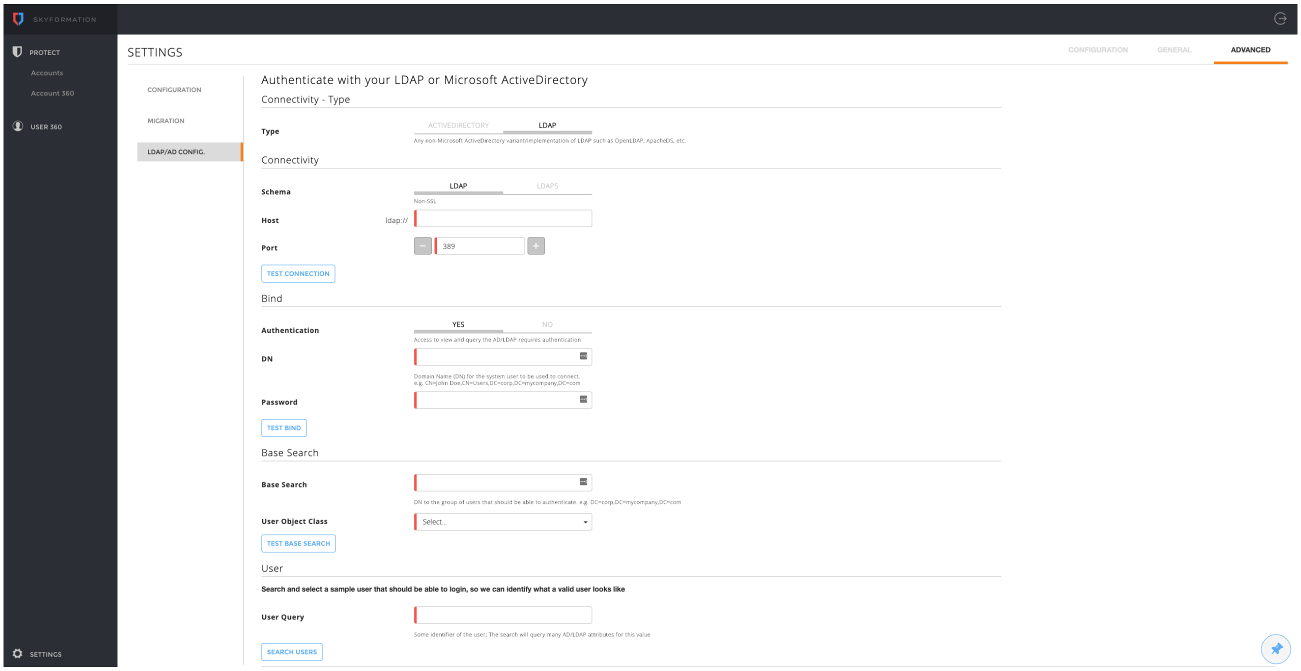
UI Page for Configuring Active Directory Authentication

Since 2.5.92

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



Authenticate with your LDAP or Microsoft ActiveDirectory

Connectivity - Type

Type: ACTIVEDIRECTORY | LDAP

Any non-Microsoft ActiveDirectory variant/implementation of LDAP such as OpenLDAP, ApacheDS, etc.

Connectivity

Schema: LDAP | LDAPS

Non-SSL

Host: ldap://

Port: 389

Bind

Authentication: YES | NO

Access to view and query the AD/LDAP requires authentication

DN

Domain Name (DN) for the system user to be used to connect.
e.g. CN=John Doe,CN=Users,DC=corp,DC=mycompany,DC=com

Password

Base Search

Base Search

DN to the group of users that should be able to authenticate. e.g. DC=corp,DC=mycompany,DC=com

User Object Class: Select...

User

Search and select a sample user that should be able to login, so we can identify what a valid user looks like

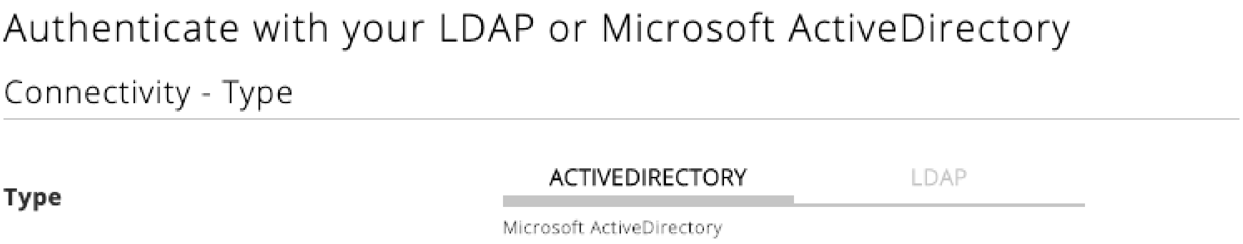
User Query

Some identifier of the user; The search will query many AD/LDAP attributes for this value

