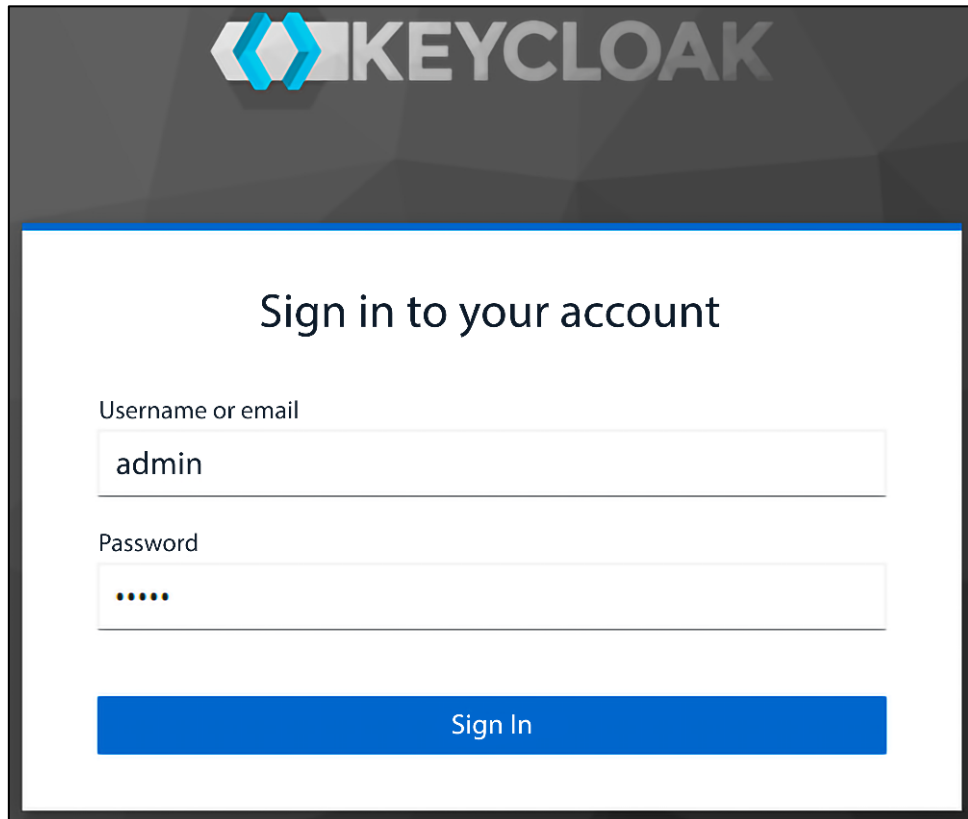


Chapter 1: Getting Started with Keycloak



The image shows the Keycloak login page. At the top, there is a dark header with the Keycloak logo (a blue and white geometric shape) and the word "KEYCLOAK" in white. Below the header, the main content area is white. It features the text "Sign in to your account" in a large, dark font. Underneath, there are two input fields: "Username or email" with the text "admin" entered, and "Password" with a masked password represented by six dots. A blue "Sign In" button is positioned below the password field.

KEYCLOAK

Sign in to your account

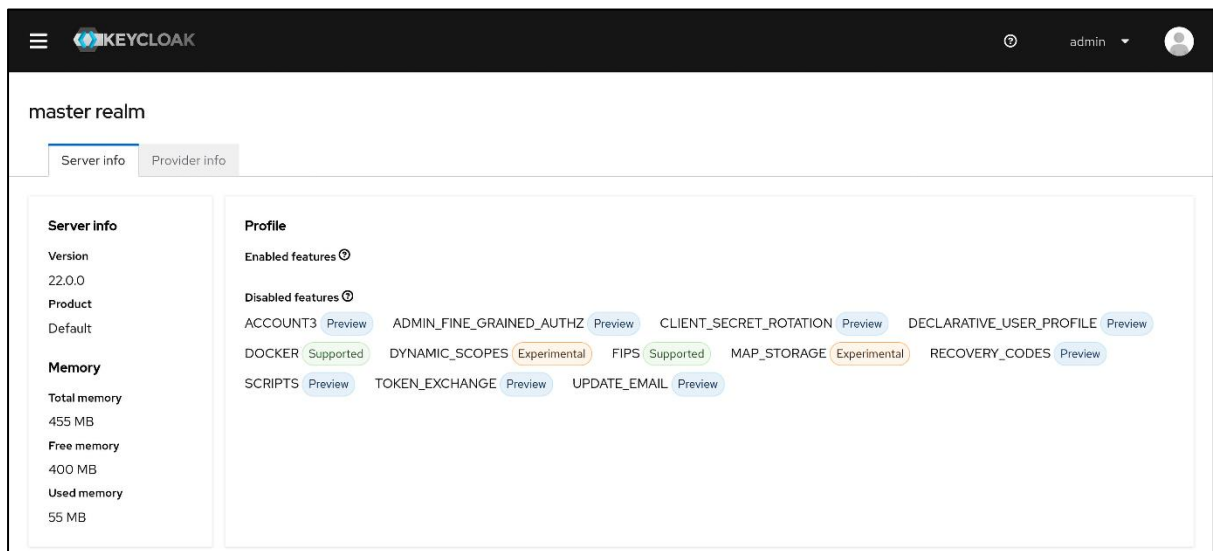
Username or email

admin

Password

.....

Sign In



The image shows the Keycloak Admin Console interface. At the top, there is a dark header with the Keycloak logo and the word "KEYCLOAK" on the left, and a user profile icon labeled "admin" on the right. Below the header, the main content area is white. It features a sidebar on the left with the text "master realm" and two tabs: "Server info" (selected) and "Provider info". The main content area is divided into two sections: "Server info" and "Profile". The "Server info" section displays the following information:

- Version:** 22.0.0
- Product:** Default
- Memory:**
 - Total memory: 455 MB
 - Free memory: 400 MB
 - Used memory: 55 MB

The "Profile" section displays the following information:

- Enabled features:** (indicated by a green checkmark icon)
- Disabled features:** (indicated by a red X icon)
- 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
- UPDATE_EMAIL:** Preview

KEYCLOAK

admin

Master

Master

Create Realm

Realm roles

Users

Groups

Sessions

Events

8e866b879b3637d1eca326151

tures

tures

DE_GRAINED_AUTHZ CLIENT_SECRET_ROTATION DECLARATIVE_USER_PROFILE

DYNAMIC_SCOPES MAP_STORAGE OPENSIFT_INTEGRATION

_CODES SCRIPTS TOKEN_EXCHANGE UPDATE_EMAIL

Users > Create user

Create user

Required user actions

Select action

Username *

keycloak

Email

keycloak@keycloak.org

Email verified

No

First name

Ola

Last name

Nordmann

Groups

Join Groups

Create

Cancel

Welcome to Keycloak Account Management

Personal Info

Manage your basic information

[Personal Info](#)

Account Security

Control your password and account access

[Signing In](#)

