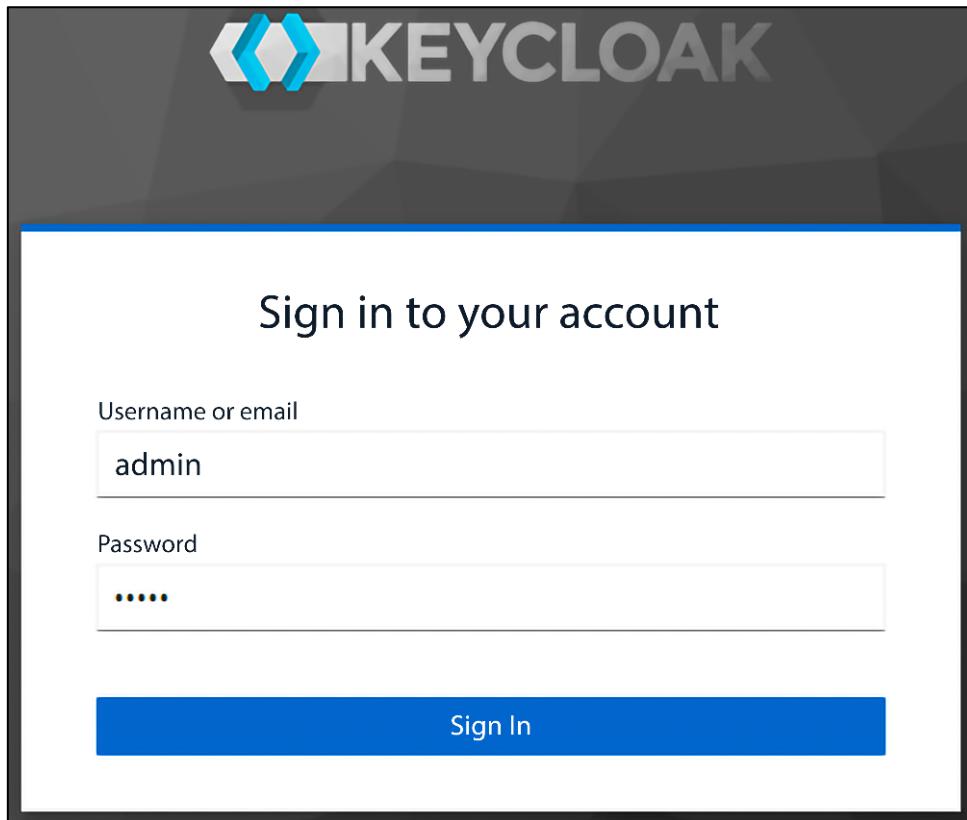
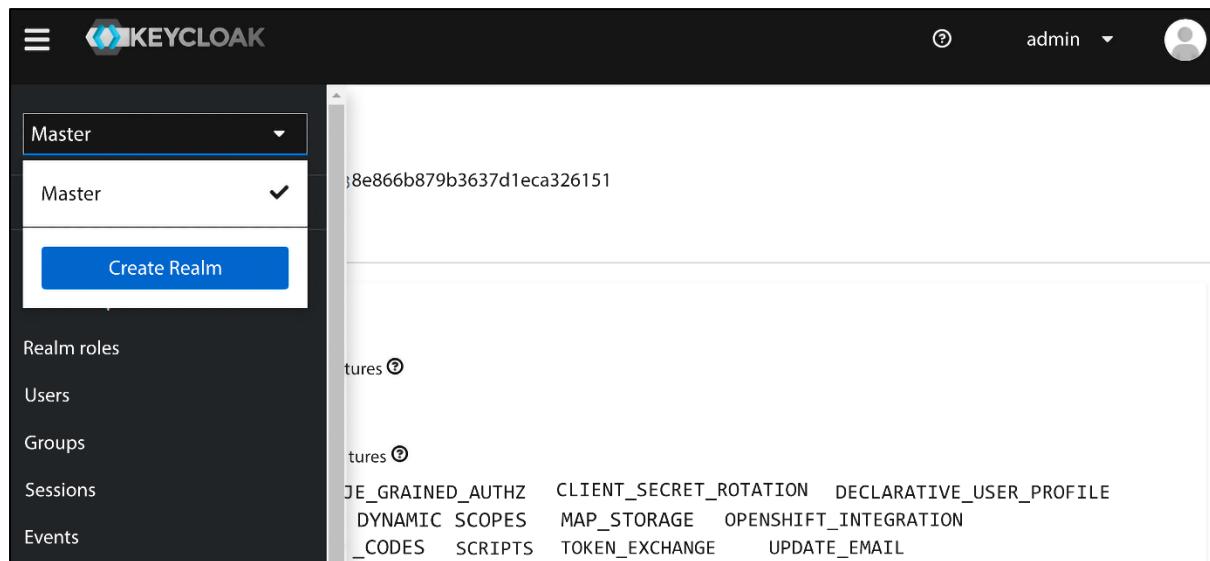


Chapter 1: Getting Started with Keycloak

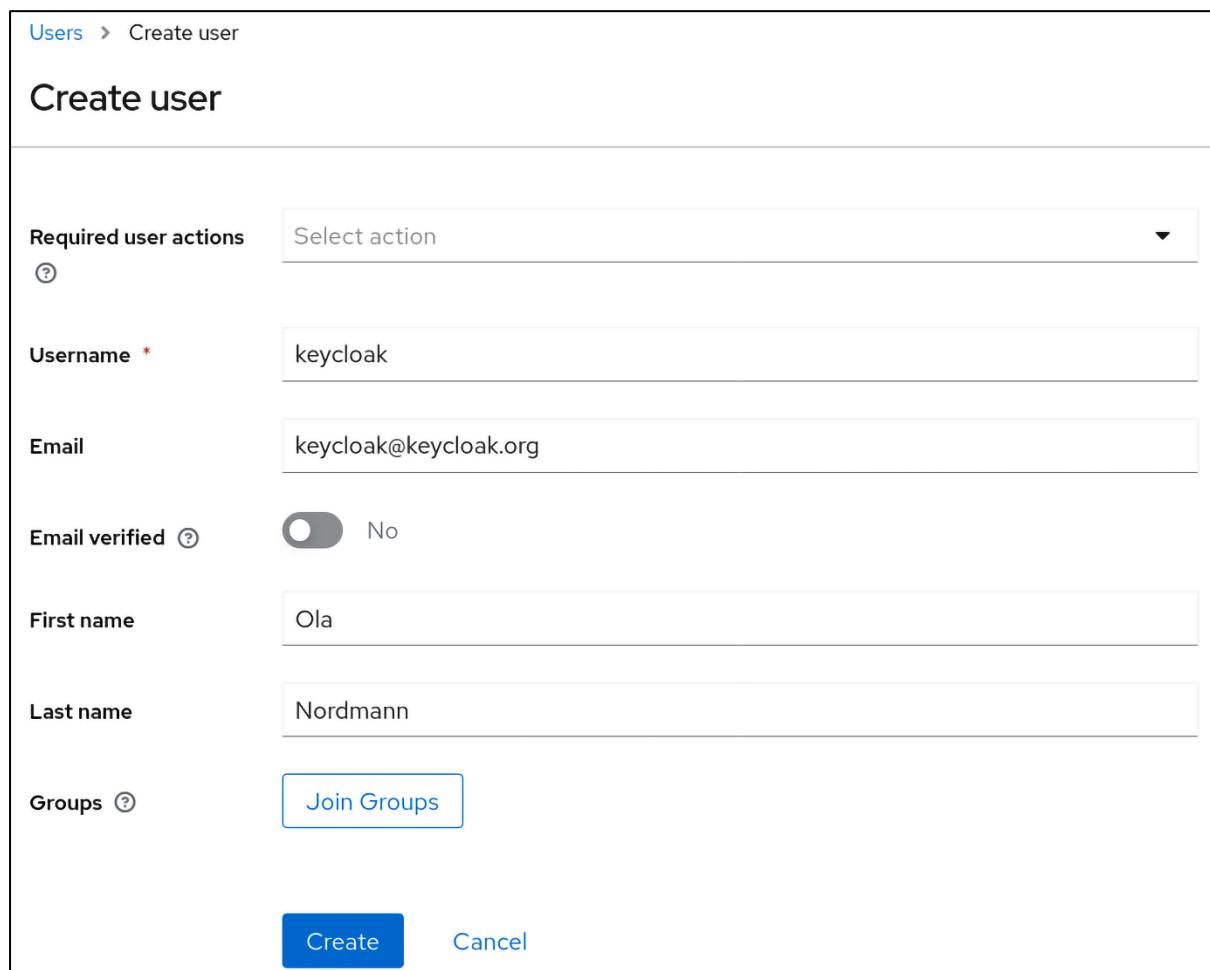


A screenshot of the Keycloak dashboard for the "master realm". The top navigation bar shows the Keycloak logo, a menu icon, the realm name "master realm", and a user profile for "admin". The main content area is titled "master realm" and contains two tabs: "Server info" (which is selected) and "Provider info". The "Server info" tab displays details such as the "Version" (22.0.0), "Product" (Default), and "Memory" usage (Total memory: 455 MB, Free memory: 400 MB, Used memory: 55 MB). The "Profile" section lists various features: Enabled features include ACCOUNT3 (Preview), ADMIN_FINE_GRAINED_AUTHZ (Preview), CLIENT_SECRET_ROTATION (Preview), DECLARATIVE_USER_PROFILE (Preview), DOCKER (Supported), DYNAMIC_SCOPES (Experimental), FIPS (Supported), MAP_STORAGE (Experimental), RECOVERY_CODES (Preview), SCRIPTS (Preview), TOKEN_EXCHANGE (Preview), and UPDATE_EMAIL (Preview).



The screenshot shows the Keycloak Admin UI. On the left, a sidebar menu is open under the 'Master' realm. The menu items include 'Create Realm', 'Realm roles', 'Users', 'Groups', 'Sessions', and 'Events'. A blue button labeled 'Create Realm' is visible. The main content area shows a list of realms, with 'Master' selected. To the right of the realm list, there is a large text area containing various configuration parameters:

```
18e866b879b3637d1eca326151
tories ②
tories ②
JE_GRAINED_AUTHZ  CLIENT_SECRET_ROTATION  DECLARATIVE_USER_PROFILE
DYNAMIC_SCOPES  MAP_STORAGE  OPENSOURCE_INTEGRATION
_CODES  SCRIPTS  TOKEN_EXCHANGE  UPDATE_EMAIL
```



The screenshot shows the 'Create user' form in the Keycloak Admin UI. The top navigation bar indicates the user is creating a new user. The form fields are as follows:

- Required user actions:** A dropdown menu labeled 'Select action'.
- Username ***: keycloak
- Email**: keycloak@keycloak.org
- Email verified**: A toggle switch is set to 'No'.
- First name**: Ola
- Last name**: Nordmann
- Groups**: A button labeled 'Join Groups'.

At the bottom of the form are two buttons: 'Create' (blue) and 'Cancel'.



Sign In

Welcome to Keycloak Account Management

Personal Info

Manage your basic information

[Personal Info](#)

