

ALM – How to configure Active Directory Authentication



Oude Oeverstraat 120-4
6811 JZ
Arnhem
The Netherlands

t: +31(0) 88 1221 800
f: +31(0) 88 1221 899
www.rsconnect.net
info@rsconnect.net

How to configure Active Directory Authentication within ALM

This How-To guide explains how to configure Active Directory in ALM.

The default behaviour of ALM is that it prompts the user for its Extension Mobility user name and PIN at first use.

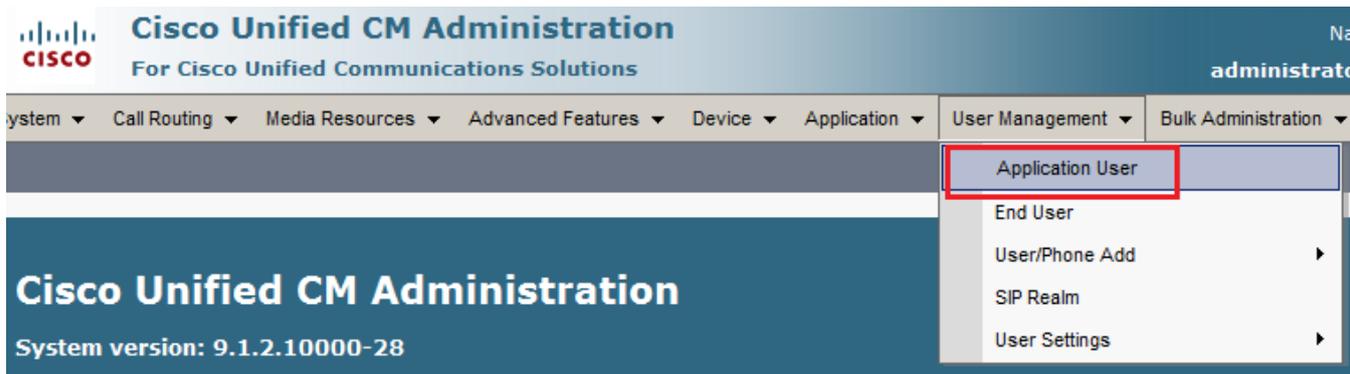
However, if your CallManager is configured to accept the Windows login name as the user id, then ALM can automatically login the user's phone without the need to enter a username or PIN. This document applies to to ALM v4 and up.

To support lower versions, please contact support@rsconnect.net

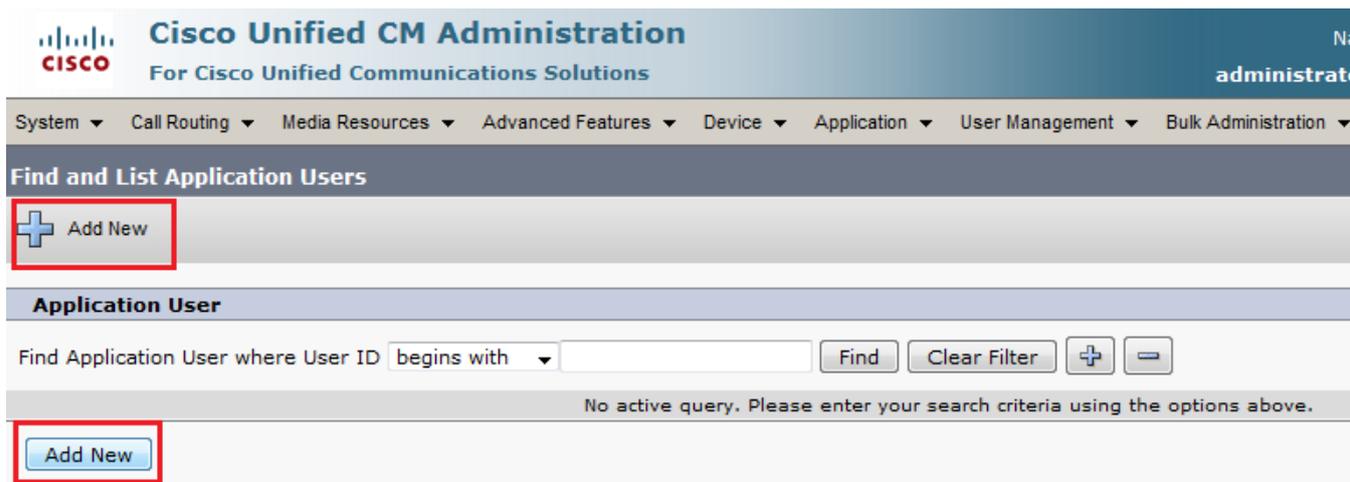
Required CUCM configuration

The First step is to configure one generic Application User in CUCM with permissions to 3rd party applications (ALM) to login Extension Mobility:

- a) Login to the CCM admin page
- b) Open User Management/Application User



- c) Click Add new user



- d) Create a User ID and an App Password and add the user to the "Standard EM Authentication Proxy rights" group. Remember the chosen user ID and App password for step 2.