Type

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

- Select type **ACTIVE DIRECTORY**



Authenticate with your LDAP or Microsoft ActiveDirectory

Connectivity - Type

Type: ACTIVEDIRECTORY | LDAP

Microsoft ActiveDirectory

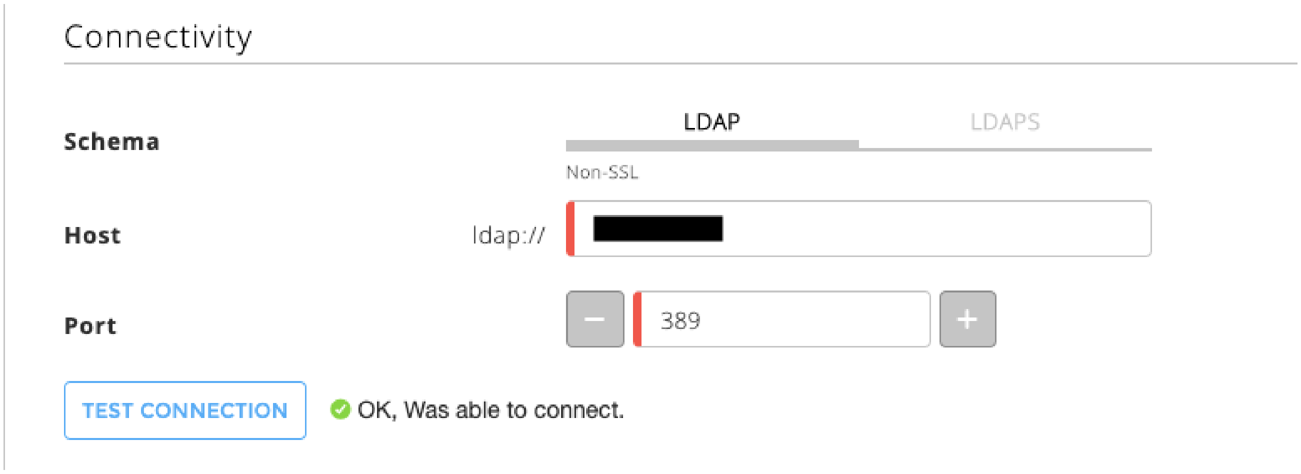
Connectivity

The goal of this section is to configure and test successful connection to the Active Directory

- 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



Connectivity

Schema: LDAP | LDAPS

Non-SSL

Host: ldap:// [redacted]

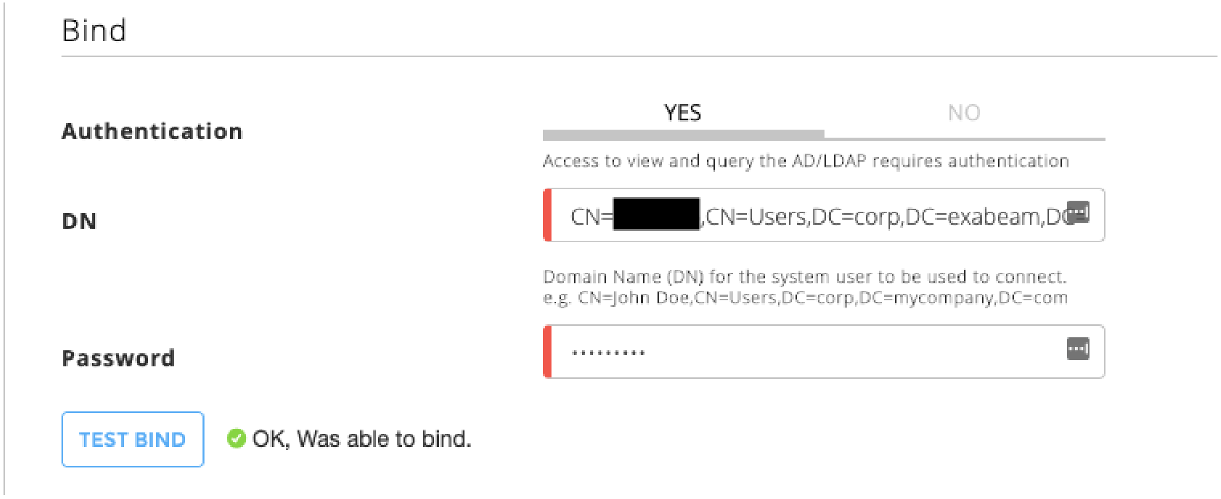
Port: − 389 +

TEST CONNECTION ✓ OK, Was able to connect.

