

Active Directory Integration Mobility & Care Manager

M-000023.en – 1.0.0

Content

CONTENT.....	2
1. SCOPE.....	2
2. TERMS AND ABBREVIATIONS.....	2
3. PREREQUISITES.....	2
4. CONFIGURATION.....	3
5. TESTING.....	8
6. ADDITIONAL OPTIONS.....	9

1. Scope

This document describes how to integrate an existing Mobility & Care Manager installation with the existing Active Directory to enable Single Sign On (SSO) for the Mobility & Care Manager application.

2. Terms and Abbreviations

Term	Meaning
MCM	Mobility & Care Manager
AD	Active Directory
SSO	Single Sign On

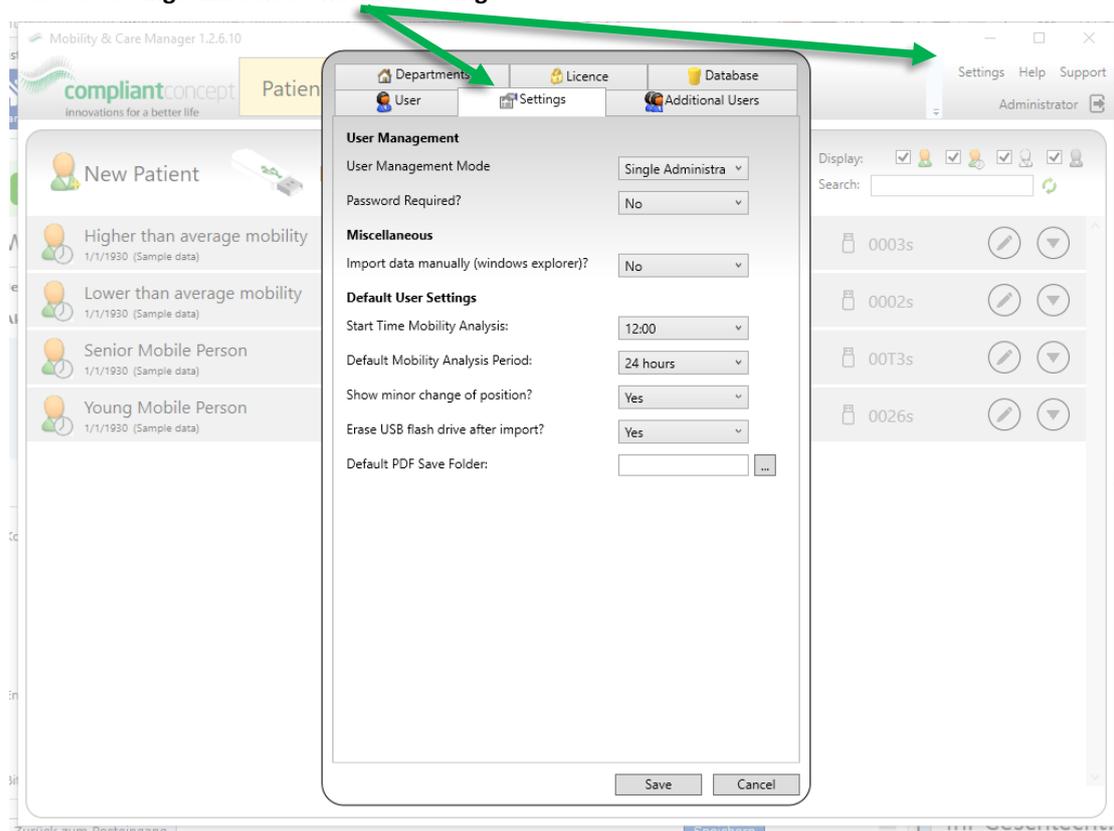
3. Prerequisites

- 3.1. MCM is installed and connected to a database. MCM must have revision 1.2.6.10 or higher.
- 3.2. AD Domain is properly set up.

