Keycloak Get Users returns 403 forbidden

Asked 3 years, 4 months ago Modified 9 months ago Viewed 56k times

21

I create token using `http://localhost:8080/auth/realms/{realm_name}/protocol/openid-connect/token endpoint`.

grant_type=client_credentials
client-id: ------------
client-secret: 78296d38-cc82-4010-a817-65c283484e51

Now I want to get users of realm. Then I send request to `http://localhost:8080/auth/admin/realms/{realm_name}/users?username=demo` endpoint with token. But I got `403 forbidden` response with `"error": "unknown_error"`. How to solve it?

rest authentication keycloak access-token keycloak-rest-api

Share Edit Follow

edited Sep 8, 2021 at 9:32
Andrii Abramov
10.5k ● 12 ● 79 ● 101

asked Mar 3, 2021 at 6:54
Azhagesan
297 ● 1 ● 2 ● 13

6 Answers

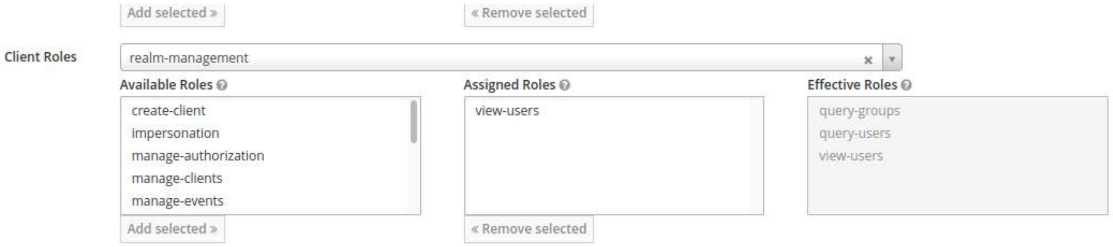
Sorted by: Highest score (default)

53

The service account associated with your client needs to be allowed to view the realm users.

1. Go to http://localhost:8080/auth/admin/{realm_name}/console/#/realms/{realm_name}/clients
2. Select your client (which must be a confidential client)
3. In the settings tab, switch **Service Account Enabled** to **ON**
4. Click on save, the Service Account Roles tab will appear
5. In Client Roles, select **realm_management**
6. Scroll through available roles until you can select **view_users**
7. Click on **Add selected**

You should have something like this :



You client is now allowed to access users through the REST API.

Share Edit Follow

edited May 19, 2022 at 9:41

answered Mar 3, 2021 at 10:02
Lucas Declercq
1,700 ● 12 ● 19

2 Was this changed in Keycloak 17? The `Service Account Enabled` is not showing on my screen. – ash Mar 28, 2022 at 22:31

4 I needed to add `view-users` role to the user: Users -> <user-name> -> Role Mappings -> Client Roles -> realm-management -> `view-users` -> `[Add Selected >>]` – ash Mar 29, 2022 at 15:43

1 @ash to display it you need to set the Access Type of your client to "confidential" – Max R. May 10, 2022 at 23:01

2 even after adding all roles I'm still getting the 403 error. Any clue? PS. I have Service Account enabled, and it is log in without issues. – Kostanos Aug 7, 2022 at 15:51

2 Hey, I did resolve, but I don't remember how. Make sure you that JWT token has roles inside, I think it was the problem, but I don't remember, sorry. – Kostanos Feb 13, 2023 at 20:29

8

to create(add) user

send POST request to:

```
http://localhost:8180/admin/realms/YOUR_REALM_NAME/users
```

with this body sample:

```
{
"firstName":"Amir",
"lastName":"Sharafkar", "email":"amirh.sharafkar@gmail.com", "enabled":"true",
"username":"sharafkar",
"credentials":[{
"type":"password",
"value":"1234",
"temporary":false
}]}
```

to get all users

send GET request to:

```
http://localhost:8180/admin/realms/YOUR_REALM_NAME/users
```

with "Authorization" key header with value: `Bearer {YOUR_TOKEN}`

to get individual user

send GET request to:

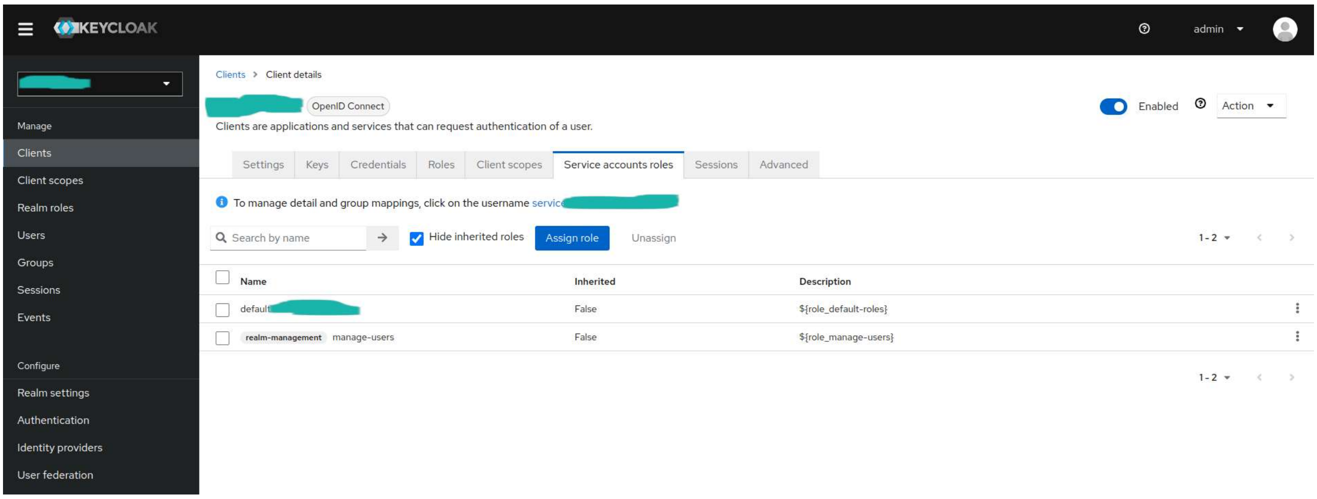
```
http://localhost:8180/admin/realms/YOUR_REALM_NAME/users/{id}
```

with "Authorization" key header with value: `Bearer {YOUR_TOKEN}`

DO NOT FORGET - Keycloak "version: 20.0.2"

assign role to your client with this steps:

1. Click Assign role button



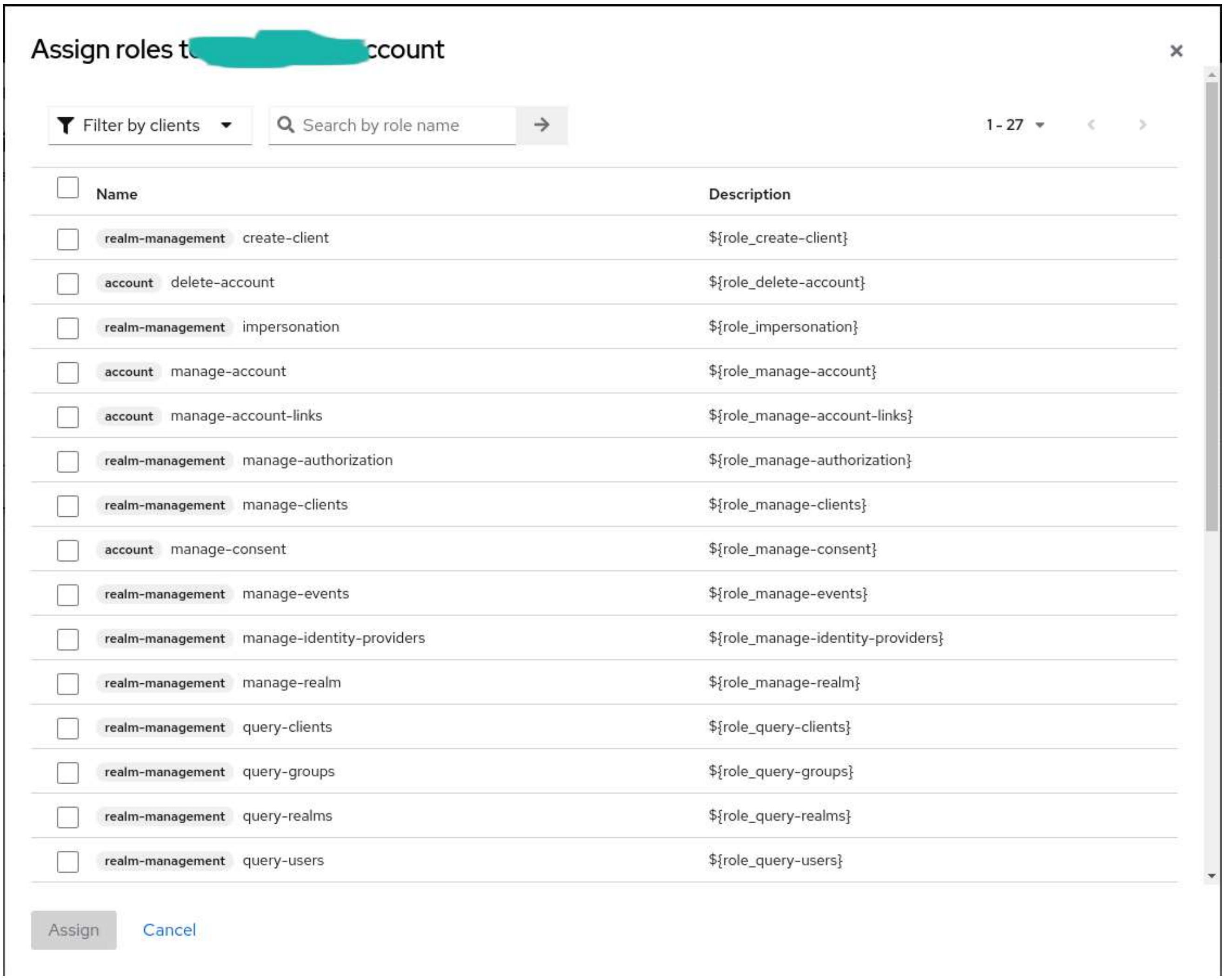
Clients are applications and services that can request authentication of a user.

