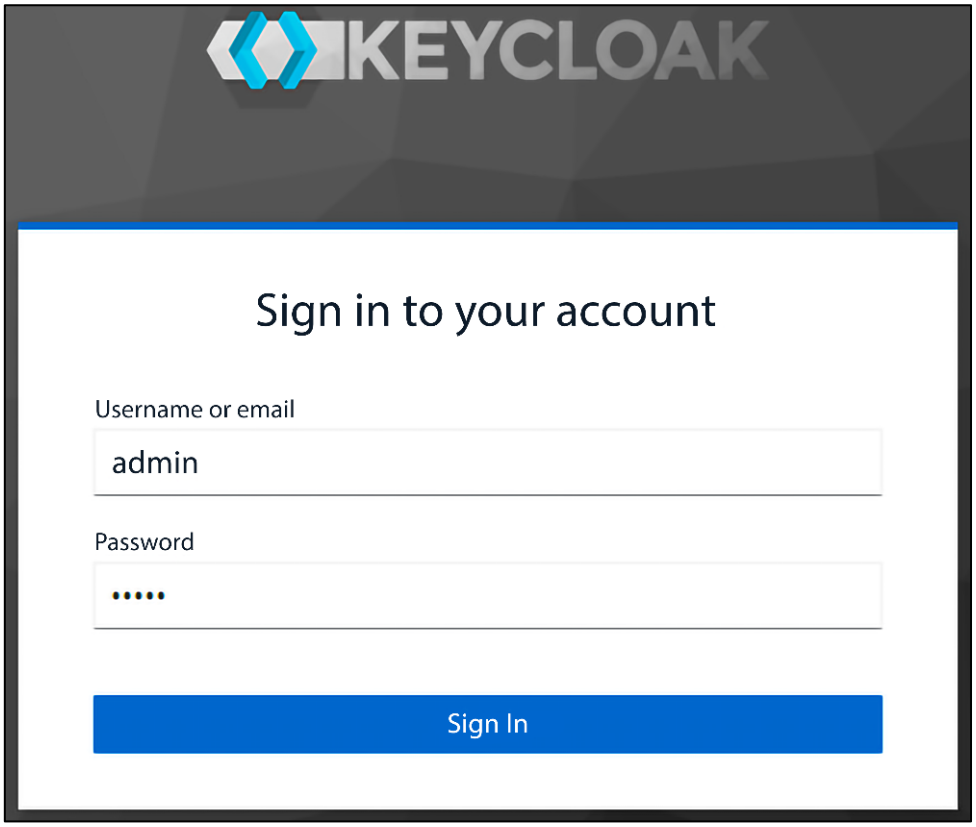
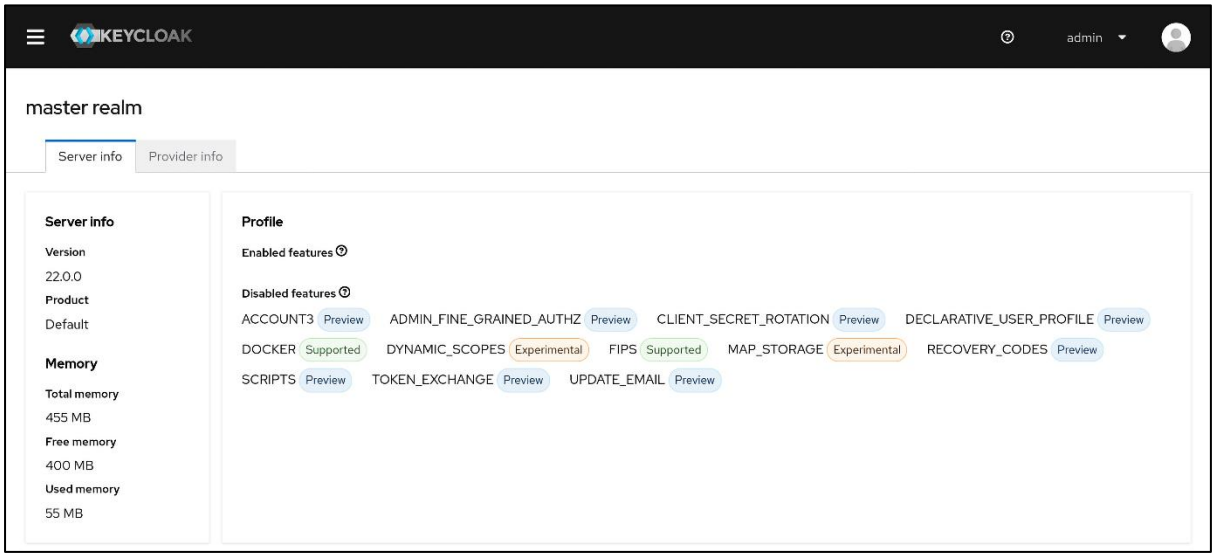
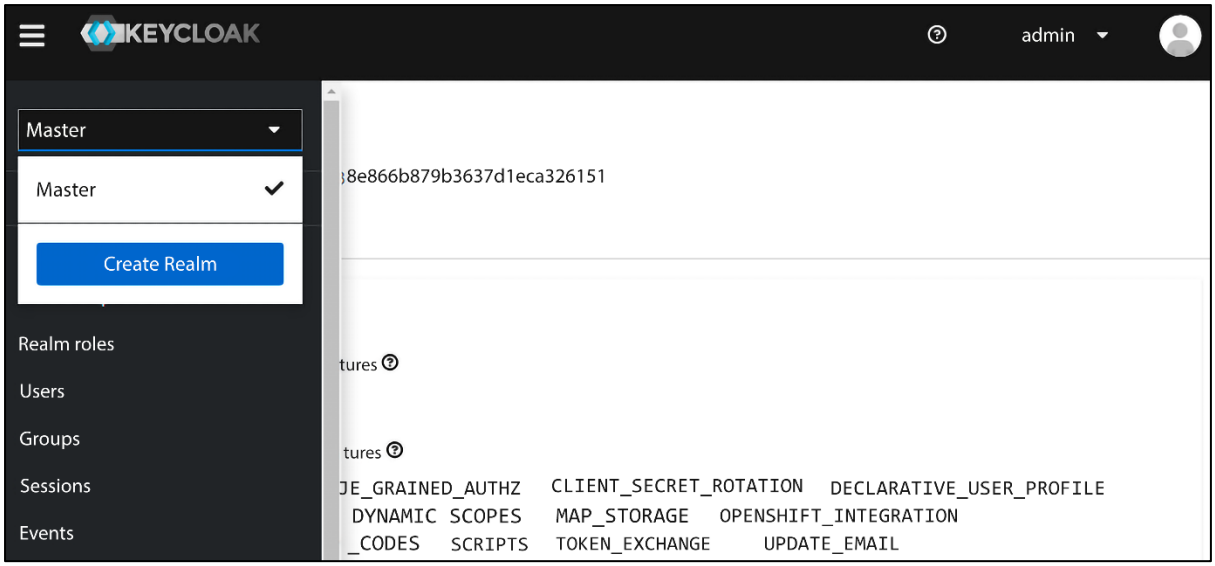
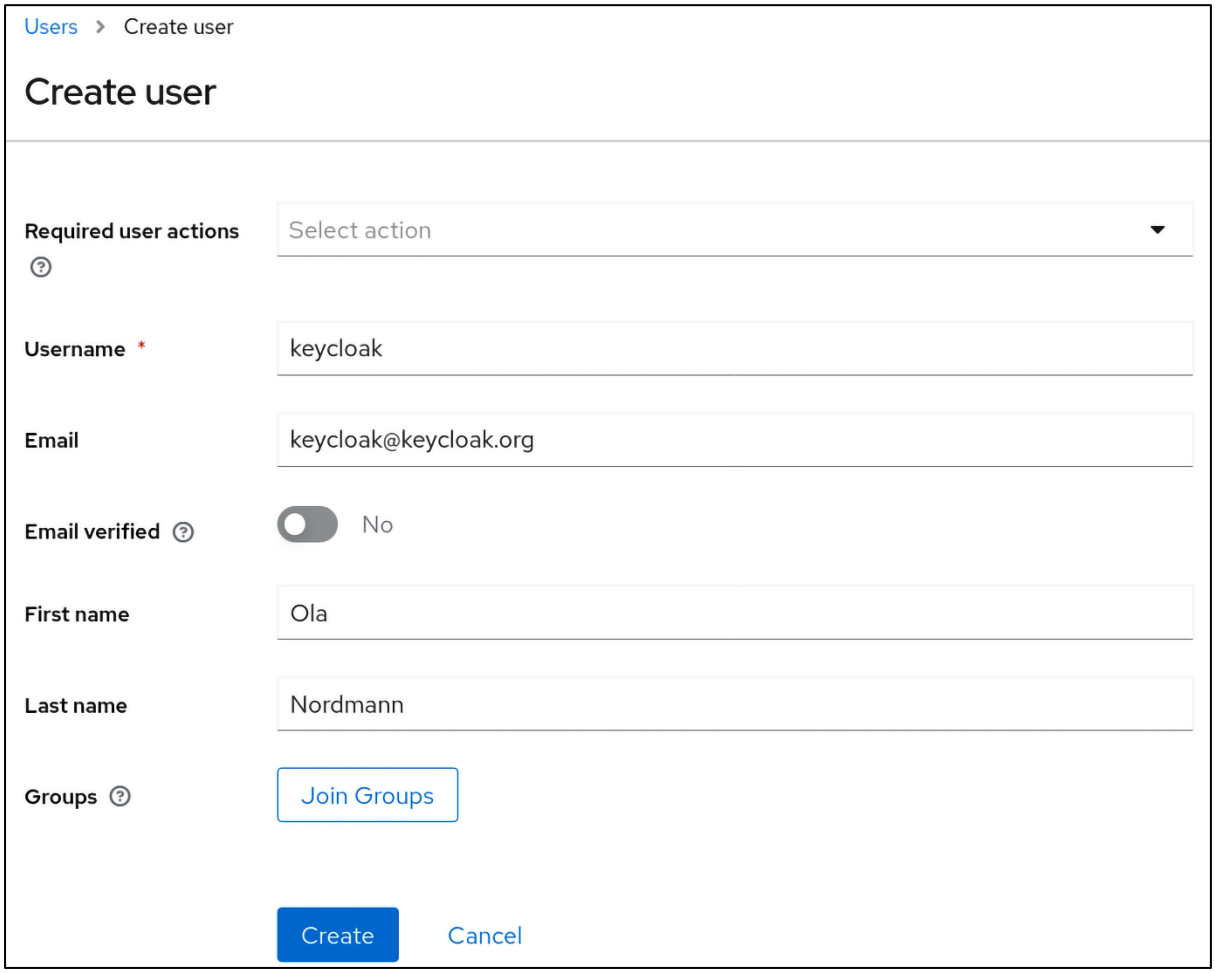
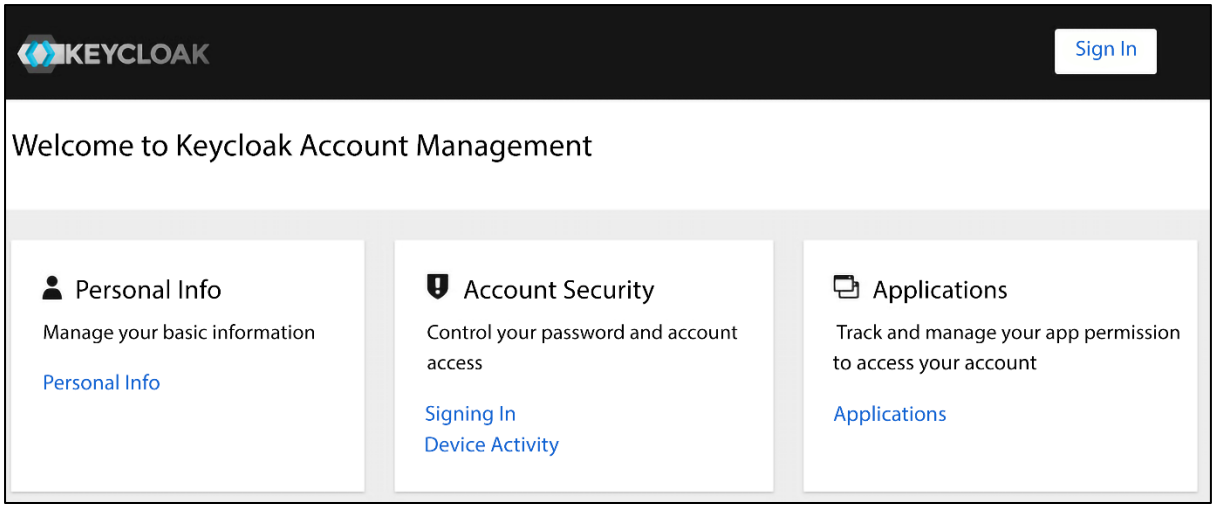
Chapter 1: Getting Started with Keycloak



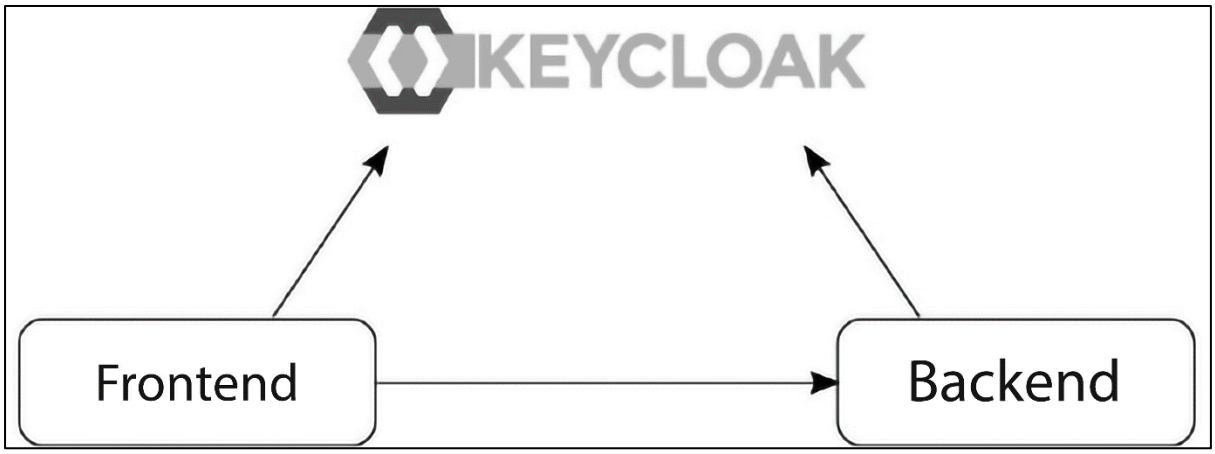


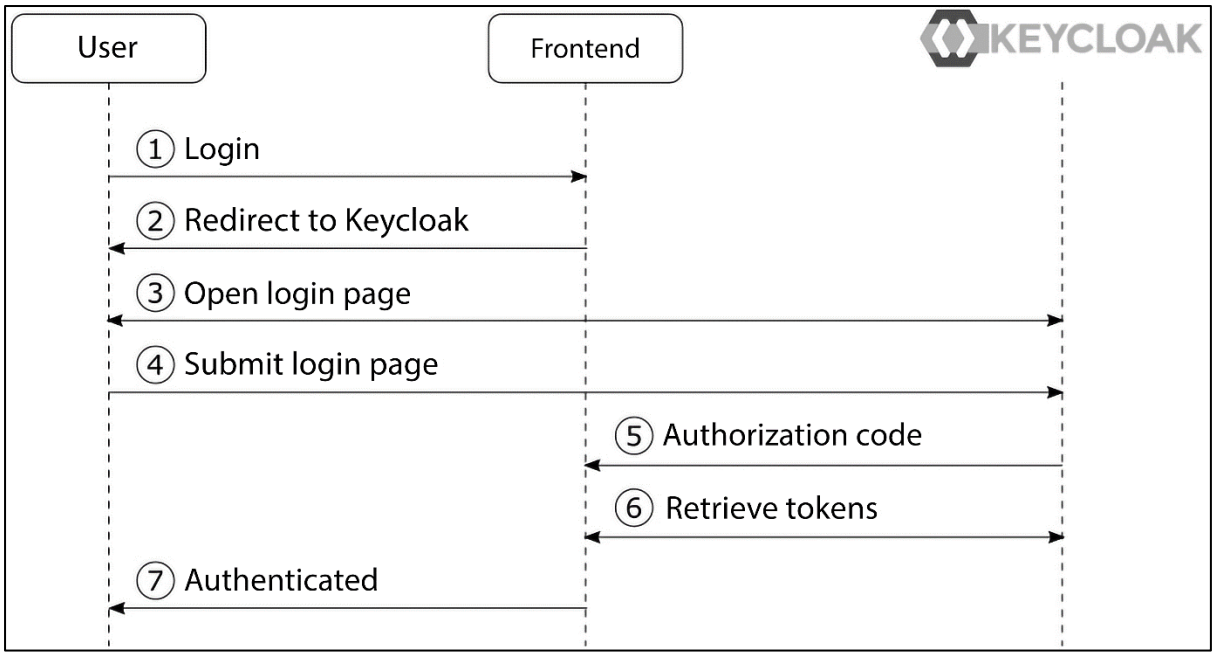

KEYCLOAK
admin
Master
Master
Create Realm
Realm roles
Users
Groups
Sessions
Events
8e866b879b3637d1eca326151
tures
tures
JE_GRAINED_AUTHZ
CLIENT_SECRET_ROTATION
DECLARATIVE_USER_PROFILE
DYNAMIC SCOPES
MAP_STORAGE
OPENSHIFT_INTEGRATION
_CODES
SCRIPTS
TOKEN_EXCHANGE
UPDATE_EMAIL

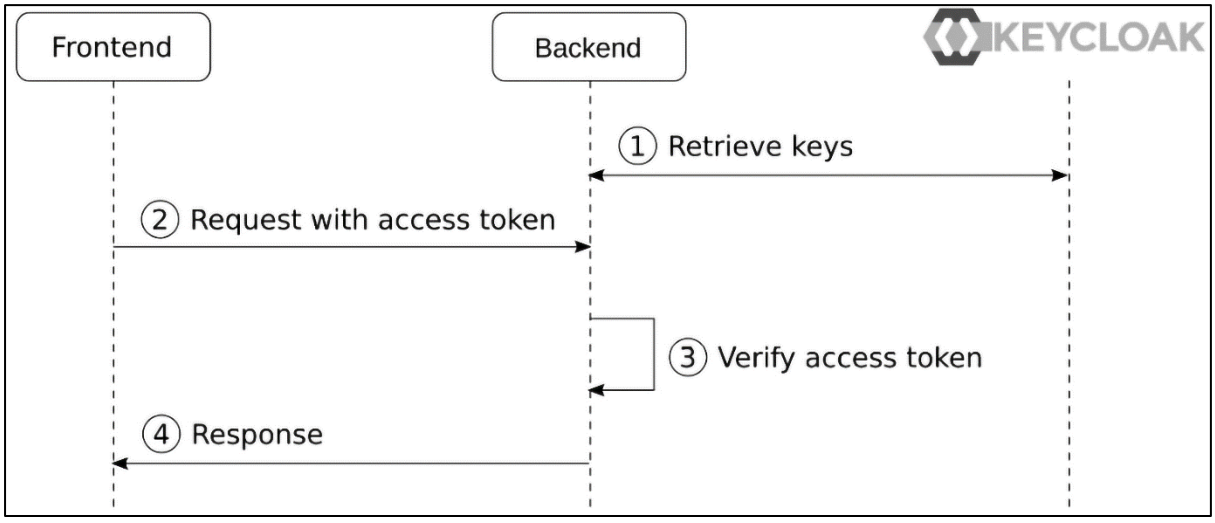

Users
Create user
Create user
Required user actions
Select action
Username *
keycloak
Email
keycloak@keycloak.org
Email verified
No
First name
Ola
Last name
Nordmann
Groups
Join Groups
Create
Cancel

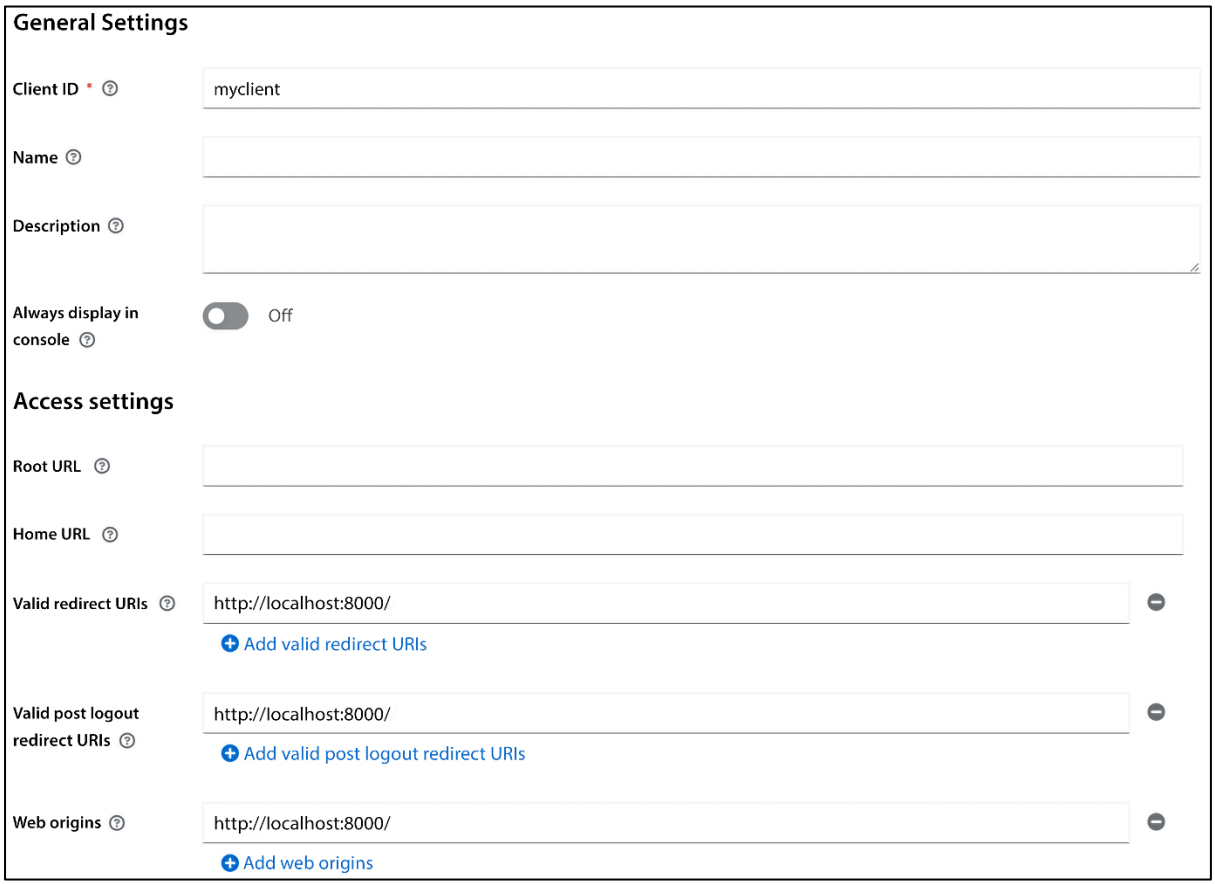

KEYCLOAK
Sign In
Welcome to Keycloak Account Management
Personal Info
Manage your basic information
Personal Info
Account Security
Control your password and account access
Signing In
Device Activity
Applications
Track and manage your app permission to access your account
Applications

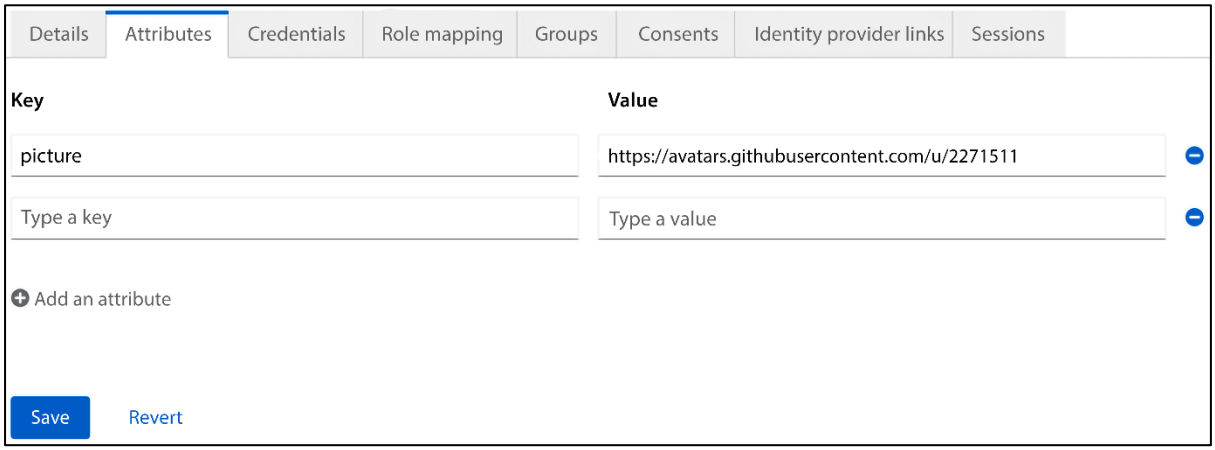
Chapter 2: Securing Your First Application



