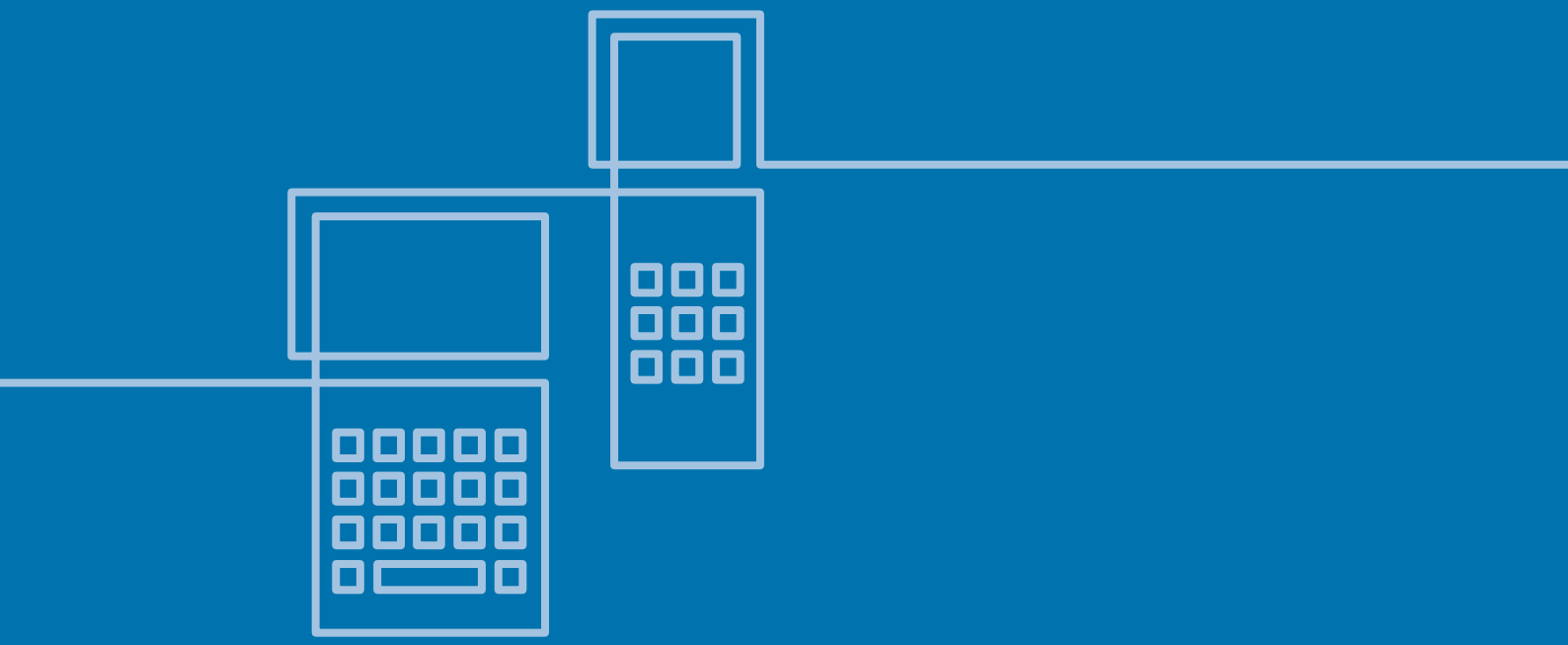
vodafone

Vodafone Global Enterprise

Mobile Device Management

Technical paper

power to you



Introduction

Managing for the future

Secure control over your mobile data, devices and applications.

The multi-national business must manage a fleet of devices including PCs, laptops, printers and bespoke machinery on a daily basis.

They are managed because each is an integral part of a functioning business and as such their efficient use, maintenance and security feeds directly into the company's performance.

However, when it comes to the mobile device in the pocket of employees, frequently this management fades.

Historically this situation may have been acceptable. As recently as six years ago a mobile device was a simple communication tool with voice and possibly text functionality, without any data exchange and processing power.

Today, the mobile devices in the hands of executives are small, handheld computers that house contact databases, email, enterprise VPN connections, mobile business applications, spreadsheets, documents, presentations and more.

Most importantly these devices are generally used at the leading-edge of the business, helping to ensure that employees are responsive and connected.

Their management has now become business critical.

However organisations have typically lacked any sort of inventory and asset management for their mobile devices.

