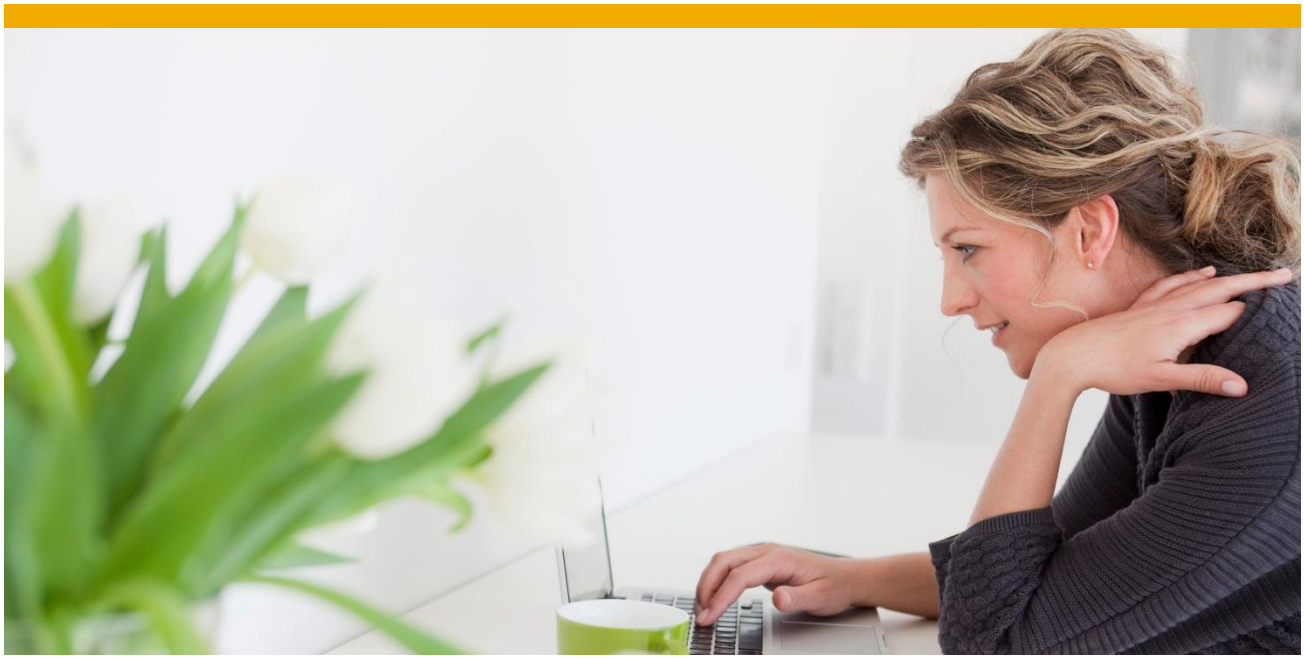
www.sap.com



How to Configure REX Application and SUP/SMP 2.3 to Support LDAP Authentication

PURPOSE

This technical document explains how to configure a REX application to support LDAP in SAP Mobile Platform 2.2.x or higher.

REQUIRED SOFTWARE

1. SUP 2.2.x/SMP 2.3.x or higher
2. Working LDAP server
3. REX 3.2

ASSUMPTION

This document assumes the following:

1. You have a working SUP/SMP2.3 environment
2. A REX application is deployed successfully to its own domain in SUP or SMP and users can register and synchronizes successfully using standard user id and password no LDAP

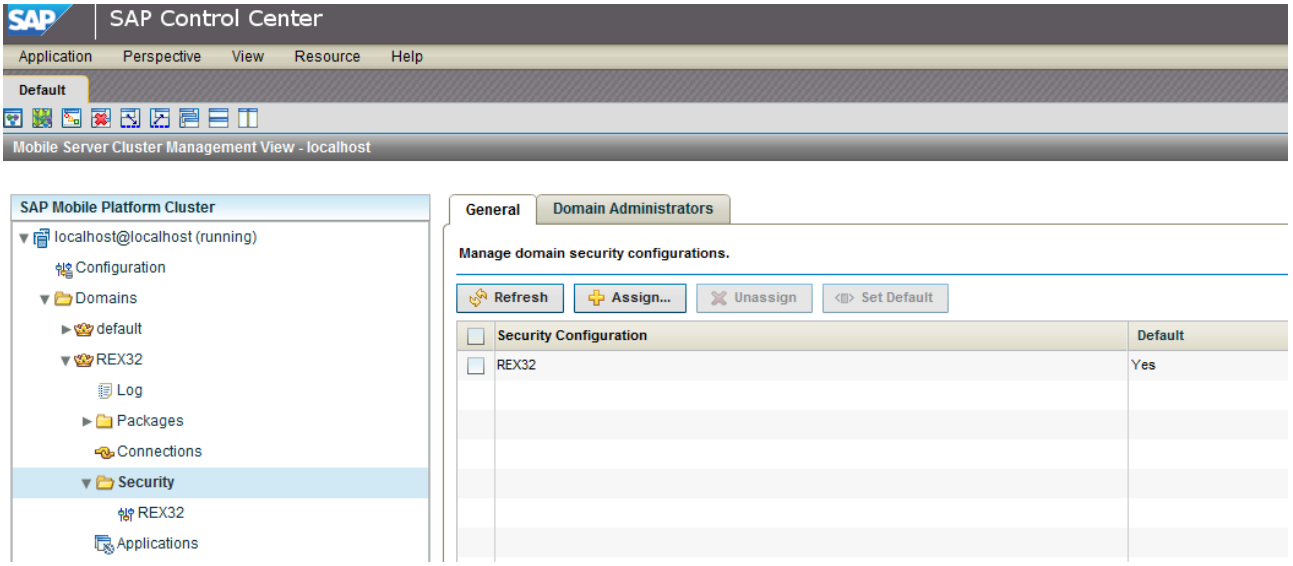
REQUIREMENT

1. A working LDAP server
2. **LDAP user and password, MUST match the CRM user ID and password, otherwise, the data synchronization will fail and only the registration will succeed**. Please refer to this KBA 2037783.

ENVIRONMENT

This paper is tested in the following environment:

1. This document was tested on Microsoft LDAP server
2. The REX application is deployed to a domain called REX32
3. The REX application has a security profile assigned to it. In our test we called this security configuration “REX32” as well. See the figure below to get an idea

