User Manual

Netcentric Mobile Device Management (MoDM)

T-Systems International GmbH

Date: February 03, 2012

Editorial details

Published by	T-Systems International GmbH

Document name	User Manual_MoDM_T-Systems.docx
Version	1.0
Status	final

Contents

1 Introduction

Netcentric MoDM offers mobile device management for any device or any platform from a single portal. Users can access to the portal, if the administrator has provided them with the correct login details. The portal shows information about the device and as a user a few actions can be initiated (e.g. Remote wipe).

1.1 Help files & Tooltips

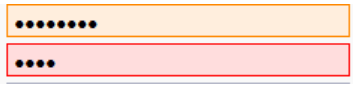
Netcentric MoDM provides much of the information regarding using the portal within the portal itself. In the portal help files are available, indicated with question mark icons and tooltips .

- Help files provide information regarding relevant screens or panels. They describe procedures, steps and further information about settings, tasks or groups. From time to time references are made to the Netcentric MoDM Wiki pages.
  All the help file information is content related and only shows information regarding the current actions or screens.

  To open the help file simply click on the icon, this will open a new screen.

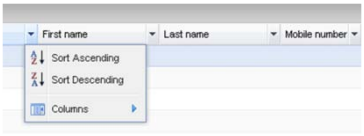
- Tooltips provide lines of text with information regarding a specific field or reference. A tooltip is displayed the moment the mouse hovers over the icon and closes again when the mouse pointer is moved away.

Fields coloured orange are mandatory fields. The correct information must be entered here. Sometimes information is required in a specific format. The tooltip at these fields provides additional information. If a field changes from orange to red, the information entered does not conform to the required format. For example when confirming a password the two values entered may not match. When attempting to save the screen error messages warn about incorrect details.



1.2 Filtering

Lists or overviews can be ordered per column. Simply click on the small triangle at the end for the column name. A submenu opens offering the option to sort the column in ascending or descending order.



Note: This filter is not available for all columns.

2 Getting started.

Browse to the portal using an Internet browser. Browsers currently supported:

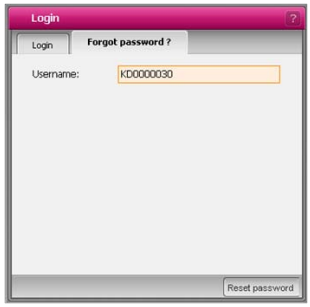
- IE 8,9
- Firefox 3,6 – 8
- Chrome 16

The login screen already provides some options. Select the desired language. Currently German, English and Dutch are supported languages. Changing language is also possible after logging in.

The credentials for logging in have been provided to you by your partner or supplier.

2.1 Forgotten your password?

If you have forgotten your password there is a procedure to reset it. You need to know the username and the correct answer to your security question (security question and answer are defined in your profile). Select the tab 'Forgot password?' Fill in the username and click 'Reset password'. Answer the security question resets the password. The answer to the security question needs to have been answered at an earlier stage in the password (e.g. within first enrollment). If the information is unknown contact your administrator to reset the password for you.



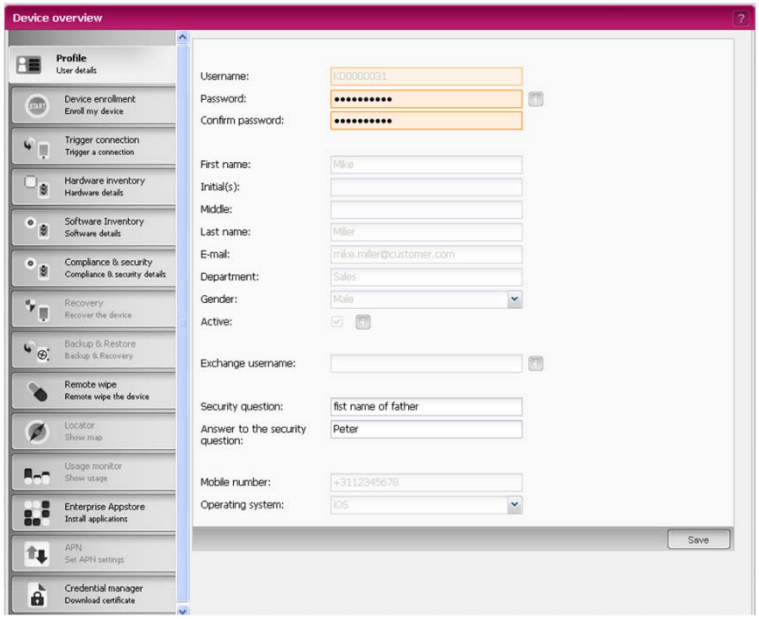
2.2 Opening screen

After logging into the portal the "Device overview" screen is displayed. This screen features a number of tabs on the left site, with relevant information or input fields on the right. Tabs that are not available are greyed out. Not all features are available for all types of operating systems on the device.