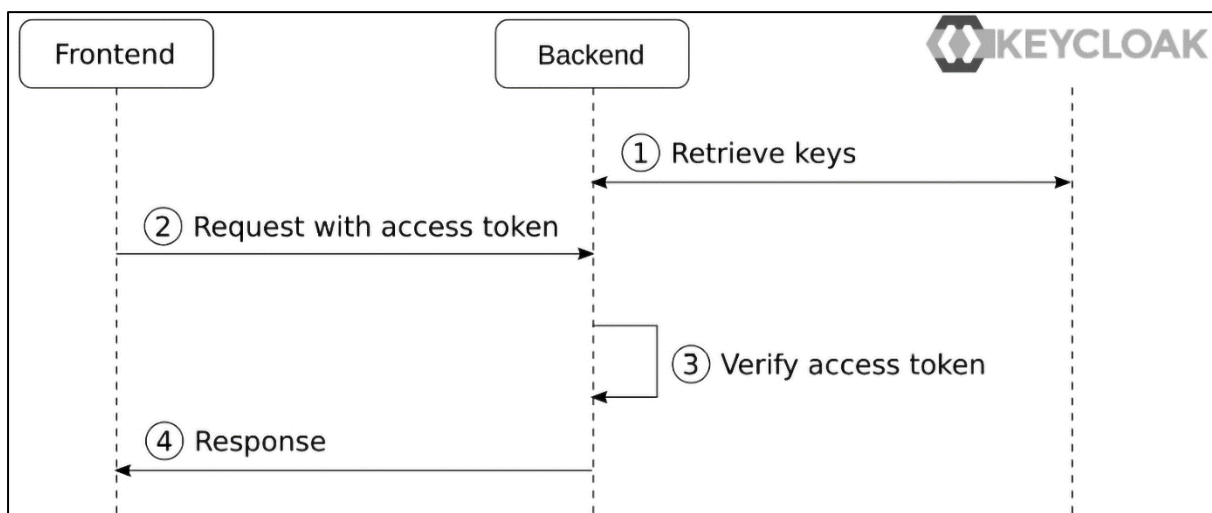
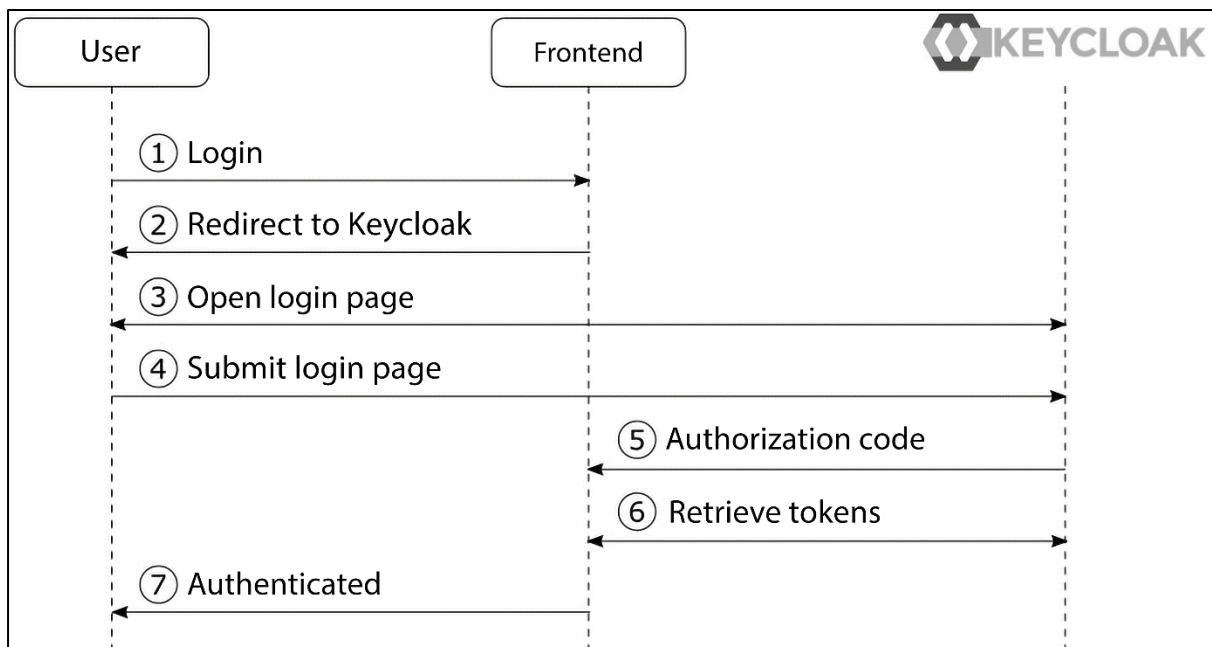
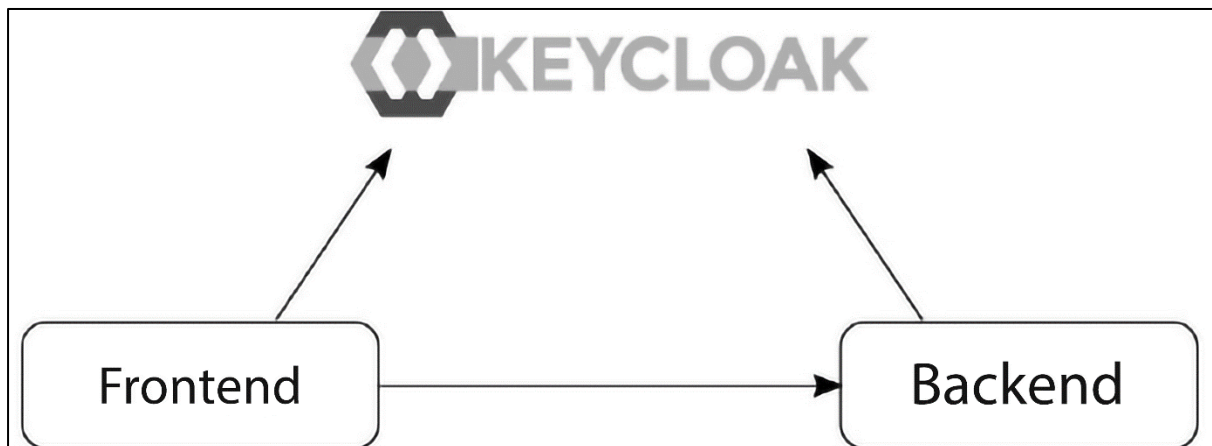
[Device Activity](#)

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

DetailsAttributesCredentialsRole mappingGroupsConsentsIdentity provider linksSessions

KeyValue

picture

https://avatars.githubusercontent.com/u/2271511

Type a key

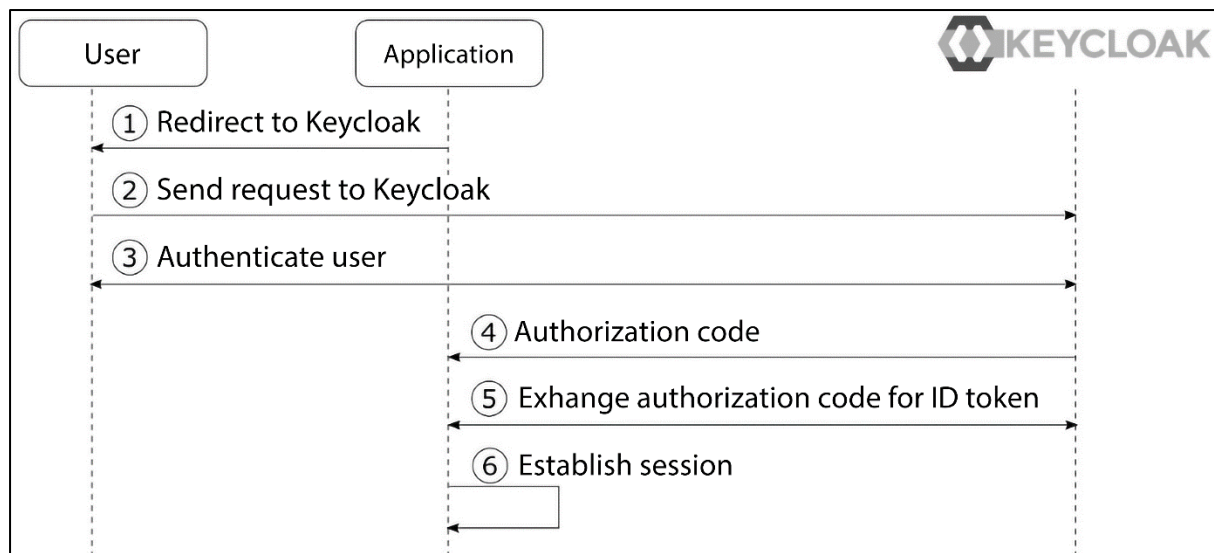
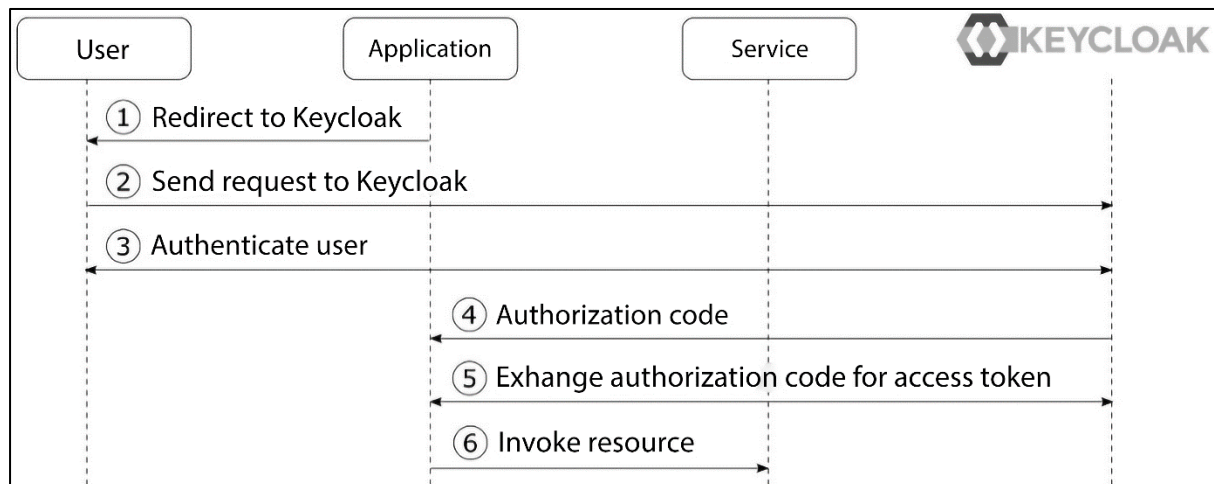
Type a value