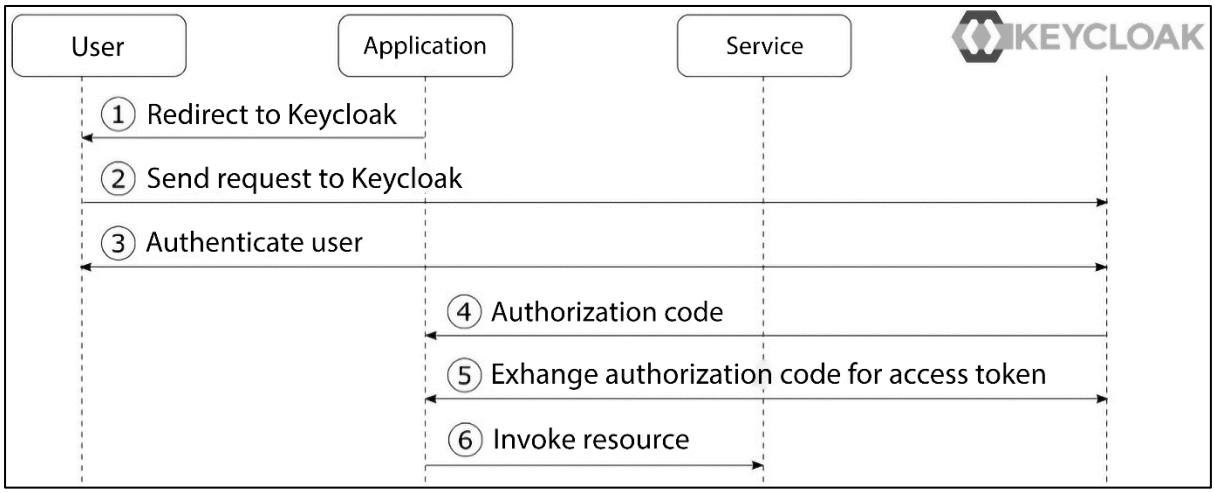


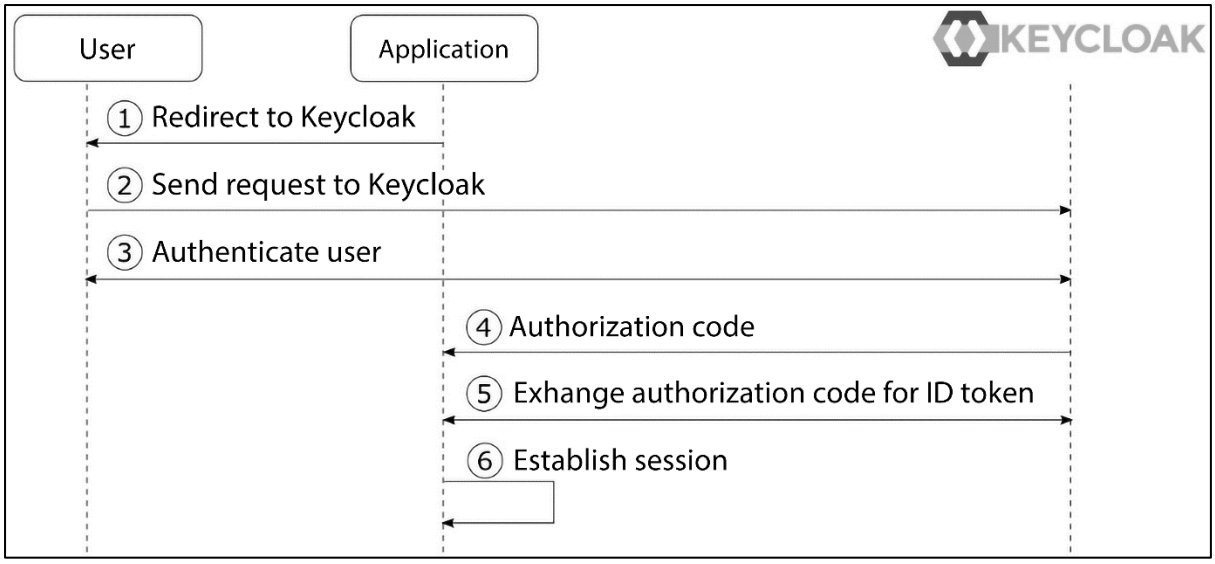


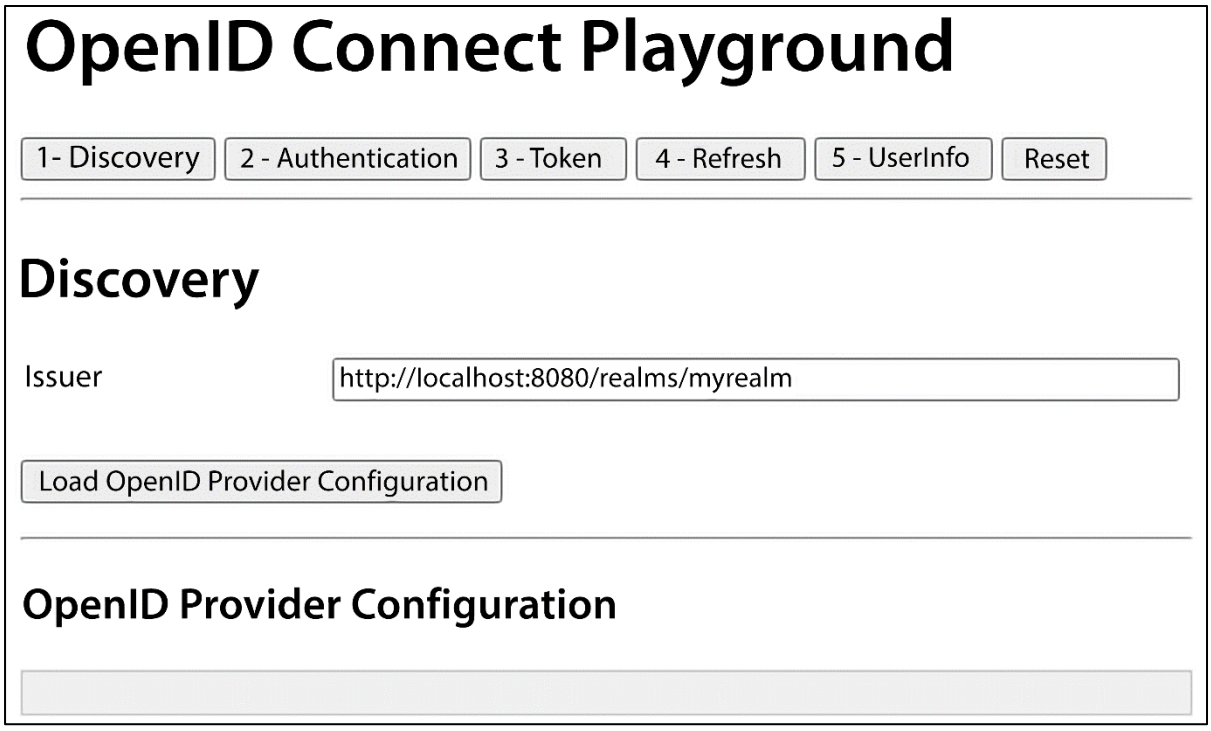

General Settings
Client ID *
myclient
Name
Description
Always display in console
Off
Access settings
Root URL
Home URL
Valid redirect URIs
http://localhost:8000/
Add valid redirect URIs
Valid post logout redirect URIs
http://localhost:8000/
Add valid post logout redirect URIs
Web origins
http://localhost:8000/
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

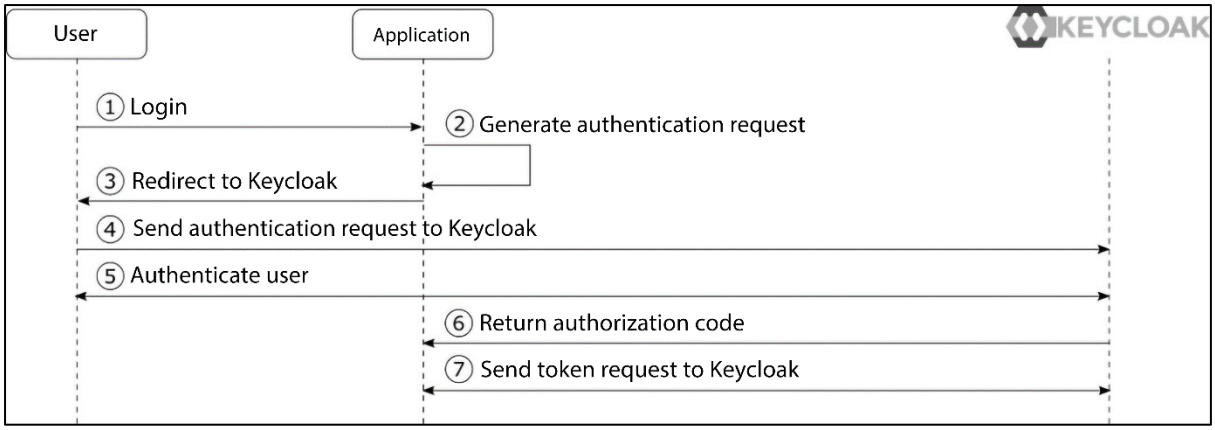






OpenID Provider Configuration


```
{
  "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/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-986e1cfladd7
client_id=oidc-playground
redirect_uri=http://localhost:8000/
```

Token Response


```
{
  "access_token": "eyJhbGci0iJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabX
  "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/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": "pWygiLi18hq3gIpd8-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-i79IzxBoyOOYKEK9cmKaDoAy0G-0DA7zVYirbEYhkPv66C6MAUQu4EmXzJ73-aM3xdngEPUA0rYSgg-PHkiYug3IiJgDyc-
```


Refresh Request


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

grant_type=refresh_token
refresh_token=eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJkMTAzMTcxYillMzA5LTQ1NWYtYWJhZiliYjk2NTQxYTAyMjkifQ
client_id=oidc-playground
scope=openid
```


Refresh Response


```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUliwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKWFpzTW8tTmxzSVIFGQj1KcVlabX
  "expires_in". 300,
  "refresh_expires_in": 1800,
  "refresh_token": "eyJhbGciOiJIUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJkMTAzMTcxYillMzA5LTQ1NWYtYWJZiliYjk2NTQxYTAyM
  "token_type": "Bearer",
  "id_token": "eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmmiSFBkVFU4TmNKWFpzTW8tTmxzSWFGQj1KcVlabXkObV
  "not-before-policy": 0,
  "session_state": "3b403853-8afa-4b0a-9f29-84b689768d1a",
  "scope": "openid profile email"
}
```

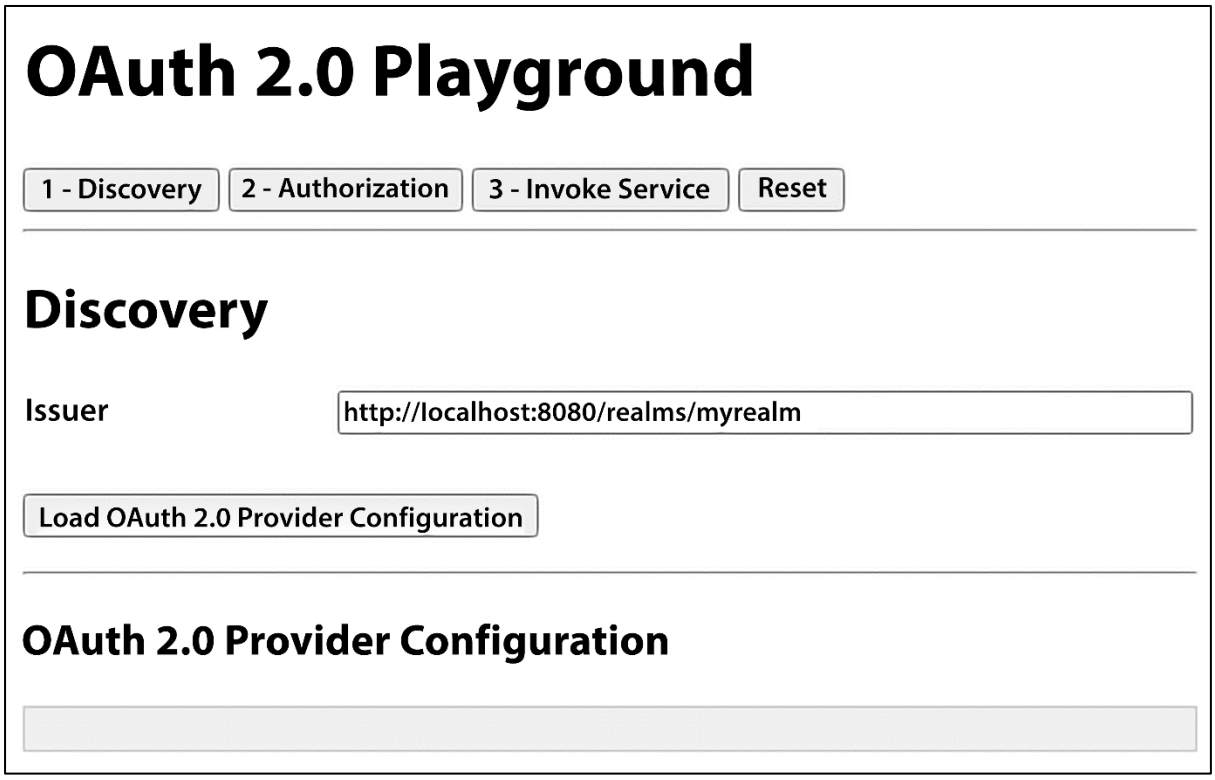
UserInfo Request

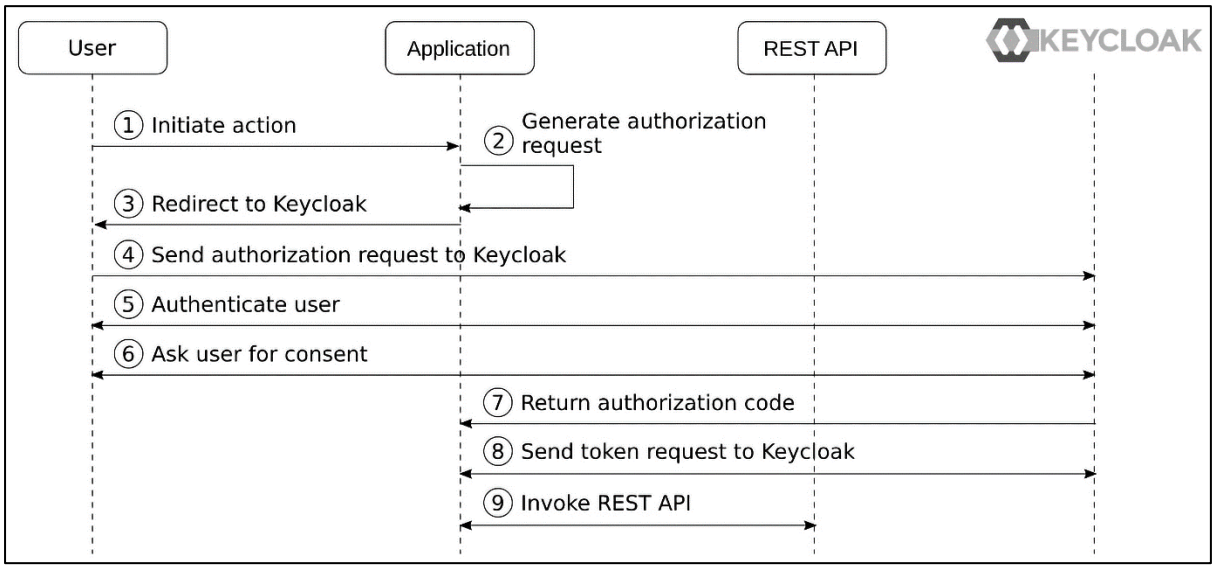
```
http://localhost:8080/realms/myrealm/protocol/openid-connect/userinfo

Authorization: Bearer eyJhbGciOiJSUzIlNiIsInR5cCIgOiAiSldUIiwia21kIiA6ICJNU1JhVmwwSFBkVFU4TmNKW
```

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





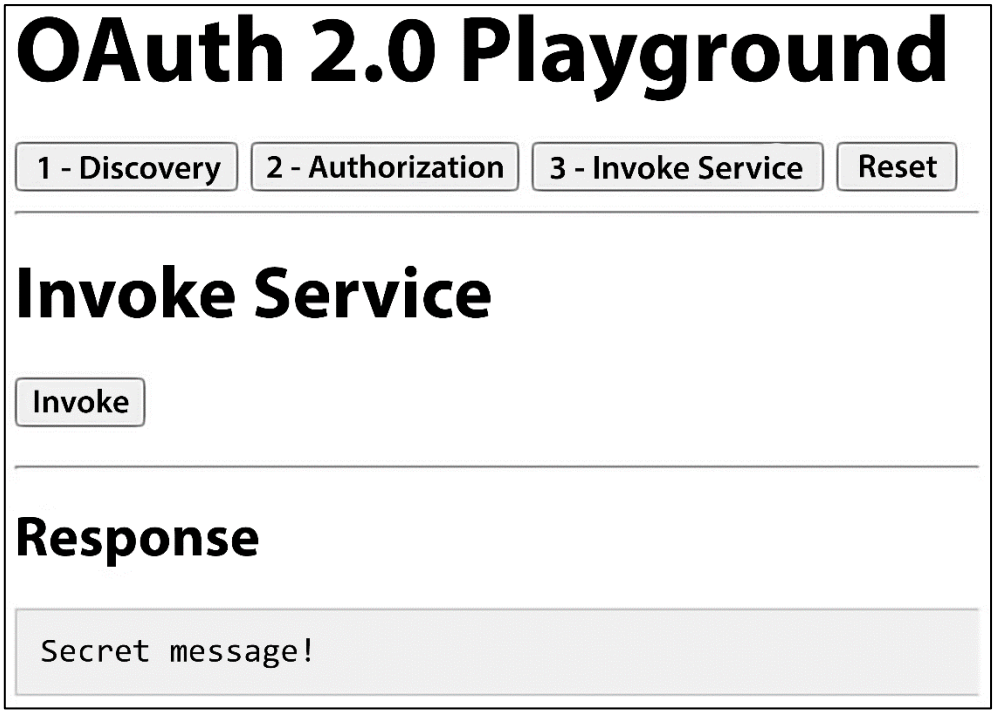
Access Token

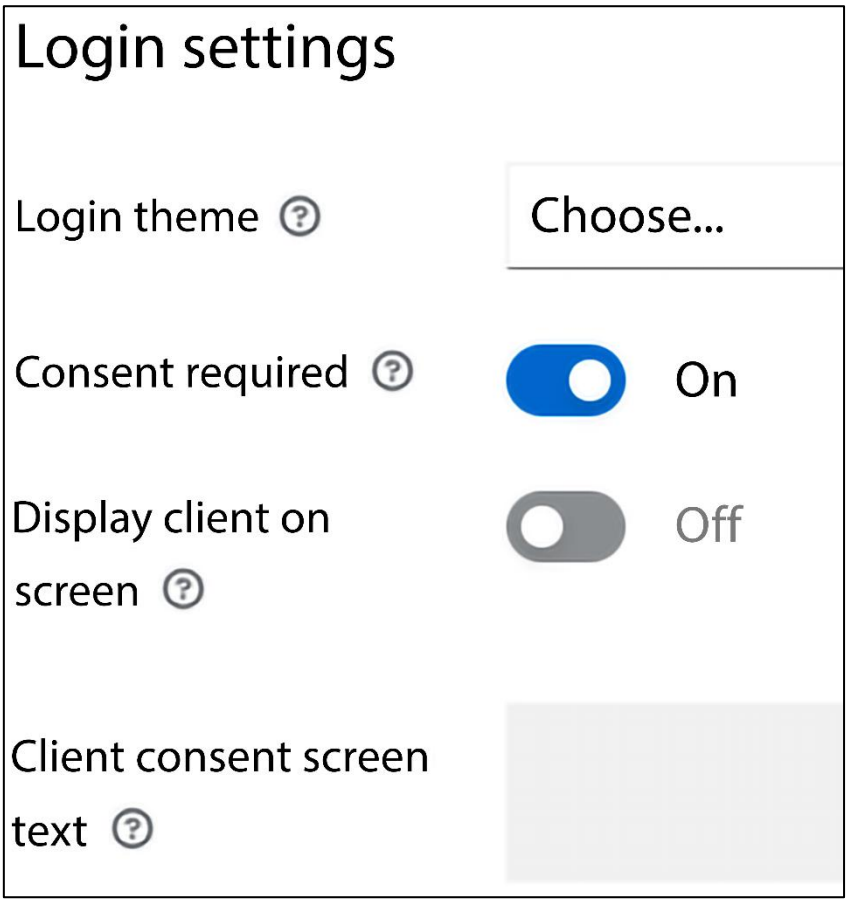
Header

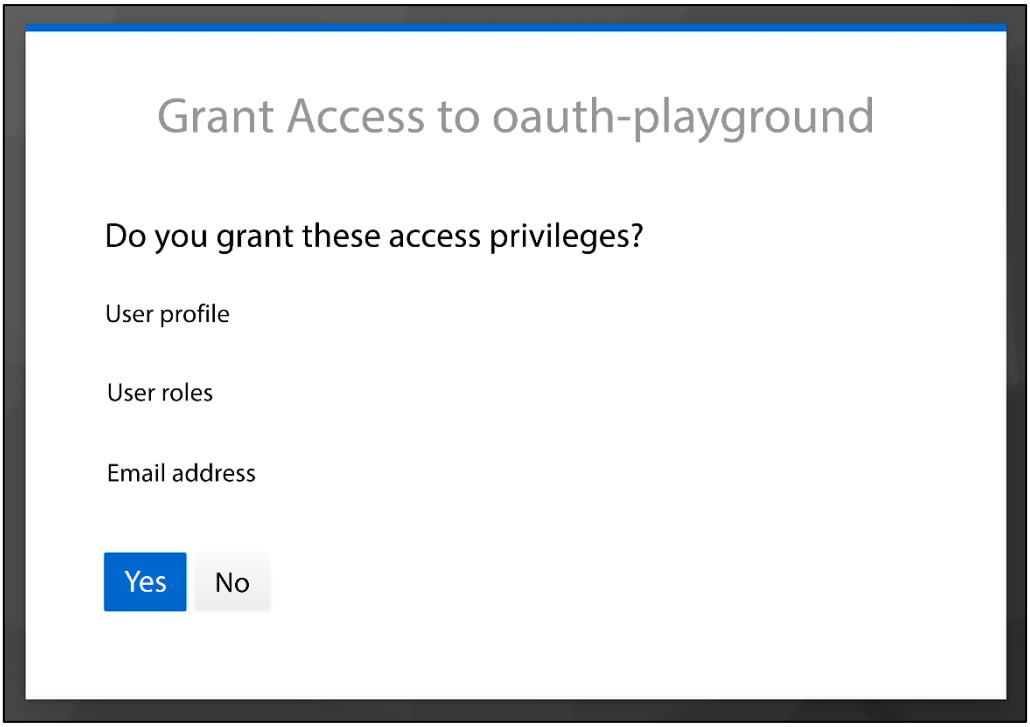

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "JI0_xxUiSi7oUkx0xLQe8xsdRTnKOirURnBuik6EyyQ"
}
```