3 Explanation of the tabs.

3.1 Profile

This tab shows the various details available for the device. Some of the fields can be altered. Most fields are fixed and can only be altered by the portals administrator.

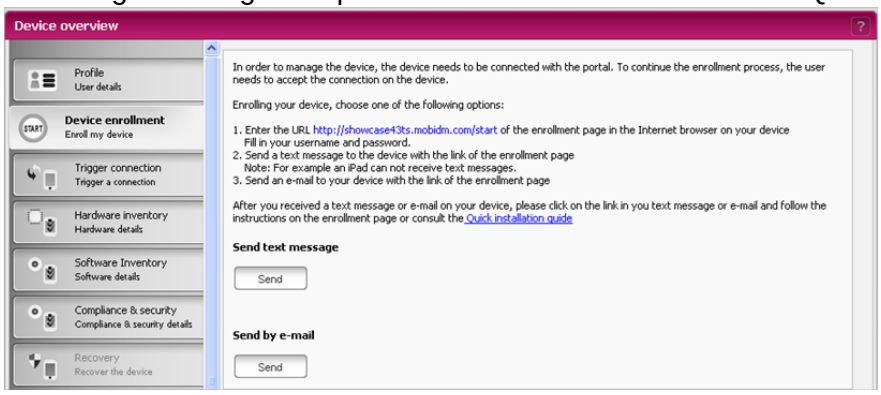


Fields to be changed by the user are: Password, Security question and answer.

It is important to enter information about the security question and its answer. This enables the option to recover a password in case it is forgotten. Enter a question in the first field for example: 'My mother's maiden name was:'. Next enter the answer to the question. This question is presented when attempting to recover the lost password. (See chapter 2.1. Forgotten your password)

3.2 Device enrollment

Before the device can be managed through the portal it first needs to be enrolled. Quite often the enrollment procedure will be started by the administrator but it can also be initiated by the user. For example to reenroll a device after it has been wiped, or in case of loss or theft, to enroll a new device.

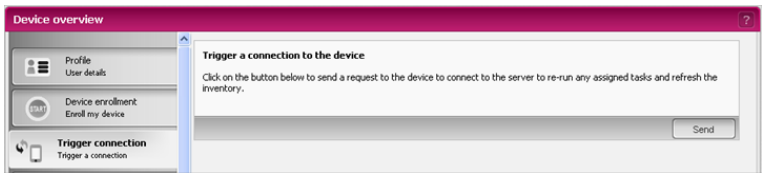


If the device that needs to be enrolled uses a different operating system than shown in your Profile, contact the administrator to change it. Do not attempt to enroll a device with an incorrect operating system.

To enroll the device, select the tab "Device enrollment"and click one of the "Send" buttons in the screen. Devices able to receive a text message can use the enrollment procedure using information in a text message send to the device. Devices able to receive only email can us an enrollment procedure from an email message.

For details on how to enroll a device see the Quick guides for device enrollment for the type of device or operating system on the Wiki.

