MachPanel KeyCloak SSO Authentication

Summary

This article provides you information about how to configure MachPanel KeyCloak SSO Authentication in MachPanel.

Applies to

Applies to MachPanel v7.2.11 and above.

KeyCloak Single-Sign On Overview

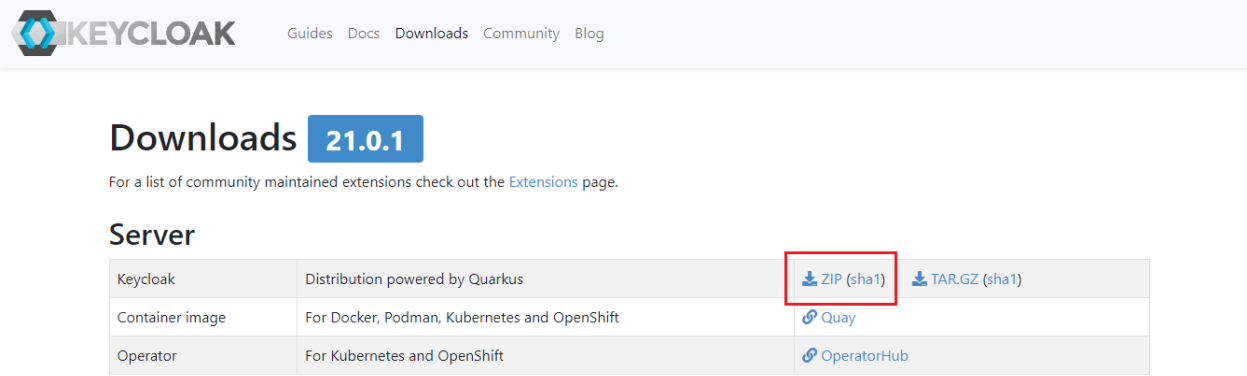
KeyCloak is an Open Source Identity and Access Management. It is used to Add authentication to applications and secure services with minimum effort.

Users authenticate with KeyCloak rather than individual applications. This means that your applications don't have to deal with login forms, authenticating users, and storing users. Once logged-in to KeyCloak, users don't have to login again to access a different application.This also applied to logout. KeyCloak provides single-sign out, which means users only have to logout once to be logged-out of all applications that use KeyCloak.

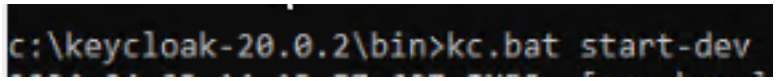
Integrating KeyCloak SSO with MachPanel

Step 1:

- Download KeyCloak



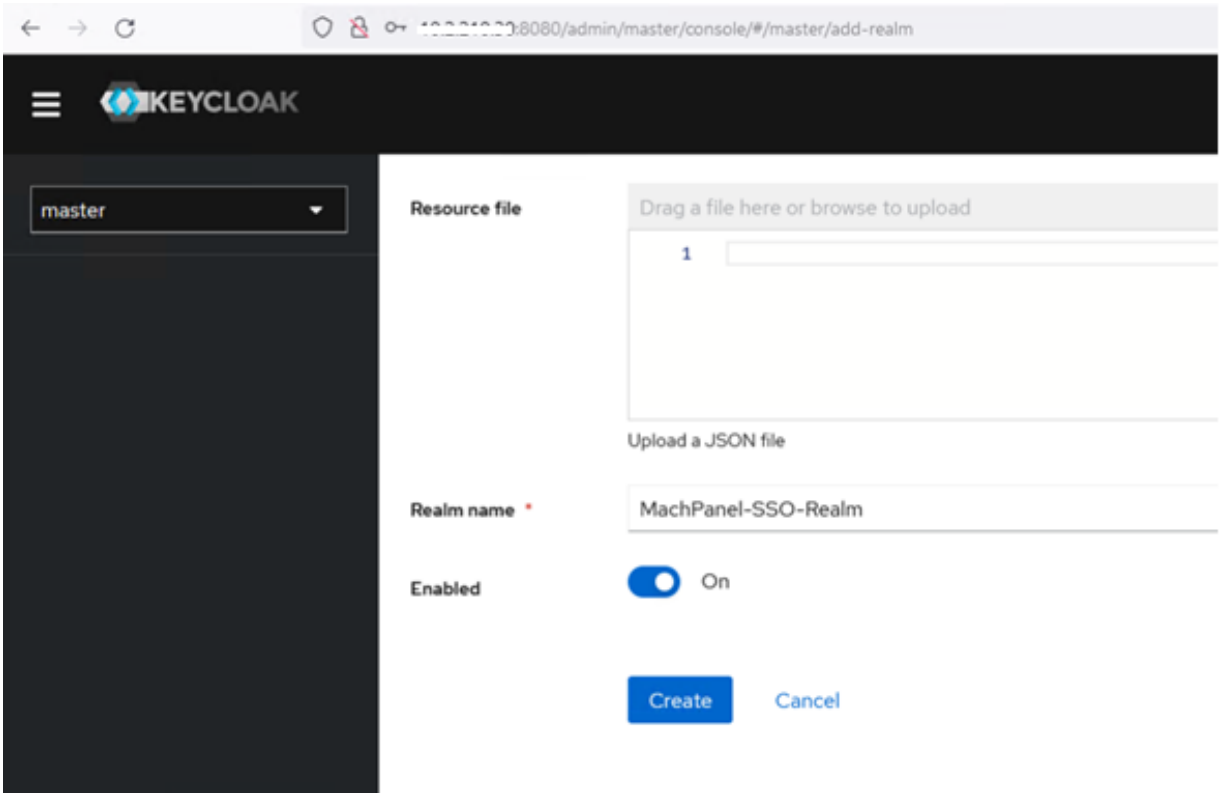
- Unzip the Package.
- Open CMD and navigate to BIN folder inside the directory containing the unzipped package.
- Execute: **kc.bat start-dev**



