

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](#)

 **KEYCLOAK**

Guides Docs Downloads Community Blog

Downloads

21.0.1

For a list of community maintained extensions check out the [Extensions](#) page.

Server

Keycloak	Distribution powered by Quarkus	ZIP (sha1)	TAR.GZ (sha1)
Container image	For Docker, Podman, Kubernetes and OpenShift	Quay	
Operator	For Kubernetes and OpenShift	OperatorHub	

MachPanel KeyCloak SSO Authentication

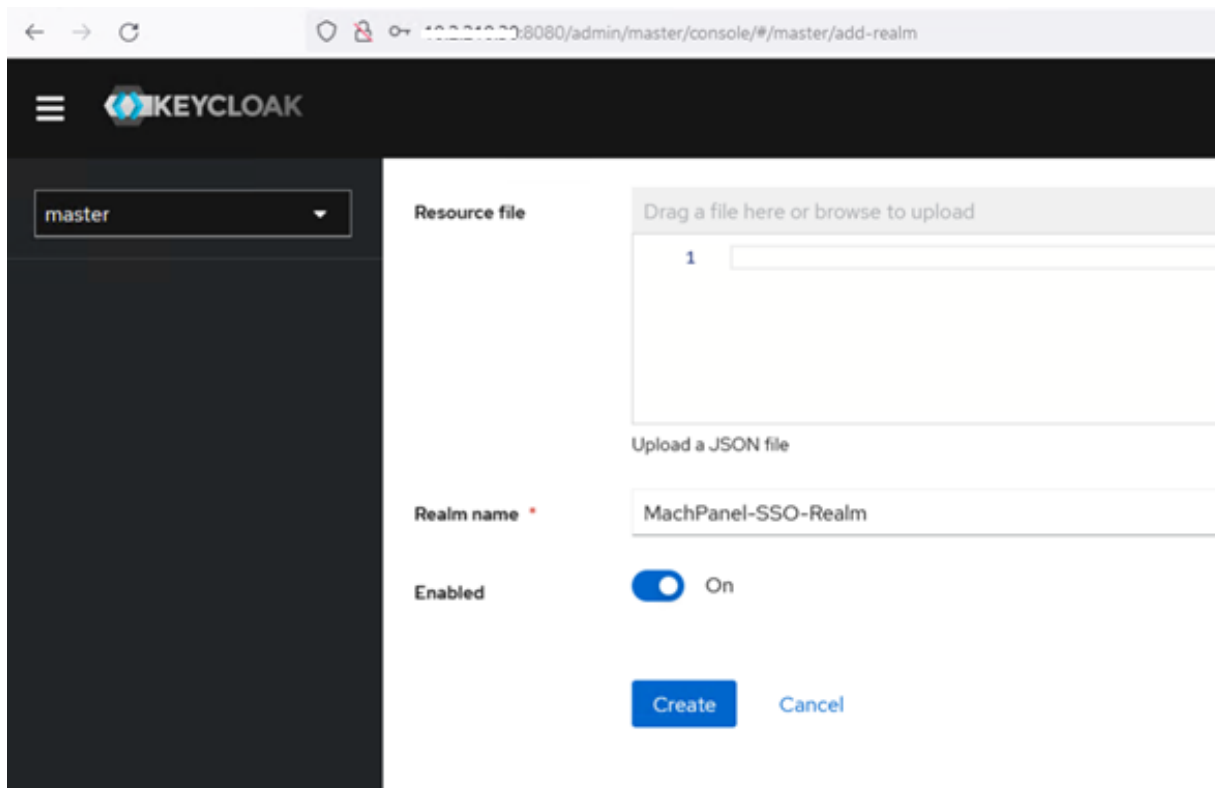
- Unzip the Package.
- Open CMD and navigate to BIN folder inside the directory containing the unzipped package.