Account Security

Control your password and account access

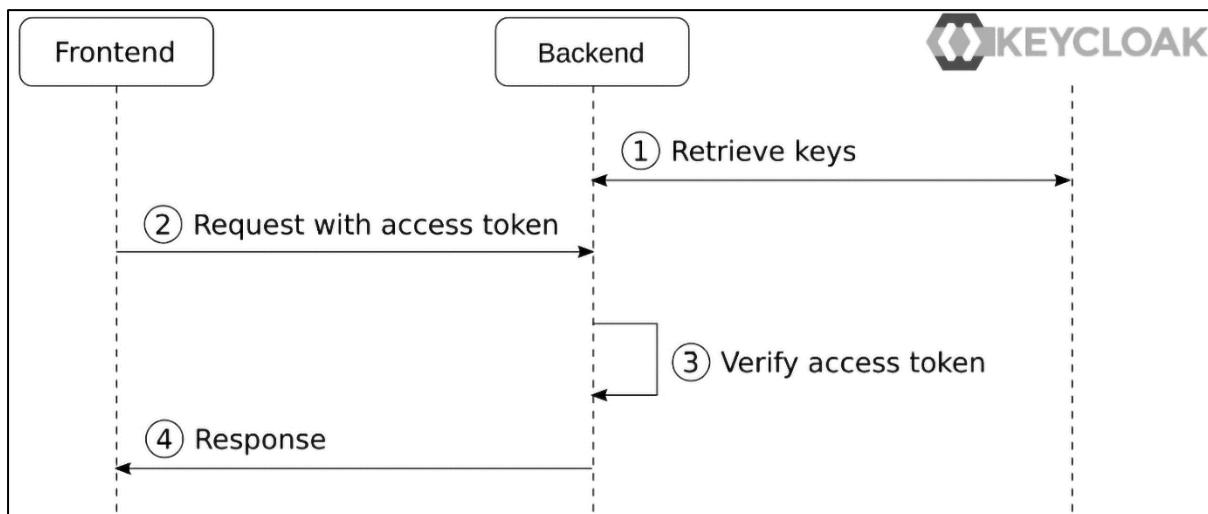
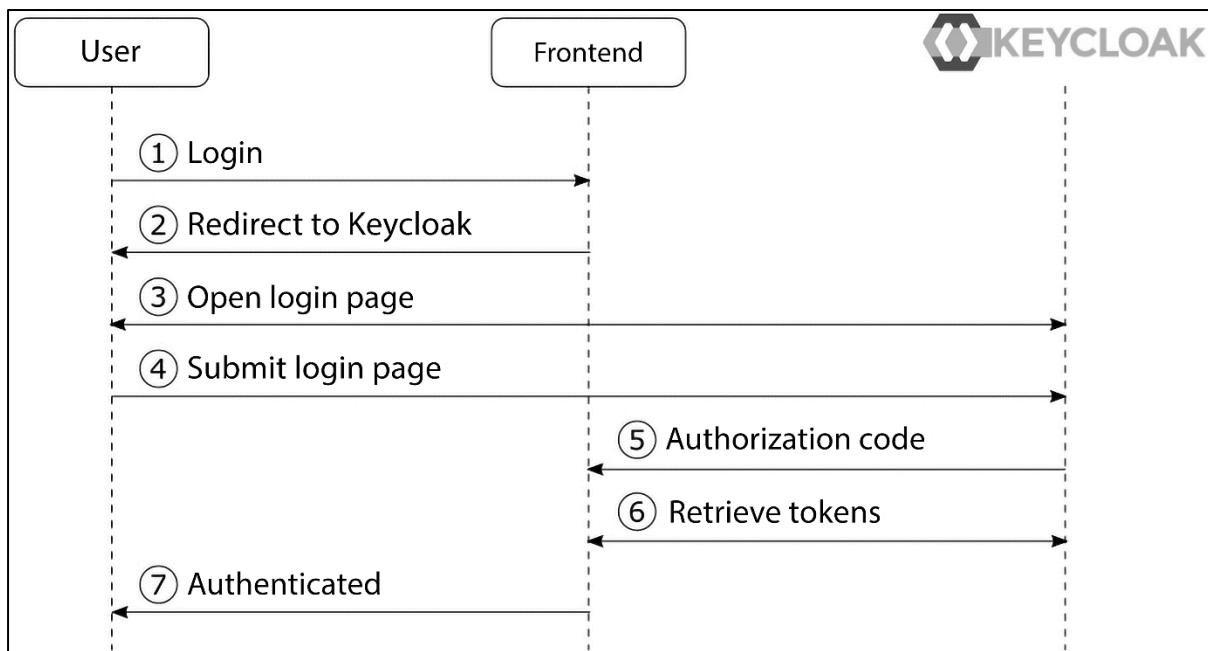
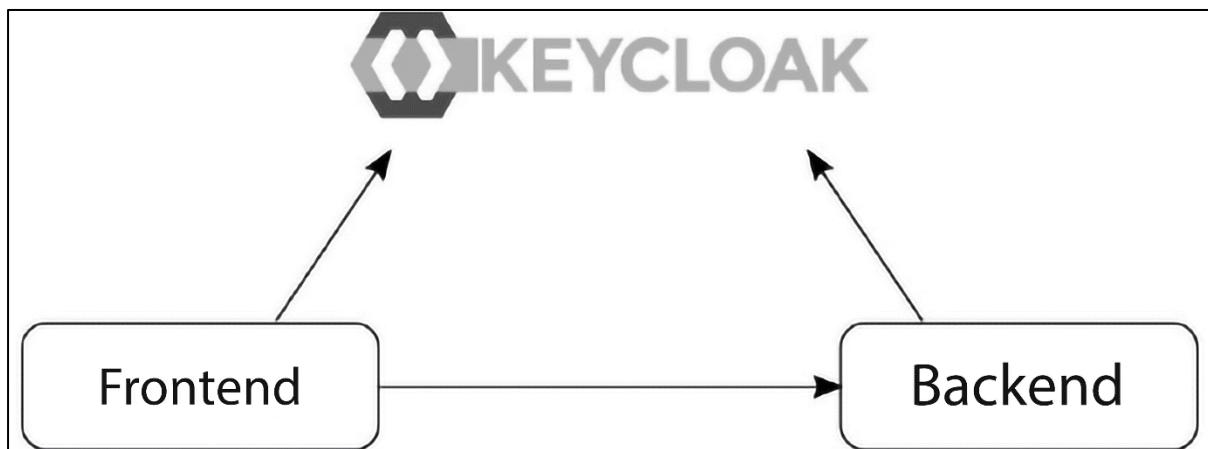
[Signing In](#)
[Device Activity](#)

Applications

Track and manage your app permission to access your account

[Applications](#)

Chapter 2: Securing Your First Application



General Settings

Client ID * myclient

Name

Description

Always display in console Off

Access settings

Root URL

Home URL

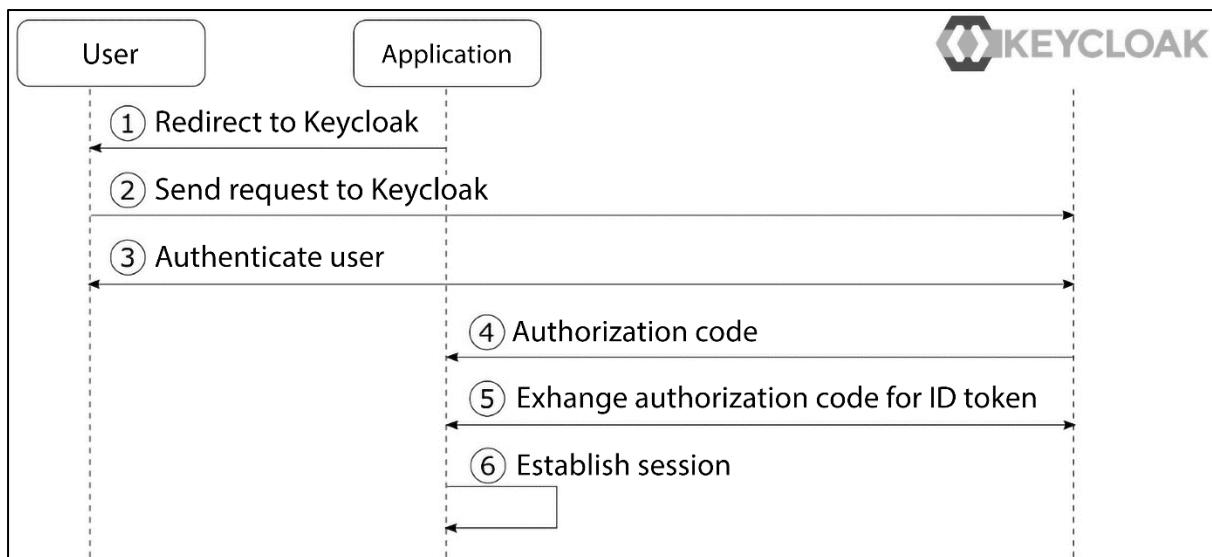
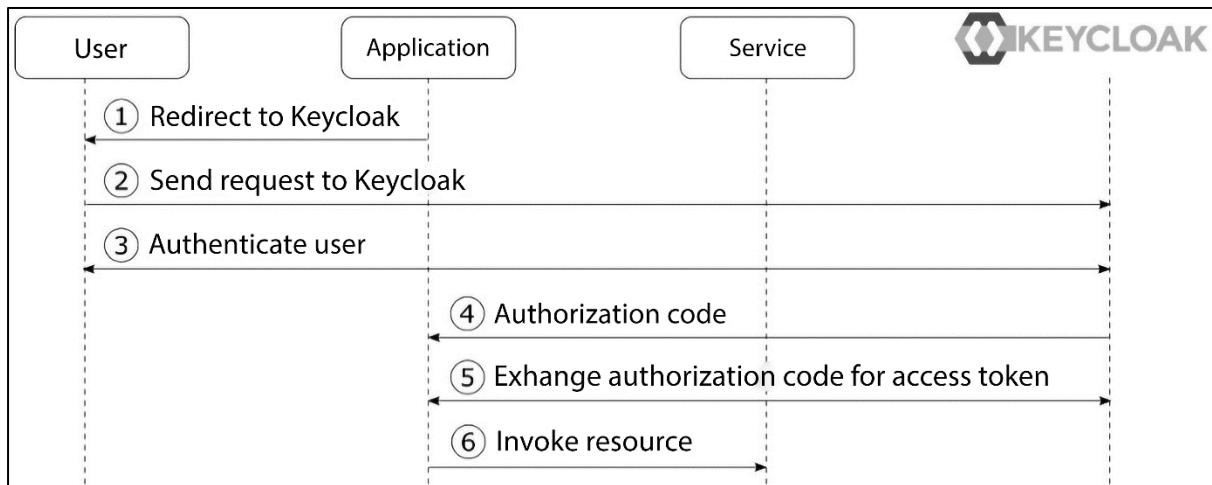
Valid redirect URIs http://localhost:8000/ [+ Add valid redirect URIs](#)

Valid post logout redirect URIs http://localhost:8000/ [+ Add valid post logout redirect URIs](#)

Web origins http://localhost:8000/ [+ Add web origins](#)

Details	Attributes	Credentials	Role mapping	Groups	Consents	Identity provider links	Sessions	
Key	Value							
picture	https://avatars.githubusercontent.com/u/2271511 -							
Type a key	Type a value -							
+ Add an attribute								
Save		Revert						

Chapter 3: Brief Introduction to Standards



Chapter 4: Authenticating Users with OIDC

OpenID Connect Playground

[1 - Discovery](#) [2 - Authentication](#) [3 - Token](#) [4 - Refresh](#) [5 - UserInfo](#) [Reset](#)

Discovery

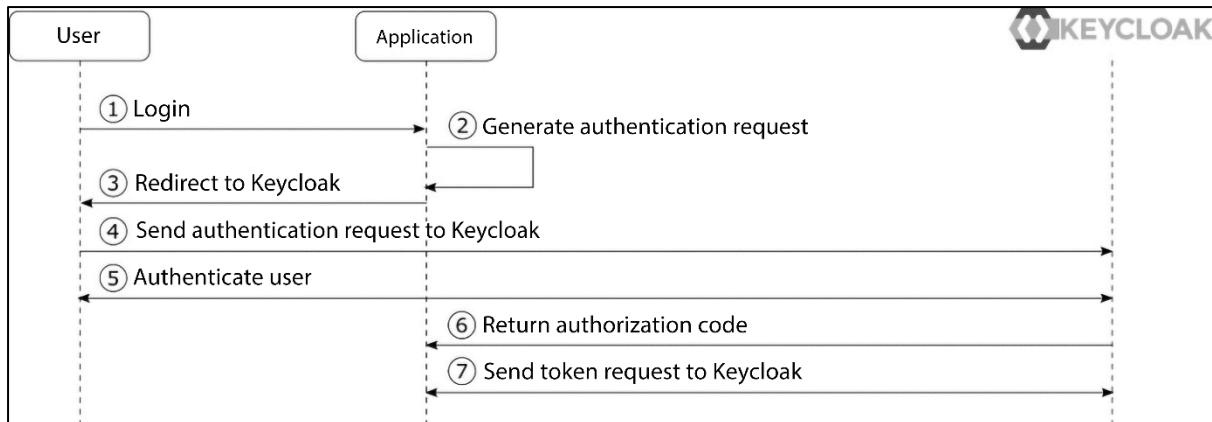
Issuer

[Load OpenID Provider Configuration](#)

OpenID Provider Configuration

OpenID Provider Configuration

```
{
  "issuer": "http://localhost:8080/realms/myrealm",
  "authorization_endpoint": "http://localhost:8080/realms/myrealm/protocol/openid-connect/auth",
  "token_endpoint": "http://localhost:8080/realms/myrealm/protocol/openid-connect/token",
  "introspection_endpoint": "http://localhost:8080/realms/myrealm/protocol/openid-connect/token/introspect",
  "userinfo_endpoint": "http://localhost:8080/realms/myrealm/protocol/openid-connect/userinfo",
  "end_session_endpoint": "http://localhost:8080/realms/myrealm/protocol/openid-connect/logout",
  "frontchannel_logout_session_supported": true,
  "frontchannel_logout_supported": true,
  "jwks_uri": "http://localhost:8080/realms/myrealm/protocol/openid-connect/certs",
  "check_session_iframe": "http://localhost:8080/realms/myrealm/protocol/openid-connect/login-status-iframe.html",
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "refresh_token",
    "password",
    "client_credentials",
    "urn:ietf:params:oauth:grant-type:device_code",
    "urn:openid:params:grant-type:ciba"
  ],
  "acr_values_supported": []
}
```



Authentication Request

```

http://localhost:8080/realm/myrealm/protocol/openid-connect/auth

client_id=oidc-playground
response_type=code
redirect_uri=http://localhost:8000/
scope=openid

```

Token Request

```

http://localhost:8080/realm/myrealm/protocol/openid-connect/token

grant_type=authorization_code
code=14472ec2-69aa-4c79-8b8b-c6e2b3cc1877.3b403853-8afa-4b0a-9f29-84b689768d1a.73b9bd53-1831-485a-940b-986e1cf1add7
client_id=oidc-playground
redirect_uri=http://localhost:8000/

```

Token Response

```
{
  "access_token": "eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX
  "expires_in": 300,
  "refresh_expires_in": 1800,
  "refresh_token": "eyJhbGciOillUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJkMTAzMTcxYillMzA5LTQ1NWYtYWAZiliYjk2NTQxYTAyM
  "token_type": "Bearer",
  "id_token": "eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxz514FGQj1KcVlabXkObV
  "not-before-policy": 0,
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",
  "scope": "openid profile email"
}
```

```

"token_type": "Bearer"
"id_token": "eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabXkObV
"not-before-policy": 0,

```

ID Token

Header

```
{  
  "alg": "RS256",  
  "typ": "JWT",  
  "kid": "MRRaVl0HPdTU8NcJXZsMo-NlsIaFB9JqYZmy4mUeXDM"  
}
```

