

# Using Keycloak with Ignition



(800) 266-7798

[inductiveautomation.com](http://inductiveautomation.com)

# Table of Contents

Introduction	<b>3</b>
Running Keycloak as a Docker Container	<b>4</b>
Configuring and Creating a New Realm	<b>5</b>
Configuring Keycloak as Ignition Identity Provider	<b>14</b>
Testing Keycloak as Ignition Identity Provider	<b>18</b>
Configuring Two-Factor Authentication (2FA)	<b>25</b>
User Federation - Active Directory	<b>30</b>
Appendix - Resources	<b>35</b>

# Introduction

Keycloak is an open-source Identity and Access Management solution for adding authentication to applications or services. With Ignition, Keycloak functions as an Identity Provider to authenticate users and define roles to access client/session views.

A major benefit of Keycloak is that this solution provides a strong security option external of Ignition that functions within a local or on-premise-only network architecture. There are no requirements to connect to a cloud provider for any additional authentication (unless desired).

Keycloak also provides easily configurable Two-Factor Authentication (2FA) using either the Google Authenticator or Red Hat's FreeOTP authenticator apps (iOS, Android). This functionality can be used as a second level of authentication to existing identity management systems, such as Active Directory.

# Running Keycloak as a Docker Container

See [Appendix](#) for additional resource links about Docker if needed.

1. Run the following command to start Keycloak Docker container

```
docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e  
KEYCLOAK_ADMIN_PASSWORD=admin quay.io/keycloak/keycloak:20.0.1 start-dev
```

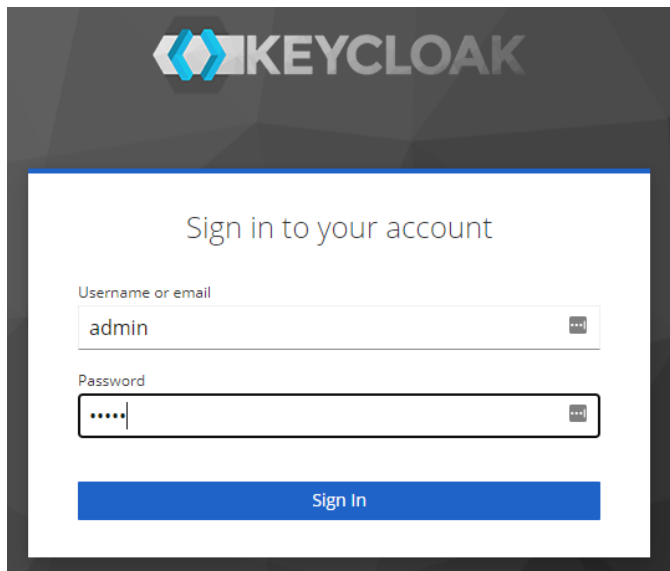
2. Once Keycloak is running, navigate to the admin console.

<http://localhost:8080/admin>

3. Login using credentials defined in Docker run command.

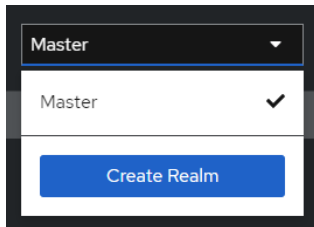
username: admin

password: admin



## Configuring and Creating a New Realm

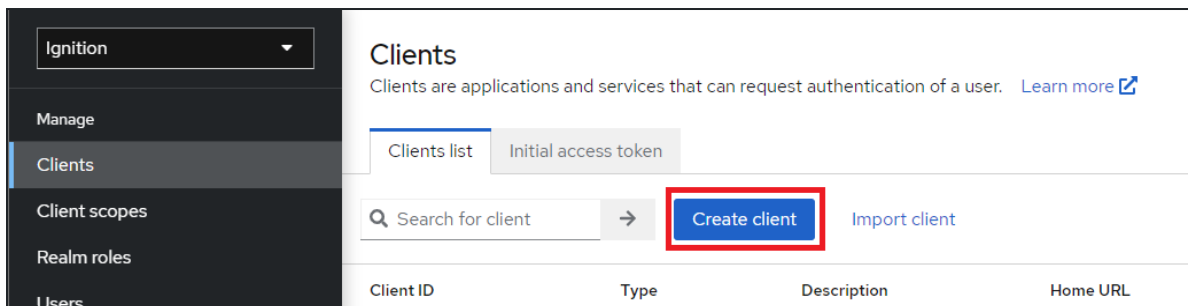
1. Create a new realm by selecting 'Create Realm' in the dropdown.



2. Name the realm 'Ignition' and click Create.

A screenshot of the 'Create realm' form. At the top, it says 'Create realm' and provides a description: 'A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.' Below this is a 'Resource file' section with a drag-and-drop area and 'Browse...' and 'Clear' buttons. Underneath is a text input for 'Realm name \*' with 'Ignition' entered; this input field is highlighted with a red rectangle. There is also an 'Enabled' toggle switch set to 'On'. At the bottom are 'Create' and 'Cancel' buttons.

3. Select the newly created Ignition realm from the dropdown. In the Clients tab, click Create client.



4. Select OpenID Connect as the Client type. Enter 'ignition-client' as the Client ID. Click Next.

Clients > Create client

### Create client

Clients are applications and services that can request authentication of a user.

1 General Settings

Client type ⓘ OpenID Connect

Client ID \* ⓘ ignition-client

Name ⓘ

Description ⓘ

Always display in console ⓘ ☐ Off

Next Back Cancel

5. Set Client authentication to On and Authentication flow to Standard flow (disable others unless desired) , and click Save.

Clients > Create client

### Create client

Clients are applications and services that can request authentication of a user.

1 General Settings

2 Capability config

Client authentication ⓘ ☒ On

Authorization ⓘ ☐ Off

Authentication flow

☒ Standard flow ⓘ

☐ Direct access grants ⓘ

☐ Implicit flow ⓘ

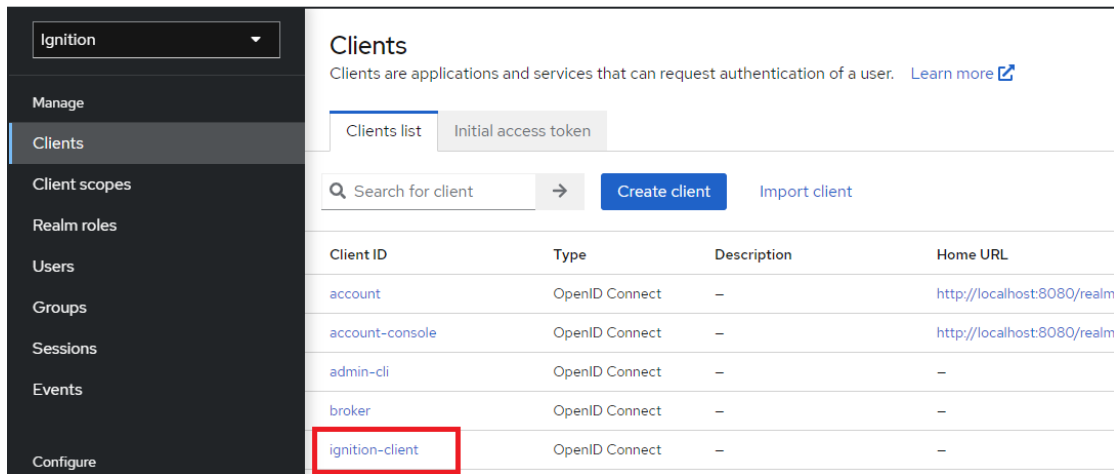
☐ Service accounts roles ⓘ

☐ OAuth 2.0 Device Authorization Grant ⓘ

☐ OIDC CIBA Grant ⓘ

Save Back Cancel

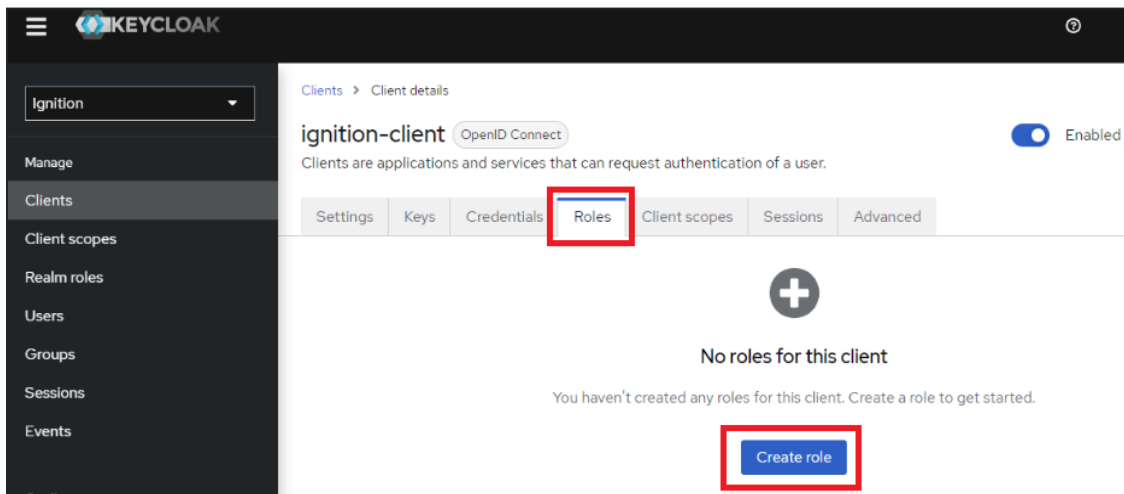
6. From the Clients list tab, select the new ignition-client.



