Yasith Kumara Follow
Oct 1, 2021 · 4 min read · Listen

Active Directory as a User Federation in Keycloak

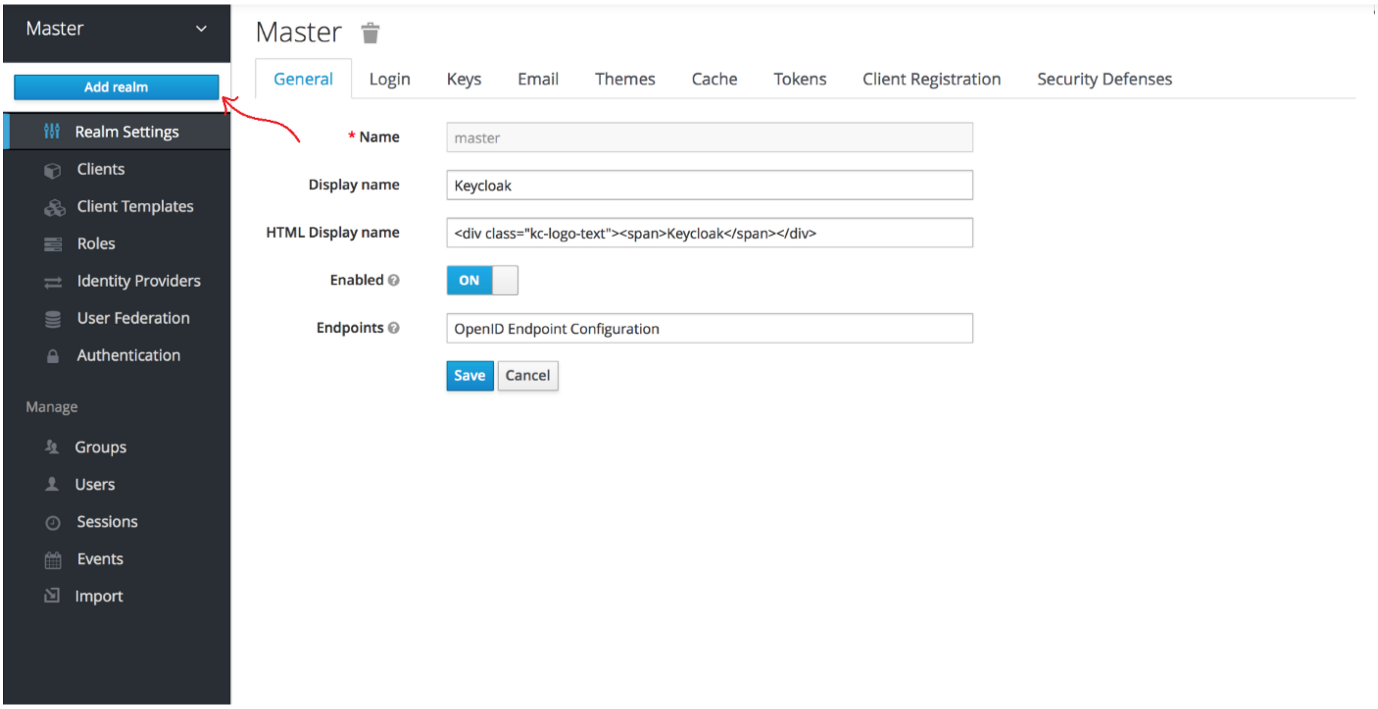
If you want to know how to connect an Active Directory to Keycloak through LDAP as a User Federation, You have come to the write place. I will go through the process step by step with commentary for more clarity.

Prerequisites

All you will need is Keycloak and an active directory you can connect to. But windows 10 does not allow users to create an active directory. You will need a Windows Server for that and a virtual machine is the easiest way to set one up. So If you are on windows 10 and don't have an active directory, check out my other articles on Creating a Windows Server Virtual Machine and creating an Active Directory in a Windows Server.

Assuming that you have the perquisites checked, we will now move further step by step.

1. When you log into Keycloak for the first time, there will only be one realm, the master realm. To create a new realm, click on the little arrow next to the label 'master' in the upper left corner and click 'Add realm'.