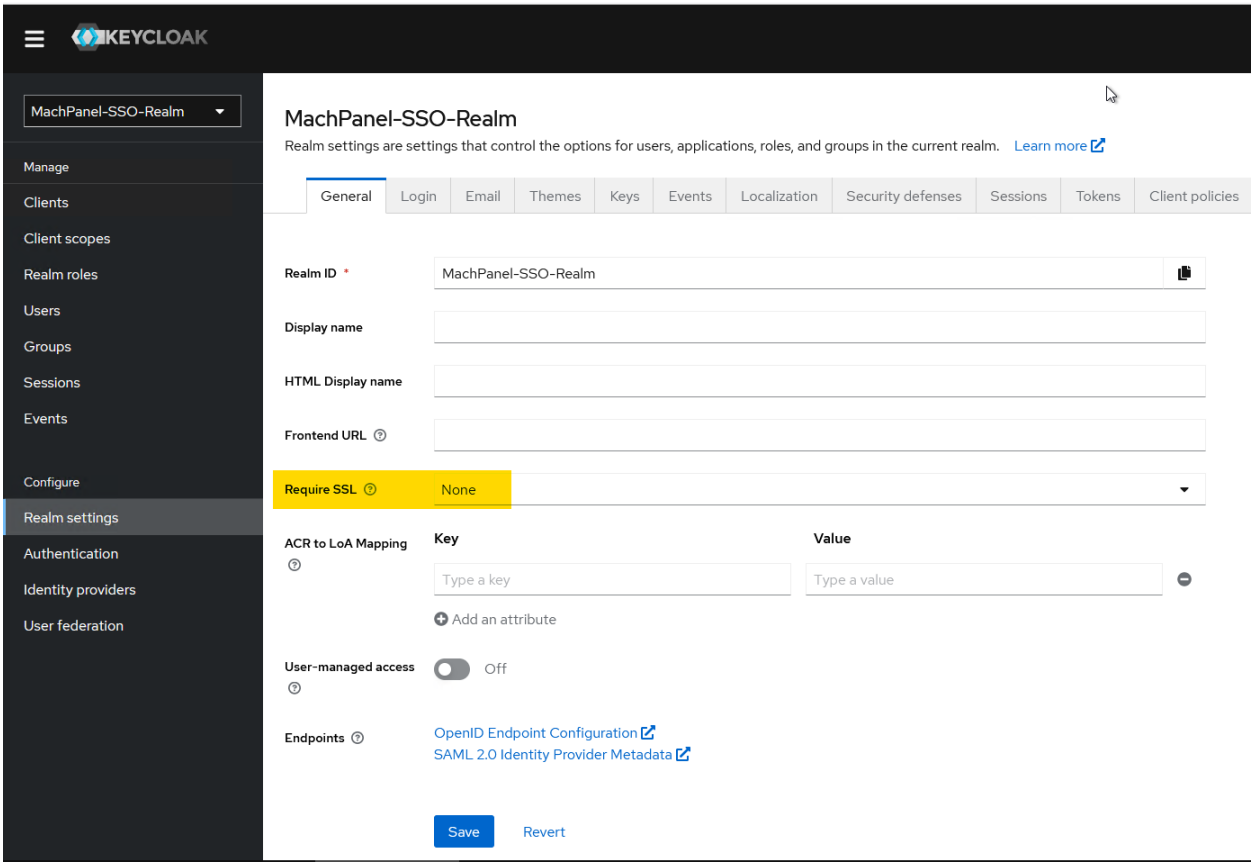
- Browse **https://<IP.of.KeyCloak.Machine>:8080** (Replace "<IP.of.KeyCloak.Machine>" with the IP of KeyCloak Server.
- Create Admin user for Master Realm. Like:
  - Username: Admin
  - Password: Admin
- Login via Admin User.

Step 2: (If you already have Realm available then Skip this step and move to Next Step)

- Always create New Realm. Do not use Master Realm

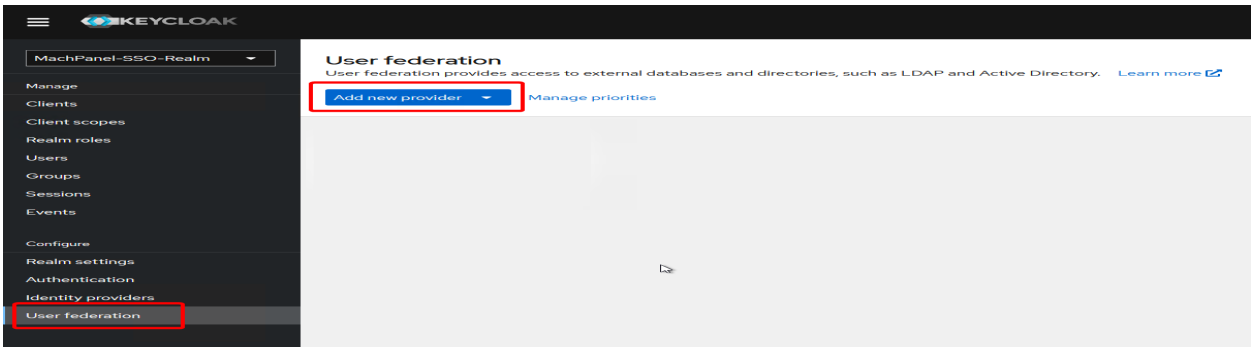


After creation go to Realm Settings and set "Require SSL" to "None".