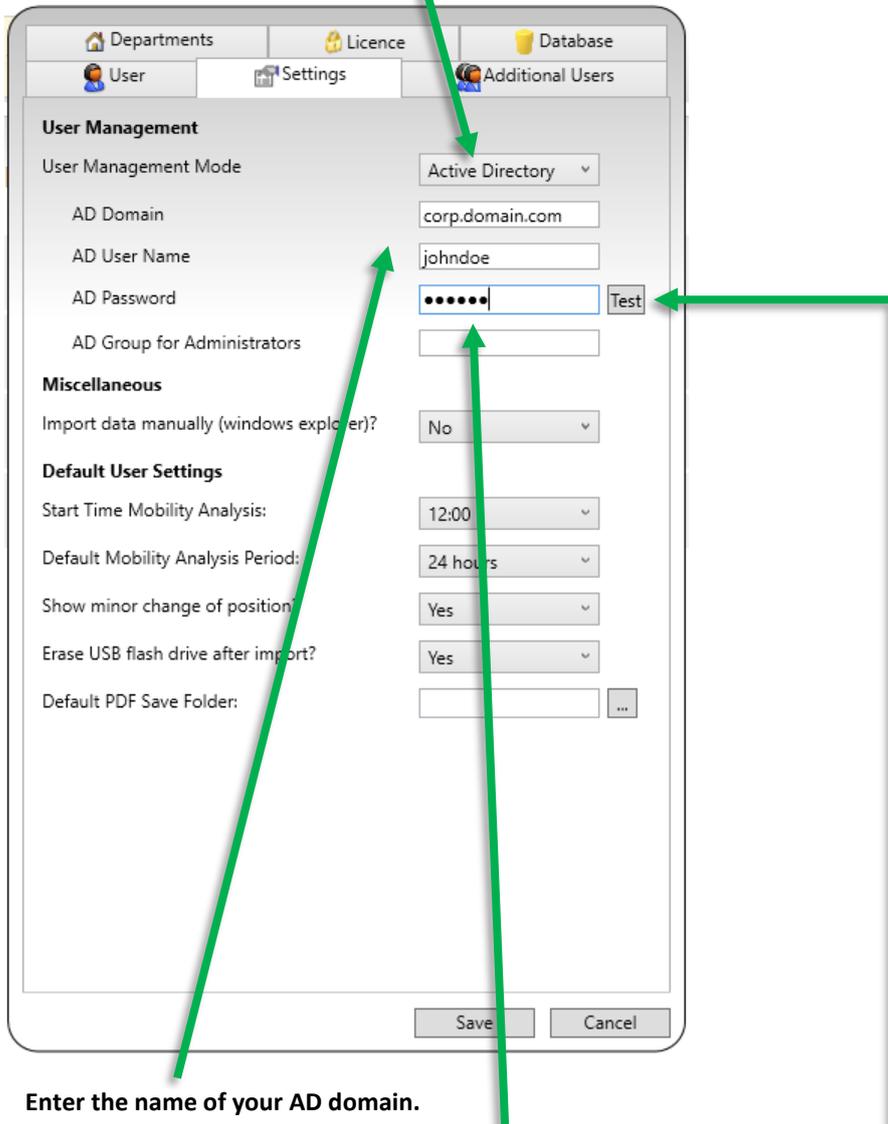
4. Configuration

4.1. Connect with the Active Directory

1. Start MCM and log in as Administrator if multiple users are configured.
2. Go to Settings and select the tab "Settings"



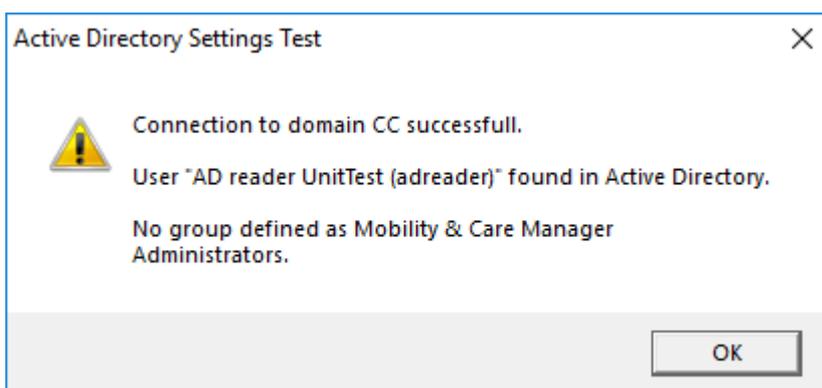
3. In the *User Management Mode* drop down select *Active Directory*



The screenshot shows the 'User Management' settings dialog. The 'User Management Mode' is set to 'Active Directory'. The 'AD Domain' is 'corp.domain.com', 'AD User Name' is 'johndoe', and 'AD Password' is masked with dots. A 'Test' button is visible next to the password field. Green arrows point to the 'Active Directory' dropdown, the 'AD User Name' field, the 'AD Password' field, and the 'Test' button.