+ 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

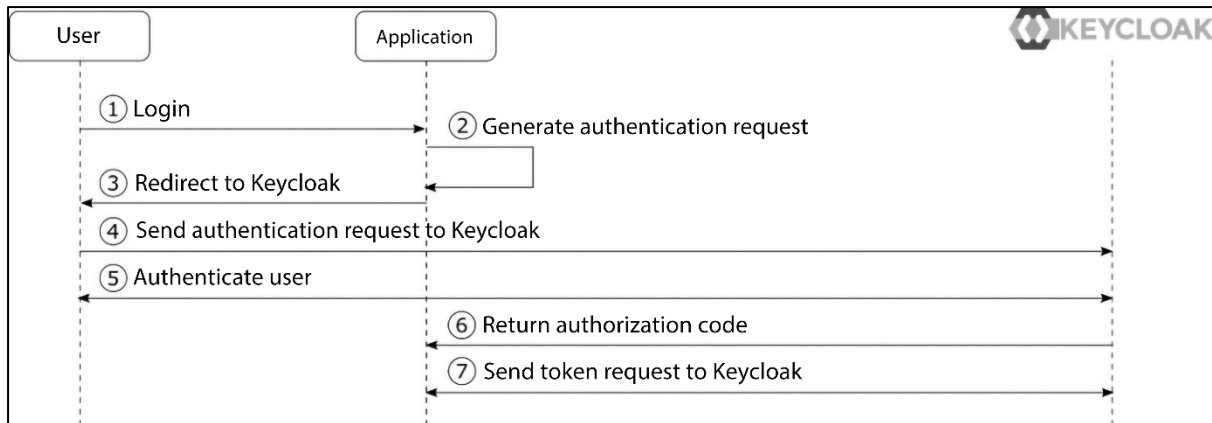
Issuer

[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"
  ],
  "response_types_supported": [
    "code",
    "token",
    "id_token",
    "code,id_token",
    "token,id_token",
    "code,id_token,token,id_token"
  ],
  "scopes_supported": [
    "openid",
    "profile",
    "email",
    "address",
    "phone",
    "offline_access"
  ],
  "subject_types_supported": [
    "pairwise",
    "public"
  ],
  "id_token_signed_response_alg": "RS256",
  "userinfo_signed_response_alg": "none",
  "request_object_supported": true,
  "request_uri_parameter_supported": false,
  "require_request_uri_registration": true,
  "op_typed_response": true
}
```



Authentication Request

```
http://localhost:8080/realms/myrealm/protocol/openid-connect/auth

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

Token Request

```
http://localhost:8080/realms/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": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXLTJ1Iiwia2kiOiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX",
  "expires_in": 300,
  "refresh_expires_in": 1800,
  "refresh_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXLTJ1Iiwia2kiOiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX",
  "token_type": "Bearer",
  "id_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXLTJ1Iiwia2kiOiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX",
  "not-before-policy": 0,
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",
  "scope": "openid profile email"
}
```

```
"token_type": "Bearer"
"id_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXLTJ1Iiwia2kiOiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX",
"not-before-policy": 0,
```

ID Token

Header

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "MRRaVl0HPdTU8NcJXZsMo-Nl5IaFB9JqYZmy4mUeXDM"
}
```

Payload

```
{
  "exp": 1665296255,
  "iat": 1665295955,
  "auth_time": 1665295938,
  "jti": "daf6072b-d376-47eb-ba7a-cb203336c6c3",
  "iss": "http://localhost:8080/realms/myrealm",
  "aud": "oidc-playground",
  "sub": "65588621-32e8-4655-8cfd-86fb8054822e",
  "typ": "ID",
  "azp": "oidc-playground",
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",
  "at_hash": "pWygilI1h8q3gIpd8-lIwA",
  "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

X2hfrpAyDb4tFRWbvnpGc-i79IzxBoy00YKEK9cmKaDoAy0G-0DA7zVYirbEYhkPv66C6MAUQu4EmXzJ73-aM3xdngEPUA0rYSgg-PHkiYug3IiJgDyc-

Refresh Request

`http://localhost:8080/realms/myrealm/protocol/openid-connect/token`

```
grant_type=refresh_token
refresh_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50L3N1bWUiLCJ1aWQiOiA6IiwiaWF0IjE6IjE2MTAzMTcxYi1MzA5LTQ1NWYtYVJhZiliYjYk2NTQxYTAYmjk1fQ
client_id=oidc-playground
scope=openid
```

Refresh Response

```
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2kiOiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSVIFGQj1KcVlabX",
  "expires_in": 300,
  "refresh_expires_in": 1800,
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2kiOiA6ICJMTAzMTCxYiIlMzA5LTQ1NWYtYWJZIlilYjk2NTQxYTAYM",
  "token_type": "Bearer",
  "id_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2kiOiA6ICJNU1JhVmNmiSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabXkObV",
  "not-before-policy": 0,
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",
  "scope": "openid profile email"
}
```

UserInfo Request

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

`Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJNU1JhVmwwSFBkVFU4TmNKW`

UserInfo Response

```
{
  "sub": "65588621-32e8-4655-8cfd-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

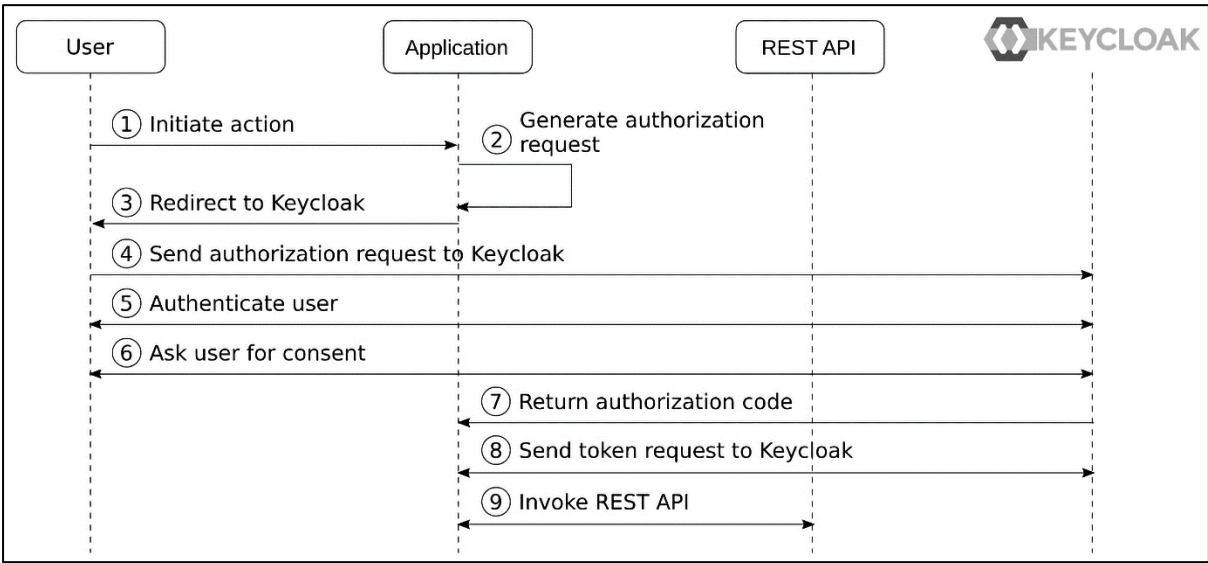
- 1 - Discovery
- 2 - Authorization
- 3 - Invoke Service
- Reset

Discovery

Issuer

Load OAuth 2.0 Provider Configuration

OAuth 2.0 Provider Configuration



Access Token

Header

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "JI0_xxUiSi7oUkx0xLQe8xsdRTnK0irURnBuik6EyyQ"
}
```

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 ?