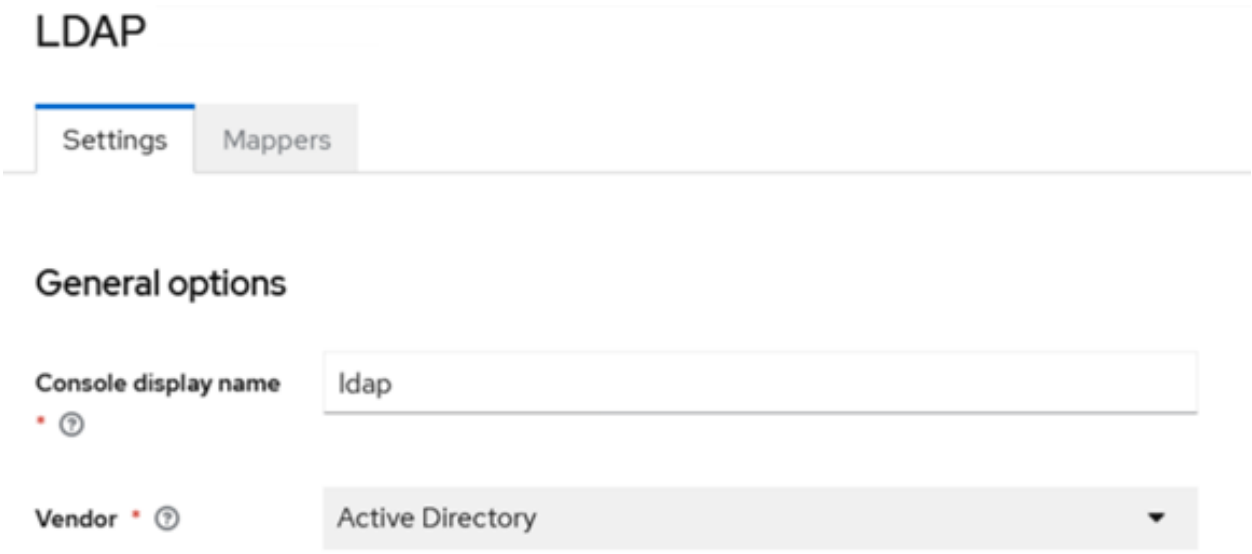
Step 3: Configure "User Federation" (If you already have Federation Configured then Skip this step and move to Next Step)

- Navigate to "User Federation" and click on "Add new Provider" button:

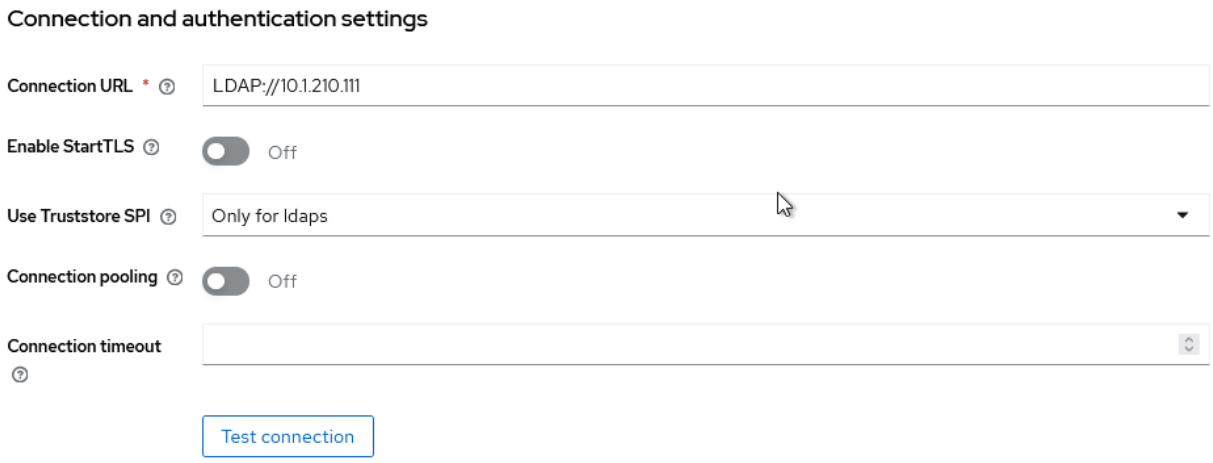


Configure as follows:

Set "Console display name" and select "Vendor" as "Active Directory" from drop down:



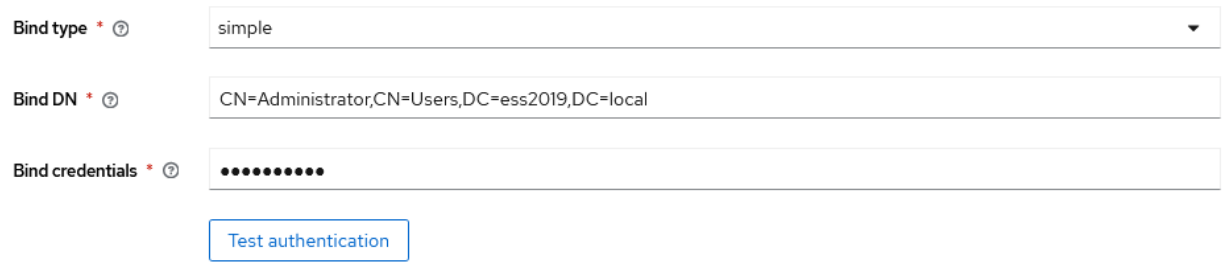
Set "Connection URL" as LDAP://<AD Server IP>:



Set "Bind Type" as "Simple".

Set "Bind DN" by copying "Distinguished Name" of your "Administrator" account.

Set "Password" of the Administrator account.

