

# Lab 02 - Configuring Keycloak

Keycloak is an open-source Identity and Access Management tool with a focus on modern applications such as single-page applications, mobile applications, and REST APIs. By delegating authentication to Keycloak, your applications do not need to worry about different authentication mechanisms, or how to safely store passwords. This approach also provides a higher level of security as applications do not have direct access to user credentials; they are instead provided with security tokens that give them only access to what they need. Keycloak builds on industry standard protocols supporting OAuth 2.0, OpenID Connect, and SAML 2.0. Using industry standard protocols is important from both a security perspective and in terms of making it easier to integrate with existing and new applications.

## Goal:

Keycloak comes with an admin console that allows you to configure and manage Keycloak. Before any clients can be configured to use the keycloak services, it is essential to configure an admin account that acts a super user having privileges to manage all features of keycloak. Once you have the admin account setup you can create realms, users, register clients or applications that is necessary for securing the applications.

## Lab tasks

In this lab you will:

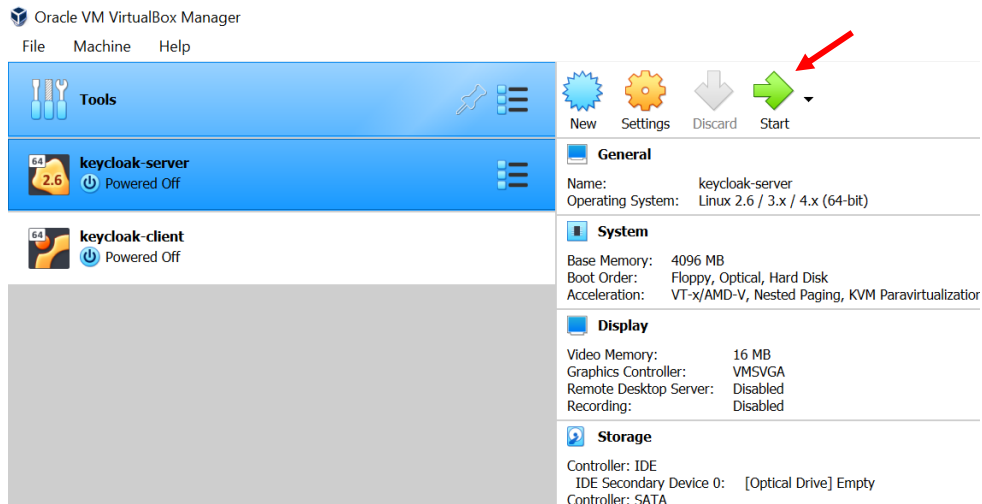
1. Updrading keycloak to version 12.0
2. Learn how to create admin accounts to manage the keycloak application
3. Create realm, users, groups and roles

## Task01: Upgrading Keycloak

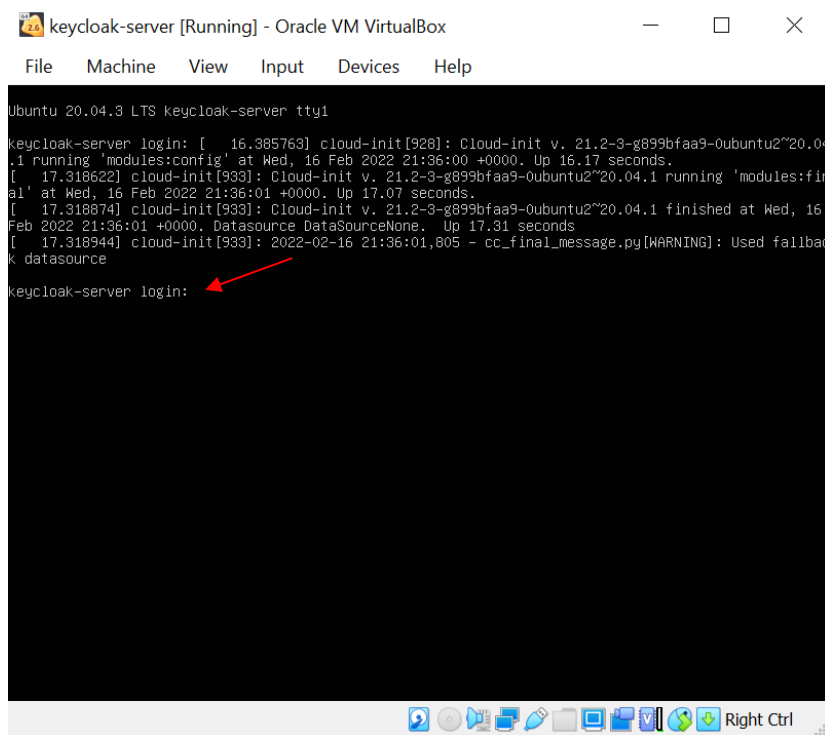
In this task we will first upgrade the Keycloak application to version 12. This task is for only those students who were able to successfully download and install the provided OVA file from Week 01. If you proceeded with Keycloak installation steps from the pre-requisite2 document, then you may do step1 and step2 to connect the Ubuntu server via SSH and then head directly for Task02.