- Execute: **kc.bat start-dev**

```
c:\keycloak-20.0.2\bin>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:
 - o Username: Admin
 - o 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**



The screenshot shows the Keycloak Admin Console interface. The browser address bar indicates the URL: `https://192.168.1.10:8080/admin/master/console/#/master/add-realm`. The interface has a dark sidebar on the left with the Keycloak logo and a dropdown menu showing 'master'. The main content area is titled 'Resource file' and contains a file upload section with the text 'Drag a file here or browse to upload' and a list item '1'. Below this is a section for 'Realm name' with a text input field containing 'MachPanel-SSO-Realm'. There is also an 'Enabled' toggle switch which is currently turned 'On'. At the bottom right, there are 'Create' and 'Cancel' buttons.

MachPanel KeyCloak SSO Authentication

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

The screenshot shows the Keycloak administration interface for the 'MachPanel-SSO-Realm'. The left sidebar contains a menu with options like 'Manage', 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', 'Authentication', 'Identity providers', and 'User federation'. The 'Realm settings' section is active, showing tabs for 'General', 'Login', 'Email', 'Themes', 'Keys', 'Events', 'Localization', 'Security defenses', 'Sessions', 'Tokens', and 'Client policies'. The 'General' tab is selected, displaying fields for 'Realm ID' (MachPanel-SSO-Realm), 'Display name', 'HTML Display name', and 'Frontend URL'. The 'Require SSL' dropdown is highlighted in yellow and set to 'None'. Below this, there is a table for 'ACR to LoA Mapping' with columns for 'Key' and 'Value'. The 'User-managed access' toggle is set to 'Off'. At the bottom, there are links for 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata', and 'Save' and 'Revert' buttons.

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

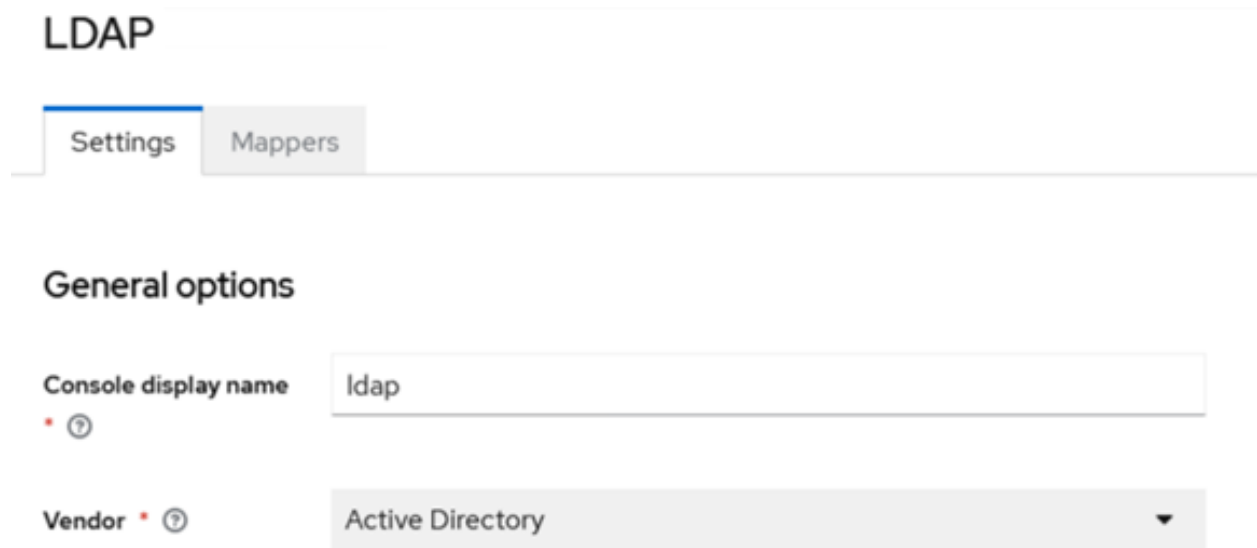
- Navigate to "User Federation" and click on "Add new Provider" button:

The screenshot shows the Keycloak administration interface for the 'MachPanel-SSO-Realm', specifically the 'User federation' tab. The left sidebar is the same as in the previous screenshot, but the 'User federation' option is highlighted. The 'User federation' tab is selected, displaying a description: 'User federation provides access to external databases and directories, such as LDAP and Active Directory.' Below this, there is a blue button labeled 'Add new provider' which is highlighted with a red box. To the right of this button is a link for 'Manage priorities'.

