



A Laymans guide to Device Managment Part 1

Date: 27th July 2009

Website: <http://www.ruggedandmobile.com>

Learn with us blog: <http://blog.ruggedandmobile.com>

Innovation Twitter: <http://www.twitter.com/ruggedandmobile>

Facebook group: <http://www.facebook.com/ruggedandmobile>

Our forum: <http://forum.ruggedandmobile.com>



About Rugged and Mobile

What do we do?

Rugged and Mobile develops mobile, data and web solutions, delivering into the rugged, enterprise and consumer mobile markets. Offering end to end solutions our services include:

- Hardware reselling of rugged and mobile devices, selling anything from barcode readers to Windows mobile phones and supporting them.
- Bespoke software consultancy, delivering tailored software and project management into businesses. We deliver both Microsoft and Apple iPhone solutions.
- SOA/SaaS solutions, serving businesses and individual customers with new, exciting and flexible mobile services.

Our Culture

Rugged and Mobile is a newly founded company. We understand how to run a tech company right and how to treat the people within it. We work hard, we play hard and mostly the two are the same thing!

Company Vision

We want to become the leading UK provider of mobile solutions. We intend to do this by keeping at the forefront of mobile and data capture technologies, by providing excellent service to our customers and by employing the right people who can help deliver our vision.



Overview

Part of offering great service, in our view, is offering our customers the right software and management solutions to their IT and mobile platform. You might have the right hardware, the right software solution that's working for you but are you doing anything to keep track of and service all these new mobile devices that are flying around the country! One area in the mobile domain that I see lots of confusion in, is how to look after and manage devices that are working remotely. I've worked with many Device Management companies employing their products into both large and small platforms and I'll be totally honest when I say this; All the options out there currently bring a lot of issues with them. They're either too technical and resource intensive for customers to install and run or they're too costly as vendors take advantage of an ill-educated market.

This article takes a look at Device Management (DM) and gives the lay person a chance at understanding what is it they need and how easily they can manage devices and data that are essential to their business.

In Part 1, we take a look at the market and why DM is needed and take a look at some of the challenges we face in employing a DM solution.

Part 2 looks at the benefits of DM

Lastly Part 3 looks at the options out there and why we feel we could have an exciting new option for our customers.

So onto this section...

Part 1 – What is Device Management?

It's estimated that approximately 70% of business data typically now exists on various mobile based equipment of some kind, whilst at the same time about the same percentage of businesses leave the responsibility of security up to the user or don't think about it at all. At the very least, valuable names, addresses and PIM data such as birthdays and travel arrangements are pretty much uniformly saved to business phones. However as the drive towards data capture in the field gives us fantastic new services, it also means the risks increase as more and more data is required and generated in the field.

Take a typical parcel delivery application. Now we don't want to go into the ins and outs of how an application of this nature is actually written but just think for one moment about what kind of data the device could have stored on it. In the case of customer data that it must keep secure, it will have:

- Names, addresses and possibly contact numbers
- Parcel details
- Signatures in the event of delivery proof made
- Photos of front doors in the case of non-delivery



- Details of alternative delivery instructions
- Whether the person will be in or out at a particular time

And in the case of business data:

- Parcel itineraries
- Driver data
- Business contact information
- Messaging data
- Wireless/3G connection access
- GPS tracking data
- Telematics data

The list could go on but the point being made here is that in the case of the delivery company this is all stuff that you would hate to get into the hands of your competitors and in the case of the customer, this data could severely put your personal data and even home security at risk.

Not enough businesses are doing what they should be to keep data secure and this article takes a look at device management, what it is, the reason we need it and the challenges it faces. It then looks at why we need to seriously think about it in this day and age and finally takes a look at what you need to do to keep your data secure. Surprise, surprise there is also a look at our own Management application and why we feel there is simply no excuse to not employ device management in your company any more.

What is Device Management

Device Management (DM), in a nutshell, is ensuring that your business can see, connect to and then manage in some way a device that it owns. Some of the areas DM should address can be seen below:

Provisioning

This is about providing the user with an easy way to upload required data, applications and settings to their device whether new or ongoing. It takes away the laborious task of setting up a device every time it is needed and it also provides a more secure way to update settings on live devices. No more carrying around that WPA key on a piece of paper!

Security

DM can also cover many aspects of security. Ensuring data security travelling to/from the device can be managed by a DM service, setting passwords, locking a device down in a "Kiosk" fashion or when all else fails, wiping a device remotely when needed.

Asset Management

It should allow IT Managers to be able to group and manage their device family better so that they do not lose track of the devices they should be managing. Making changes to groups of devices should be easily accomplished and tracked so that settings and status' can be understood at a glance. Its no good having a DM service if IT can't use it easily.



Monitoring and Support

Devices with a problem could easily alert the DM central server. Whether this is a reboot, a failure of some kind or a simple notification of battery levels it can be used to prompt and aid the support teams.

