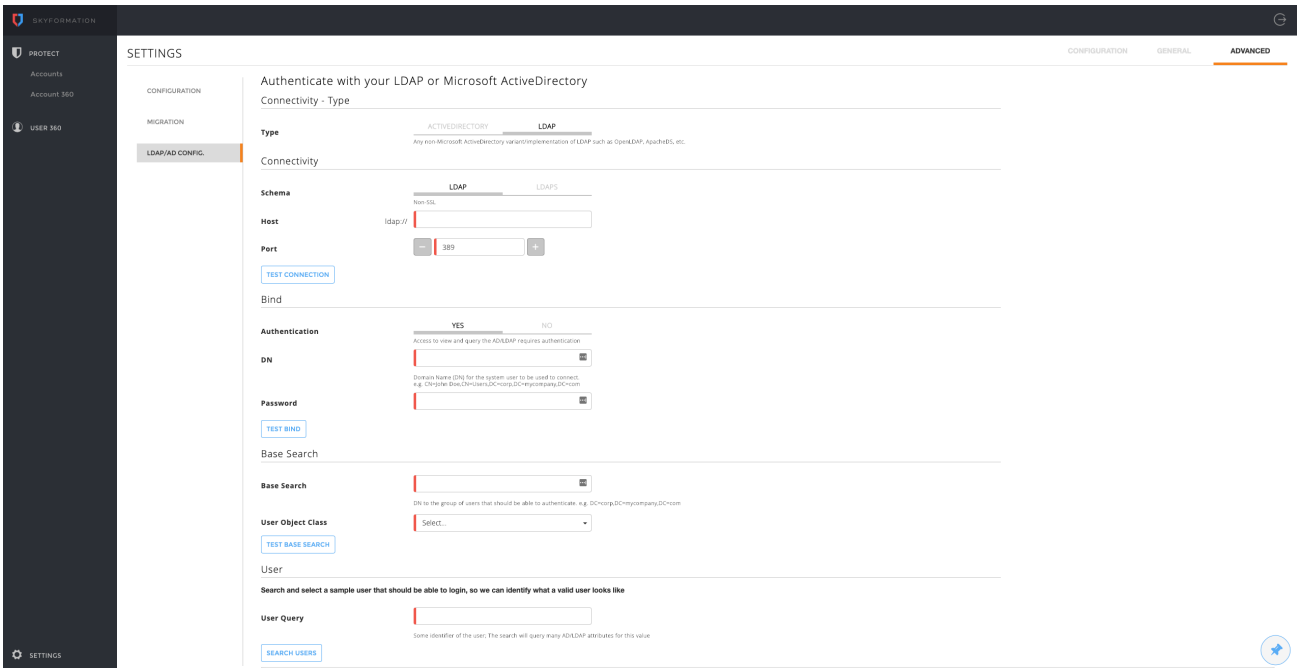
UI Page for Configuring LDAP Authentication

Since 2.5.92

If your LDAP implementation is the **Microsoft Active Directory** please use UI Page for Configuring Active Directory Authentication

- Login you Cloud Connectors (CC) UI
- Select **SETTINGS**
- Select **ADVANCED** tab at the upper right corner
- Select **LDAP/AD CONFIG**



Type

The goal of this section is to differentiate between Microsoft Active Directory and other LDAP implementations (OpenLDAP, Apache Directory and more)

