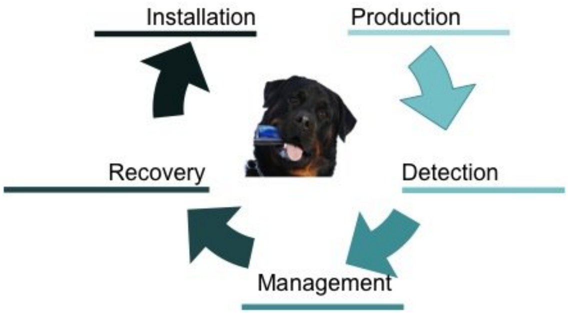
Fall 08

MobiDM COM

10 Reasons for Device Management



1. How to manage multiple mobile devices in a cost effective way.

The growing diversity in mobile platforms makes management and security more complex and results in more tools, knowledge and time, which in turn leads to higher costs.

Solution: MobiDM support a variety of mobile platforms, like Windows Mobile and Symbian. Therefore you get a clear and low Total Cost of Ownership, and a quick Return on Investment.

2. What to when a mobile phone is stolen or lost?

Confidential data will be accessible for unauthorized persons. How can you safeguard against unauthorized use of confidential data?

Solution: MobiDM uses *Data Fading* technology to ensure the confidentiality and integrity of the data on mobile devices, even when they are out of reach. Smart encryption technology guarantees the safety of the data on mobile devices.

3. Do you allow your end-users to install applications on their phone?

Devices become more vulnerable to viruses and malware, which leads to security breaches, malfunctioning mobile devices, more pressure on support and IT department etc.

Solution: MobiDM includes the Black/White listing and *Port control* functionalities, which makes it possible to block (external) applications and to let the mobile device only synchronize with trusted computers.

4. Do you allow your end-users to configure their own devices?

A faulty configuration causes disrupted mobile devices: no data connection, malfunction of mail functionality or malfunction of the mobile phone.

Solution: MobiDM includes functionality that makes it possible to block the configuration display and other settings from the end-users.

5. What to do when an end-user forgot the password of his mobile phone?

If the user initiates a Hard Reset, all data and specific settings on the mobile phone will be lost which will create unnecessary work for your support and IT department.

Solution: MobiDM includes a diversity of password recovery functionality, which also includes generating a temporary password function. The end-user is able to generate the recovery code on the portal.

6. Would you prefer to make a central backup of the data on mobile devices?

Confidential information can be lost and fall in the hands of unauthorized persons. The end-user is responsible for making a decent backup of the data.

Solution: MobiDM ensures centralized backup, which is automatic and provisioned *"Over The Air"*. The data will be preserved in a secured environment and can be restored quickly at any time.

7. Do you have standard procedures for Mobile Device Management?

From the moment that mobile devices are handed out till the moment of return, all mobile devices go through a complete *life cycle.* To preserve the integrity of mobile devices, there are few extra challenges that have to be solved. These procedures, if done incorrectly, can be time consuming and costly.

Solution: Installation is the beginning and the moment of return is the end point in the five phases of the *Life-cycle* process. Production, detection and managing are random tasks, which are continually being repeated. It is possible to assign different tasks to different groups/individuals, by using simple templates. You can be up and running with MobiDM within 15 minutes!

8. Do you want to limit your users in the amount of data traffic?

Mobile devices use more data, which leads to higher costs. Meanwhile the performance of the device is also being affected. This leads to low acceptation and inefficient use of the devices.

Solution: The data that is being send and for backup will be compressed to factor 6, which leads to a minimum of data use. In addition MobiDM also provides the possibility to maximize battery life, from a central console.

9. Do you want to encrypt sensitive data on your mobile devices?

Confidential information, if unencrypted, will be easy to access.

Solution: MobiDM provides security by intelligent file or full device encryption using intelligent algorithms.

10. Do you want your mobile devices to synchronize with unidentified computers?

Confidential information will still be accessible to unauthorized persons. This causes a major security breach.

Solution: MobiDM allows the possibility to manage the synchronization settings (USB or otherwise) wherefore the communication between the mobile device and the Exchange server can be enforced only *Over The Air* with a certificate. The certificate can be distributed *Over The Air* to the devices by Software Management.

Comparison

Features	Mobi-DM Full suite	Do it YourSelf Exchange2007
Self help	Portal interface & online manuals	
Templates	standard policies	
Security:		
PIM encryption	Yes	Yes
Smart file & folder encryption	Yes	no
Port Control	Yes	no
Remote lockdown	Yes	no
Remote wipe	PIN	Yes
Policy beheer	Yes	limited
Recovery code generator	Yes	no
Intelligent access control	Yes	no
Device Management:		
APN & communication settings	Yes	No
Device Inventory	Yes	No
Registry Settings	Yes	No
Software management:		
Software deployment & install	Yes	No
Software update	Yes	No
Documents deployment	Yes	No
Configuration management:		
Device configuration	Yes	No
Network settings	Yes	No
Backup & Restore management:		
Backup files	Yes	Only PIM Sync
Restore files	Yes	Only PIM Sync
Central management	Yes	Yes
Server infrastructure	Shared high availability environment	64 bit
TCO	Fixed fee per device	Variable
Installation / Roll-out time	< 15 min.	na installatie server & training
Technical knowledge	Beginner	Advanced
Platform support	Windows Mobile & Symbian	WM 5, WM 6, WM 6.1