Master

* Name: master

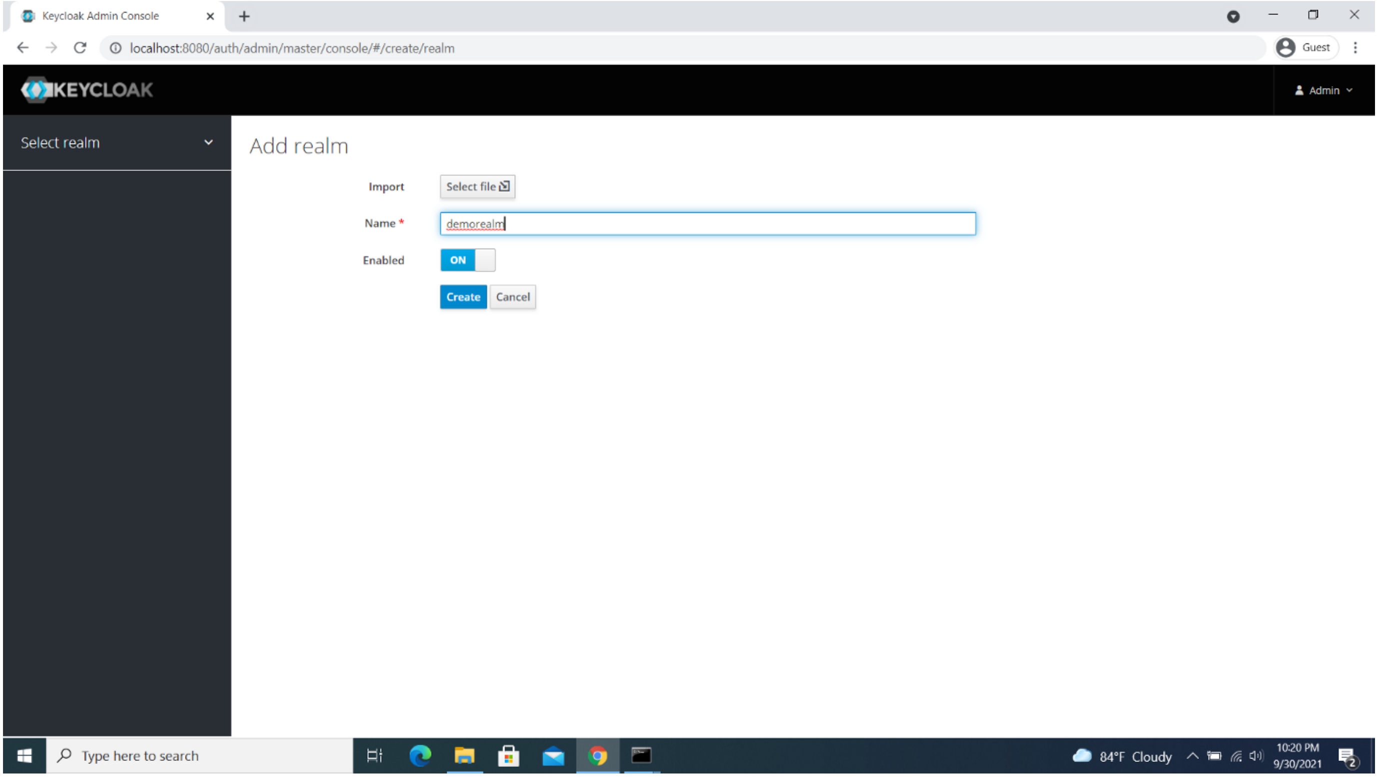
Display name: Keycloak

HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>

Enabled: ON

Endpoints: OpenID Endpoint Configuration

2. Choose a name for your new realm and click ‘Create’.



localhost:8080/auth/admin/master/console/#/create/realm

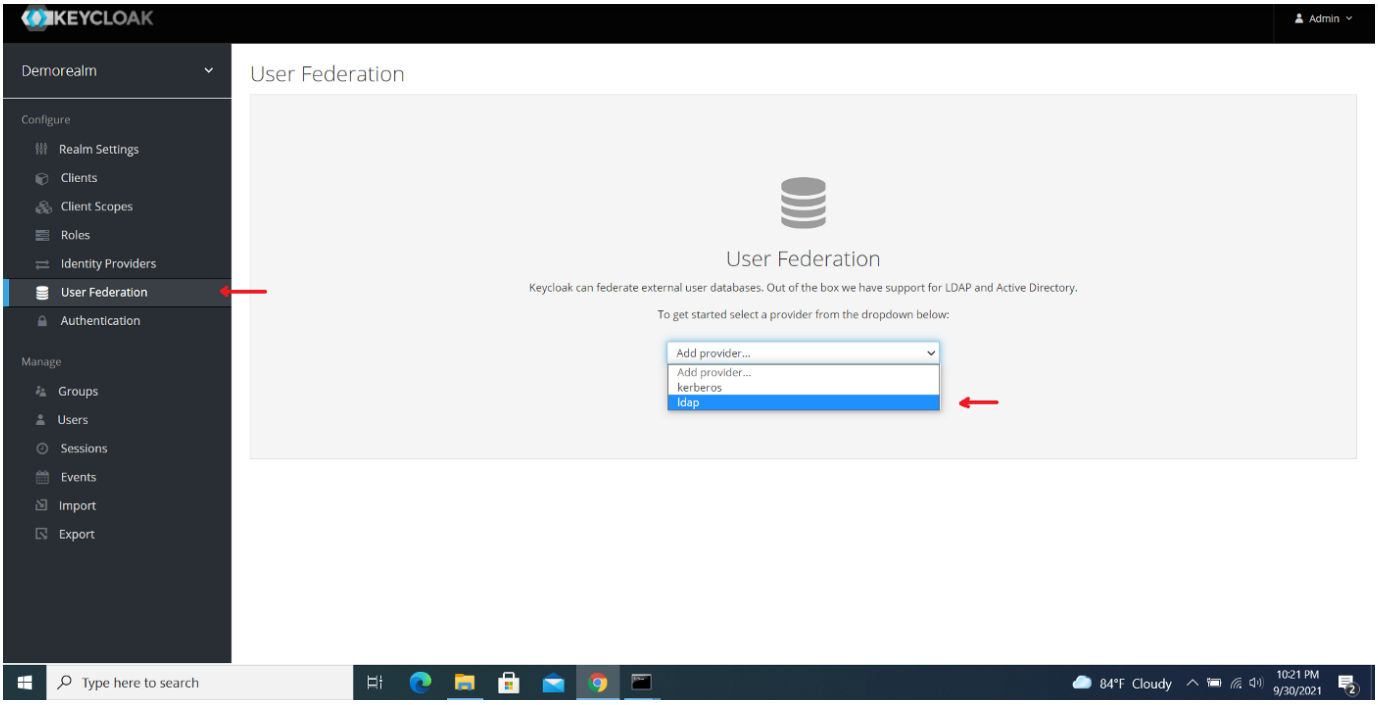
Add realm

Import