Bind

The goal of this section is to configure and test successful binding to the Active Directory

- Authentication
  - If the Active Directory 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



Bind

Authentication: YES | NO

Access to view and query the AD/LDAP requires authentication

DN: CN=[redacted],CN=Users,DC=corp,DC=exabeam,DC

Domain Name (DN) for the system user to be used to connect.
e.g. CN=John Doe,CN=Users,DC=corp,DC=mycompany,DC=com

Password: ••••••••••

TEST BIND ✓ OK, Was able to bind.

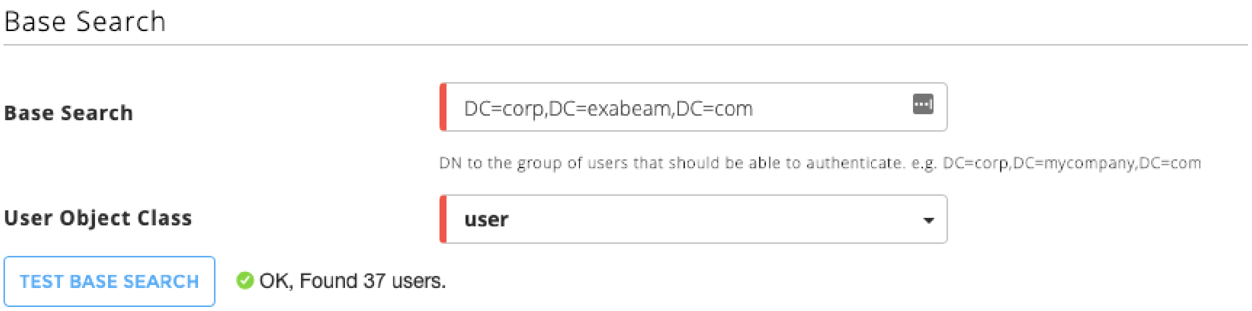
Base Search

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

- Insert he base search DN

> All users that should be authorized to CC and the Active Directory group 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 (**user** by default)
- TEST BASE SEARCH - only if test base search succeeds can you continue to the next User section



Base Search

Base Search DC=corp,DC=exabeam,DC=com

DN to the group of users that should be able to authenticate. e.g. DC=corp,DC=mycompany,DC=com

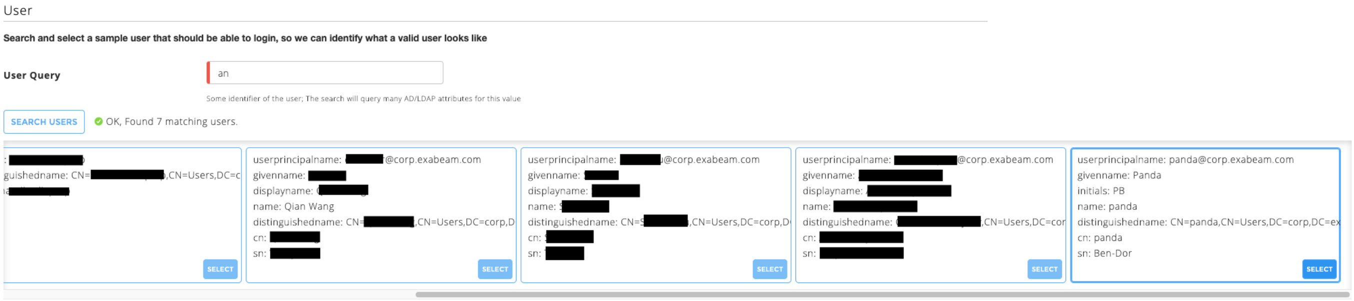
User Object Class user

OK, Found 37 users.

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 Active Directory group and an optional suffix.

