



WHITE PAPER

Ten Steps to an Enterprise Mobility Strategy



Changing the Economics of Mobility and Revolutionizing the Connectivity Experience

Corporate Headquarters +1 650-232-4100
iPass Inc. +1 650-232-4111 fx
3800 Bridge Parkway
Redwood Shores, CA 94065 www.ipass.com



Table of Contents

Introduction	3
The Rapid Evolution of Enterprise Mobility	3
The Need to Cut Mobility Costs	3
Reducing Vulnerability and Compliance Risks	4
Lifecycle Management of Mobility Services	4
Three Approaches to Managing Mobility	5
iPass Open Mobile Platform	6
iPass Solution Benefits	7
Conclusion	7
About iPass	7

Ten Steps to an Enterprise Mobility Strategy

Changing the Economics of Mobility and Revolutionizing the Connectivity Experience

Introduction

Managing mobile connectivity used to be simple. Companies provided their mobile workers with a cell phone or maybe a BlackBerry, negotiated a good carrier rate plan, and they were done. If they were ahead of the curve, they had a strategy for managing Wi-Fi connectivity for laptops, complete with a remote VPN solution that kept everything safe and secure.

Then somebody turned that cell phone into a computer, and someone else figured out a way to stick a cellular modem into a laptop. The options for mobile connectivity multiplied overnight. At the same time, people started building web interfaces for mission-critical applications that had once lived only on the corporate LAN, safely inside the company firewall. Suddenly security was a major concern and mobility management became a nightmare as everybody from the boardroom to the shipping dock wanted access to everything on any device, all the time, from anywhere.

With millions of users having downloaded billions of applications to their iPhones and other mobile devices, it's easy to think that mobile connectivity has been with us for a long time. But seasoned IT managers know better. They know that the era of an always-connected workforce is just beginning, carrying with it many facets that greatly increase the complexity of mobility management. There are now serious penalties for managing mobility poorly - fiscally, strategically, security-wise, and perhaps even career-wise.

The good news is that mobility doesn't have to be a severe financial drain or a challenge that should be avoided. In fact, it can't be avoided. If companies don't address mobility, users will choose their own off-the-shelf technologies that fit their needs - resulting in spiraling expenses and few or no tools for security management. But if companies do get strategic about mobility management today, this can provide a tremendous competitive advantage for any enterprise.

The Rapid Evolution of Enterprise Mobility

From the home to the corporation and the local hotspot (free or commercial) - today more than 187.9 million workers are mobile. And the numbers are going up rapidly. Forrester Research expects that 397.1 million workers will be mobile by 2012, representing 73 percent of the global enterprise workforce.

Employees are now demanding anytime, anywhere access to information without concerns for potential compliance, security, or cost implications. IDC estimates that 70 percent or more of enterprise data now resides in some form on mobile devices, yet remarkably, approximately three out of four organizations lack comprehensive formalized policies for dealing with the management or security of all of their mobile devices.

Today's mobile technology innovations and mobile network connectivity options are being driven by the consumer market. This comes as no surprise, considering consumers buy the vast majority of smartphones and other advanced communications devices. And from the Apple iPhone, to devices based on the Symbian operating system and Goggle's Android, the rise of the consumer market also means people have gotten a lot smarter and more demanding when it comes to technology - and less patient with outdated office gear.

The Need to Cut Mobility Costs

Connectivity expenses for mobile workers can quickly get out of hand. Gartner predicts that 80% of companies will overspend on their wireless services in 2012. The reasons are many:

- **Expensive employee-purchased devices.** Cell phones and other communication devices are often initially purchased by employees to meet their personal needs, and then used for business. By not leveraging negotiated corporate rates, these employee-purchased devices incur much higher contract costs for the enterprise. IDC predicts that in 2013, more than 56 percent of corporate mobile



devices will be individual-liable devices, which means individuals will make the mobile decisions regardless of cost, and bill back their costs to their companies.

- **Uncontrollable roaming charges.** Employee's mobile devices are often used internationally, and can result in huge roaming charges. The surprise \$6,000 3G roaming bill, which used to be a shocker, is now a common IT war story.
- **Idle or unused devices.** Infrequently used or abandoned devices will continue to generate monthly service charges even after the equipment is discarded or the employee has left the company.
- **Lack of visibility into mobility spend.** Connectivity charges for these high-speed devices often get buried inside employees' expense reports, further obscuring the company's attempts to get accurate information about the real costs of mobile computing.