Name *: demorealm

Enabled: ON

3. Now click on ‘User Federation’ on the left pane to navigate to user federation window. Select ‘ldap’ from the drop down selector to navigate further.



User Federation

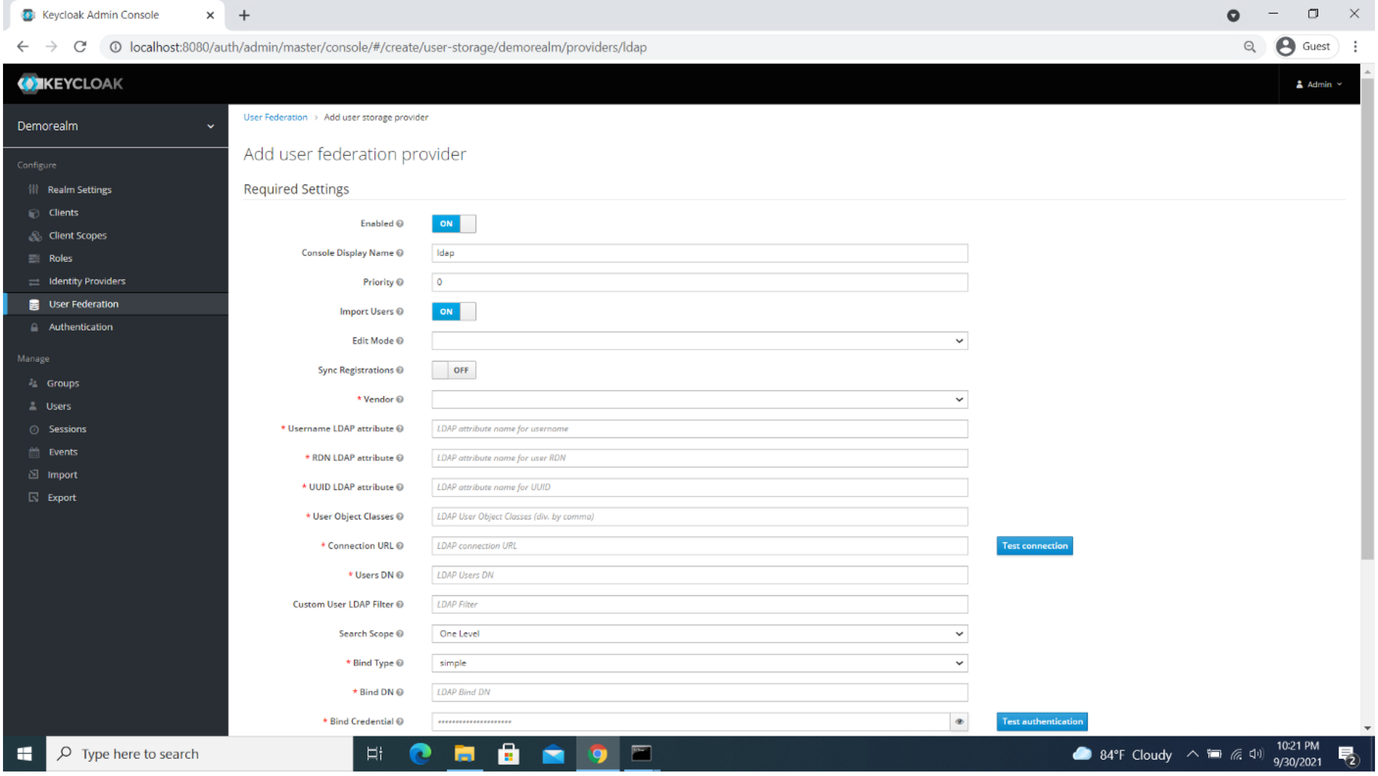
User Federation

Keycloak can federate external user databases. Out of the box we have support for LDAP and Active Directory.