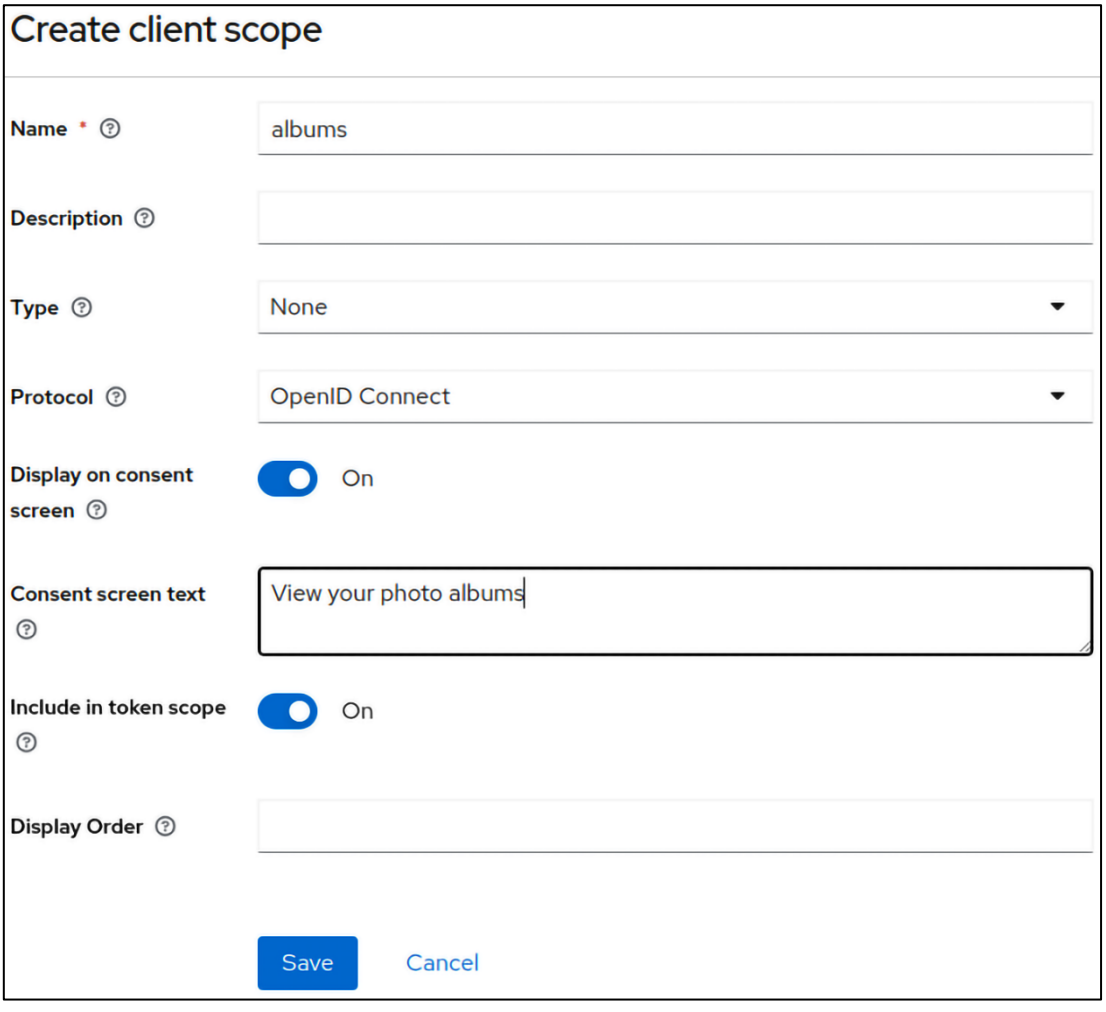

Payload

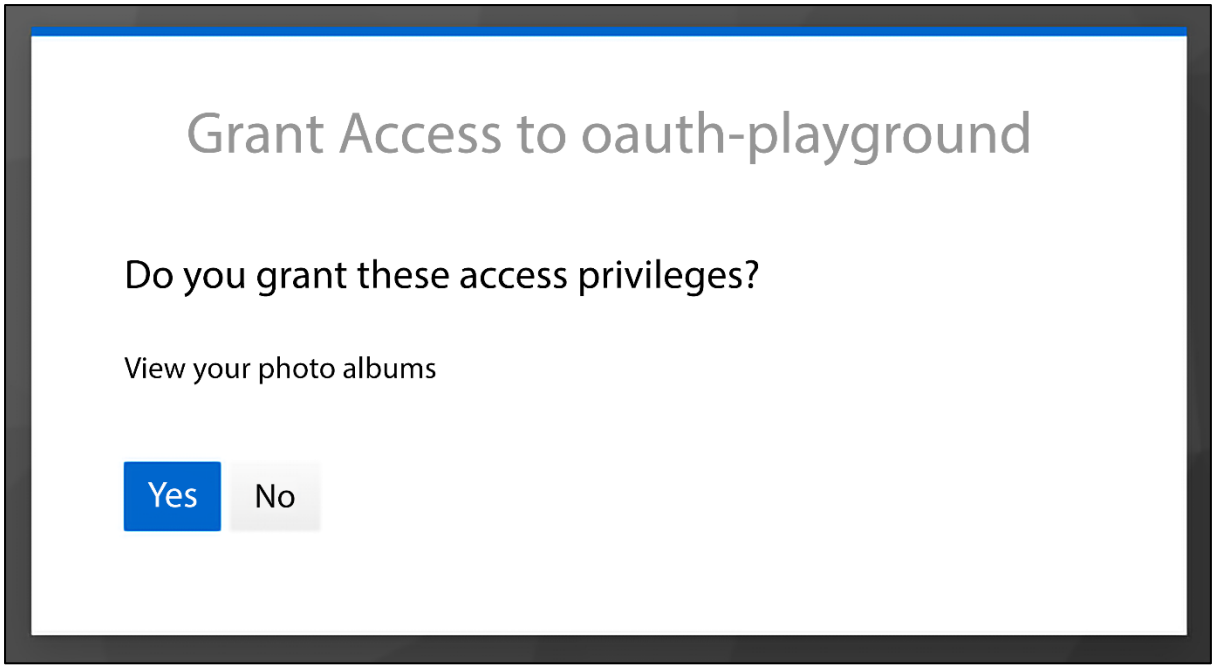

```
{
  "exp": 1667145073,
  "iat": 1667144773,
  "auth_time": 1667144773,
  "jti": "dc6caecb-7f4e-49c6-a9ed-bf2fd5af0db0",
  "iss": "http://localhost:8080/realms/myrealm",
  "aud": "account",
  "sub": "f89a8358-de60-4238-883b-9143af28c56b",
  "typ": "Bearer",
  "azp": "oauth-playground",
  "session_state": "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!

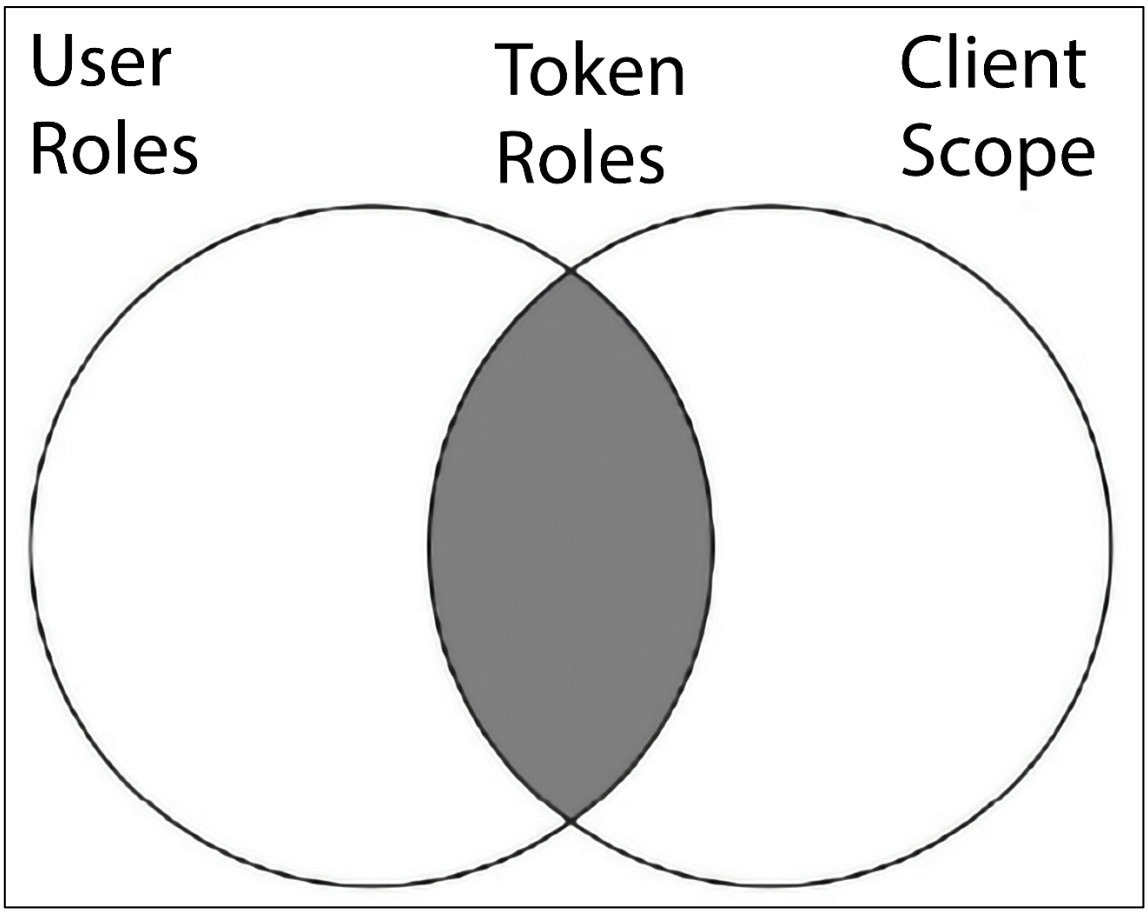

Login settings
Login theme
Choose...
Consent required
On
Display client on screen
Off
Client consent screen text

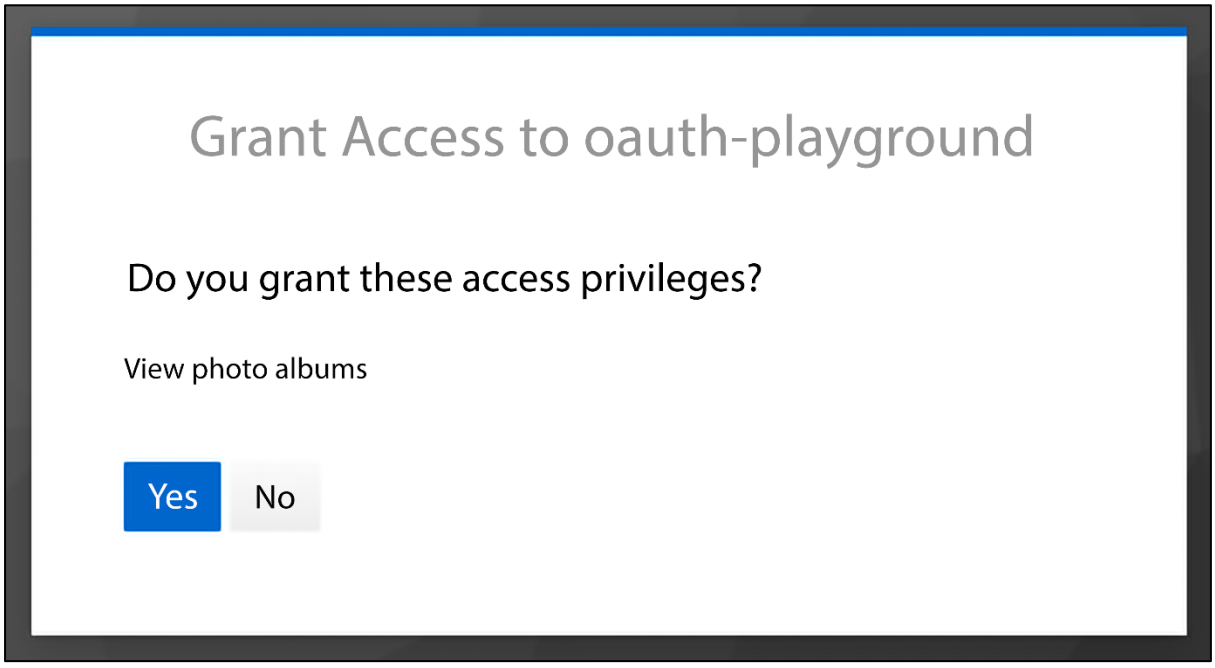

Grant Access to oauth-playground
Do you grant these access privileges?
User profile
User roles
Email address
Yes
No


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



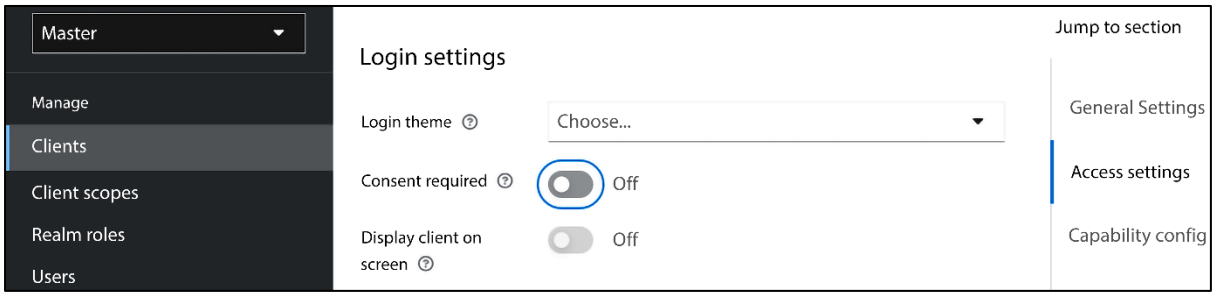