- Insert substring of one of the the user’s identifying attributes (UserPrincipalName, name, display name, mail, DN, CN, sAMAccountName, …)
- Press the **SEARCH USERS**
- Scroll and find the user you are looking for
- **SELECT**



User

Search and select a sample user that should be able to login, so we can identify what a valid user looks like

User Query an

Some identifier of the user; The search will query many AD/LDAP attributes for this value

OK, Found 7 matching users.

: [redacted]
guishedname: CN=[redacted],CN=Users,DC=c
[redacted]

userprincipalname: [redacted]@corp.exabeam.com
givenname: [redacted]
displayname: [redacted]
name: Qian Wang
distinguishedname: CN=[redacted],CN=Users,DC=corp,D
cn: [redacted]
sn: [redacted]

userprincipalname: [redacted]@corp.exabeam.com
givenname: [redacted]
displayname: [redacted]
name: [redacted]
distinguishedname: CN=[redacted],CN=Users,DC=corp,D
cn: [redacted]
sn: [redacted]

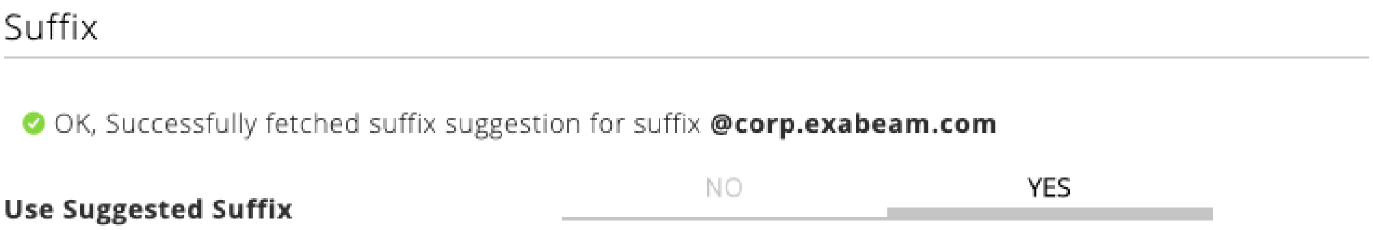
userprincipalname: [redacted]@corp.exabeam.com
givenname: [redacted]
displayname: [redacted]
name: [redacted]
distinguishedname: [redacted],CN=Users,DC=cor
cn: [redacted]
sn: [redacted]

userprincipalname: panda@corp.exabeam.com
givenname: Panda
initials: PB
name: panda
distinguishedname: CN=panda,CN=Users,DC=corp,DC=ex
cn: panda
sn: Ben-Dor

Suffix

In case the UserPrincipalName of the system user provided in the **bind** section and the UserPrincipalName of the user provided in the **user** section share a suffix, for example: **@myorg.com**, then the CC administrator would be asked whether or not to configure this suffix for all users and allow them to login by providing only the UserPrincipalName prefix

> If among the users that should access CC more than a single suffix exists (for example **@myorg.com** and **@myorg.co.uk**) a suffix should **not** be configured



Suffix

OK, Successfully fetched suffix suggestion for suffix **@corp.exabeam.com**

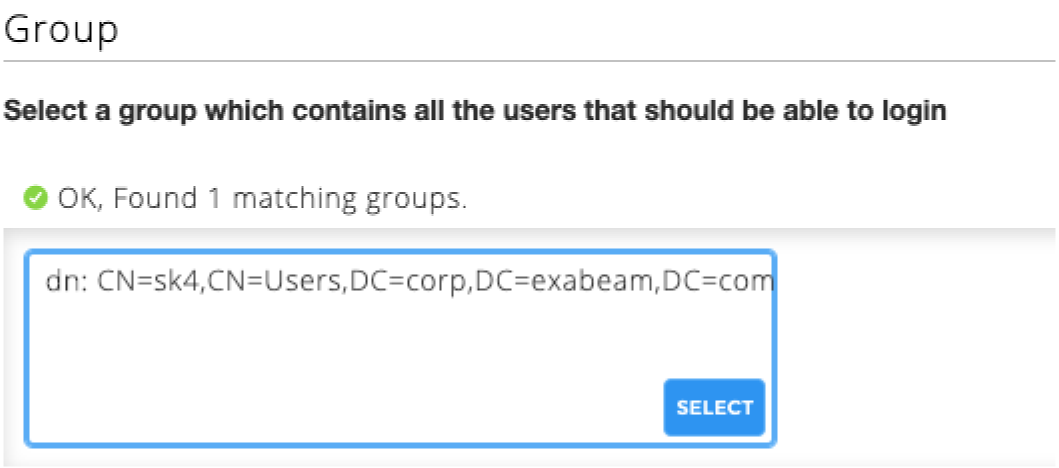
Use Suggested Suffix NO [✓ YES]