Reducing Vulnerability and Compliance Risks

Data security used to be handled nicely with the company VPN. Now, IT must deal with the reality of unknown and potentially insecure mobile networks, as well as SaaS-based apps and devices living unprotected on the Internet. Not only is the data actually on the mobile devices at risk - these laptops, iPhones, BlackBerrys, and other devices carry corporate credentials that afford full client access to mission-critical applications, which are at risk even if the user is only accessing the email system.

As the point of control shifts from the VPN to the Internet connection, companies are now left exposed. Many organizations don't have an enterprise mobility strategy in place or strong internal controls that require employees to back up all their data, to run the latest antivirus software, or to comply with company policies. Most companies don't even know what devices are deployed across their user base and what they are being used for. At the same time, many IT departments are starting to evaluate cloud computing technologies and SaaS-based applications, like Salesforce.com. But these apps reside outside of the company firewall and render the VPN ineffective as a policy enforcement point.

Shutting off these new applications and methods of access isn't an option, because always-on connectivity that drives employee productivity and business workflow velocity is a competitive necessity. Key decision makers and revenue generators across the enterprise need to make judgments better and faster. To accomplish this, they need the convenience of mobility for access to the information and applications that the enterprise runs on.

Properly implemented, mobility can be embraced and extended to support more efficiency, improve customer responsiveness, and enhance employee productivity - with costs accurately aligned to the actual value delivered. And beyond these soft dollar improvements, there are hard dollar savings available from reduced real estate and power costs. The key question then, is how can an enterprise empower its mobile workforce in a cost effective, responsible, and professional way?

Lifecycle Management of Mobility Services

Managing mobility across today's webified enterprise is much different than the "good old days" of supporting one mobile application (email) on one type of standard corporate-issued device. Today, companies need to design mobile services delivery around the idea that the "new normal" will be one that changes constantly in scope, devices, networks, and applications.

This requires a comprehensive lifecycle management approach, where IT can manage users through an efficient process for provisioning, updating, and eventually decommissioning users, devices, and services on a continual basis within the context of constantly evolving technology. But this can be a challenging task.

The best way to start is by building a framework of questions to ask and bases to cover upfront, to make sure the mobility lifecycle management plan doesn't become obsolete when inevitable changes occur. Steps include:

- **Step 1. Define all business goals and requirements.** The first step for any mobility initiative is to determine



what the company's objectives are (e.g., higher sales efficiency, better availability of key staff), what use cases might support those goals, and what technologies and devices will map to those goals.

- **Step 2. Add the information technology view.** Once the business requirements are well understood, then it's time to add the information technology view, evaluating key corporate requirements for manageability, flexibility, and scalability.
- **Step 3. Create a timeline for delivery.** A detailed time-frame for delivery and service roadmap is the next step.
- **Step 4. Create a preliminary budget** with a rough cost-to-serve envelope as a budgetary starting point.
- **Step 5. List the risks and policy tools.** A full list of risks and the policy tools used to mitigate them should be incorporated, as well as any device-security requirements and applications that might be needed.
- **Step 6. Add it all up.** And finally, adding it all up will provide the information needed to determine if the projected costs are aligned with the desired value of the mobility deployment.
- **Step 7. Begin the vendor and technology selection process.** Only then - with all of this preliminary work done - should IT management seriously begin the vendor and technology selection process, since they will have a much stronger and sensible place to start negotiations when they know what the end functionality and costs should look like.
- **Step 8. Start with a test deployment.** The final go-live process should include a test deployment, followed by a wider rollout.
- **Step 9. Expand to a wider roll-out.** Ongoing end-user education and communication is essential so that all parties can learn as they go and guarantee a successful outcome.
- **Step 10. Rinse and repeat.** It is important to remember that launching a mobility initiative isn't the end of the road - it's only the beginning of the journey. The inevitable software patches, device updates, and technological improvements will probably begin shortly after deployment. Enterprises should think of this as the "rinse and repeat" management cycle, one that continually evolves services to embrace new mobile technologies and functionality, while retaining the goals and objectives of the initial, well thought out plan supported by the necessary management tools.