Payload

```
{  
  "exp": 1665296255,  
  "iat": 1665295955,  
  "auth_time": 1665295938,  
  "jti": "daf6072b-d376-47eb-ba7a-cb203336c6c3",  
  "iss": "http://localhost:8080/realm",  
  "aud": "oidc-playground",  
  "sub": "65588621-32e8-4655-8cf8-86fb8054822e",  
  "typ": "ID",  
  "azp": "oidc-playground",  
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",  
  "at_hash": "pWygili18hq3gIp8-1IwA",  
  "acr": "1",  
  "sid": "3b403853-8afa-4b0a-9f29-84b689768d1a",  
  "email_verified": false,  
  "name": "Stian Thorgersen",  
  "preferred_username": "st",  
  "given_name": "Stian",  
  "family_name": "Thorgersen",  
  "email": "st@localdomain.localhost"  
}
```

Signature

```
X2hfRpAyDb4tFRWbvPGc-i79IZxBoY0YKEK9cmKaDoAy0G-0DA7zVYirbEYhkPv66C6MAUQu4EmXzJ73-aM3xdngEPUA0rYSgg-PHkiYug3IiJgDyc-
```

Refresh Request

```
http://localhost:8080/realm/protocol/openid-connect/token  
  
grant_type=refresh_token  
refresh_token=eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJkMTAzMTcxYillMzA5LTQ1NWYtYWJZiliYjk2NTQxYTAyMjkifQ  
client_id=oidc-playground  
scope=openid
```

Refresh Response

```
{  
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSVIFGQj1KcVlabX",  
  "expires_in": 300,  
  "refresh_expires_in": 1800,  
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJkMTAzMTcxYillMzA5LTQ1NWYtYWJZiliYjk2NTQxYTAyM",  
  "token_type": "Bearer",  
  "id_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwiSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabXkObV",  
  "not-before-policy": 0,  
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",  
  "scope": "openid profile email"  
}
```

UserInfo Request

```
http://localhost:8080/realm/myrealm/protocol/openid-connect/userinfo
```

```
Authorization: Bearer eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJNU1JhVmwwSFBkVFU4TmNKW
```

UserInfo Response

```
{
  "sub": "65588621-32e8-4655-8cf8-86fb8054822e",
  "email_verified": true,
  "name": "Stian Thorgersen",
  "preferred_username": "st",
  "given_name": "Stian",
  "family_name": "Thorgersen",
  "email": "st@localdomain.localhost",
  "myattribute": "myvalue"
}
```

Chapter 5: Authorizing Access with OAuth 2.0

OAuth 2.0 Playground

[1 - Discovery](#) [2 - Authorization](#) [3 - Invoke Service](#) [Reset](#)

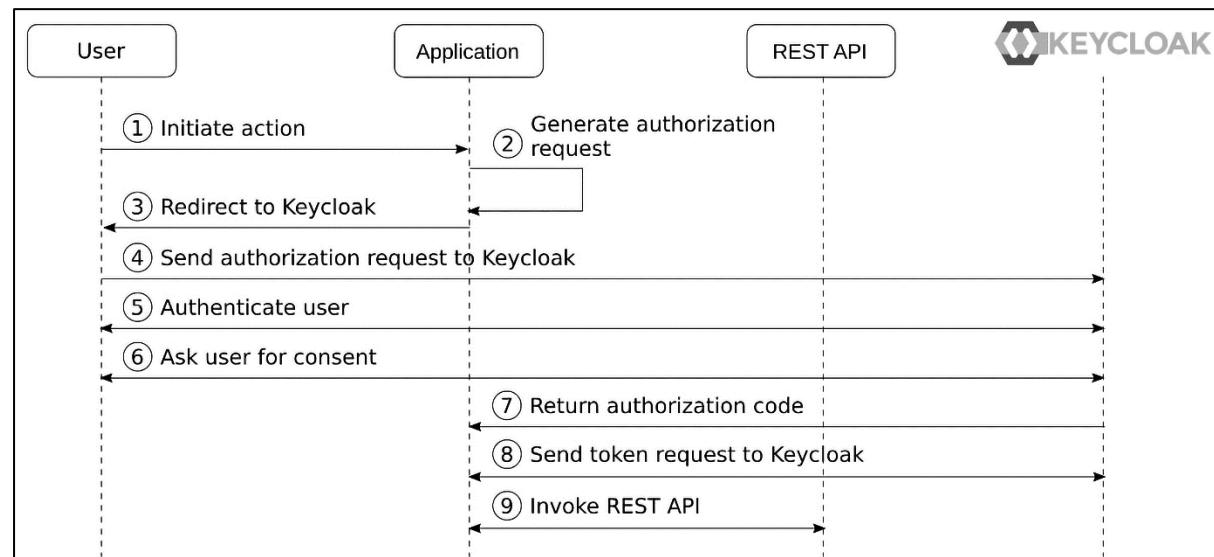
Discovery

Issuer

<http://localhost:8080/realm/myrealm>

[Load OAuth 2.0 Provider Configuration](#)

OAuth 2.0 Provider Configuration



Access Token

Header

```
{  
  "alg": "RS256",  
  "typ": "JWT",  
  "kid": "JI0_xxUiSi7oUkx0xLQe8xsdRTnKOirURnBuik6EyyQ"  
}
```

Payload

```
{  
  "exp": 1667145073,  
  "iat": 1667144773,  
  "auth_time": 1667144773,  
  "jti": "dc6caecb-7f4e-49c6-a9ed-bf2fd5af0db0",  
  "iss": "http://localhost:8080/realms/myrealm",  
  "aud": "account",  
  "sub": "f89a8358-de60-4238-883b-9143af28c56b",  
  "typ": "Bearer",  
  "azp": "oauth-playground",  
  "session_state": "567f4493-18dc-4f85-853c-4d3490f67f8f",  
  "acr": "1",  
  "allowed-origins": [  
    "http://localhost:8000"  
,  
  "realm_access": {  
    "roles": [  
      "default-roles-myrealm",  
      "offline_access",  
      "uma_authorization",  
      "myrole"  
    ]  
  },  
  "resource_access": {  
    "account": {  
      "roles": [  
        "manage-account",  
        "manage-account-links",  
        "view-profile"  
      ]  
    }  
  },  
  "scope": "profile email",  
  "sid": "567f4493-18dc-4f85-853c-4d3490f67f8f",  
  "email_verified": true,  
  "name": "Stian Thorgersen",  
  "preferred_username": "st",  
  "given_name": "Stian",  
  "family_name": "Thorgersen",  
  "email": "st@localhost.localdom"  
}
```

OAuth 2.0 Playground

1 - Discovery

2 - Authorization

3 - Invoke Service

Reset

Invoke Service

Invoke

Response

Secret message!

Login settings

Login theme [?](#)

Choose...

Consent required [?](#)



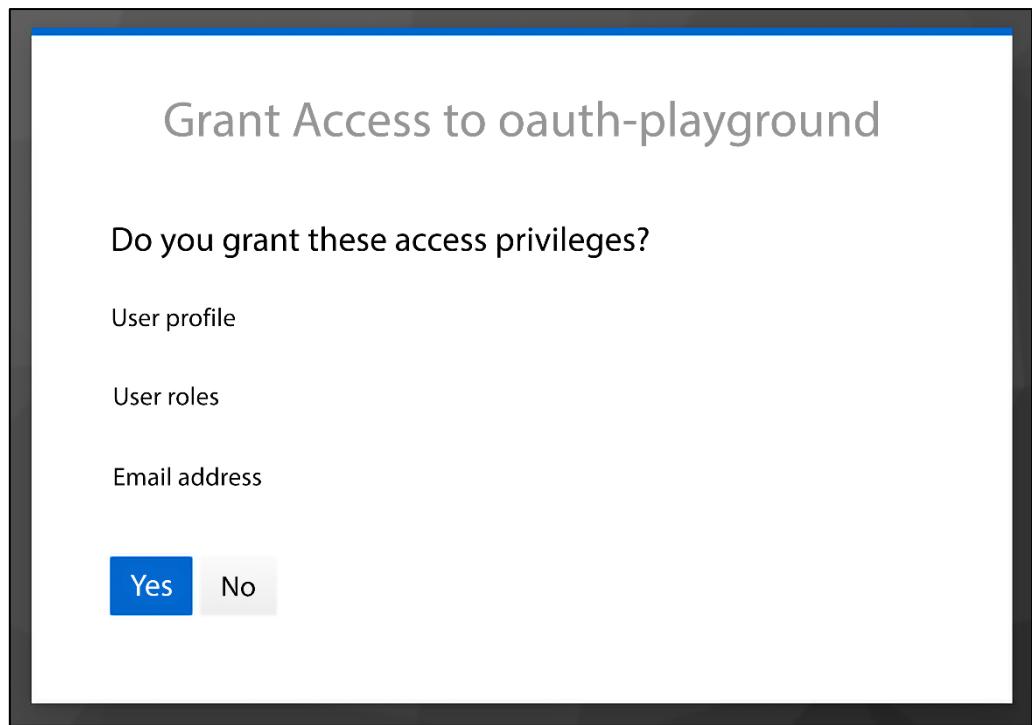
On

Display client on
screen [?](#)



Off

Client consent screen
text [?](#)



Create client scope

Name <small>?</small>	albums
Description <small>?</small>	
Type <small>?</small>	None
Protocol <small>?</small>	OpenID Connect
Display on consent screen <small>?</small>	<input checked="" type="checkbox"/> On
Consent screen text <small>?</small>	View your photo albums
Include in token scope <small>?</small>	<input checked="" type="checkbox"/> On
Display Order <small>?</small>	

[Save](#) [Cancel](#)

Grant Access to oauth-playground

Do you grant these access privileges?

View your photo albums

Yes

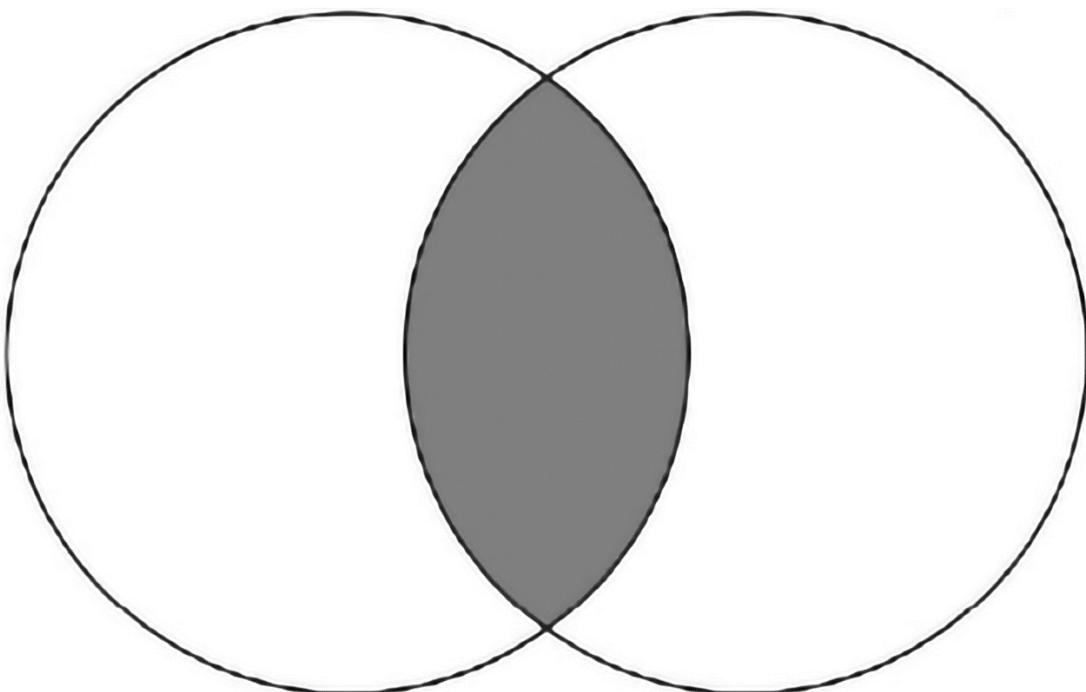
No

```
1 {
2   "realm": "myrealm",
3   "bearer-only": true,
4   "auth-server-url": "${env.KC_URL:http://localhost:8080/auth}",
5   "resource": "oauth-backend",
6   "verify-token-audience": true
7 }
```

User
Roles

Token
Roles

Client
Scope



Grant Access to oauth-playground

Do you grant these access privileges?