- Select type **LDAP**

Connectivity

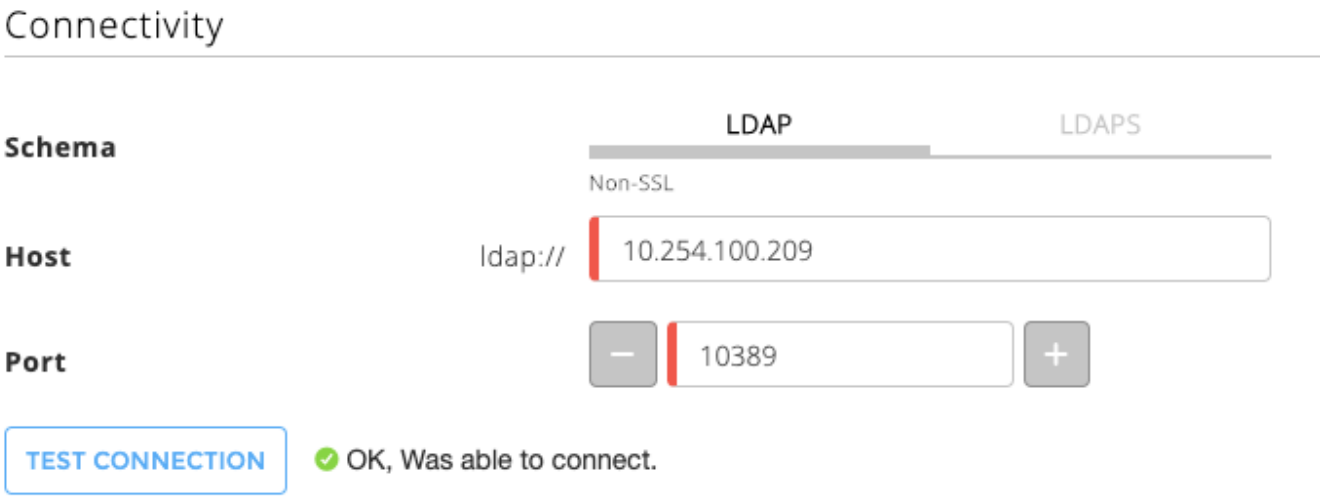
The goal of this section is to configure and test successful connection to the LDAP server

- Select **LDAP** or **LDAPS**

Before configuring **LDAPS** the certificate must be imported to the CC trust store How to Add a SSL Certificate to the Trusted Certificates Store

- Provide hostname or IP
- Provide port number

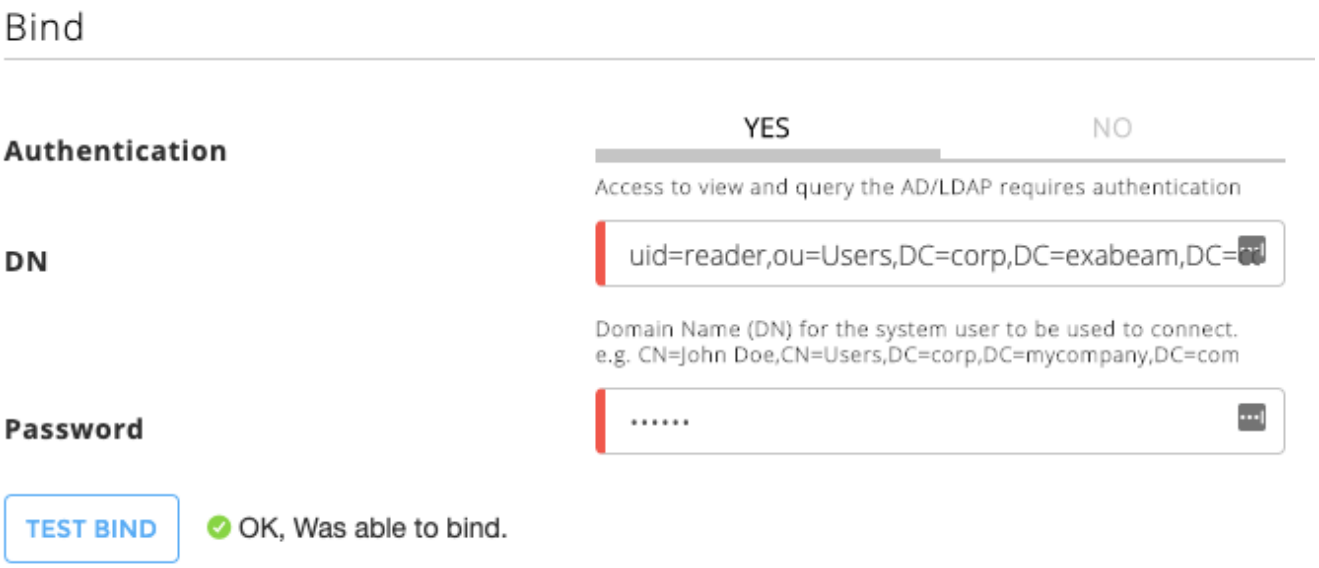
- TEST CONNECTION - only if test connection succeeds can you continue to the next Bind section