The screenshot shows the Keycloak administration console. On the left is a sidebar with navigation options: Ignition, Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, and Configure. The 'Clients' tab is selected. The main area shows the 'Clients list' tab. Below the tabs is a search bar and buttons for 'Create client' and 'Import client'. A table lists the following clients:

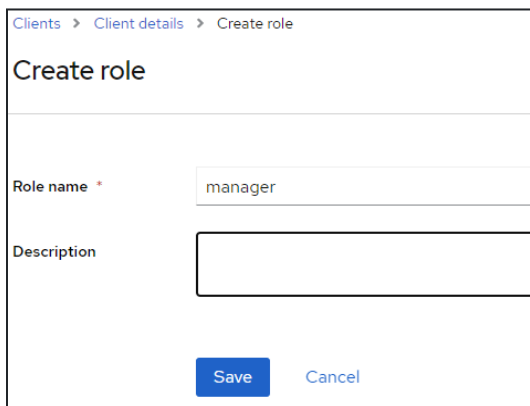
Client ID	Type	Description	Home URL
account	OpenID Connect	-	http://localhost:8080/realms
account-console	OpenID Connect	-	http://localhost:8080/realms
admin-cli	OpenID Connect	-	-
broker	OpenID Connect	-	-
ignition-client	OpenID Connect	-	-

7. Select the Roles tab and click Create role.



The screenshot shows the 'ignition-client' details page in Keycloak. The 'Roles' tab is selected and highlighted with a red box. The page shows 'No roles for this client' and a 'Create role' button, which is also highlighted with a red box.

8. Create a new role called 'manager' and click Save.



The screenshot shows the 'Create role' form. The 'Role name' field is filled with 'manager'. The 'Description' field is empty. At the bottom, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted.

9. Following the same process, create another role called 'operator'. Two roles should be available for the client name 'ignition-client'.

Clients > Client details

### ignition-client OpenID Connect

Clients are applications and services that can request authentication of a user.

Settings Keys Credentials **Roles** Client scopes Sessions Ad

Search role by name → [Create role](#)

Role name	Composite
<a href="#">manager</a>	False
<a href="#">operator</a>	False

10. Once the roles have been created, the client needs to be configured to pass the roles, along with the response, when authenticating a user.

Navigate to Client scopes > roles.

Ignition

Manage

Clients

**Client scopes**

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

### Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between multiple clients. [Learn more](#)

Name Search for client scope → [Create client scope](#) Change type to

Name	Assigned type	Protocol	Display order	Description
<input type="checkbox"/> <a href="#">acr</a>	Default	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">address</a>	Optional	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">email</a>	Default	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">microprofile-jwt</a>	Optional	OpenID Connect	–	Microprofile - JWT
<input type="checkbox"/> <a href="#">offline_access</a>	Optional	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">phone</a>	Optional	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">profile</a>	Default	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">role_list</a>	Default	SAML	–	SAML role list
<input type="checkbox"/> <a href="#">roles</a>	Default	OpenID Connect	–	OpenID Connect
<input type="checkbox"/> <a href="#">web-origins</a>	Default	OpenID Connect	–	OpenID Connect



11. Select the Mappers tab, then select client roles.

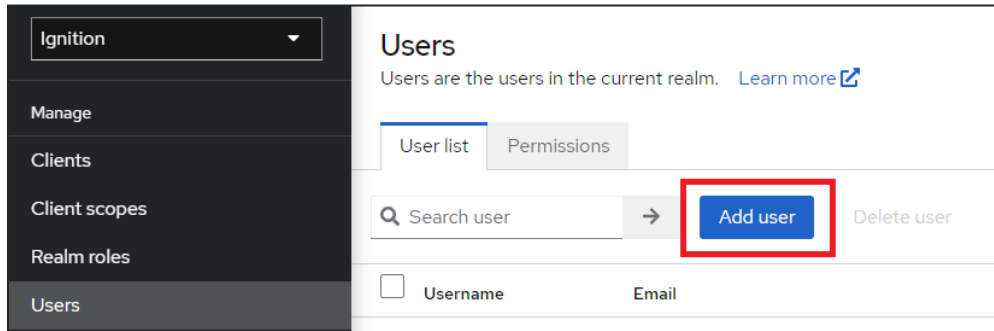
The screenshot shows the Ignition web interface. On the left is a dark sidebar with a menu. The 'Client scopes' menu item is highlighted. In the main content area, the breadcrumb is 'Client scopes > Client scope details'. Below this, the word 'roles' is followed by a blue pill containing 'openid-connect'. There are three tabs: 'Settings', 'Mappers' (which is selected and highlighted with a red box), and 'Scope'. Below the tabs is a search bar with the text 'Search for mapper' and an 'Add mapper' button. A table lists mappers with columns 'Name' and 'Category'. The table contains three rows: 'audience resolve' (Token mapper), 'realm roles' (Token mapper), and 'client roles' (Token mapper). The 'client roles' row is highlighted with a red box.

Name	Category
audience resolve	Token mapper
realm roles	Token mapper
client roles	Token mapper

12. For Client ID, select the ignition-client from the dropdown. Next, set the Token Claim Name to 'roles' only, which will make parsing the roles simpler in the Ignition User Attribute Mapper.

The screenshot shows the 'User Client Role' configuration page in Ignition. The breadcrumb is 'Client scopes > Client scope details > Mapper details'. The title is 'User Client Role' with a unique ID '61026098-b835-4edb-8bc2-62cd23a9b741'. The 'Mapper type' is 'User Client Role'. The 'Name' field is 'client roles'. The 'Client ID' dropdown is set to 'ignition-client' and is highlighted with a red box. The 'Client Role prefix' field is empty. The 'Multivalued' toggle is turned 'On'. The 'Token Claim Name' field is 'roles' and is highlighted with a red box. The 'Claim JSON Type' is 'String'. There are three toggle switches at the bottom, all turned 'On': 'Add to ID token', 'Add to access token', and 'Add to userinfo'. At the bottom right are 'Save' and 'Cancel' buttons.

13. Navigate to the Users tab to create some new users for the Ignition realm. Click Add user.



14. Create a new user. Note some of the options for required user actions, such as OTP. These will be discussed later in the document. Leave this blank for now.

The screenshot shows the 'Create user' form. At the top, it says 'Users > Create user' and 'Create user'. The form contains several input fields and toggle switches: 'Username \*' with the value 'johnlennon', 'Email' with the value 'john@email.com', 'Email verified' with a toggle switch set to 'Off', 'First name' with the value 'John', 'Last name' with the value 'Lennon', and 'Enabled' with a toggle switch set to 'On'. Below these is a 'Required user actions' section with a dropdown menu currently showing 'Select action'. The dropdown menu is open, displaying a list of options: 'Configure OTP', 'Terms and Conditions', 'Update Password', 'Update Profile', 'Verify Email', 'Delete Account', 'Webauthn Register', and 'Webauthn Register Passwordless'. There is also a 'Groups' label with a help icon.

15. Once the user has been created, navigate to the Credentials tab for that user and select Set password.

The screenshot shows the 'User details' page for a user named 'johnlennon'. The 'Credentials' tab is selected and highlighted with a red box. Below the tabs, there is a large plus icon and the text 'No credentials'. A message states: 'This user does not have any credentials. You can set password for this user.' At the bottom right, the 'Set password' button is highlighted with a red box, and a 'Credential Reset' link is visible below it.

16. Set the initial password for the user. Leave Temporary set to On. This will force the user to create a new password on initial login. Click Save.

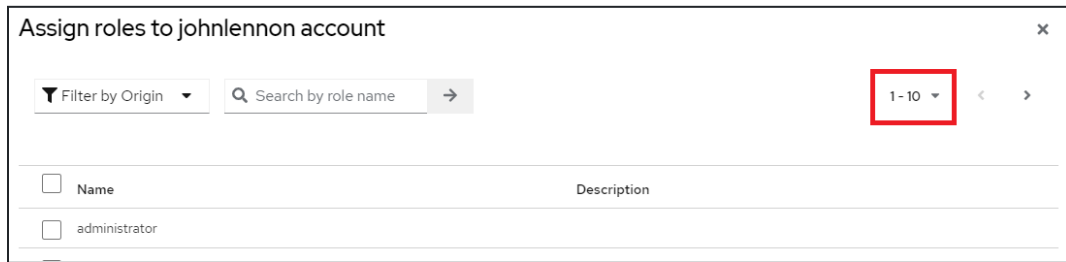
The screenshot shows a dialog box titled 'Set password for johnlennon'. It contains two password input fields: 'Password' and 'Password confirmation', both containing the text 'password'. Below these fields is a 'Temporary' toggle switch which is turned 'On'. At the bottom left are 'Save' and 'Cancel' buttons.