MachPanel KeyCloak SSO Authentication

Configure as follows:

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



LDAP

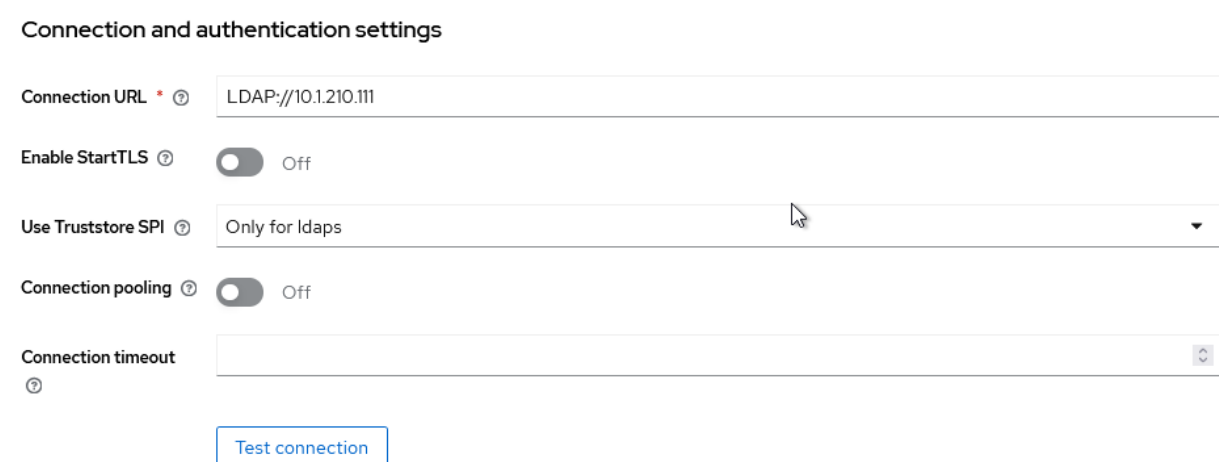
Settings Mappers

General options

Console display name

Vendor

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



Connection and authentication settings

Connection URL

Enable StartTLS ☐ Off

Use Truststore SPI

Connection pooling ☐ Off

Connection timeout

[Test connection](#)

Set "Bind Type" as "Simple".

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

MachPanel KeyCloak SSO Authentication

Set "Password" of the Administrator account.

Bind type * ?	<input type="text" value="simple"/>
Bind DN * ?	<input type="text" value="CN=Administrator,CN=Users,DC=ess2019,DC=local"/>
Bind credentials * ?	<input type="password" value="••••••••"/>
<input type="button" value="Test authentication"/>	

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:

LDAP searching and updating	
Edit mode * ?	<input type="text" value="READ_ONLY"/>