Bind

The goal of this section is to configure and test successful binding to the LDAP server

- Authentication
  - If the LDAP server supports anonymous bind select **NO**
  - Otherwise select **YES**
    - Insert of a system DN and password with read permission to be used by CC to authorize the logged in user
  - TEST BIND - only if test bind succeeds can you continue to the next Base Search section



Base Search

The goal of this section is to configure and successfully test base search in the LDAP tree

- Insert he base search DN

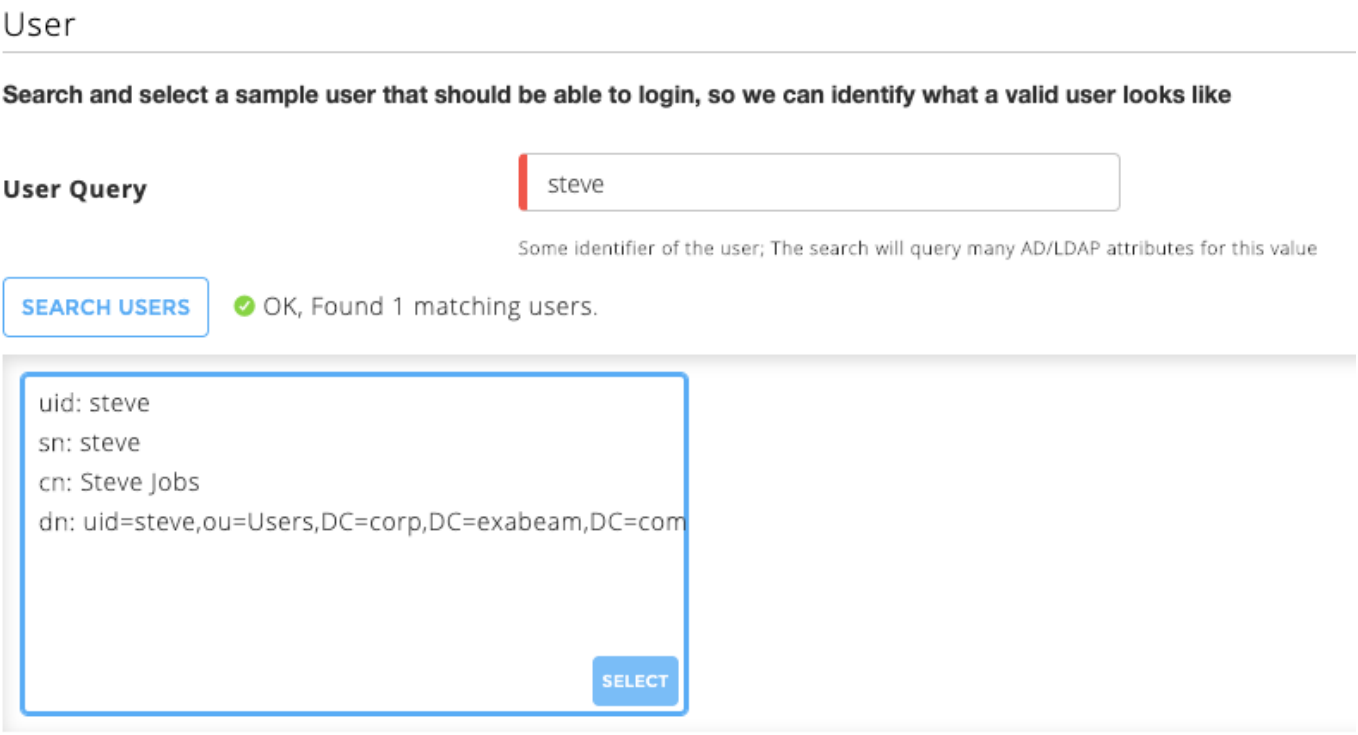
> All users that should be authorized to CC and the LDAP group or role that should be mapped to CC admin role must be under the base search entry