### Step 1: Powering up keycloak virtual machine

1. In Virtualbox, select keycloak-server and press start.



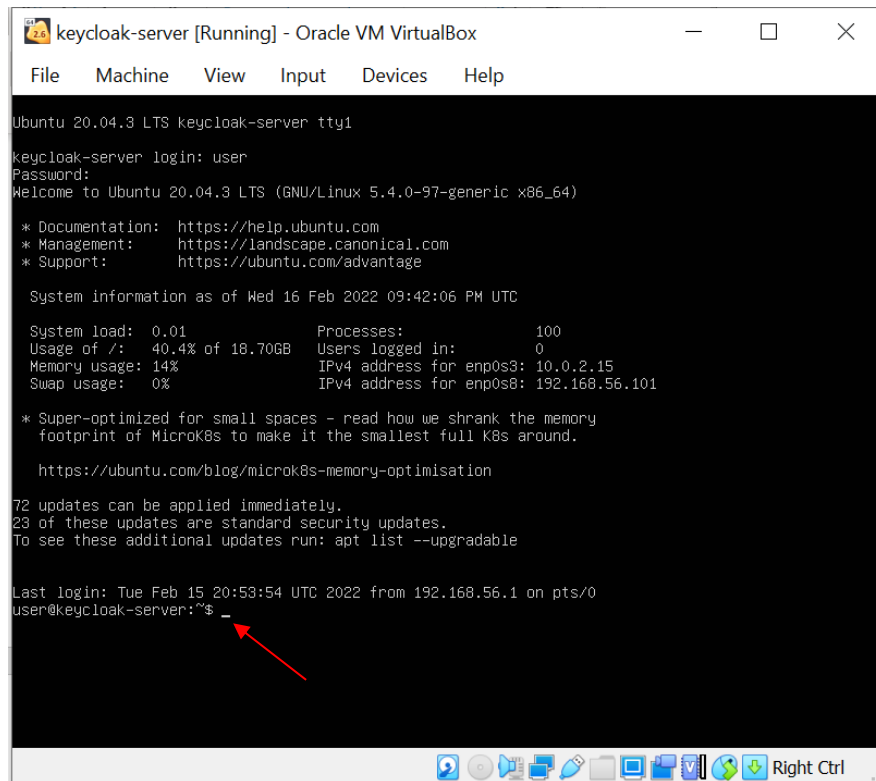
- Once the virtual-machine powers up, you will be prompted for the login credentials. (if you see some warning messages, click on the console scree and press enter you will be presented with login prompt)



- Enter the username as “user” and hit enter, when prompted for password type “Password-1”

```
keycloak-server login: user
Password: _
```

Note: In Linux, you will not see the password being typed on the screen, when prompted for password, start typing the password and hit enter when completed.



```
keycloak-server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 20.04.3 LTS keycloak-server tty1
keycloak-server login: user
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 16 Feb 2022 09:42:06 PM UTC

System load: 0.01          Processes: 100
Usage of /:  40.4% of 18.70GB    Users logged in: 0
Memory usage: 14%             IPv4 address for enp0s3: 10.0.2.15
Swap usage:  0%               IPv4 address for enp0s8: 192.168.56.101

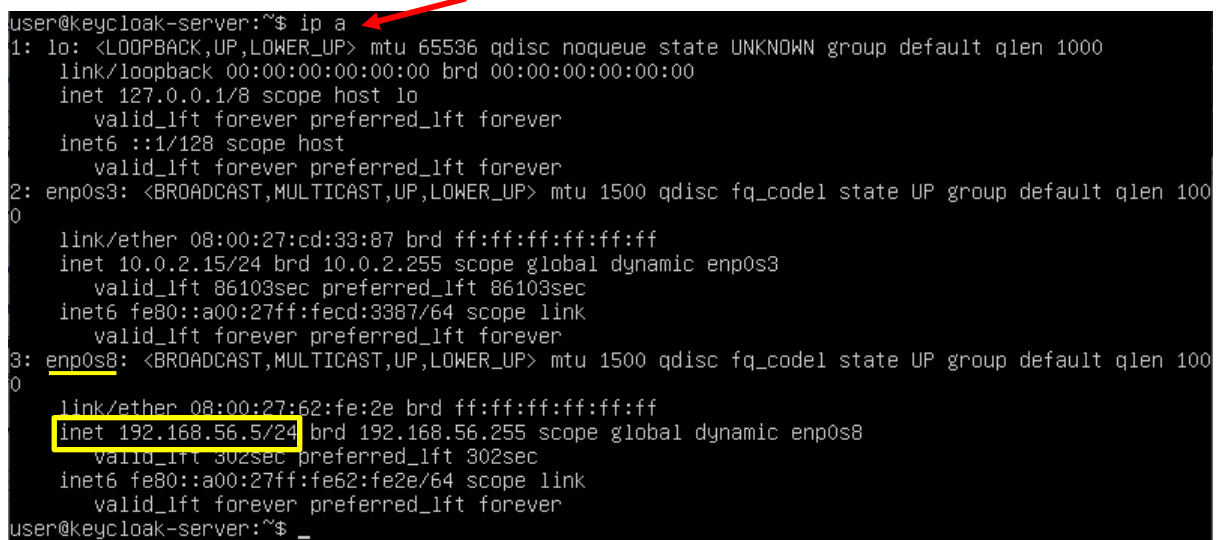
 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.
   https://ubuntu.com/blog/microk8s-memory-optimisation

72 updates can be applied immediately.
23 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Feb 15 20:53:54 UTC 2022 from 192.168.56.1 on pts/0
user@keycloak-server:~$
```

4. Once logged in you will see the user command prompt, enter the command:

`ip a`



```
user@keycloak-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cd:33:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86103sec preferred_lft 86103sec
    inet6 fe80::a00:27ff:fedc:3387/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:62:fe:2e brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.5/24 brd 192.168.56.255 scope global dynamic enp0s8
        valid_lft 302sec preferred_lft 302sec
    inet6 fe80::a00:27ff:fe62:fe2e/64 scope link
        valid_lft forever preferred_lft forever
user@keycloak-server:~$
```

## Step2: Connecting to the keycloak server using SSH

You can access the keycloak virtual machine through SSH to execute the commands from your host machine rather than directly on the Virtualbox virtual machine interface. This is especially useful to copy and paste the commands with ease. To connect via SSH:

1. Open a command prompt or Terminal window on a Mac and type the following:

ssh user@ip\_address

replace the highlighted text with keycloak sever's IP address you noted in step 5.

