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

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

← → C 0 8	0- 1000000:8080/admin	/master/console/#/master/add-realm
master -	Resource file	Drag a file here or browse to upload
		Upload a JSON file
	Realm name	MachPanel-SSO-Realm
	Enabled	On On
		Create Cancel

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

MachPanel-SSO-Realm	MachPanel-SS	50-Realm	ntions for us		tions roles a	ad groups in the surrout re			
Manage	Real in settings are se	tungs that control the c	ptions for us	sers, applica	tions, roles, a	in groups in the current re		nore 🖸	
Clients	General Log	gin Email Them	es Keys	Events	Localizatio	on Security defenses	Sessions	Tokens	Client policies
Client scopes									
Realm roles	Realm ID *	MachPanel-SSO-Re	alm						نل
Users	Display name								
Groups	Display hame								
Sessions	HTML Display name								
Events	Frontend URL ③								
Configure	Require SSL ③	None							•
Realm settings		Kov				Value			
Authentication	ACR to LoA Mapping	Ney				value			
Identity providers		Type a key				Type a value			•
User federation		🔂 Add an attribute							
	User-managed access	Off							
	Endpoints ⑦	OpenID Endpoint Co SAML 2.0 Identity Pr	nfiguration 🖸	data 🗹					
		Save Revert							

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:

MachPanel-SSO-Realm +	User federation
Manage	
Clients	Add new provider - Manage priorities
Client scopes	
Realm roles	
Users	
Groups	
Sessions	
Events	
Configure	
Realm settings	
Authentication	
Identity providers	
User federation	

Configure as follows:

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

LDAP		
Settings Mapper	rs	
General options		
Console display name • ⑦	Idap	
Vendor * 🗇	Active Directory -	

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

Connection and authentication settings		
Connection URL * ③	LDAP://10.1.210.111	
Enable StartTLS 💿	Off	
Use Truststore SPI ⑦	Only for Idaps	•
Connection pooling ③	Off	
Connection timeout ⑦		\bigcirc
	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 * ⑦	simple		
Bind DN * 💿	CN=Administrator,CN=Users,DC=ess2019,DC=local		
Bind credentials * ③	•••••		
	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 * ③	READ_ONLY			
Users DN * ⑦	DC=ess2019,DC=local			
Username LDAP attribute * 💿	userPrincipalName			
RDN LDAP attribute *	userPrincipalName			
UUID LDAP attribute * ⑦	objectGUID			
User object classes * ⑦	person, organizationalPerson, user			
User LDAP filter 💿				
Search scope ③	Subtree 🔹			
Read timeout 💿	5			
Pagination ⑦	Off			

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

Synchronization s	ettings	
Import users 💿	On	
Sync Registrations ⑦	On	
Batch size ⑦		\sim
Periodic full sync ③	On	
Full sync period ⑦	3600	\sim
Periodic changed users sync ⑦	On	
Changed users sync period ⑦	3600	$\langle \rangle$
	-	
Kerberos integrati	ion	
Allow Kerberos authentication ⑦	Off	
Use Kerberos for password authentication ⑦	Off	
Cache settings		
Cache policy ③	DEFAULT	•
Advanced setting	s	
Enable the LDAPv3 password modify extended operation ⑦	Off Off	
Validate password policy ⑦	Off	
Trust email 💿	Off	
	Query Supported Extensions	
Save Cancel		

Step 4: Create and Configure Client:

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

Manage	Clianta				
Clients	Clients Clients are applicatio	ns and services 1	hat can request au	thentication of a user. Learn more	Z
Client scopes					
Realm roles	Clients list Initi	al access token			
Users	Q Search for client	\rightarrow	Create client	Import client	1-7 🔻
Groups					

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

General Settings			
Client ID * 💿	MP-Test		
Name ⑦	MP-Test		
Description ⑦			
			11.
Always display in console ⑦	On On		
Access settings			2
Root URL ⑦			
Home URL ⑦	https://supportpanel.machsol.com		
Valid redirect URIs 💿	https://supportpanel.machsol.com/*	0	
	O Add valid redirect URIs		
Valid post logout	https://supportpanel.machsol.com	•	
Tedirect Onis (O Add valid post logout redirect URIs		
Web origins 💿	https://supportpanel.machsol.com	0	
	O Add web origins		
Admin URL ⑦			

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:

₫	Home > System Configuration > Authentication			
	Authentication	Two Factor Authentication Settings		

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:	\checkmark
* Issuer Endpoint:	http://10.1.210.177:8080/realms/MachPanel-SSO-Realm
* Client Id:	MP-Test
* Secret:	oreJKM6byQVzYYucFr6qk2xv0CoMNgfr
* Auto-Redirect to KeyCloak Login:	
* Signout from KeyCloak on panel signout:	
* Comma separated IPs to not use KeyCloak:	
	<i>li</i> .
Save Settings	

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

			0	admin 👻	
MachPanel-SSO-Rea				8	
Manage Frontend URL ③					
Clients Require SSL ⑦	None		•		
Client scopes					
Realm roles October Control ACR to LoA Mapping	Кеу	Value			
Users	Type a key	Type a value	0		
Groups	Add an attribute				
Sessions User-managed acces	s Off				
Events	-				
Endpoints ①	OpenID Endpoint Configuration 🗹				
Configure	SAML 2.0 Identity Provider Metadata 🗹				
Realm settings					
Authentication	Save Revert				
JSON Raw Data Headers					
Save Copy Collapse All Expand All 🗑 Filter JSON					
/ issuer:	"http://10.1.210.	177:8080/realms/NachPanel-SSO-Realm"			
authorization_endpoint:	7				
token_endpoint:	7				
introspection_endpoint:	7				ť
/ userinfo_endpoint:	7				
<pre>v end_session_endpoint:</pre>	Thesper 1 avreneed.	177, аварут вислау послечилествоветновыму разова	cosy open concorned by	/ coguere	

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

MachPanel-SSO-Rea •	Clients	ns and services that car	request authentication of a u	ser Learn more
Manage		is and services that can	request autientication of a u	ser. Learninge
Clients	Clients list Ir	nitial access token		
Client scopes	Q Search for client	→ Cr	eate client Import client	
Realm roles				
Users	Client ID	Туре	Description	Home URL
Groups	MP-Test	OpenID Connec	t –	

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

MachPanel KeyCloak SSO Authentication

MachPanel-SSO-Rea	Clients > Client	details OpenID Co	nnect							Enabled	0
Manage	Clients are applie	, cations a	nd services that	can reque	st authentication	of a user.					
Clients	Settings	Kevs	Credentials	Roles	Client scopes	Sessions	Advanced				
Client scopes	occurigo	najo	oredentideb	110100	unerre scopes	0.0000000	1010100				
Realm roles											
Users	Client Authen	ticator	Client Id and	Secret						•	
Groups	0										
Sessions			Save								
Events											
									_		
Configure	Client secret		•••••	•••••	•••••			ø	Reg	jenerate	
Realm settings											

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:

+	MACHPANEL-SSO-REALM	6
	Sign in to your account Username or email	
	Password	
	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:

Login to Mach	Sol-Support Control Panel
Authentication Faile disabled. LogOut a	ed. No user match found for user: 'contactzohaib9@onenetex1.com', or user is nd try different Login
Jser name (e-mail addre	(22
Select Language	
English	-

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...