- Select the object class for a user in your organization (**InetOrgPerson** by default)
- TEST BASE SEARCH - only if test base search succeeds can you continue to the next User section

User

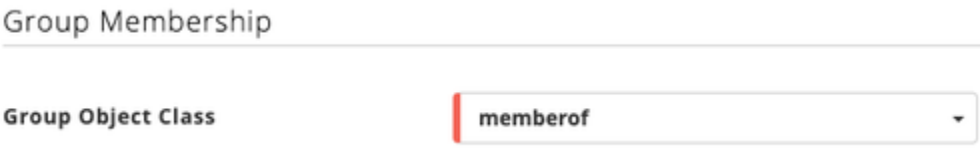
The goal of this section is to find and select one user that should be authorized access to CC. Usually the CC administrator should search and select himself. The selected user would then be used as a template for selecting LDAP group or role

- Insert substring of one of the the user's identifying attributes (uid, cn, mail, sAMAccountName, …)
- Press the **SEARCH USERS**
- Scroll and find the user you are looking for
- **SELECT**



Group Membership

The goal of this section is to select one of the attributes of the user you have just selected indicating a group or role membership in the LDAP server

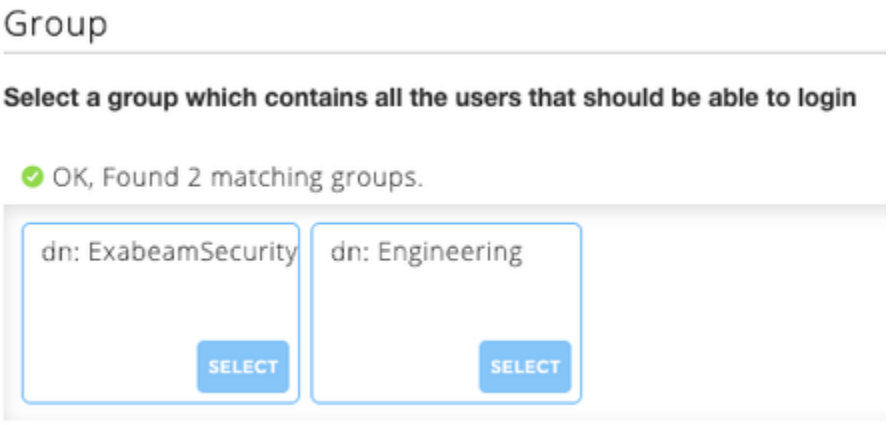


Group

The goal of this section is to select the LDAP group or role whose members are the users in the organization that should be authorized to access CC. The groups or roles CC administrator can select from are groups or rols that the user from the previous section is a member of

> If such group does not exist please create such group and add yourself (the CC administrator) as a member of that group before you continue