17. Navigate to Role mapping and click Assign role.

The screenshot shows the 'User details' page for 'johnlennon' with the 'Role mapping' tab selected and highlighted with a red box. Below the tabs, there is a search bar labeled 'Search by name' and a checkbox for 'Hide inherited roles'. The 'Assign role' button is highlighted with a red box. Below this is a table of roles:

<input type="checkbox"/>	Name	Inherited
<input type="checkbox"/>	default-roles-ignition	False
<input type="checkbox"/>	uma_authorization	True
<input type="checkbox"/>	offline_access	True
<input type="checkbox"/>	account view-profile	True
<input type="checkbox"/>	account manage-account	True
<input type="checkbox"/>	account manage-account-links	True

18. Select the dropdown box to display all available roles.



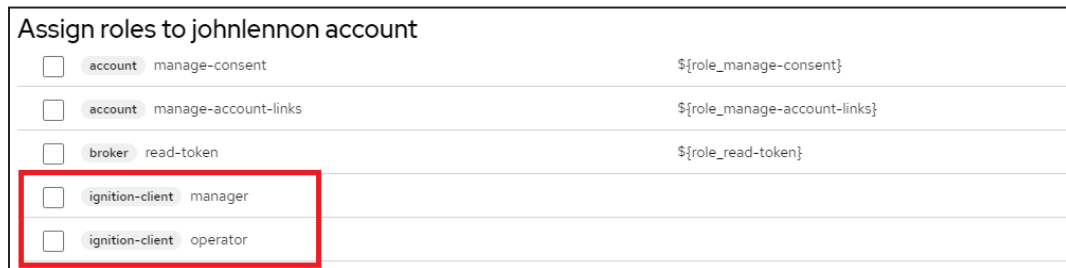
Assign roles to johnlennon account

Filter by Origin Search by role name

1-10

Name	Description
administrator	

19. Select either one or both of the *ignition-client* roles for the user, and then click Assign.



Assign roles to johnlennon account

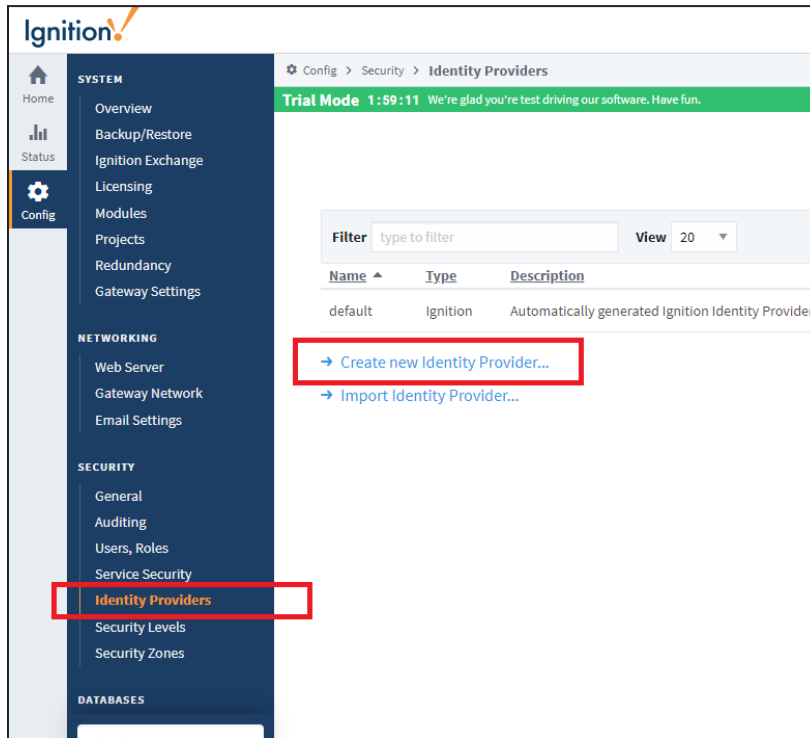
<input type="checkbox"/>	account	manage-consent	\${role_manage-consent}
<input type="checkbox"/>	account	manage-account-links	\${role_manage-account-links}
<input type="checkbox"/>	broker	read-token	\${role_read-token}
<input type="checkbox"/>	ignition-client	manager	
<input type="checkbox"/>	ignition-client	operator	

20. This completes the initial setup of the Ignition realm. Next, Ignition will be configured to utilize this Keycloak identity provider.

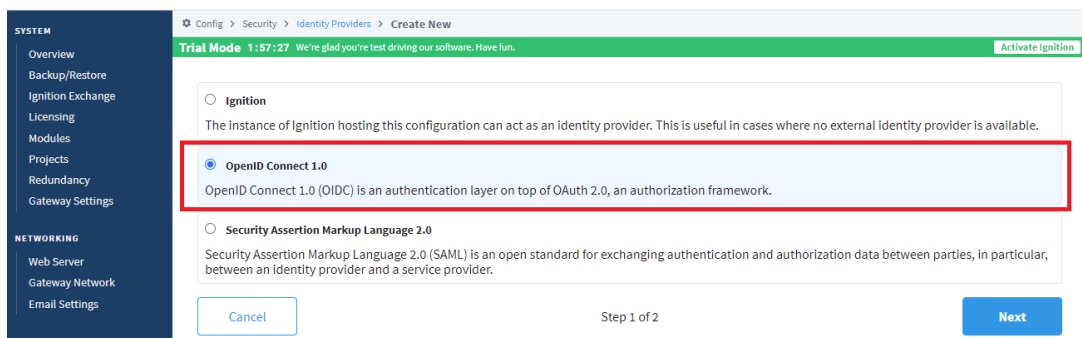
**NOTE:** Please keep the Keycloak admin console open, as additional items will need to be referenced and added during the rest of the Ignition configuration.

# Configuring Keycloak as Ignition Identity Provider

1. Open the Ignition Gateway page, login, and navigate to Config > Security > Identity Providers. Select Create new Identity Provider...



2. Select OpenID Connect 1.0 and click Next.



3. Enter in the Provider Name as 'keycloak'.

Basic Details	
Provider Name *	keycloak <small>Give the provider a name.</small>
Provider Description	<input type="text"/>

4. For the Provider Metadata, return back to Keycloak and navigate to the Ignition realm Realm Settings. Click on the OpenID Endpoint Configuration link. This will open a browser window. Copy and paste the endpoint URL.

NOTE: It is strongly recommended that Require SSL be enabled in Keycloak for all requests in a production environment.

Default endpoint:

<http://localhost:8080/realms/Ignition/.well-known/openid-configuration>

The screenshot shows the Keycloak administration interface for the 'Ignition' realm. The left sidebar contains a 'Configure' section with 'Realm settings' highlighted. The main panel shows various realm configuration options. At the bottom, the 'Endpoints' section is highlighted, displaying two links: 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'.

- Once the URL has been pasted into Ignition, click Import. Ignition will respond with a successful or failed import of the metadata.

**Import Provider Metadata**

Import Method: From URL

Import from URL:

URL to the OpenID Provider Configuration document. Typically, if the issuer is "https://example.org/foo" then the metadata URL would be "https://example.org/foo/.well-known/openid-configuration"

- There are two additional parameters for the provider configuration that need to be manually entered. These are the Client ID and Client Secret. The Client ID is the client created in Keycloak, which is called 'ignition-client' for this example.

**Provider Configuration**

Client ID \*:  The client identifier registered within the identity provider.

Client Secret \*:  The client secret registered within the identity provider.

The Client Secret is found in Keycloak by navigating to the Clients > ignition-client > Credentials tab in Keycloak. The Client secret can be copied from here and pasted back into the provider configuration in Ignition.

**KEYCLOAK**

Ignition

Manage

**Clients**

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Clients > Client details

**ignition-client** OpenID Connect

Clients are applications and services that can request authentication of a user.

Settings Keys **Credentials** Roles Client scopes Sessions Advanced

Client Authenticator

Save

Client secret

7. Locate the redirect URI located directly above the Provider Configuration section. Copy this value for use in the next step. Click Save to complete the Provider Configuration.

Most OpenID Providers will require registering Ignition as a client. After the registration process is complete, the provider will generate a client ID and secret for Ignition, which is required below. This gives Ignition the ability to communicate securely with the provider. Most providers will also require a set of redirect URIs. This Ignition Gateway's Redundancy Role is set to **Independent**. The redirect URI for this Ignition Gateway is: **http://localhost:8088/data/federate/callback/oidc**

Provider Configuration		* Required Field
Client ID *	<input type="text" value="ignition-client"/>	The client identifier registered within the identity provider.