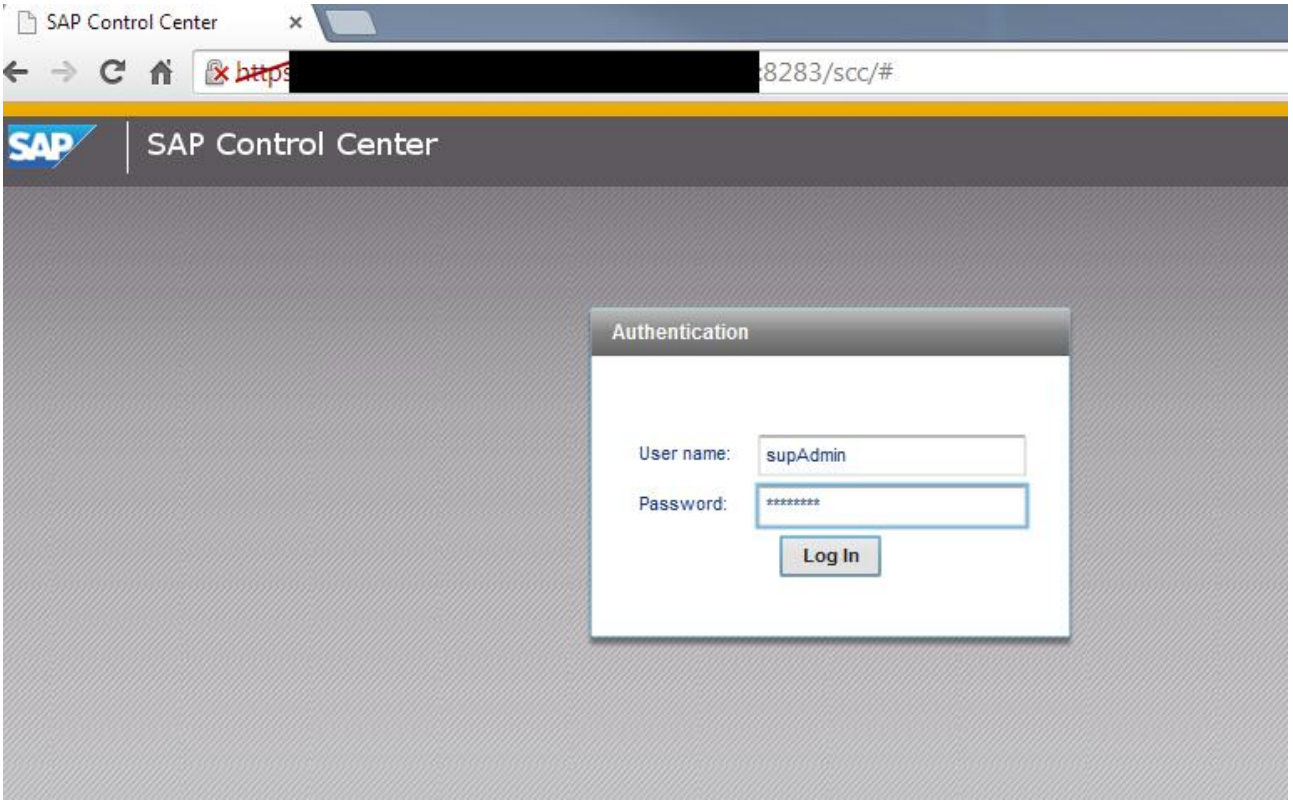


GETTING STARTED

CONFIGURING REX TO SUPPORT LDAP USING SUP/SMP

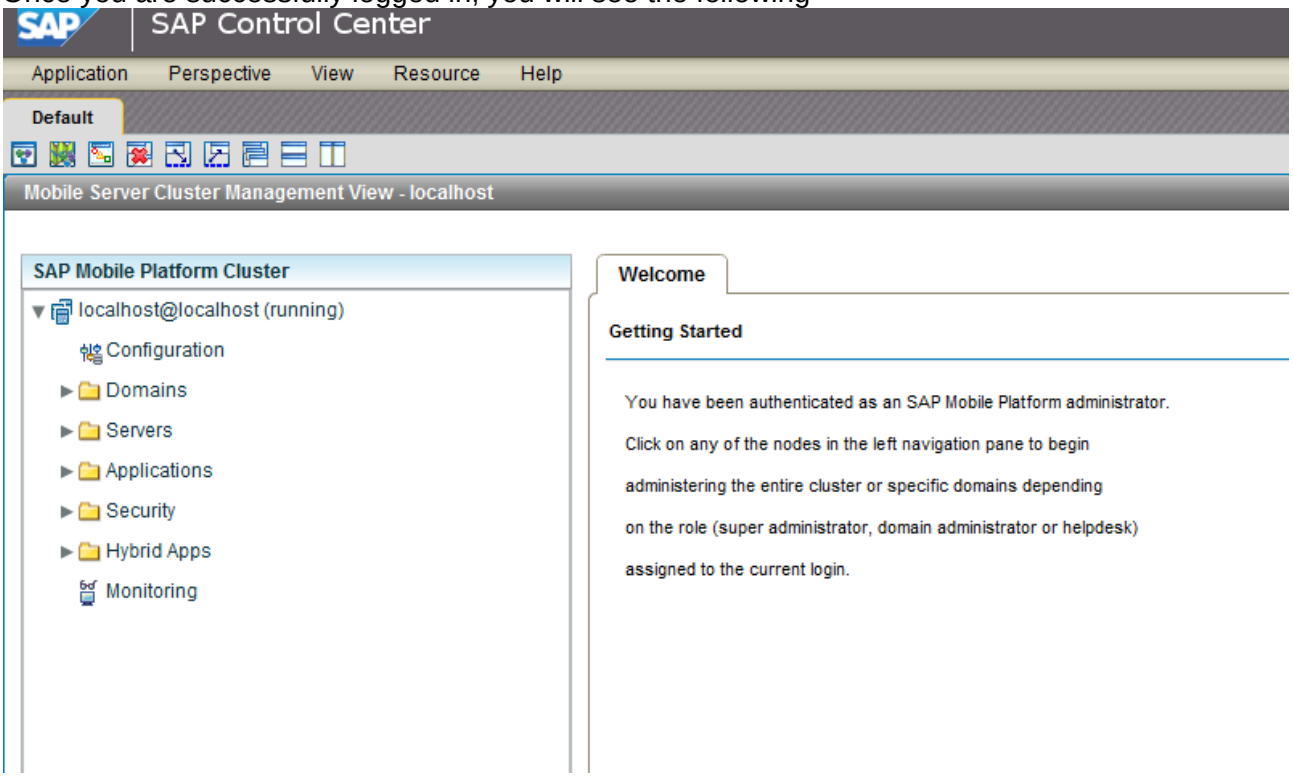
In these steps, we are going to go through the configuration that is needed to enable LDAP in SUP or SMP and allow the REX application to use LDAP

1. Login to SUP or SMP 2.3 server using SAP Control Center (SCC) by opening the browser and type https://<host-server-name>:8283