To get started select a provider from the dropdown below:

Add provider...
Add provider...
kerberos
ldap

4. In the ‘Add user storage provider’ window, there is a lot to fill up. But i will go through them one by one.



User Federation › Add user storage provider

Add user federation provider

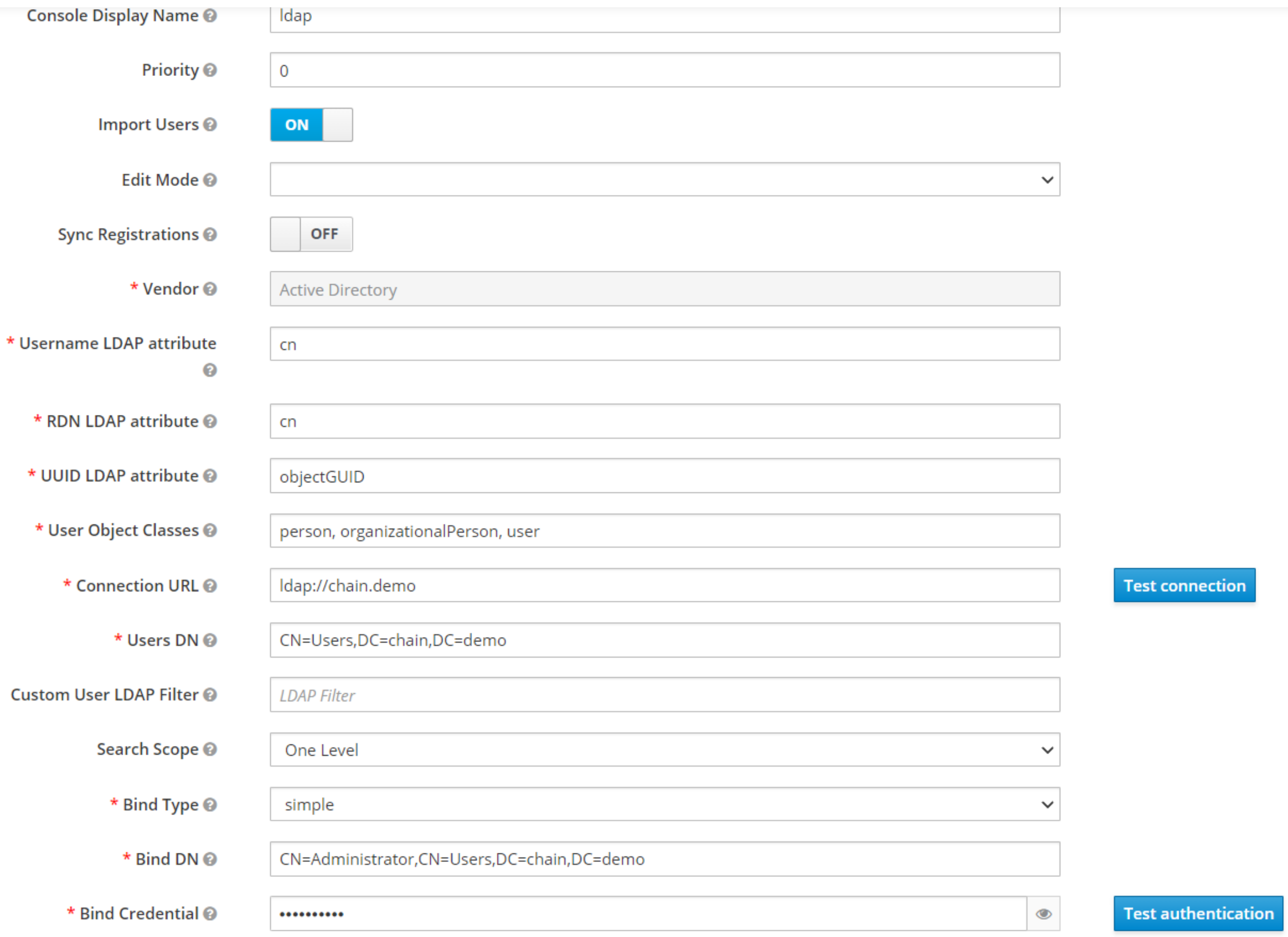
Required Settings

Enabled	ON
Console Display Name	ldap
Priority	0
Import Users	ON
Edit Mode	
Sync Registrations	OFF
* Vendor	
* Username LDAP attribute	LDAP attribute name for username
* RDN LDAP attribute	LDAP attribute name for user RDN
* UUID LDAP attribute	LDAP attribute name for UUID
* User Object Classes	LDAP User Object Classes (div. by comma)
* Connection URL	LDAP connection URL
* Users DN	LDAP Users DN
Custom User LDAP Filter	LDAP Filter
Search Scope	One Level
* Bind Type	simple
* Bind DN	LDAP Bind DN
* Bind Credential	**********************

Test connection

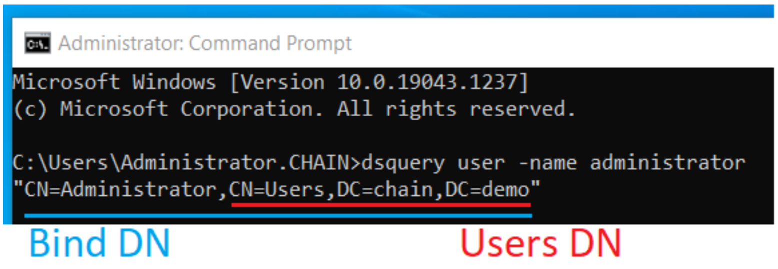
Test authentication

5. Select ‘Active Directory’ as the vendor to fill the fields ‘Username LDAP attribute’, ‘RDN LDAP attribute’, ‘UUID LDAP attribute’ and ‘User Object classes’ automatically.