To manage detail and group mappings, click on the username servic[redacted]

☑ Hide inherited roles

Name	Inherited	Description
default[redacted]	False	${role_default-roles}
realm-management manage-users	False	${role_manage-users}

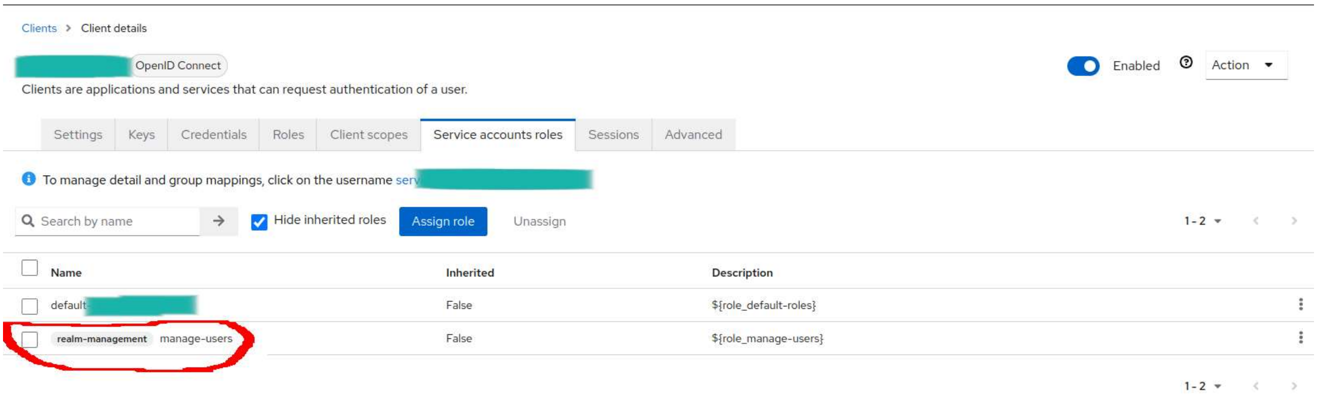
2. Select Filter by clients



Assign roles t[redacted]ccount ×

□ Name	Description
□ realm-management create-client	${role_create-client}
□ account delete-account	${role_delete-account}
□ realm-management impersonation	${role_impersonation}
□ account manage-account	${role_manage-account}
□ account manage-account-links	${role_manage-account-links}
□ realm-management manage-authorization	${role_manage-authorization}
□ realm-management manage-clients	${role_manage-clients}
□ account manage-consent	${role_manage-consent}
□ realm-management manage-events	${role_manage-events}
□ realm-management manage-identity-providers	${role_manage-identity-providers}
□ realm-management manage-realm	${role_manage-realm}
□ realm-management query-clients	${role_query-clients}
□ realm-management query-groups	${role_query-groups}
□ realm-management query-realms	${role_query-realms}
□ realm-management query-users	${role_query-users}

3. and finally add "manage-users" role to your client



[redacted] OpenID Connect

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

To manage detail and group mappings, click on the username serv[redacted]

☑ Hide inherited roles

□ Name	Inherited	Description
□ default[redacted]	False	${role_default-roles}
□ realm-management manage-users	False	${role_manage-users}

Share Edit Follow

edited Feb 5, 2023 at 8:10

answered Jan 31, 2023 at 14:23

Amir Sharafkar
111 ● 1 ● 2

2 Jizz! `2. Select Filter by clients` - that was I was looking for so long today. Thank you! **Why they hide it so deep!?** – MrHIDEn Mar 23, 2023 at 18:23

You need to assign a target realm-management role for your custom user. E.g. Keycloak version 19.02 to assign any realm-management role such as manage-users, manage-clients or realm-admin, you must follow these steps:

5

1. create a new user
2. Navigate to user details and open the Role Mapping tab.
3. click the Assign role button
4. select Filter by clients
5. you will see the first 10 results, click ">" to see the next 10 results, etc., or use the search box
6. select one target role

[Filter by client](), [realm-management roles]()