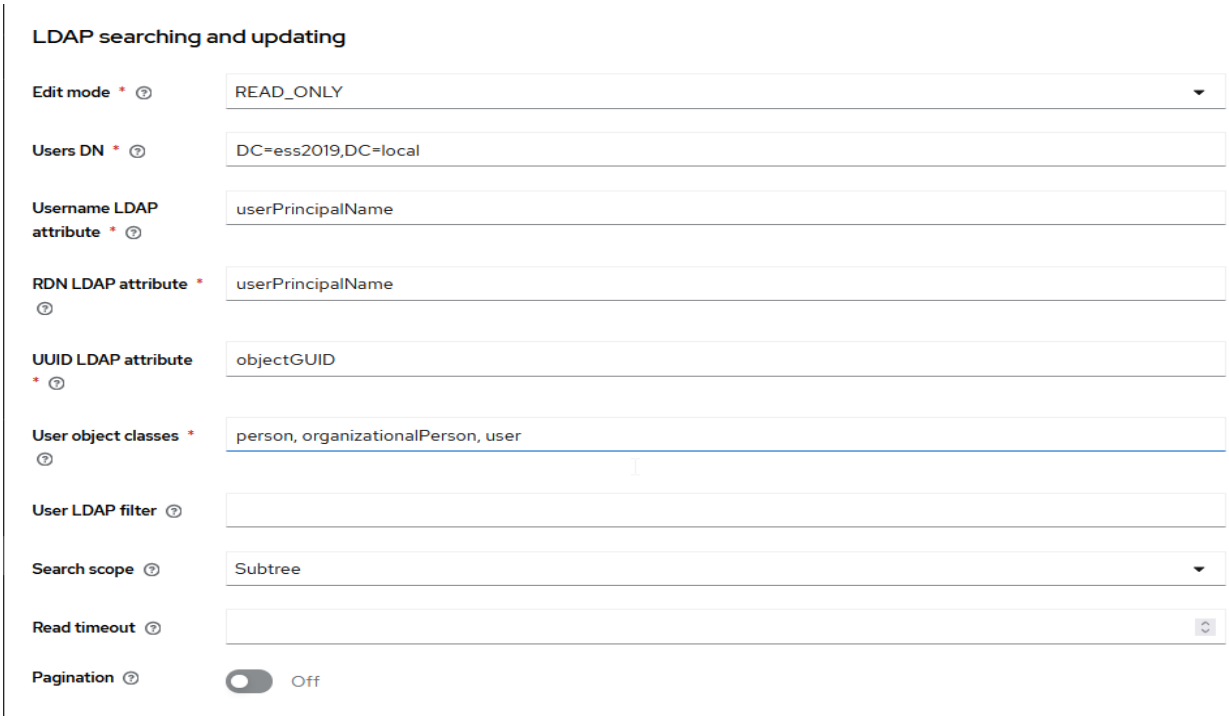


Configure LDAP Settings for searching and updating users from AD to Realm as follows:

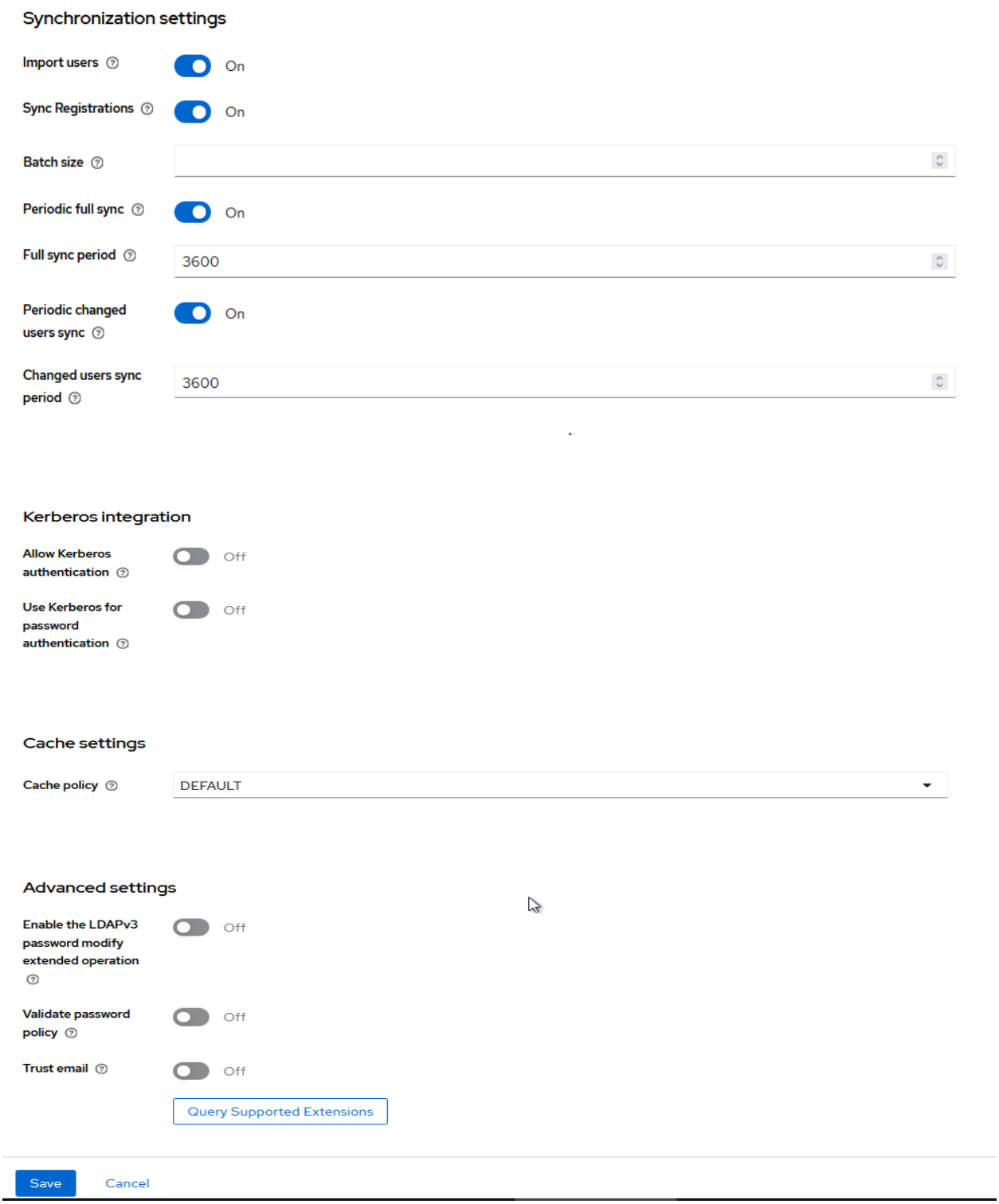
"Users DN" = Distinguished Name of OU from where the users have to be searched / updated.