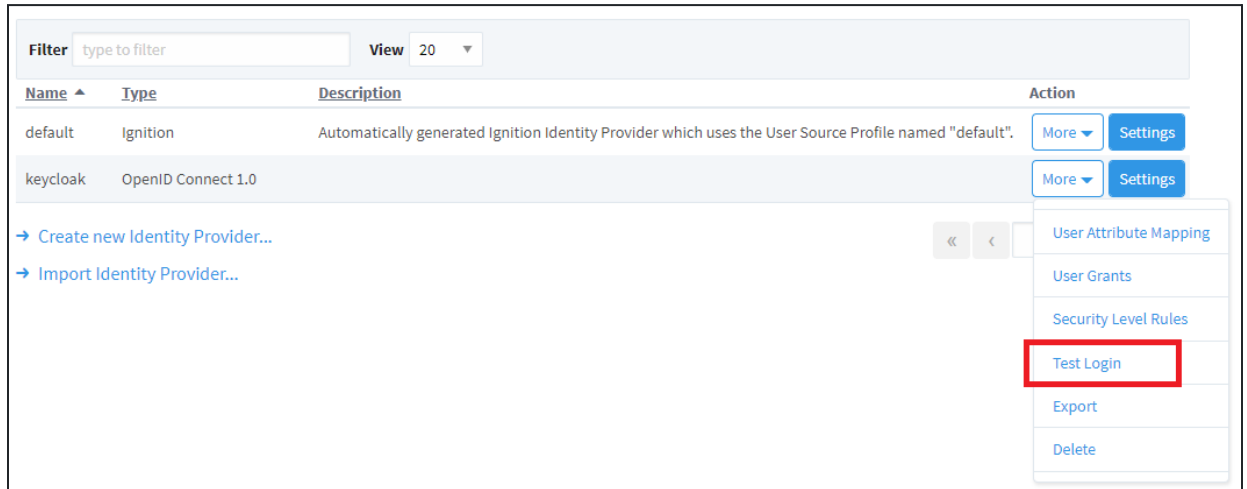
8. In Keycloak, navigate to the Clients > ignition-client > Settings tab. Paste the redirect URI from Ignition into the Valid redirect URIs box. Also, add a '+' symbol into the Valid post logout redirect URIs box. This notifies Keycloak to use the same list of valid redirect URIs. Click Save to complete changes.

The screenshot shows the Keycloak Admin Console interface. On the left is a sidebar with navigation options: Ignition, Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'ignition-client' and has tabs for Settings, Keys, Credentials, Roles, Client scopes, Sessions, and Advanced. The 'Settings' tab is selected and highlighted with a red box. Below the tabs are sections for 'General Settings' and 'Access settings'. In the 'General Settings' section, the 'Client ID' is 'ignition-client'. In the 'Access settings' section, the 'Valid redirect URIs' field contains 'http://localhost:8088/data/federate/callback/oidc' and is highlighted with a red box. Below it is a button to 'Add valid redirect URIs'. The 'Valid post logout redirect URIs' field contains a '+' symbol and is also highlighted with a red box. Below it is a button to 'Add valid post logout redirect URIs'. On the right side of the 'Settings' tab, there is a 'Jump to section' menu with links to General Settings, Access settings, Capability, Login settings, and Logout settings.

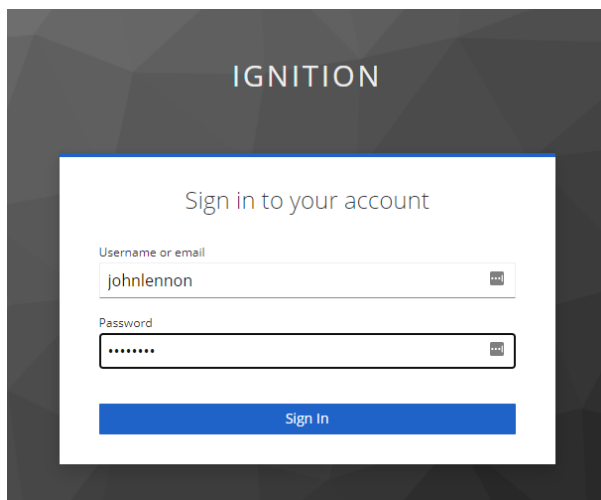


# Testing Keycloak as Ignition Identity Provider

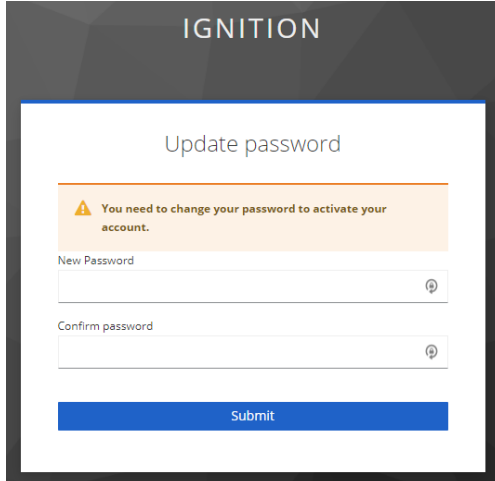
1. From within Ignition, navigate to Security > Identity Providers. Use the More dropdown menu for keycloak and select Test Login.



2. The default Keycloak login screen will appear. Note the 'IGNITION' name, which is referring to the Ignition realm created in Keycloak.
  - a. Sign in with one of the usernames created during setup.



3. Since this is the initial sign in, a prompt will appear to update the password for this account. Again, for this example, the initial password credential was set to temporary, which forces an update to the password. Update the password and click Submit.



The image shows a web interface for Ignition. At the top, the word "IGNITION" is displayed in white capital letters on a dark background. Below this, the title "Update password" is centered. A yellow warning box with a triangle icon contains the text: "You need to change your password to activate your account." Below the warning box are two input fields: "New Password" and "Confirm password", each with a password icon on the right. At the bottom of the form is a blue "Submit" button.

4. Upon a successful login, the response from Keycloak can be seen within Ignition.



The image shows a screenshot of the "Test Results - OpenID Connect 1.0" window. It has three tabs: "IdP Response Data", "Mapped User Attributes", and "Security Level Grants". The "IdP Response Data" tab is selected, displaying a JSON response. The JSON includes fields for "idTokenClaims" (with sub-claims like exp, iat, auth\_time, jti, iss, aud, sub, typ, azp, nonce, session\_state, at\_hash, acr, sid, email\_verified, roles, name, preferred\_username, given\_name, family\_name, email) and "tokenEndpointResponse".

```
{
  "idTokenClaims": {
    "exp": 1661367976,
    "iat": 1661367676,
    "auth_time": 1661367676,
    "jti": "557866cc-7e87-4a1c-b30f-0000aeca8e9",
    "iss": "http://localhost:8080/realms/Ignition",
    "aud": "ignition-test",
    "sub": "4ec1690a-70d8-485a-ba58-89a700a860e9",
    "typ": "ID",
    "azp": "ignition-test",
    "nonce": "eQpWWiHMHDbk0sGb0RihaU6CSe3kyxo6y0-DZCOMAtM",
    "session_state": "a5f80228-34ca-4c43-b382-099cd44a291b",
    "at_hash": "ZfbMg392oVax0ygaF3zCcg",
    "acr": "1",
    "sid": "a5f80228-34ca-4c43-b382-099cd44a291b",
    "email_verified": false,
    "roles": [
      "manager"
    ],
    "name": "John Lennon",
    "preferred_username": "johnlennon",
    "given_name": "John",
    "family_name": "Lennon",
    "email": "john@email.com"
  },
  "tokenEndpointResponse": {
```

5. Specifically, note the 'roles' token nested in the 'userInfo' token. This was previously configured in Keycloak.

```
{
  "userInfo": {
    "sub": "4ec1690a-70d8-485a-ba58-89a700a860e9",
    "email_verified": false,
    "roles": [
      "manager"
    ],
    "name": "John Lennon",
    "preferred_username": "johnlennon",
    "given_name": "John",
    "family_name": "Lennon",
    "email": "john@email.com"
  }
}
```

6. Navigate to the Mapped User Attributes tab. Notice that only the ID is properly mapped.

Test Results - OpenID Connect 1.0

IdP Response Data	Mapped User Attributes	Security Level Grants
-------------------	------------------------	-----------------------

Attribute Name	Attribute Value
ID	4ec1690a-70d8-485a-ba58-89a700a860e9
Username	4ec1690a-70d8-485a-ba58-89a700a860e9
First Name	
Last Name	
Email	
Roles	

7. To set up the mapping, navigate to Security > Identity Providers. Use the More dropdown menu for keycloak and select User Attribute Mapping.