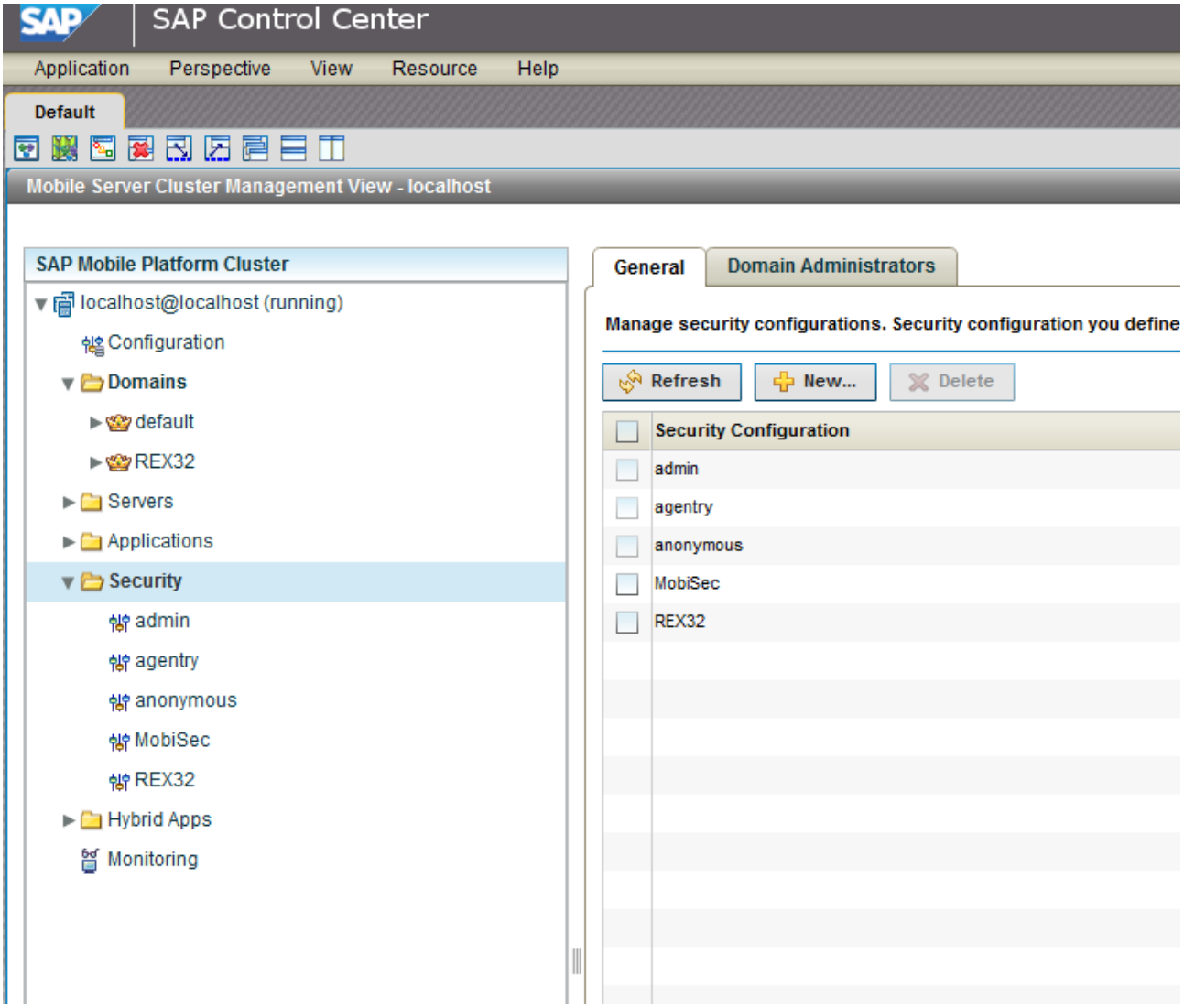


2. By default user ID is supAdmin and password is s3pAdmin

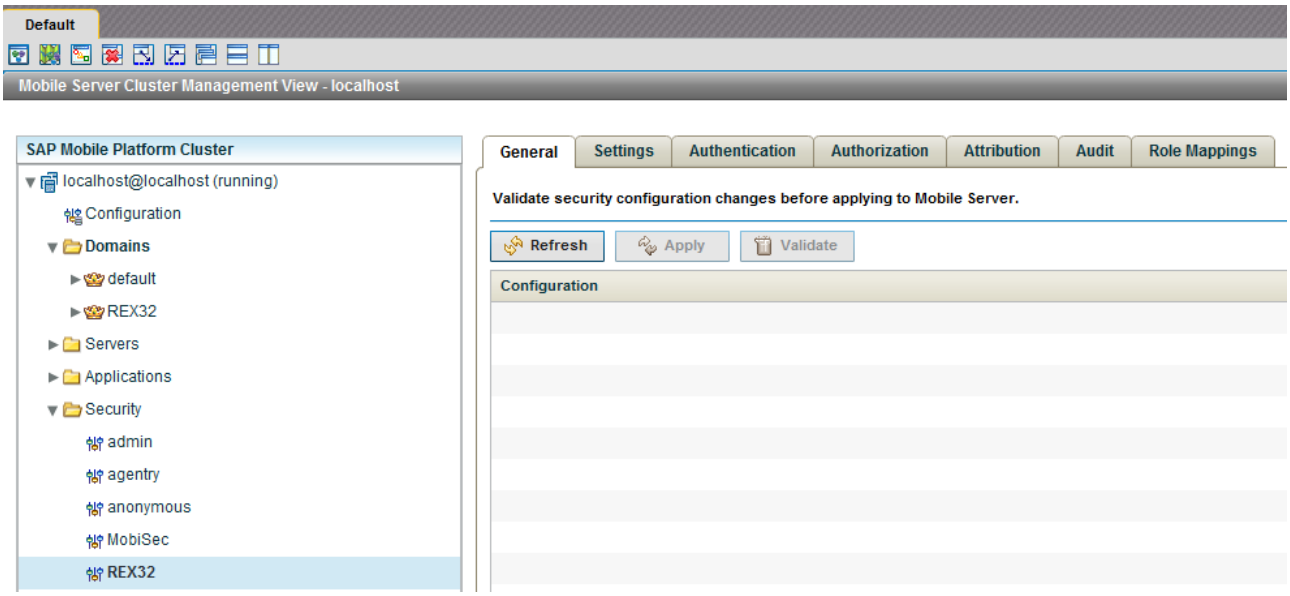
3. Once you are successfully logged in, you will see the following



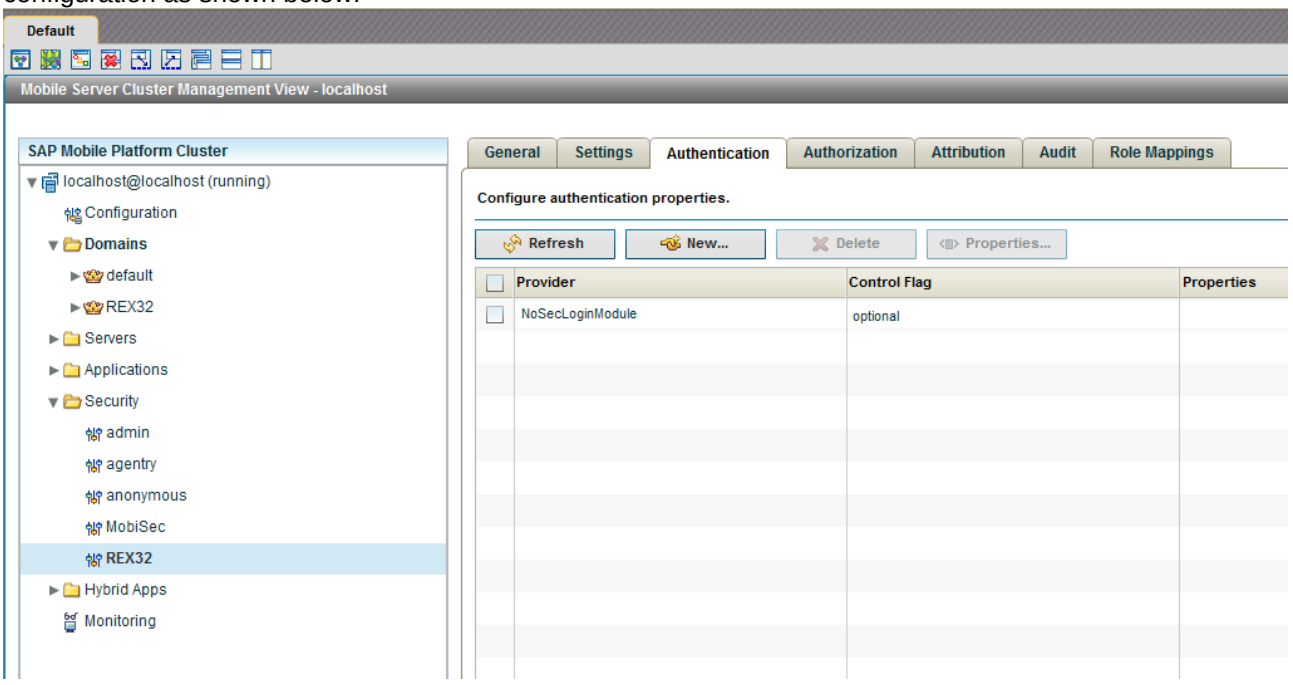
4. Expand the Security folder to select the security configuration that is assigned to the REX domain. In our test, it is called REX32. See below:



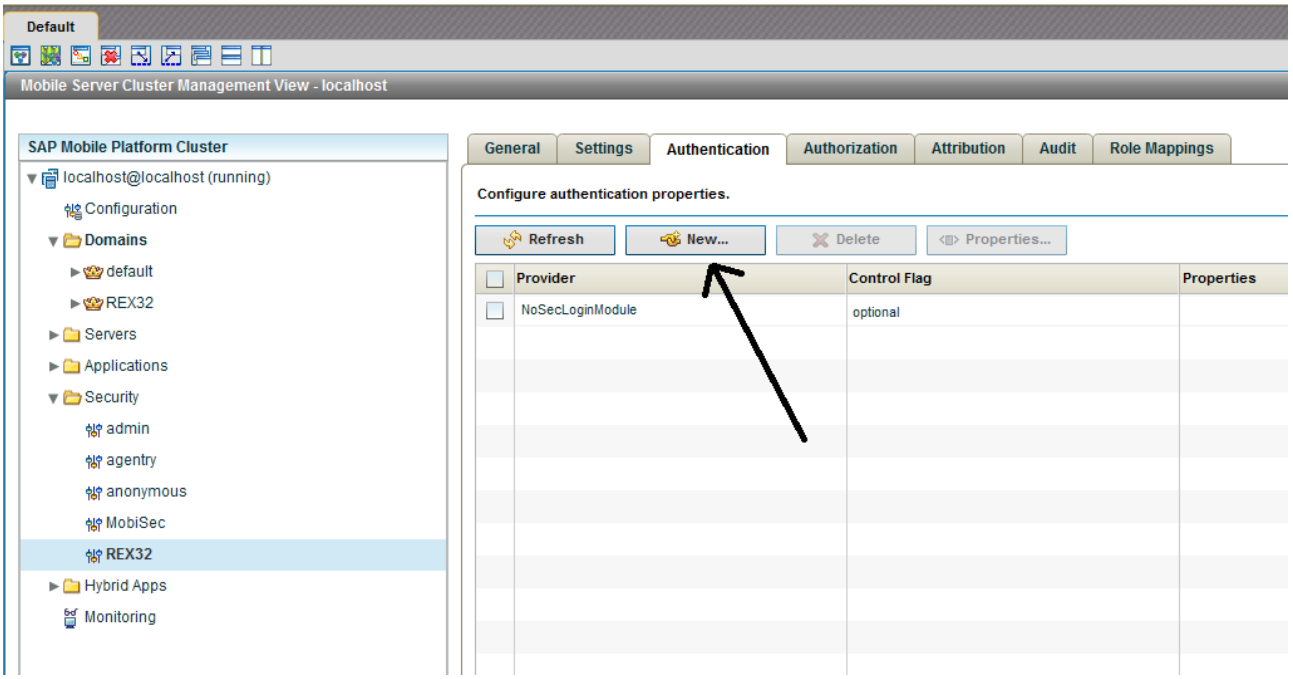
5. Under Security folder, click on REX32 so we can have access to the Authentication tab as shown below