When prompted for password enter the and hit enter

```
H:\>ssh user@192.168.56.5
user@192.168.56.5's password:
```

You will see the following login screen with access user command prompt

```
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed 16 Feb 2022 11:46:44 PM UTC

System load:  0.06               Processes:            125
Usage of /:   42.6% of 18.7GB    Users logged in:     1
Memory usage: 15%              IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%                IPv4 address for enp0s8: 192.168.56.5

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

64 updates can be applied immediately.
15 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Feb 16 23:46:02 2022
user@keycloak-server:~$
```

The current version of keycloak needs to be upgraded to version 12.

2. Enter the following command:

sudo wget <https://github.com/keycloak/keycloak/releases/download/12.0.2/keycloak-12.0.2.zip>

```
user@keycloak-server:~$ sudo wget https://github.com/keycloak/keycloak/releases/download/12.0.2/keycloak-12.0.2.zip
[sudo] password for user:
--2022-03-17 04:40:45-- https://github.com/keycloak/keycloak/releases/download/12.0.2/keycloak-12.0.2.zip
Resolving github.com (github.com)... 52.64.108.95
Connecting to github.com (github.com)|52.64.108.95|:443... connected.
HTTP request sent, awaiting response...
```

sudo apt-get install unzip

sudo systemctl stop keycloak

sudo rm -r /opt/keycloak/

sudo mkdir -p /opt/keycloak

```
sudo unzip keycloak-12.0.2.zip -d /opt/keycloak

sudo ln -s /opt/keycloak/keycloak-12.0.2 /opt/keycloak/current

cd /opt

sudo chown -R keycloak: keycloak

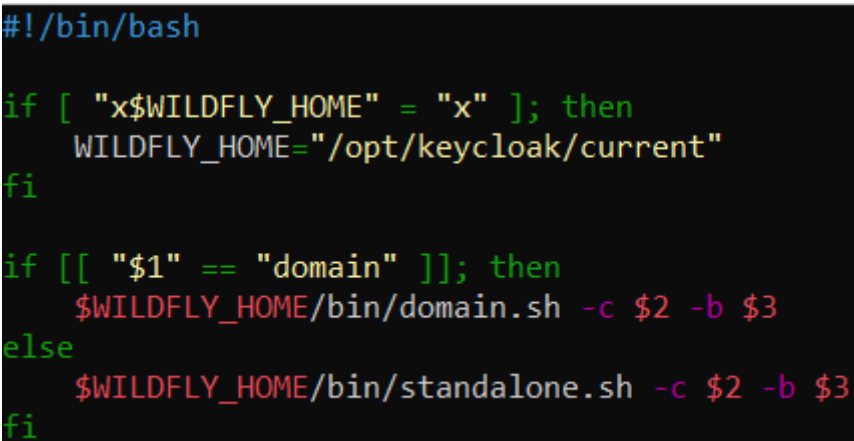
sudo chmod o+x /opt/keycloak/current/bin/

sudo cp /opt/keycloak/current/docs/contrib/scripts/systemd/wildfly.conf
/etc/keycloak/keycloak.conf

sudo cp /opt/keycloak/current/docs/contrib/scripts/systemd/launch.sh
/opt/keycloak/current/bin/

sudo chown keycloak: /opt/keycloak/current/bin/launch.sh

sudo nano /opt/keycloak/current/bin/launch.sh
```



```
#!/bin/bash

if [ "x$WILDFLY_HOME" = "x" ]; then
    WILDFLY_HOME="/opt/keycloak/current"
fi

if [[ "$1" == "domain" ]]; then
    $WILDFLY_HOME/bin/domain.sh -c $2 -b $3
else
    $WILDFLY_HOME/bin/standalone.sh -c $2 -b $3
fi
```

3. Press Ctrl+o to save and Ctrl+x to exit the nano editor

```
sudo cp /opt/keycloak/current/docs/contrib/scripts/systemd/wildfly.service
/etc/systemd/system/keycloak.service
```

```
sudo nano /etc/systemd/system/keycloak.service
```

```

[Unit]
Description=Keycloak Server
After=syslog.target network.target
Before=httpd.service

[Service]
Environment=LAUNCH_JBOSS_IN_BACKGROUND=1
EnvironmentFile=-/etc/keycloak/keycloak.conf
User=keycloak
Group=keycloak
LimitNOFILE=102642
PIDFile=/var/run/keycloak/keycloak.pid
ExecStart=/opt/keycloak/current/bin/launch.sh $WILDFLY_MODE $WILDFLY_CONFIG $WILDFLY_BIND
StandardOutput=null

[Install]
WantedBy=multi-user.target