View photo albums

Yes

No

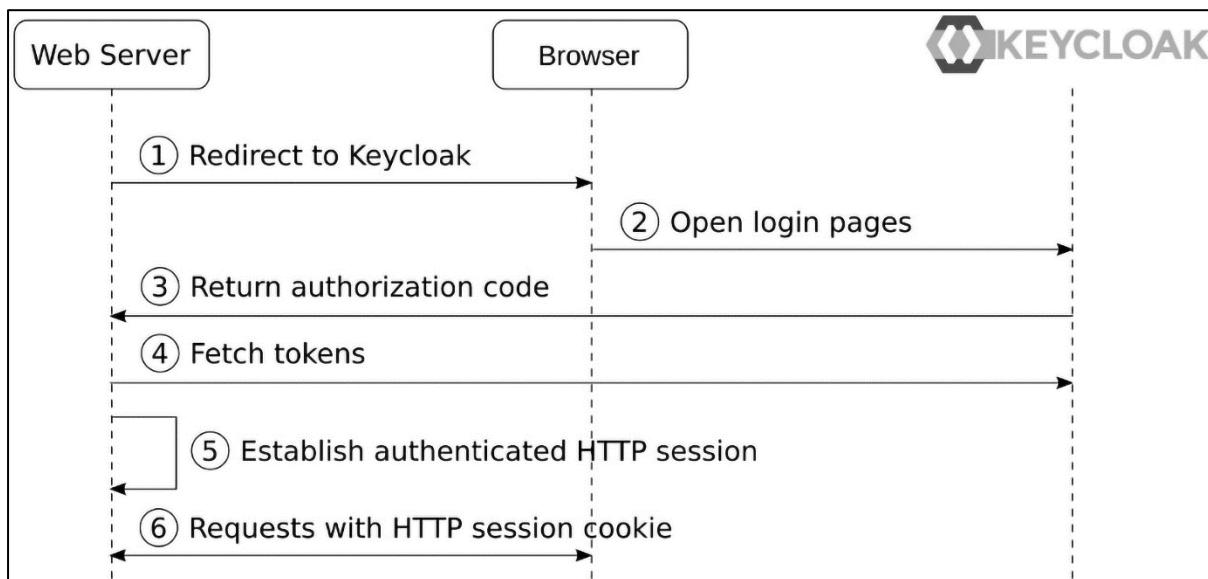
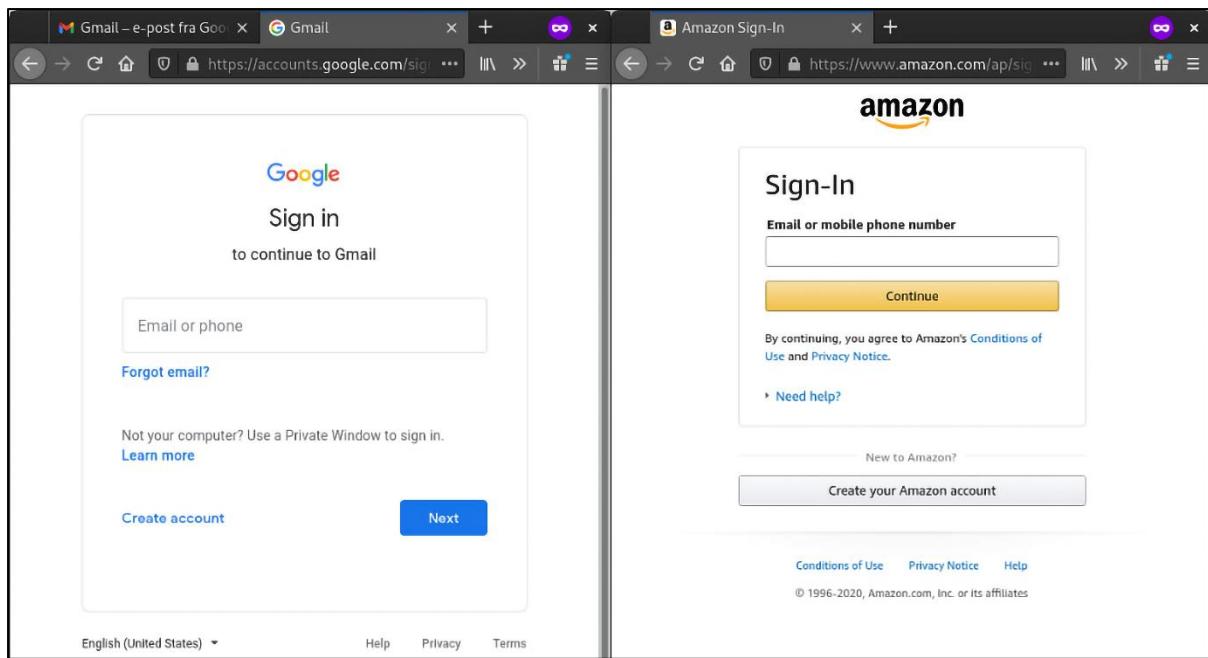
```
{  
    "exp": 1667147808,  
    "iat": 1667147508,  
    "auth_time": 1667144773,  
    "jti": "681209f3-0b87-4ef2-b68d-21d46f615fc5",  
    "iss": "http://localhost:8080/realm/myrealm",  
    "aud": "oauth-backend",  
    "sub": "f89a8358-de60-4238-883b-9143af28c56b",  
    "typ": "Bearer",  
    "azp": "oauth-playground",  
    "session_state": "567f4493-18dc-4f85-853c-4d3490f67f8f",  
    "name": "Stian Thorgersen",  
    "given_name": "Stian",  
    "family_name": "Thorgersen",  
    "preferred_username": "st",  
    "email": "st@localhost.localdom",  
    "email_verified": true,  
    "acr": "0",  
    "allowed_origins": [  
        "http://localhost:8000"  
    ],  
    "realm_access": {  
        "roles": [  
            "myrole"  
        ]  
    },  
    "scope": "myrole albums:create profile email albums:view",  
    "sid": "567f4493-18dc-4f85-853c-4d3490f67f8f",  
    "client_id": "oauth-playground",  
    "username": "st",  
    "active": true  
}
```

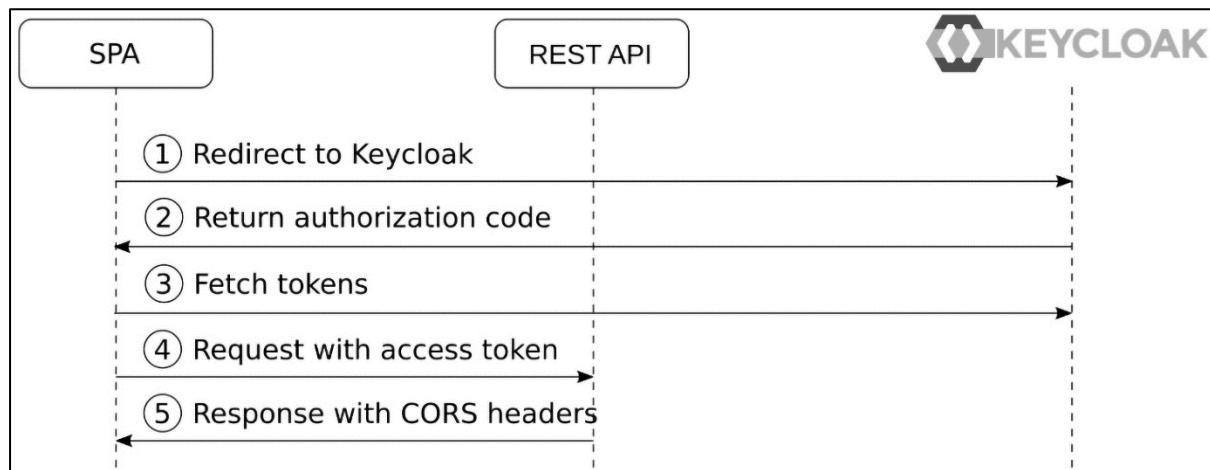
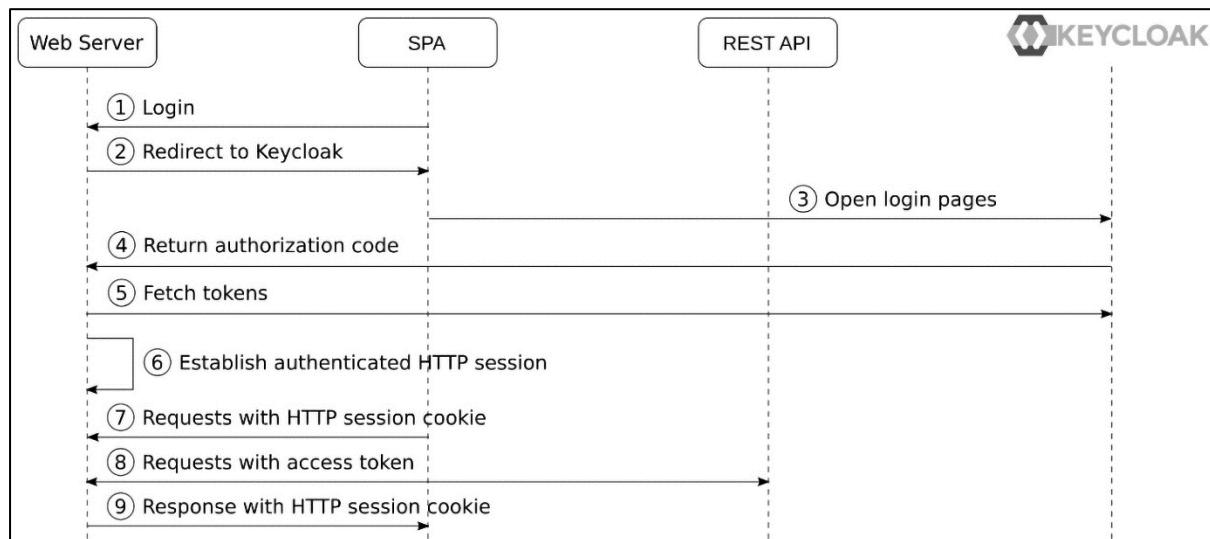
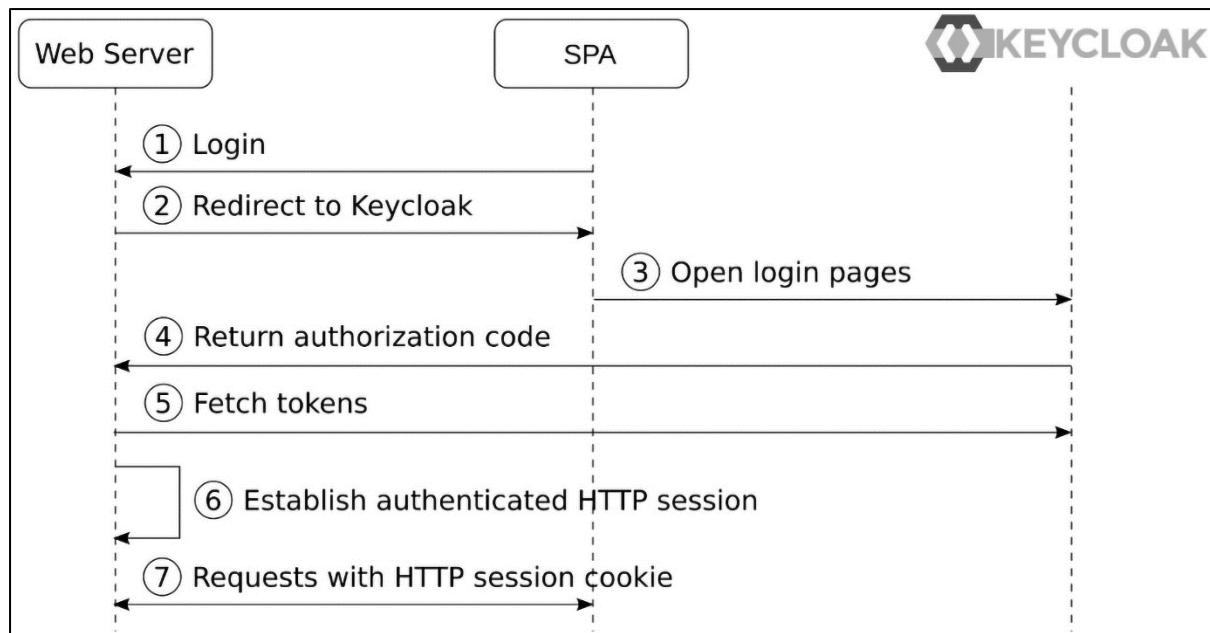
Chapter 6: Securing Different Application Types

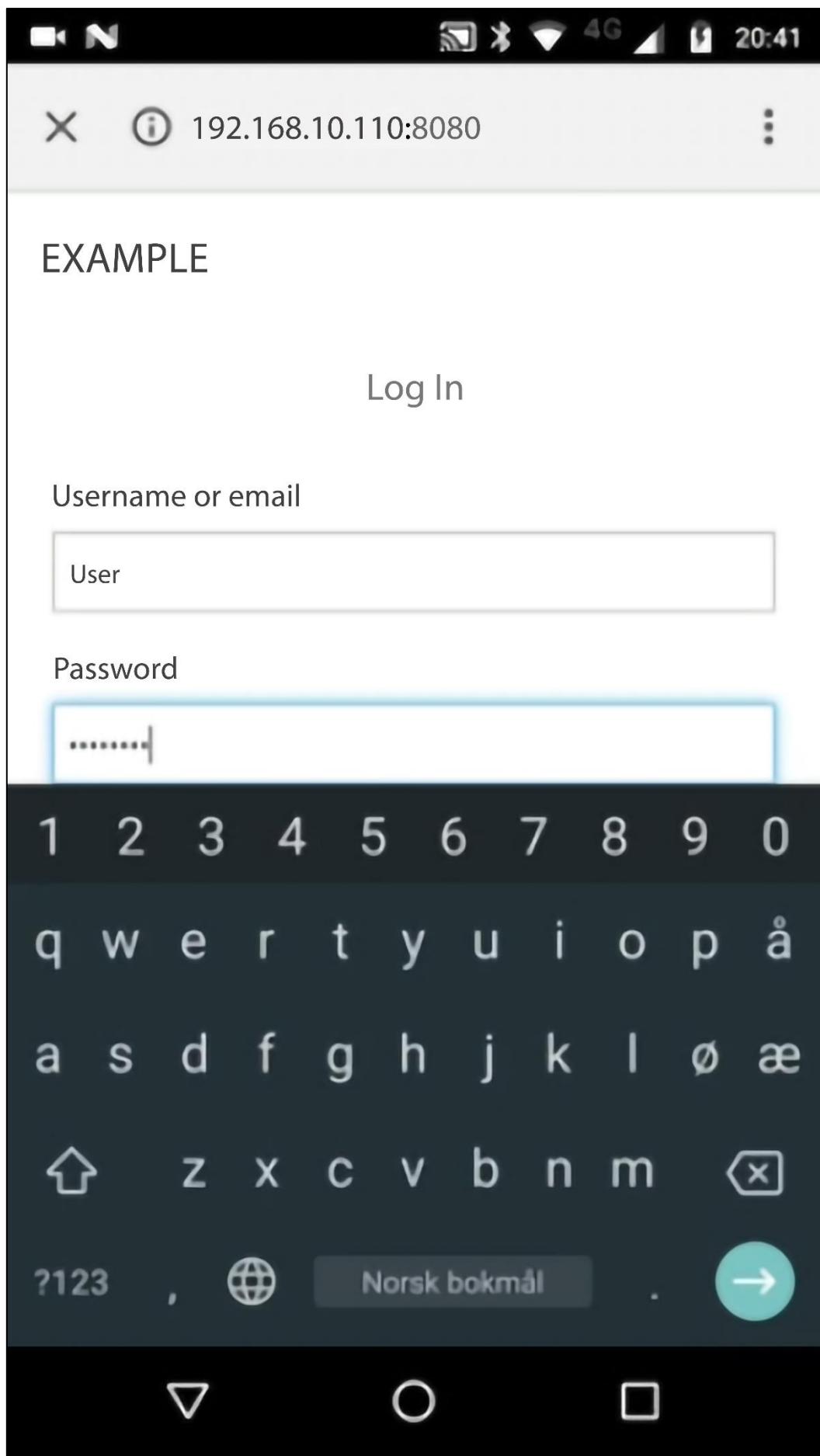
This screenshot shows the 'Clients' configuration page under the 'Manage' section. The left sidebar includes options like Master, Manage, Clients (which is selected), Client scopes, Realm roles, and Users. The main content area is titled 'Login settings' and contains three configuration items: 'Login theme' (with a dropdown menu labeled 'Choose...'), 'Consent required' (with a toggle switch set to 'Off'), and 'Display client on screen' (with a toggle switch set to 'Off'). To the right, there are three vertical tabs: 'Jump to section', 'General Settings', 'Access settings', and 'Capability config'. The 'Access settings' tab is currently active.