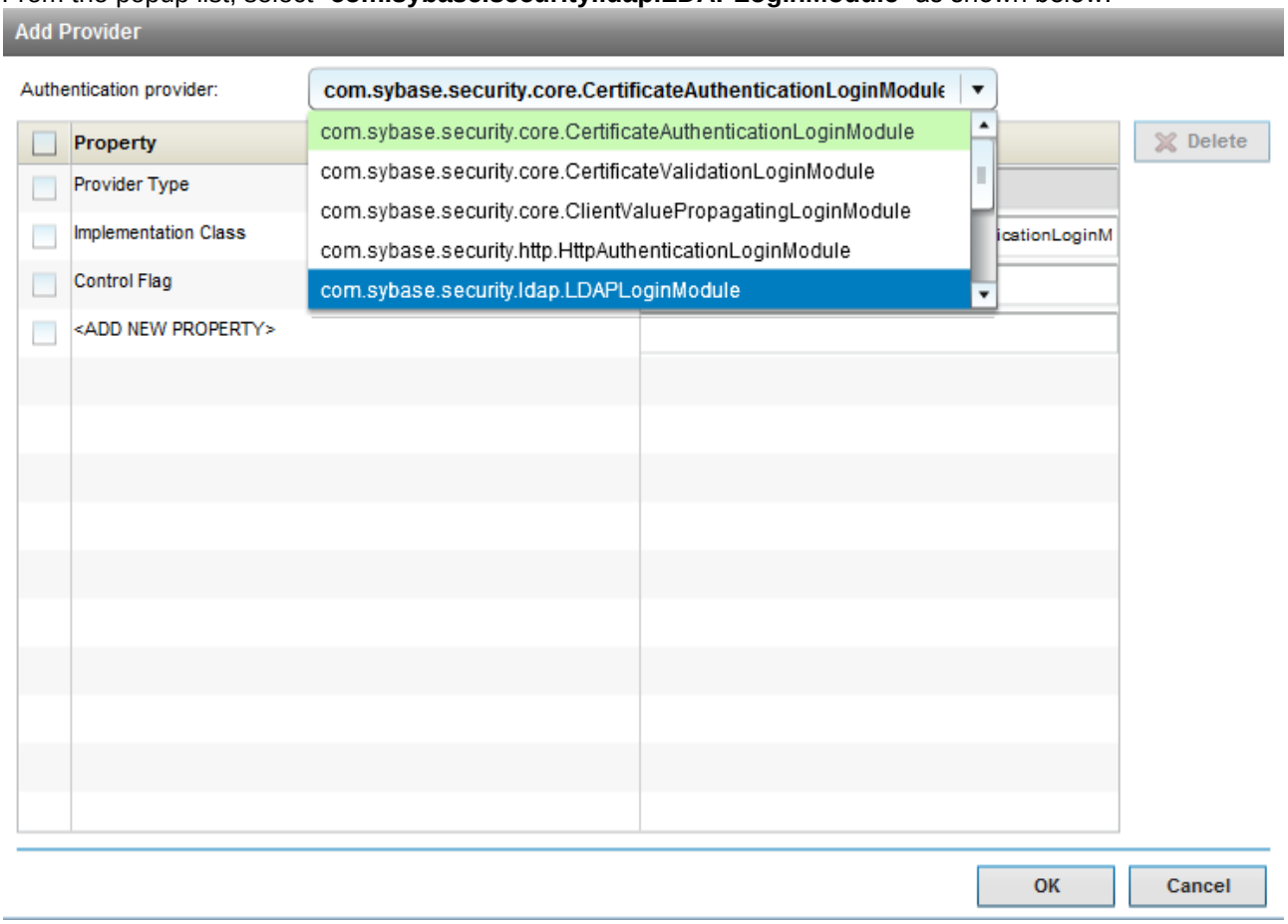
6. Now click on Authentication tab, you should see security modules assigned to this security configuration as shown below:



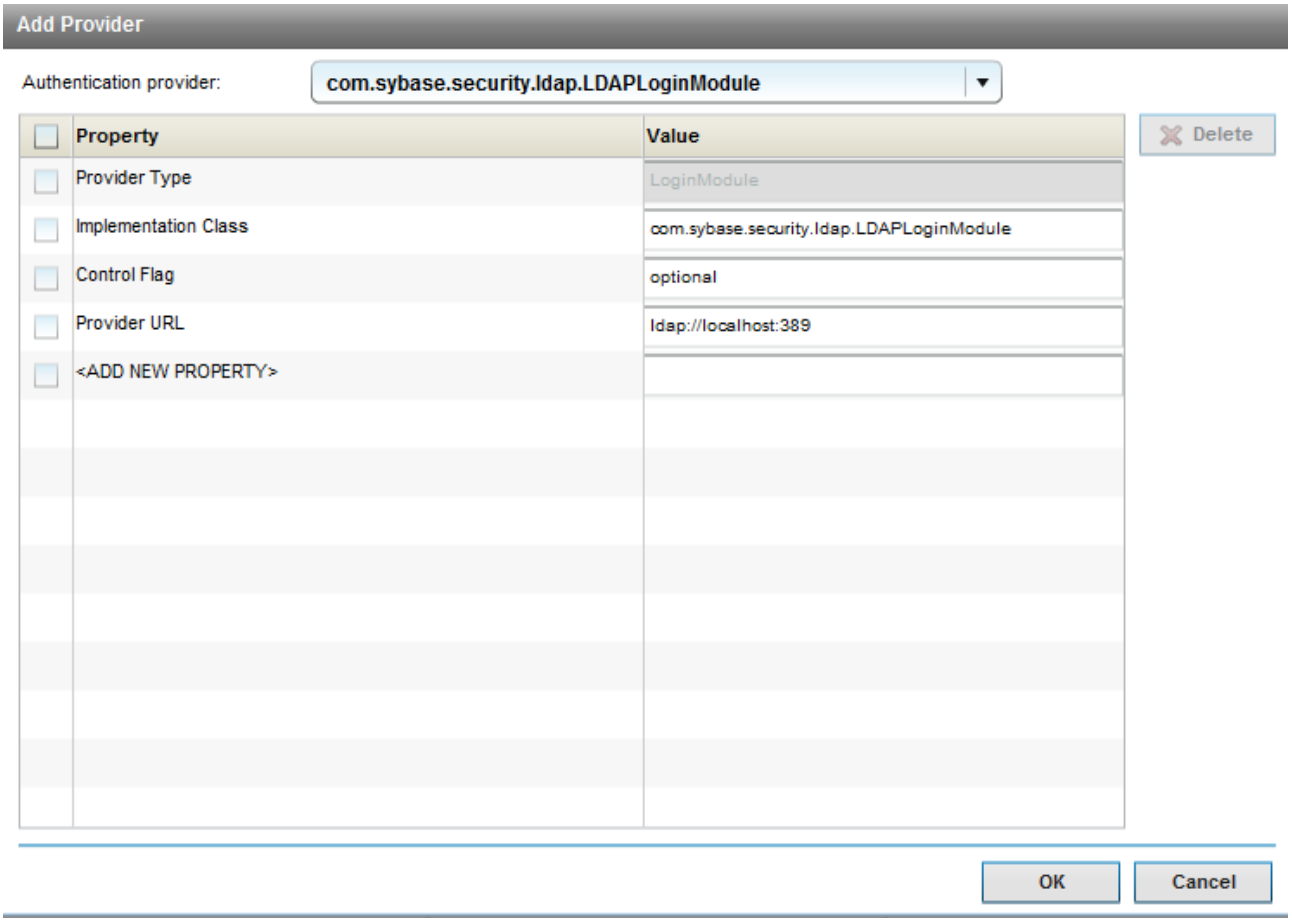
7. This security configuration, “REX32”, is using by default “NoSecLoginModule”, that means anyone can login and register with SUP/SMP. We need to change that and add the LDAP security provider. Click on New to select the LDAP provider module as shown below:



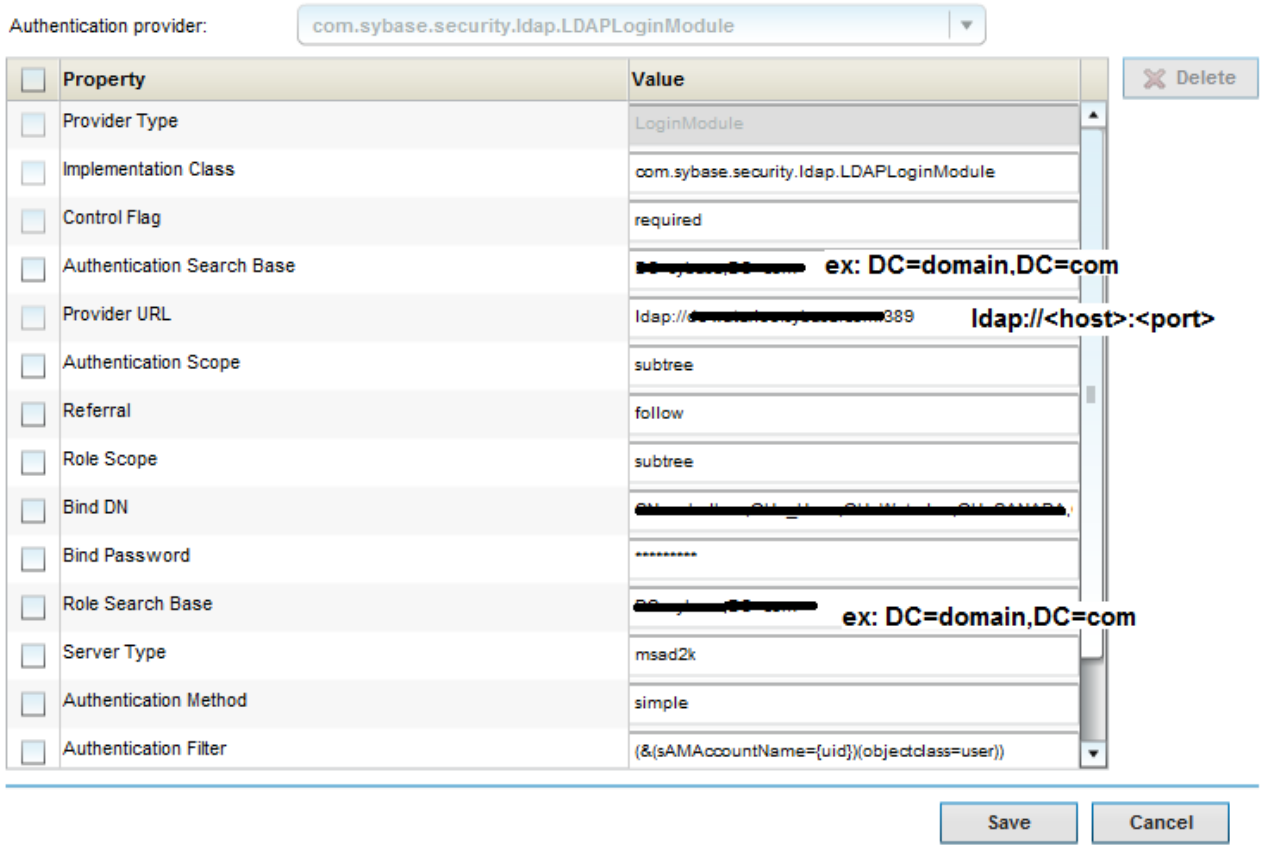
8. From the popup list, select “**com.sybase.security.ldap.LDAPLoginModule**” as shown below:



9. You should see the following screen:


Add Provider
Authentication provider:
com.sybase.security.ldap.LDAPLoginModule
Property
Value
Delete
Provider Type
LoginModule
Implementation Class
com.sybase.security.ldap.LDAPLoginModule
Control Flag
optional
Provider URL
ldap://localhost:389
<ADD NEW PROPERTY>
OK
Cancel

10. Now you need to configure your LDAP according to your environment. Here is a sample of our environment where this paper was tested:



11. Here is explanation of what we have:

    a. **Control Flag:** “required”, that means only LDAP can do the authentication and nothing else. If set it to “optional” or “sufficient”, then if the LDAP fails to authenticate, and if another security provider exists, it will be evaluated. Once everything is working fine, we need to make sure we set it to “required” so no other authentication will be allowed

    b. **Authentication Search Base:** Basically you are telling LDAP the path to take to perform the search or the lookup and from where LDAP is going to start the base search

    c. **Provider URL:** This the LDAP host name. You need to replace <ldap-host> with your LDAP server name and if the port is not the default, you need to change 389 to your LDAP port

    d. **Authentication Scope:** We need to tell LDAP how deep to go below the Authentication Search Base

    e. **Referral:** This is very important. LDAP supports the ability to have many LDAP servers across the globe. Meaning the engineers in one location they can have an LDAP that is part of the enterprise LDAP server located in another head office location. So instead of going to the head office in different location to search across the globe, we can contact our local server and get the path we need. But what if someone from different region tries to login to our server, SCC we need to tell our local LDAP that if the user does not exist on our path, follow through to figure out on what server this user reside. Therefore the value for this attribute is follow

f. **Role Scope:** This works in conjunction with the Role Search Base, is what we need to find belongs one level below the Role Search Base or more than one level. For our example, we are going to use subtree

g. **BIND DN:** It must be a valid DN (distinguished name) that identifies uniquely the user in the organization

h. **Bind Password:** Is the BIND DN user name's password

i. **Role Search Base:** This is used to determine your role in the organization and how to map it to SUP roles

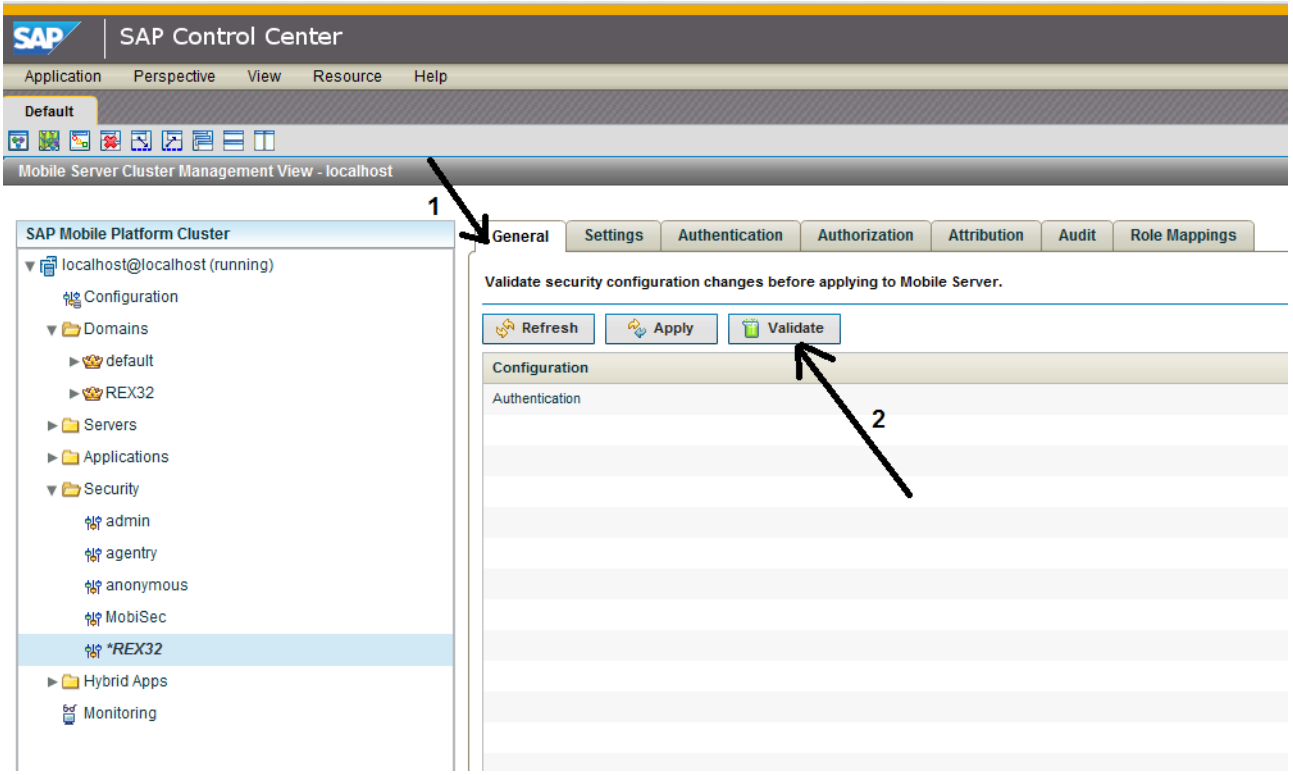
j. **ServerType:** This is the important one. We need to tell SUP what the LDAP server we are talking to. In this document we are going to select Windows LDAP server. So the value should be msad2k

k. **Authentication Method:** We only support "Simple"