Name ^	Type	Description	Action	
default	Ignition	Automatically generated Ignition Identity Provider which uses the User Source Profile named "default".	<a href="#">More ▾</a>	<a href="#">Settings</a>
keycloak	OpenID Connect 1.0		<a href="#">More ▾</a>	<a href="#">Settings</a>
<a href="#">→ Create new Identity Provider...</a>			<div><div>«</div><div>◀</div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	

8. Map as follows:

- a. Username: Type=direct, Source=ID Token Claims, Path=preferred\_username
- b. First Name: Type=direct, Source=ID Token Claims, Path=given\_name
- c. Last Name: Type=direct, Source=ID Token Claims, Path=family\_name
- d. Email: Type=direct, Source=ID Token Claims, Path=email
- e. Roles: Type=direct, Source=ID Token Claims, Path=roles

Username *	<p>Type direct</p> <p>The type of mapping to apply for usernames.</p> <p>Source ID Token Claims</p> <p>The name of the attribute source.</p> <p>Path preferred_username</p> <p>Path to the attribute to map.</p>
First Name	<p>Type direct</p> <p>The type of mapping to apply for first names.</p> <p>Source ID Token Claims</p> <p>The name of the attribute source.</p> <p>Path given_name</p> <p>Path to the attribute to map.</p>
Last Name	<p>Type direct</p> <p>The type of mapping to apply for last names.</p> <p>Source ID Token Claims</p> <p>The name of the attribute source.</p> <p>Path family_name</p> <p>Path to the attribute to map.</p>

Email	<p>Type direct</p> <p>The type of mapping to apply for email addresses.</p> <p>Source ID Token Claims</p> <p>The name of the attribute source.</p> <p>Path email</p> <p>Path to the attribute to map.</p>
Roles	<p>Type direct</p> <p>The type of mapping to apply for user roles.</p> <p>Source ID Token Claims</p> <p>The name of the attribute source.</p> <p>Path roles</p> <p>Path to the attribute to map.</p>

9. Click Save.

10. Test the Login again and navigate to the Mapped User Attributes. Notice the user info attributes are now properly mapped.

Test Results - OpenID Connect 1.0

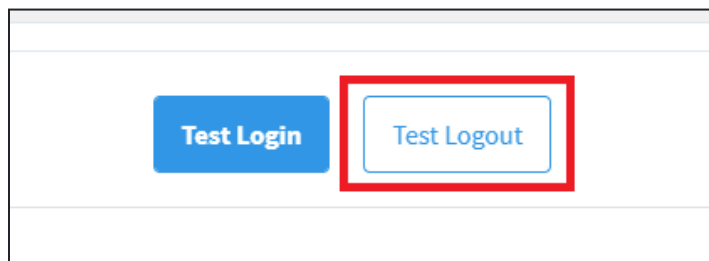
IdP Response Data	Mapped User Attributes	Security Level Grants
Attribute Name		Attribute Value
ID	4ec1690a-70d8-485a-ba58-89a700a860e9	
Username	johnlennon	
First Name	John	
Last Name	Lennon	
Email	john@email.com	
Roles	manager	

11. If a user has multiple roles, those will appear as a comma-separated list.

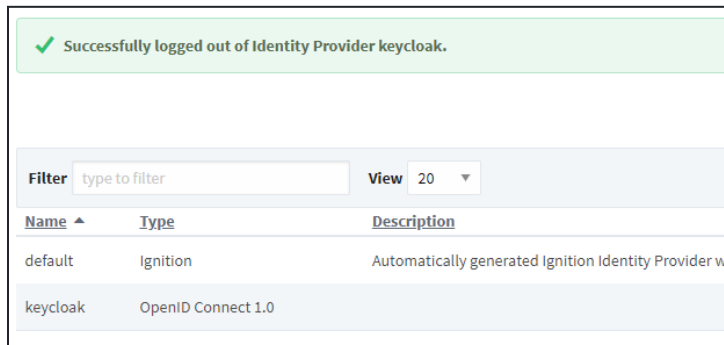
Test Results - OpenID Connect 1.0

IdP Response Data	Mapped User Attributes	Security Level Grants
Attribute Name		Attribute Value
ID	6465246a-11c6-493b-8f71-938ba4b71392	
Username	paulmccartney	
First Name	Paul	
Last Name	McCartney	
Email	paul@email.com	
Roles	manager, operator	

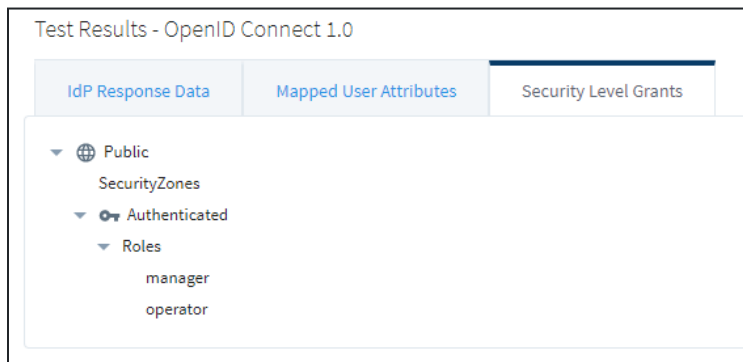
12. Verify the Test Logout redirects correctly as well.



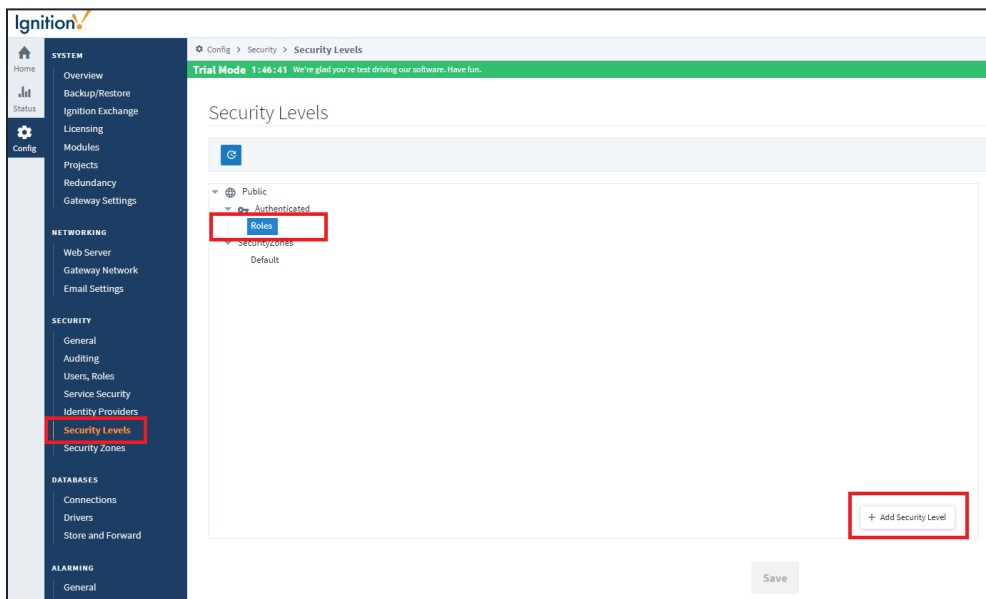
13. Ignition will confirm a successful logout.



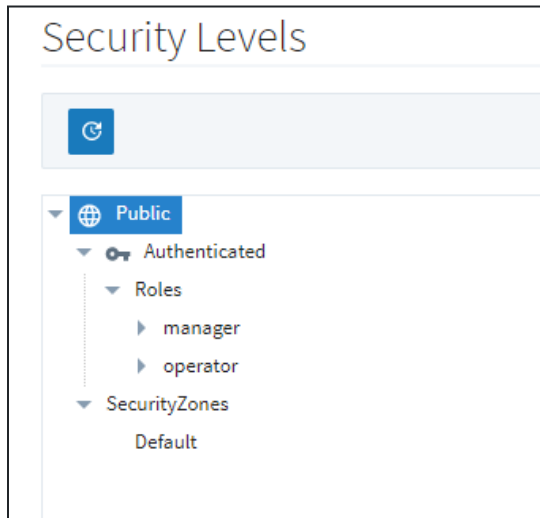
14. Finally, the security levels need to be defined in Ignition. The Security Level Grants in the test login results shows both of the configured keycloak roles.



These roles need to be added to Ignition's security levels. Navigate to Security > Security Levels and add the roles under the Roles branch.



