

datasheet

A datasheet about

## MobiDM & iOS4 (iPhone 4 and iPad)

The Apple iPhone gained a strong position in the market. The Apple iPad – redefining the definition of a mobility device – is also clearly here to stay. Both devices fuel the 'bring your own' trend in which the user determines what device to use for private and business purposes at the same time.

As these devices are (partly) being used as business devices, many enterprises are deciding to deploy corporate apps on iOS4 and to start managing these mobile assets. As a result, some key questions emerge right away.

December 2010

## Introduction

The Apple iPhone gained a strong position in the market. The Apple iPad – redefining the definition of a mobility device – is also clearly here to stay. Both devices fuel the ‘bring your own’ trend in which the user determines what device to use for private and business purposes at the same time.

As these devices are (partly) being used as business devices, many enterprises are deciding to deploy corporate apps on iOS4 and to start managing these mobile assets. As a result, the following key questions emerge right away:

- Can we secure iOS devices according to the corporate policies?
- How do we deploy and manage enterprise applications on iOS devices?
- Can we protect access to corporate assets based upon device compliance?
- How to maintain corporate control without interrupting the user experience?
- Can we deploy and configure mobile device clients remotely?
- Which solution can manage all versions of iPhone (OS 3.x, 3GS, 4.0)?

Let us introduce you to MobiDM, the preferred enterprise mobile device management solution for iOS4 because of its effective, simple and secure capabilities.

## In a Nutshell

The MobiDM features can be divided into two categories, namely management features and security features. Each of the features will be explained in more detail. In short, the iOS4 Management Features are:

- **Enterprise Application Deployment:**
- **Device Management without user interaction**
- **iPhone End-User Experience**

The iOS4 Security Features contains:

- **Corporate Security:**
- **Accurate and up-to-date Asset Tracking Data:**

# Management Features

## ■ Enterprise Application Deployment

- o MobiDM allows delivering enterprise in-house apps Over-The-Air, providing distribution control and a reliable delivery.
- o The MobiDM Enterprise Appstore allows users to download both enterprise and suggested apps on the device through the MobiDM client portal.
- o Enterprise apps can be managed and enforced separately from user applications
- o Ability to revoke application usage remotely
- o Allows authorized apps to be assigned to different user groups
- o Supports both 'required' and 'optional' models for package deployment
- o Enables tracking and reporting of enterprise package installation

## ■ Device Management without user interaction

- o iOS management is part of the MobiDM multi tenancy group structure
- o Configuration profiles are now policies within MobiDM:
  - Create and edit configuration policies from the MobiDM portal
  - No longer requires iPhone Configuration Utility (iPCU)
  - Ability to import policies from iPCU in case that new policies are available before they are in MobiDM
- o Send OTA commands to erase, lock the device and reset pass codes using native Apple commands no longer requiring Active Sync
- o View and manage iOS devices in client data views:
  - Add, edit, delete client from within the MobiDM i/f
- o Integrated inventory views, log data and reports displayed in data views
- o If MDM relationship is terminated, managed applications are disabled, configuration data is removed from the device and managed Exchange account information and data is removed
- o Once a MDM relationship is established only that entity can manage the device using MDM protocol
- o Push configuration settings via MobiDM:
  - OTA delivery of APN settings
  - Ability to push Exchange settings to devices
  - Ability to push certificates to devices
  - Ability to set restrictions of apps
  - Ability to push Wi-Fi settings
  - Ability to push VPN settings

### ■ iPhone End-User Experience

- o Devices are provisioned using the SCEP protocol
  - MDM-config file sent to the device
  - User 'opts in' by accepting the MDM relationship
- o Continued management performed in the background without requiring user interaction
- o User can terminate MDM relationship:
  - Managed applications are disabled
  - Configuration data is removed from the device
  - Managed Exchange account information and data is removed
- o Applications are accessed through MobiDM portal

## Security Features

### ■ Corporate Security:

- o Devices can be locked and wiped remotely from through commands sent through the Apple push notification service
- o Pass code reset commands can be sent to the device requiring a pass code change
- o Policies and device configurations are reliably applied to the device with status being reported back to the server
- o Enterprise application usage can be revoked by removing provisioning profile
- o Removing managed Exchange credentials removes account and PIM data from the device
- o Able to gate access to Exchange email based upon device policy compliance, time, date of last client connection including jailbreak status

### ■ Accurate and up-to-date Asset Tracking Data:

- o Accurate and comprehensive asset tracking provides a real time view of current inventory and device status
- o Data is easily accessed through MobiDM portal
- o MDM allows a queries to the device that report the following information:



The screenshot shows an iPhone 'Info' screen with the following data:

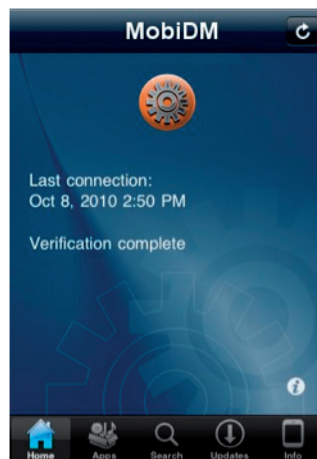
Device	
Name	QA iPod
Model	iPod touch
System Name	iPhone OS
System Version	4.0
UDID	c330d7ba4572323ea9d09c...
Battery Level	69%
Battery State	Unplugged
Multitasking Supported	No

Below the device information, the 'File System' section is partially visible. The bottom dock of the iPhone is also visible, showing icons for Home, Apps, Search, Updates, and Info.

