

ENTERPRISE MOBILITY

Mobile Device Management Done Inexpensively

By Phil Lachmann

8/5/2008

INTRO

So many white papers go through the 'Total Cost of Ownership' of a mobile deployment and tell you that device management and support must be included in the final project cost for a complete picture. They are correct. What most whitepapers don't cover are the messy details that are involved in the management and support of the devices, and thus the potential costs that may be overlooked.

The significance of this oversight can be significant and put projects into dangerous cost overruns. After all, items associated with managing the devices are expensive, like additional staff, new servers, and whatever else the IT guys tell you they need.



According to the Information Week study noted above, more than half of the respondents with mobile solutions decided to forego the Mobile Device Management component with over 25% citing expense and over 44% citing staffing reasons. Both reasons actually boil down to cost. If you're reading this, then you are already ahead of these companies in learning how inexpensive this critical component can really become.

THE PROBLEM AREAS

Mobile computing projects often start out with such great enthusiasm about the potential savings in both dollars and man hours. At this point the only costs that have been considered are those of the mobile devices and the software. Often times it is only after the initial giddiness has worn off that companies realize that to implement the project properly they will need to manage, track, update, and support a new class of devices that the current IT staff has no expertise with. Beyond this is also the risk of taking potentially sensitive data outside the safety of the company's four walls. The problems can quickly stifle even the best mobile computing project.

The four most common problem areas involve device management, support, security and backup procedures. These are all areas of mobile computing that may have significant differences from the desktop environment. The challenge is to realize these differences and to apply the appropriate solution.

DEVICE MANAGEMENT

Like laptops and users workstations, mobile devices must be set up and maintained with the software and tools necessary for the user to work efficiently. Many companies have fantastic tools in place to make this happen within the four walls, but these tools and processes quickly fall apart when mobile computers are brought into the mix.

SOFTWARE UPDATES

The task of providing software updates to devices that are not always connected can be daunting and not always easily implanted. Critical updates must be applied in a timely fashion. Updates must be tracked. Users without updates need to be identified.

Device management tools currently have many great features to create update packages and track who has or has not received the updates. Users can be grouped so those like users receive the same software. Roles allow users to be setup in a different manner than managers.

Time windows can be set up so that updates are sent to the mobile device in off hours instead of during the work day when interruptions would be undesirable. If necessary multiple time windows can be set up to schedule updates around other events such as backups.

DEVICE ATTRIBUTES

Mobile devices have attributes such as current battery levels, net work addresses, SIM card status that may be important to see in near real time. Critical battery levels may necessitate action in the form of a message to the user to charge the device.

Today's device management tools present these critical performance indicators and more. Preemptive help can be provided to a user before a real issue arises, preventing potential downtime and lost revenue.

SECURITY

The red flags go up and the sirens start blaring and the internal controls staff gets really uptight when the idea of taking sensitive data into the field comes up. Data is the lifeblood of any company and needs to be protected and secured. The mobility of the data that so excited the operations staff, is what most concerns the management and controls people. The fears of the device being left behind or stolen from a vehicle are real and do occur.

POLICIES

The key is to know how to respond when bad things happen. Profiles can be set up to delete all data and wipe a device clean. When a device is identified as lost or stolen, the profile can be sent to the device to effectively destroy its contents and remove critical data.

Policies can also be set up to help protect against the unknown loss of a device. Devices can be set to connect with a preset time interval. If devices are not connected within the interval they are set to delete the contents. Thus if a device is used infrequently and it is misplaced, there are protections in place.

ACCESS

Access may generally mean the use of a password to use this device. Almost all modern management tools have password features. It is the baseline of access control and makes management feel that their data is protected.

Mobile devices have features that may or may not be desirable to give users access to. Restricting the use of features such as Bluetooth, built in cameras, or SD card access may fit into a company's general security policy.

The user may also be set to only allow access to a handful of key applications. Allowing users to see only what they need to see can greatly benefit user groups who are less sophisticated, and make the move to the mobile technology smoother. Restricting access may also be desirable for complex setups where user's access to connection settings is unwanted.

ENCRYPTION

Encrypting data is another feature that has come to be expected in almost every company's standard security policy.

Encryption setups with current management tools allow file and folder level encryption. Locations on the device that don't contain sensitive information can be left unencrypted for maximum performance.

SUPPORT

Even the best users will occasionally encounter a problem while in the field. Supporting a device that is hundreds of miles away and in an unknown state presents some obvious challenges. At times the problem is hard to convey to the help desk staff through a phone conversation. The solution may be to dispatch a new mobile device to the user, but this means that the user must stop working and wait until they receive the new device. The result is lost time and potentially angry customers.

The current generation of tools available to the help desk allows the technician to remotely connect to the device and provide real time assistance. When the technician can see the issue, the solution is often much more obvious. If a real time fix is available the user can continue working within a short time. Customers can be serviced without interruption and no shipping costs have been incurred unnecessarily.

BACKUP

The popular saying is that you are only as good as your last backup. Backups of devices that are not always connected can be particularly challenging. Devices connect at irregular schedules making it impossible to get a backup of all data at any given time.

Backups of key files and data can be done as users connect. Files can then be pulled from the device and placed in a traditional server location that is backed up according to company policies.

On device backups can also be made to the storage card to give the ability to recover from a device failure without data loss.

If a failure occurs devices can be reloaded with the backup files and the user is on their way without a significant amount of lost time.

OFFSITE OPTIONS

Of course all of this can be setup in house with a substantial commitment of both time and money. Outsourcing this type of work to a company who deals with mobile technology on a daily basis may provide both a cost saving and a compressed schedule for your mobile project. Offerings may include anything from just hosting the management tools, to a complete help desk offering.

SHAMELESS SELF PROMOTION

Enterprise Mobility offers complete management solutions for your mobile project. Hosting and help desk offerings are available at reasonable and affordable prices. Let Enterprise Mobility take care of the management and support of your mobile devices. Contact Enterprise Mobility at 1-888-478-4447 for more details or visit www.powerofmobile.com to see a complete list of offerings.