Application Username	almappuser
Application Password	

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾

Application User Configuration

Save Delete Copy Add New

Status
Status: Ready

Application User Information

User ID* [Edit Credential](#)

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

BLF Presence Group*

Accept Presence Subscription

Accept Out-of-dialog REFER

Accept Unsolicited Notification

Accept Replaces Header

e) Add the AppUser to the "Standard EM Authentication Proxy Rights" Access Control Group

Find and List Access Control Groups

Select All Clear All Add Selected Close

- Standard CCM Server Monitoring
- Standard CCM Super Users
- Standard CTI Allow Call Monitoring
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode
- Standard CTI Allow Reception of SRTP Key Material
- Standard CTI Enabled
- Standard CTI Secure Connection
- Standard EM Authentication Proxy Rights
- Standard Packet Sniffer Users
- Standard RealtimeAndTraceCollection
- Standard TabSync User

Select All

Permissions Information

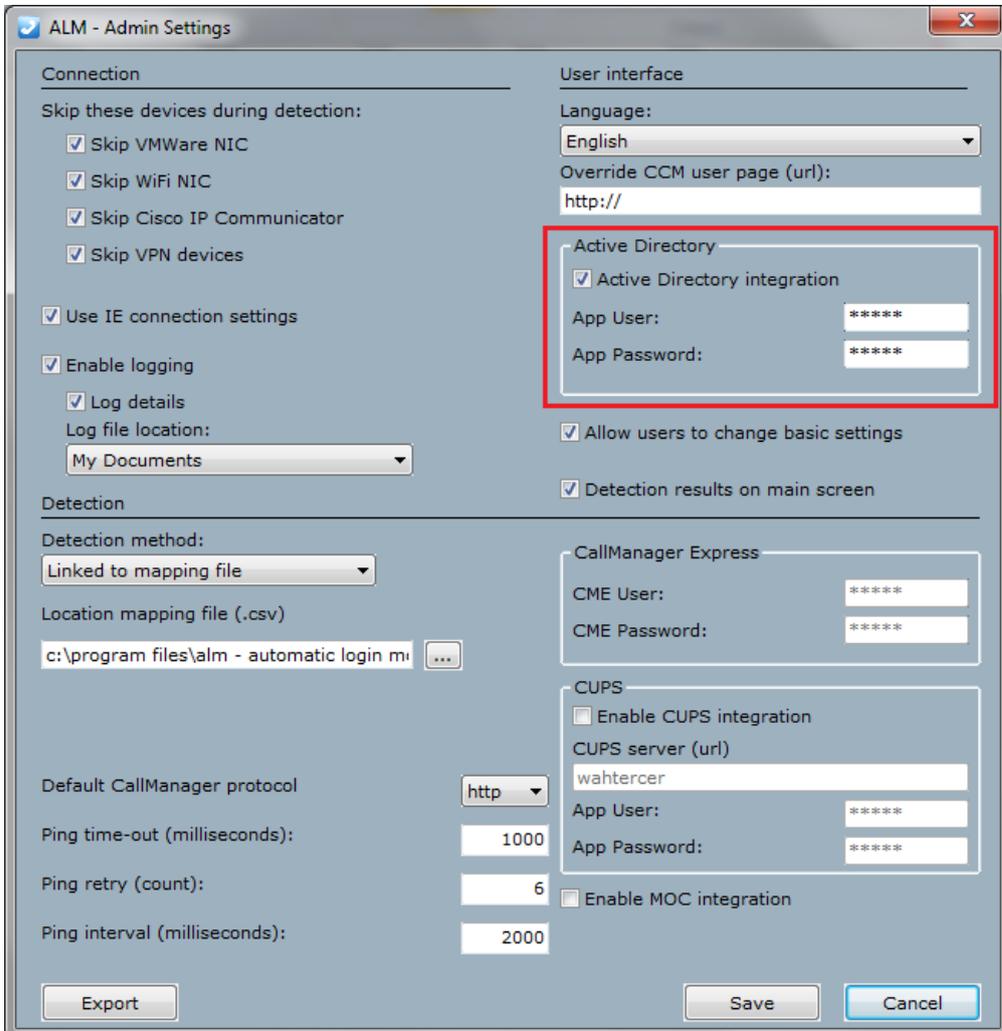
Groups [View Details](#)

Roles [View Details](#)

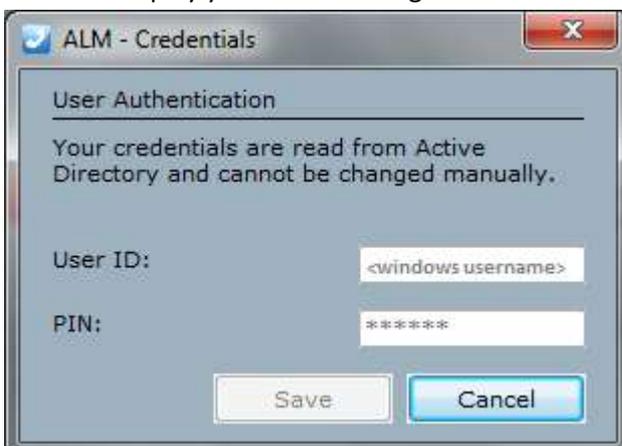
Save

The second step is to configure the ALM client to use the created App user from step 1.

- a) Open ALM (double click ALM icon in the system tray)
- b) Click on Options/Admin settings (If this option is disabled, then make sure you run ALM as administrator, even if you already have administrator permissions.)
- c) Enter the app user ID and app password created in step 1d



- d) Click Save
- e) Within ALM click on Options/Change credentials
- f) It should display your Windows login name and disabled PIN and Save button as listed below:



Ordering Information

Please send your quotation requests to sales@rsconnect.net along with the number of licenses you require.

1 license is required for 1 PC/Phone combination, the license is not user or phone based.
If two employees use 1 computer in combination with 1 IP Phone you will require 1 license.

Additional Information

For any additional information please contact or visit:

- United Kingdom: +44 203 608 8259
- Other countries: +31 88 1221 800
- <http://www.rsconnect.net>
- sales@rsconnect.net