NetMotion® WIRELESS

Managing Enterprise Mobility

The Dozen Challenges to Successful Deployments

MOBILITY. UNCOMPROMISED.

Executive Summary

Users and IT departments are familiar with wired environments. Given that experience, the challenges of managing enterprise mobility over wireless networks are not always anticipated. Those challenges are many and varied: from the practicalities of device management to users struggling with repeat logins, from unexpected application crashes to broad business issues. Knowledge of them will assist IT departments in planning a smooth rollout.

The Importance of Mobility

As wireless network capacity expands and mobile devices become more powerful, enterprises are able to bring full application access directly to mobile workers in the field. Those workers roam across multiple networks, use multiple connection types and encounter coverage gaps, all while expecting the same reliable, continuously available access to network resources that they experience in the office.

Similarly, IT departments need to manage the mobile elements of the business in the same way they support the business over the internal wired network, for efficiency and to keep costs down. But the difference between wired and wireless environments presents a set of challenges. Knowledge of them up-front will assist IT departments as they plan their mobile deployments. If they are not aware of them beforehand, they certainly will learn some or all of them when the deployment goes into production.

What follows are the top 12 challenges that organizations face as they expand their mobile workforce and systems to support them, and the solutions to help overcome them.

Knowledge of wireless challenges will assist IT departments as they plan mobile deployments.

The Dozen Challenges

IT Service Deliver

Automate Patch Management and Upgrades

Managing a large mobile deployment on a device-by-device basis can be an administrative nightmare. Ideally the same systems management suites used on the internal wired network can be extended to the mobile environment, allowing those devices to be managed “over the air.” Patches and upgrades should be applied after-hours, or at other times when users aren’t actively using or logged onto their devices, to avoid impacting productivity. “Bandwidth-aware” capabilities ensures that systems management proceeds not just at an appropriate time, but over a connection with appropriate speed. Depending on use patterns and the various connections available, that optimal connection might be over a cellular network after-hours; while a device is in range of a corporate Wi-Fi connection in a parking garage; connected via home Wi-Fi; or mounted in a docking station.

Keep Trouble Tickets in Check

A mobile environment adds new variables to the application-delivery equation including intermittent connectivity, access over third-party networks, and a need for more complex security and authentication schemes. It is difficult for typical workers to recognize when a problem is due to their connection as opposed to their device, to an application, or to conditions on the host network or server. A solution that manages the complexities of connections on the worker's behalf, effectively taking connection problems out of the equation, has been shown to greatly reduce the number of help desk calls. This not only lowers support costs but eliminates the lost productivity that those support calls represent.

Achieve Reliable Operation Without Burdening IT

Just as the wireless infrastructure should be "hands-off" for the user, it should be "hands-off" for IT as well. Active load-balancing and automated failover built into a solution allow a "set-and-forget" operation. A proactive alerting capability allows the IT department to manage by-exception and receive automatic notification of problems or potential problems, without having to constantly monitor the deployment. Oftentimes, they can intervene before issues impact workers and trigger trouble tickets.

Organizational Security

Enforce Security Without Hampering Workers

Protecting data and devices from unauthorized access is important, but sometimes requires a balancing act. Whether single-factor passwords are sufficient or two or multi-factor strong authentication is called for, authentication needs to be straightforward and a lost connection shouldn't require workers to have to perform repeat logins.

Devices need verification that security precautions are active to avoid introducing malware that would place the enterprise and its user community at risk. Data streams need to be encrypted to protect corporate information and in some cases, to meet regulatory requirements. An ideal solution accounts for all of these security concerns, in a way that doesn't burden the user into having to take extra steps, and protects assets in a way that is as hands-off as possible.

Protecting data and devices from unauthorized access is important, but sometimes requires a balancing act.

Protect Against Stolen Devices or Unauthorized Access

A mobile device configured to access internal applications and data that is lost or stolen can be a huge security risk. The ability to immediately quarantine a device that has been reported lost, or to recognize that a device is being used by an unauthorized person (through too many wrong password attempts) protects the corporate network. Digital certificates may also be used to verify that only devices that have been preapproved may connect to corporate resources; this prevents a user from using corporate credentials to connect via an unsecure home machine or other personal device. A common practice is to automatically place any newly distributed device into immediate quarantine on the first connection, so the administrator can verify the device's configuration and user identity before allowing full access.

Gain Control over Workers, Devices and Networks

Mobile assets are constantly on the go and this presents challenges that don't exist with fixed assets tethered to a wired network. Administrators need control over who's using a device, through authentication that integrates with corporate directories for easier management. Control over which devices may connect, and the users who are authorized to use them. Control of access by specific applications, and over which networks. The ideal solution incorporates flexible policy control. Devices and users may be given a degree of freedom to access the Internet and use other applications. Or they may be tightly locked down so that only specific applications are allowed access, only over authorized networks, with enforcement via controls that cannot be bypassed.

