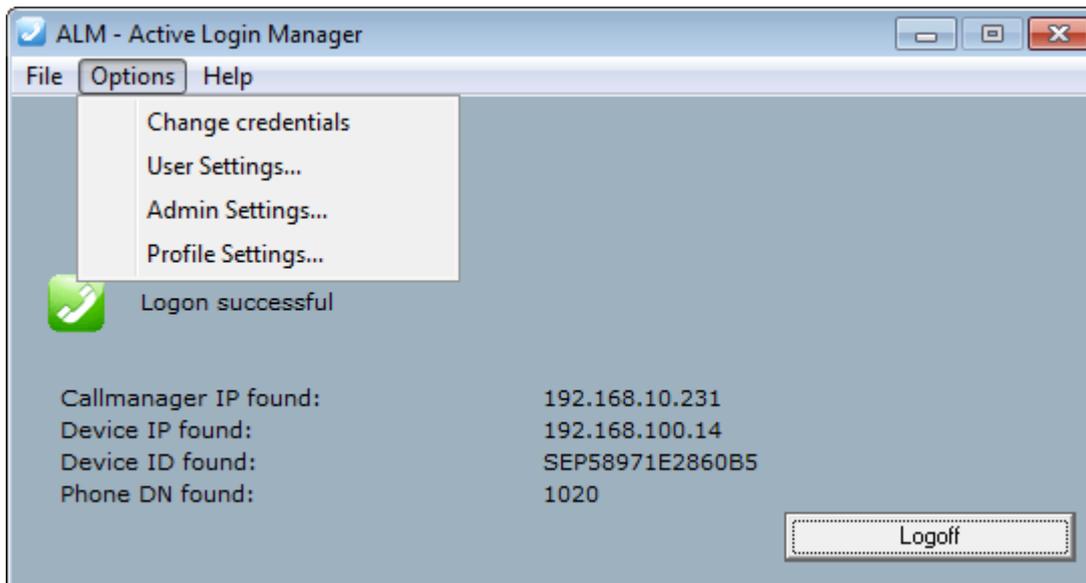


General

This How-To guide explains how to disable or enable certain menu options in ALM. The ALM Menu is accessible from the ALM icon in the system tray.



1 ALM main window

Configurable menu options

The following menu option can be enabled/disabled (grayed out):

- Options / Admin Settings...

The following menu options can be locked (visible, but not editable)

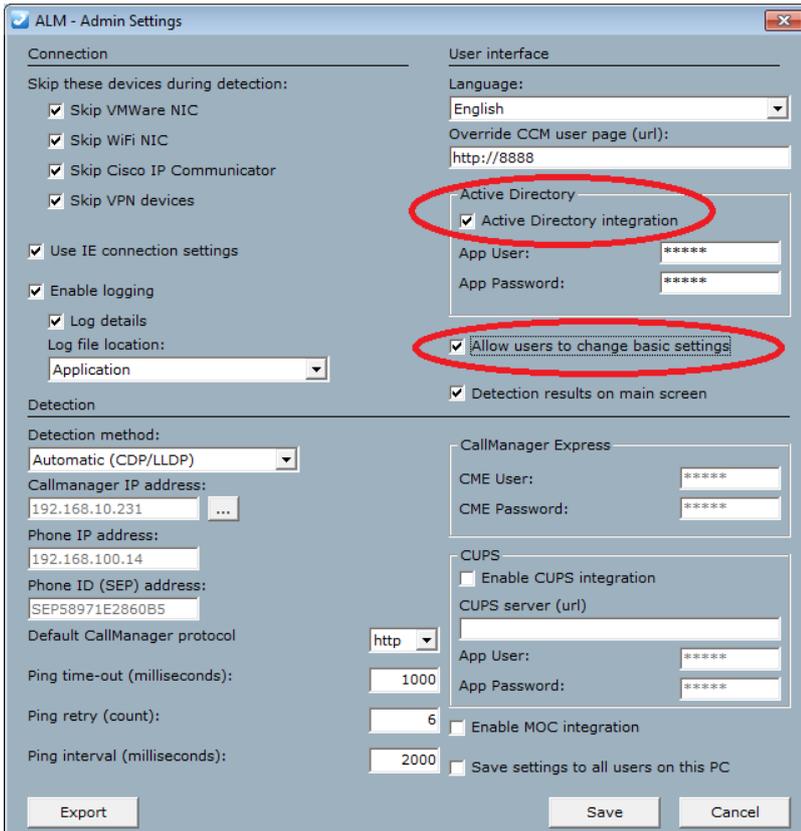
- Options / Change credentials
- Options / User Settings...