"Username LDAP Attribute" = Attribute that needs to be used for login authentication. Set "userPrincipalName" here.

Set other parameters as follows:

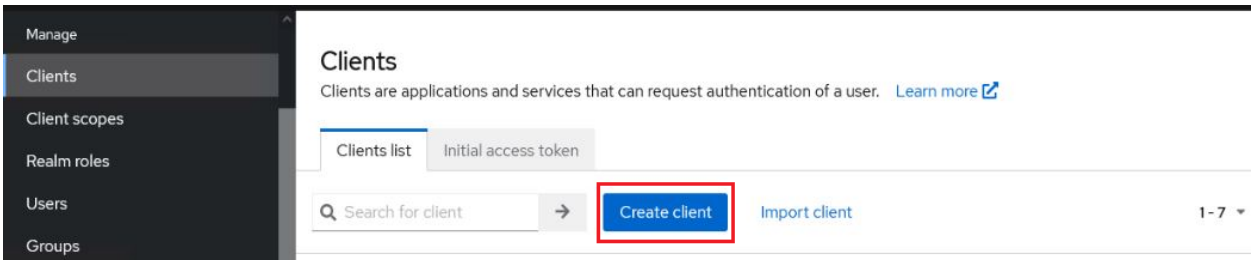


Set "Synchronization Settings", "Kerberos Integration" and "Advanced settings" as shown below and finally hit "Save" button:

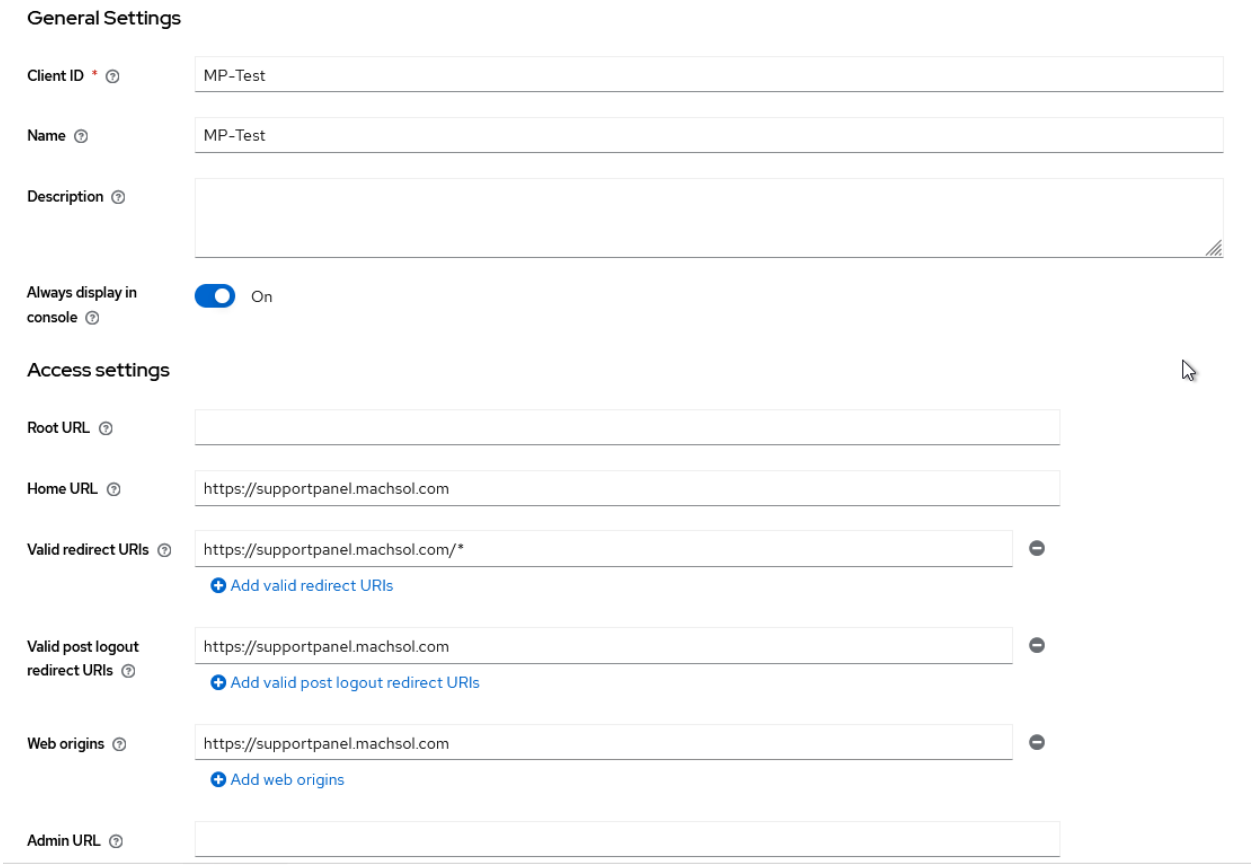


Step 4: Create and Configure Client:

Navigate to "Clients" under Newly configured Realm and click on "Create Client" button:

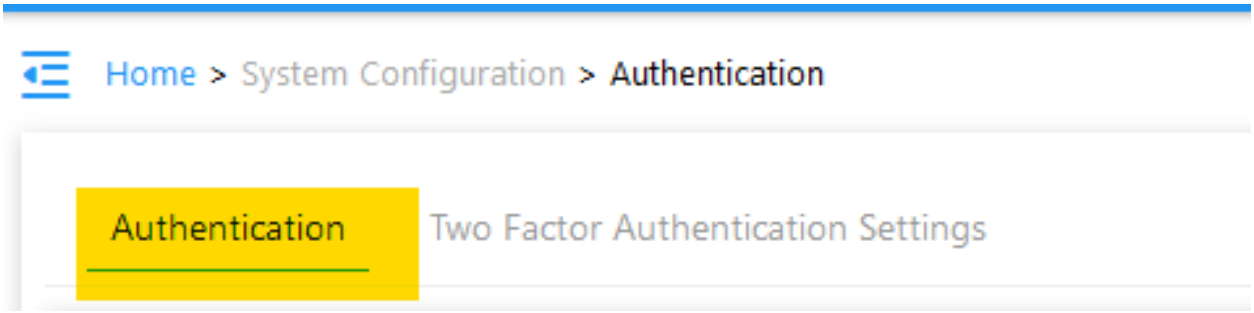


Configure as follows (replace **https://supportpanel.machsol.com** with **https://<yourpanel.yourdomain.com>** where applies):