Remote access

Remote assistance could be in the shape of a remote helper application that can help walk-through users through a particular application or it could allow support teams to browse the file system and get hold of dump files.

Location

Location is becoming the next big thing in DM and along with a whole host of other interesting services, knowing where a device is can be critical in supporting or knowing whether the device has been lost or stolen early on.

User Behaviour

Key metrics can be stored and sent back to teams in order to view user and device behaviours. Do your van drivers use the charging cradle? How many batteries go flat in the day? What kind of call/SMS usage are your phones experiencing?

These are just a few of the key areas DM should address. You could also manage software licenses and distribution and by doing so you will be on the road to keeping your devices safe and more importantly your business and customer data secure.

The challenges of Device Management

For years we have seen our friendly neighbourhood IT Managers lock down and control our PC's or laptops. Nearly all of these have Windows on them of some flavour and typically they will connect through a certain firewall/gateway or server. So why do companies fail to employ a DM service for their remote mobile devices? At Rugged and Mobile we see the same problems and hear the same excuses time and time again! Lets look at some of these challenges (or excuses!) in more detail:

Too expensive

Your right....until now!! Typically DM services have been very expensive to buy and then you find that its only half the story. You have to maintain the service yourself, get tied in and then be subject to costly updates, support and training needs. It seems that employing something that really should be integral and key to keeping your customers and your own business data safe is just out of reach of most businesses.

It's way too complicated

Again, you're right until now!! Most DM services require you to install different client applications for different devices, you need to buy costly servers and install complex server software, maintain secure communication between your solutions and then have people to learn, run and administer a system that constantly requires updating. Installing and running a classic DM system can be very complex and this is when everything goes to plan!



Wouldn't it be nice if there was a true SOA DM service on the market, meaning you pay for what you use, you don't have any set-up costs or administration worries and you just have to install the client application and you manage your family of devices.

My DM system is too old and insecure

Data security protocols are changing all the time in the fight to keep our data secure. Your DM System will inevitably become out of date and you'll need to go through the rigmarole of pulling out and then installing a new system. Some companies have gone through this process and simply give up in the face of locked in, aging software that requires costly licenses updating before anything can be done with it. Surely you need a DM tool that uses the most up to date and appropriate ways of keeping your devices secure without exposing you to the risks or complexities of keeping it that way?

We just don't understand the need for DM

Everything's been fine up to now why do we need to bother with it? Well we see so many businesses with this attitude, completely disregarding what could happen in the future and at the same time completely ignoring the fact that a mobile device can be anywhere and in any situation despite the rules and regulations they may set to their users. I've personally seen devices being left in cars (Because they're too big and the company will pay for it if it goes missing!!) I have also seen phones being taken out to pubs/bars at the weekend. No-one uses a mobile device as it is intended!! As Mobility becomes central to our work and personal lives, we need to ensure that we start to look after the data and devices that we own. Things may have been fine up to now but will they in the future as hackers and thieves turn their attention to mobile devices.

There are also lots of technical challenges we have to face to:

- Devices have limited bandwidth and could run out of bandwidth.
- What protocol do you use to communicate with the device? GPRS/3G, SMS, MMS, WiFi or even GSM. What happens when 1 or more are available? What if the device is cradled or connected to a laptop?
- Mobile devices have unreliable, intermittent and slow connectivity (At best!!). What happens when you drive through a tunnel mid-way through an update?
- Absolutely no local support will be available unless you are Bill Gates and can afford to have a personal support bod follow you around everywhere you go!!
- There is an astonishing variety of client platforms that you have to consider. It's not just about Windows, Linux and OSX. Nokia, Blackberry, Apple, Android and even Windows mobile/CE devices can be flavoured differently device to device as can OS40/60.
- Mobile devices can very easily go missing, whether lost or stolen.
- Battery life is a big issue. You can't rely on the power being on 24/7 like a PC can.
- And there's more...What happens if the SIM card is taken out? A new one put in? What happens if the device is stolen and rebooted or wiped by the thief?

You're probably beginning to see why so many businesses haven't bothered with DM systems. It's a potential nightmare and I have been a-party to some installations from certain companies where lots of money is spent and DM simply never works properly!!! However the risks of doing nothing are ever-increasing as hackers turn their efforts to mobile devices and mobile OS's as well as starting to see regulations now appearing in this world, forcing businesses to adopt some kind of strategy.



rugged hardware, solid service
rugged and mobile

Just stop and think for 1 minute. How damaging could it be to your business if a customer's data was stolen that resulted in some kind of personal loss to them. What if that customer complained to all sorts of blogs, forums, papers or simply to other people? Would you use that company after hearing about that? Chances are even 1 incident like this could impact your business very heavily indeed. It is time to act.

In the next part we lift the mood a little bit and start talking about all the wonderful benefits DM can bring you. Check back soon.....