Grant Access to oauth-playground

Do you grant these access privileges?

User profile

User roles

Email address

Yes

No

Create client scope

Name * ?

albums

Description ?

Type ?

None

Protocol ?

OpenID Connect

Display on consent
screen ?



On

Consent screen text
?

View your photo albums

Include in token scope
?



On

Display Order ?

Save

Cancel

Grant Access to oauth-playground

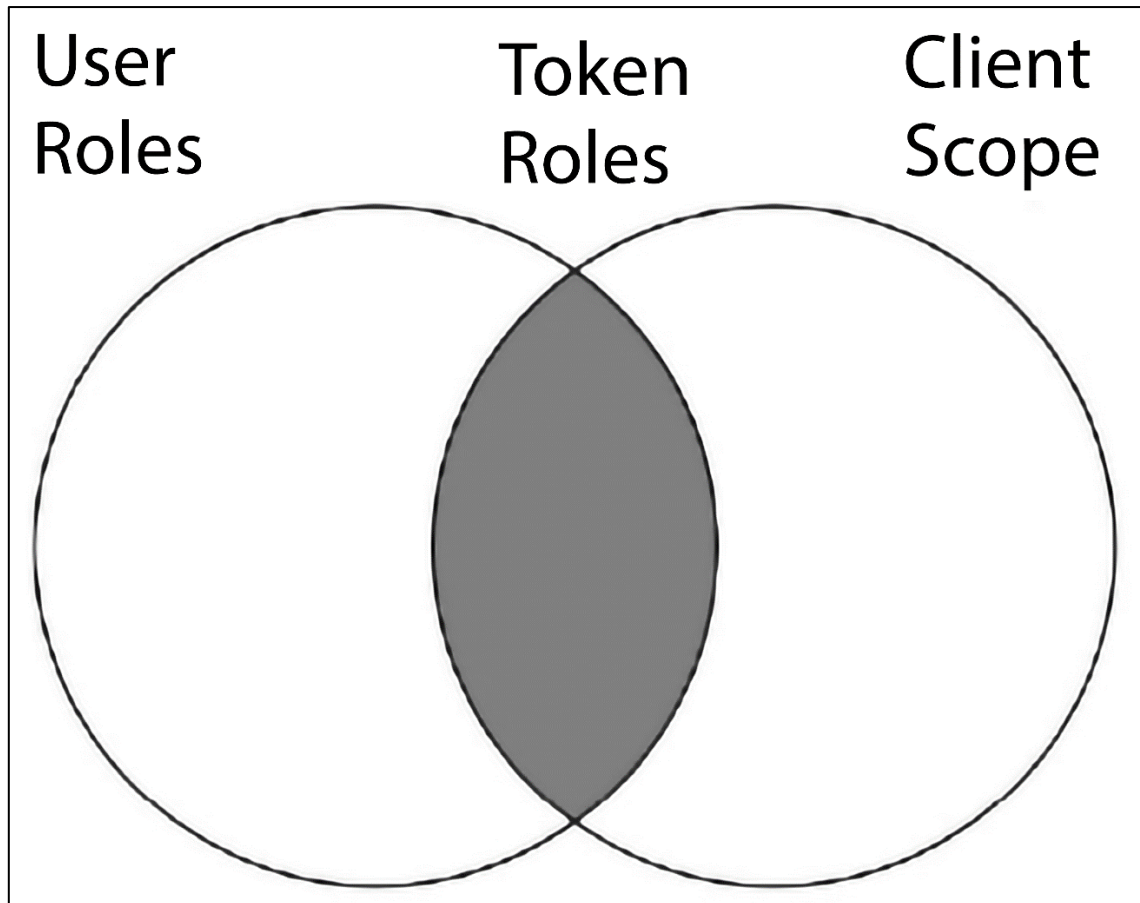
Do you grant these access privileges?