15. Once complete, click Save. The new roles should be visible in Ignition's Security Levels tree.

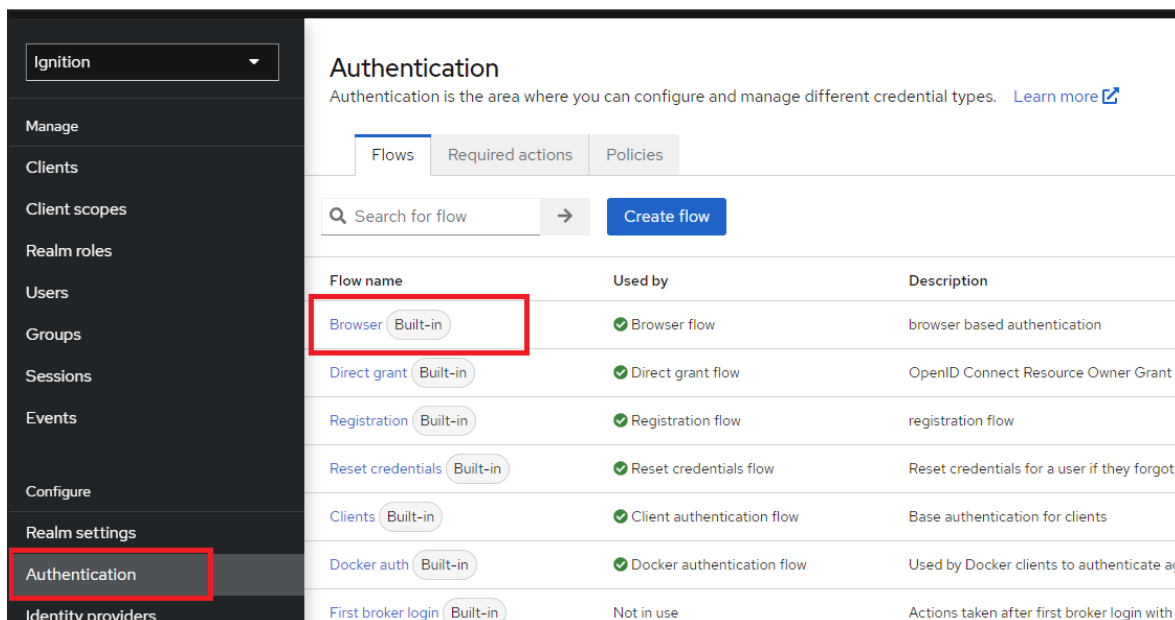


# Configuring Two-Factor Authentication (2FA)

Keycloak supports the use of a one-time password (OTP) via the Google Authenticator or FreeOTP apps. This feature is fully supported standalone (i.e., on-prem or offline).

1. Enforcing the OTP can be configured for all users or on a per user basis.

To configure an OTP for all users, navigate to the Authentication > Flows > Browser Flow name.

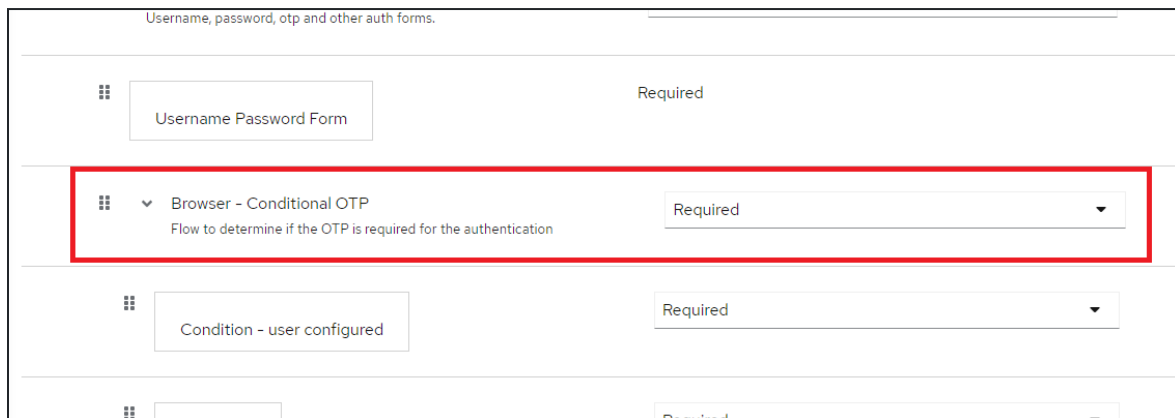


The screenshot shows the Keycloak Administration Console. On the left, the 'Authentication' menu item is highlighted. The main panel is titled 'Authentication' and contains a table of authentication flows. The 'Browser' flow is highlighted with a red box.

Flow name	Used by	Description
Browser Built-in	✓ Browser flow	browser based authentication
Direct grant Built-in	✓ Direct grant flow	OpenID Connect Resource Owner Grant
Registration Built-in	✓ Registration flow	registration flow
Reset credentials Built-in	✓ Reset credentials flow	Reset credentials for a user if they forgot t
Clients Built-in	✓ Client authentication flow	Base authentication for clients
Docker auth Built-in	✓ Docker authentication flow	Used by Docker clients to authenticate ag
First broker login Built-in	Not in use	Actions taken after first broker login with i

2. Find the Browser - Conditional OTP step and change it to Required.

NOTE: This will force all users to utilize an OTP with every login.



The screenshot shows the configuration of the 'Browser - Conditional OTP' flow. The flow is highlighted with a red box, and its status is set to 'Required'.

Step	Status
Username Password Form	Required
Browser - Conditional OTP Flow to determine if the OTP is required for the authentication	Required
Condition - user configured	Required



- Another option is to set OTP on a per user basis in the Required user actions when configuring a user. If this is configured, this particular user will be required to utilize the OTP with each login.

Users > User details

## paulmccartney

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider

ID \*

6465246a-11c6-493b-8f71-938ba4b71392

Created at \*

8/23/2022, 9:36:09 AM

Username \*

paulmccartney

Email

paul@email.com

Email verified ?

☐ Off

First name

Paul

Last name

McCartney

Enabled ?

☒ On

Required user actions ?

Configure OTP ✕

Select action

Save


Revert


4. In either case, when the user logs in for the first time, the user will be prompted to set up the Mobile Authenticator (either FreeOTP or Google Authenticator).

NOTE: The FreeOTP or Google Authenticator app must be downloaded on a mobile device to proceed.

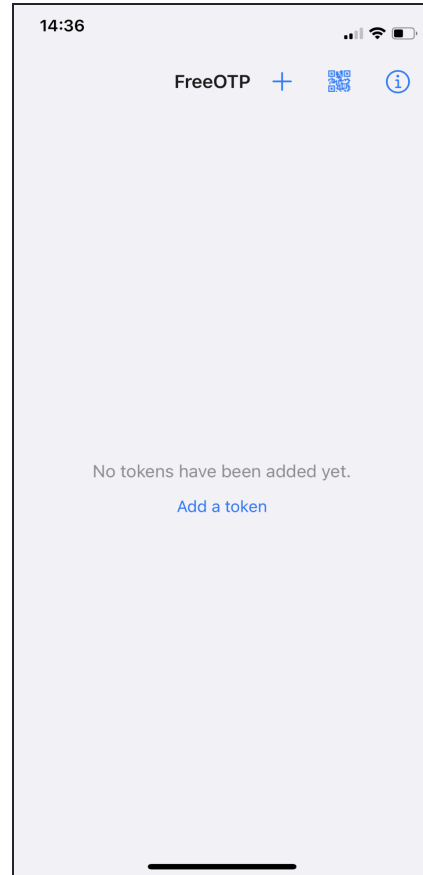
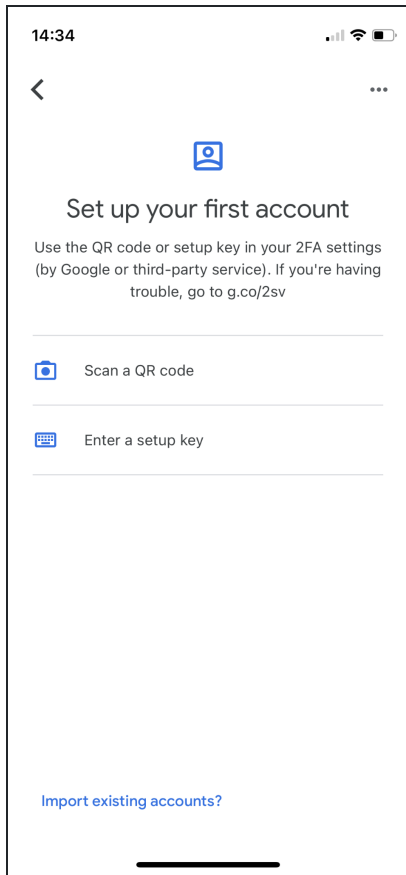
# IGNITION

## Mobile Authenticator Setup

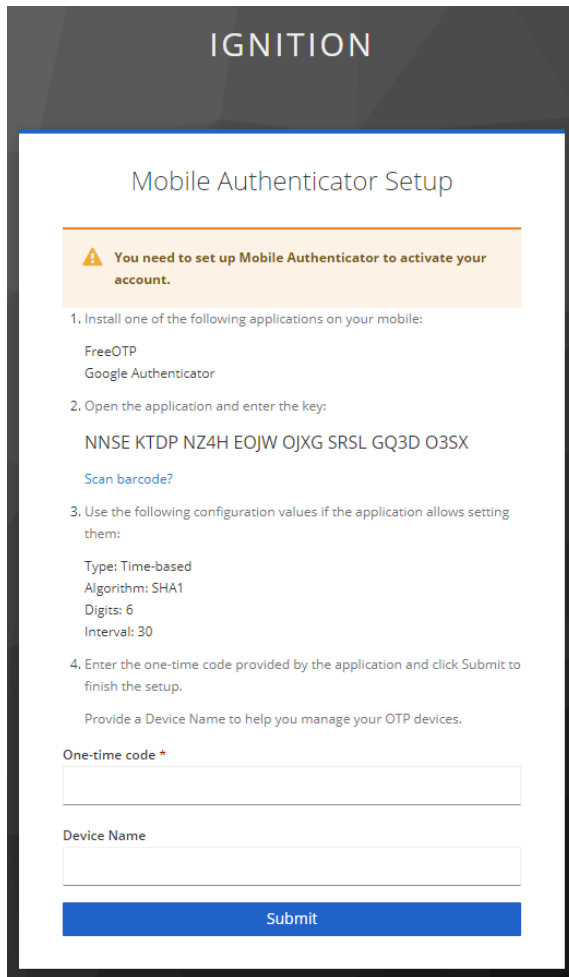
 **You need to set up Mobile Authenticator to activate your account.**