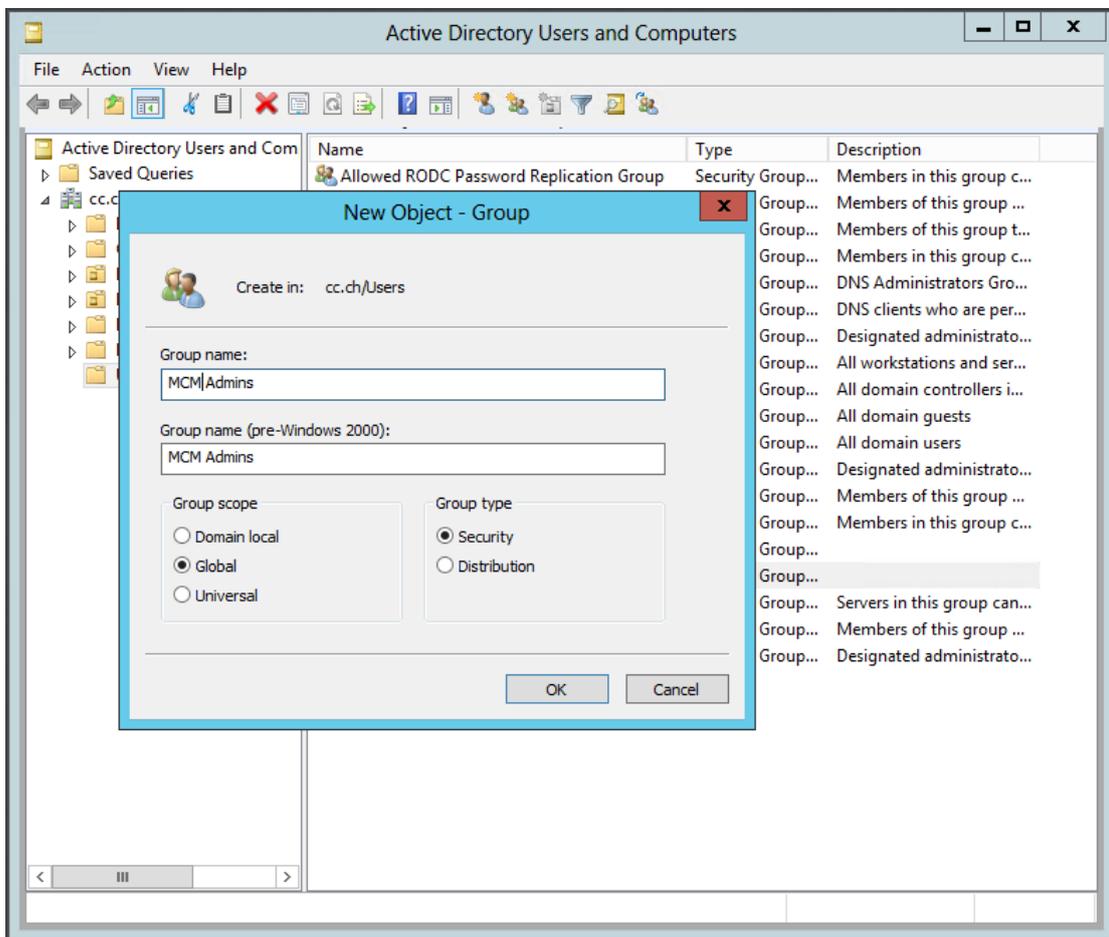
4. Enter the name of your AD domain.
5. Enter an AD user name (login name) and password.
This user is needed to read from AD.
6. With the *Test* button you can check the configuration.

