrative tasks.
- ◆ *Monitor and be alerted when handheld devices change:* track changes on handheld devices. You can be notified visually or through an alert when key parameters have changed on a handheld device, such as a decrease in available memory or removal of a key application.

- ◆ *Troubleshooting support:* Monitoring for changes to devices or reviewing the inventory scan data gives your helpdesk the knowledge for troubleshooting and support.

Step 3: The Applications

Version X.Anything: How to standardize mobile applications and keep them current.

Recent growth in handheld devices has created tremendous freedom for mobile users — and tremendous headaches for IT staff. As employees continue to purchase consumer technologies for corporate use, the pressure is on to standardize software and bring these devices under corporate control. Unfortunately, it's not as simple as posting a few patches for download on the company extranet. There are simply too many platforms to deal with. Only adding to the mayhem are users themselves, downloading software and creating sync processes that may or may not fit into the enterprise mobile plan.

The easy way to gain control: centralized, automated application distribution and management.

Control - at Your Fingertips

In the typical LAN environment, several options exist for managing software applications and troubleshooting systems. For example, it's possible to walk down to the specific client or server and get it up and running. The mobile environment presents a new set of problems. If a system breaks, do users have to mail in the device? This is usually impossible, because if the device is truly mission-critical, how can the user afford not to have the device for several days? How can the company afford to lose the productivity of that user? Furthermore, the relative immaturity of these devices make them more fragile than Win32 computing, thus rendering them prone to break more often.

Given this harsh reality, it's easy to see why a centralized system that can reach out to these devices and pull information back - or push information to - the device is critical. For example, imagine being able to run a query on a device and find out exactly what software is loaded, what type of device the user has, what hardware is being used, and what peripherals are attached.

In a standard client/server environment, managing software applications creates fewer headaches. Version tracking and control happen automatically. Updates, patches, and upgrades occur seamlessly and transparently in the background. However, in a mobile environment, disparate platforms make these tasks difficult — but not impossible.

By adding a layer of software intelligence, you can now easily manage mobile device applications — from tracking to troubleshooting to upgrades — from virtually any Web browser. With convenient, centralized control, you can ensure users are running the right software and minimize the downtime required to handle mobile administrative tasks, all while reducing the burden on your IT staff, who has to manage it all.

Overcoming the Mobile Software Distribution Challenge

A mobile infrastructure solution can be designed to reduce the costs and hassles of distributing, managing and maintaining mobile applications. Capabilities like these should be included in your mobile infrastructure:

- ◆ *Software license tracking:* What apps are already out there? What versions are currently running? Get a quick picture of the software deployed across your enterprise.
- ◆ *Proactive troubleshooting:* Monitor software for corrupt or missing files. If an issue is found, the software can automatically replace these files so that problems are proactively fixed before the user has to log a support call. Extensive logging can also provide help desks with additional data to help diagnose user problems.
- ◆ *Keeping software versions consistent:* When rolling out strategic apps or updating support files, we make it easy to uniformly distribute software to groups or individuals, all from a central location.
- ◆ *Controlling software distribution with criteria checking:* Check for software and hardware requirements before you actually try to download and install an update or new applications. Send software upgrades only if certain conditions are met, for example, only if the device is connecting via a high-speed connection.

Step 4: The Data

Rock Solid Sync: How to keep critical data accurate and accessible for a growing mobile workforce.

Whether by default or by plan, thousands of companies have adopted a mobile mentality. Unfortunately, this explosive growth in handheld devices has created a serious lack of corporate control. Employees are purchasing virtually every type of device — from Palms to iPAQs — then using them to sync and share corporate data in an unsupervised, unsecured environment.

Of course, before you lose sleep or debate a career change, consider this: it is possible for IT to sync and support these devices without draining time and resources. All it takes is some smart planning.

The Benefits of a Secure, Reliable Infrastructure.

Establishing a secure, reliable infrastructure can make supporting handheld devices much like supporting a wired LAN. Whether client applications are thin, fat, hybrid or a combination of all three, your data flows smoothly and safely without the hassles of incompatible platforms or communication errors. Even if devices aren't corporate sanctioned, they can be incorporated — increasing device productivity while reducing support questions to your help desk.

Today, it is possible to provide a secure, reliable, and inexpensive way for enterprises to give users access to corporate groupware applications without circumventing corporate policy. Making the right infrastructure decision today will help you when users need access to other mission-critical applications tomorrow.

