

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.

🕝 ALM - Active Login Manager		
File Options Help		
Change credentials User Settings Admin Settings Profile Settings		
Logon successful		
Callmanager IP found:	192.168.10.231	
Device IP found:	192.168.100.14	
Device ID found:	SEP58971E2860B5	
Phone DN found:	1020	

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

How-To Guide Configure menu options in ALM



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

ALM - Admin Settings			x
Connection		User interface	
Skip these devices during detection:		Language:	
Skip VMWare NIC		English	•
Skip WiFi NIC		Override CCM user page (url):	
Skip Cisco IP Communicator		http://8888	
Skin VPN devices		Active Directory	
		Active Directory integration	ノ
Use IE connection settings		App User: **	***
		App Password:	***
Enable logging			
✓ Log details	_		
Log file location:		Allow users to change basic s	ettings
Application		Detection results on main con	
Detection		Detection results on main sch	
Detection method:		- CallManager Express	
Automatic (CDP/LLDP)		CNE LINE	*****
Callmanager IP address:		CME User:	
192.168.10.231		CME Password:	****
Phone IP address:		CUPS	
192.168.100.14		Enable CUPS integration	
SEP58971E2860B5		CUPS server (url)	
Default CallManager protocol			
	nttp 💌	App User:	****
Ping time-out (milliseconds):	1000	App Password:	****
Ping retry (count):	6	Enable MOC integration	
Ping interval (milliseconds):	2000	Save settings to all users on t	his PC
Export		Save	Cancel

2 Admin Settings

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

🔁 ALM - Creden	tials	×	
User Authenti	cation		
Your credentials are read from Active Directory and cannot be changed manually.			
User ID:		Vantanta	
PIN:		****	
	Save	Cancel	

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:

ALM - User Settings		
Basic Settings		
🗹 Log off when standby/hibernate		
📕 Log off when screensaver starts		
🗹 Log off when PC is locked		
🗹 Log on when PC is unlocked		
🗹 Log off when PC is undocked		
📕 Log off when exit ALM		
🗹 Log off when terminal session disconnects		
📕 Detect manual device log off		
📕 Log on when device is logged off		
🗹 Force WiFi logout when PC is disconnected		
The administrator has disabled modifications to these settings		
Save		

4 Disabled User Settings

How-To Guide Configure menu options in ALM



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.

options neip	
Change credentials	
User Settings	
Admin Settings	
Profile Settings	

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\AIm

For all users (64 bit Windows):

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Alm

Add a <u>String value</u> (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.

💣 Register-editor					×
<u>B</u> estand Be <u>w</u> erken Beel <u>d</u> <u>F</u> avorieten	<u>H</u> elp				
	*	Naam	Туре	Gegevens	*
Alps		ab AllowAdminsToChangeAdminSettings	REG_SZ	true	
AppDataLow		AllowUsersToChangeAdminSettings	REG_SZ	false	
Apple Computer, Inc.	Ξ	ab AllowUsersToChangeSettings	REG_SZ	false	E

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 changed 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