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 }
```



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/realms/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

Master ▾	Login settings	Jump to section
Manage	Login theme ⓘ Choose...	General Settings
Clients	Consent required ⓘ ☒ Off	Access settings
Client scopes	Display client on screen ⓘ ☐ Off	Capability config
Realm roles		
Users		

Master ▾	Login settings	Jump to section
Manage	Login theme ⓘ Choose...	General Settings
Clients	Consent required ⓘ ☐ Off	Access settings
Client scopes	Display client on screen ⓘ ☐ Off	Capability config
Realm roles		
Users		

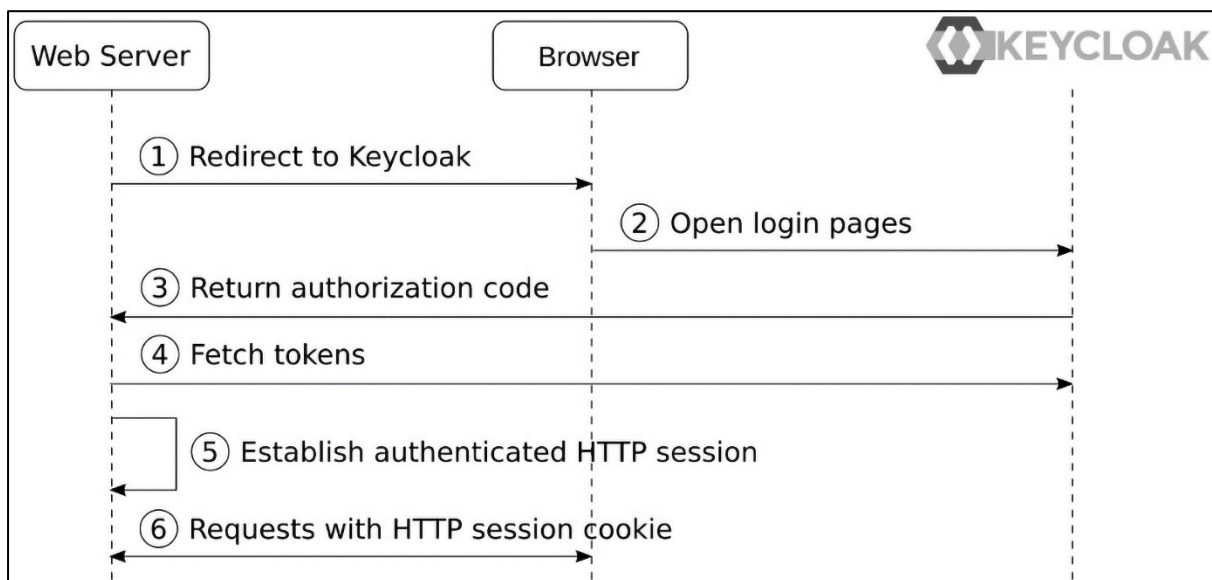
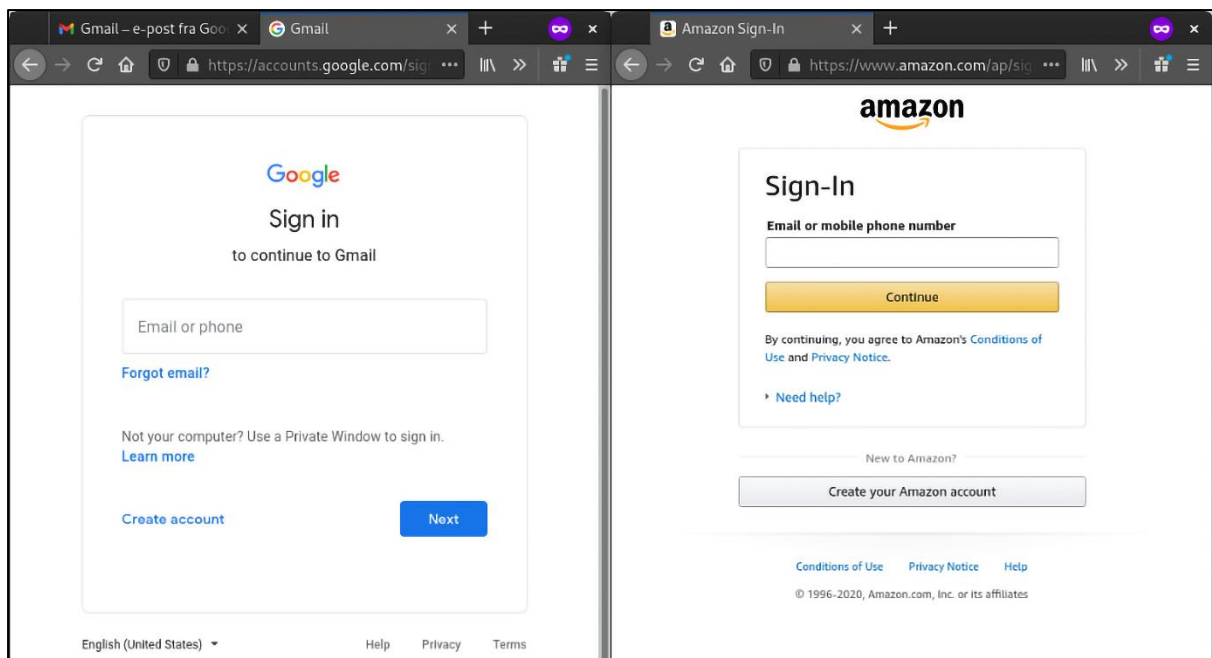
MY REALM

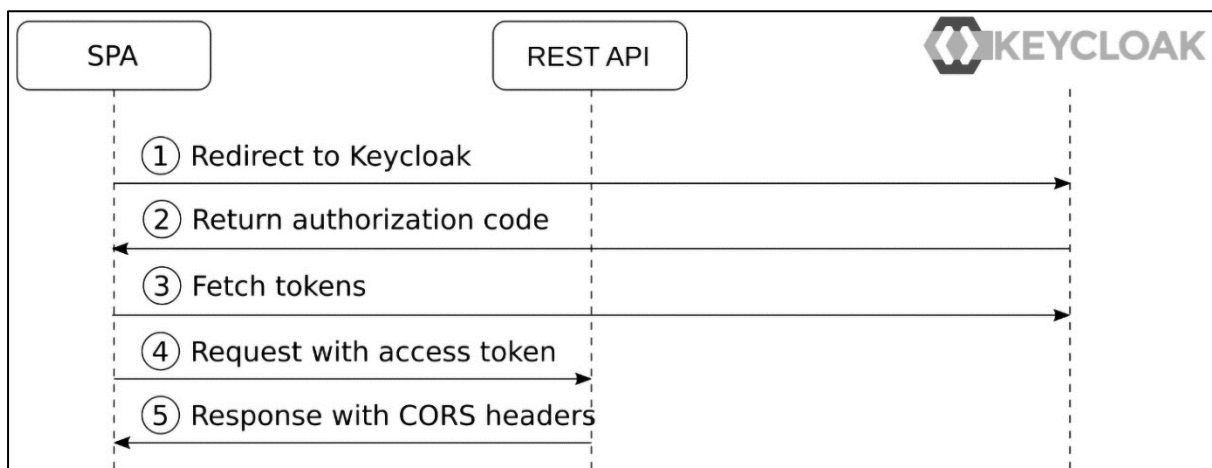
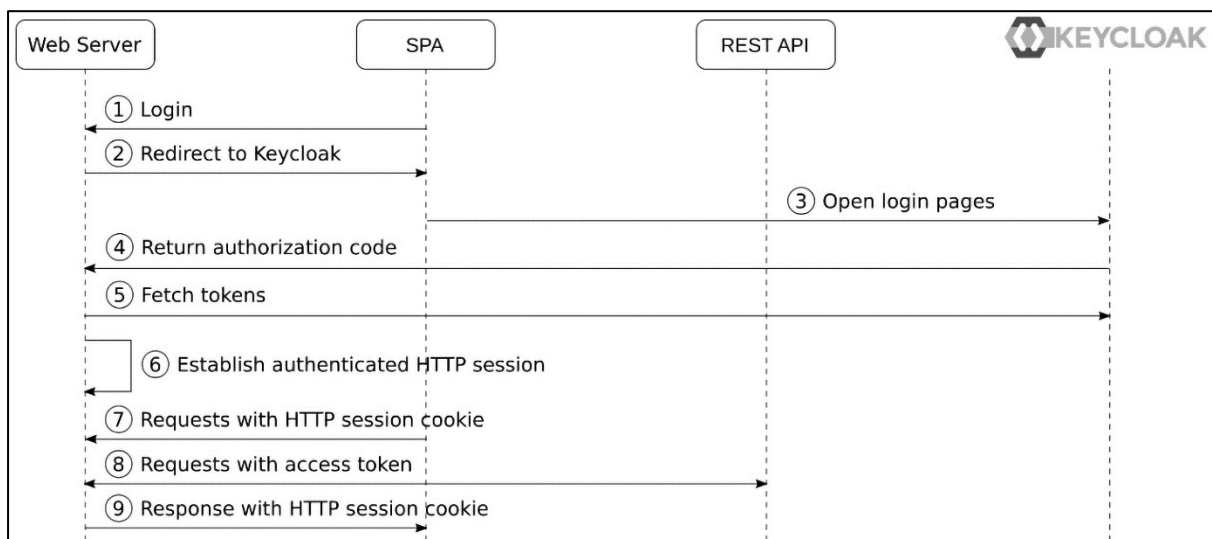
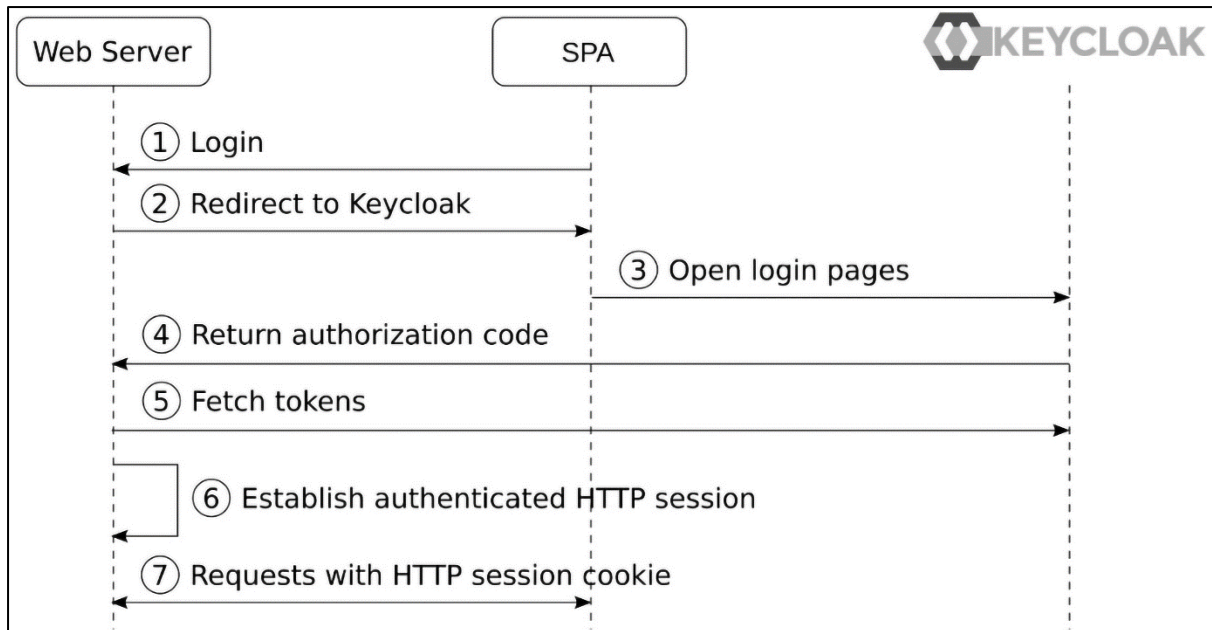
Grant Access to External Application

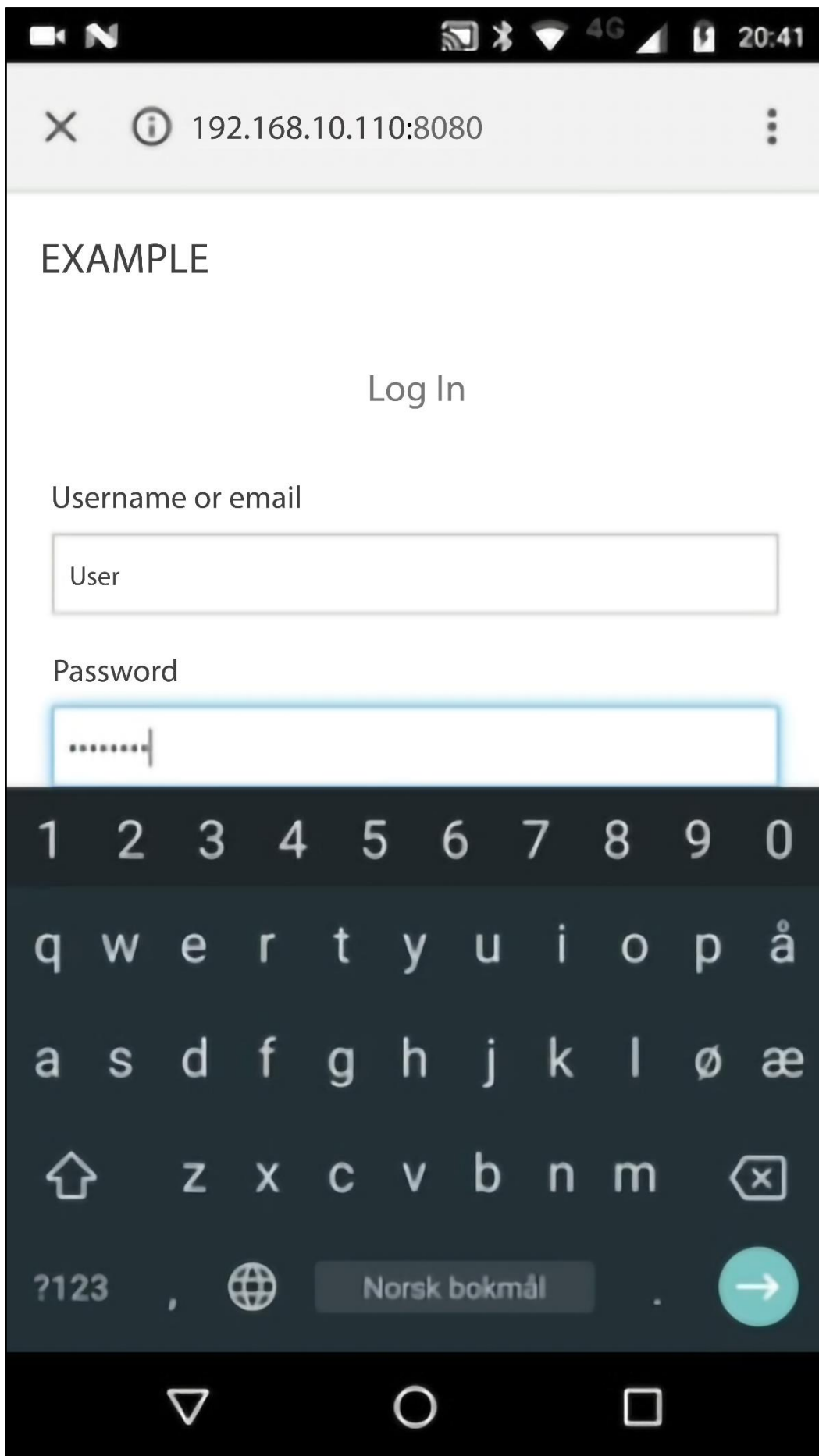
Do you grant these access privileges?

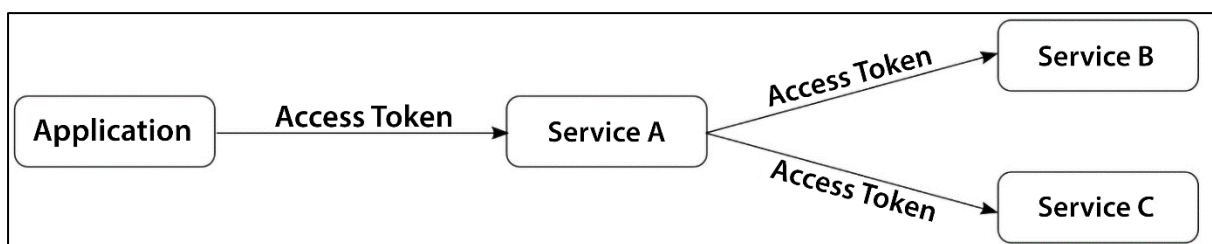
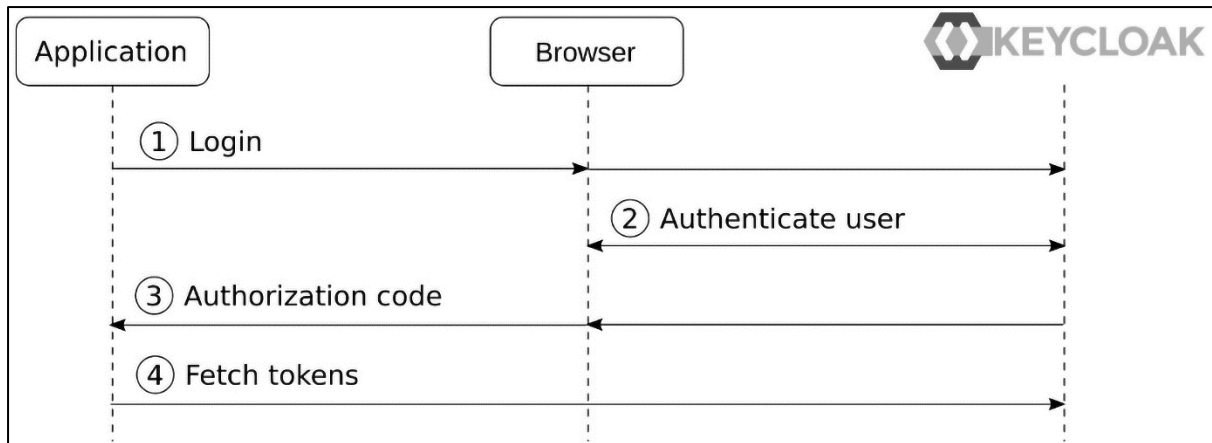
User profile