Anticipating Changes

A good mobile infrastructure design needs to extend beyond a simple point solution. Planning will allow you to incorporate a groupware sync today and add more sophisticated synchronization and system management tasks as your needs dictate. Create a standard environment in which your mobile devices can become a seamless extension of your LAN. Highlights include:

- ◆ *Synchronization e-mail:* Allows users to synchronize Exchange and Domino groupware applications, including e-mail, contacts, calendars and to-do lists.
- ◆ *Synchronization enterprise applications:* Sync with major client and server databases without requiring changes to applications and databases.
- ◆ *Move data between applications:* Integrate with leading technologies like COM, XML and ODBC.
- ◆ *Security:* Authenticate with active directory, NT, LDAP, or custom log-in. Encryption via SSL or digital certificate.
- ◆ *Support any type of connectivity:* Support wireless, wired modem or cradle devices as well as most communications protocols including http, CDPD, GSM, CDMA, MOBITEK, and 802.11.
- ◆ *Centralized administration:* Provide a single console for all mobile devices including Palm, PPC/Win CE, RIM Blackberry, and Win32.

Step 5: The Network

Ending The Mobile Network Nightmare: How to optimize bandwidth usage and ensure connectivity.

How will you communicate safely and securely with mobile devices that are always used outside the office? Gartner Research predicts that by 2005, more than 40% of corporate data will be stored on mobile devices. What's more, the mission-critical nature of these apps will place an increasing demand on the IT staff, who will have to ensure that they can send and receive application data and software updates to these devices.

With the success of your mobile workforce on the line, the need for a comprehensive network strategy is paramount. What's the most efficient way to upload and download data in order to minimize session times and connection fees while keeping the user experience satisfactory? The right strategy can help you turn a potential nightmare into a corporate success story.

Prioritizing: the First Priority

The current state of mobile networking is anything but ideal. Slow, unreliable (and often costly) network connections make it difficult to keep your people and your back-end systems working off of the same page.

The key to better performance is prioritization.

Intelligent networking technologies now exist to help you prioritize and allocate precious resources (like bandwidth) in order to boost efficiency and performance. Session got dropped during file transfer? Resume where you left off, minimizing connection time and fees. Not using the full bandwidth available during your current session? Fill the pipe by pushing software updates in the background, maximizing the value of your connection time.

The ideal network solution doesn't start from scratch. Rather, it injects a layer of intelligence that helps PDAs and other mobile devices work smarter with your existing infrastructure while providing the flexibility to meet future needs.

Preparing for Tomorrow, Today

A comprehensive mobile infrastructure solution should overcome today's mobile network limitations and prepare for the future with robust features including:

- ◆ *Checkpoint restart*: Intelligently tracks the progress of file transfers as they occur. Broken file transfers are resumed at the point the connection was lost, rather than re-transferring the entire file.

- ◆ *Dynamic bandwidth throttling*: Automatically adjusts the amount of information being transmitted if the user is in the middle of another task or the pipeline is empty. This ensures that the user doesn't get bogged down by synchronization or management processes taking place in the background.
- ◆ *Byte-level differencing*: Reduces connection times by transferring only the bytes of a file that have changed, rather than transferring the entire file.
- ◆ *Other optimization techniques*: Best practices for optimizing your network also include: segmented delivery, compression, scheduling, offline processing, and criteria checking.

About XcelleNet

XcelleNet, Inc. is the leading provider of Mobile Infrastructure solutions and expertise. For 15 years, XcelleNet has been on the leading edge of helping companies build business solutions that guarantee the continuous flow of information across a widespread computing environment to a broad range of device types. XcelleNet today meets the challenges of mobile deployments by providing solutions that (1) gain control over a myriad of devices, from laptops to PDAs to smartphones (2) maintain corporate applications (3) ensure currency of data (4) enable communications over diverse networks and (5) enforce security policies to protect corporate data. Industry leaders such as Schering-Plough, Federated Insurance, Aid Association for Lutherans, BNP, Coinstar, Blockbuster, Clark Shoes, Hercules Incorporated, TVF, American Greetings, Novartis, Schwarz Pharma, Movie Gallery and Chick-fil-A are just a few of the more than 2,500 customers worldwide benefiting from XcelleNet's products. XcelleNet's partners include technology leaders such as Compaq, Microsoft, Hewlett Packard, Casio, Verizon IT, Symbol, RIM, Palm, and Handspring.

For more information please visit <http://www.XcelleNet.com>.