Users DN * ?	<input type="text" value="DC=ess2019,DC=local"/>
Username LDAP attribute * ?	<input type="text" value="userPrincipalName"/>
RDN LDAP attribute * ?	<input type="text" value="userPrincipalName"/>
UUID LDAP attribute * ?	<input type="text" value="objectGUID"/>
User object classes * ?	<input type="text" value="person, organizationalPerson, user"/>
User LDAP filter ?	<input type="text"/>
Search scope ?	<input type="text" value="Subtree"/>
Read timeout ?	<input type="text"/>
Pagination ?	<input type="checkbox"/> Off

MachPanel KeyCloak SSO Authentication

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

Synchronization settings

Import users ⓘ ☒ On

Sync Registrations ⓘ ☒ On

Batch size ⓘ

Periodic full sync ⓘ ☒ On

Full sync period ⓘ

Periodic changed users sync ⓘ ☒ On

Changed users sync period ⓘ

Kerberos integration

Allow Kerberos authentication ⓘ ☐ Off

Use Kerberos for password authentication ⓘ ☐ Off

Cache settings

Cache policy ⓘ

Advanced settings

Enable the LDAPv3 password modify extended operation ⓘ ☐ Off

Validate password policy ⓘ ☐ Off

Trust email ⓘ ☐ Off

[Query Supported Extensions](#)

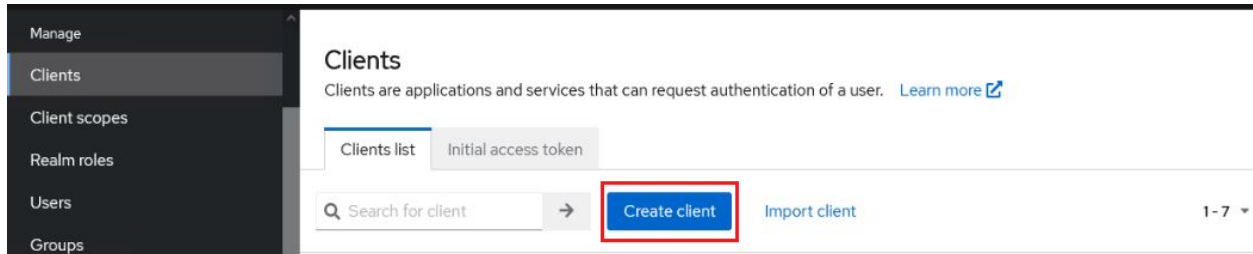
[Save](#)

[Cancel](#)

MachPanel KeyCloak SSO Authentication

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):

General Settings

Client ID * ⓘ MP-Test

Name ⓘ MP-Test

Description ⓘ

Always display in console ⓘ ☒ On

Access settings

Root URL ⓘ

Home URL ⓘ https://supportpanel.machsol.com

Valid redirect URIs ⓘ https://supportpanel.machsol.com/* ⊖
[+ Add valid redirect URIs](#)

Valid post logout redirect URIs ⓘ https://supportpanel.machsol.com ⊖
[+ Add valid post logout redirect URIs](#)

Web origins ⓘ https://supportpanel.machsol.com ⊖
[+ Add web origins](#)

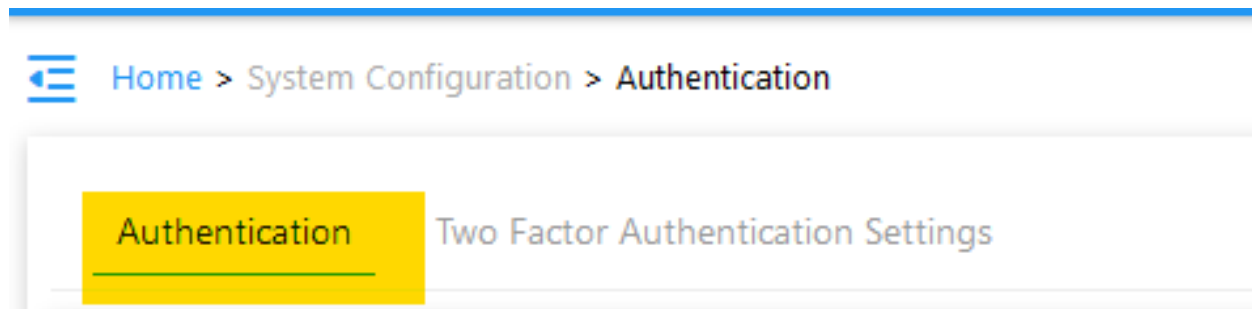
Admin URL ⓘ

MachPanel KeyCloak SSO Authentication



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:

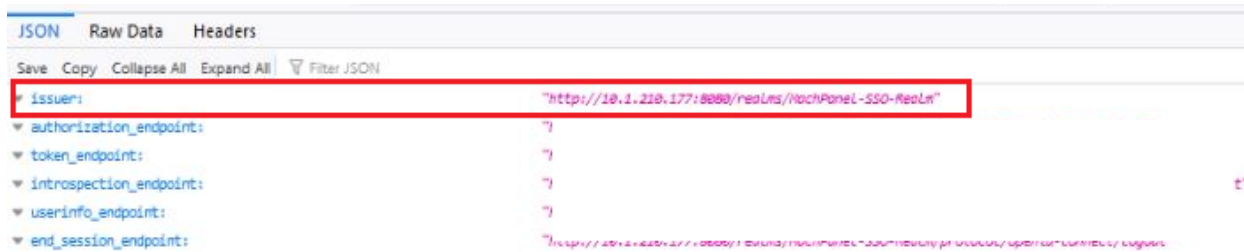
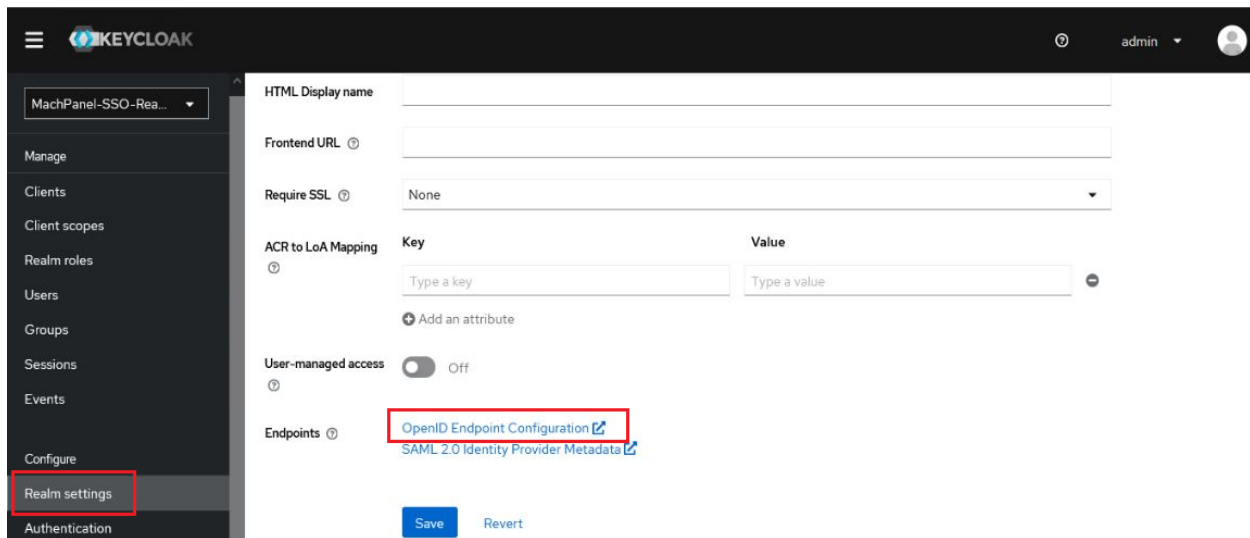
Make sure the "Issuer Endpoint" URL is accessible from MachPanel Control Panel server.