Step 5 (Configure MachPanel to work with KeyCloak):

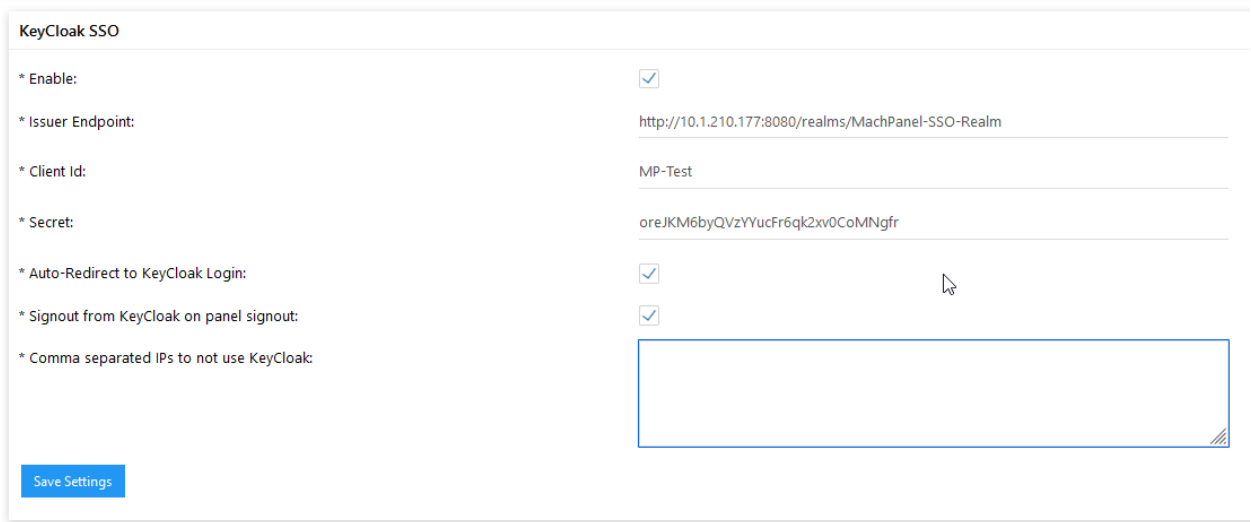
- Configure following in MachPanel, Navigate to **Home > System Configuration > Authentication** being logged in as Provider in MachPanel:



Scroll down to enable "KeyCloak SSO" and enter the required details:

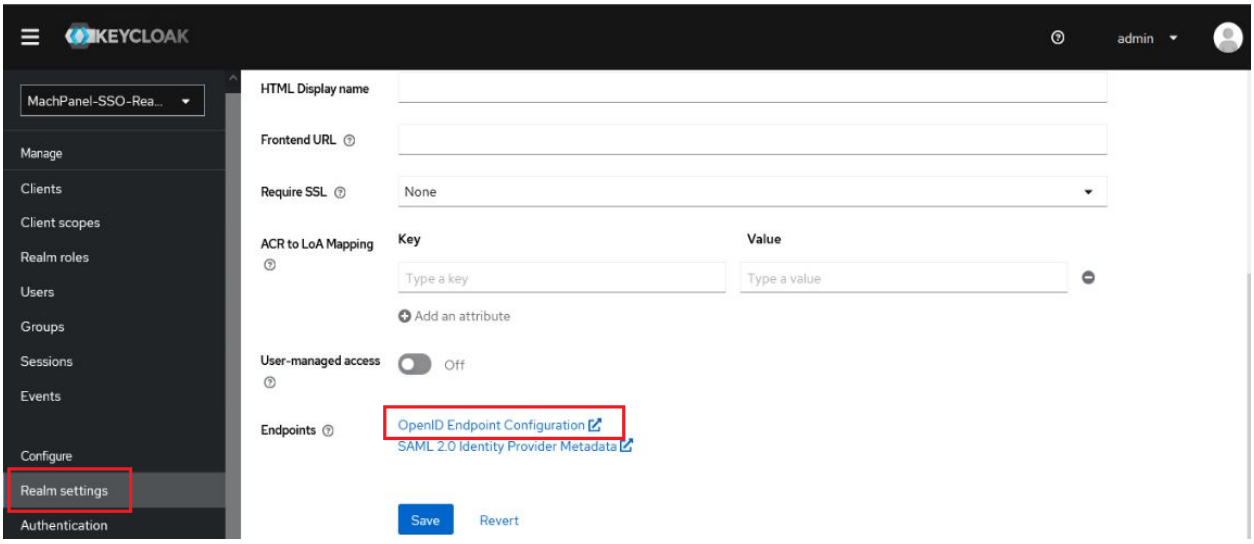
Make sure the "Issuer Endpoint" URL is accessible from MachPanel Control Panel server.

Its up to you to enable or disable the "Auto-Redirect to KeyCloak Login" and "Signout from KayCloak on panel Signout" options.