By default, depending on the permissions of the Windows user that starts ALM, the following menu options are enabled/disabled:

Windows login	Change credentials	User settings	Admin settings
Standard user	Enabled	Enabled	Disabled
User with admin rights	Enabled	Enabled	Disabled
Administrator	Enabled	Enabled	Enabled
Active Directory			
Standard user	Disabled	Enabled	Disabled
Administrator	Disabled	Enabled	Enabled

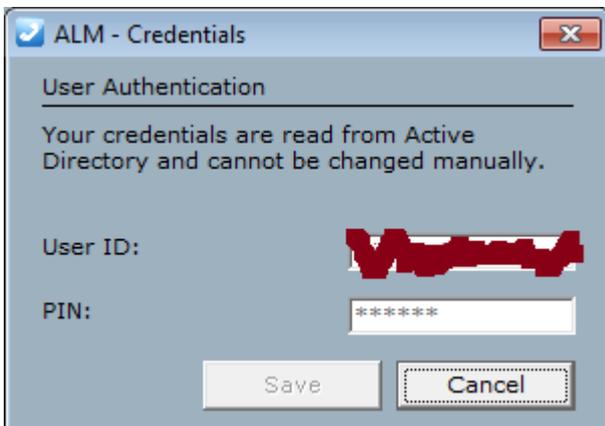
Configure user options

The default behaviour of the **Change credentials** and **User settings** menus can only be modified by an administrator from the Admin settings menu



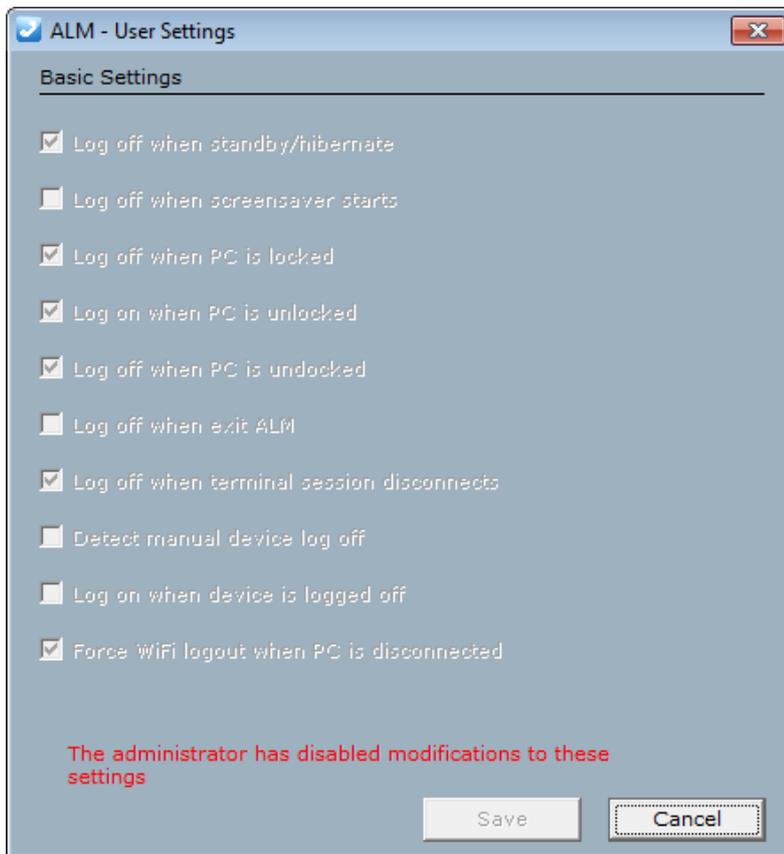
2 Admin Settings

When Active Directory integration is enabled and the user clicks on the **Change credentials** menu, the following screen will appear:



3 Disabled Change credentials

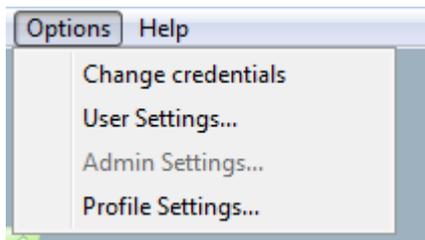
When "Allow users to change basic settings" is unchecked and a user clicks on the **User Settings** menu, the following screen will appear:



4 Disabled User Settings

Configure admin option

The admin menu contains advanced settings that influence the technical behaviour of ALM and it's integration with other software. By default the admin settings are disabled.



5 ALM options menu

To allow temporary access to the admin menu, an administrator can right click on the ALM menu icon and click Run As Administrator (even if he already is an administrator). **Note that when running ALM as an administrator, all changes made to the admin menu will be saved to the admin profile only, unless "Save settings to all users on this PC" is checked.**

The default behaviour of the **Admin and user settings** can also be modified by an administrator by adding/changing the following ALM registry keys:

key	value	menu
AllowAdminsToChangeAdminSettings	true / false	Options / Admin Settings...
AllowUsersToChangeAdminSettings	true / false	Options / Admin Settings...
AllowUsersToChangeSettings	true / false	Options / User Settings...

The location of these registry keys and how to apply them is explained in the following paragraph:

Manual Configuration

To enable/disable a menu option, use the registry editor to add specific keys to one of the following locations:

For the current user (both 32bit and 64bit):

HKEY_CURRENT_USER\Software\Alm

For all users (32 bit Windows):

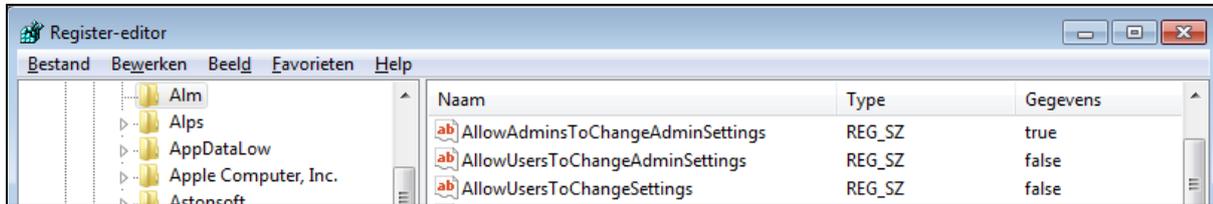
HKEY_LOCAL_MACHINE\SOFTWARE\Alm

For all users (64 bit Windows):

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Alm

Add a String value (REG_SZ) with key name of the registry key above.
e.g. for Admin settings add the key **AllowAdminsToChangeAdminSettings**

Change it's value into **true** to enable or **false** to disable the menu option.



6 ALM settings in registry editor (regedit.exe)

Automated Configuration

To automatically deploy certain settings to all users, create a text file named ALMSettings.txt and store it in the same folder as the ALM installer.

Edit the contents to be:

```
[LocalSettings]
AllowUsersToChangeSettings=true
AllowUsersToChangeAdminSettings=false
AllowAdminsToChangeAdminSettings=true
```

Then run the installer, by using a login script or other automated deployment tool (e.g. SCCM). The installer will read the configuration from the ALMSettings.txt file and store those values into the HKEY_LOCAL_MACHINE registry keys.

Just copying the ALMSettings.txt file into the ALM folder, without running the installer has now effect, as the **actual run-time values** are stored in the registry and the .txt file only contains the default values at deployment.

Alternatively an administrator can make the required changes into his local registry, then export the registry keys to a .reg file and import the .reg file in the startup script of each user:

```
@echo off
reg import \\UNC_path_to_REG_file
```