User Experience

Foster User Acceptance and Manage Change

Mobile workers are like any other worker – their focus is on doing their jobs. If technology gets in the way or is too cumbersome to use, the entire mobile deployment may fail. Furthermore, the users themselves may introduce problems of their own making. Putting too many options in their hands might allow them to accidentally cripple their devices, open security holes, or bog down the access networks.

The best solution is one that requires minimal user intervention and makes the underlying technology as transparent as possible.

The best solution is one that requires minimal user intervention and makes the underlying technology as transparent as possible.

Make Wireless Network Use Seamless

Most mobile deployments require multiple cellular networks, often augmented with Wi-Fi access points, to provide reliable coverage throughout the organization's entire service area. Mobile workers shouldn't have to log in to separate networks, worry about making configuration changes, or deal with the other intricacies and complexities of mobile access.

Ideally the mobile environment mimics the in-office wired experience.

Ideally the mobile environment mimics the in-office wired experience. It furnishes a single sign-on; allows the worker to access multiple networks as though it were a single network; does it all within a single persistent session so workers only have to log in once; and pushes down any necessary configuration changes without user intervention. This user-transparent experience is also easiest for the IT department to support.

Deliver Seamless Access to More Applications

The number of applications and types used by mobile workers is growing, beyond scheduling and dispatch. More and more, customer and task-specific applications are being deployed that are an integral part of doing the in-field job. They can include CRM, work-order management, GIS and mapping, parts inventory databases and many more. Voice-over-IP, camera software and video software enable new capabilities for communicating from the field. These applications are rarely if ever designed with mobile access in mind, where connections break without warning (for instance, when a user goes out of range) which in turn makes the applications prone to crash.

The easiest way to manage the problem is with a solution that allows any software used in a LAN environment to be used in a mobile environment. It is also useful to prioritize application traffic that is critical or time-sensitive over less-critical traffic.

Business Operations

Gain Visibility Into Use of Corporate Assets

Investments in wireless technology including devices, networks and the supporting infrastructure are like any other business investment and it is important to know they are performing and delivering properly. An ideal solution will deliver visibility on three levels:

- **Real-time Visibility**: Real-time visibility lets administrator immediately see which devices are causing problems and take immediate action.
- **Proactive Alerting:** This critical capability notifies administrators that devices or users are in need of attention, so that IT personnel don't have to spend time watching for problems, but can focus instead on fixing them.
- **Reporting and Analytics**: This capability allows administrators and managers to see the big picture of service delivery, know when assets are being underutilized, and plan for the future.

Keep Wireless Access Charges in Check

As cellular carriers replace unlimited-use data plans with usage-based rates, enterprises face a new cost-control challenge. Analytics capability that monitors network use for appropriateness, combined with a finely-tuned set of policies, helps administrators keeps unnecessary tasks off of cellular networks. User-transparent connection management switches automatically to free or lower-cost Wi-Fi where it is available. And measures such as compression and link optimization can significantly reduce bandwidth consumption while improving performance.

It is important to know if your business investments are delivering properly.

An ideal solution will deliver visibility on three levels: Real-time Visibility, Proactive Alerting and Analytics.

Be Ready to Scale

For organizations that have overcome the preceding eleven challenges of a mobile environment, the twelfth is scaling the mobile environment. Successful organizations have often extended their original mobile deployments to new users, including additional classes of mobile workers and even executives, sales personnel and other "road warriors". While some of these users might be served by an SSL-VPN or IPsec VPN, their organizations have determined they can be more effectively served by a solution with the richer feature set and user-transparency afforded by a solution that handles the specific demands of a fully mobile workforce.

Conclusion

Managing an enterprise mobility deployment can be complex. The more the wireless environment can operate and be managed like a wired environment, the more likely it is that an enterprise mobility initiative will be successful.

About NetMotion Mobility

The challenges presented in this paper are drawn from the experiences of customers who have solved them by deploying NetMotion Mobility®. Mobility handles the unique needs for security, management and reliability of connections and applications in a mobile environment.

NetMotion® Wireless

Corporate Headquarters
NetMotion Wireless, Inc.
701 N 34th Street
Suite 250
Seattle, WA 98103

TEL +1 (206) 691-5555
Toll Free: (877) 818-7626
FAX (206) 691-5501
Sales@NetMotionWireless.com

European Headquarters
50-60 Thames Street
Windsor,
Berkshire, SL4 1TX
United Kingdom

TEL +44 (0) 1753 362228
EMEA@NetMotionWireless.com

WDS

Wireless Data Solutions
TEL 1300-937-469
Sales@WirelessData.com.au