Screenshot MobiDM Device Inventory

## How do I ... ?

- Enroll an iPhone or iPad:
  - o The user browses to a general activation website and logs in with a username and password. Device-type-detection is done here automatically.
  - o A policy is created which configures an trusted relation between the device and the MobiDM server; this must be accepted by the user once.
- Deploy the MobiDM (Afaria) client on iPhone & iPad:
  - o The user browses to a general activation website and logs in with a username and password.
  - o A button/link to the MobiDM (Afaria) client is provided, which can be downloaded from the Apple App store.
  - o After the MobiDM client has been installed, the same website provides a button/link to the configuration for the client. This must be accepted by the user.
  - o (the client can be manually configured on the device if required)
  - o The MobiDM client is optional, but provides:
    - Extra jailbreak detection
    - Enterprise App store: app selection, download and updates
    - Provides Exchange Access Control by optionally requiring the client to connect periodically



Screenshot MobiDM Client App store

- Use the iOS Enterprise App Store **(for customer administrator)**
  1. The admins can upload software packages to MobiDM and assign them to user groups.
  2. Enterprise Apps can be set to be mandatory or optional use
  3. The admin can add direct links to apps from the Apple App store, for which he thinks that they are of additional value for the end-user.
  4. Application updates can be send to automatically update existing software on the device.
  5. Apps, which need provisioning info, can be added as well.
  
- Use the iOS Enterprise App Store **(for end users)**
  1. The end user can open the Enterprise App store on the device, by opening the MobiDM/Afaria client app.
  2. The App store is divided in two sections: Enterprise and App store.

The Enterprise section has apps listed, which are only available to these end-users. Apps can be set mandatory by the admin or optionally.

The App store section list apps, which are a direct link to the Apple App store, which the end-user can download by himself.



Screenshot MobiDM Apps Inventory

- Distribute certificates for iOS4:
  1. MobiDM customer admin can add certificates to a policy, which can be pushed to a group of users.

For enhanced and user-specific certificate distribution there is solid plug-in solution available. For more information please contact us at [www.veliq.com](http://www.veliq.com) or +31 10 20 60 208.

# Feature list

Passcode Settings	WIFI Settings	Restrictions	Exchange
<ul style="list-style-type: none"> <li>• <b>Require Passcode</b> <ul style="list-style-type: none"> <li>• Allow Simple Value</li> <li>• Require Alphanumeric Value</li> <li>• Minimum Passcode Length</li> <li>• Minimum Complex Characters</li> <li>• Maximum Number of Failed Attempts – device is wiped</li> <li>• Maximum Passcode Age – in Days</li> <li>• Passcode Lock – in minutes</li> <li>• Grace Period for device lock</li> <li>• Passcode History</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Service Set Identifier - SSID of the wireless network</b> <ul style="list-style-type: none"> <li>• Hidden Network</li> <li>• Security Type</li> <li>• Password</li> <li>• Accepted EAP Types</li> <li>• EAP-FAST Protected Access</li> <li>• Authentication Settings</li> <li>• Identity Certificate</li> <li>• Certificates for validating the authentication server for the Wi-Fi connection.</li> <li>• Trusted authentication servers</li> <li>• Allow Trust Exceptions                             <ul style="list-style-type: none"> <li>• SSID</li> <li>• Hidden Network</li> <li>• Encryption Type</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Allow Explicit Content</li> <li>• Allow Use of Safari</li> <li>• Allow Use of YouTube</li> <li>• Allow Use of iTunes</li> <li>• Allow Installing Apps</li> <li>• Allow Use of Camera</li> <li>• Allow Screen Capture                             <ul style="list-style-type: none"> <li>• Allow Voice Dialing</li> <li>• Force Encrypted Backups</li> <li>• Allow Multiplayer Games</li> <li>• Set Safari Security Preferences                                     <ul style="list-style-type: none"> <li>• Force Fraud Warning</li> <li>• Allow Java Script</li> <li>• Allow Pop Ups</li> <li>• Accept Cookies</li> <li>• Allow inApp Purchases</li> <li>• Content Rating</li> <li>• Disable Push while Roaming</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Account Name</b> <ul style="list-style-type: none"> <li>• Exchange Active Sync Host</li> <li>• User</li> <li>• Email Address</li> <li>• Use SSL</li> <li>• Domain</li> <li>• Password</li> <li>• Credential Name</li> </ul> </li> <li>• <b>Number of Past Days to Sync</b> User is prompted for values not set</li> </ul>
VPN Settings	Email	LDAP/CalDAV/Calendars/Web Clip	Advanced
<ul style="list-style-type: none"> <li>• Connection Name</li> <li>• Connection Type</li> <li>• Server IP or Name</li> <li>• Account</li> <li>• Authentication Type</li> <li>• Shared Secret Entry</li> <li>• Send All Traffic Through VPN Setting                             <ul style="list-style-type: none"> <li>• Proxy</li> </ul> </li> </ul> <p>VPN's Supported</p> <ul style="list-style-type: none"> <li>• L2TP/IP</li> <li>• PPTP</li> <li>• Cisco IPsec</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Account Description</b> <ul style="list-style-type: none"> <li>• Account Type – IMAP or POP</li> <li>• Path Prefix</li> <li>• Account Name</li> <li>• Email Address</li> <li>• Mail Server and Port</li> <li>• Username</li> <li>• Use Password Authentication</li> <li>• Use SSL                             <ul style="list-style-type: none"> <li>• Incoming Username</li> <li>• Outgoing Username</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• LDAP Connection Settings</li> <li>• CalDAV Connection Settings</li> <li>• Calendar Connection Settings</li> <li>• Web Clip Settings</li> <li>• Certificate Payload</li> <li>• SCEP Payload                             <ul style="list-style-type: none"> <li>• CardDAV</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>APN</b> <ul style="list-style-type: none"> <li>• AP Username</li> <li>• AP Password</li> <li>• Proxy Server and Port</li> </ul> </li> </ul>