Console Display Name	ldap
Priority	0
Import Users	ON
Edit Mode	
Sync Registrations	OFF
* Vendor	Active Directory
* Username LDAP attribute	cn
* RDN LDAP attribute	cn
* UUID LDAP attribute	objectGUID
* User Object Classes	person, organizationalPerson, user
* Connection URL	ldap://chain.demo
* Users DN	CN=Users,DC=chain,DC=demo
Custom User LDAP Filter	LDAP Filter
Search Scope	One Level
* Bind Type	simple
* Bind DN	CN=Administrator,CN=Users,DC=chain,DC=demo
* Bind Credential	••••••••••

As the connection url, use 'ldap://' followed by your domain name. Since my domain name was 'chain.demo', I used 'ldap://chain.demo'. Click on 'test connection' to see if the LDAP connection works.



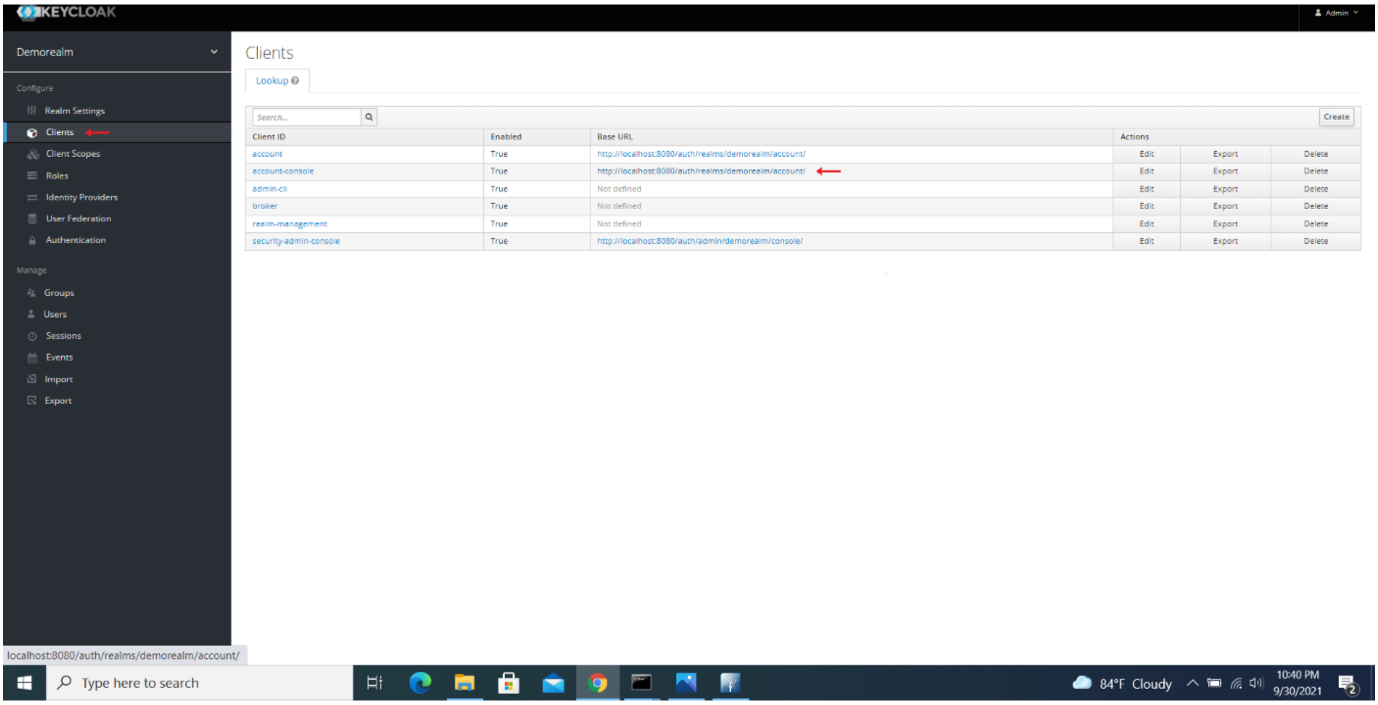
```
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator.CHAIN>dsquery user -name administrator
"CN=Administrator,CN=Users,DC=chain,DC=demo"
```

Type 'dsquery user -name ' followed by the administrator's name to get the 'Bind DN' and 'Users DN'. Use the administrator password as the 'Bind Credentials' and click 'Test Authentication' to check whether it is correct.

Click 'Save' to finish up.

Now we will test whether what we did so far works or not.