```
{
  "realm": "myrealm",
  "bearer-only": true,
  "auth-server-url": "${env.KC_URL:http://localhost:8080/auth}",
  "resource": "oauth-backend",
  "verify-token-audience": true
}
```

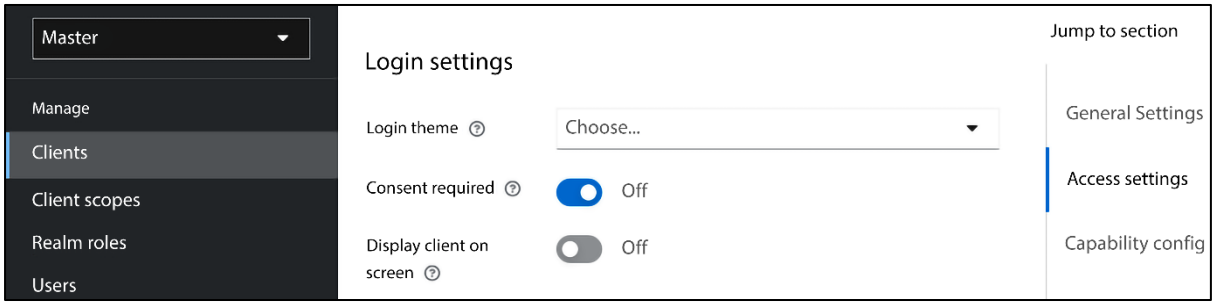

User
Roles
Token
Roles
Client
Scope

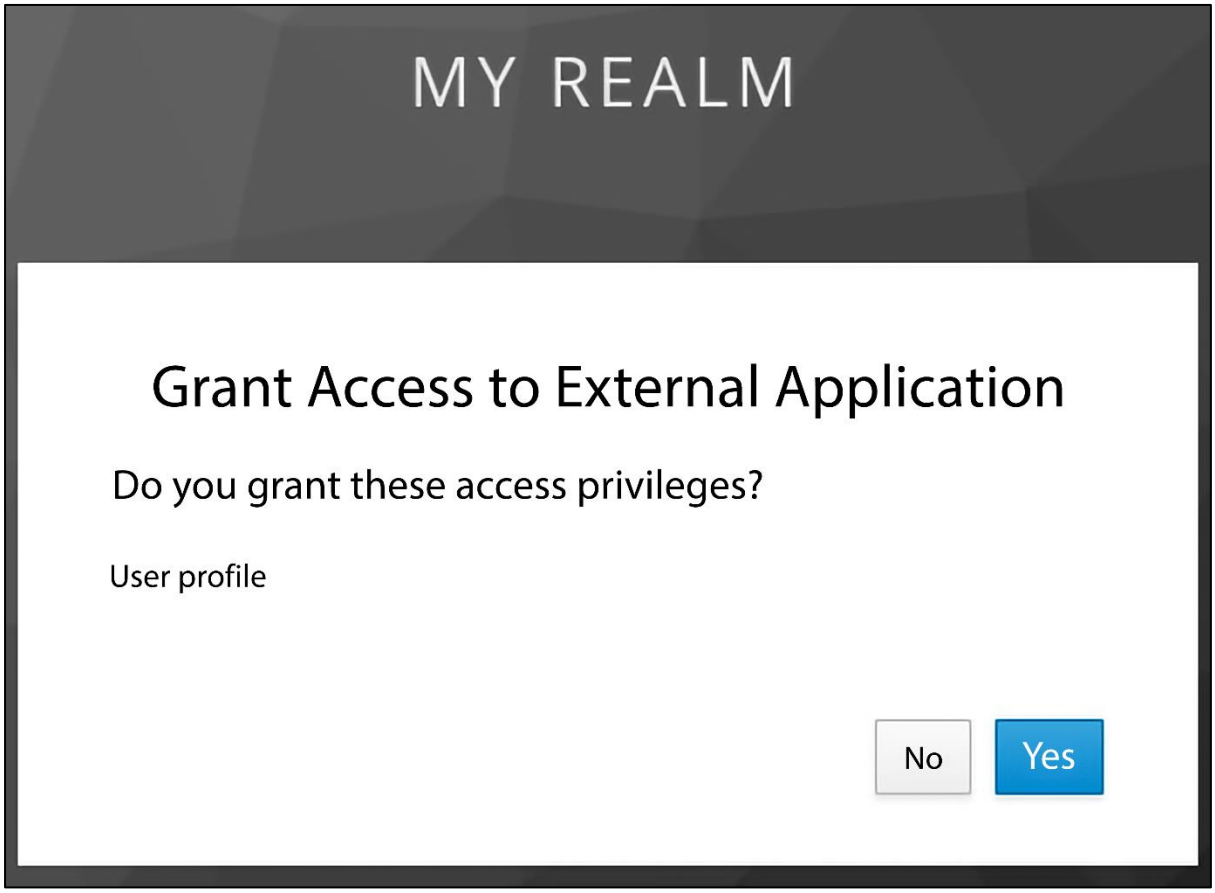

Grant Access to oauth-playground
Do you grant these access privileges?
View photo albums
Yes
No

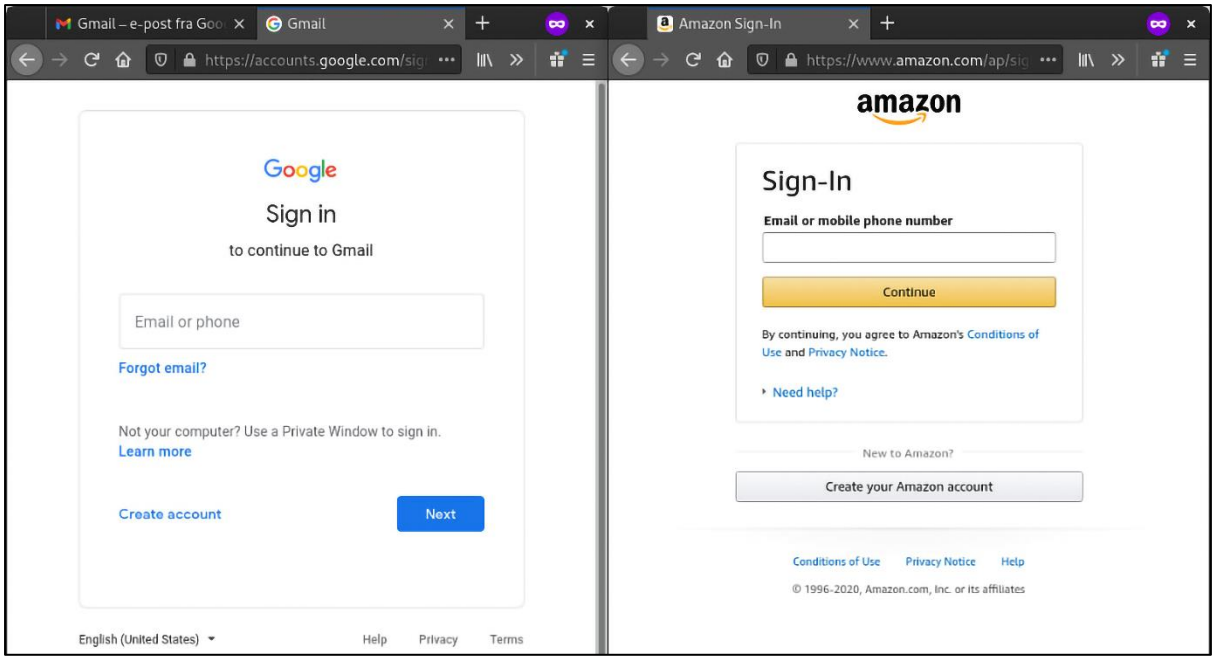
```
{
  "exp": 1667147808,
  "iat": 1667147508,
  "auth_time": 1667144773,
  "jti": "681209f3-0b87-4ef2-b68d-21d46f615fc5",
  "iss": "http://localhost:8080/realms/myrealm",
  "aud": "oauth-backend",
  "sub": "f89a8358-de60-4238-883b-9143af28c56b",
  "typ": "Bearer",
  "azp": "oauth-playground",
  "session_state": "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
}
```

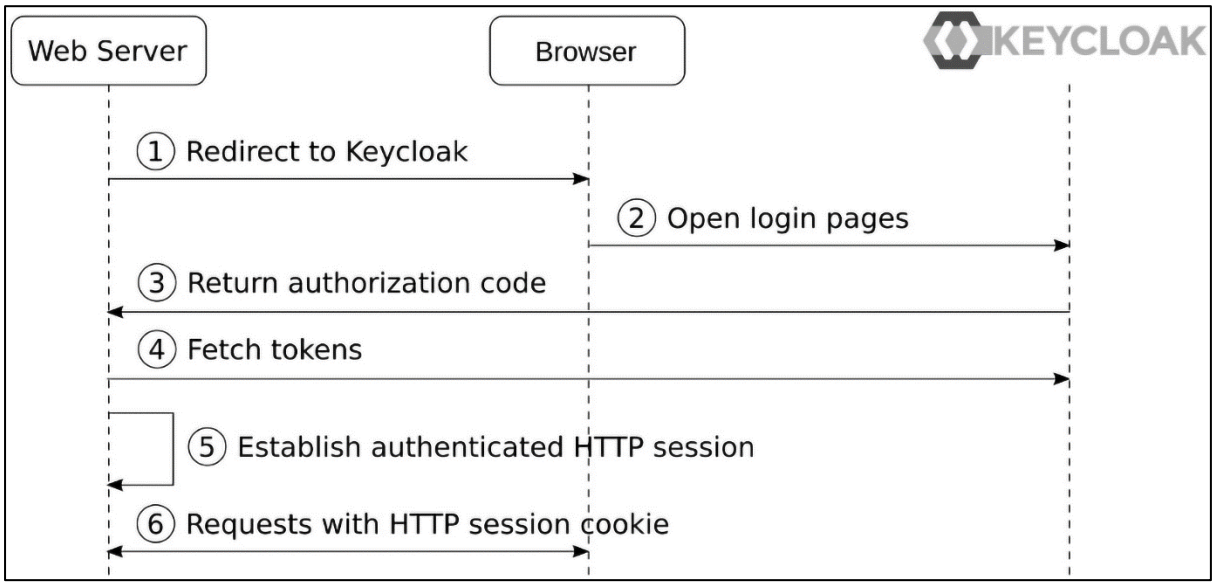
Chapter 6: Securing Different Application Types

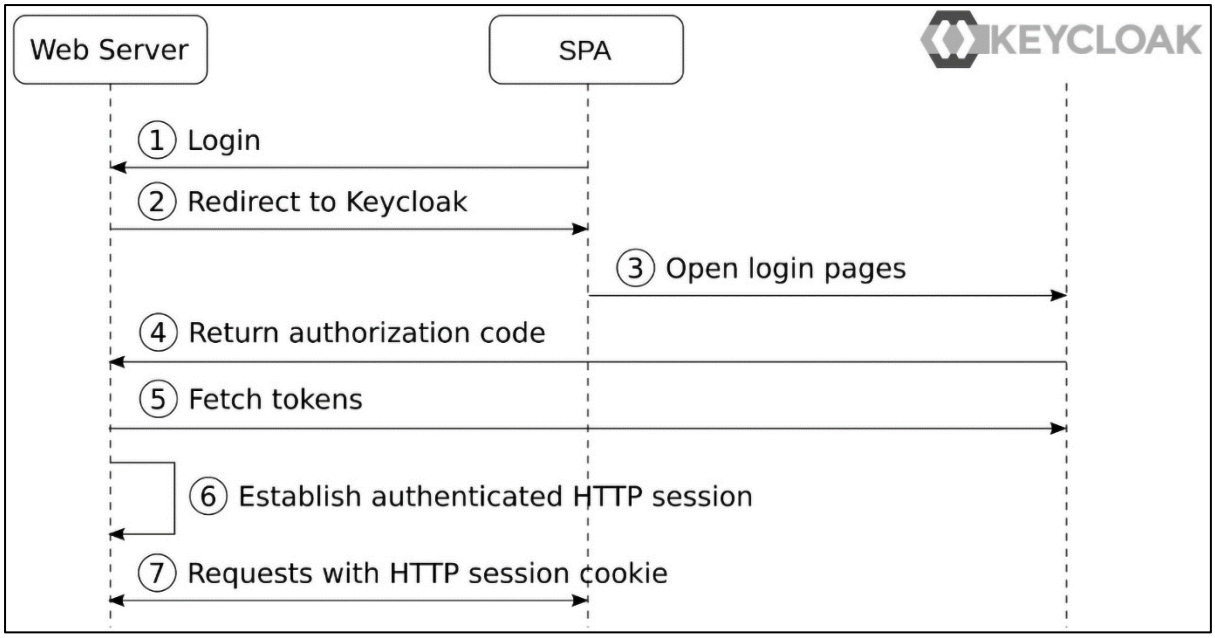


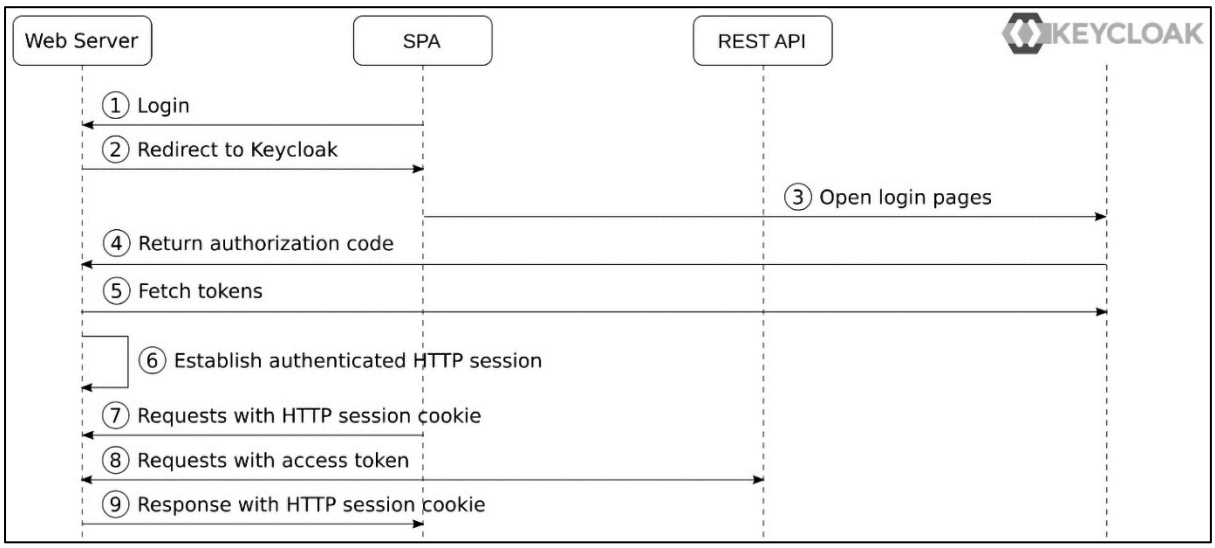


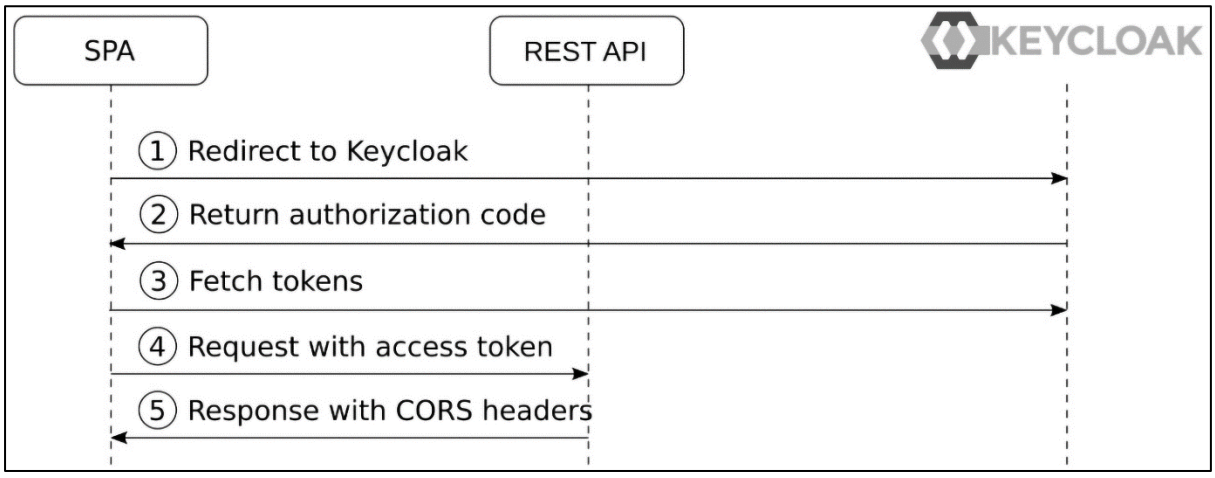


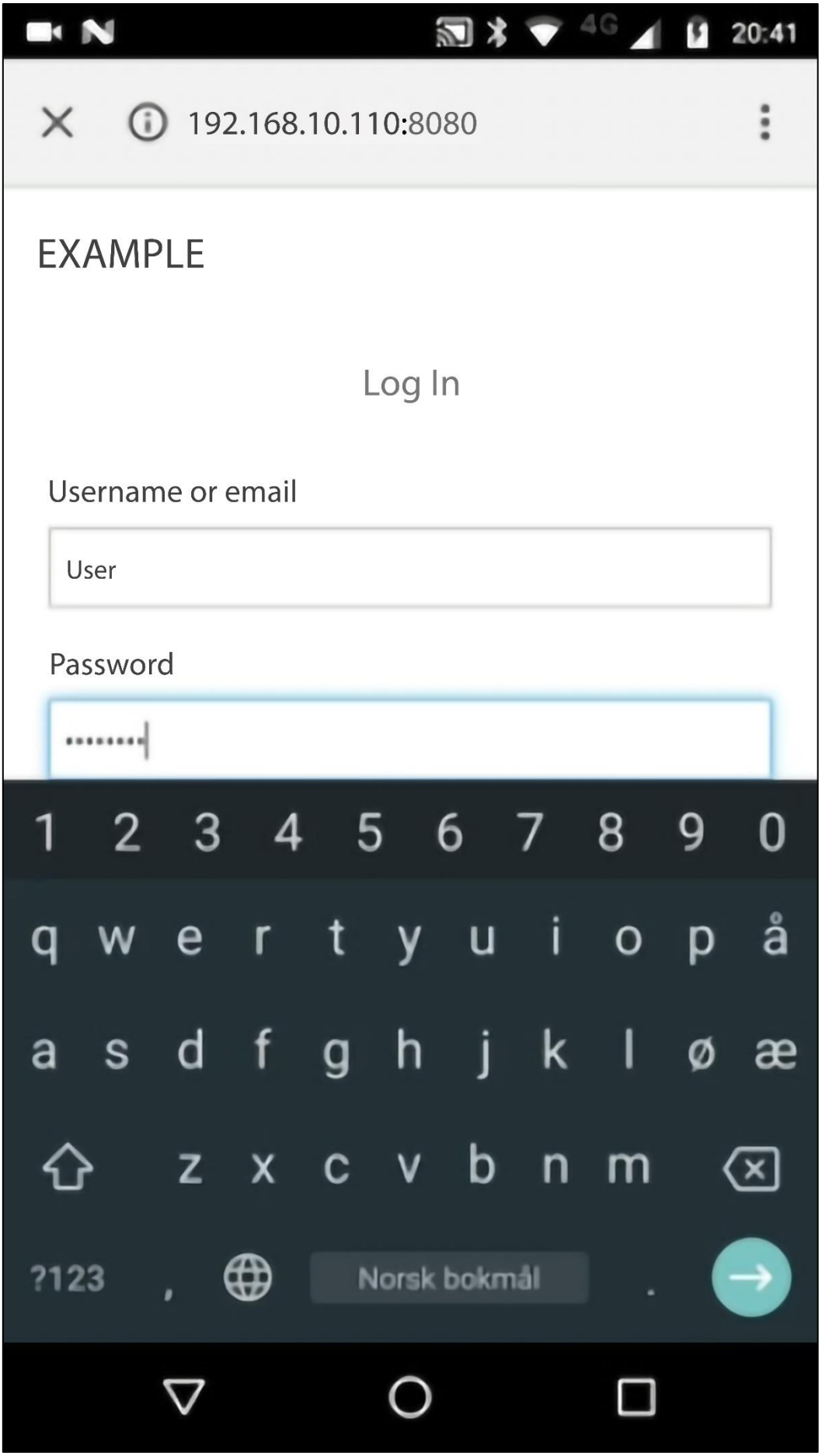

Gmail – e-post fra Goo
Gmail
https://accounts.google.com/sig
Google
Sign in
to continue to Gmail
Email or phone
Forgot email?
Not your computer? Use a Private Window to sign in.
Learn more
Create account
Next
English (United States)
Help
Privacy
Terms
Amazon Sign-In
https://www.amazon.com/ap/sig
amazon
Sign-In
Email or mobile phone number
Continue
By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.
Need help?
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2020, Amazon.com, Inc. or its affiliates

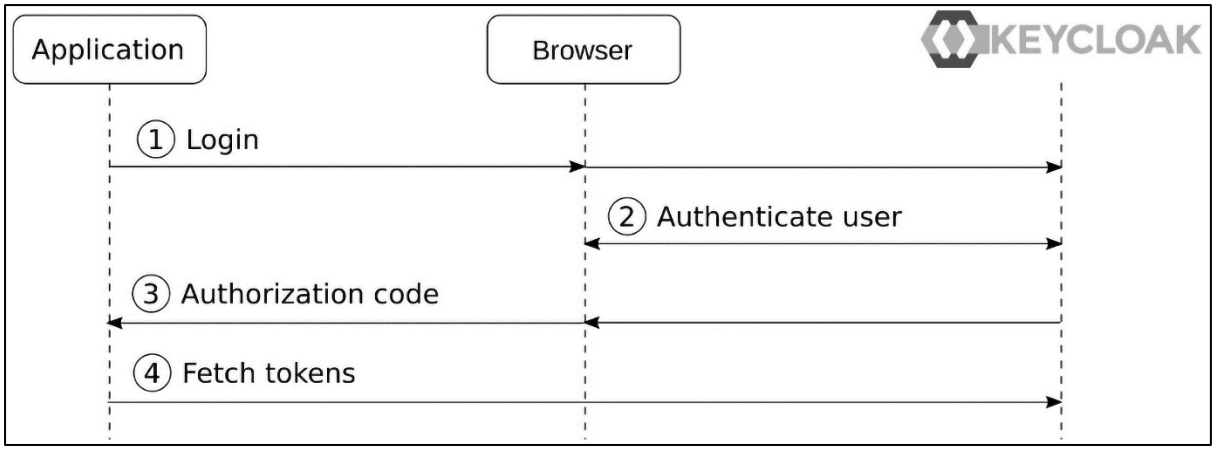

Web Server
Browser
KEYCLOAK
1 Redirect to Keycloak
2 Open login pages
3 Return authorization code
4 Fetch tokens
5 Establish authenticated HTTP session
6 Requests with HTTP session cookie

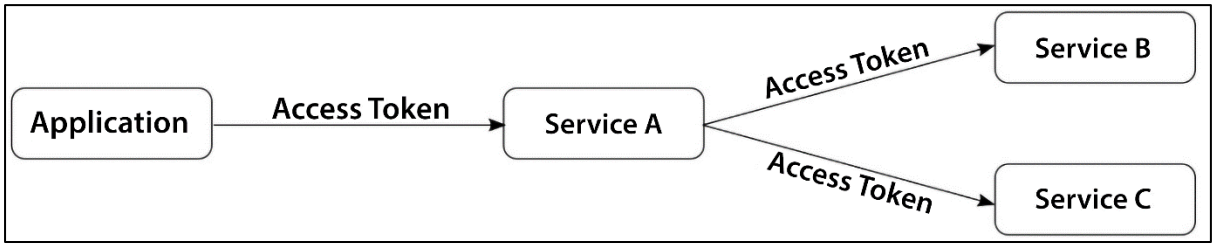

Web Server
SPA
KEYCLOAK
1 Login
2 Redirect to Keycloak
3 Open login pages
4 Return authorization code
5 Fetch tokens
6 Establish authenticated HTTP session
7 Requests with HTTP session cookie

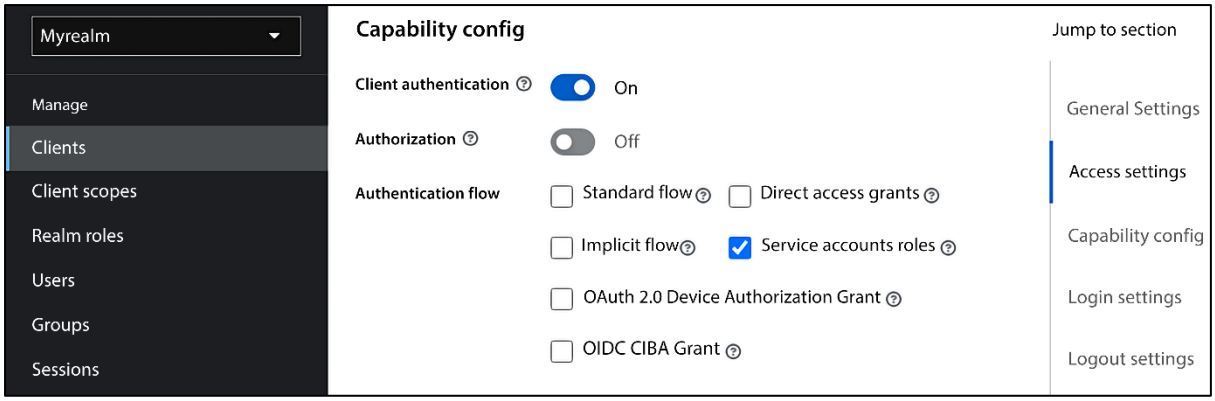

Web Server
SPA
REST API
KEYCLOAK
1 Login
2 Redirect to Keycloak
3 Open login pages
4 Return authorization code
5 Fetch tokens