The result should look similar to this:

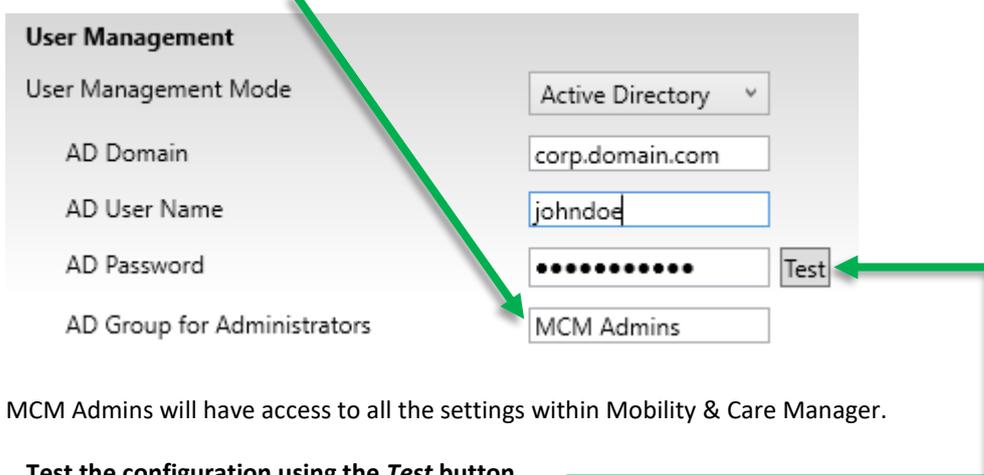


7. In AD create a user group for MCM administrators.

In the example the group is named "MCM Admins".



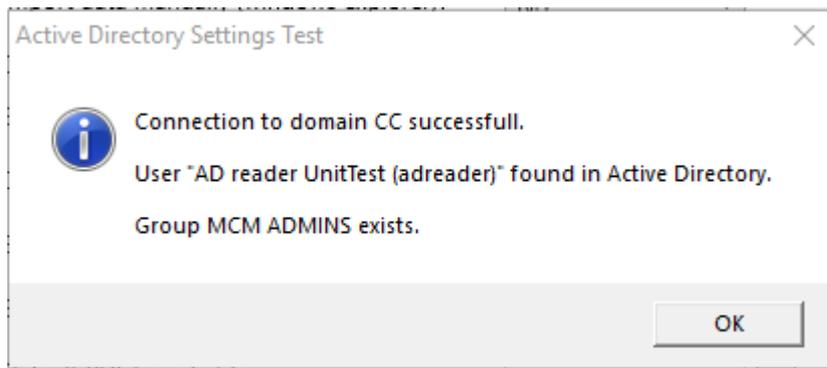
8. Enter the AD Group for Administrators in the MCM Settings window



MCM Admins will have access to all the settings within Mobility & Care Manager.

9. Test the configuration using the *Test* button.

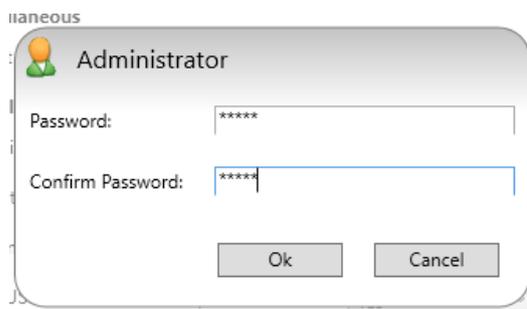
The result should look similar to this:



10. Push the *Save* button on the bottom of the Settings window to store the configuration.

All settings are stored in the MCM database. So the settings are persistent across multiple client installations.