1. Install one of the following applications on your mobile:  
FreeOTP  
Google Authenticator
2. Open the application and scan the barcode:  
  
[Unable to scan?](#)
3. Enter the one-time code provided by the application and click Submit to finish the setup.  
Provide a Device Name to help you manage your OTP devices.  
One-time code \*  
  
Device Name

5. The apps have similar interfaces. In both apps, the QR code can be easily scanned.



6. If the scan doesn't work, the setup key can be manually entered directly on the app. Select the "Unable to scan?" link on the login page. This will bring up another screen with the setup key.



IGNITION

### Mobile Authenticator Setup

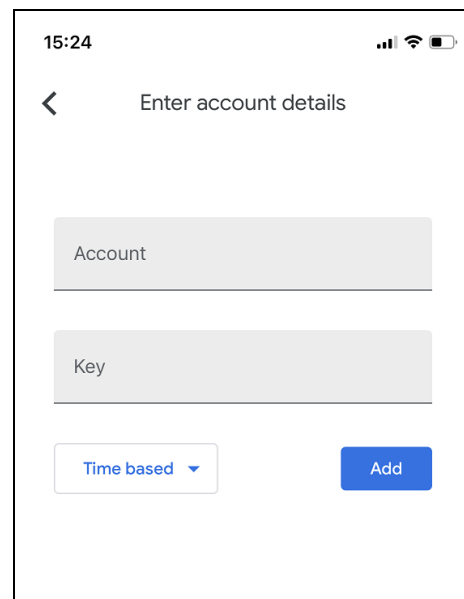
**⚠ You need to set up Mobile Authenticator to activate your account.**

1. Install one of the following applications on your mobile:  
FreeOTP  
Google Authenticator
2. Open the application and enter the key:  
**NNSE KTD P NZ4H EOJW OJXG SRSL GQ3D O3SX**  
[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:  
Type: Time-based  
Algorithm: SHA1  
Digits: 6  
Interval: 30
4. Enter the one-time code provided by the application and click Submit to finish the setup.  
Provide a Device Name to help you manage your OTP devices.

One-time code \*

Device Name

Submit



15:24


< Enter account details

Account

Key

Time based ▾ Add

7. After the initial setup, the user will be prompted on each subsequent login for an OTP.

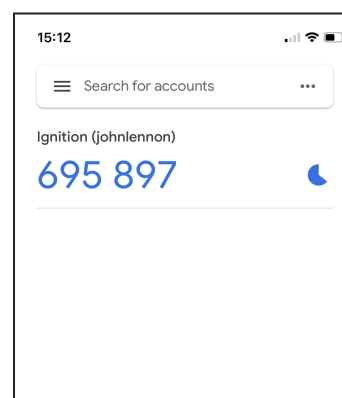


IGNITION

johnlennon

One-time code

Sign In



15:12

Search for accounts

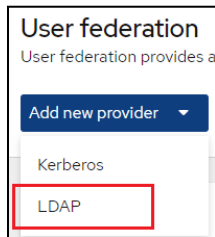
Ignition (johnlennon)

695 897

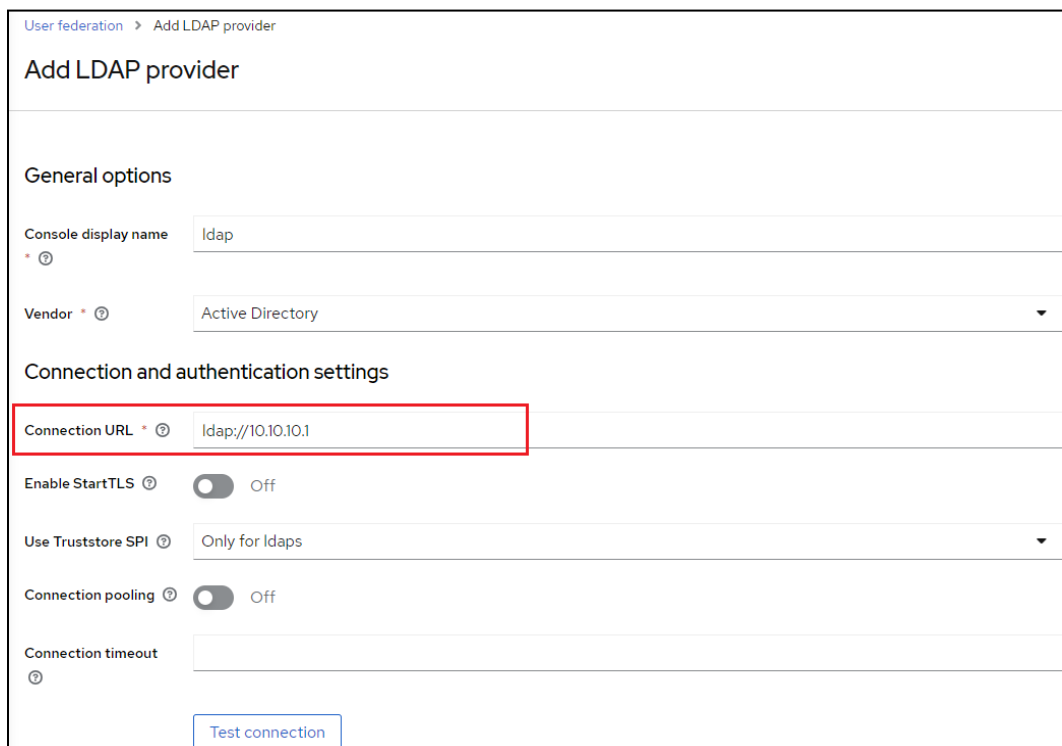
# User Federation - Active Directory

In a scenario where a customer is using an existing external database or directory (like Active Directory) for user management, but also wants to add in 2FA (two-factor authentication), implementing the User Federation component of Keycloak is a great option. Using the following steps, Keycloak can be configured to import users into the local database and incorporate additional authentication requirements, such as OTP.

1. Select User federation from the side menu.
2. Select the dropdown Add new provider > LDAP.



3. Add the Connection URL of the Active Directory server.
  - a. For example: `ldap://<myADserverIP>`

A screenshot of the 'Add LDAP provider' configuration page in Keycloak. The page has a breadcrumb 'User federation > Add LDAP provider'. The title is 'Add LDAP provider'. Under 'General options', there are fields for 'Console display name' (set to 'ldap') and 'Vendor' (set to 'Active Directory'). Under 'Connection and authentication settings', the 'Connection URL' field is highlighted with a red box and contains the value 'ldap://10.10.10.1'. Other settings include 'Enable StartTLS' (Off), 'Use Truststore SPI' (Only for ldaps), 'Connection pooling' (Off), and 'Connection timeout'. A 'Test connection' button is at the bottom.

4. Next, add in the bind distinguished name (Bind DN) information.

Bind type *	simple
Bind DN *	CN=John Lennon,CN=Users,DC=famousband,DC=com
Bind credentials *	.....
<button>Test authentication</button>	

5. In the LDAP searching and updating section, select the desired Edit mode. There are three modes available for user storage: READ\_ONLY, WRITEABLE, and UNSYNCED.

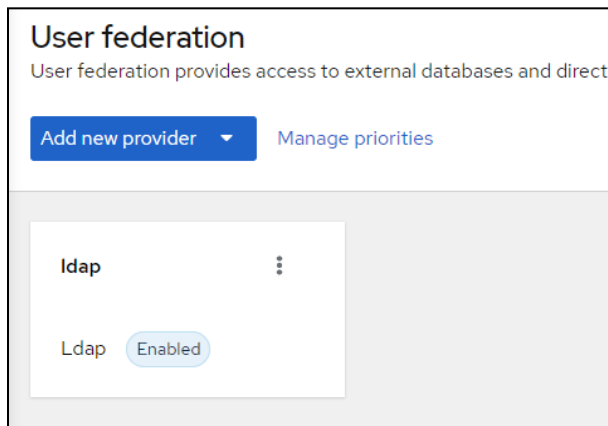
- READ\_ONLY - All mapped attributes are unchangeable from Keycloak.
- WRITEABLE - All mapped attributes (including passwords) can be updated and synchronized with the LDAP store (AD) from Keycloak, depending on the LDAP update privileges defined in AD.
- UNSYNCED - All changes to mapped attributes are stored in the local Keycloak database. Synchronization of those attributes must happen separately through a different process.