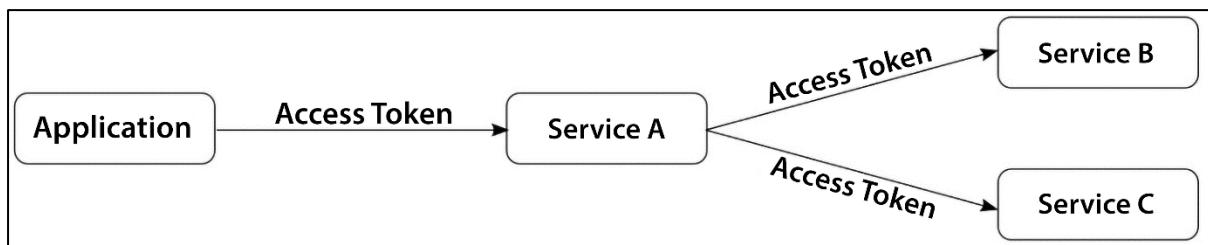
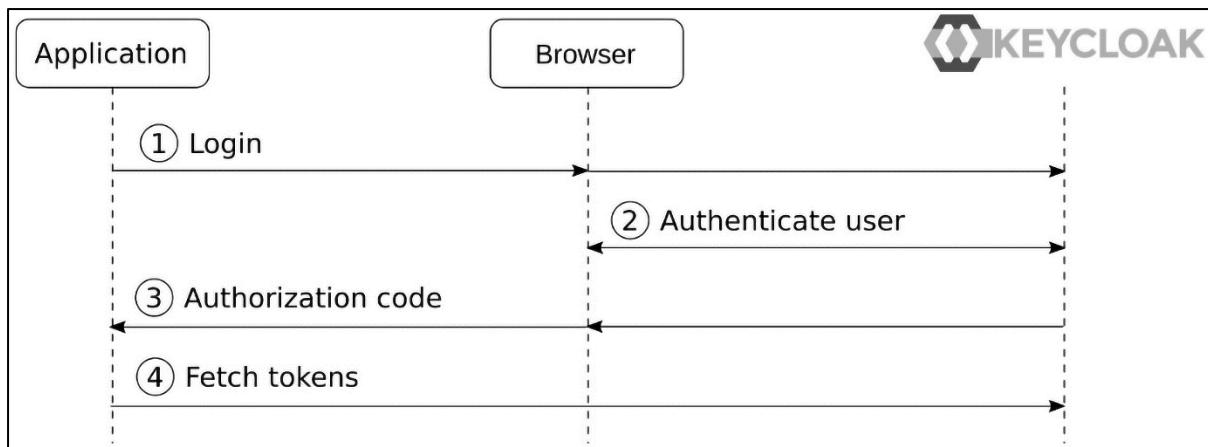
This screenshot shows the same 'Clients' configuration page as the previous one, but with a visible change: the 'Consent required' toggle switch is now set to 'On'. All other settings ('Login theme' and 'Display client on screen') remain at 'Off'. The right-hand tabs are identical to the first screenshot.

This screenshot displays a consent dialog box. At the top, it says 'MY REALM'. Below that, the title 'Grant Access to External Application' is centered. A question follows: 'Do you grant these access privileges?'. Underneath, the 'User profile' privilege is listed. At the bottom right, there are two buttons: a white 'No' button and a blue 'Yes' button.









Myrealm

Capability config

Client authentication On

Authorization Off

Authentication flow

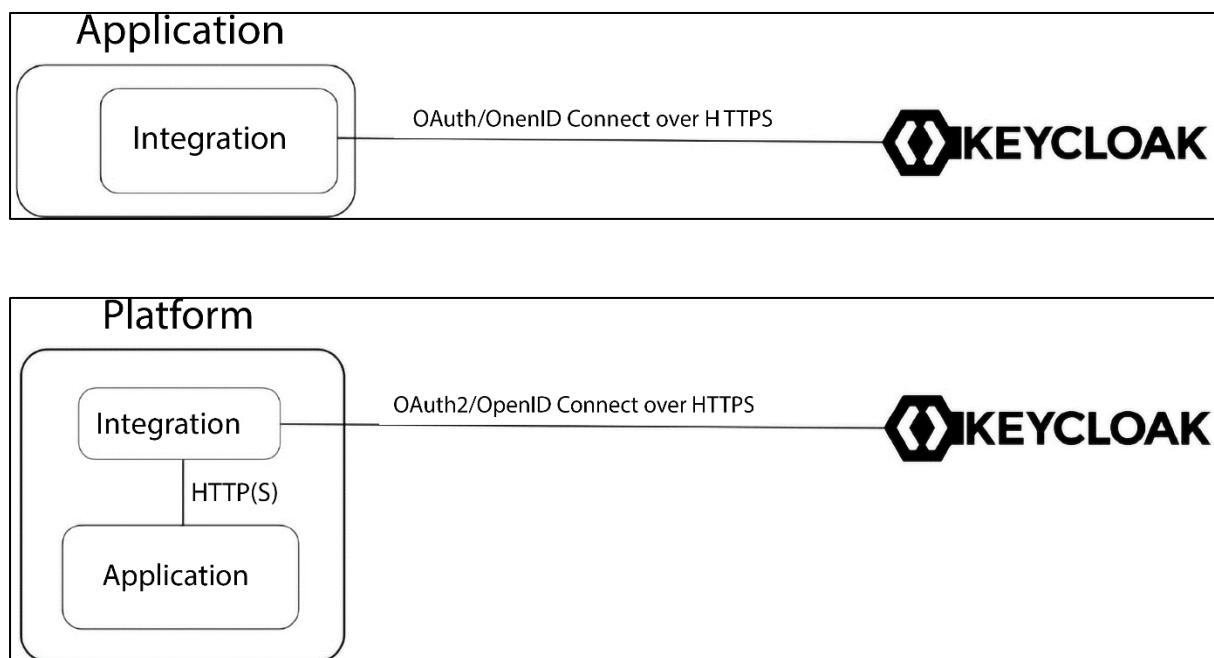
- Standard flow
- Direct access grants
- Implicit flow
- Service accounts roles
- OAuth 2.0 Device Authorization Grant
- OIDC CIBA Grant

Jump to section

- General Settings
- Access settings
- Capability config
- Login settings
- Logout settings

The screenshot shows the 'Capability config' settings for a client in the Keycloak 'Clients' section. The 'Client authentication' toggle is set to 'On'. The 'Authorization' toggle is set to 'Off'. Under 'Authentication flow', the 'Service accounts roles' option is selected. A sidebar on the right provides links to other configuration sections.

Chapter 7: Integrating Applications with Keycloak



Chapter 8: Authorization Strategies

myclient (OpenID Connect)

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

Enabled Action

Settings Roles Client scopes Sessions Advanced

Setup Evaluate

Name Search by name Add client scope Change type to 1-10

Assigned client s... Assigned type Description

myclient-dedicated none Dedicated scope and mappers for this client

acr Default OpenID Connect scope for add acr (authentication context class reference) to the token

address Optional OpenID Connect built-in scope: address

Clients > Client details > Dedicated scopes > Mapper details

Action

Group Membership

d71819de-fa5a-43c1-b501-9750ddce6c7c

Mapper type	Group Membership
Name *	groups
Token Claim Name	groups
Full group path	On
Add to ID token	On
Add to access token	On
Add to userinfo	On

Save Cancel

Groups

A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-parent organization. [Learn more](#) 



No groups in this realm

You haven't created any groups in this realm. Create a group to get started.

[Create group](#)

Create a group



Name *

Project Management Office

[Create](#)

[Cancel](#)

alice

Enabled Action ▾

Details Attributes Credentials Role mapping Groups Consents

No groups

You haven't added this user to any groups. Join a group to get started.

Join Group

This screenshot shows the 'Groups' tab of a user profile for 'alice'. At the top, there's a toggle switch labeled 'Enabled' and a dropdown menu labeled 'Action'. Below the tabs, a large plus sign icon indicates that no groups are assigned. A message encourages the user to 'Join a group to get started.' A blue 'Join Group' button is located at the bottom of the section.

Join groups for user alice x

Search for groups → 1-1

Project Management Office

1-1 ▾

Join

This screenshot shows a modal dialog titled 'Join groups for user alice'. It contains a search bar with the placeholder 'Search for groups' and a result count '1-1'. A single group, 'Project Management Office', is listed with a checked checkbox. Below the list is a pagination control showing '1-1' with a dropdown arrow. At the bottom is a blue 'Join' button.

myclient OpenID Connect Enabled Action ▾

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

Settings Roles Client scopes Sessions Advanced

Setup Evaluate

This page allows you to see all protocol mappers and role scope mappings

Scope parameter ?

openid x Select scope parameters

User ?

alice x

Setup Evaluate

This page allows you to see all protocol mappers and role scope mappings

Scope parameter ?

openid x Select scope parameters

User ?

alice x

SESSION_STATE : 342405b3-1dec-47c6-839f-d9208c9e1395 ,
"acr": "1",
"sid": "342405b3-1dec-47c6-839f-d9208c9e1395",
"email_verified": false,
"groups": [
"/Project Management Office"
,
"preferred_username": "alice",
"given_name": "",
"family_name": ""
}

Effective protocol mappers ?

Effective role scope mappings ?

Generated access token ?

Generated ID token ?

Generated user info ?

Chapter 9: Configuring Keycloak for Production

master Enabled Action ▾

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#) ↗

General Login Email Themes Keys Events Localization Security defenses ➔

Realm ID *	master
Display name	Keycloak
HTML Display name	<div class="kc-logo-text">Keycloak</div>
Frontend URL ⓘ	
Require SSL ⓘ	External requests

Inspector Console Debugger Network Style Editor Performance

Filter URLs

S...	Me	Domain	File	Initiator	T...	Transf...	S...	Headers	Cookies
200	GET	🔒 my...	step2.html	step1....	h...	1.57 KB	1...		Filter Cookies
302	GET	🔒 my...	auth?client_id=security-a	keyclo...	h...	10.72 KB	7...		Response Cookies
200	GET	🔒 my...	/auth/admin/master/cons	docu...	h...	7.62 KB	7...		Request Cookies
200	GET	🔒 my...	jquery.min.js	script	js	cached	8...		AUTH_SESSION_ID: 748
200	GET	🔒 my...	select2.js	script	js	cached	1...		AUTH_SESSION_ID: LEG
200	GET	🔒 my...	angular.min.js	script	js	cached	1...		KC_ROUTE: 'kcl'

```
issuer: "https://mykeycloak/realm/master"
authorization_endpoint: "https://mykeycloak/realm/master/protocol/openid-connect/auth"
token_endpoint: "https://mykeycloak/realm/master/protocol/openid-connect/token"
introspection_endpoint: "https://mykeycloak/realm/master/protocol/openid-connect/token/introspect"
userinfo_endpoint: "https://mykeycloak/realm/master/protocol/openid-connect/userinfo"
end_session_endpoint: "https://mykeycloak/realm/master/protocol/openid-connect/logout"
frontchannel_logout_session_supported: true
frontchannel_logout_supported: true
jwks_uri: "https://mykeycloak/realm/master/protocol/openid-connect/certs"
check_session_iframe: "https://mykeycloak/realm/master/protocol/openid-connect/login-status-iframe.html"
```