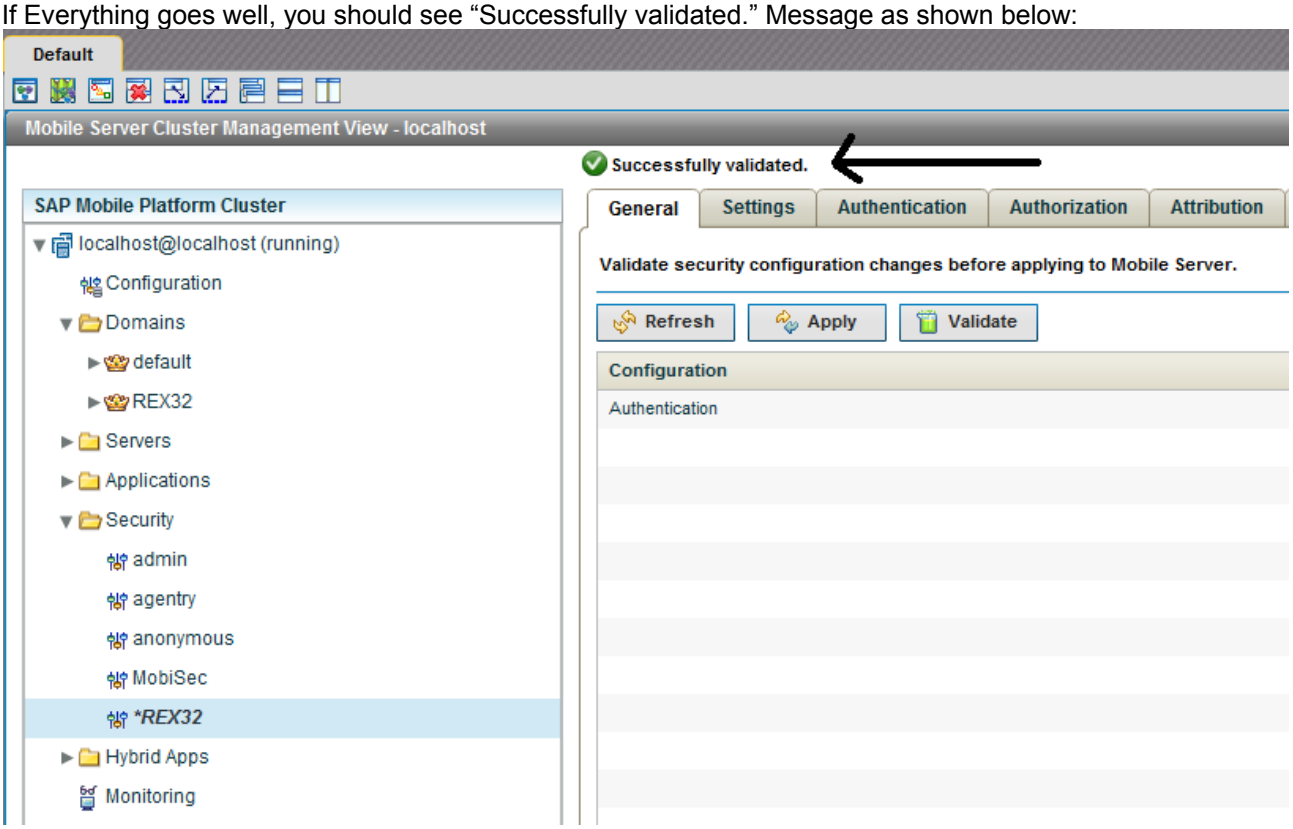
l. **Authentication Filter:** This is like the where clause of a SQL query to use in LDAP to locate what we need. In our example, we are using Microsoft Windows LDAP and SUP is using your user id to authenticate, so the value for the filter is going to be (&(sAMAccountName={uid})(objectclass=user))

m. Now click on OK to save the new configuration

12. Click back on the General tab and then click on validate and save the information as shown below and validate it:

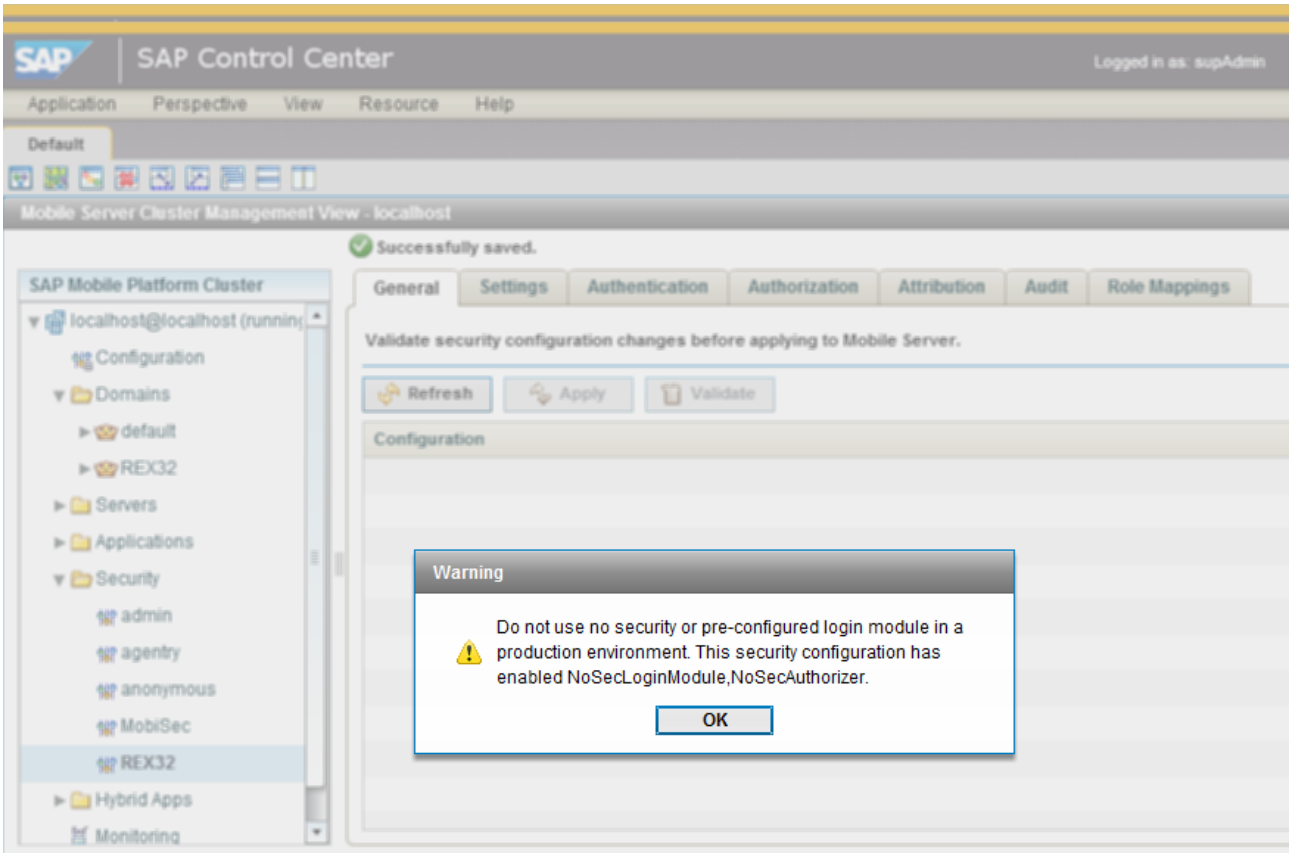


13. If Everything goes well, you should see “Successfully validated.” Message as shown below:



14. Next click on Apply.

15. If operation succeed, you should see the following:



Note: The warning here is indicating that we have a "NoSecLoginModule, NoSecAuthorizer" that needs to be removed when you are in production because anyone can register.