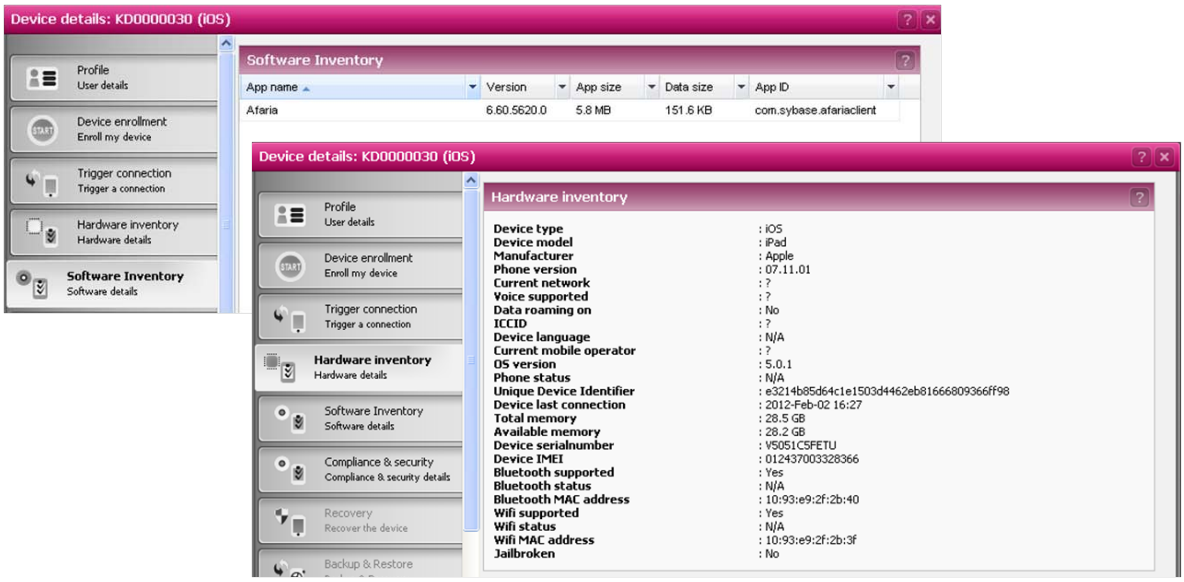
3.3 Trigger a connection



This tab is not available for all operating systems. If it is available, for example for iOS devices, it triggers a connection from the device to the portal. Simply click 'Send' to send the command to the device. This may be used to update information or details immediately instead of waiting until the next automatic connection (Heartbeat).

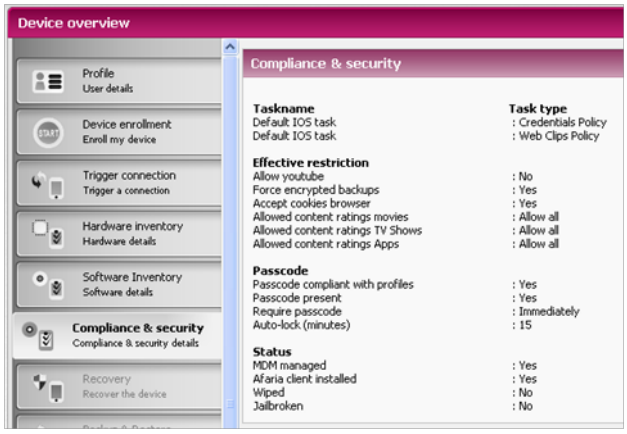
3.4 Hardware & Software inventories

These two tabs list an inventory of the available hardware on the device or the software, including installed Apps etc. The device must be enrolled first before this information can be retrieved from the device.



3.5 Compliance & Security

The compliance and security feature is available only for iOS devices. Under the device details a new tab is added showing the current state of the security settings, if the device complies with the passcode policies, the iOS tasks assigned to the device and its current status.



Tasks:

Even when tasks are created, activated and attached to a group does not ensure that is actually executed on the device. For example when a device has lost its connection with the portal the regular heartbeat may not be able to update settings or tasks. The Compliance overview shows which tasks are active on the device.

Effective restrictions:

When restrictions are set for a device this topic provides a clear overview of the restriction that is actually active on the device. In case of problems using applications or questions of users this overview can clarify why certain apps or downloads are rejected. It also allows the support staff to identify potential issues and change the required settings if necessary.

Passcode:

The passcode has several settings defined in the Configuration task. This overview lists the passcode settings for this device. Providing a quick overview of the passcode requirements in case of questions by the user or to solve any problems that passcode settings may cause.

Status:

To see if a status of a device a number of important management details are provided. For example it can be important to know if a device has been jailbroken or not. Or in case of management issues it shows if the Afaria client is actually present and installed on a device. In this overview is also shown if a device has been wiped.

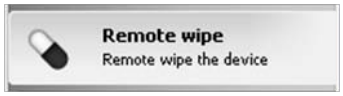
3.6 Recovery

Only available for Windows Mobile and Symbian. If the administrator has set a security profile of 1 and higher and you have forgotten the access code for this security profile on the device, it can be reset using a reset code. On the device use the menu option in the log-on screen. For Windows Mobile choose the option; “I forgot” (Windows Mobile) or for Symbian the option “recover password”. A so-called Device Key is generated on the screen of the mobile device. Enter this code here and press ‘Generate recovery code’. Enter this recovery code on your mobile device. Choose a new password to regain access to the device.