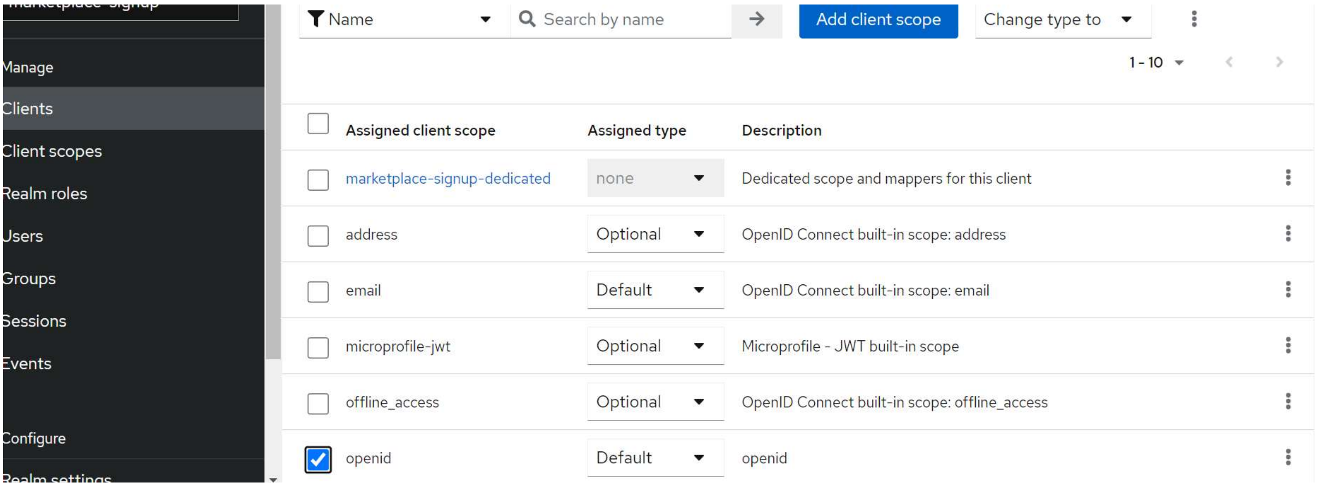
Share Edit Follow

edited Oct 9, 2022 at 10:21

answered Oct 9, 2022 at 10:18
Dzmitry Harlach
51 ●1 ●2

3

- Login to your Keycloak admin console and navigate to the "Client Scopes" section.
- Click the "Create" button to create a new client scope "openid" as default.
- then go to your realm client select client scopes tab.
- then add the openid scope.



□ Assigned client scope	Assigned type	Description
□ marketplace-signup-dedicated	none	Dedicated scope and mappers for this client
□ address	Optional	OpenID Connect built-in scope: address
□ email	Default	OpenID Connect built-in scope: email
□ microprofile-jwt	Optional	Microprofile - JWT built-in scope
□ offline_access	Optional	OpenID Connect built-in scope: offline_access
☑ openid	Default	openid

Share Edit Follow

answered Mar 27, 2023 at 21:19
Mohamed Fayek Saber
81 ●6

1 The reason why this worked, is most likely because you were using an example that had `scope=openid` in the URL at some point. This should not be needed in most scenarios unless you explicitly want to divide up scopes. – Torxed Apr 22, 2023 at 17:12

Not sure why it works but it works – Gilbert Jun 15 at 9:12

What I find strange is that it continues to work even after you remove the openid scope – Gilbert Jun 15 at 9:20

1

I ran into the same issue with the quarkus-Version 18.0.2:

- a client "tmp" identical configured like "admin-cli" (only different name)
- all roles of "realm-management" assigned to the generated service-user
- using a client-credential-Token of "tmp" for the user-Search-Endpoint (/auth/admin/realms/b2c/users/) leads to 403
- using a manually created user works well (password-credential-type)
- using the "admin-cli" client to get the client-credential-Token works well, too

I found this: "client_id is a confidential client that belongs to the realm master" here: https://github.com/keycloak/keycloak-documentation/blob/main/server_development/topics/admin-rest-api.adoc

I don't know why this restriction was introduced, but when you fetch your token from master (/auth/realms/master/protocol/openid-connect/token), then you are allowed to use a custom client and everything is fine.

Share Edit Follow

answered Aug 30, 2022 at 10:04
CNC-Parade
31 ●4

0

As the response code (`403`) says `forbidden`, it means that server has understood the request but you don't have the permissions to request that API.

So to get the access to view the users/groups/roles which are available in the Keycloak you must have to map the roles to the user. You can follow the below path to map any roles.

CLick on Users --> select your user --> click on Role Mapping --> click on Assign Roles --> Filter by clients --> select the roles and save

enter image description here

Share Edit Follow

answered Oct 10, 2023 at 5:06

M Md Abid Khan

1 ● 2