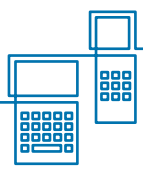
Management challenges

The effective day-to-day management of mobile devices presents unique challenges:

- Mobile devices, unlike most personal computers, come in a variety of forms, vary widely in function and are often based on different and fast changing operating systems.
- The average life cycle of a mobile device is now below 18 months compounding the difficulties of underlying operating systems (OS's) and platforms.
- Corporate users expect user settings and email configuration to all be on the device before it even touches their hands, without manual intervention or hours spent on the phone with IT.

- Mobile devices have typically been adopted ad hoc. In short, few companies plan their adoption of mobile devices, they more often inherit a range of devices that – for one reason or another – must now be brought under control.
- During their use life, many things can happen to prevent the user's productivity from reaching maximum ability. If a device is accidentally hard reset, valuable data can be lost resulting in hours of recovery time and significant cost to get back up and running with the appropriate information.
- By definition mobile devices are in the field, outside of the physical control of the enterprise and are at greater risk of being lost or stolen which makes them a potential security risk.
- They can be easily dropped or damaged, which creates back up and replacement concerns and are physically separated from the IT infrastructure, making routine IT maintenance challenging.
- Many company employees rely on their mobile devices for conducting business outside the office. In fact, in the case of field service technicians and related positions, the mobile phone might be the only device they have. As such, these devices will need immediate repair or replacement in order to maintain productivity – and that repair/ replacement might need to happen "in the field" far from the corporate office.

From an IT perspective, mobile device management often embodies the ultimate challenge: how to bring an extremely diverse collection of devices that are physically disconnected from the enterprise under control. This document outlines our approach to simplifying the management of devices for the enterprise.



Device Management

A short history

The earliest device management solutions were developed by handset manufacturers to solve a problem that had come about thanks to the evolution of mobile phones beyond a point that original standards for GSM had envisaged.

The inclusion of technologies such as WAP and early data access through Circuit Switched Data (CSD) within handsets forced users to input settings that previously had not been needed. These settings were often difficult to find and complicated to input with mistakes easy to make.

Leading handset manufacturers were the first to provide solutions to deliver settings remotely over-the-air (OTA) using SMS. The rest of the industry soon followed. This ability to 'reach out' and in some way effect the device to the benefit of the user, is the essence of all device management systems.

These early protocols were expanded and extended by the various manufacturers until the WAP Forum (an early standards body for the mobile internet) looked to define an industry wide set of standards.

This effort continued when the WAP Forum was integrated to the Open Mobile Alliance (OMA), which now defines and standardises all such solutions for the industry.

Following these early solutions, the first IP-based standards using Sync or Synchronization standards were introduced. These standards at first achieved many of the same ends the earlier SMS based solutions, but did so over a continuous IP session with the device.

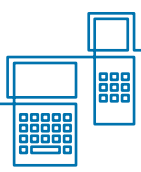
The OMA integrated the sync based standards and adapted them more specifically for the use of device management under the OMA device management working group.

The OMA issued its working papers on a range of device management capabilities and these were standardised.

At around the same time the SMS based protocols were integrated into OMA under a new working group called OMA Client Provisioning (OMA CP). This group moved to standardise the various protocols and released its OMA CP standards to which almost all devices now comply.

In parallel with the standards work, a number of what would become the industries leading suppliers and developers began to deploy solutions using bespoke downloadable clients.

These clients, common place in the PC industry, were deployed to early PDA devices and some of the first smart phones providing advanced control and management features.