6. Click 'Clients' in the left pane to navigate to clients window. Click the account-console base URL.

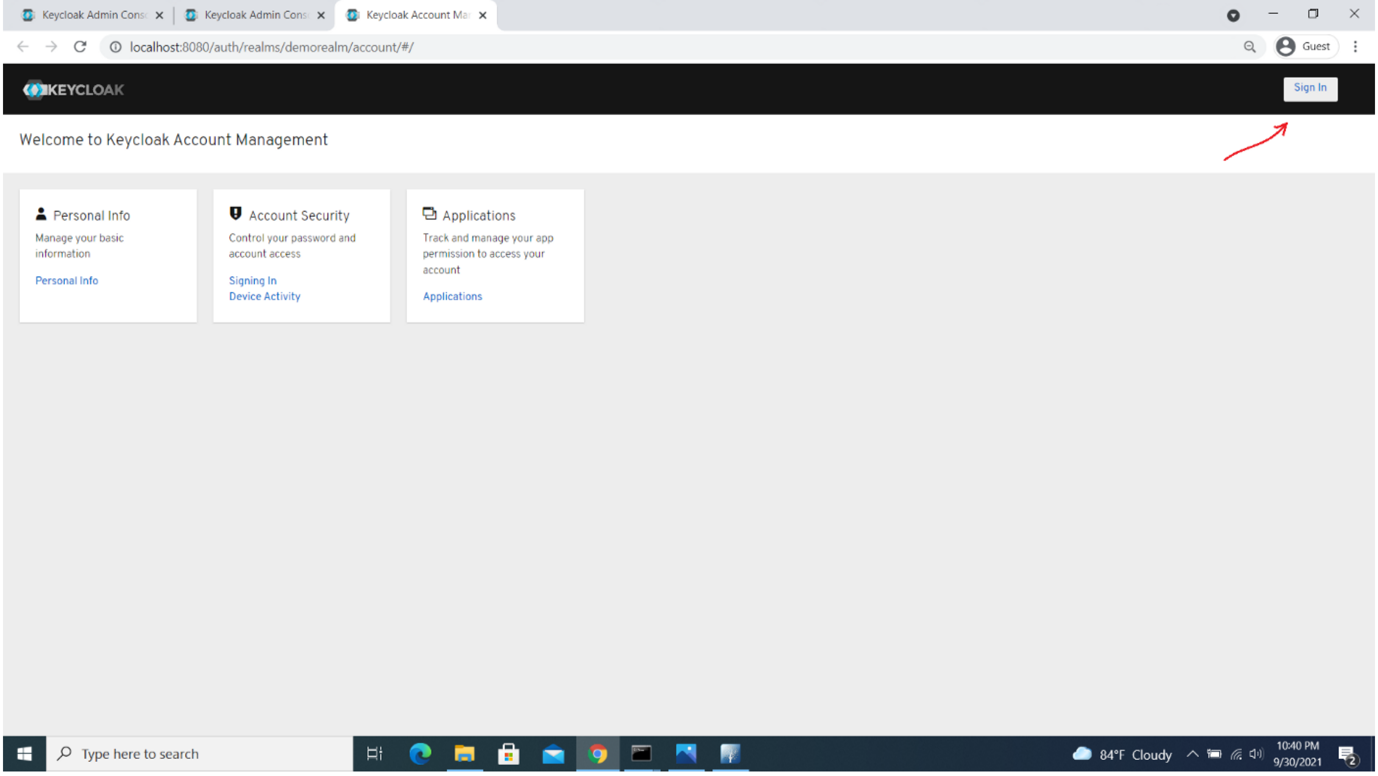


Clients

Client ID	Enabled	Base URL	Actions		
account	True	http://localhost:8080/auth/realms/demorealm/account/	Edit	Export	Delete
account-console	True	http://localhost:8080/auth/realms/demorealm/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	http://localhost:8080/auth/admin/demorealm/console/	Edit	Export	Delete