3.7 Backup & Restore

For Windows Mobile and Symbian devices it is possible to create a backup of contacts and/or folders and/or sub-folders of the device. Earlier backups can be restored to the device. Backup and restore tasks defined by the administrator are listed below. Check the checkbox in front of the backup task and select the desired backup or restore function below, by clicking on the appropriate button.

3.8 Remote wipe

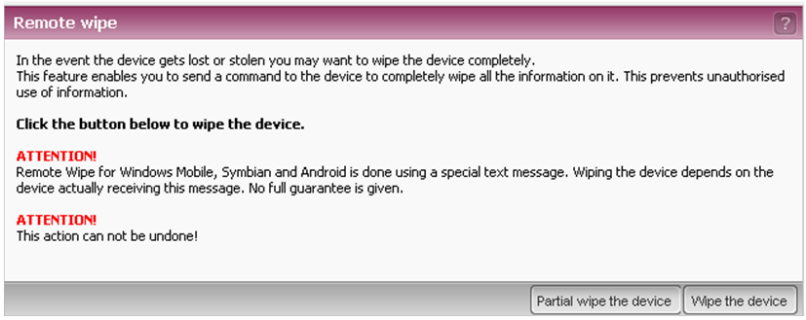


Devices that are lost or stolen can be wiped remotely. This feature uses a special text message.

For iOS there is the option to completely wipe the device or to select a partial wipe.

The complete wipe clears all data on the device (inclusive Apps).

The partial wipe only removes the trust by removing the payload.



Note: A device wipe or a partial wipe cannot be undone. Once the command has been sent, the device will be wiped as soon as it receives the command.

ATTENTION!
Remote Wipe for Windows Mobile, Symbian and Android is done using a special text message. Wiping the device depends on the device actually receiving this message. No full guarantee is given.

3.9 Locator

This tab shows the approximate location of the device. This is not available for all types of OS.

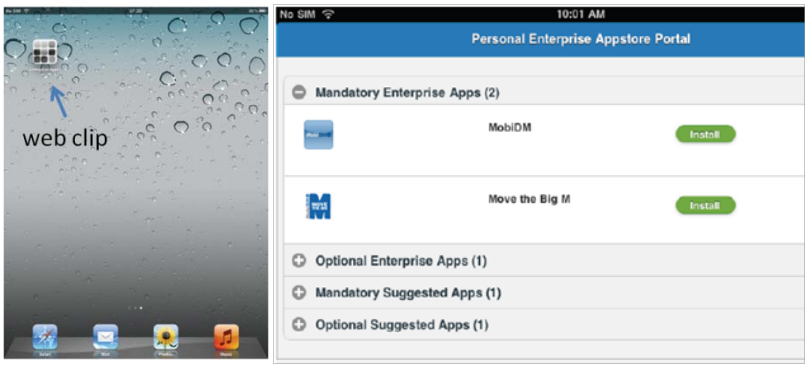
Disclaimer

There is a privacy law that applies to the Locator functionality. This legislation requires that the employees (users) must be informed if the device location data can be used by their employer. Employees must grant explicit permission to do this and must also be able to opt out. The employer is responsible for complying with these privacy laws.

T-Systems is not liable for claims arising from the inadequate compliance with this.

3.10 Personal Enterprise Appstore

To install applications from the Personal Enterprise Appstore on an iOS device, a dedicated web clip is necessary. Enterprise apps will be provided via this web clip. The web clip will be installed during the enrollment of the device.



Open the web clip on the device and click “Mandatory Enterprise Apps” or “Optional Enterprise Apps” to see what your administrator has made available. The available applications are listed there, and can be installed on your device.

The Personal Enterprise Appstore provides also a list of the suggested Apps.

3.11 Usage monitor

For Windows mobile devices a separate usage monitor is available to report the data usage as stored on the device.The device logs the usage of voice, data and text messaging. Data usage is logged per day, together with the used APN and roaming information.

3.12 APN settings

This tab shows the settings to connect a device to a Wireless network.

3.13 Credential manager

The Credential manager connects to a certificate authority server of the customer organization. The Credential Manager tab is already prepared in the current version of the portal, but cannot be used by today.