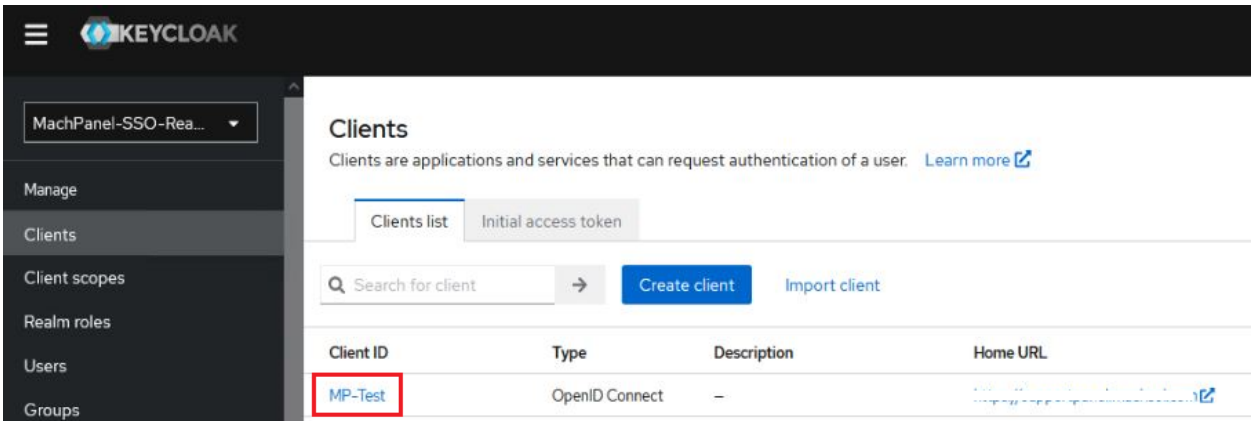


MachPanel KeyCloak SSO Authentication

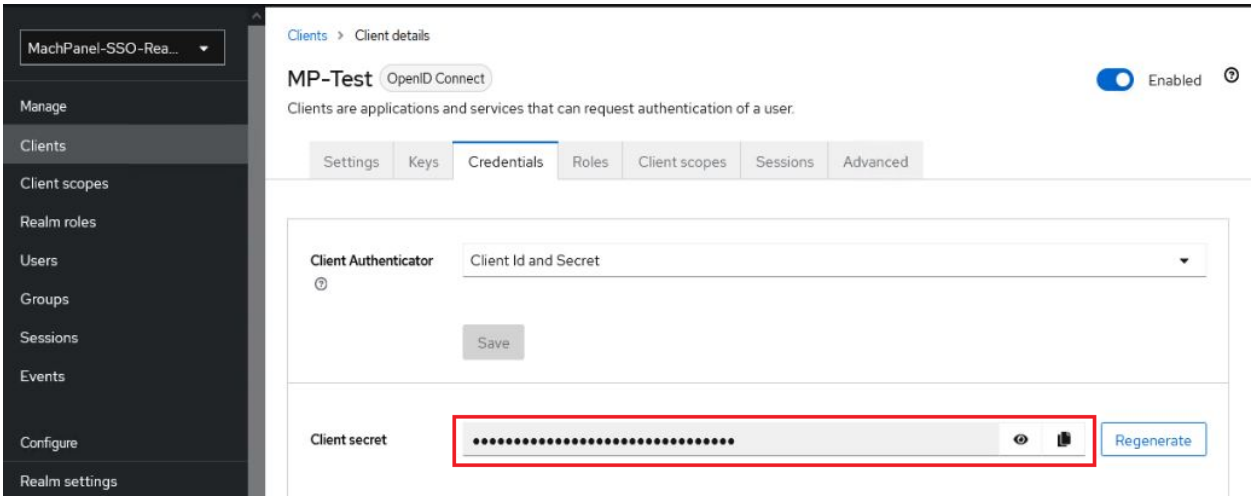
You can get "Issuer Endpoint" from following interface in "KayCloak":



You can get "Client Id" from following interface in KeyCloak:

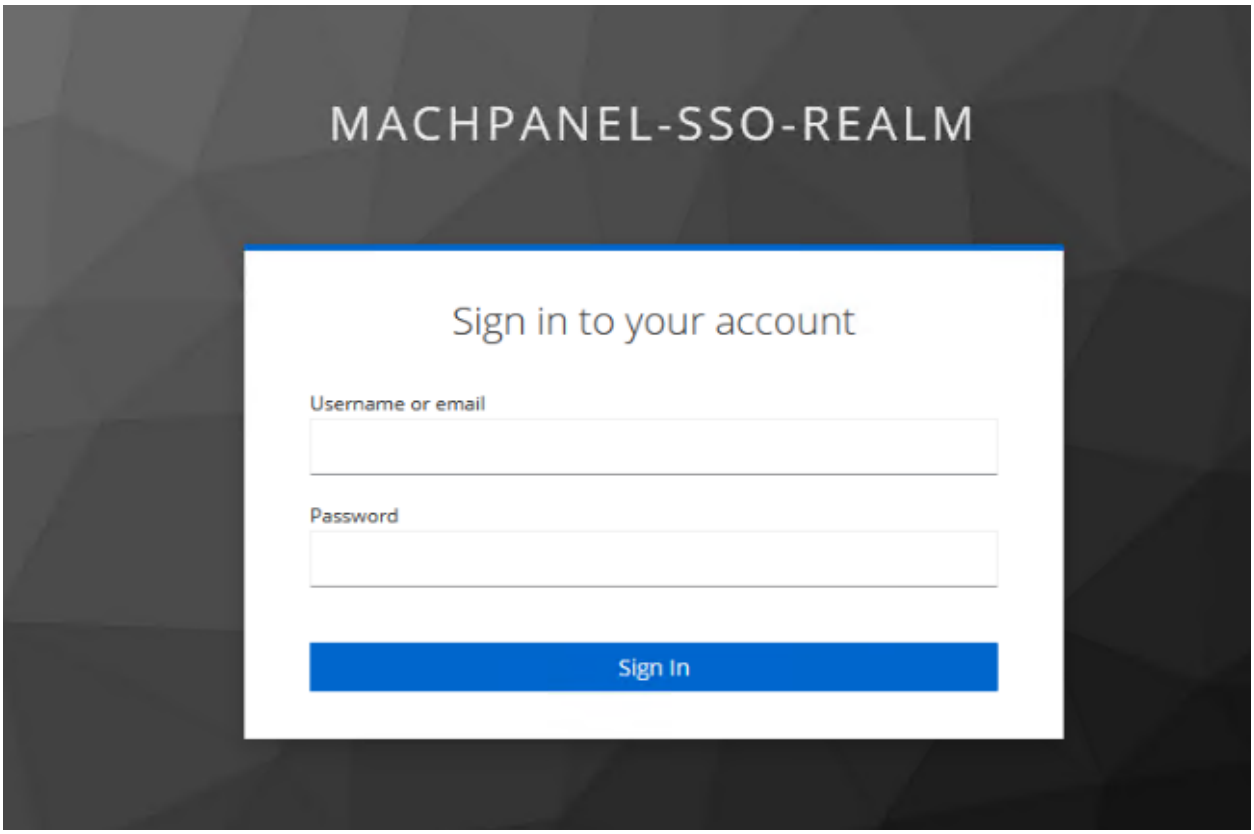


Lastly, you can get "Client Secret" by clicking on "Client ID" and then going to "Credentials" tab:



After setting all the values in MachPanel, hit save and your panel will start redirecting to KeyCloak Login Page for authentication.

- After that when you try to login to your panel you will be redirected to KeyCoak Sign showing the Machpanel SSO Realm Name in title:



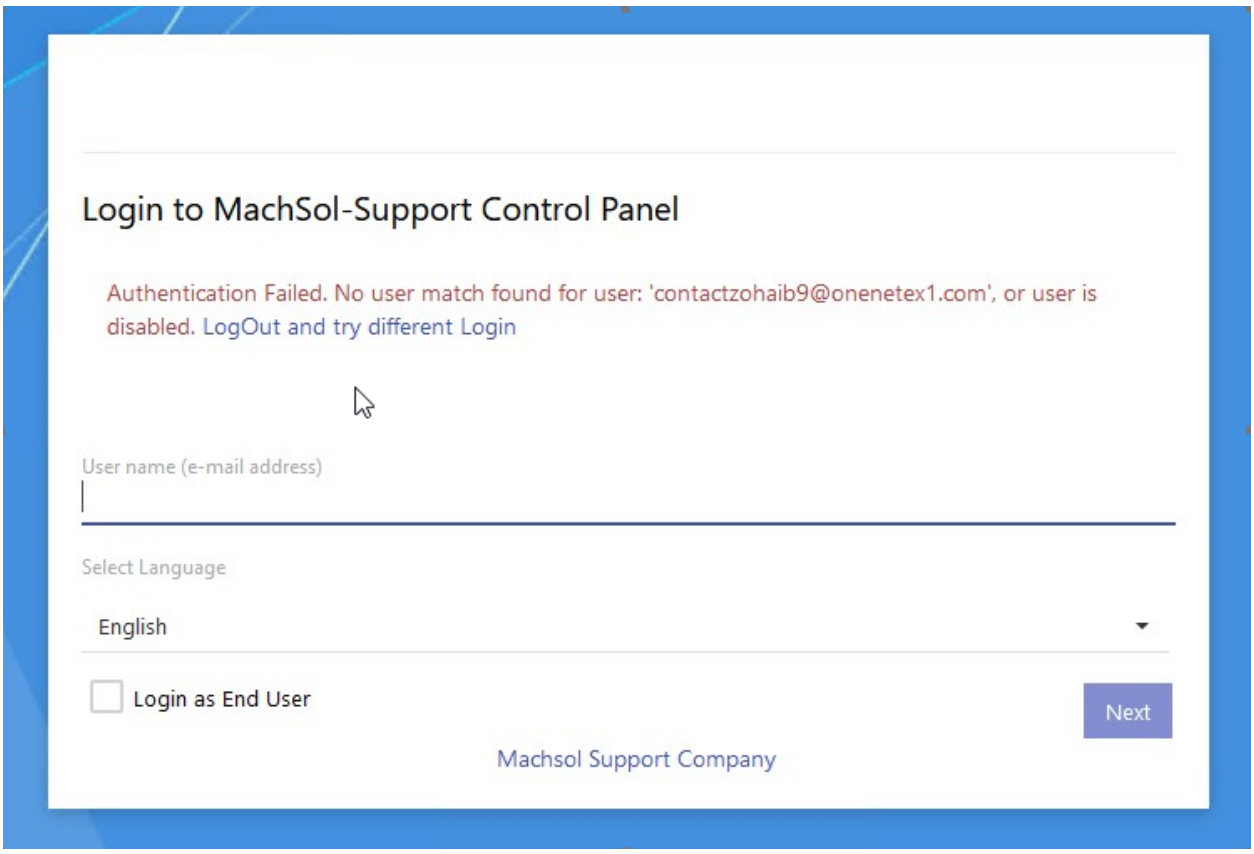
Step 6: Lastly you must associate AD Accounts with Staff and/or Customer Accounts and Contacts:

Before Login, ensure that you associate your Provider/Provider Staff, Reseller/Reseller Staff, Customer and Customer Contacts with appropriate AD Accounts in MachPanel.

You can do that by following the details on KB link below:

https://kb.machsol.com/Knowledgebase/55606/Authenticate-Active-Directory-user-Staff-Customer-and-Co

If you login to KeyCloak via a user that exists in AD and is able to authenticate, but its not associated with any staff/customer/contact in MachPanel, then you will get an error as follows:



MachPanel KeyCloak SSO Authentication

Clicking on the link will log you out of KeyCloak and allow you to login again using a correct user.

If there is ever any issue and you want to update configuration of MachPanel but cannot login due to issue with KeyCloak configuration, you can login to MachPanel directly 'bypassing SSO' by using **"http://localhost:786"** directly on the control panel server (the default URL for MachPanel).

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/55740/MachPanel-KeyCloak-SSO-Authentic...