```

4. Press Ctrl+o to save and Ctrl+x to exit the nano editor

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable keycloak
```

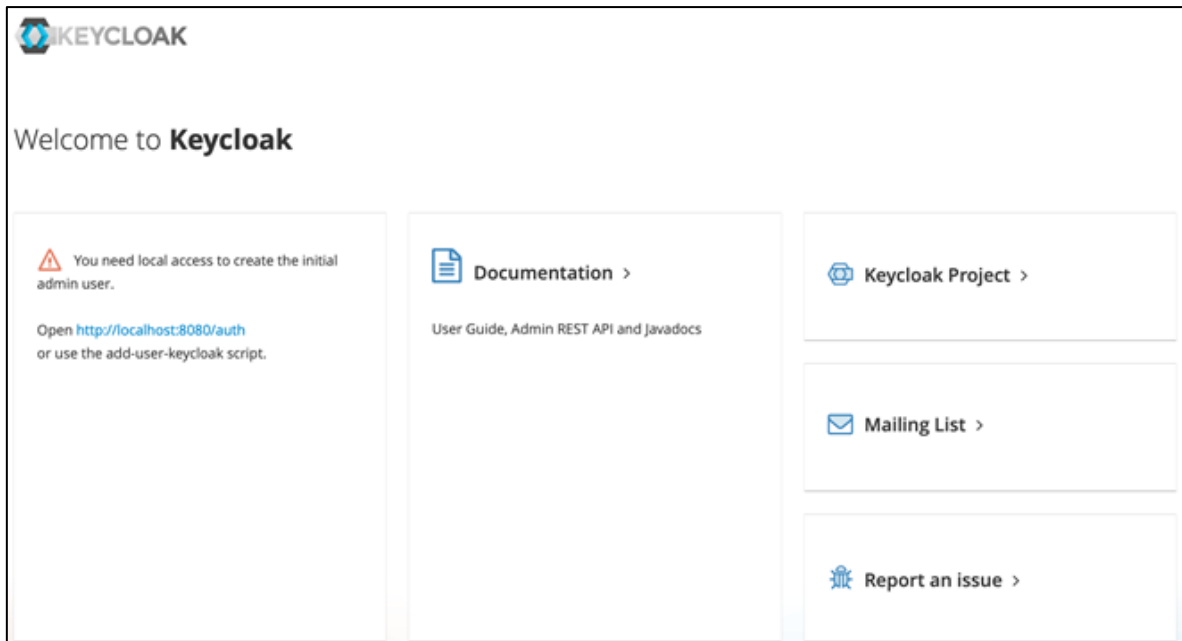
```
sudo systemctl start keycloak
```

```
sudo systemctl status keycloak
```

## Task02: Creating admin account

### Step 3: Accessing admin console and creating the first admin account

1. Note down the IP address of the third interface as highlighted in the image above.
2. Now on your host machine (either Windows or MAC OS where you installed the Virtualbox) open a web browser and type the following in the address bar: <http://keycloak-server-ip:8080/auth/>. Replace the highlighted text with keycloak server's ip you noted in the previous step (eg. <http://192.168.56.5:8080/auth/>).
3. You will see the following webpage. If there is a message on the webpage saying "you need local access to create the initial admin user". Then you need to create a admin account to access the admin console.



4. On the SSH terminal you launched on the host machine, enter the following command and set your own username and password by replacing the highlighted text with your own username and password:

```
sudo /opt/keycloak/current/bin/add-user-keycloak.sh -r master -u admin  
-p admin
```

```
user@keycloak-server:/opt$ sudo /opt/keycloak/current/bin/add-user-keycloak.sh -r master -u admin -p admin  
Added 'admin' to '/opt/keycloak/current/standalone/configuration/keycloak-add-user.json', restart server to load user
```

5. Restart the keycloak application by entering the following command:

```
sudo systemctl restart keycloak
```

6. Wait for a couple minutes for Keycloak to start and then refresh your browser window and you should now be able to login to the admin console.



Welcome to **Keycloak**



Administration Console >

Centrally manage all aspects of the Keycloak server



Documentation >

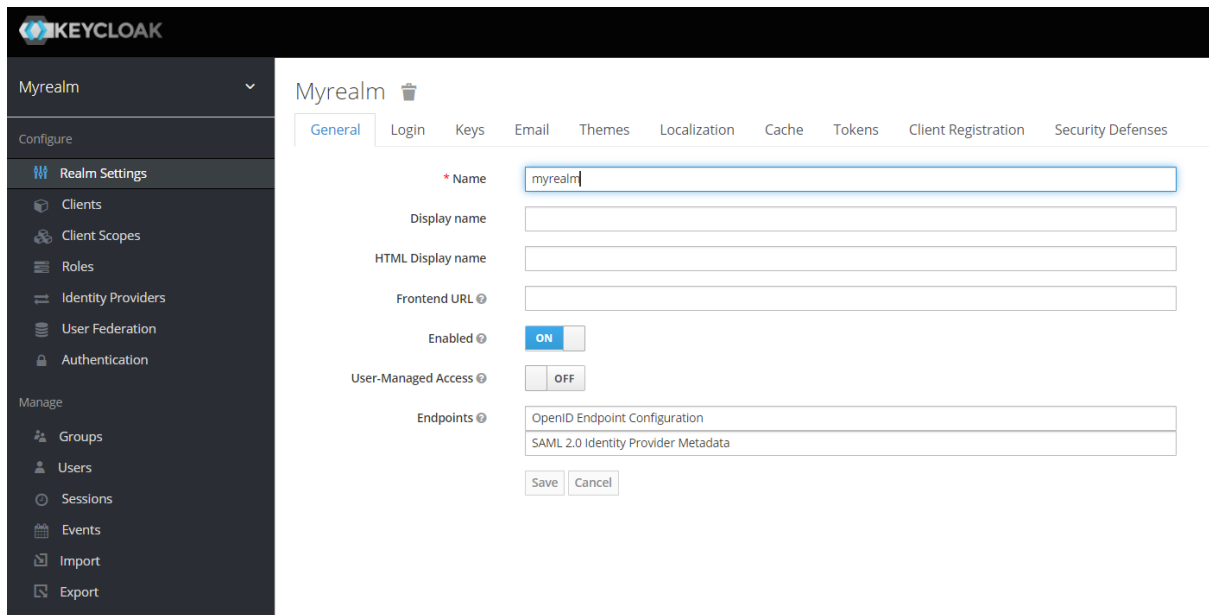
User Guide, Admin REST API and Javadocs

7. Click on the Administration Console and you will be redirected to the login screen as shown below:

The image shows the Keycloak login screen. At the top, the Keycloak logo is displayed. Below it, a white box contains the text "Sign in to your account". Underneath, there are two input fields: "Username or email" and "Password". Each field has a small icon on the right side. At the bottom of the white box, there is a blue button labeled "Sign In".

Once logged in you will see the main administration page where you can start adding realm, users, roles and clients.

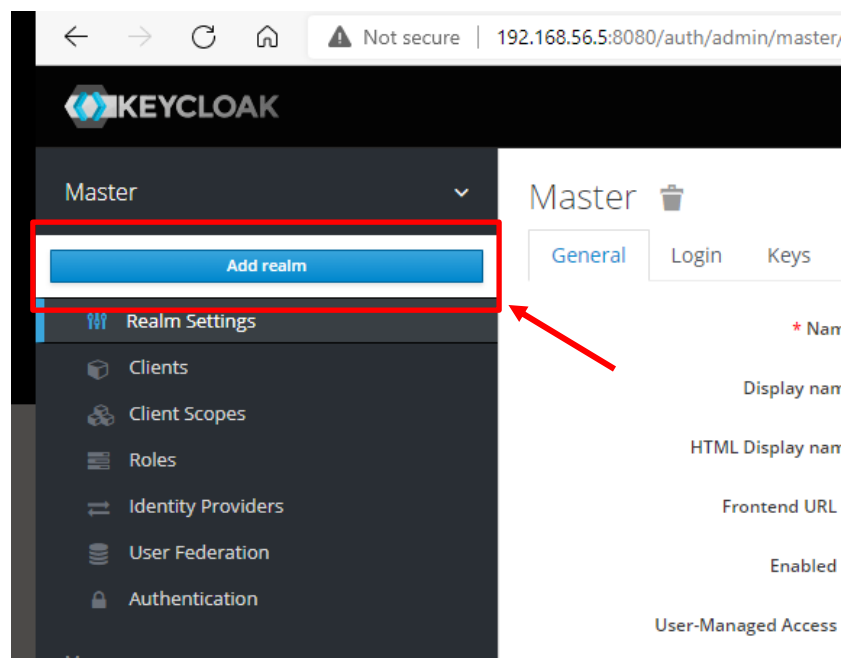




**Note:** If you get a "Can't Connect to Server" message, wait longer. Once it loads, go ahead and click that link, log in with the credentials you just created and we're in!

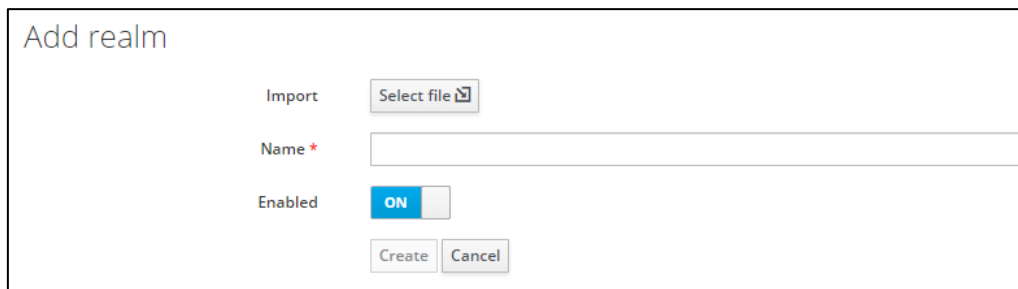
## Creating and configuring a realm

1. On the administration page you opened in the previous task, hover over the “Master” realm and you will see the “Add realm” option



Realm allows you group users/applications that share common configurations for authentication purposes. This is useful when allowing access to internal/external applications, employees/customers and so on

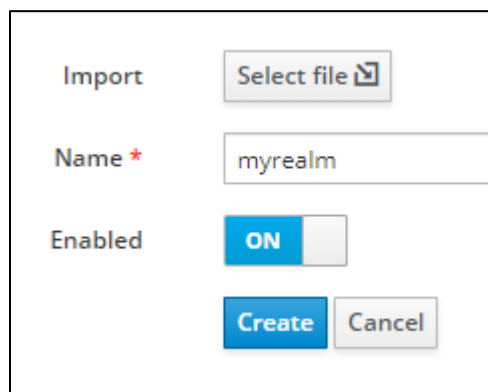
2. Enter a valid name for the realm. Avoid using special characters in the name as it will become part of the URL



The 'Add realm' form contains the following elements:

- Import:** A button labeled 'Select file' with a file icon.
- Name \*:** A text input field.
- Enabled:** A toggle switch currently set to 'ON'.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom.

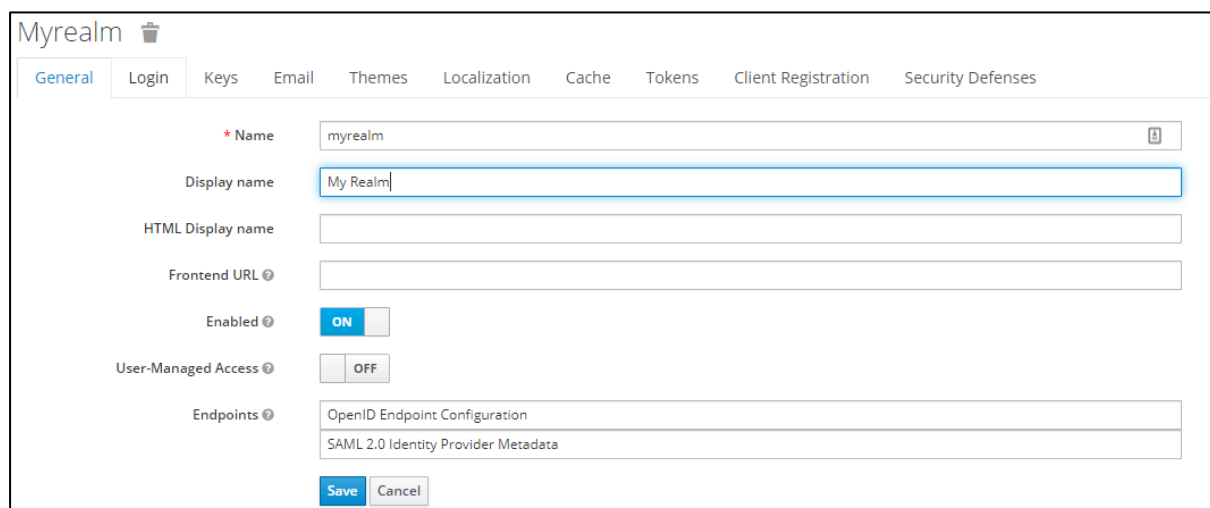
3. For the tasks in up-coming workshops create a realm with name: “myrealm”.



This is a cropped view of the 'Add realm' form with the following values:

- Import:** 'Select file' button.
- Name \*:** 'myrealm' entered in the text field.
- Enabled:** 'ON' toggle switch.
- Buttons:** 'Create' and 'Cancel' buttons.

4. Once you click “Create” you will be presented with options to add additional information about the realm. You can add a friendly name as part of the display name as shown below



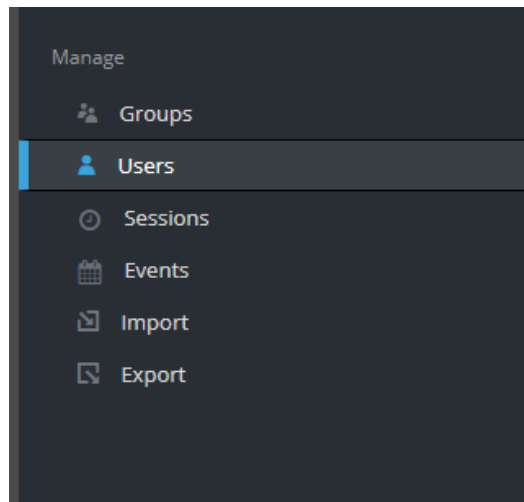
The 'Myrealm' configuration page shows the following details:

- Navigation tabs:** General (selected), Login, Keys, Email, Themes, Localization, Cache, Tokens, Client Registration, Security Defenses.
- Name:** 'myrealm' (with a lock icon).
- Display name:** 'My Realm' (highlighted with a blue border).
- HTML Display name:** Empty text field.
- Frontend URL:** Empty text field.
- Enabled:** 'ON' toggle switch.
- User-Managed Access:** 'OFF' toggle switch.
- Endpoints:** Two text fields containing 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

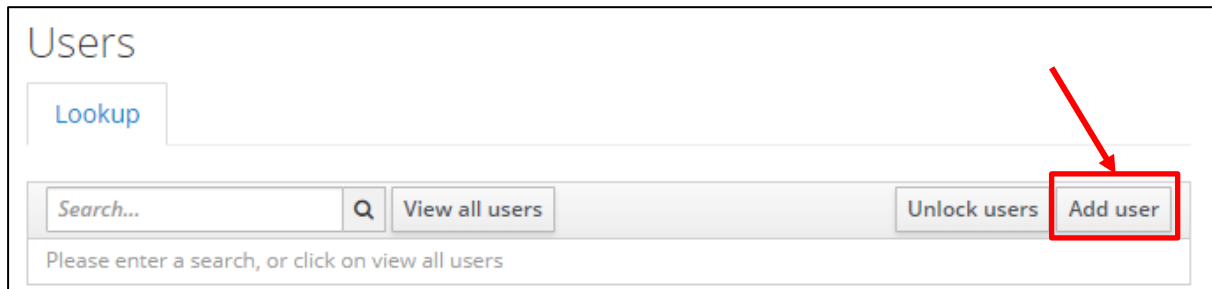
5. Press “Save” once you have completed making changes.

## Creating a user in the realm

1. On the administration page, select “Users” tab under manage section.




2. Click "Add users"




3. When creating a new user you need to provide a username for the user, email, firstname, lastname and required actions. The required actions allow administrators to force the user to perform certain actions when first logging in such as configure OTP for two factor authentication, update password, profile or verify email.

## Add user

ID	<input type="text"/>
Created At	
Username *	<input type="text" value="keycloak"/> 
Email	<input type="text" value="keycloak@localhost"/>
First Name	<input type="text" value="Keycloak"/>
Last Name	<input type="text" value="Student"/>
User Enabled ?	<input checked="" type="checkbox"/> ON
Email Verified ?	<input type="checkbox"/> OFF
Required User Actions ?	<div><div>Configure OTP</div><div>Update Password</div><div>Update Profile</div><div>Verify Email</div><div>Update User Locale</div></div>

4. For this workshop and as a requirement for upcoming workshops create the user with following details
- Username: keycloak
  - Email: keycloak@localhost
  - First Name: keycloak
  - Last name: student