6 Establish authenticated HTTP session
7 Requests with HTTP session cookie
8 Requests with access token
9 Response with HTTP session cookie


SPA
REST API
KEYCLOAK
1 Redirect to Keycloak
2 Return authorization code
3 Fetch tokens
4 Request with access token
5 Response with CORS headers

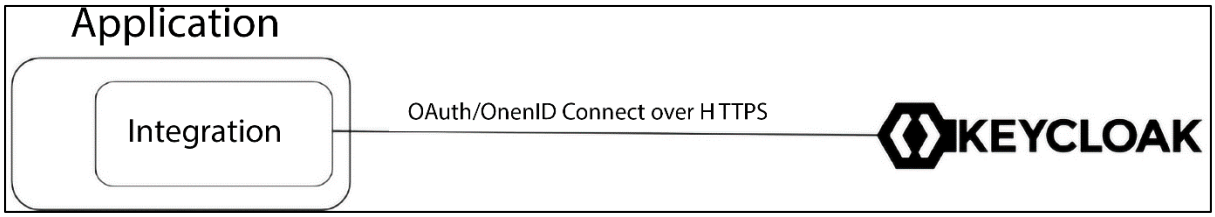

20:41
192.168.10.110:8080
EXAMPLE
Log In
Username or email
User
Password
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p å
a s d f g h j k l ø æ
z x c v b n m
?123
Norsk bokmål

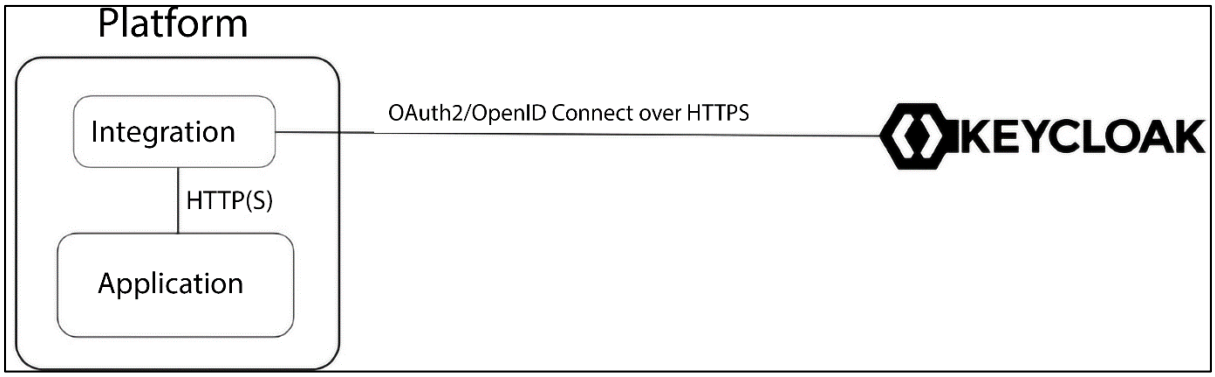

Application
Browser
KEYCLOAK
1 Login
2 Authenticate user
3 Authorization code
4 Fetch tokens


Application
Access Token
Service A
Access Token
Service B
Access Token
Service C

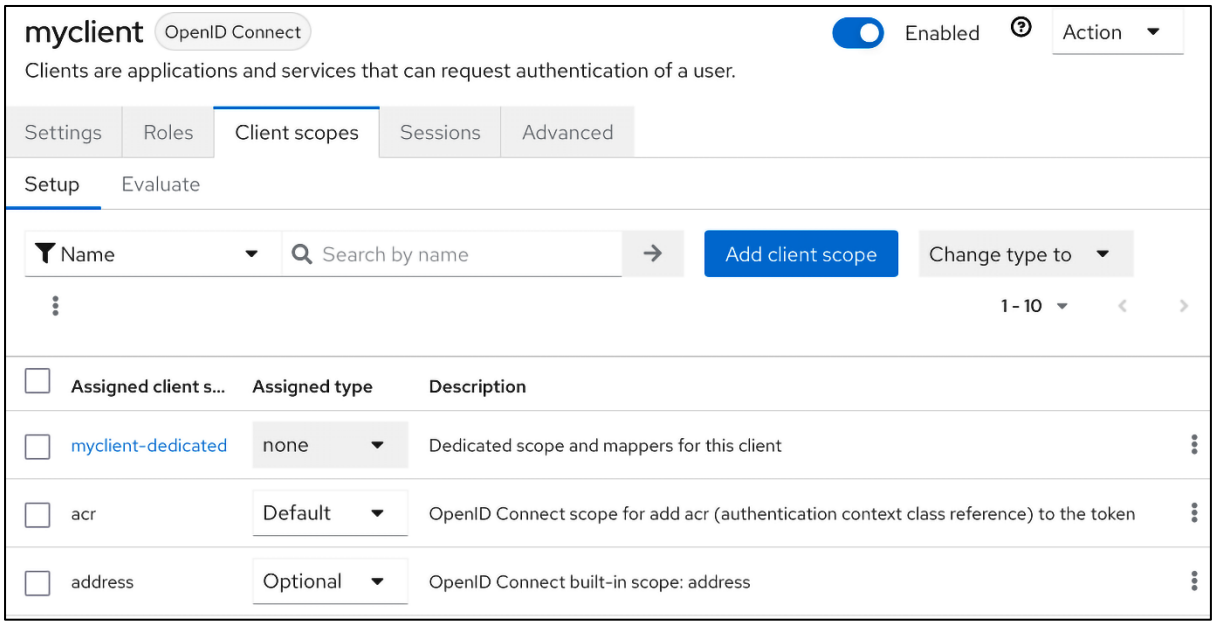

Myrealm
Manage
Clients
Client scopes
Realm roles
Users
Groups
Sessions
Capability config
Client authentication
On
Authorization
Off
Authentication flow
Standard flow
Direct access grants
Implicit flow
Service accounts roles
OAuth 2.0 Device Authorization Grant
OIDC CIBA Grant
Jump to section
General Settings
Access settings
Capability config
Login settings
Logout settings

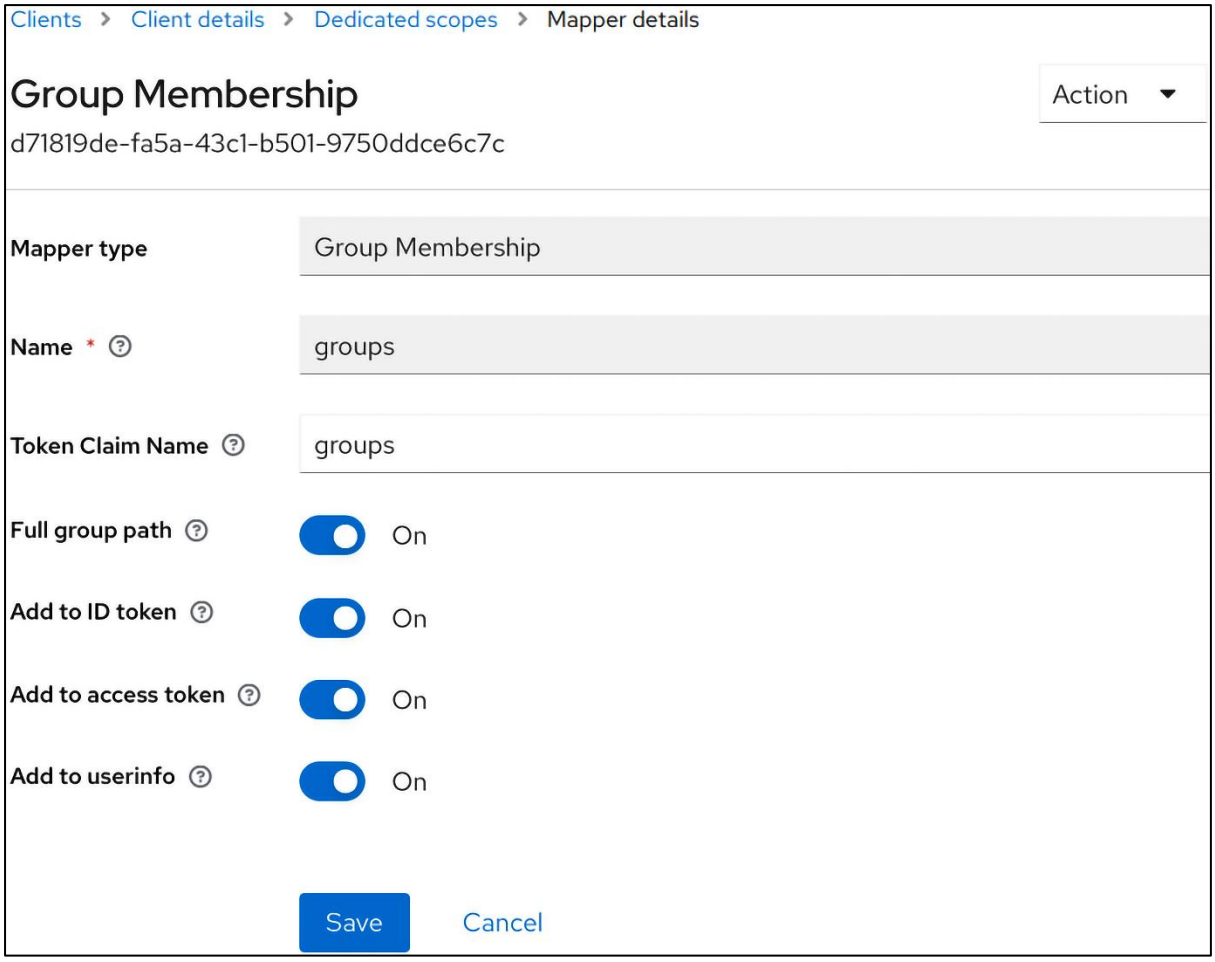
Chapter 7: Integrating Applications with Keycloak

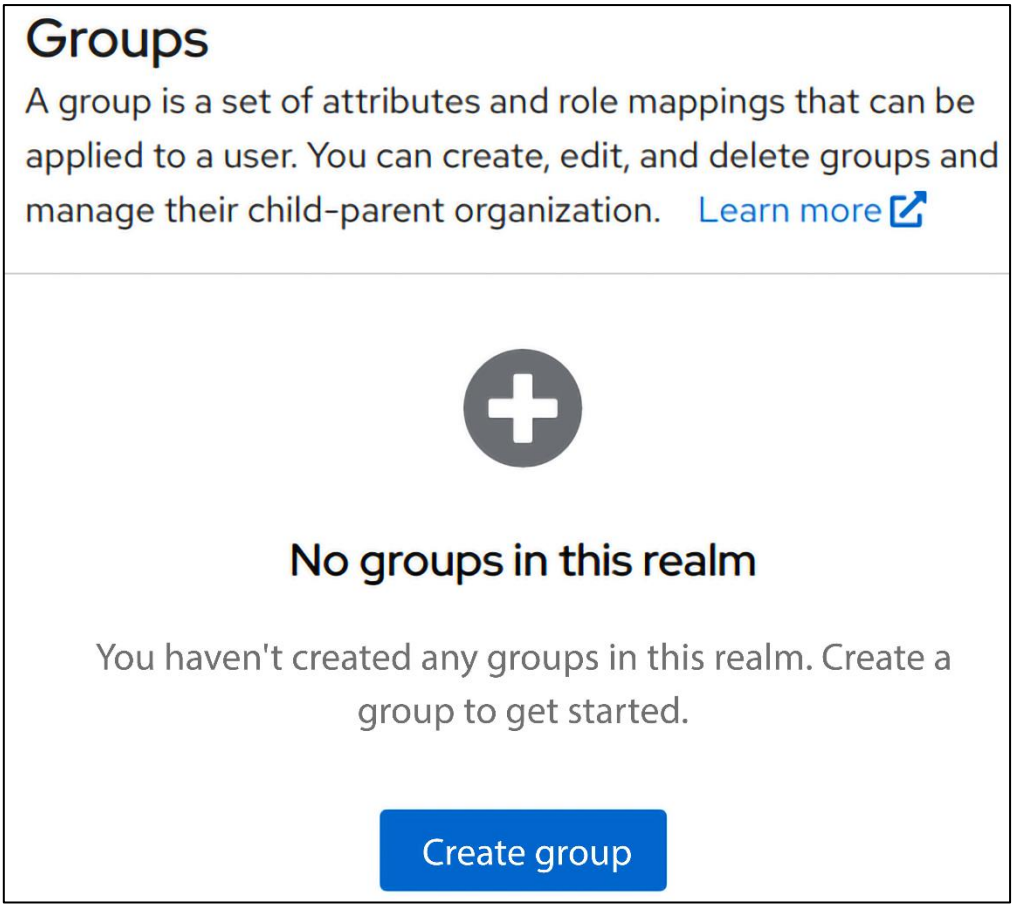


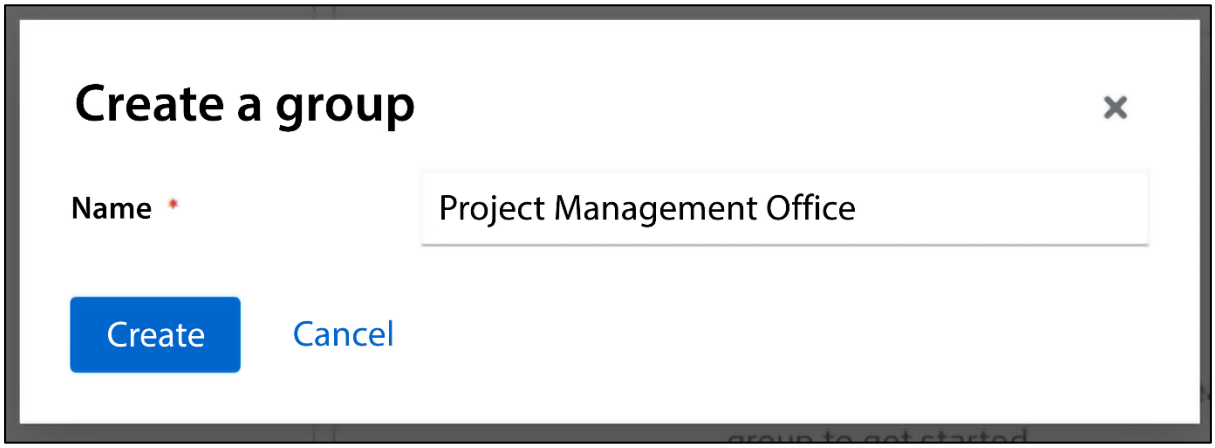


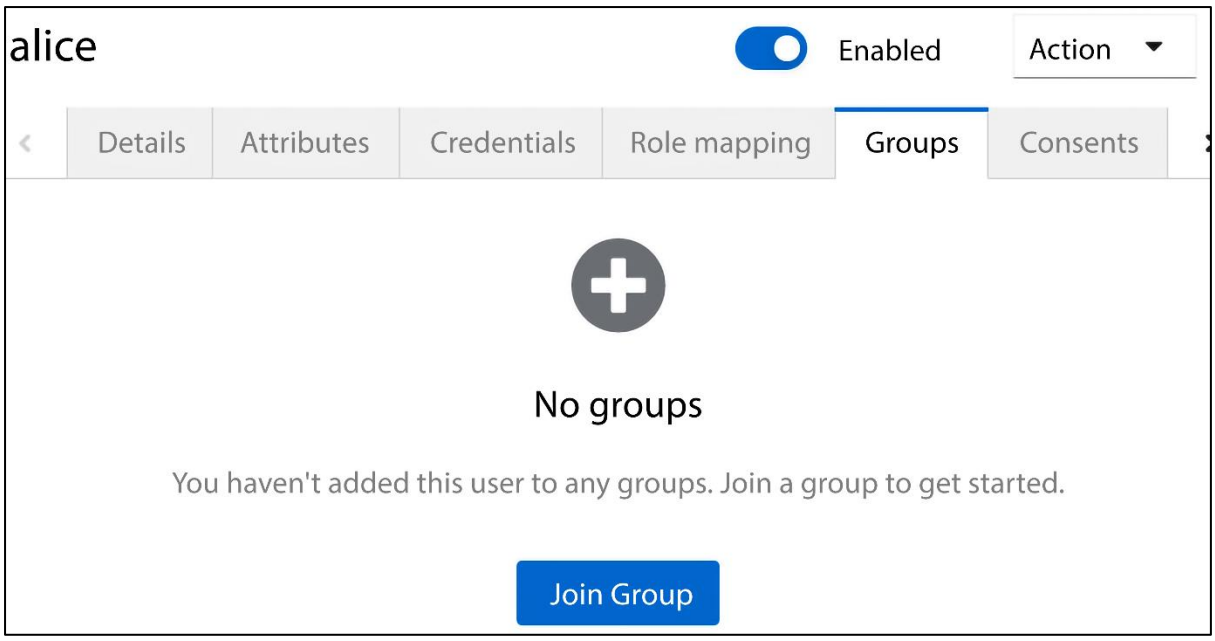
Chapter 8: Authorization Strategies

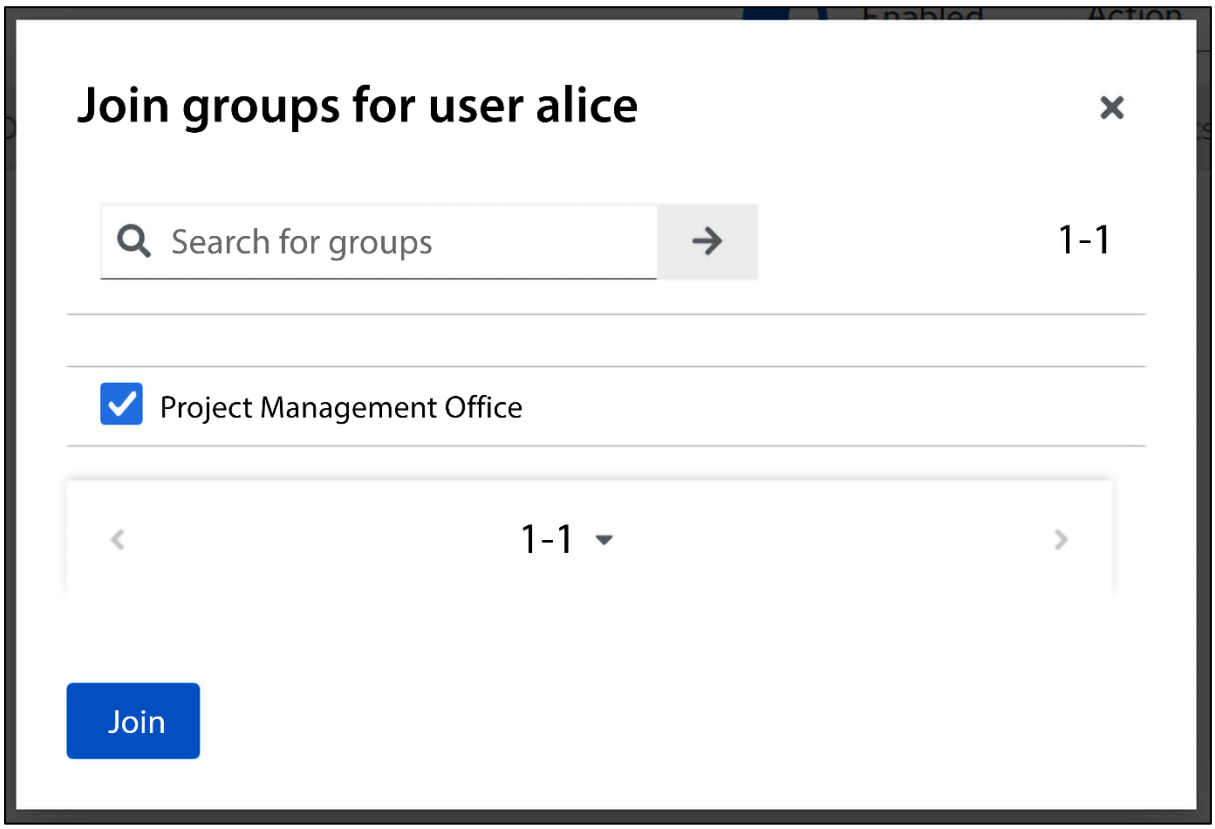


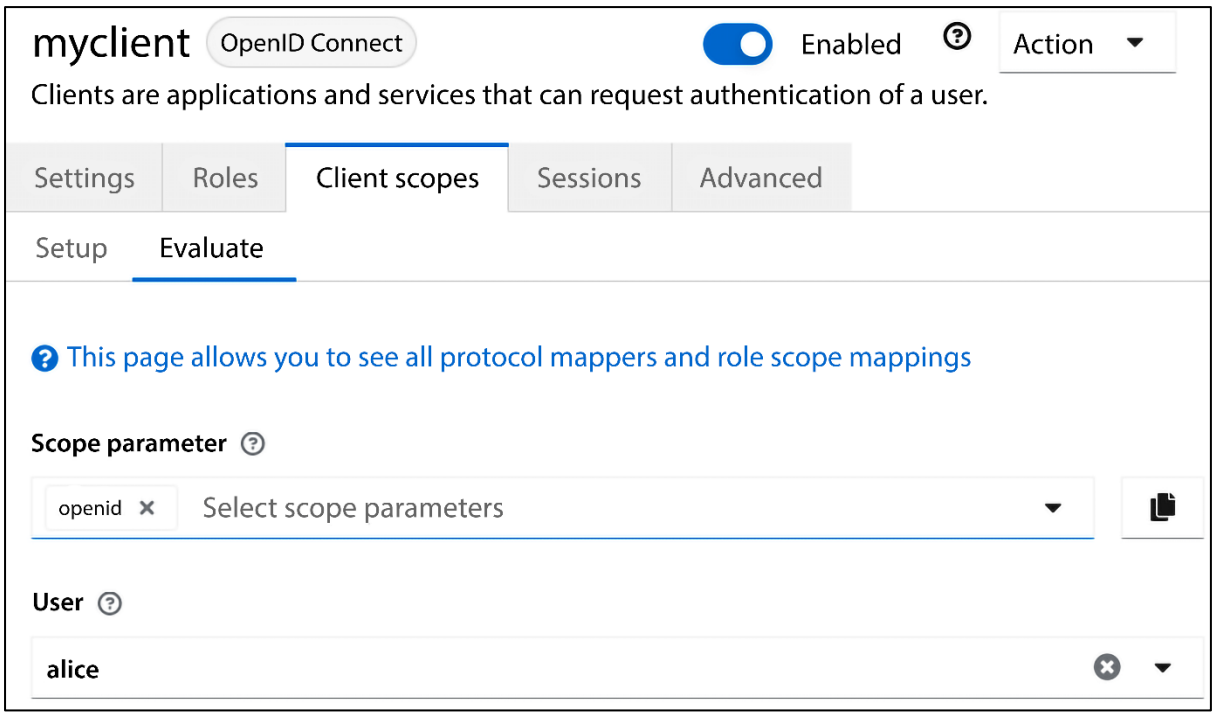


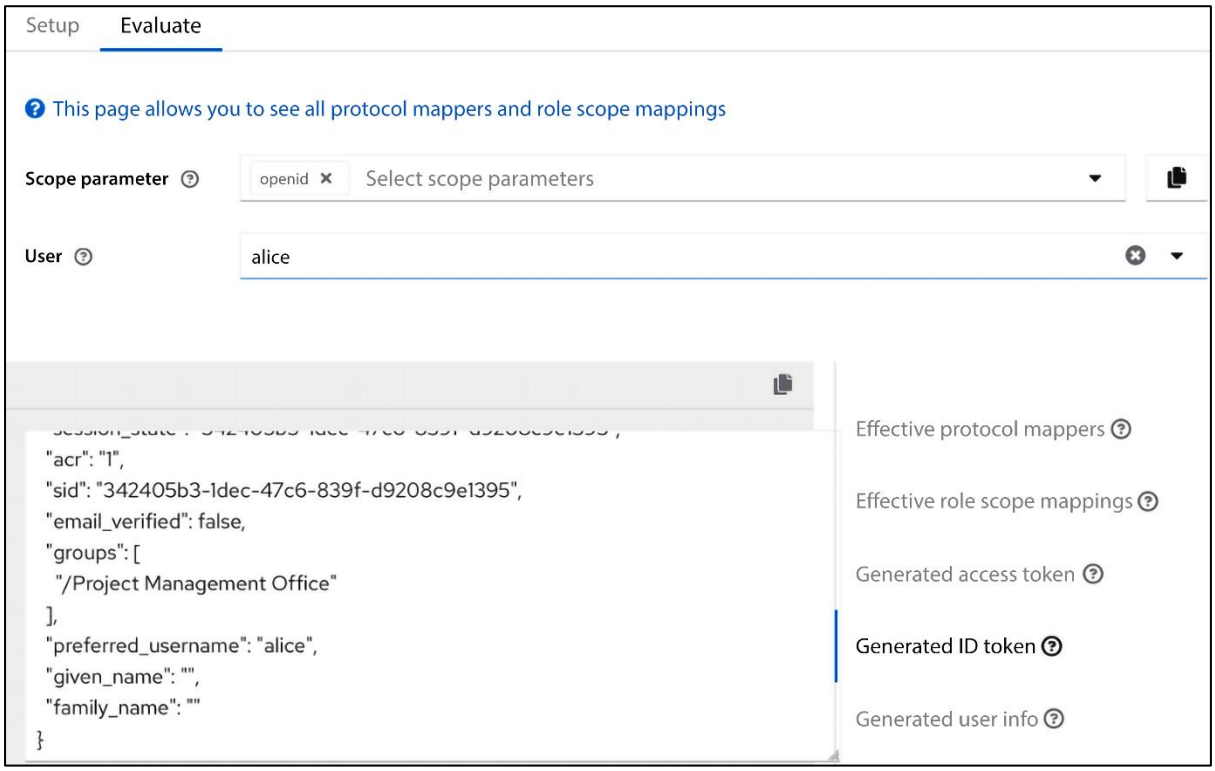

Groups
A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-parent organization. Learn more
No groups in this realm
You haven't created any groups in this realm. Create a group to get started.
Create group


Create a group
Name *
Project Management Office
Create
Cancel

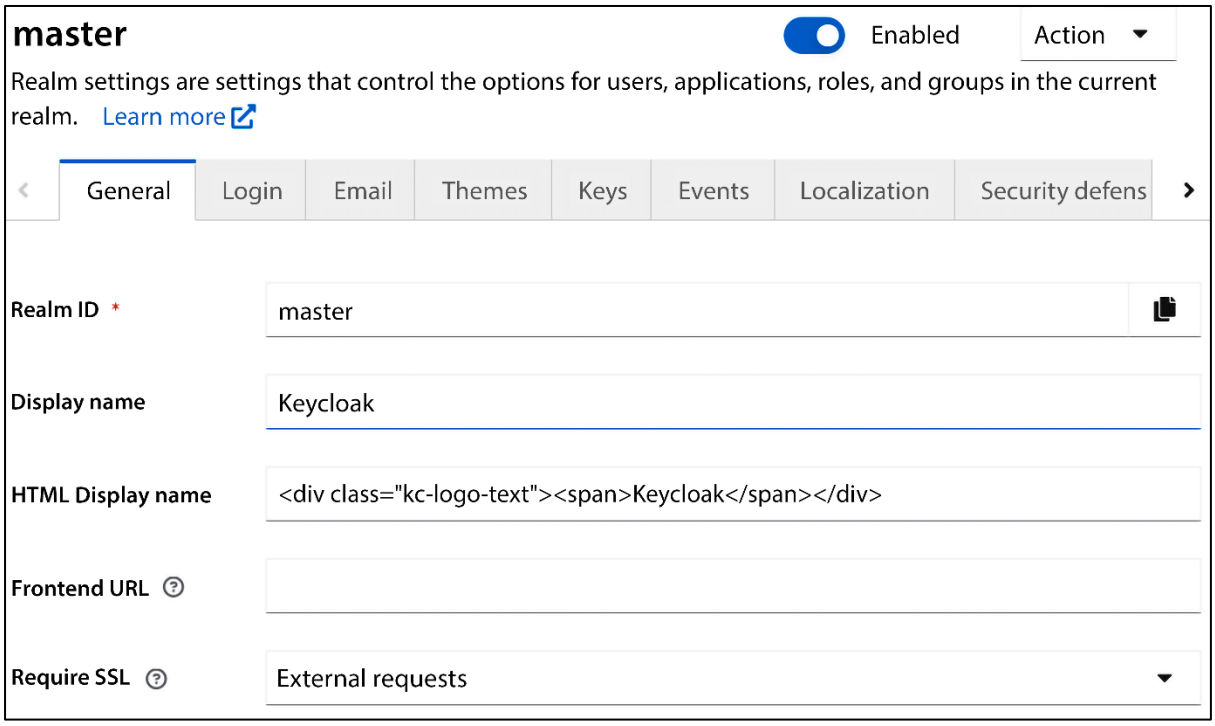

alice
Enabled
Action
Details
Attributes
Credentials
Role mapping
Groups
Consents
No groups
You haven't added this user to any groups. Join a group to get started.
Join Group

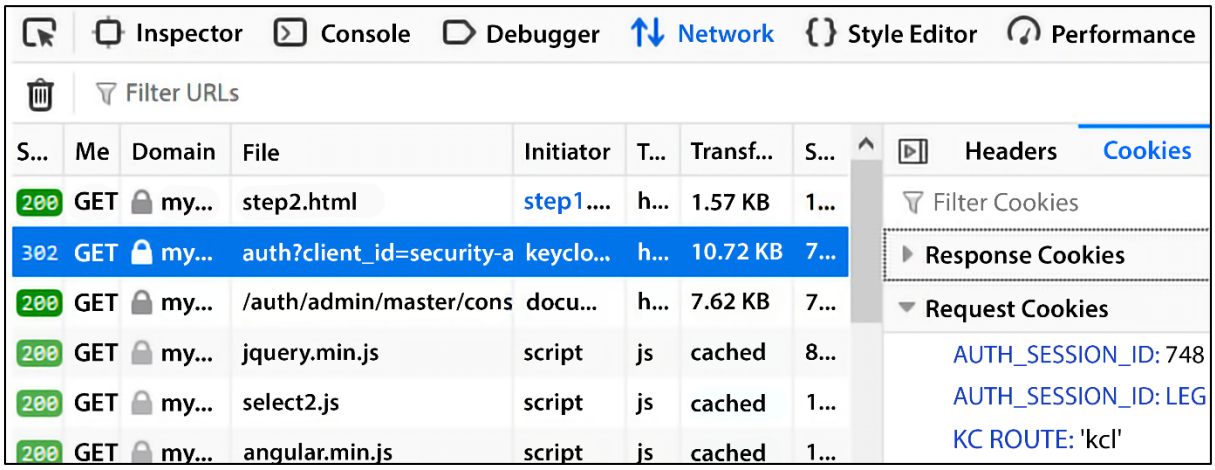

Join groups for user alice
Search for groups
1-1
Project Management Office
1-1
Join


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

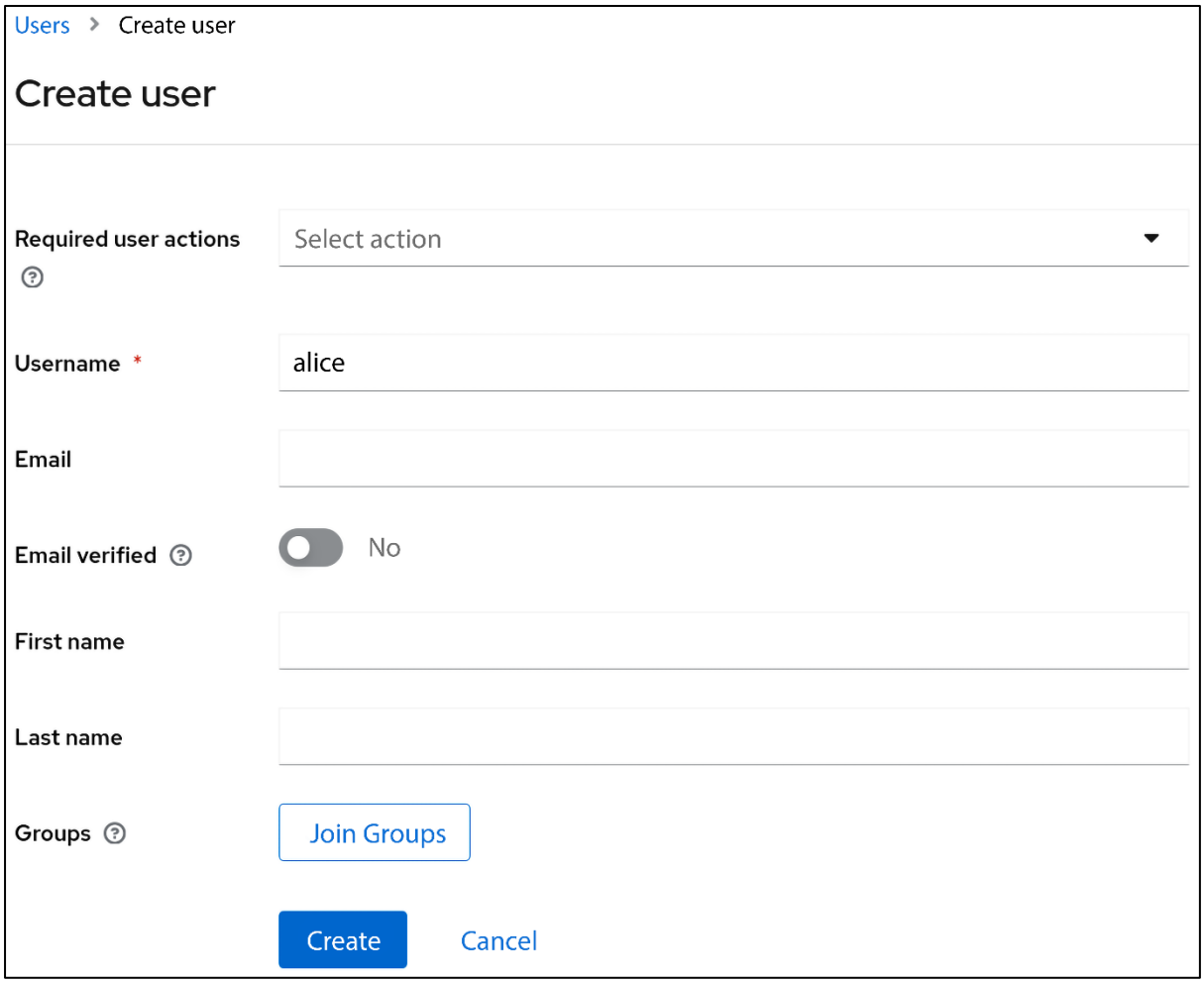

Setup
Evaluate