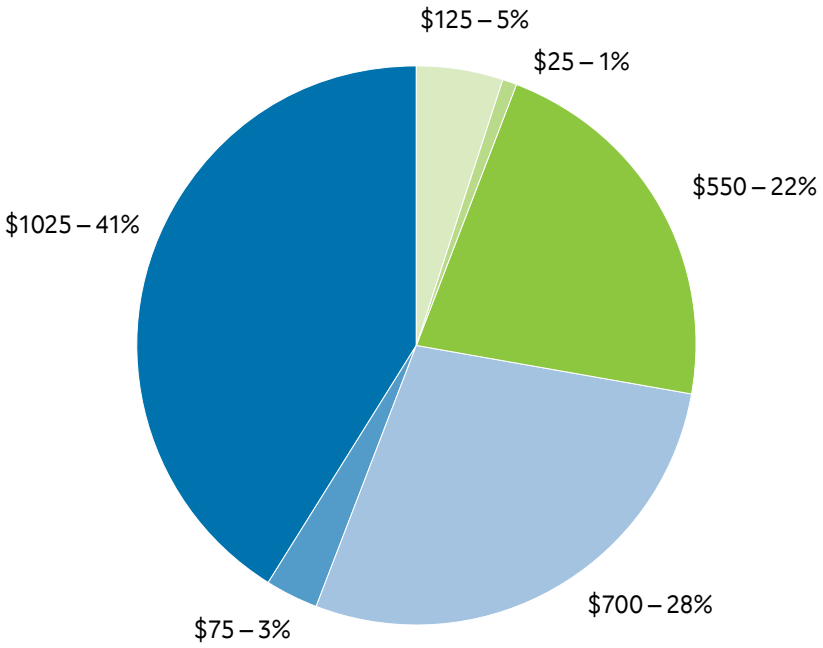


Figure 1. Breakdown of the total cost of ownership Source: Gartner

- Specific Wireless Software
- Server hardware for wireless software
- Mobile Equipment (including shrinkage)
- IT & Support Labour
- Training
- Wireless Services

Today OMA CP is in constant use around the world having been deployed on almost every network and device.

OMA device management is gaining fast with large deployments in Japan and the US. Bespoke clients continue to be the most capable in effect blazing the trail that the standards bodies then follow.

In 2008, the IDC analysed the total cost of ownership (TCO) of mobile devices, which had reached a figure of $2500 – $3000 per user in multi-national corporate businesses. Gartner produced very similar figures in 2007.

A breakdown of these costs is shown in Figure 1. The three largest areas of spend (representing 91%) are support, devices and wireless service.

Of these, device management has an impact on two of the top three areas, reducing support costs through efficient management and protecting equipment investment both through service and security.

Effective mobile device management enables the enterprise to lower the TCO of mobile devices. As with most IT management initiatives, the better control a company has over its mobile devices, the fewer employee and financial resources it must dedicate to supporting the platform(s).

A company that can readily and remotely lock, back up, wipe, initialize, restore and patch its mobile devices dramatically improves both its security in case of loss or theft, and its ability to keep devices current and consistent without disruption.

In fact, research indicates that, left to their own initiative, fewer than 5% of users employ even such minimal security processes as turning on password protection for their mobile devices. And significantly less than 5% of companies monitor and/or trace corporate data as it makes its way from the data centre to the individual users and their devices.

These factors can have a significant impact on overall corporate security, as it is not uncommon for a field team to have a 25%+ device loss/failure rate on an annual basis.

Similarly, the ability to quickly resolve problems means that devices are rapidly put back in service, or perhaps never have to leave in the first place. This ensures not only internal (IT to employee) responsiveness, but also improves external (employee to customer) service as well.

Device Management

Basic principles

Mobile device management typically includes some or all of the following capabilities:

- Remote configuration OTA – user and enterprise settings
- Wireless data back up and restore
- Remote software updates – user installed or administrator pushed
- Managed software catalogues and downloads
- Remote device security such as device lock, wipe and alert tone
- Remote administrator access
- Remote diagnostics and inventory
- Real-time registration.

Device Management solutions involve an exchange between a centralised server (running the management software) and the mobile device. See Figure 2.

In all cases there is a trigger for action. For example, this could be a user calling for help or a requirement for a bulk security update of some timed event.

The helpdesk, or with self care the user themselves, will initiate a device management session with the device (usually delivered by SMS).

If this is the first time the device has been contacted, the service will need to be setup using one of the following methods;

- For client based solutions, the device management client must be delivered to the device. This is achieved by sending an SMS with a link for a download or loading the application via some physical route.
- For OMA based solutions the device must be 'boot-strapped' to the server, that is linked to a specific server. In the main this is achieved by sending specifically encoded SMS to the device.
- In some instances the set up may already have been completed before the device was delivered to the user. This is possible for both client and OMA DM based solutions.

After the first time set up the help desk is able to reach the device using the device management service and perform the required action, for example adding an application or changing a setting.

The exchange is always the same, with the help desk sending an SMS to the device and the device responding to the request for action.

In some solutions the client on the device can initiate interaction with the server ie for timed actions or to check for updates.

At all stages the device will be communicating with a device management server of one type or another. In effect the required action from the help desk is translated into device management commands and delivered to the device by the service.