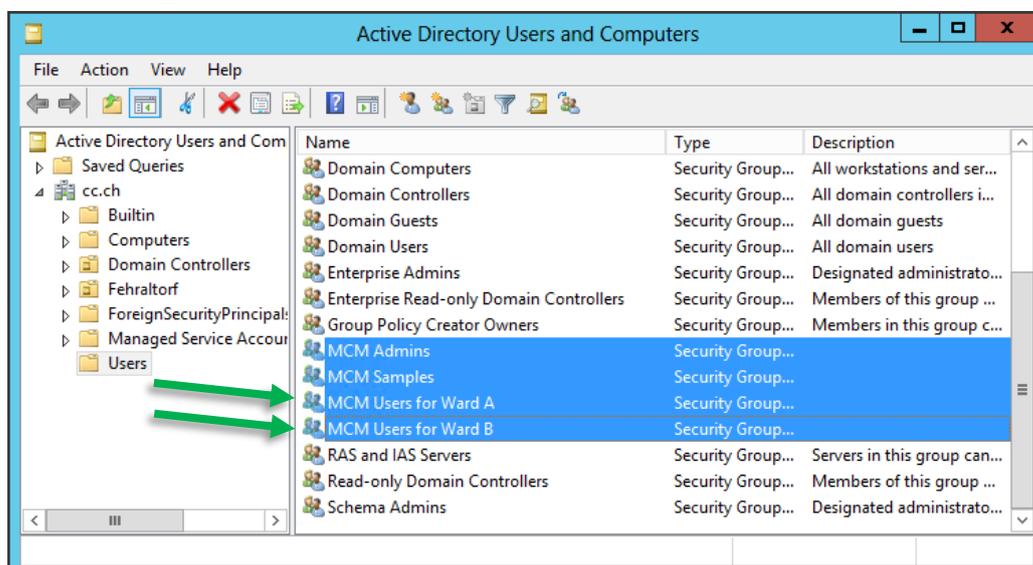
If you don't have set a password for the local application's Administrator user, then you are requested to choose a password now:



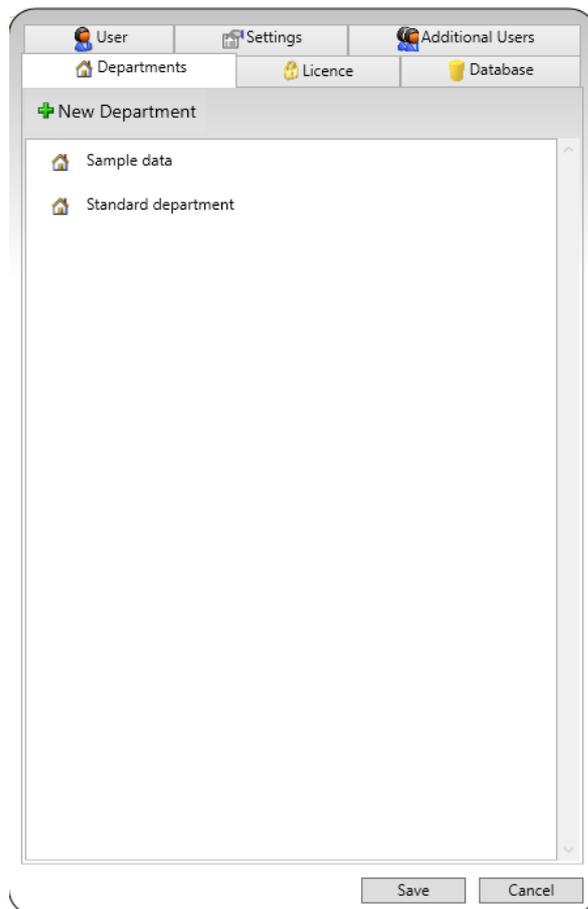
4.2. Restrict user access to patients of certain departments

Proceed with the following steps if you want to organize patient data into several departments and restrict users access to departments based on AD groups.

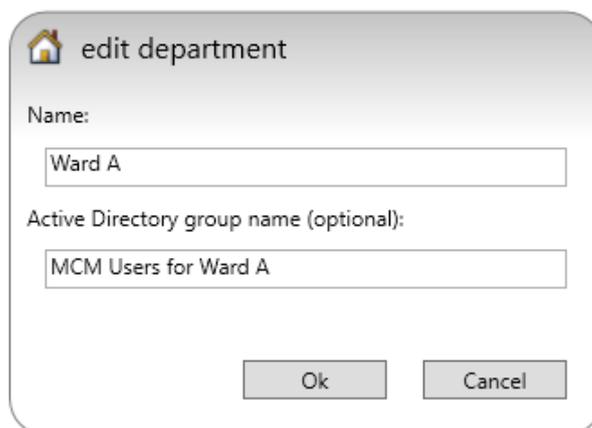
11. Create AD groups for every department.