  - User enabled: ON
  - Email verified: OFF
  - Required user actions: Update Password

## Add user

ID	<input type="text"/>
Created At	
Username *	<input type="text" value="keycloak"/> 
Email	<input type="text" value="keycloak@localhost"/>
First Name	<input type="text" value="Keycloak"/>
Last Name	<input type="text" value="Student"/>
User Enabled ?	<input checked="" type="checkbox"/> ON
Email Verified ?	<input type="checkbox"/> OFF
Required User Actions ?	<div><span>✕ Update Password</span>   <input type="text"/></div>

5. Click save once changes are completed. You will now see the user details page.

## Keycloak

Details | Attributes | Credentials | Role Mappings | Groups | Consents | Sessions

ID	586cae3f-6a83-4b90-a4ab-69c659726fe5
Created At	2/2/22 1:35:45 PM
Username	keycloak
Email	keycloak@localhost
First Name	Keycloak
Last Name	Student
User Enabled ?	<input checked="" type="checkbox"/> ON
Email Verified ?	<input type="checkbox"/> OFF

6. For the user to login for the first time a temporary password needs to be created. This can be done by navigating on the credentials tab for the user

Keycloak

Details Attributes **Credentials** Role Mappings Groups Consents Sessions

Manage Credentials

Position	Type	User Label	Data	Actions
----------	------	------------	------	---------

Set Password

Password

Password Confirmation

Temporary ☒ ON

Set Password

7. Enter a temporary password and click “Set Password”

Set Password

Password

Password Confirmation

Temporary ☒ ON

Set Password

**Explore:** how to add a custom attribute for a user such as office location details.

## Adding users to a group

Groups allow administrators to combine the users that share common attributes and all users belonging to the group inherit those attributes.

1. To create groups, navigate to groups under manage and select “New”

User Groups

Groups Default Groups ?

Search... View all groups New Edit Cut Paste Delete

Groups

2. Add a name for the group as “mygroup” and select save

Create group

Name \* mygroup

Save Cancel