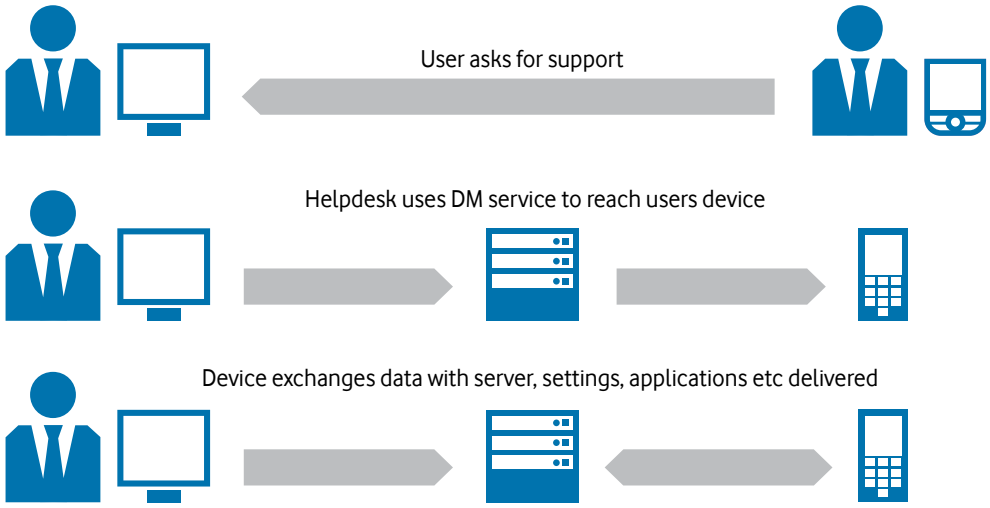


Figure 2. Basic device management exchange

User Experience

What the end user sees will very much depend on the device management service used and the specifics of the particular mobile device.

In many cases the customer would have the option to have operations on the device performed silently (ie without user interaction) or to display a user prompt asking for permission.

Management interactions require user interaction and certainly in all cases the user would be required to accept the initial set up process, be it the standards-based bootstrap or the download and install of the client.

Solutions

As detailed above, the primary differentiation within device management is proprietary client versus standards based. All device management systems support one or other of these basic options with a number supporting both.

Beyond the bespoke client versus standards split, there are two other key areas of differentiation:

'Platform-specific' versus 'Platform-agnostic'

Platform-specific solutions tend to be proprietary and client based, though there are examples where an initially standards-based solution has been extended in some bespoke and client specific way.

Examples of platform specific solutions include BlackBerry® Enterprise Server (BES) with its suite of device management techniques and iPhone with its application store-driven device update techniques. These platforms by nature are closed and tend to include both a server and client supplied by the one vendor.

Platform-agnostic can be both proprietary client based (though with limitations on device coverage) and standards based. Many of the leading vendors have now implemented standards based solutions that are manageable from multiple compliant device management servers.

Some of the device management server technology vendors have developed client based solutions that are platform agnostic in that they provide a solution for Windows, Symbian and some other emerging operating systems, for example Linux (Android).

These solutions are typically unable to support devices that are based on 'closed' operating systems such as those prevalent on lower end devices from Nokia, Motorola, Samsung and other manufacturers.

'Behind the Firewall' versus 'Hosted' or 'Managed'

'Behind the Firewall' solutions redeployed on the corporate network and can be platform agnostic or platform specific. Prime examples of this kind of solution are BlackBerry® using the BES and Microsoft® System Centre Mobile Device Manager (Yona).

The advantage of these systems is principally based on simpler integration from within the corporate LAN and an element of security control.

Disadvantages include the need to retain expert knowledge of the device management server environment and the difficulty in managing the rapidity of client side changes when new device packs may have to be added on a regular basis.

'Hosted' or Managed solutions are now available for most device management services.

Hosted solutions offer the device management features as a service normally via a web interface.

There is typically no need to mange the server environment and integrations with services such as SMSC's are provided.

Issues include the possibility that data flow between the corporate and the service may be limited by security constraints (eg active sync integration may not be possible within some security policies).

Industry Trends

The device management industry is now maturing with a marked amount of consolidation over the last two to three years.

A number of the original OMA CP vendors have been acquired. Some of the early OMA DM startups have also been acquired or have combined while some have been closed or failed. This trend is sure to continue.

OMA continues to strengthen though it remains weaker than the client based solutions. The trend is for client based solutions to add capability first and then for OMA to embrace and standardise that capability at some later date.

Generally, the industry has lost some of its start-up approach and is now consolidating both from a commercial and technical perspective. We would expect to see a continuing improvement in product quality and a strengthening of the key area of device support as the market moves towards a business as usual approach around known value add features.