Chapter 10: Managing Users

Users > Create user

Create user

Required user actions Select action

Username * alice

Email

Email verified No

First name

Last name

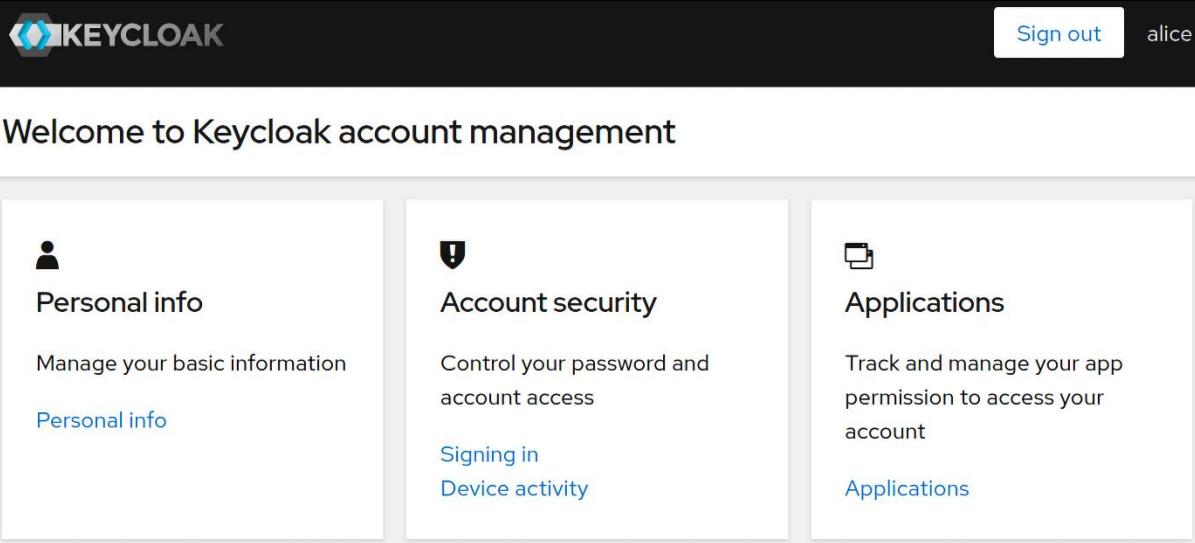
Groups

Set password for alice

>Password *

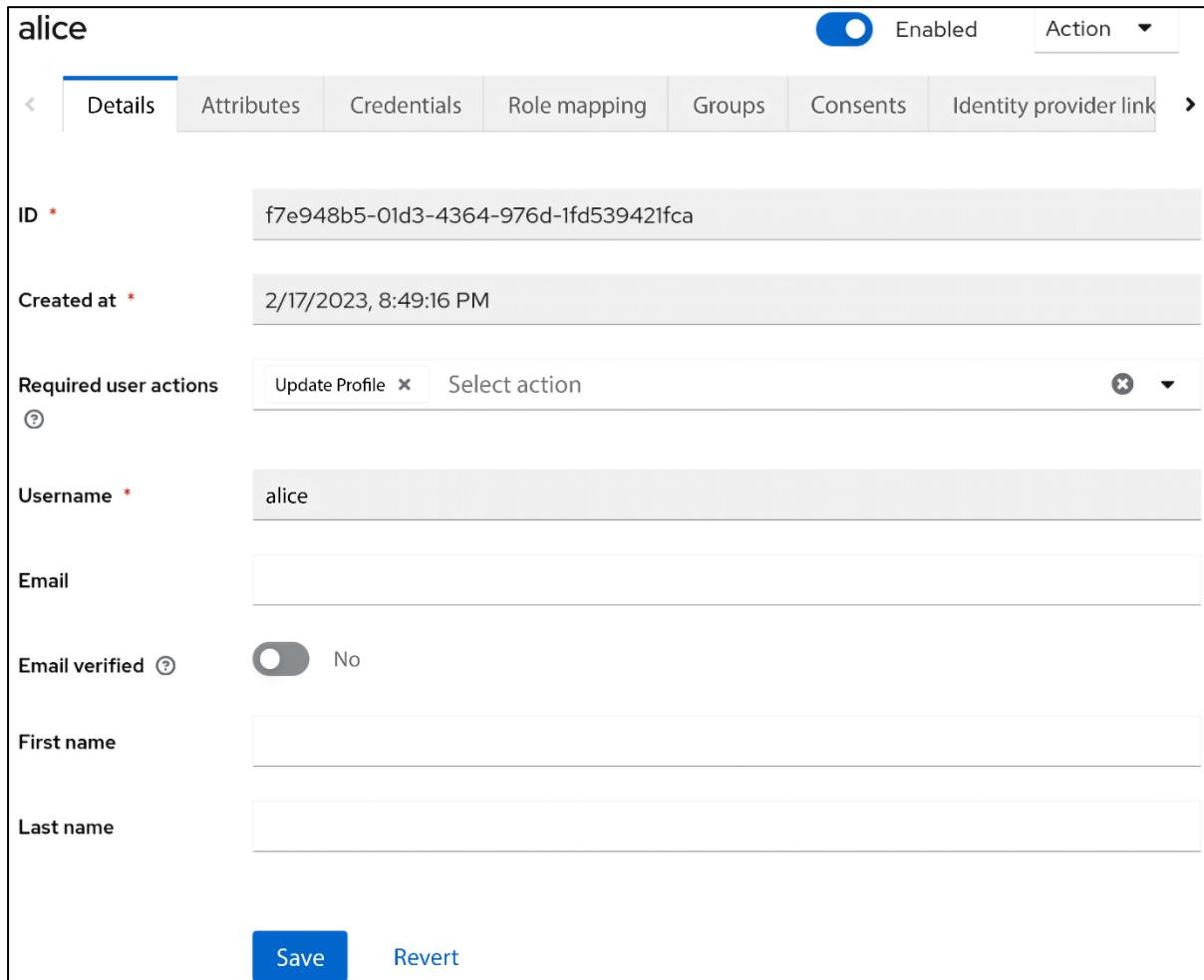
Password confirmation *

Temporary Off



The screenshot shows the Keycloak account management interface. At the top right, there are "Sign out" and "alice" buttons. Below the header, a main title "Welcome to Keycloak account management" is displayed. The interface is divided into three main sections: "Personal info", "Account security", and "Applications".

- Personal info:** Manage your basic information. Includes a "Personal info" link.
- Account security:** Control your password and account access. Includes "Signing in" and "Device activity" links.
- Applications:** Track and manage your app permission to access your account. Includes an "Applications" link.



The screenshot shows the "Details" tab of a user profile for "alice". The profile is enabled. The user has the following details:

ID *	f7e948b5-01d3-4364-976d-1fd539421fca
Created at *	2/17/2023, 8:49:16 PM
Required user actions	Update Profile Select action
Username *	alice
Email	(empty)
Email verified	<input checked="" type="checkbox"/> No
First name	(empty)
Last name	(empty)

At the bottom, there are "Save" and "Revert" buttons.

Update Account Information



You need to update your user profile to activate your account.

•

Email

First name

Last name

Submit

Sign in to your account

Username or email

Password

Sign In

New user? [Register](#)

User federation

User federation provides access to external databases and directories, such as LDAP and Active Directory. [Learn more](#)

To get started, select a provider from the list below.

Add providers



Add Kerberos providers



Add Ldap providers

Identity providers

Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. [Learn more](#)

To get started, select a provider from the list below.

User-defined:



Keycloak OpenID Connect



OpenID Connect v1.0



SAML v2.0

Social:



BitBucket



Facebook



GitHub



GitLab



Google



Instagram



LinkedIn



Microsoft



Openshift v3

Sign in to your account

Username or email

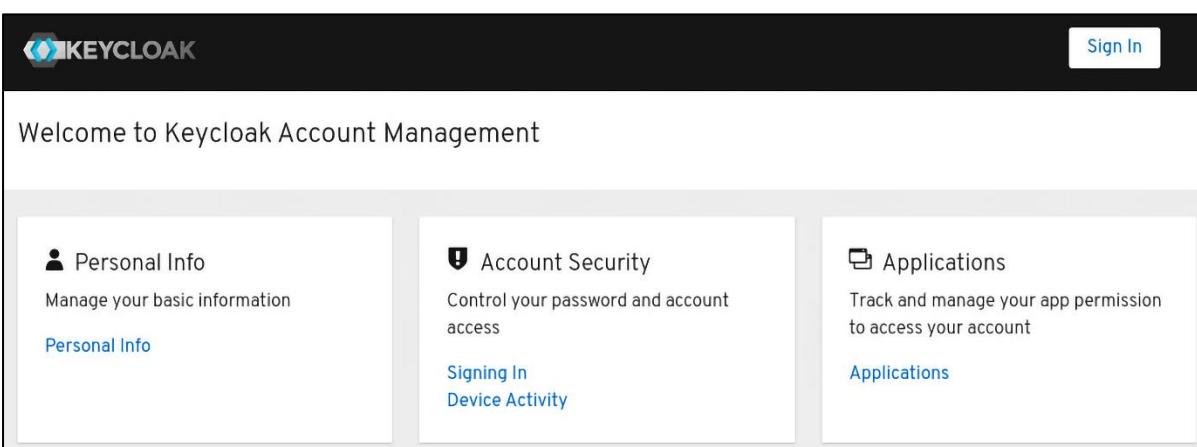
Password

Sign In

Or sign in with

My Third-Party Provider

New user? [Register](#)



The screenshot shows the Keycloak Account Management interface. At the top, there's a dark header bar with the Keycloak logo on the left and a "Sign In" button on the right. Below the header, a welcome message reads "Welcome to Keycloak Account Management". The main area is divided into three cards:

- Personal Info**: Manage your basic information. Includes a "Personal Info" link.
- Account Security**: Control your password and account access. Includes "Signing In" and "Device Activity" links.
- Applications**: Track and manage your app permission to access your account. Includes an "Applications" link.



Personal Info

Account Security >

Applications

Personal Info

Manage this basic information: your first name, last name and email

Username * alice

Email *

First name *

Last name *

Save

Cancel

Chapter 11: Authenticating Users

Authentication		
Authentication is the area where you can configure and manage different credential types. Learn more		
Flows	Required actions	Policies
<input type="text"/> Search for flow	→	Create flow
1-8	◀ ▶	
Flow name	Used by	Description
browser <small>Built-in</small>	<input checked="" type="checkbox"/> Browser flow	browser based authentication
clients <small>Built-in</small>	<input checked="" type="checkbox"/> Client authentication flow	Base authentication for clients
direct grant <small>Built-in</small>	<input checked="" type="checkbox"/> Direct grant flow	OpenID Connect Resource Owner Grant
docker auth <small>Built-in</small>	<input checked="" type="checkbox"/> Docker authentication flow	Used by Docker clients to authenticate against the IDP
registration <small>Built-in</small>	<input checked="" type="checkbox"/> Registration flow	registration flow
reset credentials <small>Built-in</small>	<input checked="" type="checkbox"/> Reset credentials flow	Reset credentials for a user if they forgot their password or something
first broker login <small>Built-in</small>	Not in use	Actions taken after first broker login with identity provider account, which is not yet linked to any Keycloak account
http challenge <small>Built-in</small>	Not in use	An authentication flow based on challenge-response HTTP Authentication Schemes

Duplicate flow

×

Name ?

Description ?

[Duplicate](#) [Cancel](#)

Steps	Requirement
Cookie	Alternative
Kerberos	Disabled
Identity Provider Redirector	Alternative
My Browser forms Username, password, otp and other auth forms.	Alternative
My Browser Browser - Conditional OTP Flow to determine if the OTP is required for the authentication	Conditional
Condition - user configured	Required
OTP Form	Required

Add step to My Browser forms

X

username

X

→

1 - 6

HTTP Basic Authentication

Validates username and password from Authorization HTTP header

Username Form

Selects a user from his username.

Username Password Form

Add

Cancel

My Browser forms
Username, password, otp and other auth forms.

Alternative

Step	Type	Status	Action
Username Form	Required		
Password Form	Required		
My Browser Browser - Conditional OTP	Conditional		
Condition - user configured	Required		
OTP Form	Required		

Bind flow

X

Choose binding type

Browser flow

▼

Save

Cancel

alice



Enabled

Action ▾

◀ Credentials Role mapping Groups Consents Identity provider links Sessions



Type

User label

Data



Password

My password



Show data

Reset password



Authentication

Authentication is the area where you can configure and manage different credential types. [Learn more](#) ↗

Flows

Required actions

Policies

Password policy

OTP Policy

Webauthn Policy

Webauthn Passwordless Policy

CIBA Policy



No password policies

You haven't added any password policies to this realm. Add a policy to get started.

Add policy

▼

alice

Enabled Action ▾

Details Attributes Credentials Role mapping Groups Consents Identity pro ▶

ID * e550c67f-66d7-410f-990b-8a5ff14a91eb

Created at * 4/3/2023, 8:29:32 AM

Required user actions Update Password X Select action X ▾

Username * alice

Email

Email verified ⓘ No

First name

Last name

Save Revert

KEYCLOAK Sign Out alice

Personal Info

Account Security ▾

Signing In

Device Activity

Applications

Signing In

Configure ways to sign in.

Basic Authentication

Password

Log in by entering your password.