Three Approaches to Managing Mobility

When it comes time to deploy a mobility service management plan, there are now three paths to choose from:

- 1. Manage mobility in-house.** Companies can do it themselves by gluing together point solutions - if they are confident they have the necessary software development resources and in-house expertise on all the latest mobile market facets and features, as well as the ability to keep up as consumer technologies change.
- 2. Use an outsourced service provider.** Or, companies can throw it all over the wall to an outsourced/managed service provider - if their budgets can stand the strain and IT doesn't mind the inevitable loss of subject matter expertise and visibility into whether the company is getting the best technology. Unfortunately, for customers who want to maintain control of their own destiny and create a flexible, cost-effective solution that crosses multiple user groups and technologies this is not a viable solution.
- 3. The iPass Open Mobile Platform.** iPass now provides enterprises with a viable third choice. The following section will introduce the iPass Open Mobile Platform, and describe the many benefits the platform provides to today's enterprises.

iPass Open Mobile Platform

The iPass Open Mobile Platform is now changing the economics of mobility by enabling carrier independence, containing expensive connectivity costs, decreasing end-user support costs, and reducing the mobility administration burden. The platform supports a basic option that just connects your users to Wi-Fi easily and quickly while travelling as well as providing more advanced configurations that provide a new level of insight and control to drive down expenses and maintain security in a world where consumers drive enterprise IT.

The Open Mobile Platform consists of the following Enterprise Mobility Services that allow the Enterprise to deploy mobility solutions tailored for their workforce:

- **iPass Mobile Connect** - a service that orchestrates policy-based Internet and corporate access for the iPass Open Mobile Client, lightweight software available for a wide range of mobile devices.
- **iPass Mobile Insight** - a service that offers companies deep reporting and analytics on mobile usage across all their networks and devices.
- **iPass Mobile Control** - provides basic connectivity policies as well as advanced policy enforcement options that enable IT staff to apply and enforce cost and compliance measures across the mobile workforce by deploying a wide variety of connectivity- and device-oriented policies in real-time.
- **iPass Mobile Network** - the world's largest broadband network, with network coverage in 160 countries including over 650,000 Wi-Fi hotspot access points in 117 countries and territories.



iPass Solution Benefits:

- Provides an **intuitive connectivity experience** across multiple devices (laptops, smartphones and tablets) and networks
- Delivers **detailed usage analytics** for understanding and improving mobility price/performance
- Offers the ability to create, deploy, and enforce policies that **control costs and maintain security**
- Enables IT to **adapt quickly to new technologies** with no new CapEx for the enterprise
- **Streamlines service administration and the user experience** by integrating with enterprise security and management systems

Conclusion

Enterprise employees are increasingly on the move, relying on the ability to work from anywhere, at any time. But to make connections from various locations, they use a wide selection of broadband technologies, creating significant security risks and financial exposure for the company and a management nightmare for IT. To regain control of the situation, companies need a strategic approach to mobility that unifies connection types, providers, and device platforms.

The iPass Open Mobile Platform mobility services provide a solid platform for executing a mobility strategy, combining connectivity and device management to empower mobile users while improving IT insight, gaining control, and cutting costs. iPass helps companies take advantage of the amazing power of mobility, while also making it a sane, managed part of a scalable IT portfolio.

To find out how iPass can make your company better at managing the entire lifecycle of enterprise mobility services today - as well as building a strong foundation for the future - contact your **iPass account manager** or visit www.ipass.com today.

About iPass

iPass helps **enterprises** and **service providers** ensure that employees and customers stay well connected. Founded in 1996, iPass (NASDAQ: IPAS) delivers the world's largest commercial-grade Wi-Fi network and most trusted connectivity platform. With more hotels, airports, and business venues than any other network, iPass gives its customers always-on, frictionless connectivity anywhere in the world - easily, quickly, securely and cost effectively.

Get best practices, industry trends, and customer stories in the **iPass Video Center**.

Additional information is available at www.ipass.com or on **Smarter Connections**, the iPass blog.



Corporate Headquarters +1 650-232-4100
iPass Inc. +1 650-232-4111 fx
3800 Bridge Parkway
Redwood Shores, CA 94065 www.ipass.com

© Copyright 2012 iPass Inc. All rights reserved. iPass and the iPass logo are registered trademarks of iPass Inc. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, iPass does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.