Vodafone
Device Manager

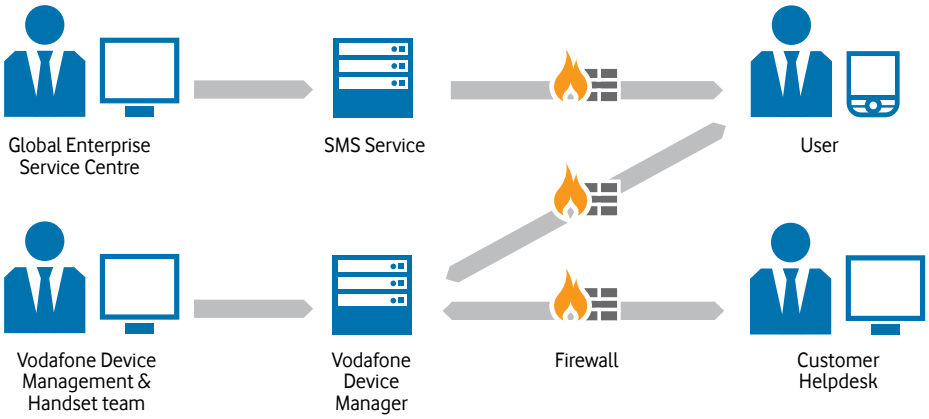


Figure 3.Vodafone Device Manager architecture

Key features include:

- Management – central management and inventory of all devices and software
- Security, including the ability to encrypt, force passwords, lock and wipe devices
- Deliver and manage applications
- Tools for diagnosing problems, sending settings and configuring devices
- Supports BlackBerry Enterprise Solution, Windows Mobile®, Palm and Symbian devices using the existing data connection across any network

Vodafone Device Manager is a hosted solution that enables multi-national businesses to remotely manage their device fleet, with IT managers able to send updates, troubleshoot, and lock or wipe devices over the air.

It requires no back-end server or additional software and is a simple and quick solution to set up and get running.

Carrier and manufacturer independent, Vodafone Device Manager enables you to intelligently configure, update and manage your mobile devices remotely.

Vodafone simply installs client software on the mobile device over the air so it can then be monitored and controlled remotely by your own IT help desk.

Vodafone Device Manager was built with a number of key principles in mind;

1. The service must be globally available.
2. The service must support all network both on and off the Vodafone footprint.
3. The service must support the widest possible set of devices whilst still offering features such as security, application management and settings support.

Based on these principles, Vodafone Device Manager has implemented a globally available hosted service using a client based technology vendor.

Figure 3 details the architecture at a high level. The service is available as a fully hosted and managed system.

Vodafone Device Manager manages the servers from within the Vodafone global data centres. New devices are tested, certified and added on a regular basis by the dedicated device team.

Vodafone Device Manager operates on all Vodafone networks and supports most mobile devices using BlackBerry Enterprise Solution, Windows Mobile® 5 and 6, and Symbian software platforms.

Vodafone Device Manager is an enterprise-grade, highly scalable solution that gives your IT help desk online access to the Vodafone Device Manager portal where they can view, interrogate and remotely control each of your organisation's mobile devices.

Summary and Conclusion

Mobile devices have become a mission critical function in running many businesses.

As the fleet grows and enterprises look to scale the use of mobile devices in their operational chain, device management will become a necessary enabler. The industry itself is still relatively young though the signs of maturity are there.

Vodafone Global Enterprise believes that its device management solution is well placed to meet growing corporate need and that the time for initial deployments is here.

The issues targeted are primarily on the cost side with lost working hours due to device problems the hardest to define but likely the most costly.

More quantifiable costs include the growth in IT support, lost and stolen devices and the logistics costs for manual solutions to application delivery or device updates.

Enterprises will need to decide on a device management strategy based on their own IT landscape.

For operations that utilise a uniform device fleet there may be a strong case for a platform specific solution where one exists. This would need to be balanced against the possibility of an expanded fleet range in the future.

For operations with multiple device types to support a platform agnostic solution, with the best feature to device support mix, would be most applicable.

The decision on hosted verses in house is largely down to costs sensitivity verses corporate policy.

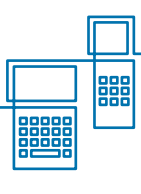
In the large majority of cases we have reviewed, the total cost of ownership for a specific service such as Vodafone Device Manager is lower for outsourced deployments.

Regardless of the approach taken there is a compelling case for deployment of a device management solution based both on cost constraint or reduction and enterprise wide efficiency gains.

To learn more about Vodafone Device Manager and how we can help you to successfully manage your mobile fleet please contact your Account Manager.

You may also find the following resources useful. They are available on the Vodafone Global Enterprise website (www.vodafone.com/globalenterprise) or through your account manager.

- **Developing your Mobility Strategy**
- **Securing your business mobility with confidence**
- **Mobility User Profiling – understanding your users and their needs**
- **Mobile Flexible Working.**



www.vodafone.com/globalenterprise

00028/10/09

vodafone