No Yes









Myrealm

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

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

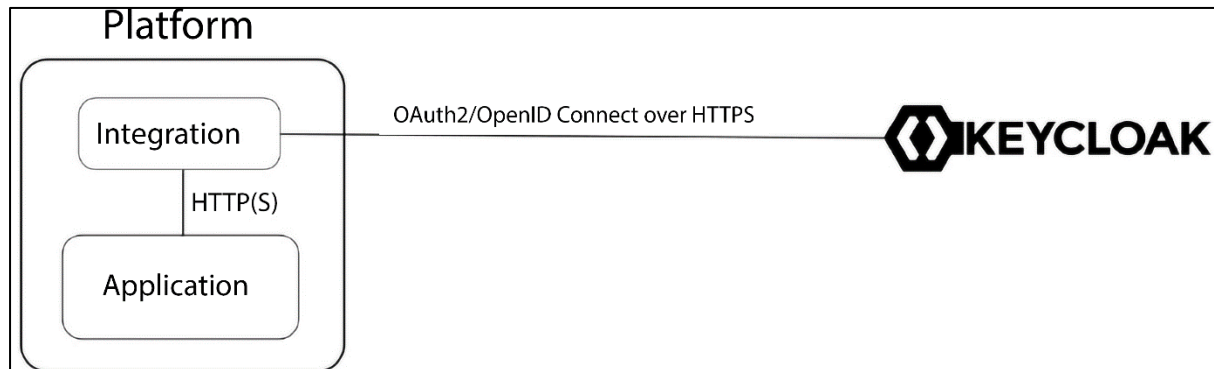
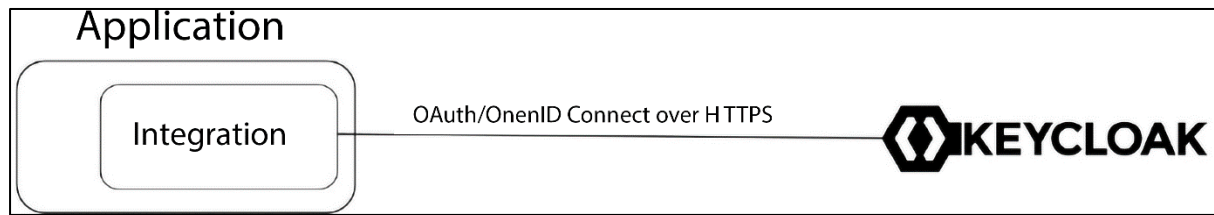
Access settings

Capability config

Login settings

Logout settings

Chapter 7: Integrating Applications with Keycloak



Chapter 8: Authorization Strategies

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

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

Group Membership

Action

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

Join groups for user alice

×

🔍 Search for groups

→

1-1

✓

Project Management Office

<

1-1 ▾

>

Join

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

 × Select scope parameters

User

?

alice

×

Setup

Evaluate

?

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

Scope parameter

?

openid

 × Select scope parameters

User

?

alice

×

Effective protocol mappers

?

Effective role scope mappings

?

Generated access token

?

Generated ID token

?

Generated user info

?