- Scroll and find the group you are looking for

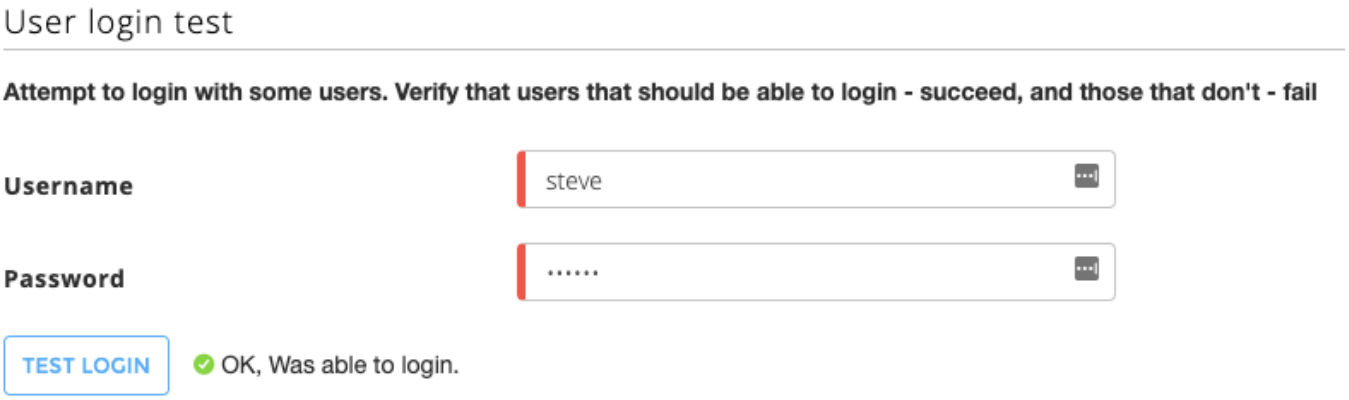


User Bind Attribute

The goal of this section is to select one of the attributes of the user you have selected that would be used as the username for the CC login

User Login Test

The goal of this section is to test authentication and authorization of users using LDAP server with the configuration provided. The expected username is the value of the bind attribute you have selected in previous section

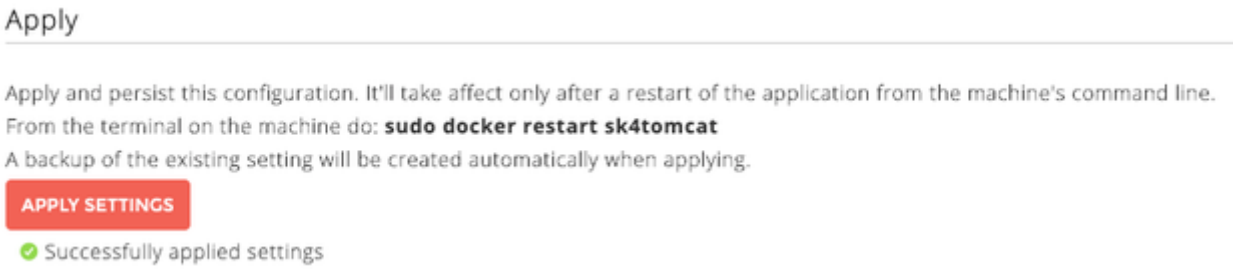


Apply

The goal of this section is to apply the provided configuration. The configuration provided is written to a **shiro/client-shiro.ini** file under the **sk4_conf** volume. The original shiro/client-shiro.ini file is copied to shiro/client-shiro.ini.bak-<DATE_TIME>. In order to apply these changes the CC administrator should restart the **sk4tomcat** container by running the following bash command in the CC server terminal

```
sudo docker container restart sk4tomcat
```

After one or two minutes the sk4tomcat container would complete its restart, the previously open session would be invalidated and the CC administrator would be asked to re-login (this time via the organization's LDAP server)



If for some reason you fail to login after applying the new configuration you can revert by doing the following:

1. Open a terminal to the CC server
2. Change to root

```
sudo -i
```

3. Find the **sk4_conf** volume directory

```
docker volume inspect sk4_conf
```

4. CD to <sk4_conf_volume>/shiro
5. override the **client-shiro.ini** with the latest **client-shiro.ini.bak-<DATE_TIME>**
6. Restart the **sk4tomcat** container

```
sudo docker container restart sk4tomcat
```