My Password Created: February 25, 2021, 5:03 AM Update

myrealm

Enabled Action ▾

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

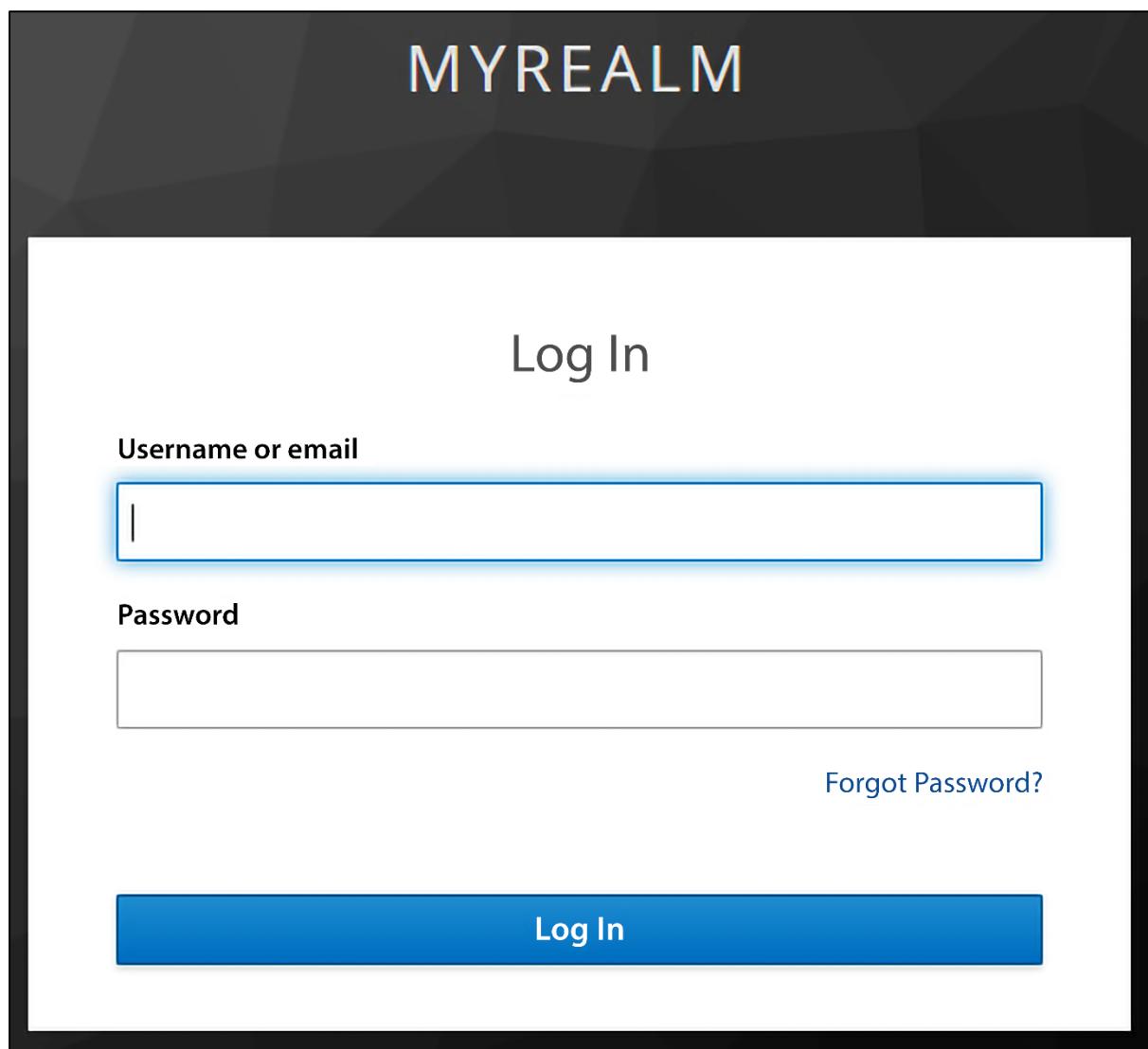
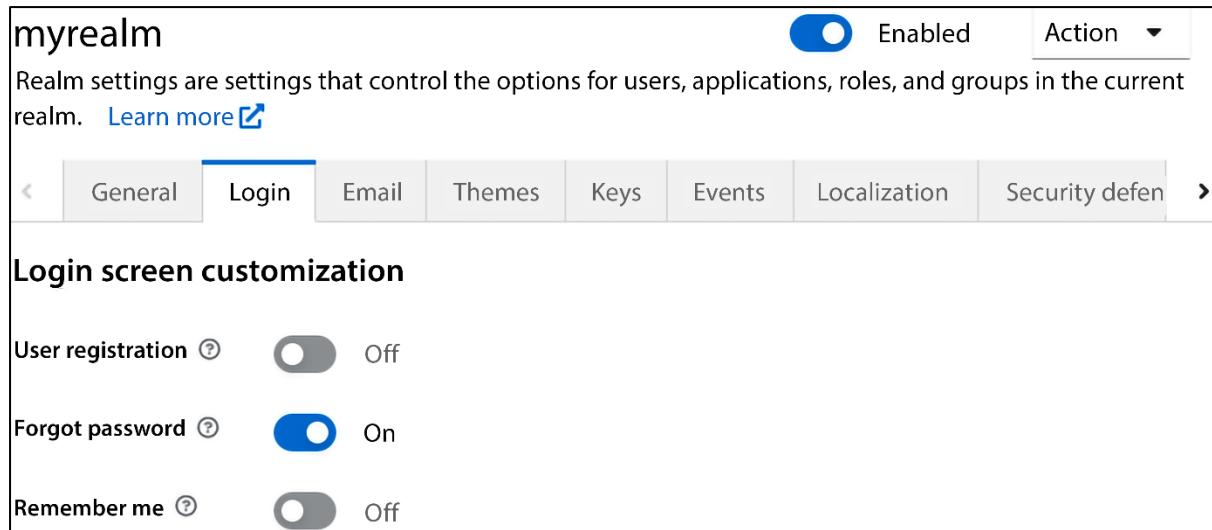
< General Login Email Themes Keys Events Localization Security defen >

Login screen customization

User registration ⓘ Off

Forgot password ⓘ On

Remember me ⓘ Off



Authentication

Authentication is the area where you can configure and manage different credential types. [Learn more ↗](#)

Flows Required actions Policies

OTP Policy

Webauthn Policy Webauthn Passwordless Policy CIBA Policy

OTP type Time based Counter based

OTP hash algorithm SHA1

Number of digits 6 8

Look ahead window

OTP Token period Seconds

Supported applications FreeOTP Google Authenticator Microsoft Authenticat...

Reusable token Off

[Save](#) [Reload](#)

≡ KEYCLOAK Sign out alice

Personal info

Account security ▾

Signing in

Configure ways to sign in.

Basic authentication

Password

Sign in by entering your password.

My password Created April 3, 2023 at 5:02 PM [Update](#)

Two-factor authentication

Authenticator application [Set up authenticator application](#)

Enter a verification code from authenticator application.

Authenticator application is not set up.

Mobile Authenticator Setup

1. Install one of the following applications on your mobile:

Microsoft Authenticator
Google Authenticator
FreeOTP

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

Submit

Cancel

alice 🔒

One-time code

Sign In

 Username Form	Required	
 Password Form	Required	
 My Browser Browser - Conditional OTP <small>Flow to determine if the OTP is required for the authentication</small>	Required	   
 Condition - user configured	Required	
 OTP Form	Required	

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

The screenshot shows the Keycloak user profile interface for a user named 'alice'. The left sidebar has navigation links: Personal info, Account security (selected), Applications, and Help. The main content area displays the following information:

- Personal info:** My password, Created April 3, 2023 at 5:02 PM, Update button.
- Two-factor authentication:** Authenticator application section: Enter a verification code from authenticator application. Status: Authenticator application is not set up.
- Security key:** Set up Security key button. Status: Security key is not set up.

MYREALM

🔑 Security Key Registration

Register

Cancel

Security key	Set up Security key
Use your security key to sign in.	
My Security Device	Created April 3, 2023 at 5:54 PM Remove

MYREALM

alice 

Windows Security



Making sure it's you

Please sign in to mykeycloak.

This request comes from Chrome, published by Google LLC.



Insert your security key into the USB
port.

Cancel

Chapter 12: Managing Tokens and Sessions

myrealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

Enabled Action ▾

General Login Email Themes Keys Events Localization Security defenses Sessions Tokens ▶

SSO Session Settings

SSO Session Idle ⓘ	30	Minutes
SSO Session Max ⓘ	10	Hours
SSO Session Idle Remember Me ⓘ	0	Minutes
SSO Session Max Remember Me ⓘ	0	Minutes

Client session settings

Client Session Idle ⓘ	0	Minutes
Client Session Max ⓘ	0	Minutes

Action ▾

Sessions

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)

All session types ▾ Search session → 1-1 ▾ < >

User	Type	Started	Last access	IP addr...	Clients
admin	REGULAR	5/2/2023, 12:44:37 PM	5/2/2023, 12:52:52 PM	127.0.0.1	security-admin-console

security-admin-console OpenID Connect Enabled Action

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

Settings Roles Client scopes Sessions Advanced

Search session → 1-1 ▾

User	Type	Started	Last access	IP address
admin	Regular SSO	5/2/2023, 12:44:37 PM	5/2/2023, 12:56:43 PM	127.0.0.1

1-1 ▾

admin Enabled Action

Details Attributes Credentials Role mapping Groups Consents Identity provider

Search session → Logout all sessions 1-1 ▾

Started	Last access	IP address	Clients
5/2/2023, 12:44:37 PM	5/2/2023, 1:00:42 PM	127.0.0.1	security-admin-console

1-1 ▾

Sessions

Sessions are sessions of users in this realm and the clients that they access with.

All session types Search session → Action Revocation Sign out all active sessions

User	Type	Started	Last access	IP addr...	Clients
admin	REGULAR	5/2/2023, 12:44:37 PM	5/2/2023, 1:02:09 PM	127.0.0.1	security-admin-console

1-1 ▾

admin

Enabled Action ▾

Details Attributes Credentials Role mapping Groups Consents Identity provider

Search session → Logout all sessions 1-1 ▾

Started	Last access	IP address	Clients
5/2/2023,12:44:37 PM	5/2/2023,1:06:11 PM	127.0.0.1	security-admin-console

Sign out 1-1 ▾

Access Token Lifespan 5 Minutes ▾

(?) It is recommended for this value to be shorter than the SSO session idle timeout: 30 minutes

Advanced Settings

This section is used to configure advanced settings of this client related to OpenID Connect protocol

Access Token Lifespan	Inherits from realm settings	5	Minutes
Client Token Idle	Inherits from realm settings	0	Minutes
Client Token Max	Inherits from realm settings	0	Minutes

Advanced Settings

This section is used to configure advanced settings of this client related to OpenID Connect protocol

Access Token Lifespan Inherits from realm settings 5 Minutes

Client Token Idle Inherits from realm settings 0 Minutes

Client Token Max Inherits from realm settings 0 Minutes

Refresh tokens

Revoke Refresh Token



Enabled

Refresh Token Max

-	0	+
---	---	---

Reuse ?

Sessions

Action ▾

Sessions are sessions of users in this realm and the client. [Learn more](#)

Revocation

Sign out all active sessions

Revocation

×

This is a way to revoke all active sessions and access tokens. Not before means you can revoke any tokens issued before the date.

Not before

None

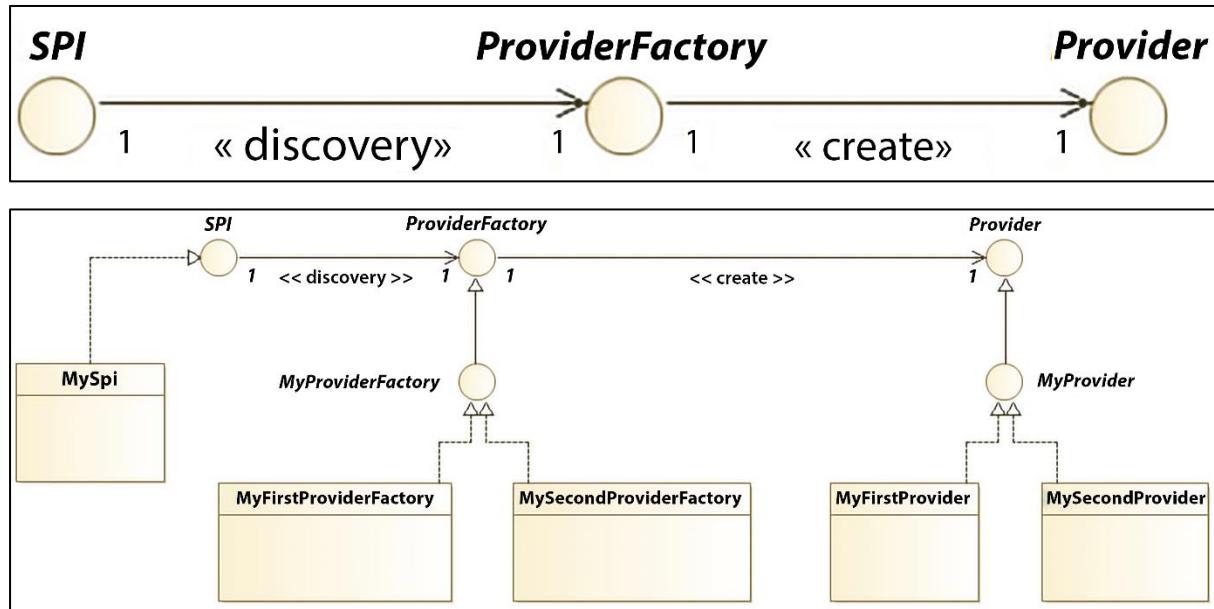
[Set to now](#)

[Clear](#)

[Push](#)

[Cancel](#)

Chapter 13: Extending Keycloak



The screenshot shows the Keycloak Admin UI interface for the "master realm".

The top navigation bar includes the Keycloak logo, a search icon, and user information (admin). A dropdown menu is open, showing options: "Manage account", "Realm info", and "Sign out".

The main content area displays the "master realm" name and two tabs: "Server info" and "Provider info". The "Provider info" tab is currently selected and active.

Below the tabs is a search bar with a magnifying glass icon and an "→" button.