```
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": ""
}
```

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

InspectorConsoleDebuggerNetworkStyle EditorPerformance

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/realms/master"
authorization_endpoint: "https://mykeycloak/realms/master/protocol/openid-connect/auth"
token_endpoint: "https://mykeycloak/realms/master/protocol/openid-connect/token"
introspection_endpoint: "https://mykeycloak/realms/master/protocol/openid-connect/token/introspect"
userinfo_endpoint: "https://mykeycloak/realms/master/protocol/openid-connect/userinfo"
end_session_endpoint: "https://mykeycloak/realms/master/protocol/openid-connect/logout"
frontchannel_logout_session_supported: true
frontchannel_logout_supported: true
jwks_uri: "https://mykeycloak/realms/master/protocol/openid-connect/certs"
check_session_iframe: "https://mykeycloak/realms/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 ?

Join Groups

Create

Cancel

Set password for alice

Password *

●●●●●

👁

Password confirmation *

●●●●●

👁

Temporary ?

☐ Off

Save

Cancel

KEYCLOAK

Sign outalice

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](#)

alice

☒ EnabledAction

<

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider link

>

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

Email verified ?

☐ No

First name

Last name

Save

Revert

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](#)



[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](#)

[Personal Info](#)[Account Security](#) >[Applications](#)

Personal Info

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

Username *

Email *

First name *

Last name *

Chapter 11: Authenticating Users

Authentication

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

Flows

Required actions

Policies

Q Search for flow

→

Create flow

1-8

<

>

Flow name	Used by	Description
browser Built-in	✓ Browser flow	browser based authentication
clients Built-in	✓ Client authentication flow	Base authentication for clients
direct grant Built-in	✓ Direct grant flow	OpenID Connect Resource Owner Grant
docker auth Built-in	✓ Docker authentication flow	Used by Docker clients to authenticate against the IDP
registration Built-in	✓ Registration flow	registration flow
reset credentials Built-in	✓ Reset credentials flow	Reset credentials for a user if they forgot their password or something
first broker login Built-in	Not in use	Actions taken after first broker login with identity provider account, which is not yet linked to any Keycloak account
http challenge Built-in	Not in use	An authentication flow based on challenge-response HTTP Authentication Schemes

Duplicate flow

×

Name *

?

My Browser

Description

?

Mu custom browser flow definition

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

Q 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

+ ▼ ✎ 🗑

Username Form

Required

🗑

Password Form

Required

🗑

My Browser Browser - Conditional OTP

Flow to determine if the OTP is required for the authentication

Conditional

+ ▼ ✎ 🗑

Condition - user configured

Required

🗑

OTP Form

Required

🗑

Bind flow

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 ✕

Select action

✕

▼

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

MYREALM

Log In

Username or email

Password

Forgot Password?

Log In

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

OTP type ?

☒ Time based

☐ Counter based

OTP hash algorithm ?

SHA1

Number of digits ?

☒ 6

☐ 8

Look ahead window ?

-

1

+

OTP Token period ?

30

Seconds

Supported applications ?

FreeOTP

Google Authenticator

Microsoft Authenticat...

Reusable token ?

☐ Off

Save

Reload

KEYCLOAK

Sign out

alice

Personal info

Account security

Signing in

Device activity

Applications

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 Flow to determine if the OTP is required for the authentication	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	

[Sign out](#)
alice

Personal info
Account security
Signing in
Device activity