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

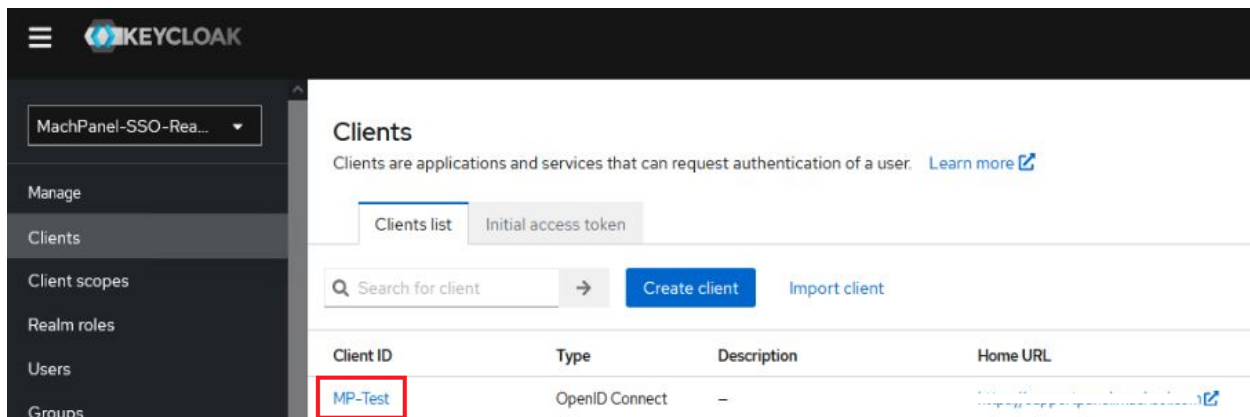
KeyCloak SSO	
* Enable:	<input checked="" type="checkbox"/>
* Issuer Endpoint:	<input type="text" value="http://10.1.210.177:8080/realms/MachPanel-SSO-Realm"/>
* Client Id:	<input type="text" value="MP-Test"/>
* Secret:	<input type="text" value="oreJKM6byQVzYYucFr6qk2xv0CoMNgfr"/>
* Auto-Redirect to KeyCloak Login:	<input checked="" type="checkbox"/>
* Signout from KeyCloak on panel signout:	<input checked="" type="checkbox"/>
* Comma separated IPs to not use KeyCloak:	<input type="text"/>
<input type="button" value="Save Settings"/>	

MachPanel KeyCloak SSO Authentication

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

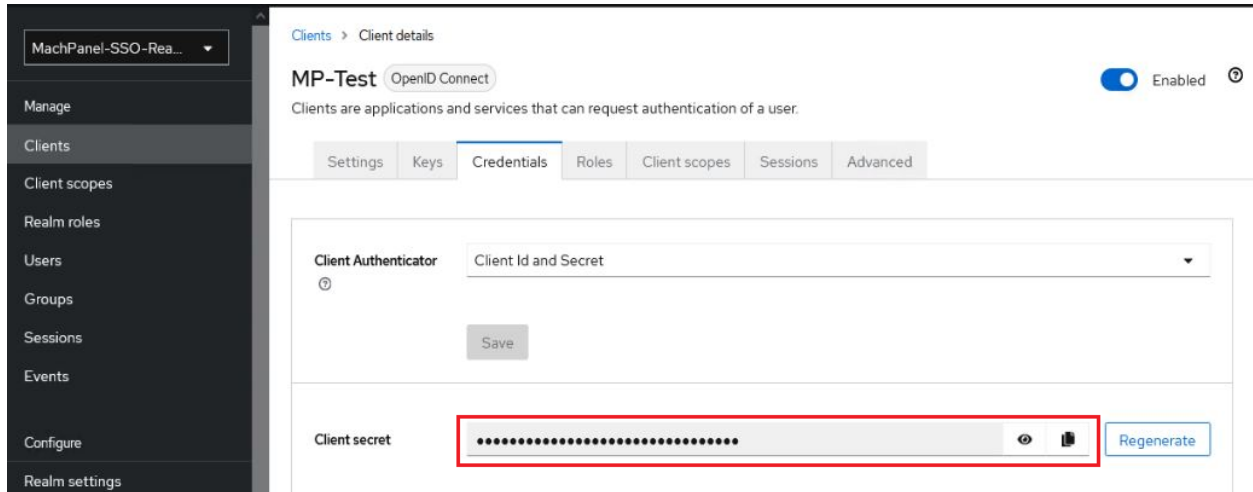


You can get "Client Id" from following interface in KeyCloak:



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

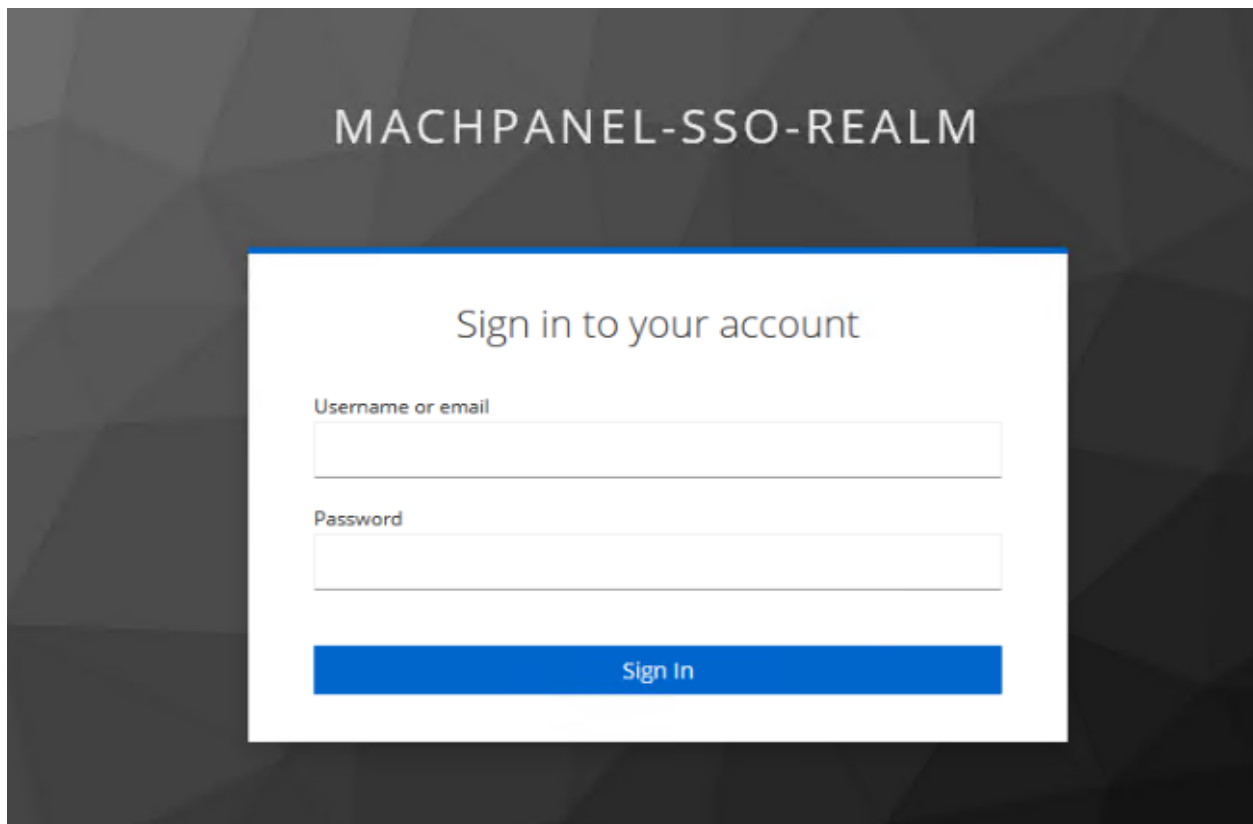
MachPanel KeyCloak SSO Authentication



The screenshot shows the Keycloak Admin Console interface. On the left is a sidebar with navigation links: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, and Realm settings. The main content area is titled 'Clients > Client details' and shows the configuration for a client named 'MP-Test' using 'OpenID Connect'. The 'Enabled' toggle is turned on. Below the client name are tabs for Settings, Keys, Credentials (selected), Roles, Client scopes, Sessions, and Advanced. The 'Credentials' tab contains a 'Client Authenticator' dropdown set to 'Client Id and Secret' and a 'Save' button. Below this is the 'Client secret' section, which includes a masked secret field (indicated by dots) and a 'Regenerate' button. A red rectangular box highlights the 'Client secret' field.

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:



The screenshot shows the Keycloak login page. The background is dark with a geometric pattern. At the top, the text 'MACHPANEL-SSO-REALM' is displayed in white. Below this is a white rectangular box containing the login form. The form has the title 'Sign in to your account' and two input fields: 'Username or email' and 'Password'. At the bottom of the form is a blue button labeled 'Sign In'.