The main table lists SPIs and their corresponding Providers:

SPI	Providers
account	freemarker
actionTokenHandler	verify-email execute-actions reset-credentials idp-verify-account-via-email update-email

KEYCLOAK

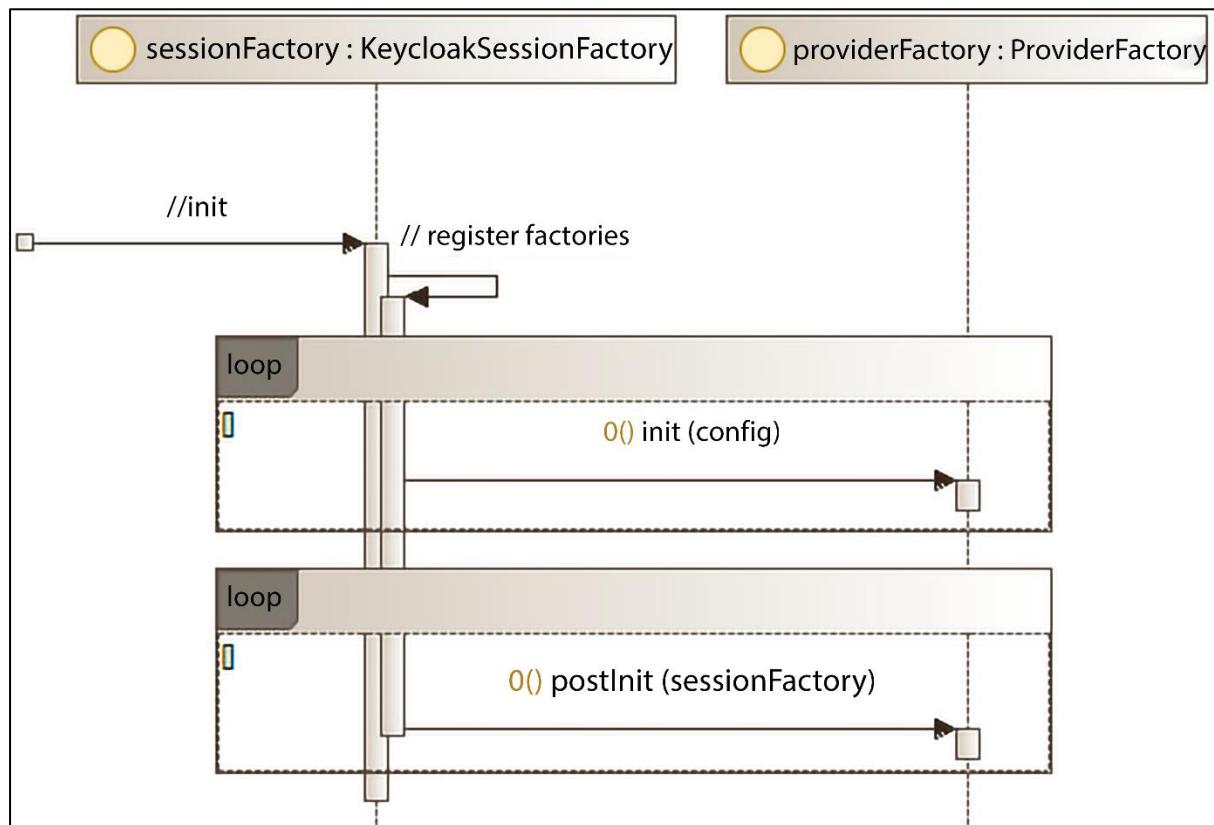
admin

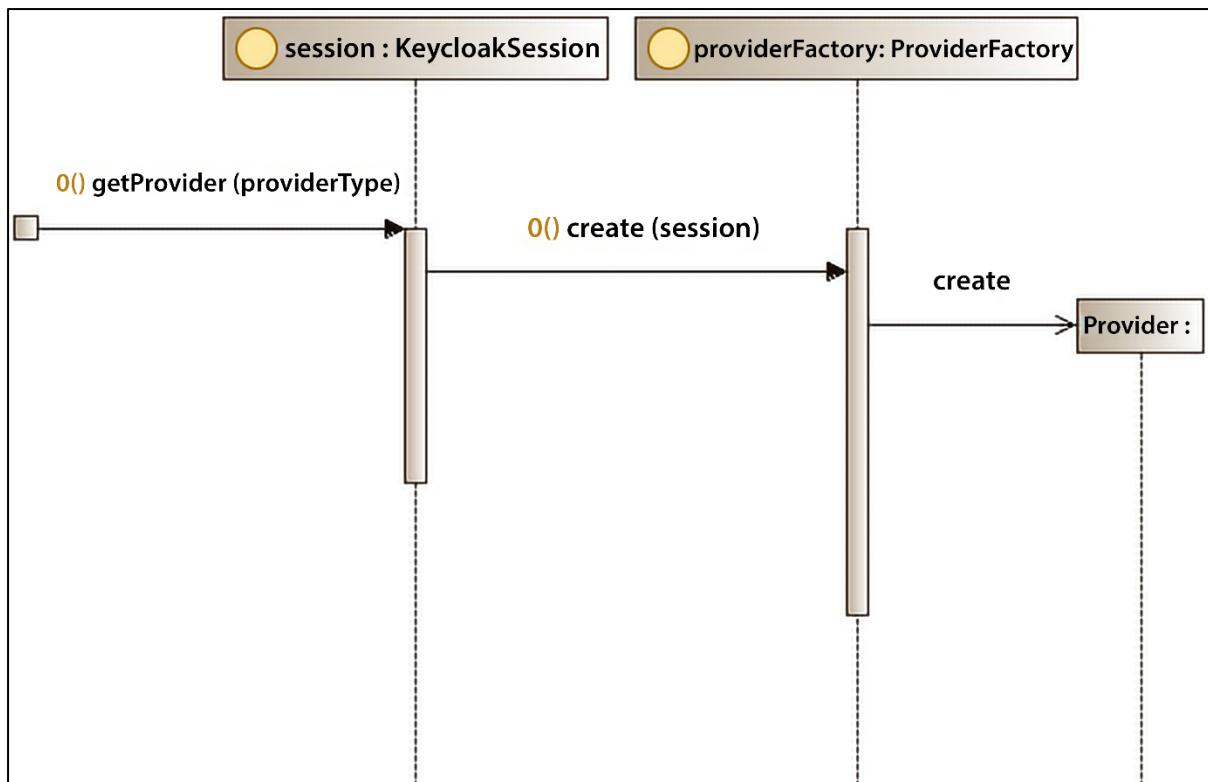
master realm

Server info Provider info

x →

SPI	Providers
social	github facebook google instagram linkedin bitbucket microsoft





myrealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

Enabled Action ▾

< General Login Email Themes **Themes** Keys Events Localization Security defenses Sessions >

Login theme ⓘ	Select a theme
Account theme ⓘ	Select a theme
Admin UI theme ⓘ	Select a theme
Email theme ⓘ	Select a theme

Save **Revert**

This screenshot shows the 'Themes' tab of the 'myrealm' configuration interface. It displays four dropdown menus for selecting themes for different components: Login, Account, Admin UI, and Email. Each dropdown has a placeholder text 'Select a theme'. Below the tabs, there are 'Save' and 'Revert' buttons.

Login settings

Login theme [?](#)

Choose...



Consent required [?](#)



Off

Display client on
screen [?](#)



Off

Client consent screen
text [?](#)

Login settings

Login theme [?](#)

mytheme



Consent required [?](#)



Off

Display client on
screen [?](#)



Off

Client consent screen
text [?](#)

MYREALM

[English v](#)

Sign in to your account

Username or email

Password

[Forgot Password?](#)

[**Sign In**](#)

New user? [Register](#)

Conditional OTP Form config

X

Alias * ⓘ

conditional-otp

OTP control User Attribute ⓘ

my.risk.based.auth.2fa.required

Skip OTP for Role ⓘ

Select Role

Force OTP for Role ⓘ

Select Role

Skip OTP for Header ⓘ

Force OTP for Header ⓘ

Fallback OTP handling ⓘ

force



Save

Cancel

Authentication > Flow details

My Risk-Based Browser Flow

Not in use

Add step Add sub-flow

Steps	Requirement
Cookie	Alternative
Kerberos	Disabled
Identity Provider Redirector	Alternative
My Risk-Based Browser Flow forms Username, password, otp and other auth forms.	Alternative
Username Password Form	Required
My Risk-Based Browser Flow - Conditional OTP Flow to determine if the OTP is required for the authentication	Conditional
Condition - user configured	Required
My Simple Risk-Based Authenticator	Required
Conditional OTP Form	Required

myrealm

Realm settings are settings that control the options for users, applications, roles, and groups.

< Email Themes Keys Events Localization Security defenses

Headers Brute force detection

Enabled On

Max login failures ? 30

Permanent lockout Off

Wait increment ? Minutes

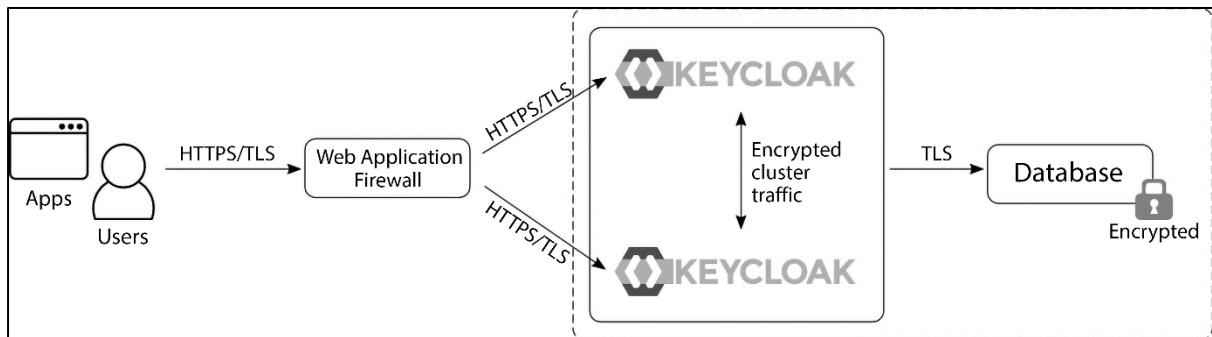
Max wait ? Minutes

Failure reset time ? Hours

Quick login check
milliseconds ? 1000

Minimum quick login
wait ? Minutes

Chapter 14: Securing Keycloak and Applications



Screenshot of the Keycloak 'Keys' management interface:

Algorithm	Type	Kid	Provider	Public keys
RSA-OAEP	RSA	rjOVU554iTBIAZzPBDt4yr_XGL3KJAYRdzK99aMeKQ	rsa-enc-generated	Public key Certificate
AES	OCT	c42814bb-8b61-4a74-926f-a1eb590e5c50	aes-generated	
RS256	RSA	2csknI6J3mAYjNUgpvGjIC_378VH0hIStcJ_JvCOV9c	rsa-generated	Public key Certificate
HS256	OCT	c2e33f29-6f2c-4acf-b657-7141b4d313d5	hmac-generated	

Add provider

Name * rsa-generated-2

Priority 200

Enabled On

Active On

Key size 2048

Algorithm RS256

Save **Cancel**

Keys list						Providers
Active keys						
Algorithm	Type	Kid	Provider	Public keys		
RS256	RSA	HN5qkKYqN5Tj0I1re4r4P56TzicWViFRJqSjH-hd7Wo	rsa-generated-2	Public key	Certificate	
RS256	RSA	2csknl6J3mAYjNUgpvGjIC_378VH0hIStcJ_JvCOV9c	rsa-generated	Public key	Certificate	

Flows	Required actions	Policies			
Password policy	OTP Policy	Webauthn Policy			
Webauthn Passwordless Policy					
Add policy ▾					
Minimum Length * ⓘ					
<table border="1"><tr><td>-</td><td>8</td><td>+</td></tr></table>			-	8	+
-	8	+			
Special Characters * ⓘ					
<table border="1"><tr><td>-</td><td>1</td><td>+</td></tr></table>			-	1	+
-	1	+			
Uppercase Characters * ⓘ					
<table border="1"><tr><td>-</td><td>1</td><td>+</td></tr></table>			-	1	+
-	1	+			
Lowercase Characters * ⓘ					
<table border="1"><tr><td>-</td><td>1</td><td>+</td></tr></table>			-	1	+
-	1	+			
Digits * ⓘ					
<table border="1"><tr><td>-</td><td>1</td><td>+</td></tr></table>			-	1	+
-	1	+			

[General](#) [Login](#) [Email](#) [Themes](#) [Keys](#) [Events](#) [Localization](#) **Security defenses** [S](#)

Headers **Brute force detection**

Enabled On

Max login failures [?](#) [-](#) [+](#)

Permanent lockout Off

Wait increment [?](#) Minutes [▼](#)

Max wait [?](#) Minutes [▼](#)

Failure reset time [?](#) Hours [▼](#)

Quick login check milliseconds [?](#) [-](#) [+](#)

Minimum quick login wait [?](#) Minutes [▼](#)

[Save](#) [Revert](#)

Access settings

Root URL [?](#)

Home URL [?](#)

Valid redirect URIs [?](#)

https://acme.corp/myclient/oauth-callback



[+ Add valid redirect URIs](#)

Valid post logout
redirect URIs [?](#)

https://acme.corp/myclient/oauth-logout



[+ Add valid post logout redirect URIs](#)

Web origins [?](#)

https://acme.corp



[+ Add web origins](#)

Admin URL [?](#)

Capability config

Client authentication [?](#)



Off

Authorization [?](#)



Off

Authentication flow

Standard flow [?](#)

Direct access grants [?](#)

Implicit flow [?](#)

Service accounts roles [?](#)

OAuth 2.0 Device Authorization Grant [?](#)