12. In the MCM Settings window go to the *Departments* tab.



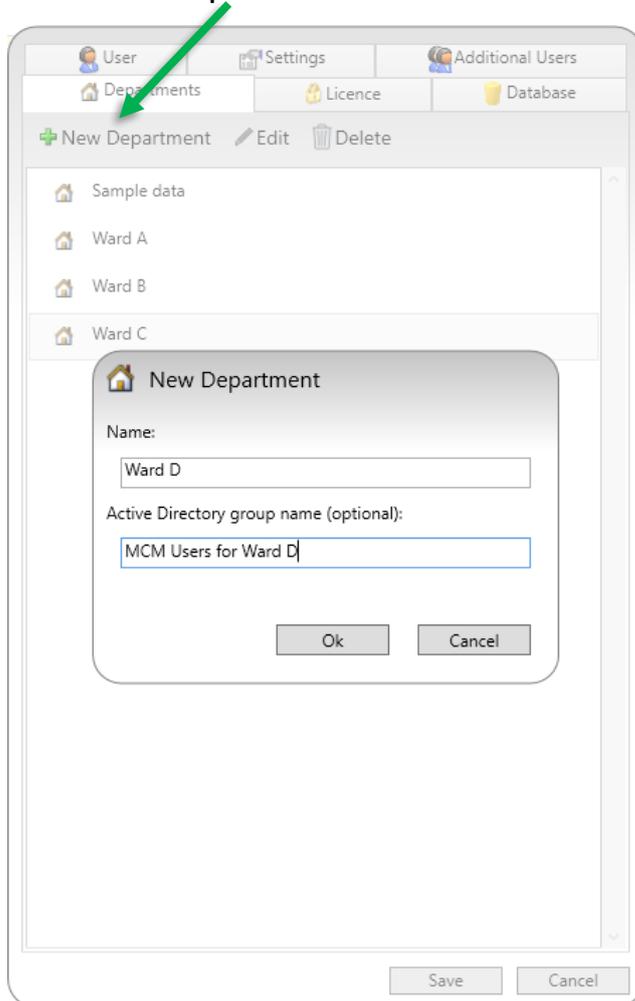
13. Rename the "Standard department"



You may use any display name for the Department (Ward)

14. Assign an AD group to this department.

15. Allocate new Departments as needed



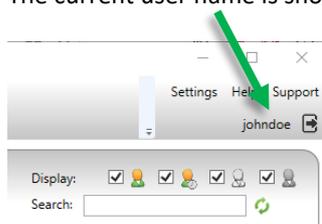
16. You may also define a AD group for the “Sample data” department.

5. Testing

Start MCM.

If the current windows user name is found in the AD and is a member of group which is assigned to a department, then the application will open without requesting to login.

The current user name is shown in the right upper corner of the MCM window.

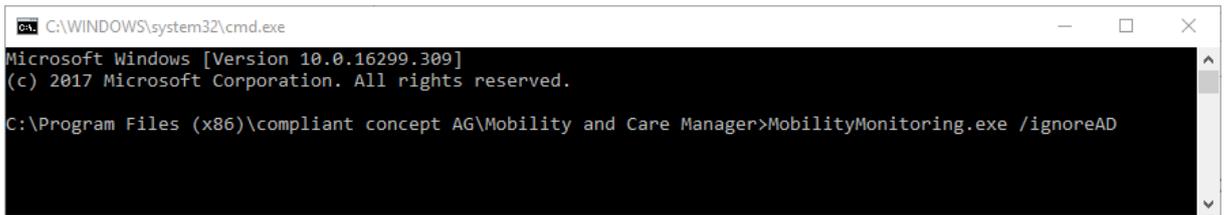


If the user is not found in the AD, then a login screen is displayed and a password for a local application user is needed.

6. Additional options

6.1. Ignore Active Directory

It is possible to bypass the AD lookup and force to use local users:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\compliant concept AG\Mobility and Care Manager>MobilityMonitoring.exe /ignoreAD
```

Providing argument `/ignoreAD` to the application will force to display the login window where one of the predefined local application users may be chosen. This is helpful when the AD configuration is somehow wrong and it is not possible to access the administrator settings with the AD user.