Group

The goal of this section is to select the Active Directory group whose members are the users in the organization that should be authorized to access CC. The groups CC administrator can select from are groups 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


Group

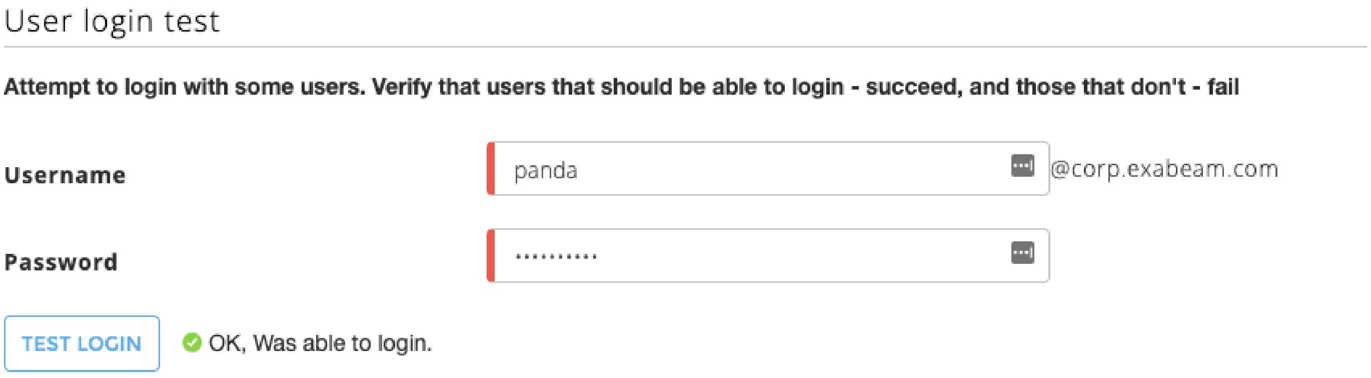
Select a group which contains all the users that should be able to login

✓ OK, Found 1 matching groups.

dn: CN=sk4,CN=Users,DC=corp,DC=exabeam,DC=com

User Login Test

The goal of this section is to test authentication and authorization of users using Microsoft Active Directory with the configuration provided. The expected username is the **UserPrincipalName** (without the suffix if such was configured)


User login test

Attempt to login with some users. Verify that users that should be able to login - succeed, and those that don't - fail

Username panda @corp.exabeam.com

Password ••••••••••

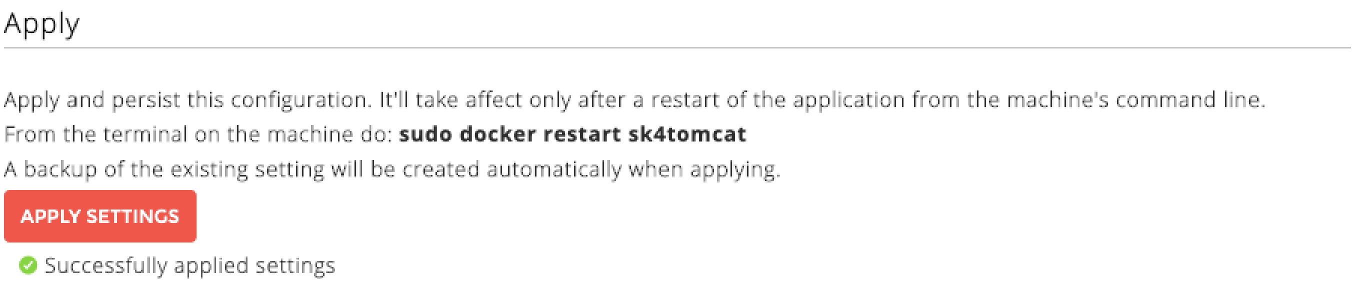
✓ OK, Was able to login.

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 Active Directory)



Apply and persist this configuration. It'll take affect only after a restart of the application from the machine's command line.
From the terminal on the machine do: **sudo docker restart sk4tomcat**
A backup of the existing setting will be created automatically when applying.

✓ Successfully applied settings

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
   ```