This page allows you to see all protocol mappers and role scope mappings
Scope parameter
openid
Select scope parameters
User
alice
"acr": "1",
"sid": "342405b3-1dec-47c6-839f-d9208c9e1395",
"email_verified": false,
"groups": [
"/Project Management Office"
],
"preferred_username": "alice",
"given_name": "",
"family_name": ""
}
Effective protocol mappers
Effective role scope mappings
Generated access token
Generated ID token
Generated user info

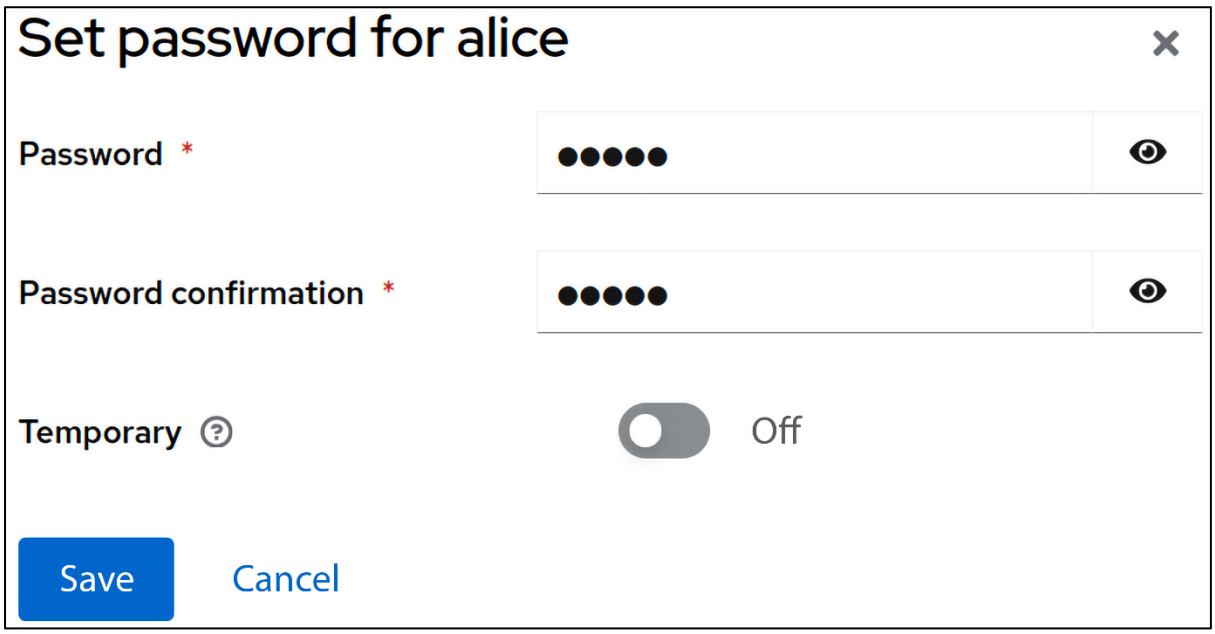
Chapter 9: Configuring Keycloak for Production

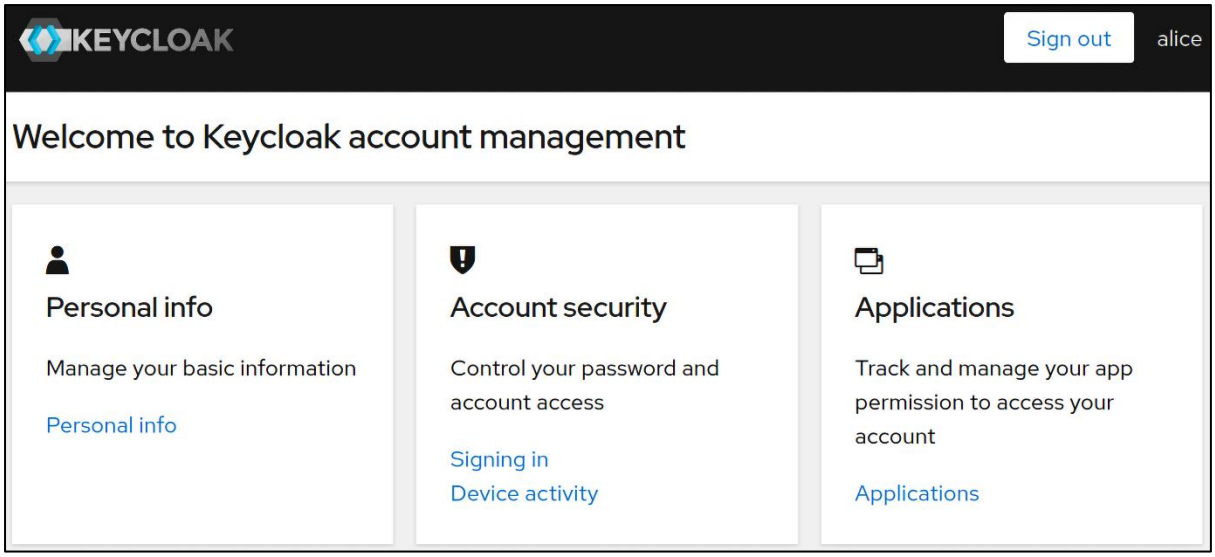


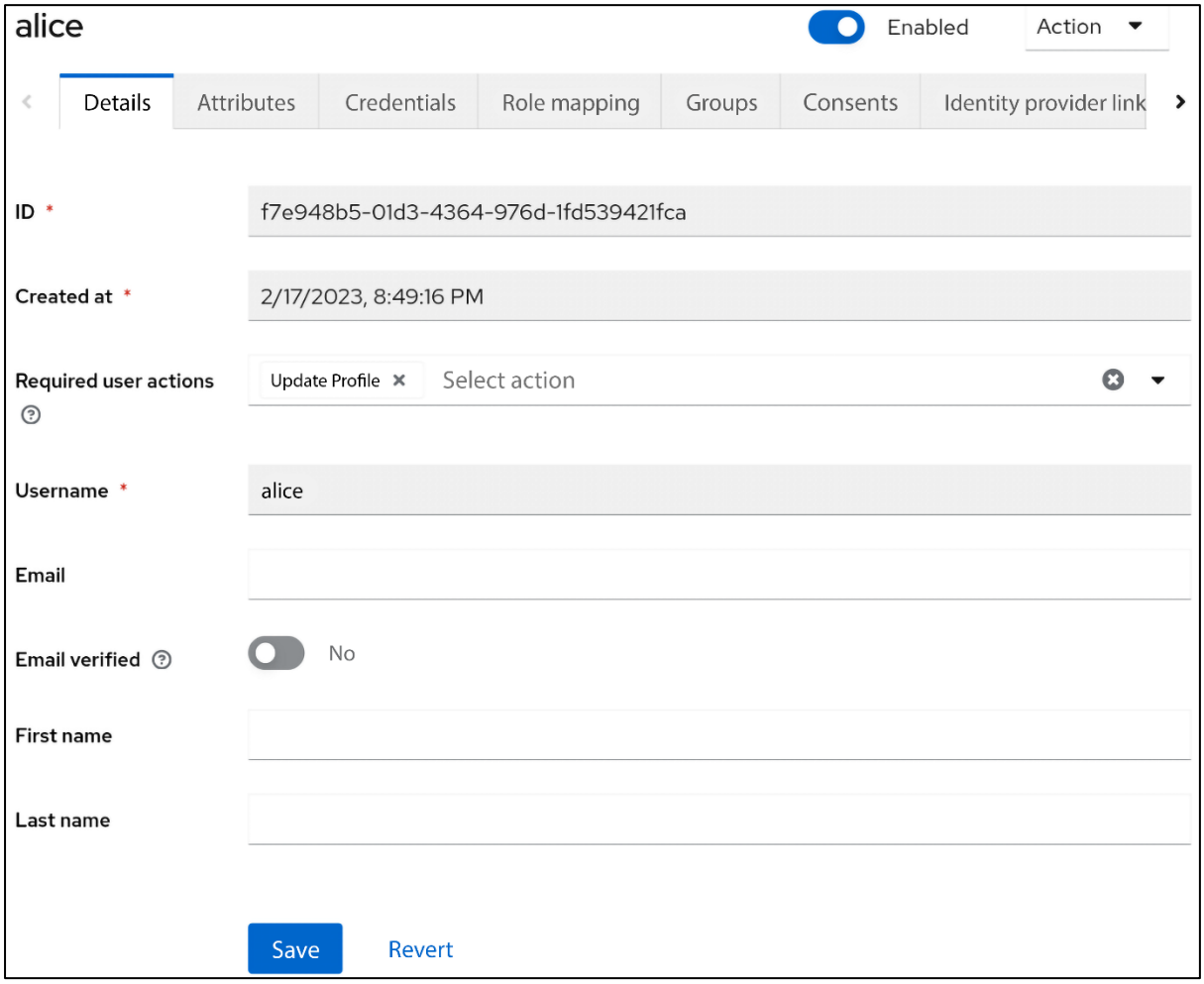


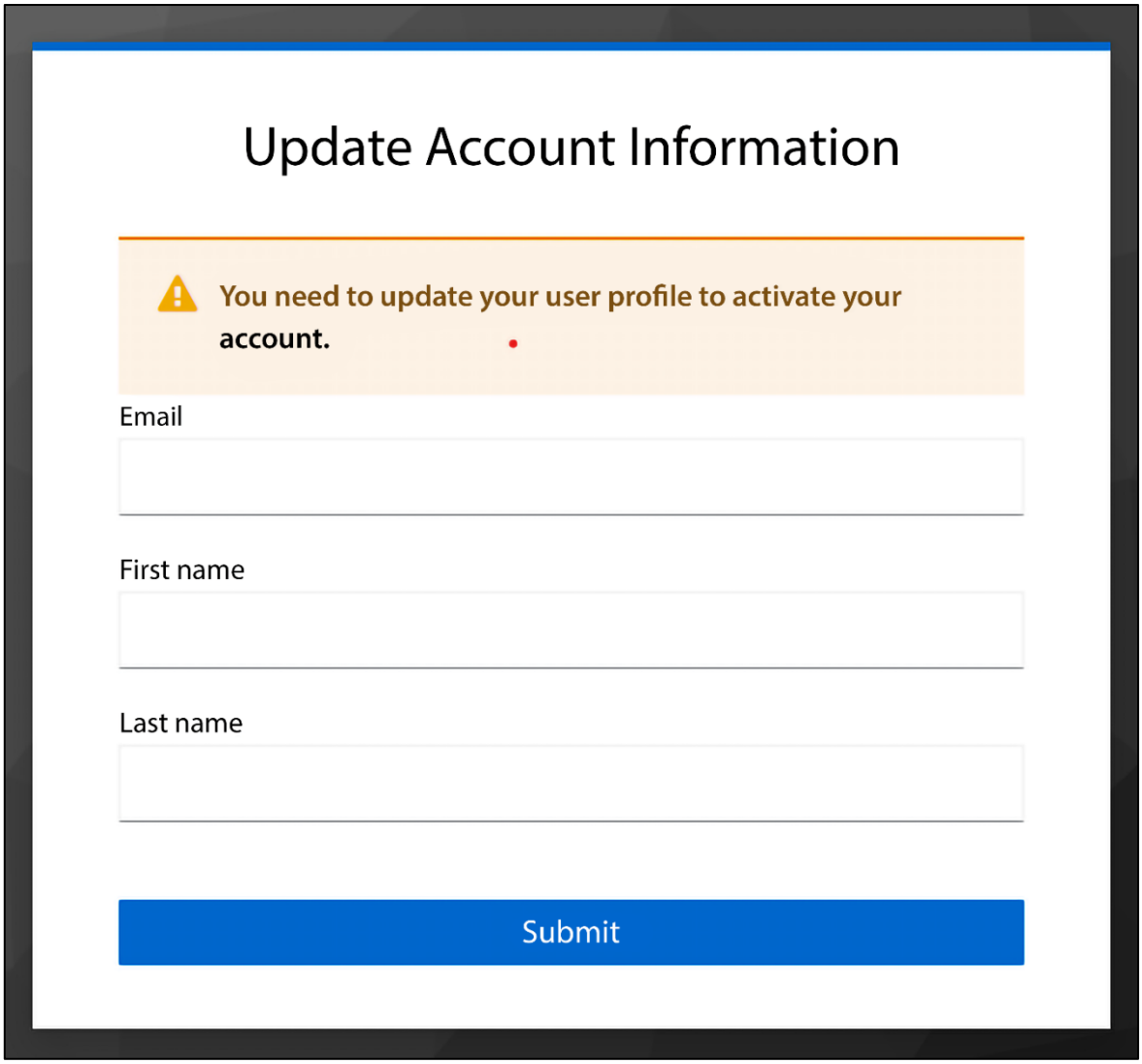
Chapter 10: Managing Users

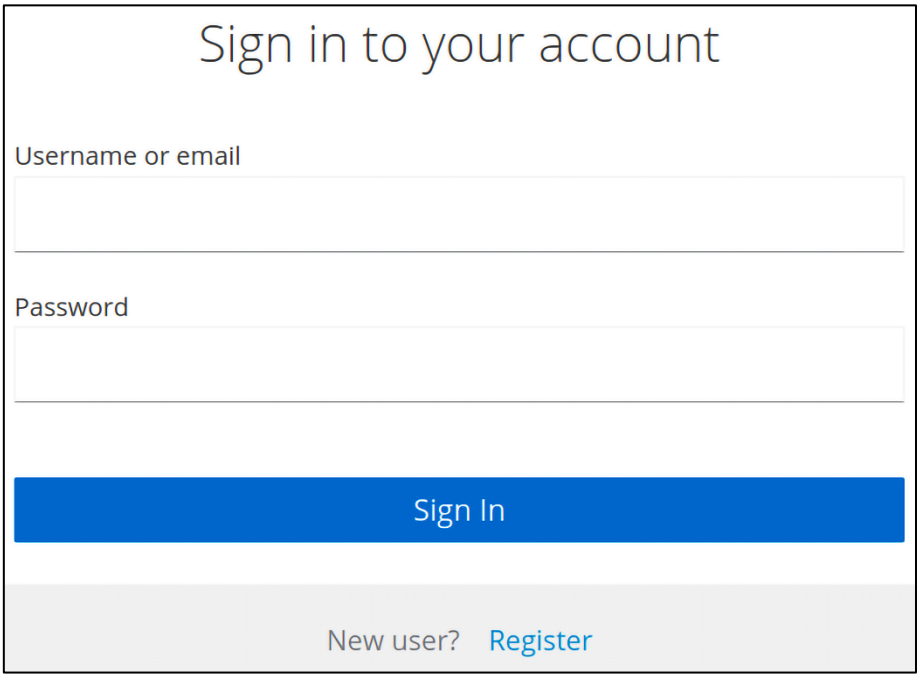


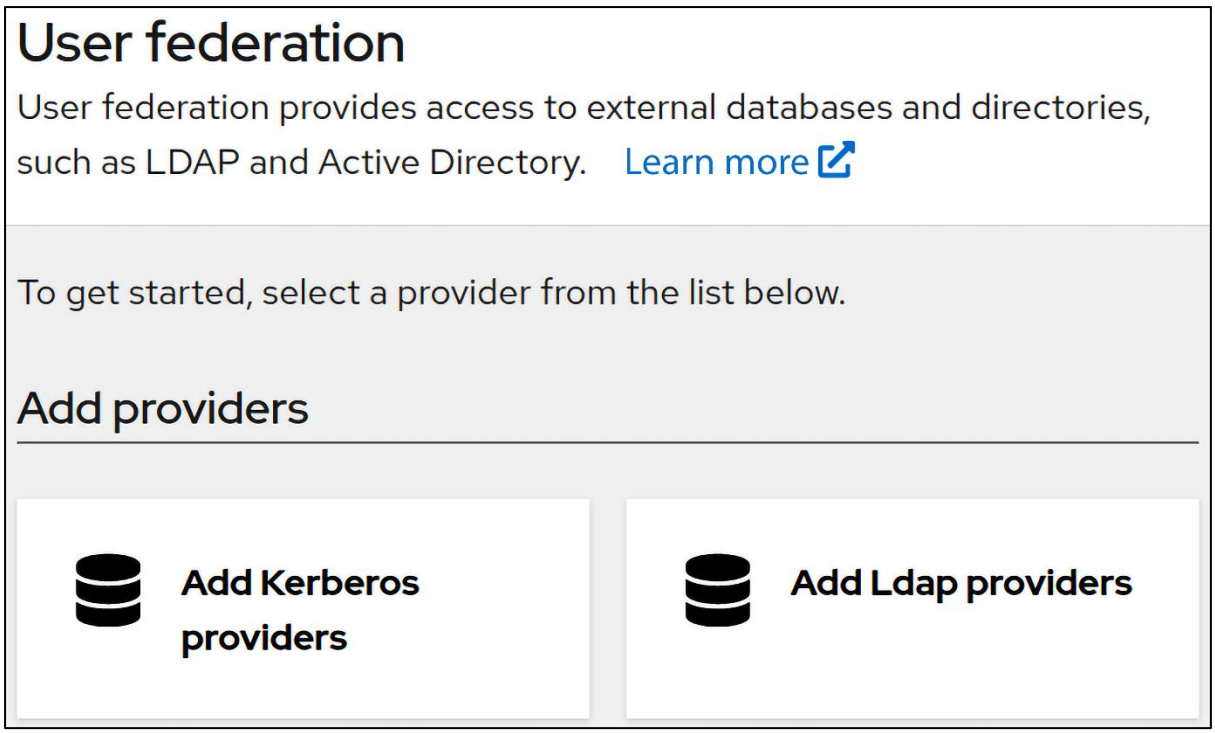


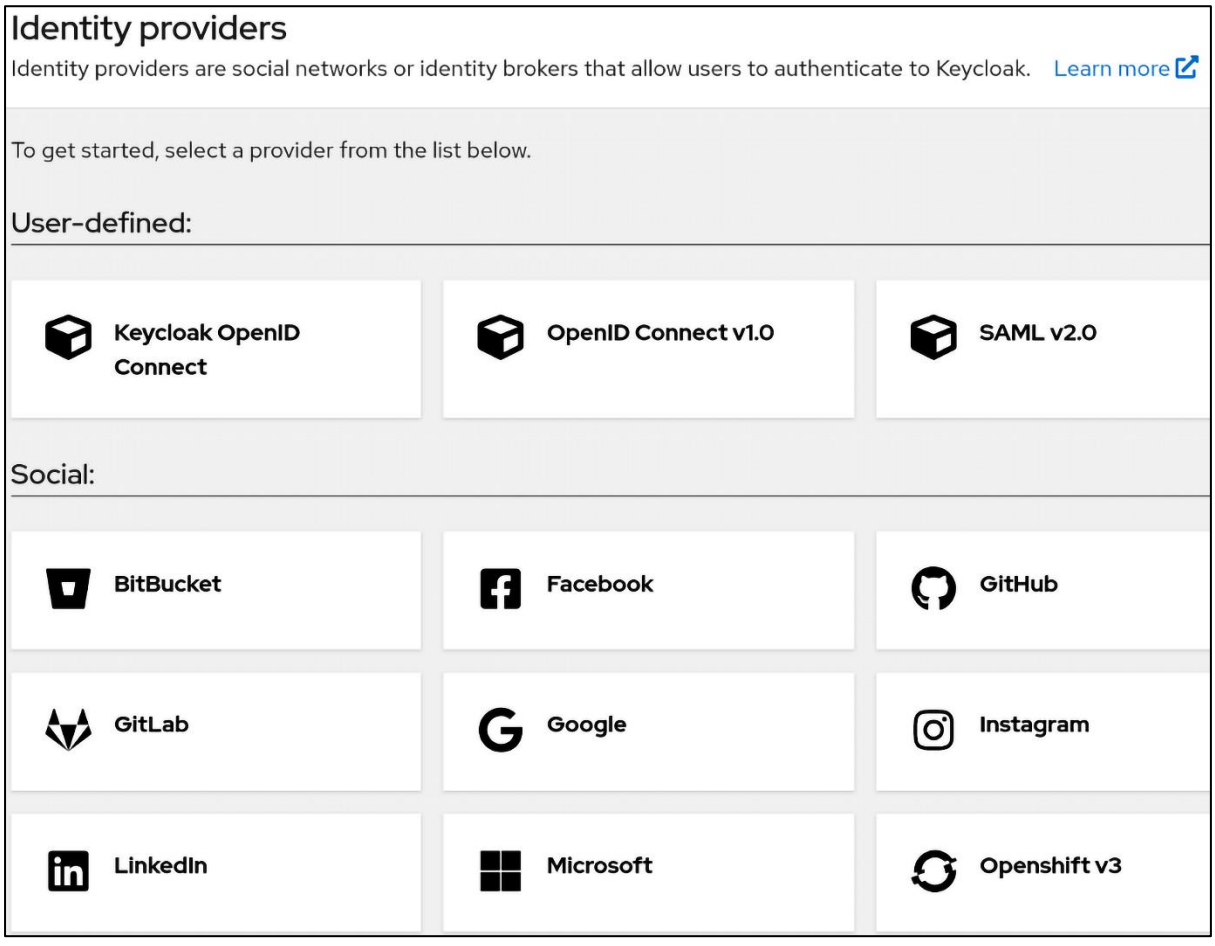

KEYCLOAK
Sign out
alice
Welcome to Keycloak account management
Personal info
Manage your basic information
Personal info
Account security
Control your password and account access
Signing in
Device activity
Applications
Track and manage your app permission to access your account
Applications

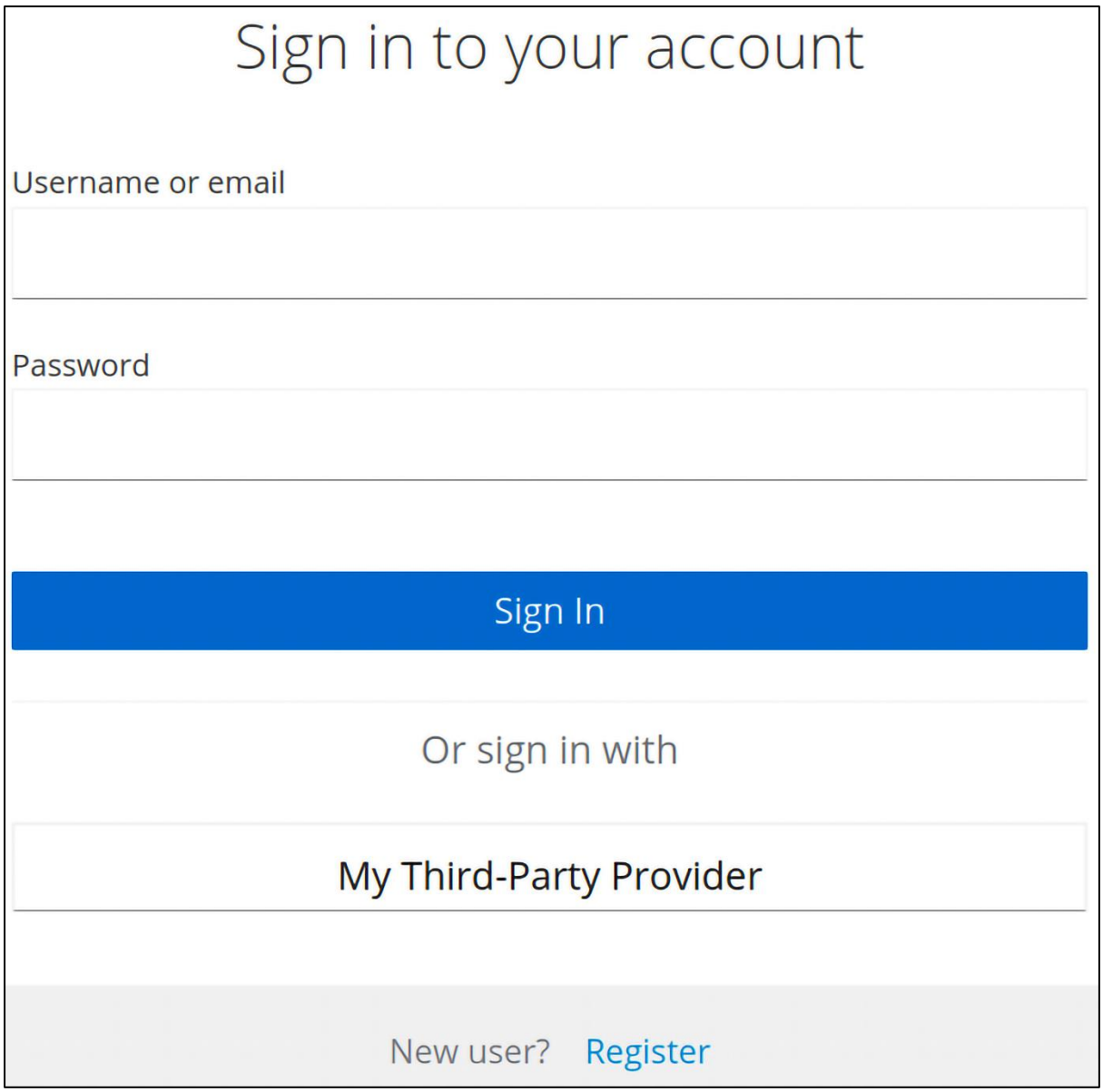

alice
Enabled
Action
Details
Attributes
Credentials
Role mapping
Groups
Consents
Identity provider link
ID *
f7e948b5-01d3-4364-976d-1fd539421fca
Created at *
2/17/2023, 8:49:16 PM
Required user actions
Update Profile
Select action
Username *
alice
Email
Email verified
No
First name
Last name
Save
Revert

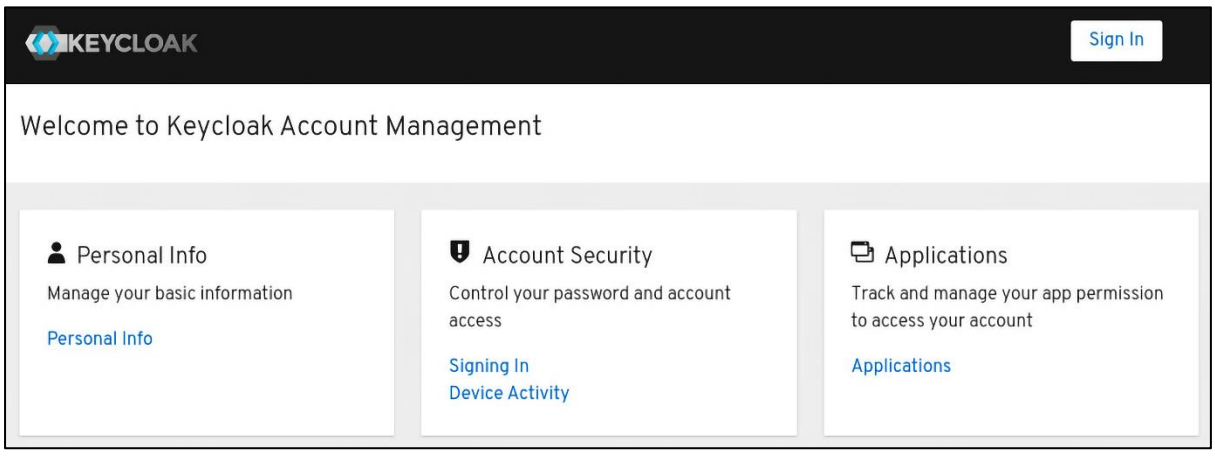

Update Account Information
You need to update your user profile to activate your account.
Email
First name
Last name
Submit

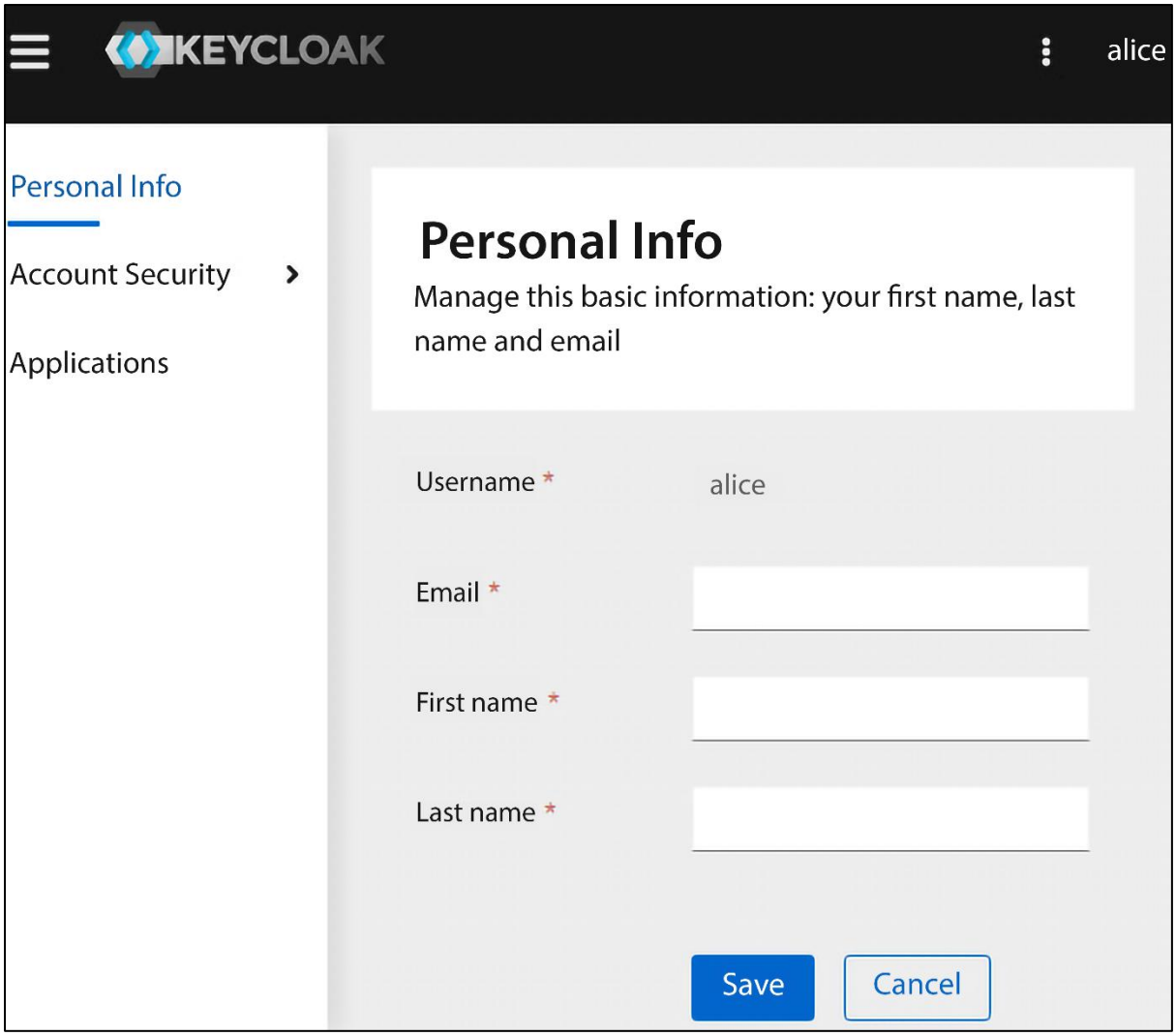

Sign in to your account
Username or email
Password
Sign In
New user? Register


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

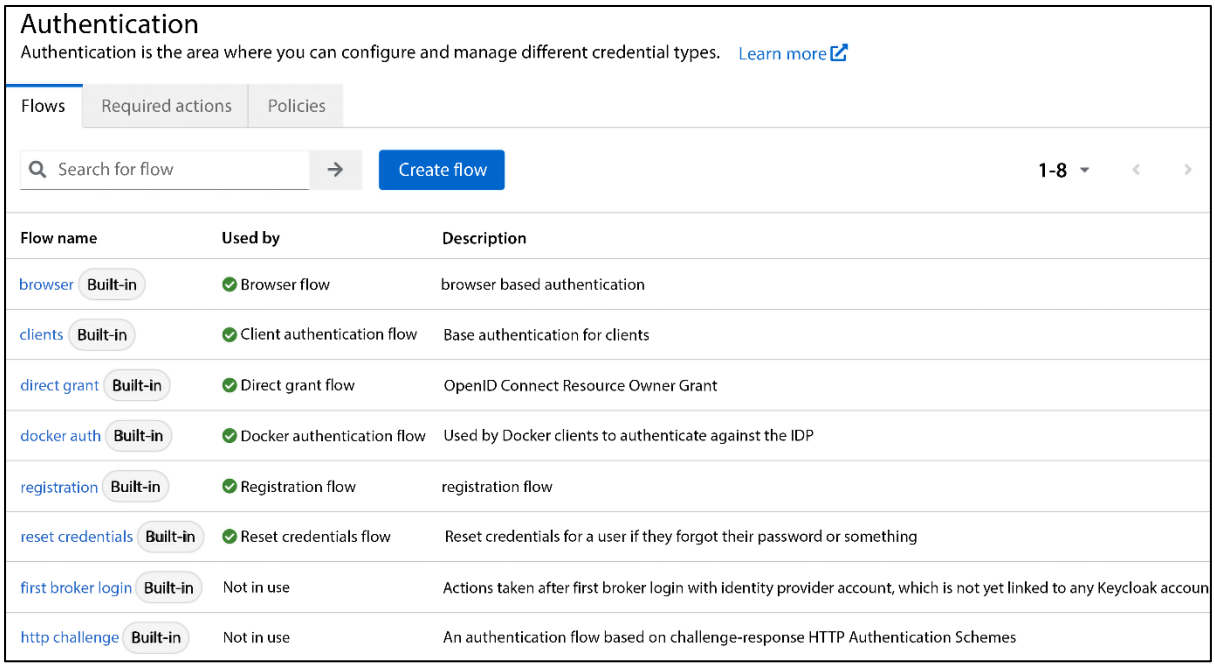

Identity providers
Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. Learn more
To get started, select a provider from the list below.
User-defined:
Keycloak OpenID Connect
OpenID Connect v1.0
SAML v2.0
Social:
BitBucket
Facebook
GitHub
GitLab
Google
Instagram
LinkedIn
Microsoft
Openshift v3

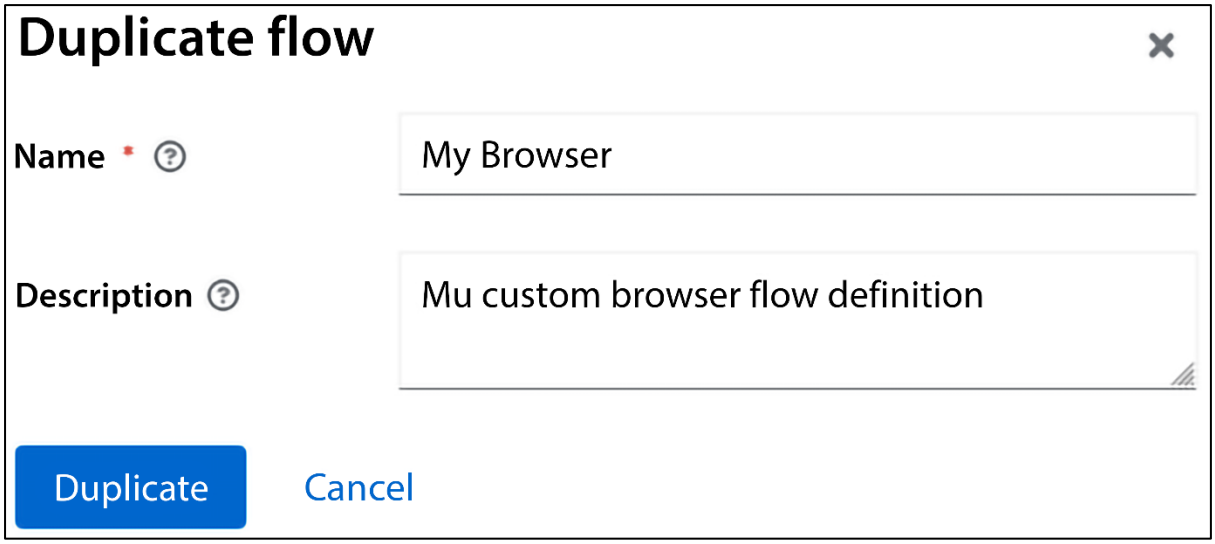

Sign in to your account
Username or email
Password