**Explore:** How to assign a “department-name” attribute to all the user belonging to the HR department

3. To assign a user to a group, navigate to the user profile and change the group settings. All the available groups are listed, and you can choose the group and click “join”. Add the keycloak user to the mygroup we created earlier.

Users > keycloak

Keycloak

Details Attributes Credentials Role Mappings Groups Consents Sessions

Group Membership ?

Search... View all groups Leave

/mygroup

Available Groups ?

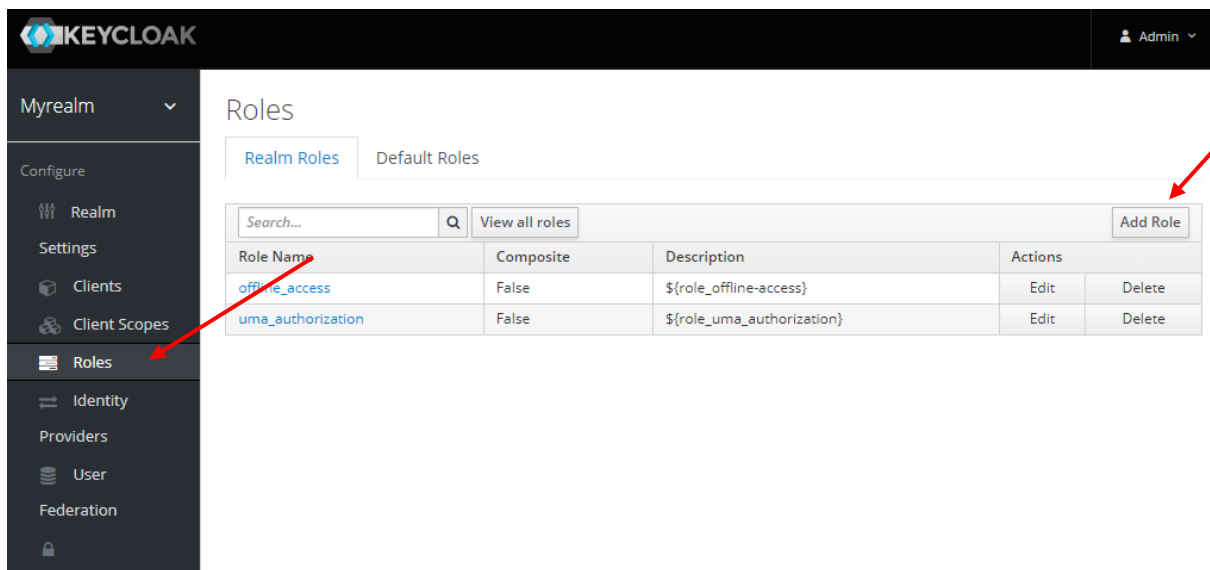
Search... View all groups Join

mygroup

## Creating roles and assigning user to roles

Roles allow administrators to control access policies by the role of the users. If there are multiple administrators, they can be added to an administrator role and users having those privileges can be added to the role.

1. To create a new role, select Roles under configure section.

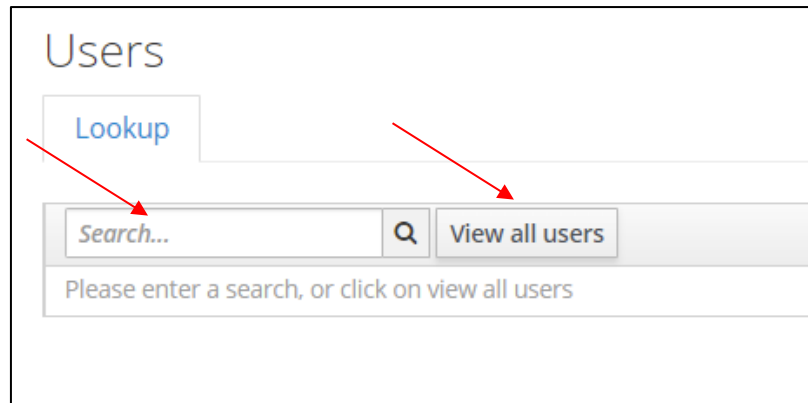


2. Click Add role and you will see the Add Role page.

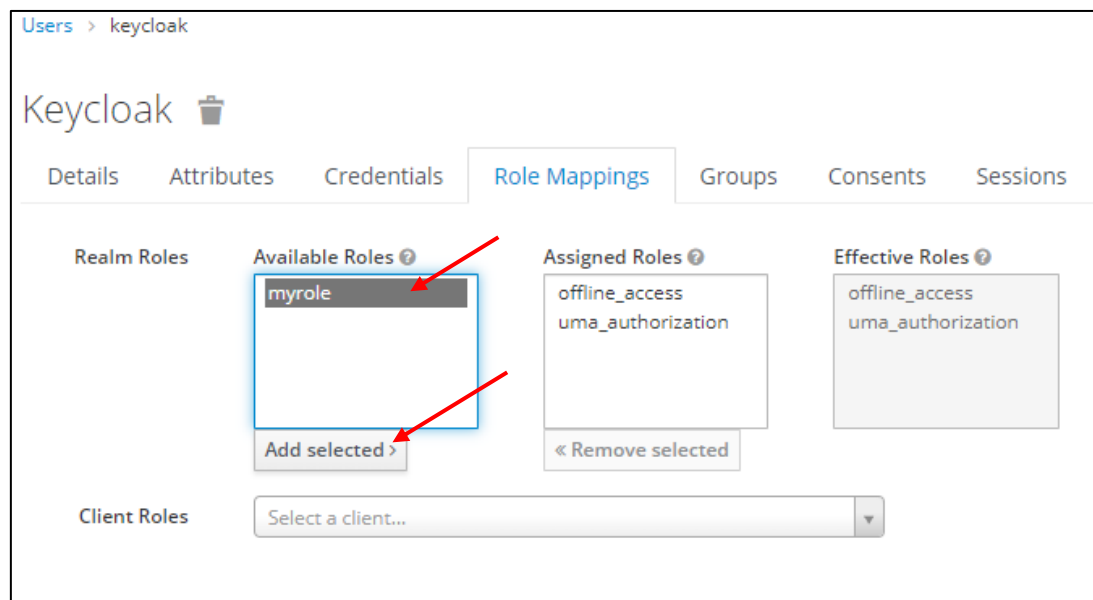
The screenshot shows the 'Add Role' page. At the top, it says 'Roles > Add Role'. The main heading is 'Add Role'. There is a form with two fields: 'Role Name' (marked with a red asterisk) and 'Description'. The 'Role Name' field contains the text 'myrole'. Below the form are two buttons: 'Save' and 'Cancel'.

3. Create a role with role name as: "myrole"
4. Now navigate Users tab under manage. You will see the users page

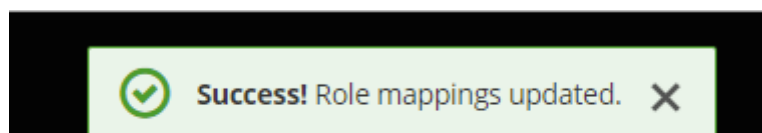




5. Either enter the user name in search bar and click the search icon next to the search box or click on View all users and select the user. In this case, select the keycloak user. You will see the keycloak user page.
6. Select the Role Mappings tab and select myrole from the Available Roles field. Click Add selected to map the role for the keycloak user.



7. Now the myrole will be added to the assigned roles. You will see following message once settings are updated



Keycloak

Details

Attributes

Credentials

Role Mappings

Groups

Consents

Sessions

Realm Roles

Available Roles

Add selected >

Assigned Roles

myrole  
offline\_access  
uma\_authorization

« Remove selected

Effective Roles

myrole  
offline\_access  
uma\_authorization

Client Roles

Select a client...

**Explore:** Can a role be part of another role?