**NOTE:** Only the WRITEABLE and UNSYNCED modes allow for use of OTP, which attaches to the user locally stored in the Keycloak database.

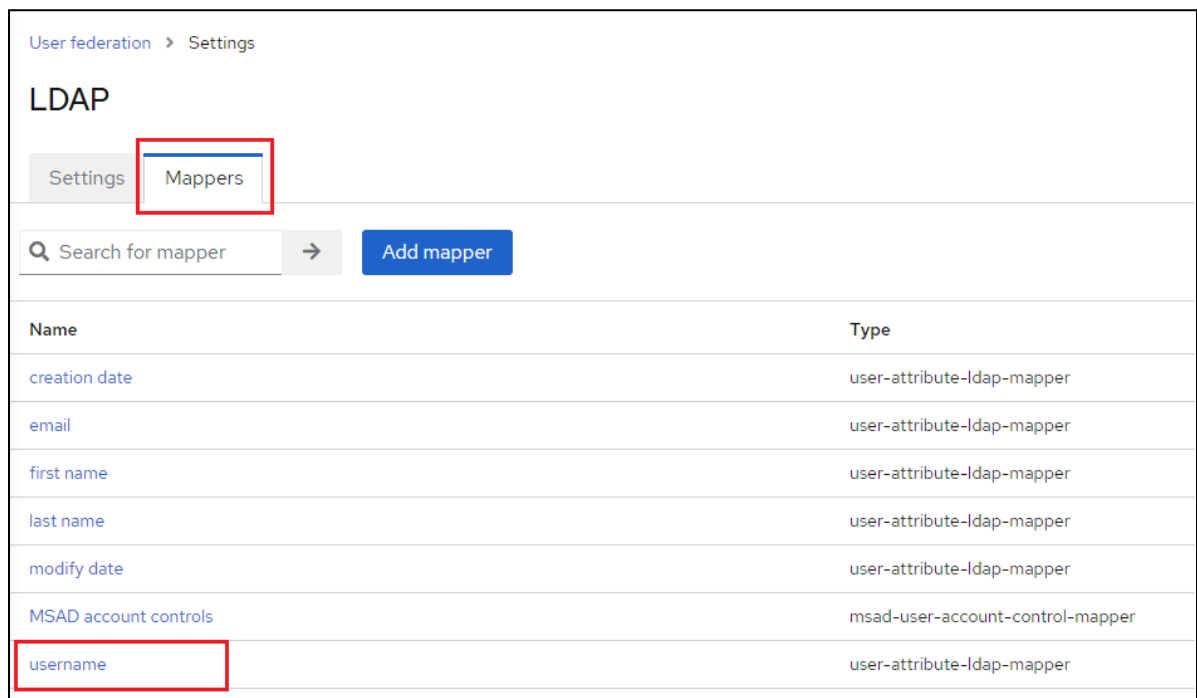
- For this example, UNSYNCED will be selected for the mode.
- Enter in the full DN of the LDAP tree for the Users.
- Since Active Directory is being used, the Username LDAP attribute will be sAMAccountName.

LDAP searching and updating	
Edit mode *	UNSYNCED
Users DN *	CN=Users,DC=famousband,DC=com
Username LDAP attribute *	sAMAccountName
RDN LDAP attribute *	cn
UUID LDAP attribute *	objectGUID
User object classes *	person, organizationalPerson, user
User LDAP filter	

6. Click Save to add the new LDAP provider.
7. Select the newly added provider again.



8. Select the Mappers tab. Then, select the username mapper.



9. Modify the User Model Attribute to match the Username LDAP attribute previously entered during configuration. In this example, that value is sAMAccountName.

User federation > Settings > Mapper details

username

ID	5fb2 [REDACTED]
Name * ⓘ	username
Mapper type * ⓘ	user-attribute-ldap-mapper
User Model Attribute ⓘ	sAMAccountName
LDAP Attribute ⓘ	sAMAccountName
Read Only ⓘ	<input checked="" type="checkbox"/> On

10. Click Save to apply the new mapper values.

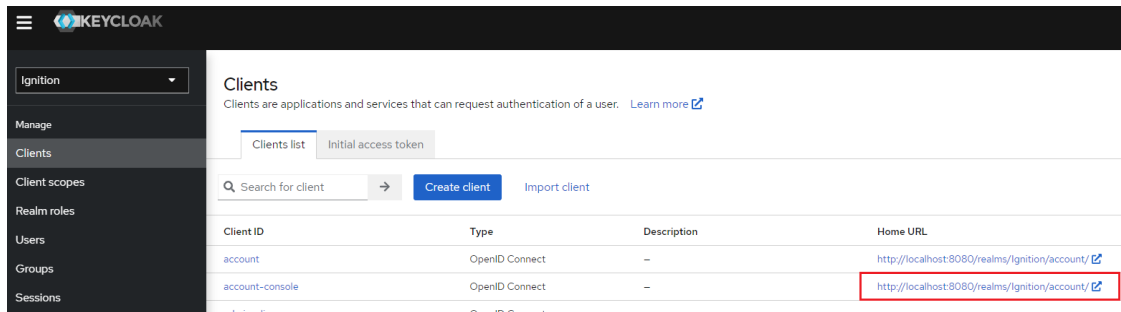
11. Navigate back to the User federation settings. Verify that both the connection and authentication are successful by clicking Test connection and Test authentication.

Connection and authentication settings

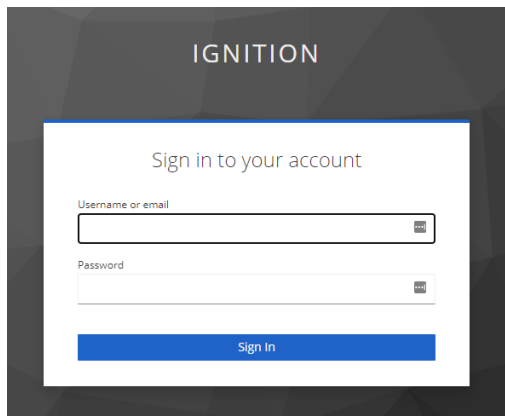
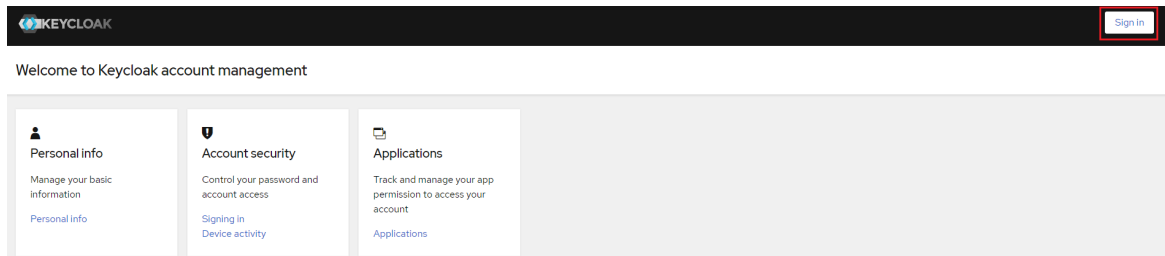
Connection URL * ⓘ	ldap://10.10.10.1
Enable StartTLS ⓘ	<input type="checkbox"/> Off
Use Truststore SPI ⓘ	Only for Idaps ▼
Connection pooling ⓘ	<input type="checkbox"/> Off
Connection timeout ⓘ	
	<input type="button" value="Test connection"/>
Bind type * ⓘ	simple ▼
Bind DN * ⓘ	CN=John Lennon,CN=Users,DC=famousband,DC=com
Bind credentials * ⓘ	.....
	<input type="button" value="Test authentication"/>



12. Once a successful connection has been established with Active Directory, verify that the user can be authenticated from Keycloak. Navigate to the Clients > Clients list > account-console Home URL.



13. From this screen, click Sign in and enter a valid user within Active Directory to test.



14. To implement 2FA (two-factor authentication), please review the previous section for additional setup and configuration. [Configuring Two-Factor Authentication](#).

## Appendix - Resources

Installation:

<https://www.keycloak.org/guides#getting-started>

Docker:

<https://docs.docker.com/get-started/#download-and-install-docker>

<https://www.keycloak.org/getting-started/getting-started-docker>

Two-Factor Authentication:

[https://www.keycloak.org/docs/latest/server\\_admin/#one-time-password-otp-policies](https://www.keycloak.org/docs/latest/server_admin/#one-time-password-otp-policies)

LDAP:

[https://www.keycloak.org/docs/latest/server\\_admin/#\\_ldap](https://www.keycloak.org/docs/latest/server_admin/#_ldap)

<https://medium.com/@yasithkumara/active-directory-as-a-user-federation-in-keycloak-926fd7cc3256>