Applications

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.

Security key

Set up Security key

Use your security key to sign in.

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

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

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

Sessions

Action

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

1-1

<

>

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

Q 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 provid

>

Q 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

Action

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

⌵ All session types

Q Search session

→

⌵

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 provid

>

Q 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

1 - 1

Sign out

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

Reuse



–

0

+

Sessions

Action ▼

Sessions are sessions of users in this realm and the cli session. [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

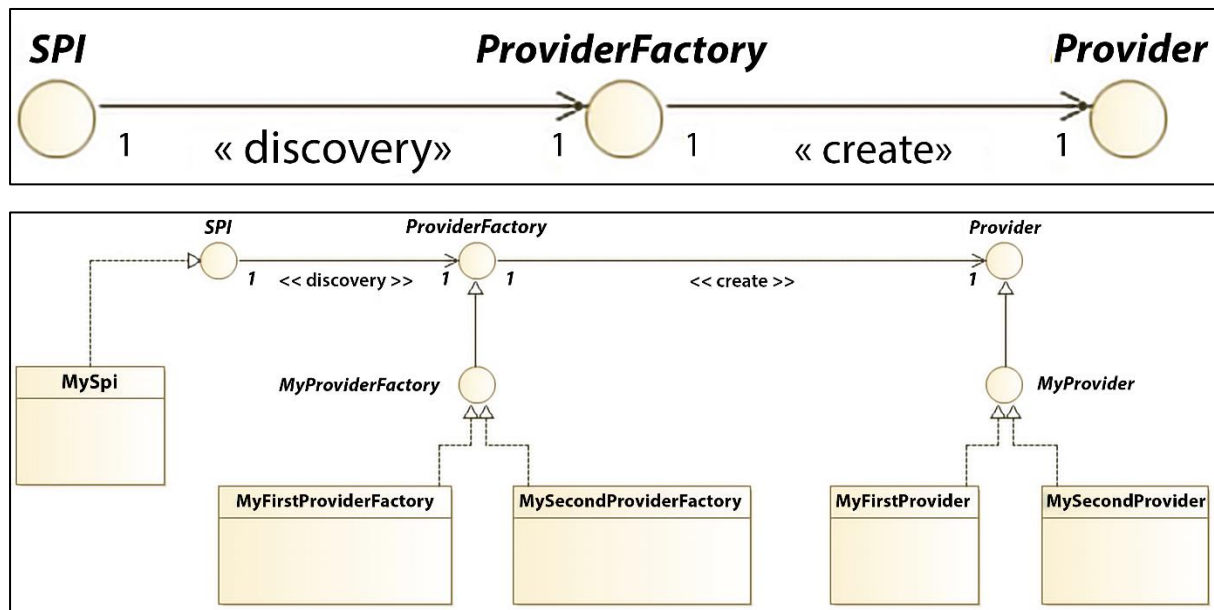
Set to now

Clear

Push

Cancel

Chapter 13: Extending Keycloak



 **KEYCLOAK**

admin



master realm

Server info

Provider info

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

 KEYCLOAK

 admin 

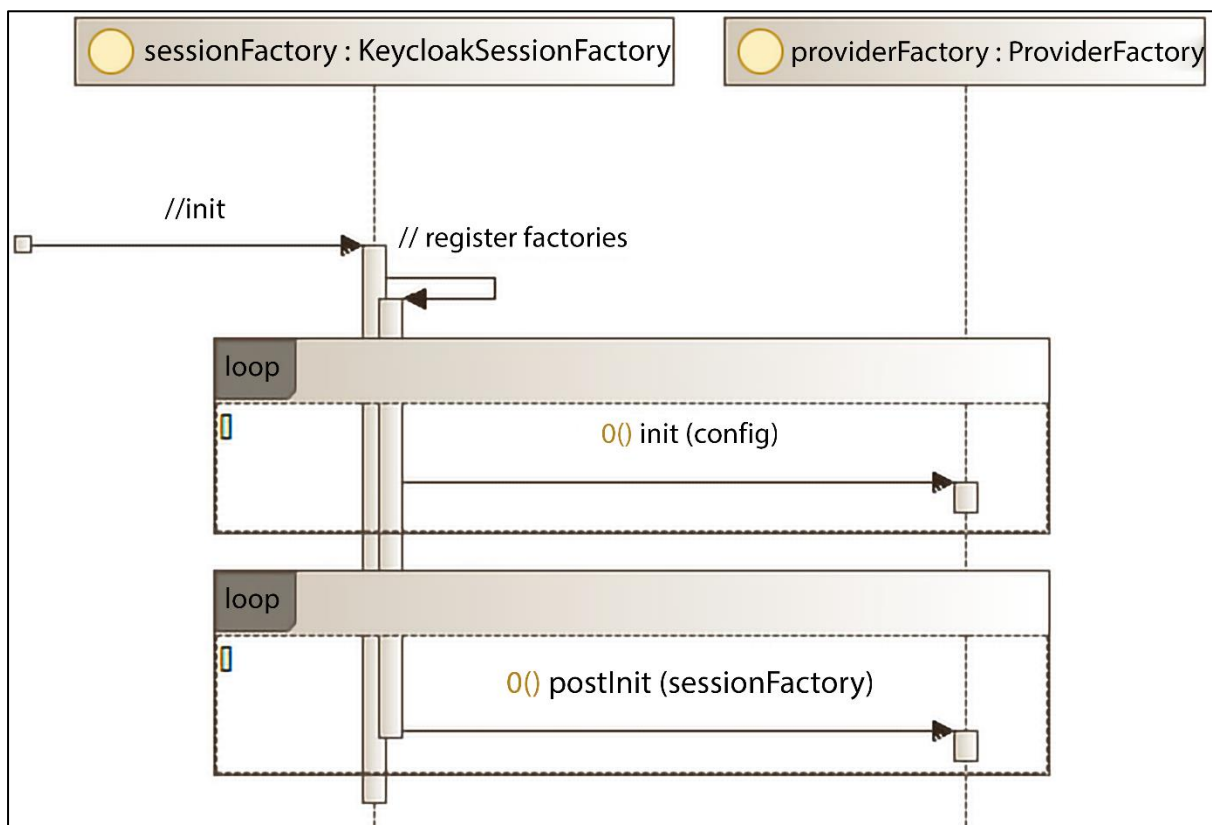
master realm

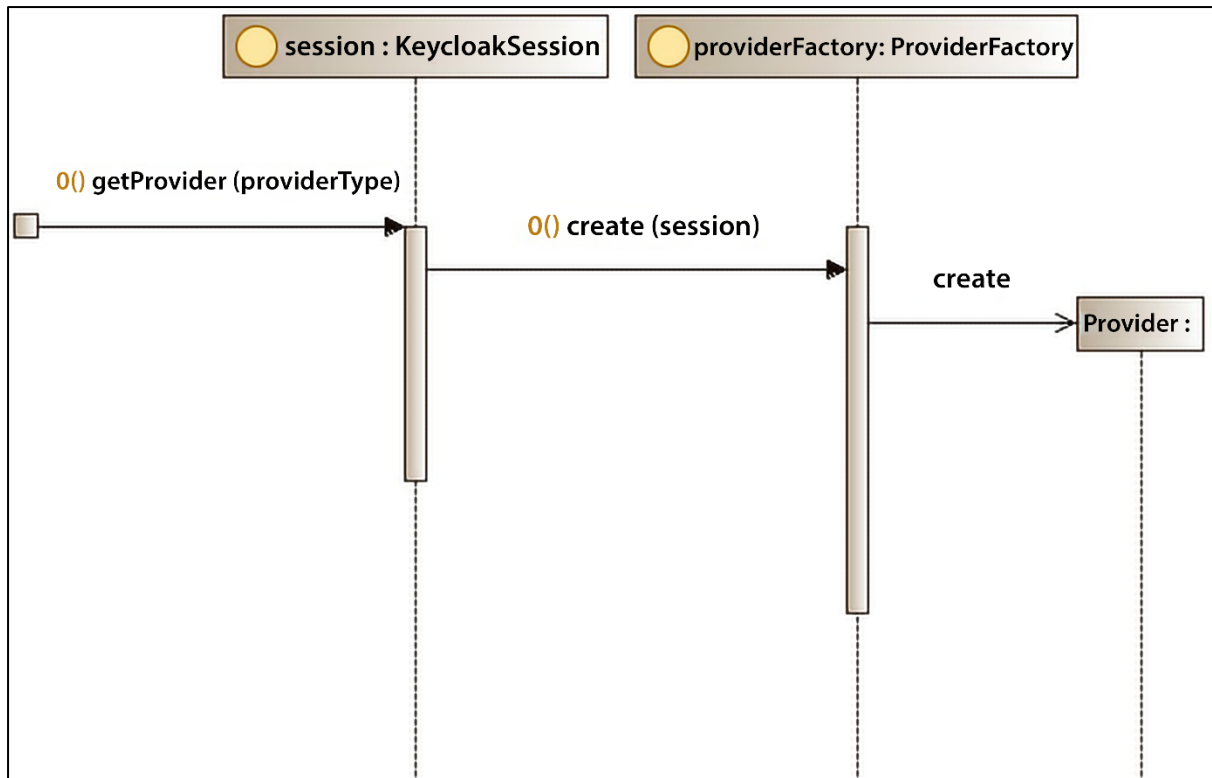
Server info

Provider info

SPI	Providers
social	github facebook google instagram linkedin bitbucket microsoft





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 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

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



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

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 Browser - 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 logout



Off

Wait increment

1



Minutes



Max wait

15



Minutes



Failure reset time

12



Hours



Quick login check
milliseconds

−

1000

+

Minimum quick login
wait

1



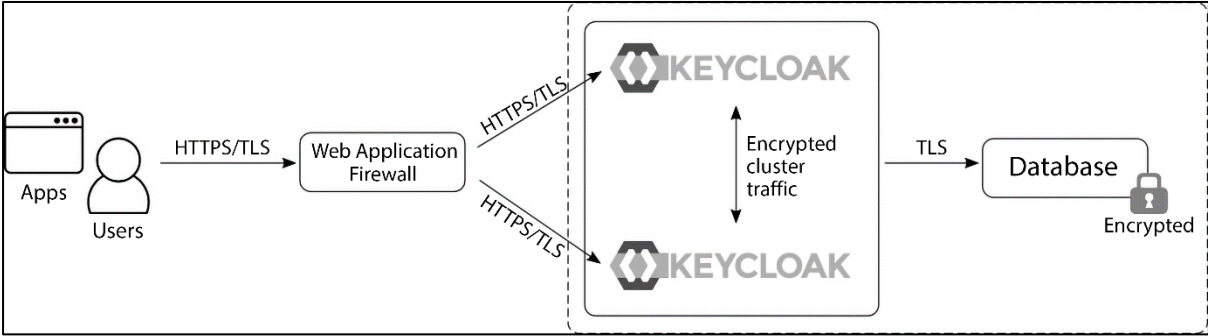
Minutes



Save

Revert

Chapter 14: Securing Keycloak and Applications



< General Login Email Themes Keys Events Localization Security defenses Sessions Tokens Client >				
Keys listProviders				
Active keys Search key → 1-4 < >				
Algorithm	Type	Kid	Provider	Public keys
RSA-OAEP	RSA	rj0VU554iTBIAZzPBDt4yr_XGL3KJAYRdzbK99aMeKQ	rsa-enc-generated	Public keyCertificate
AES	OCT	c42814bb-8b61-4a74-926f-a1eb590e5c50	aes-generated	
RS256	RSA	2csknI6J3mAYjNUgpvGjIC_378VH0hIStcJ_JvCOV9c	rsa-generated	Public keyCertificate
HS256	OCT	c2e33f29-6f2c-4acf-b657-7141b4d313d5	hmac-generated	
1-4 < >				

Add provider

Name

rsa-generated-2

Priority

200

Enabled

On

Active

On

Key size

2048

Algorithm

RS256

Save

Cancel

<

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client

>

Keys list

Providers

Active keys

RS256

1-2

Algorithm	Type	Kid	Provider	Public keys
RS256	RSA	HN5qkKYqN5Tj0l1re4r4P56TzicWViFRJqSjH-hd7Wo	rsa-generated-2	Public key Certificate
RS256	RSA	2csknI6J3mAYjNUgppvGjIC_378VH0hIStcJ_JvCOV9c	rsa-generated	Public key Certificate

1-2

Flows

Required actions

Policies

Password policy

OTP Policy

Webauthn Policy

Webauthn Passwordless Policy

Add policy

Minimum Length * ?

-

8

+

Special Characters * ?

-

1

+

Uppercase Characters * ?

-

1

+

Lowercase Characters * ?

-

1

+

Digits * ?

-

1

+

<

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

S

Headers

Brute force detection

Enabled

On

Max login failures ?

-

30

+

Permanent lockout

Off

Wait increment ?

1

Minutes ▼

Max wait ?

15

Minutes ▼

Failure reset time ?

12

Hours ▼

Quick login check milliseconds ?

-

1000

+

Minimum quick login wait ?

1

Minutes ▼

Save

Revert

Access settings

Root URL [?](#)

Home URL [?](#)

Valid redirect URIs [?](#)



[+ Add valid redirect URIs](#)

Valid post logout
redirect URIs [?](#)



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

Web origins [?](#)



[+ 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 [?](#)