localhost:8080/auth/realms/demorealm/account/

7. By clicking ‘Sign in’ button in the upper left corner to navigate to sign in page.



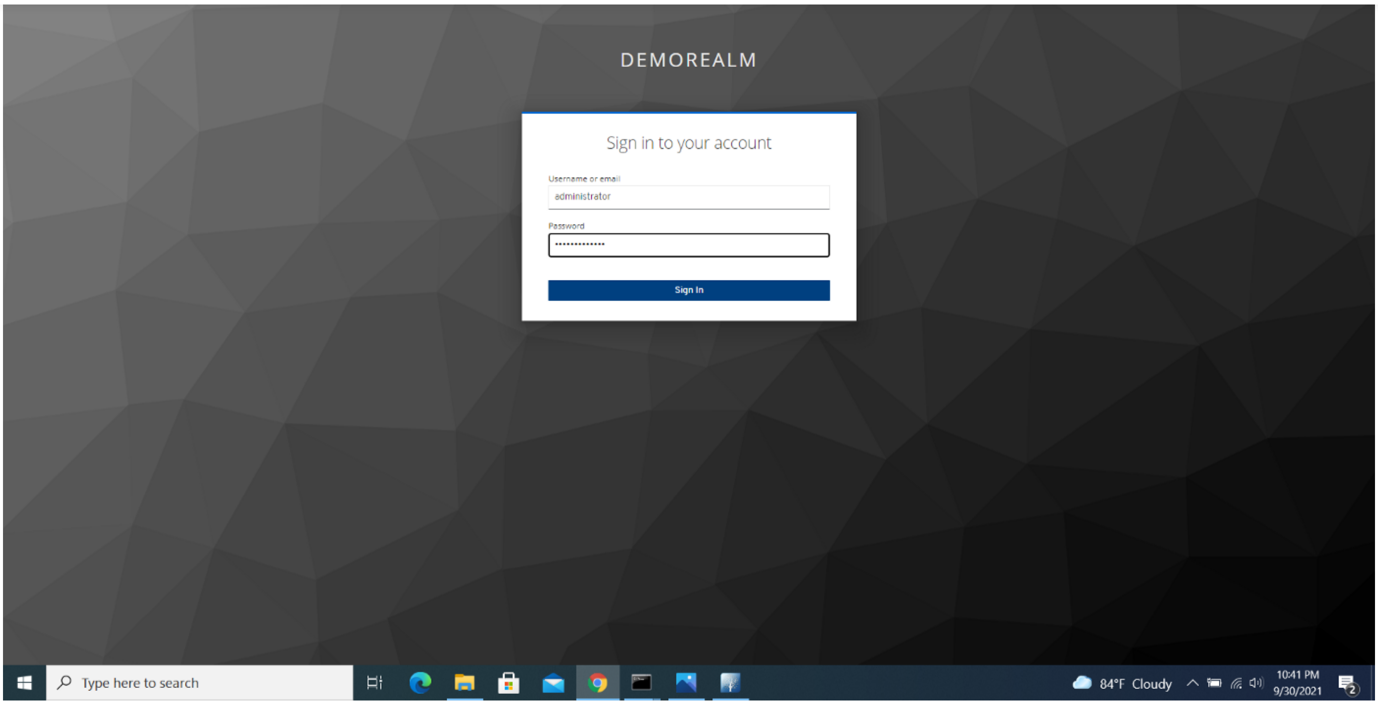
Welcome to Keycloak Account Management

Personal Info
Manage your basic information
Personal Info

Account Security
Control your password and account access
Signing In
Device Activity

Applications
Track and manage your app permission to access your account
Applications