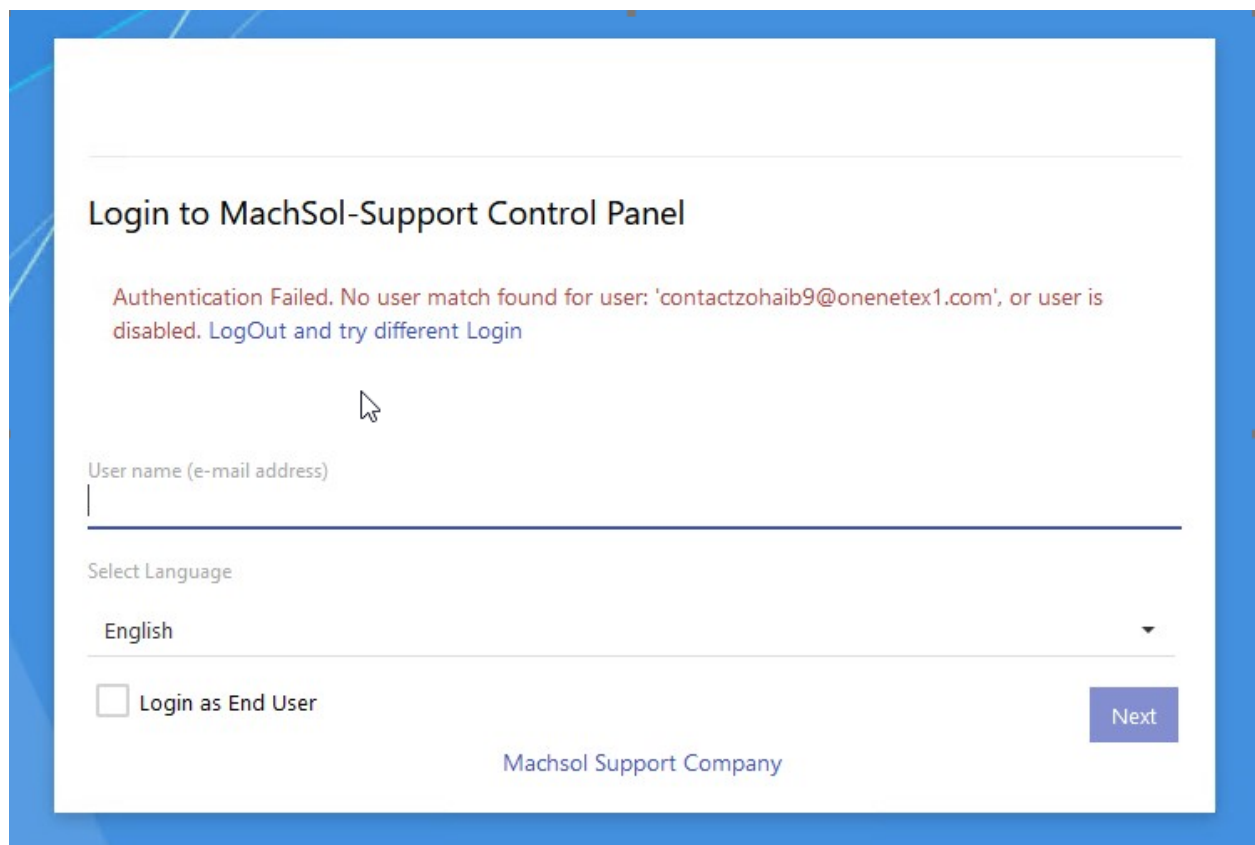
Step 6: Lastly you must associate AD Accounts with Staff and/or Customer Accounts and Contacts:

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:



The screenshot shows a login page for the MachSol-Support Control Panel. The page has a blue header and a white main content area. The title "Login to MachSol-Support Control Panel" is displayed. Below the title, a red error message states: "Authentication Failed. No user match found for user: 'contactzohaib9@onenetex1.com', or user is disabled. LogOut and try different Login". Below the error message, there is a text input field for "User name (e-mail address)" and a "Select Language" dropdown menu currently set to "English". At the bottom left, there is a checkbox labeled "Login as End User". At the bottom right, there is a blue "Next" button. The footer of the page reads "Machsol Support Company".

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...>