Sign In
Or sign in with
My Third-Party Provider
New user?
Register

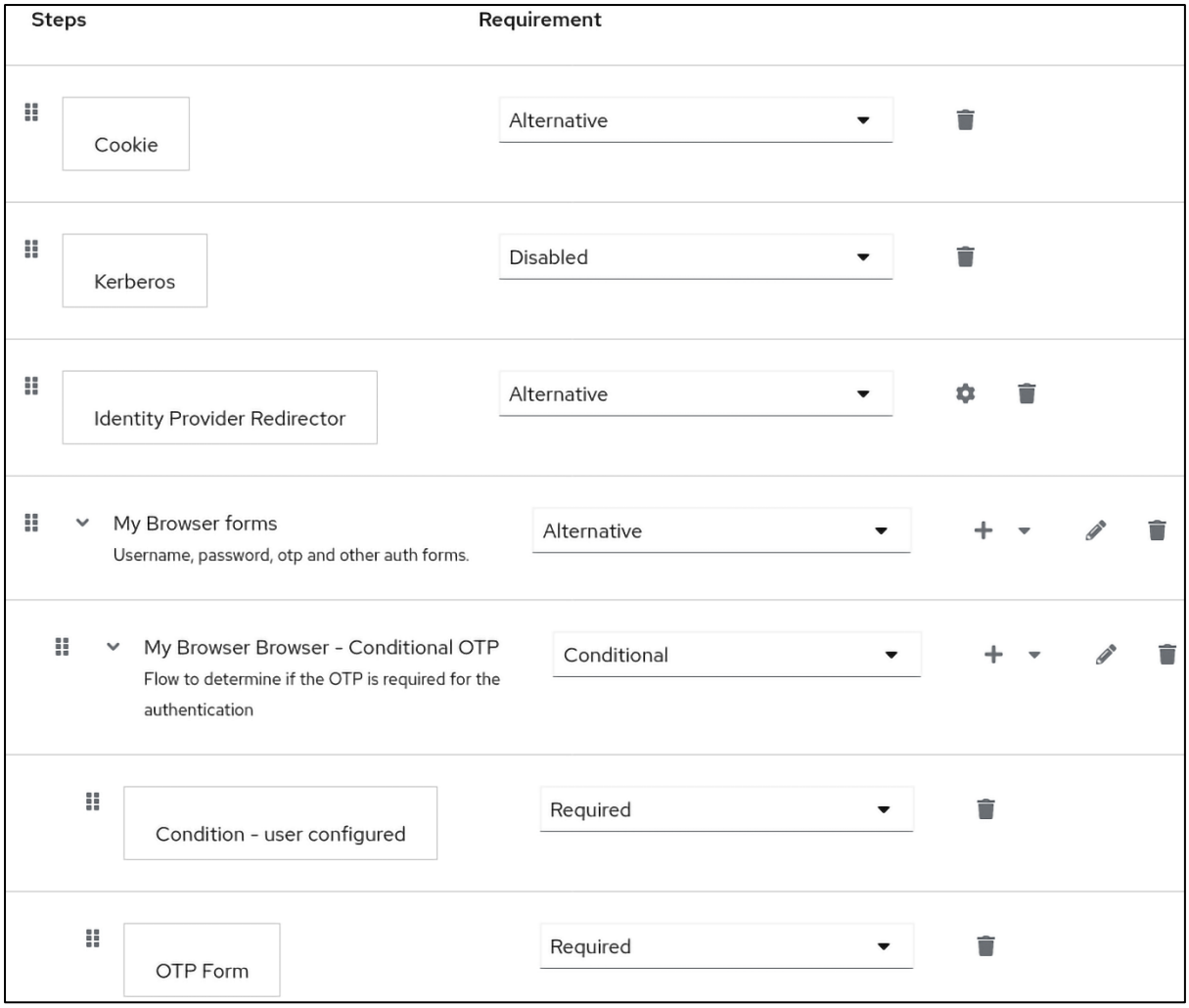

KEYCLOAK
Sign In
Welcome to Keycloak Account Management
Personal Info
Manage your basic information
Personal Info
Account Security
Control your password and account access
Signing In
Device Activity
Applications
Track and manage your app permission to access your account
Applications

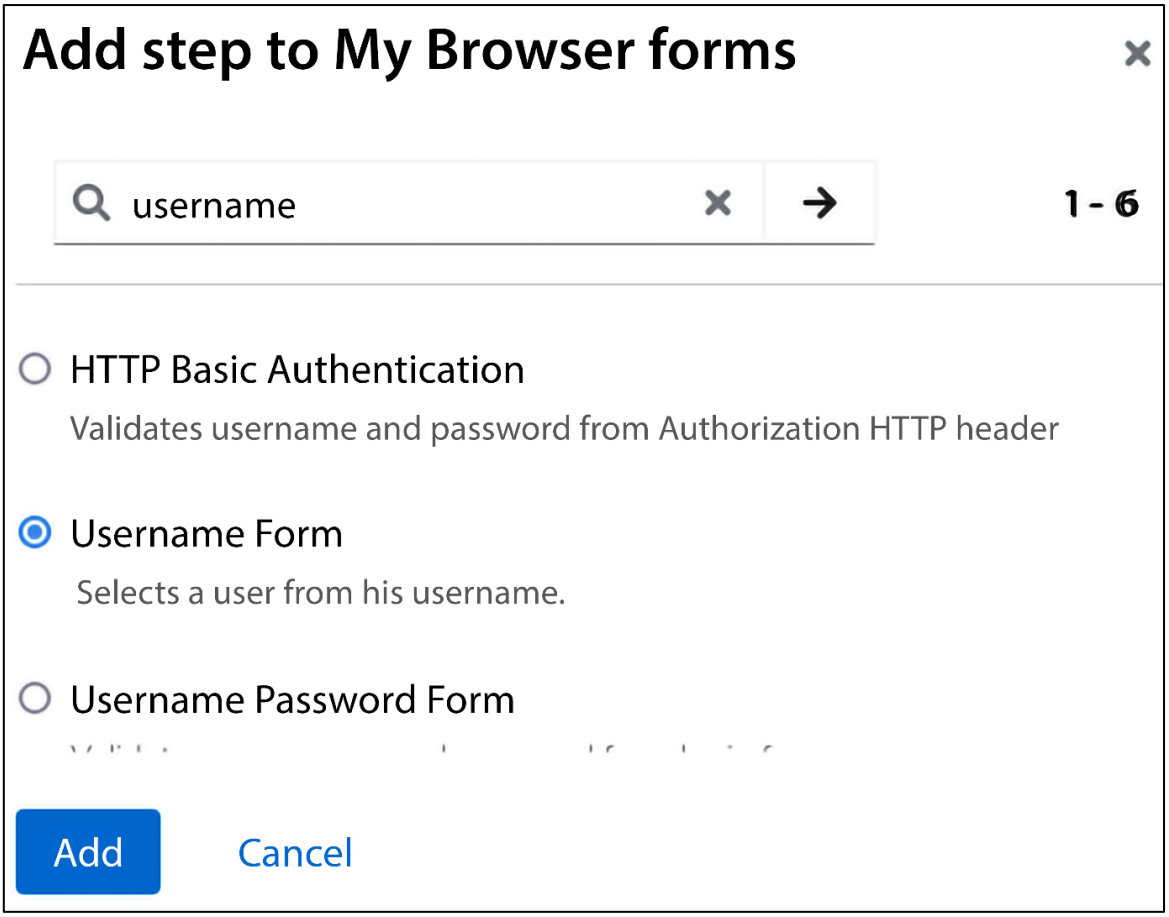

KEYCLOAK
alice
Personal Info
Account Security
Applications
Personal Info
Manage this basic information: your first name, last name and email
Username *
alice
Email *
First name *
Last name *
Save
Cancel

Chapter 11: Authenticating Users

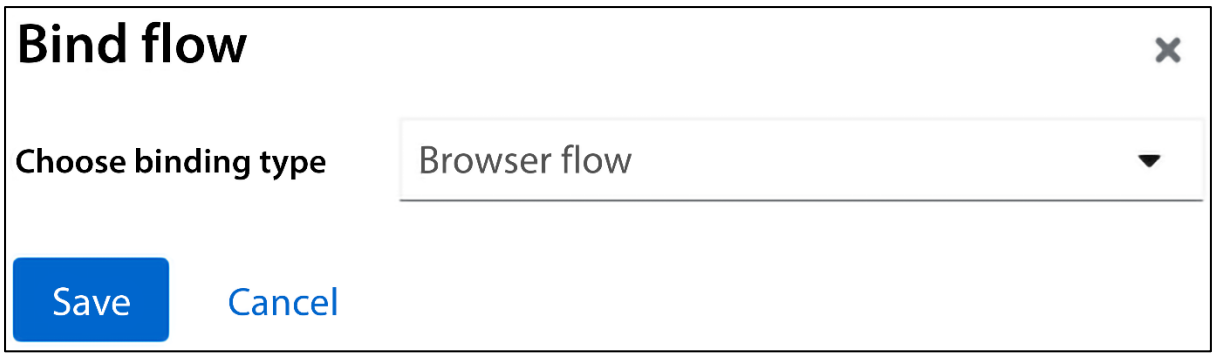


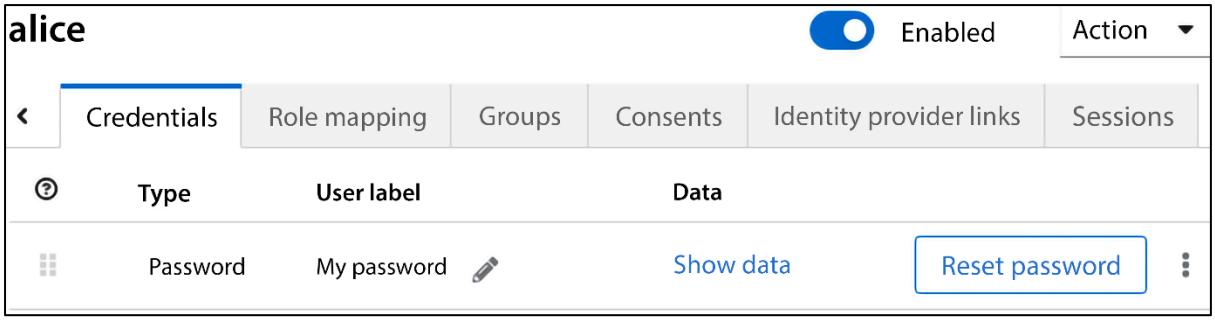


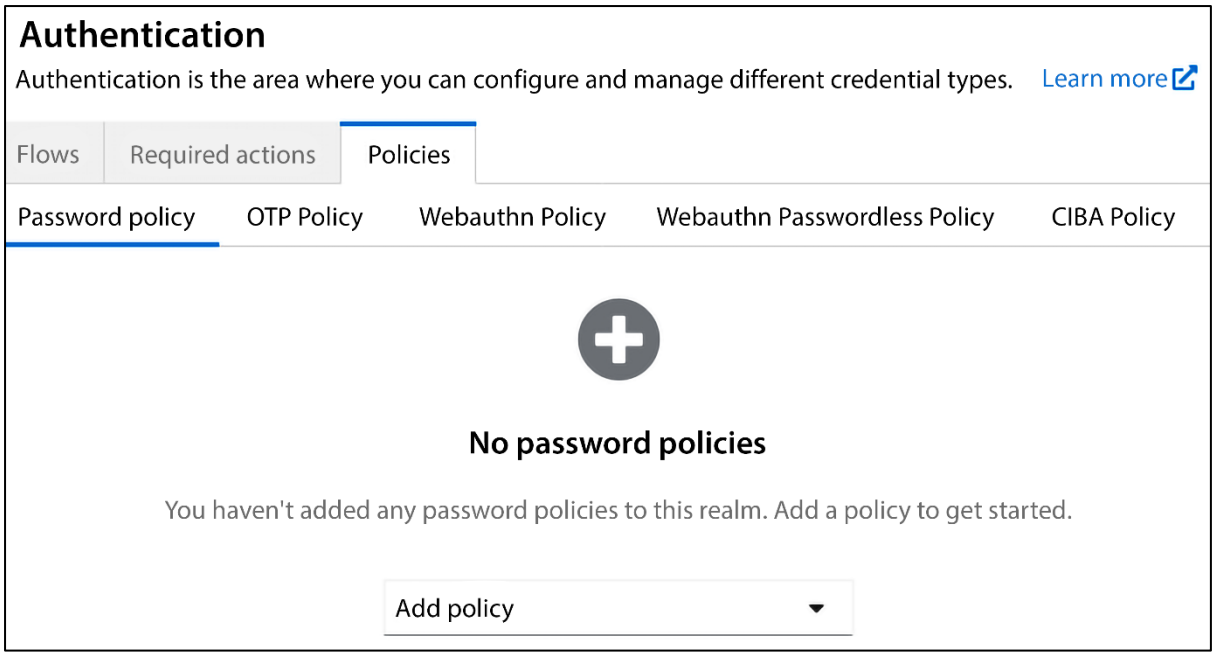

Steps
Requirement
Cookie
Alternative
Kerberos
Disabled
Identity Provider Redirector
Alternative
My Browser forms
Username, password, otp and other auth forms.
Alternative
My Browser Browser - Conditional OTP
Flow to determine if the OTP is required for the authentication
Conditional
Condition - user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

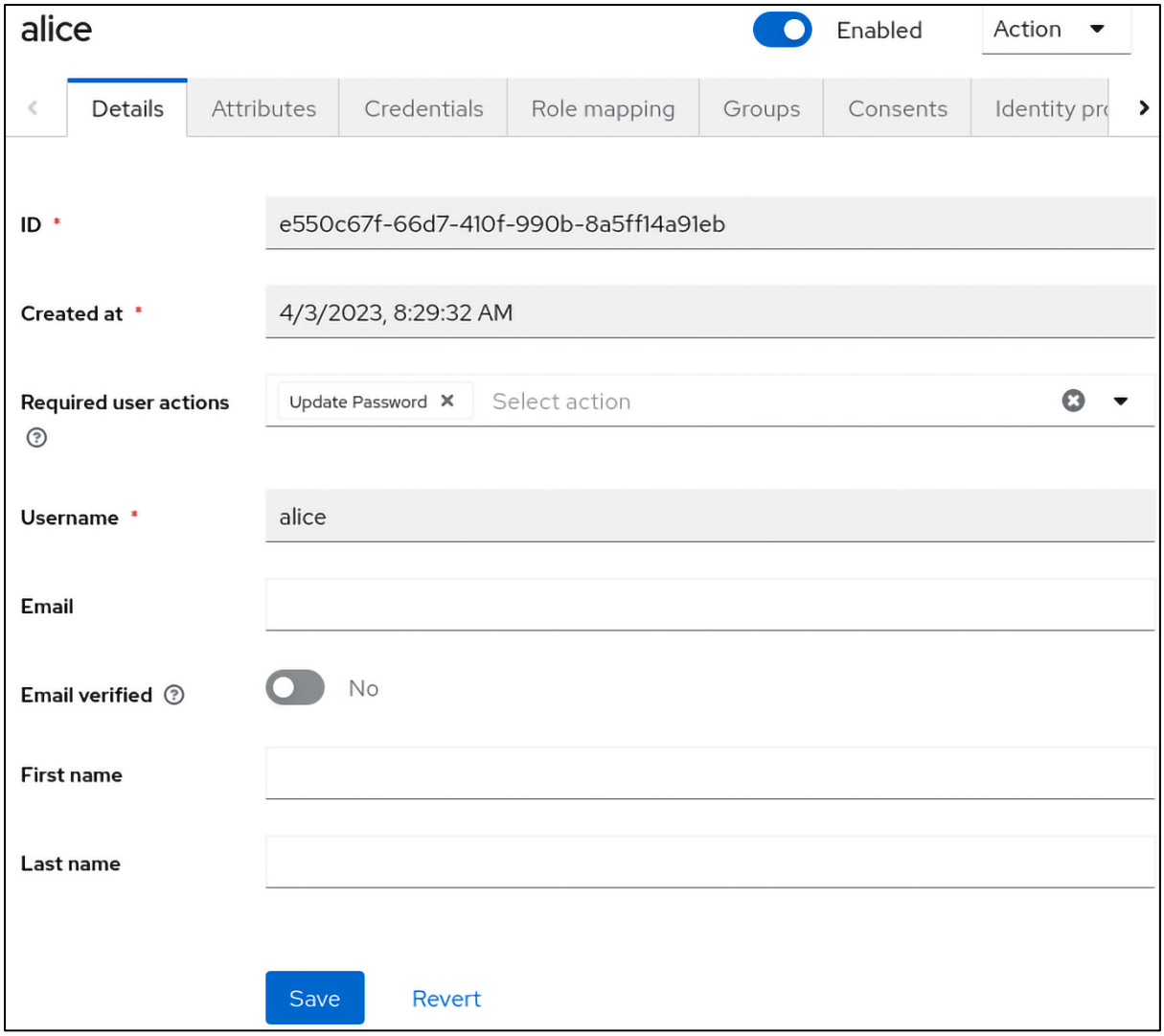

Add step to My Browser forms
username
1 - 6
HTTP Basic Authentication
Validates username and password from Authorization HTTP header
Username Form
Selects a user from his username.
Username Password Form
Add
Cancel

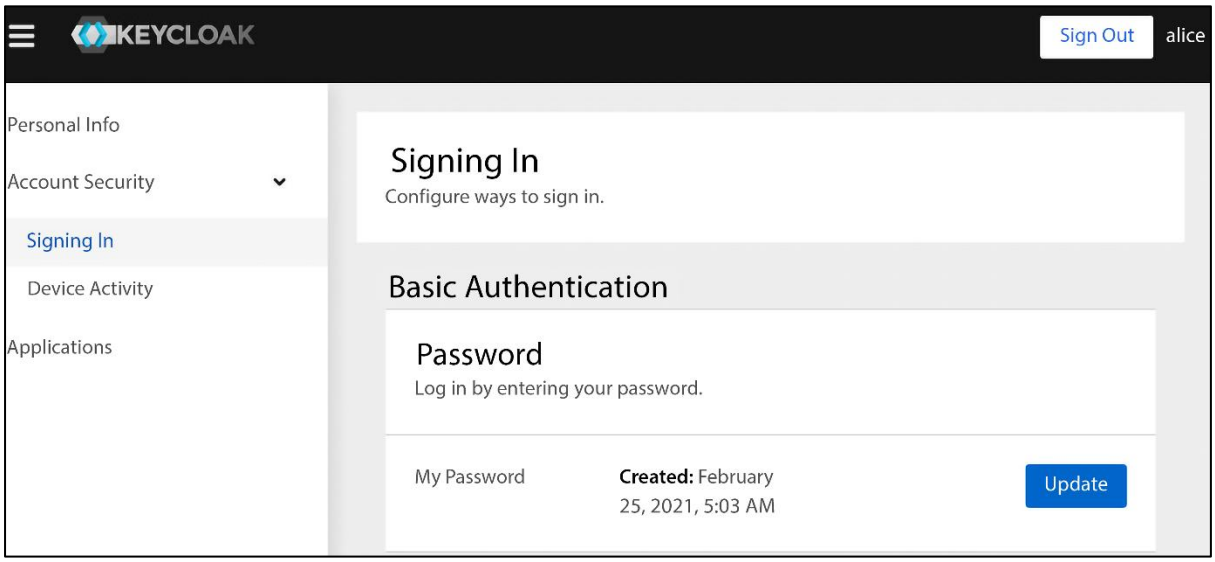

My Browser forms
Username, password, otp and other auth forms.
Alternative
Username Form
Required
Password Form
Required
My Browser Browser - Conditional OTP
Flow to determine if the OTP is required for the authentication
Conditional
Condition - user configured
Required
OTP Form
Required

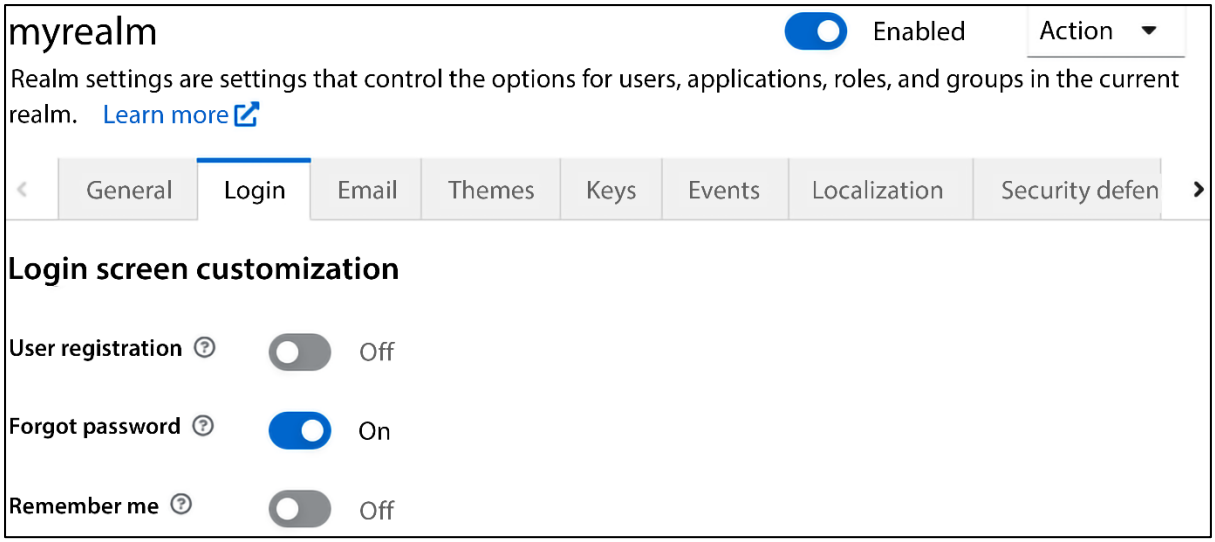

Bind flow
Choose binding type
Browser flow
Save
Cancel

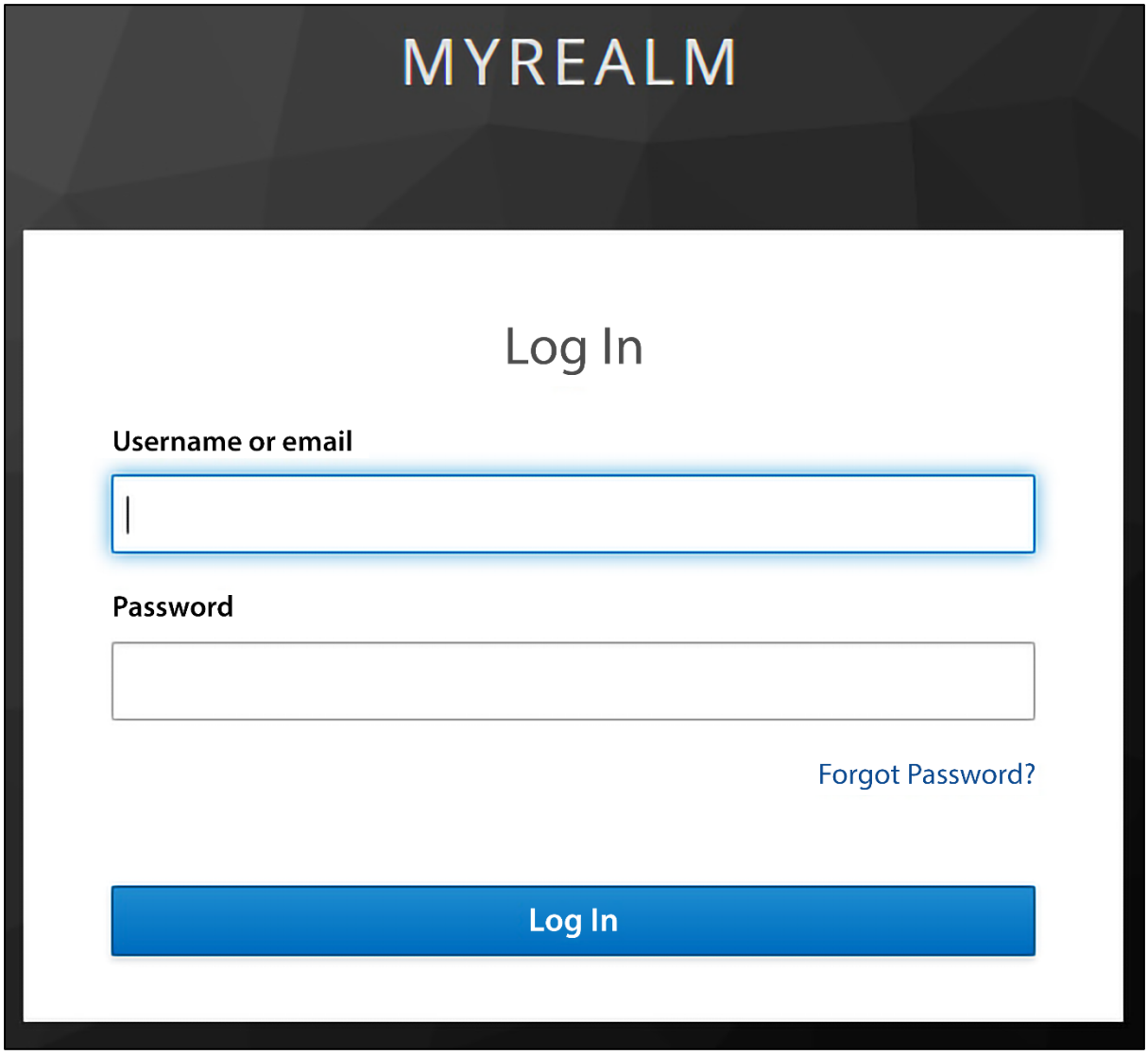

alice
Enabled
Action
Credentials
Role mapping
Groups
Consents
Identity provider links
Sessions
Type
User label
Data
Password
My password
Show data
Reset password

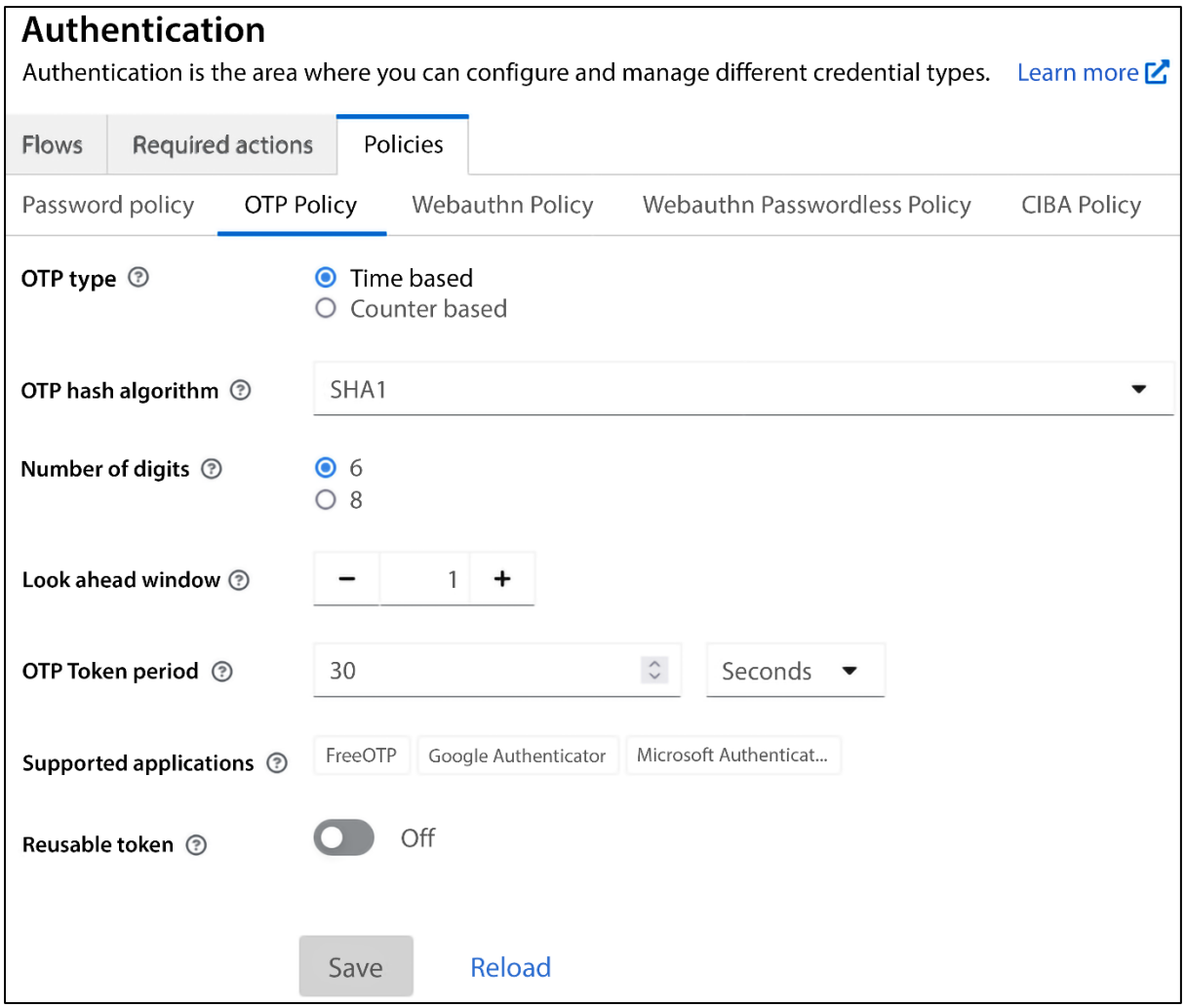

Authentication
Authentication is the area where you can configure and manage different credential types.
Learn more
Flows
Required actions
Policies
Password policy