8. Use the credentials of any user in your active directory to sign in.



DEMOREALM

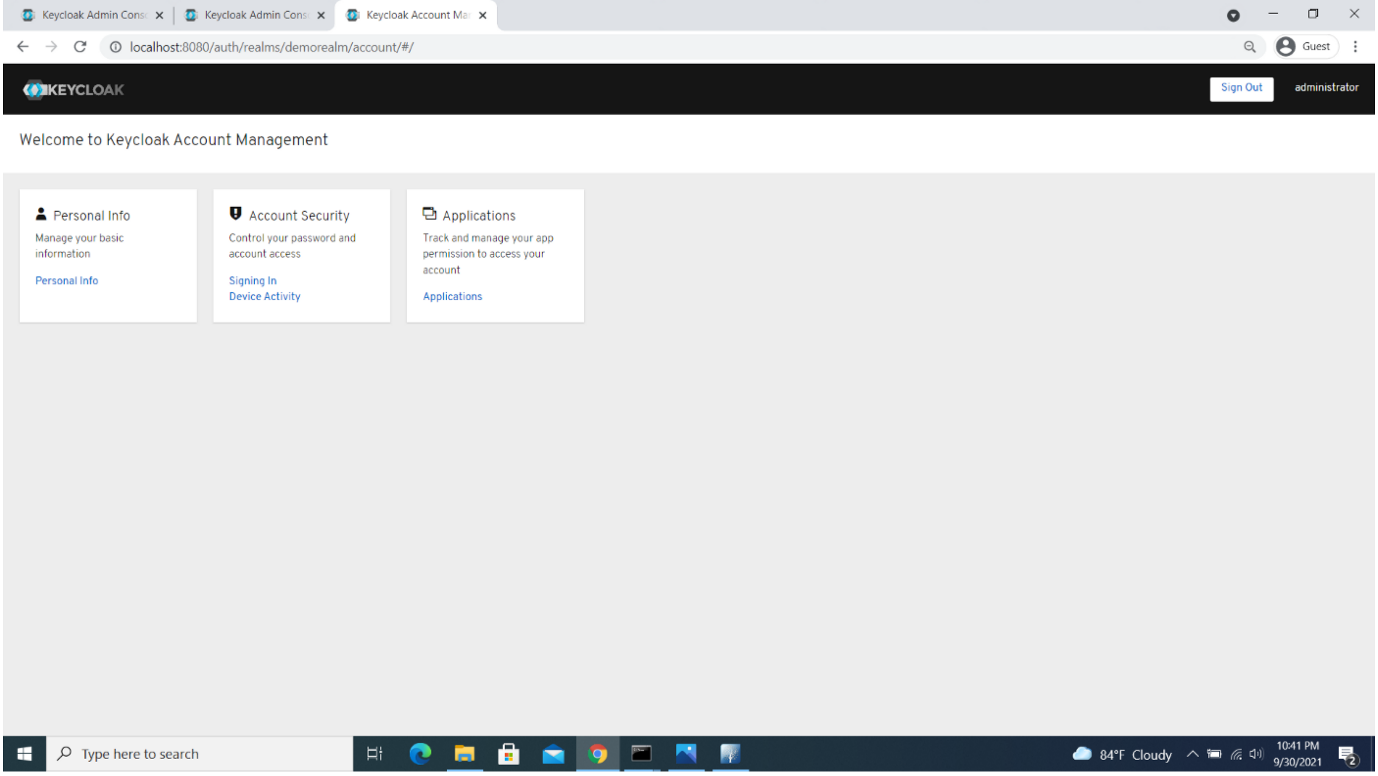
Sign in to your account

Username or email: administrator

Password: ••••••••••••••

Sign In

9. Voila, we just authenticated a user using an Active Directory. You can see that users account now.



localhost:8080/auth/realms/demorealm/account/#/

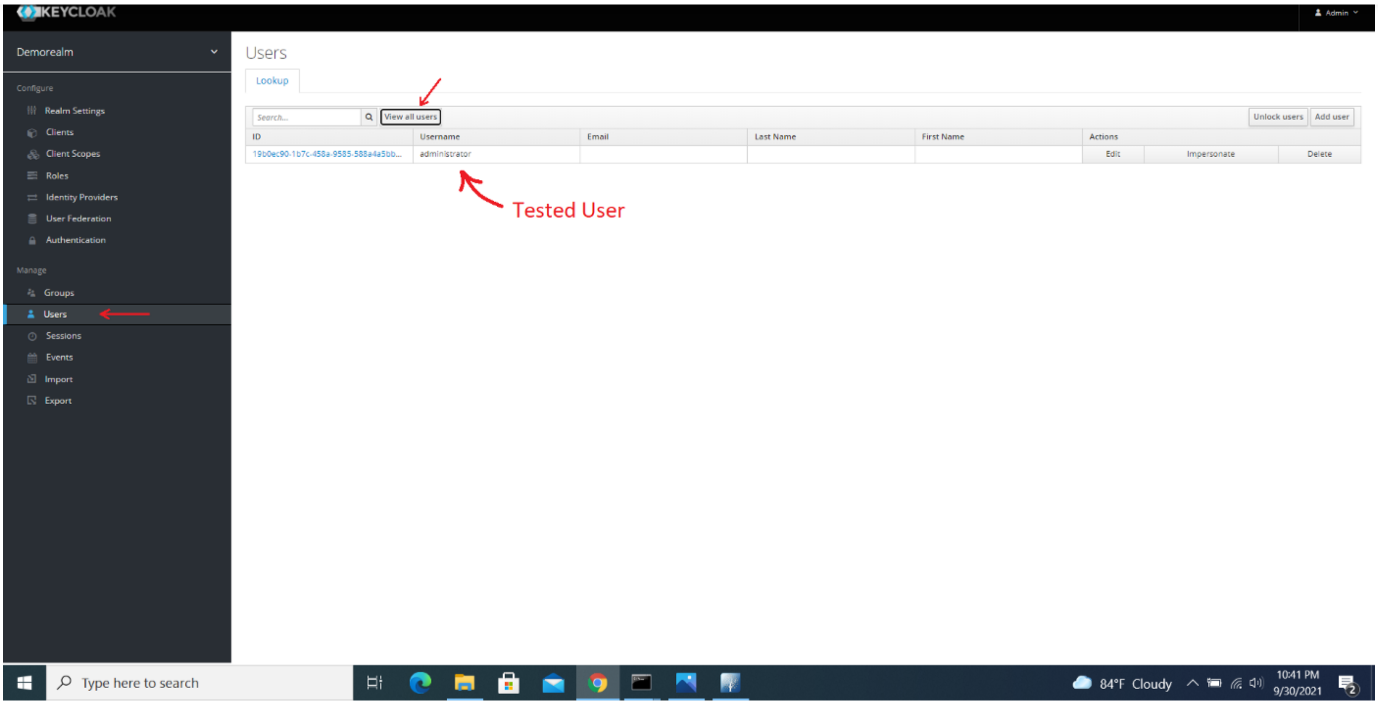
Welcome to Keycloak Account Management

Personal Info
Manage your basic information
Personal Info

Account Security
Control your password and account access
Signing In
Device Activity

Applications
Track and manage your app permission to access your account
Applications

10. To see the user we just tested, navigate to the Users tab by clicking 'Users' in the left pane and click 'View all users'.



ID	Username	Email	Last Name	First Name	Actions		
19b0ec90-1b7c-458a-9585-588a4a5bb...	administrator				Edit	Impersonate	Delete

Congratulations! You have now connected an Active Directory as a User Federation in Keycloak.