16. Click on OK

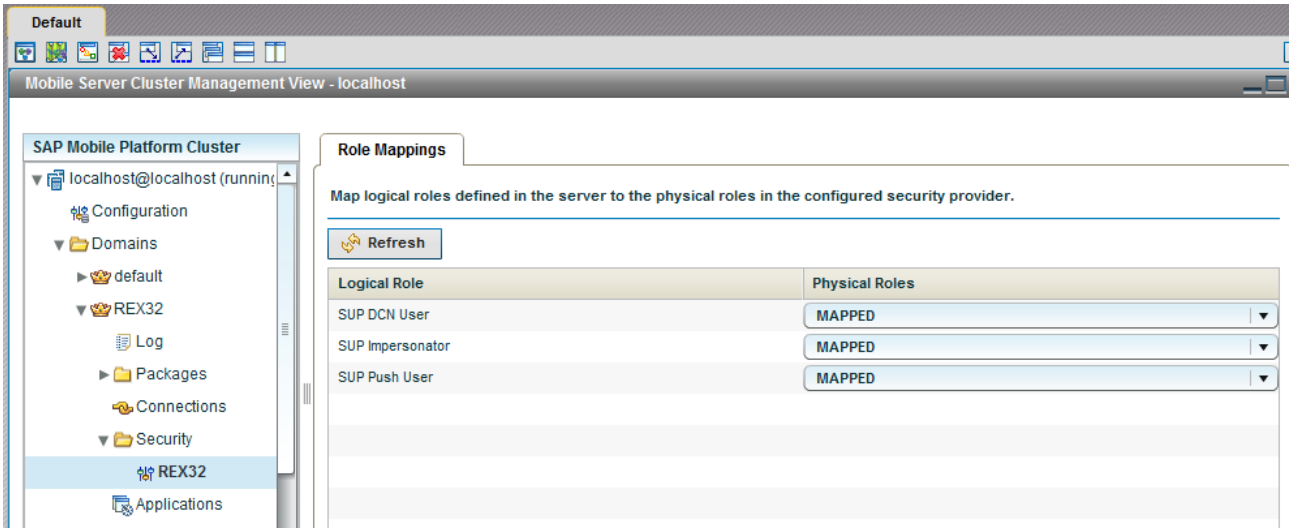
17. Now your system is configured with LDAP

TESTING LDAP CONFIGURATION

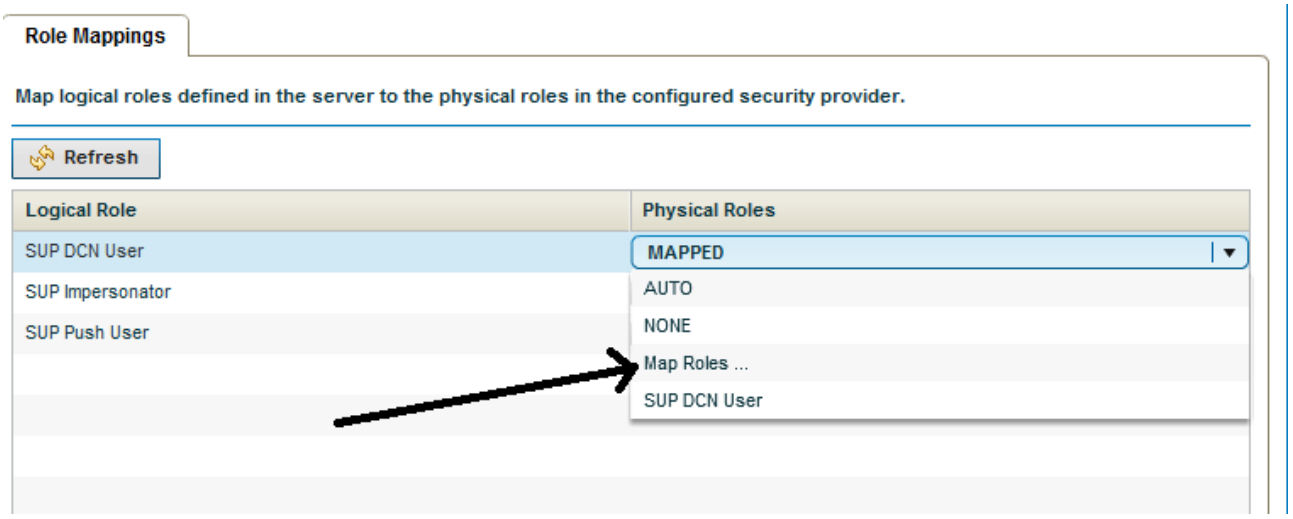
We can test and see if the configuration is working correctly and we can make a successful connection to the LDAP server. To do that, do the following:

1. Expand the Domains folder in SCC
2. Expand the REX domain name
3. Expand the Security folder

4. Click on the REX domain name as shown below:

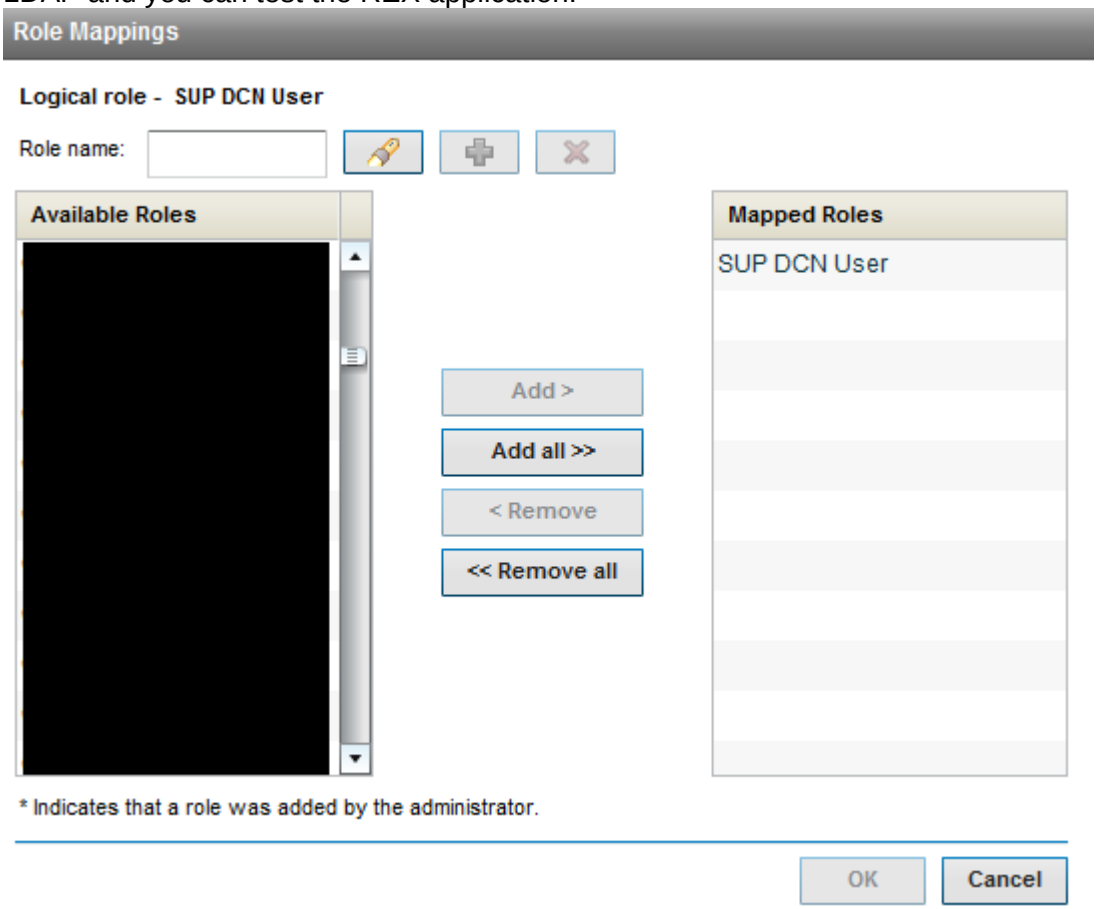


5. Choose any Logical Role and click on the Physical Roles drop down list of that Logical Role. In this example, we are using SUP DCN user Role and we are going to click on MAPPED for this Role as shown below:

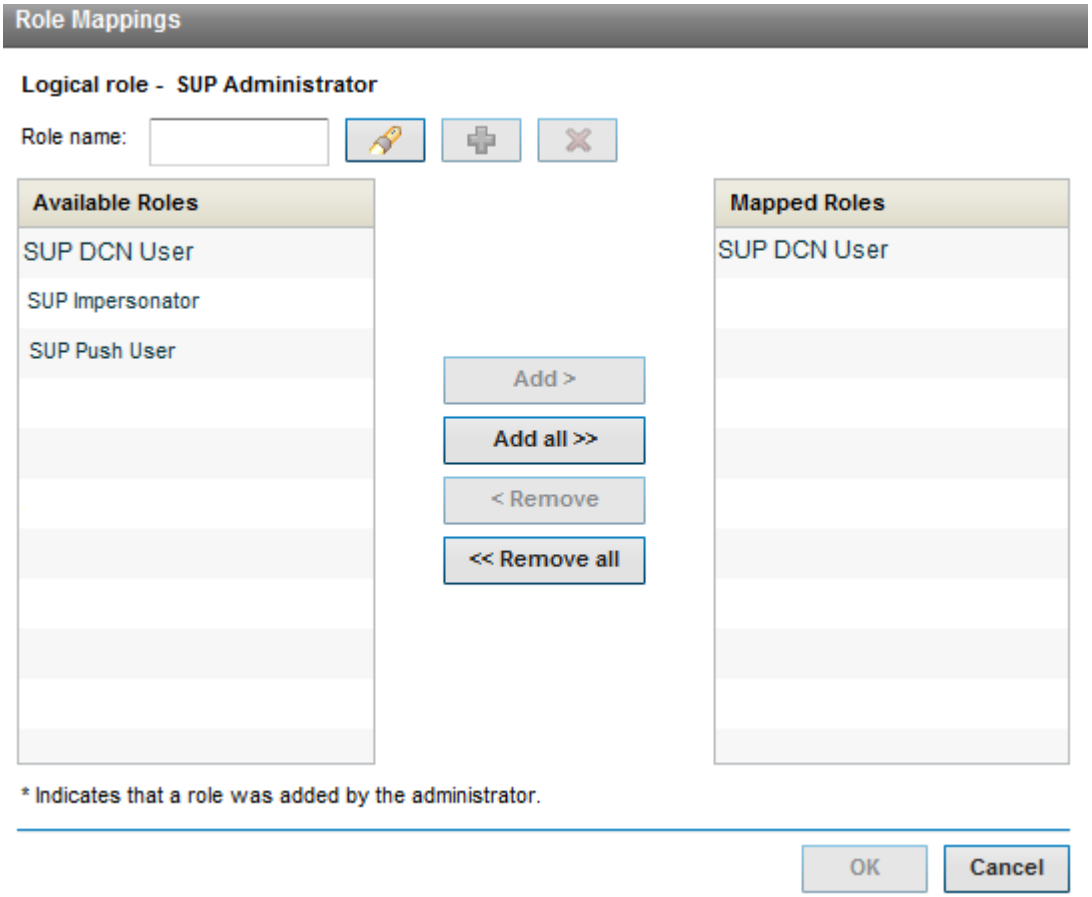


6. Now we are going to click on “Map Roles…”. The idea here is to see if SUP / SMP 2.3.x can communicate with the LDAP server and list all the groups. If we can see all the groups or at least some of the groups, that means, we have successfully communicated with the

LDAP and you can test the REX application.



Note: In our test case, we were able to see all the LDAP groups listed and we can scroll down the list. If you only see the following:



That means, the LDAP is not working properly, unless you have no groups in your LDAP

7. Once you confirm the LDAP is working fine, click Cancel since we do not want to do any mapping.

TESTING REX APPLICATION WITH LDAP CONFIGURATION

1. After downloading the “SAP Retail Execution v3.2” from the App Store and run it , you should be able to configure authentication screen using your LDAP user ID and password

2. Then the application will ask you for a PIN number at least 8 characters if the LDAP is working correctly

3. Last screen, you will be asked for the CRM user ID and password to synchronizes with the CRM using SUP/SMP2.3

4. If everything works well, the application will start synchronizing the MBO objects

MOVING TO PRODUCTION

Once the LDAP configuration is confirmed and working fine and the REX application using LDAP is working successfully, you need to do the following:

1. To make sure only the LDAP is the source of authentication, you need to change the control setting from “sufficient”, or “optional” to **“required”**. This is required if you need only LDAP to be the source of authentication and nothing else

2. Remove the following login module from your system “NoSecLoginModule”. To learn how to do that, please refer to this KBA 2038240

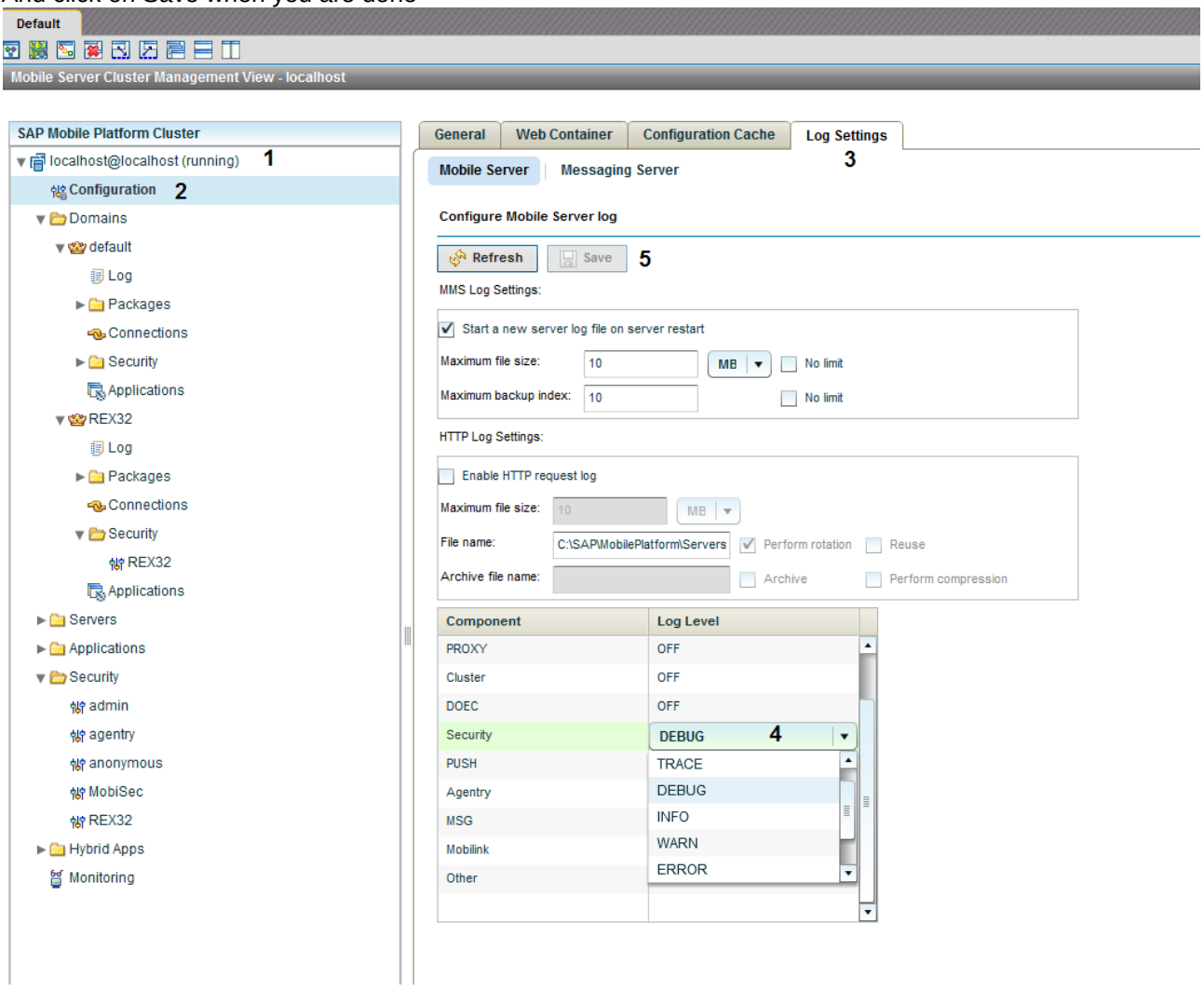
TROULESHOOTING

This section will describe what steps can be taking to debug LDAP configuration and make sure it is working fine:

Registration with SUP is failing using LDAP

When the following situation arises, we need to enable debugging for the security module in SUP/SMP2.3. To do that, do the following:

1. In SCC Expand localhost@localhost(running)
2. Click on Configuration
3. Click on Log Settings
4. Set Security to Debug
5. And click on Save when you are done



6. Repeat the registration process
7. Look at the SUP/SMP server log anything related to the LDAP and see if there is an exception

Registration is successful, but data synchronization is failing

When you face this situation that means, the CRM user ID and LDAP user ID are not the same or the password of the LDAP user and CRM user are not the same.

SUMMARY

This document explained all the steps needed to configure REX application with SUP or SMP 2.3 using LDAP. As well it describes how to do a basic troubleshooting and it discussed the requirement needed in order to get the application configured.

www.sap.com