OTP Policy
Webauthn Policy
Webauthn Passwordless Policy
CIBA Policy
No password policies
You haven't added any password policies to this realm. Add a policy to get started.
Add policy

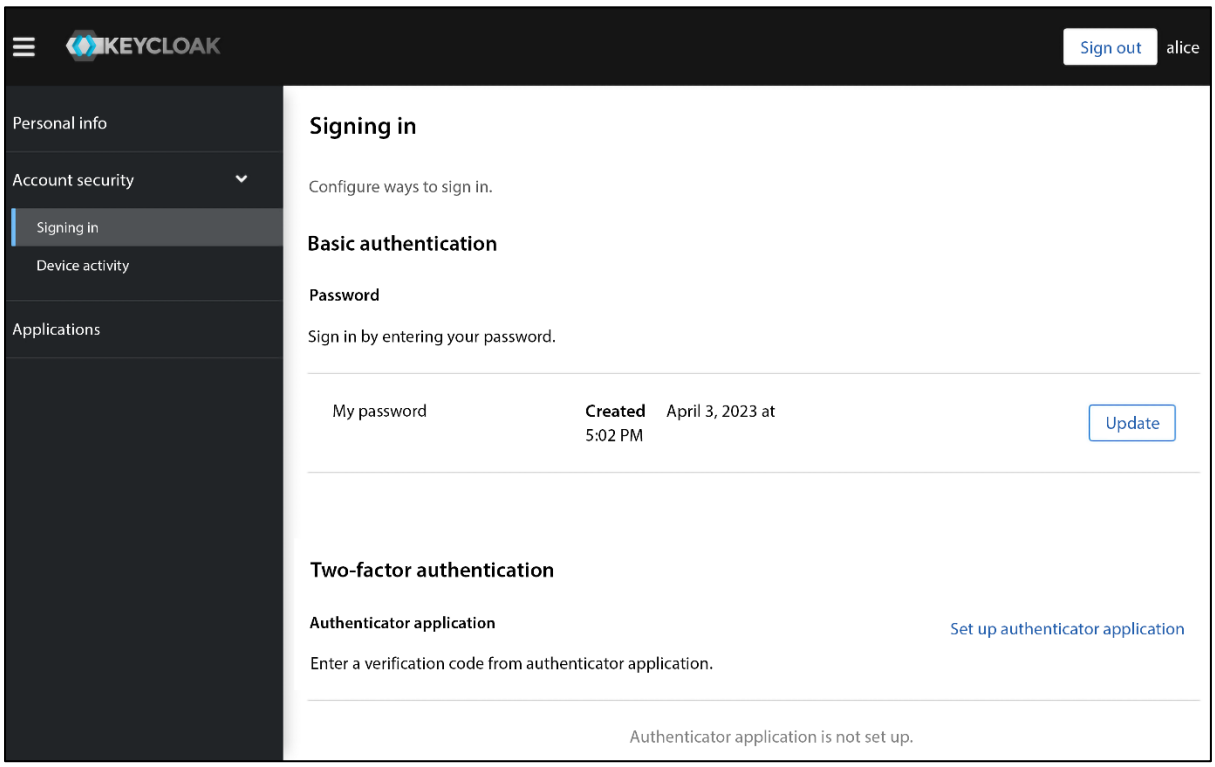

alice
Enabled
Action
Details
Attributes
Credentials
Role mapping
Groups
Consents
Identity pr
ID *
e550c67f-66d7-410f-990b-8a5ff14a91eb
Created at *
4/3/2023, 8:29:32 AM
Required user actions
Update Password
Select action
Username *
alice
Email
Email verified
No
First name
Last name
Save
Revert


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.

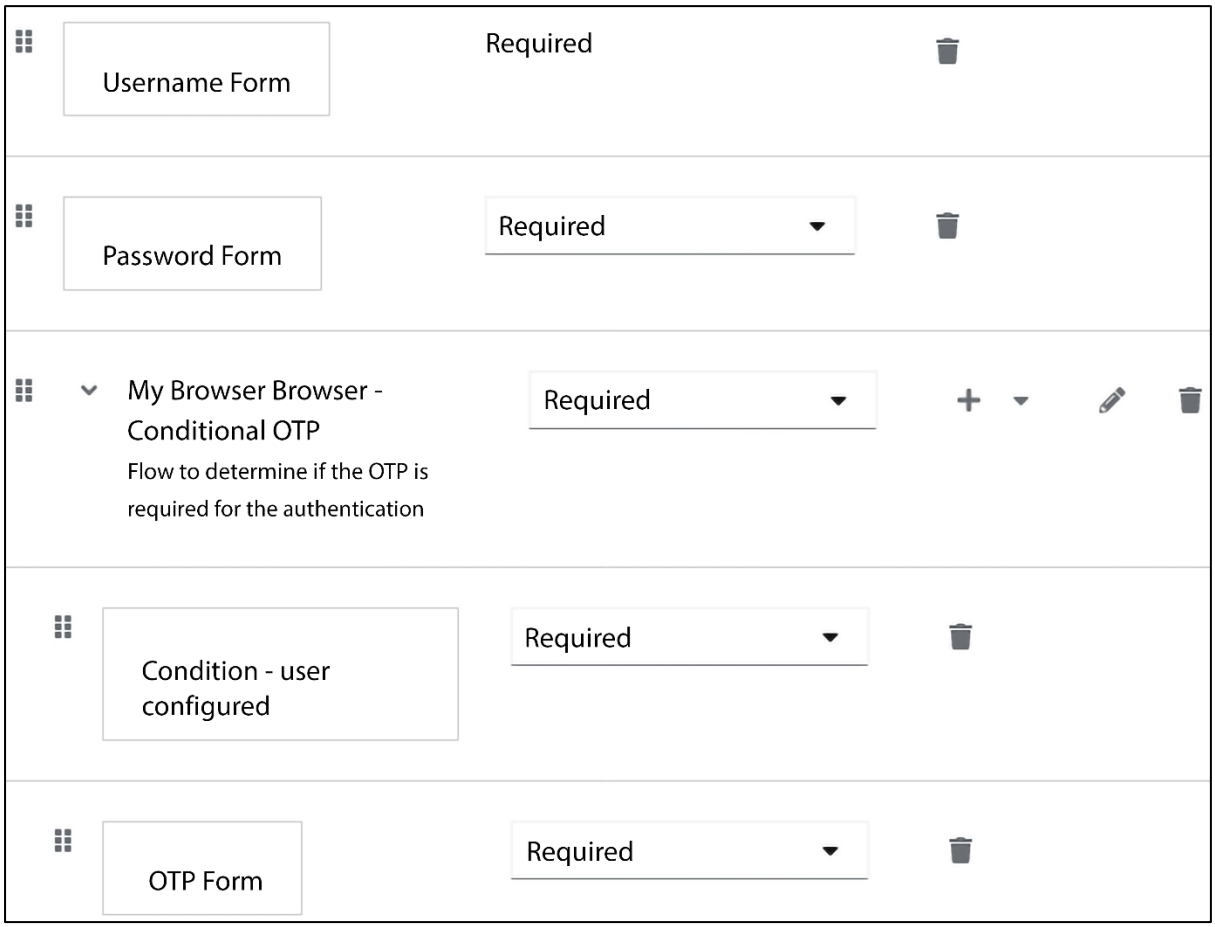
   Provide a Device Name to help you manage your OTP devices.

One-time code *

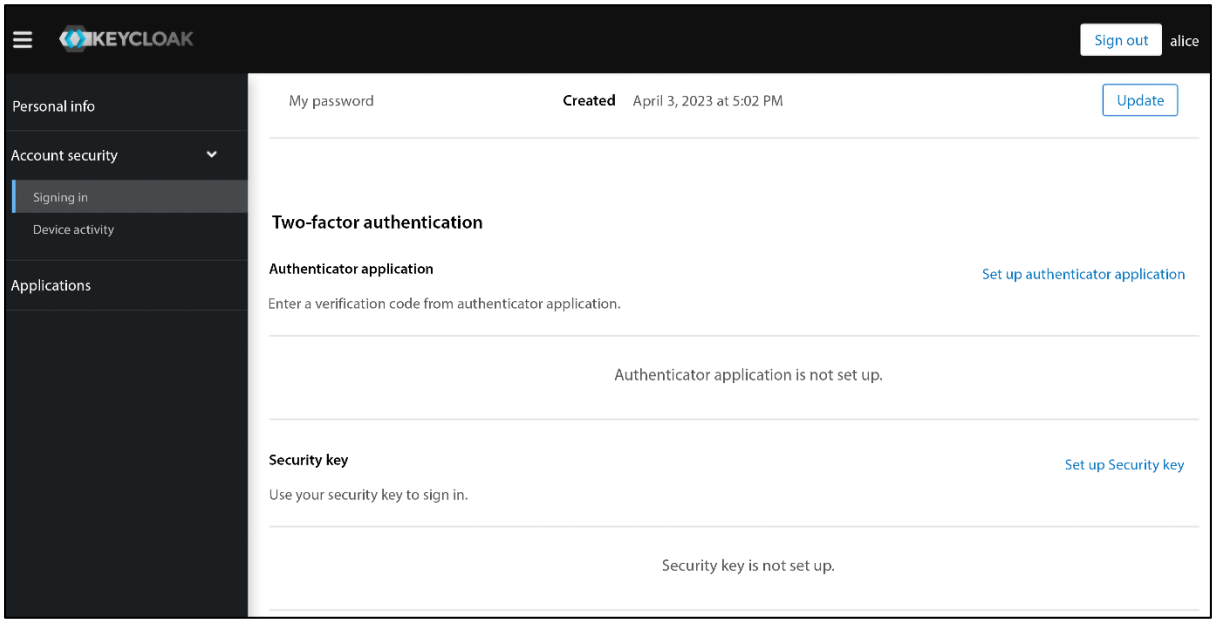
Device Name

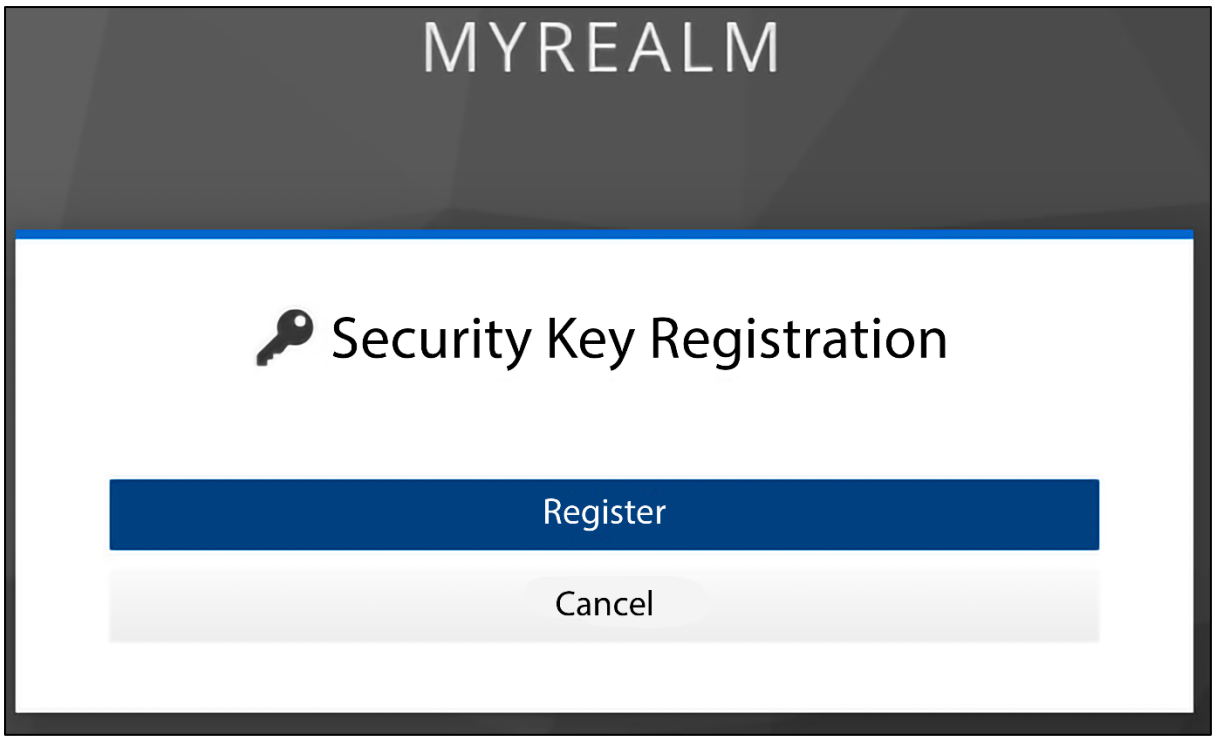
Submit Cancel

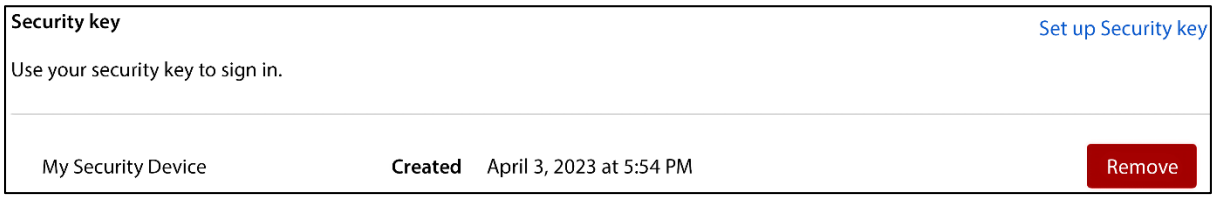

alice
One-time code
Sign In

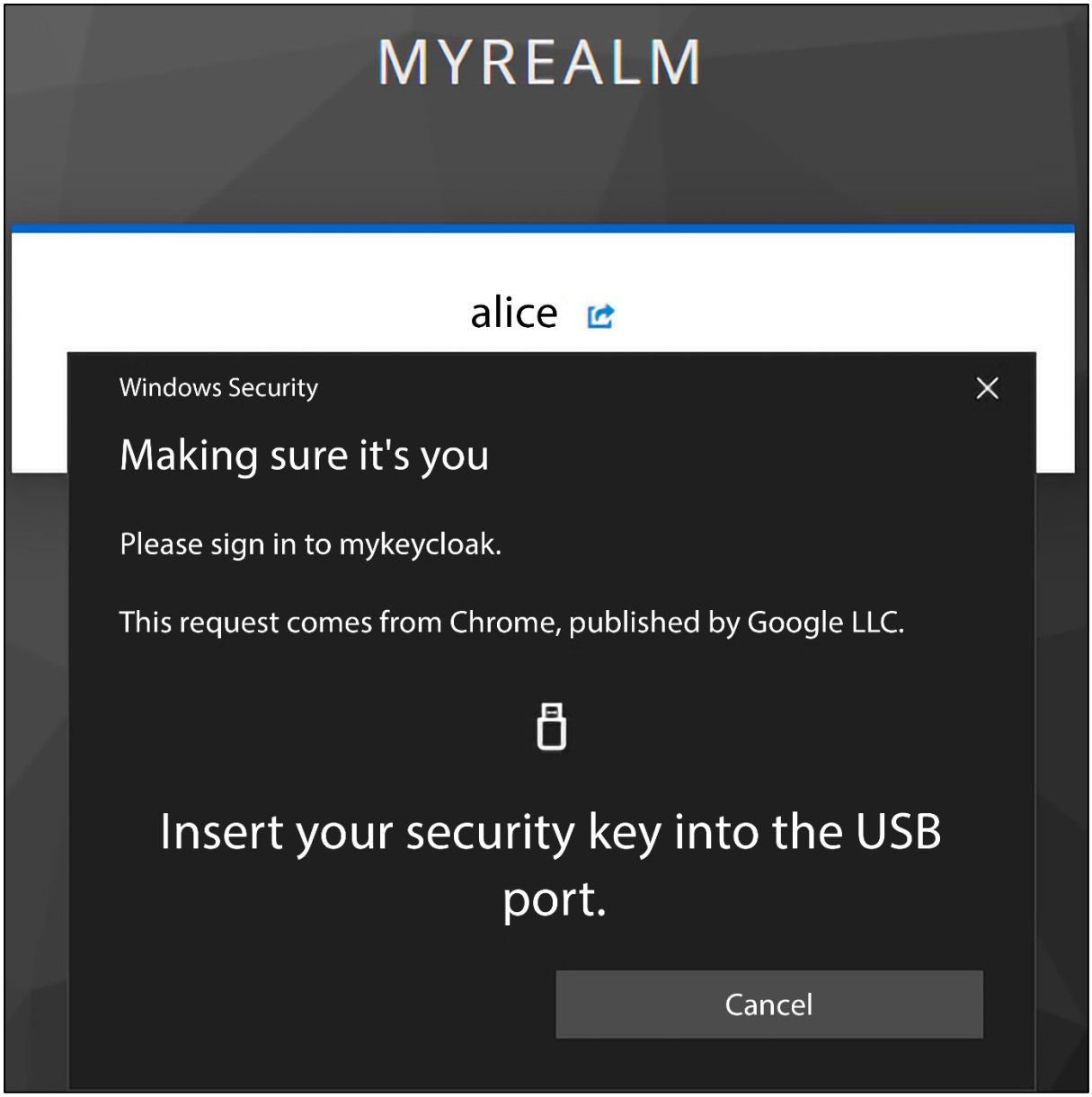

Username Form
Required
Password Form
Required
My Browser Browser - Conditional OTP
Flow to determine if the OTP is required for the authentication
Required
Condition - user configured
Required
OTP Form
Required


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

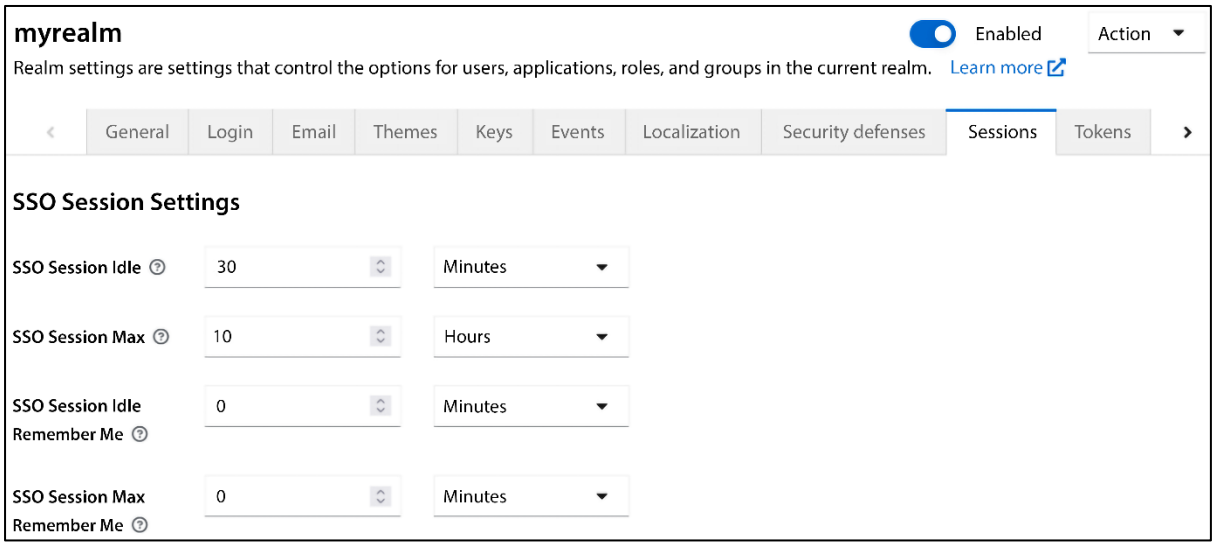

KEYCLOAK
Sign out
alice
Personal info
Account security
Signing in
Device activity
Applications
My password
Created April 3, 2023 at 5:02 PM
Update
Two-factor authentication
Authenticator application
Set up authenticator application
Enter a verification code from authenticator application.
Authenticator application is not set up.
Security key
Set up Security key
Use your security key to sign in.
Security key is not set up.

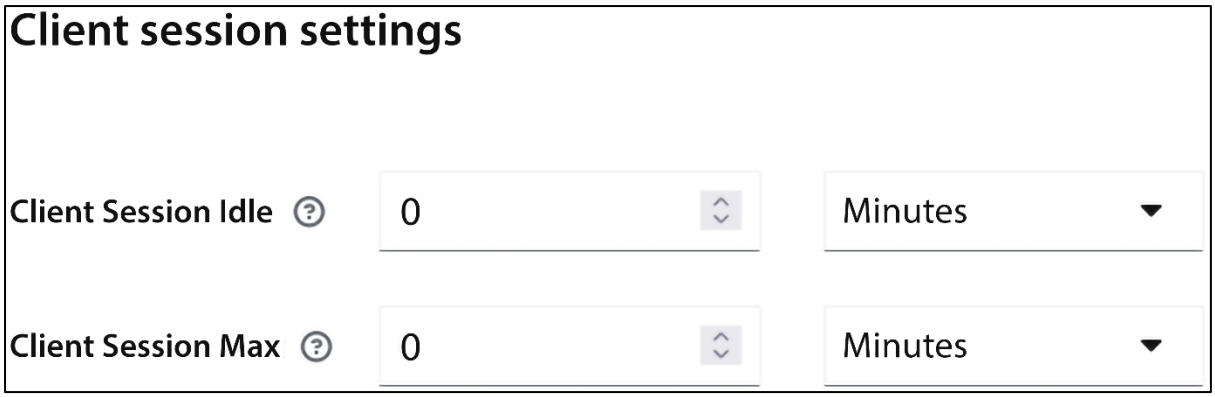

MYREALM
Security Key Registration
Register
Cancel

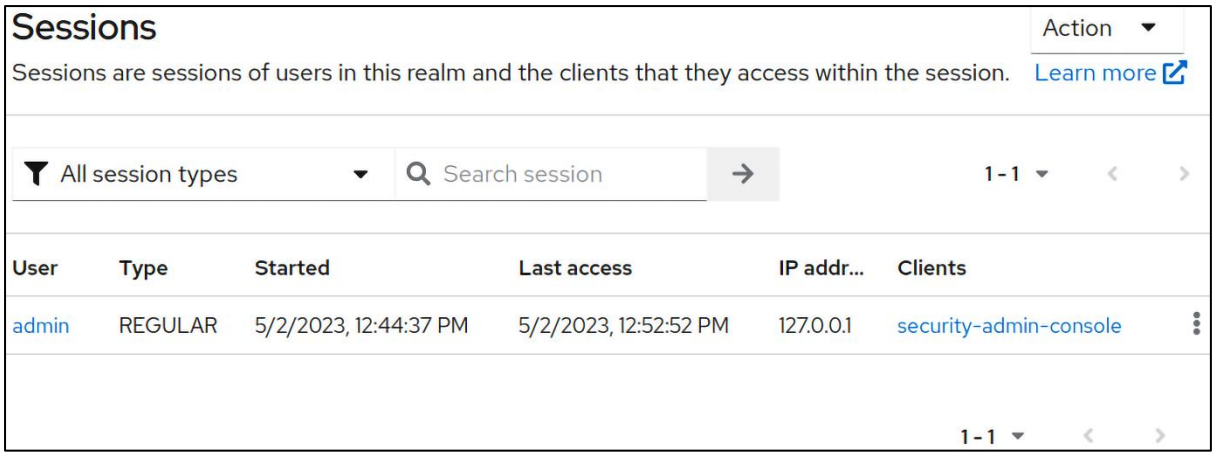

Security key
Set up Security key
Use your security key to sign in.
My Security Device
Created
April 3, 2023 at 5:54 PM
Remove

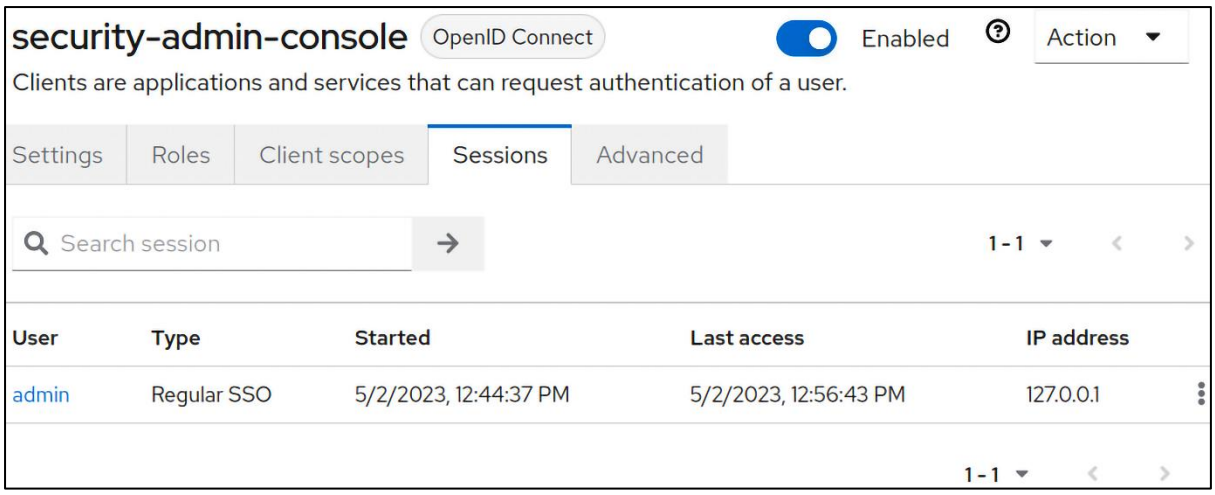

MYREALM
alice
Windows Security
Making sure it's you
Please sign in to mykeycloak.
This request comes from Chrome, published by Google LLC.
Insert your security key into the USB port.
Cancel

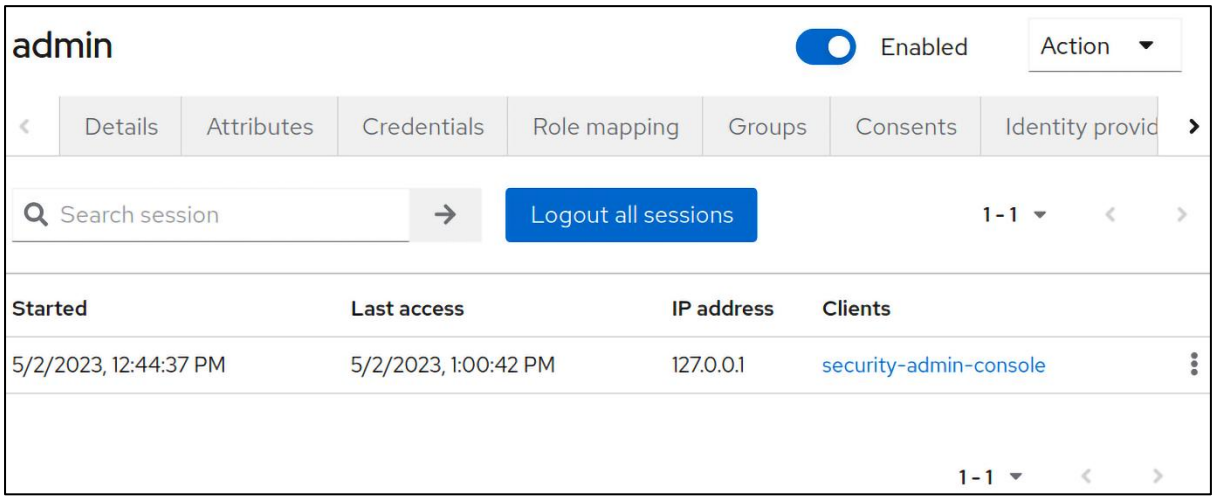
Chapter 12: Managing Tokens and Sessions

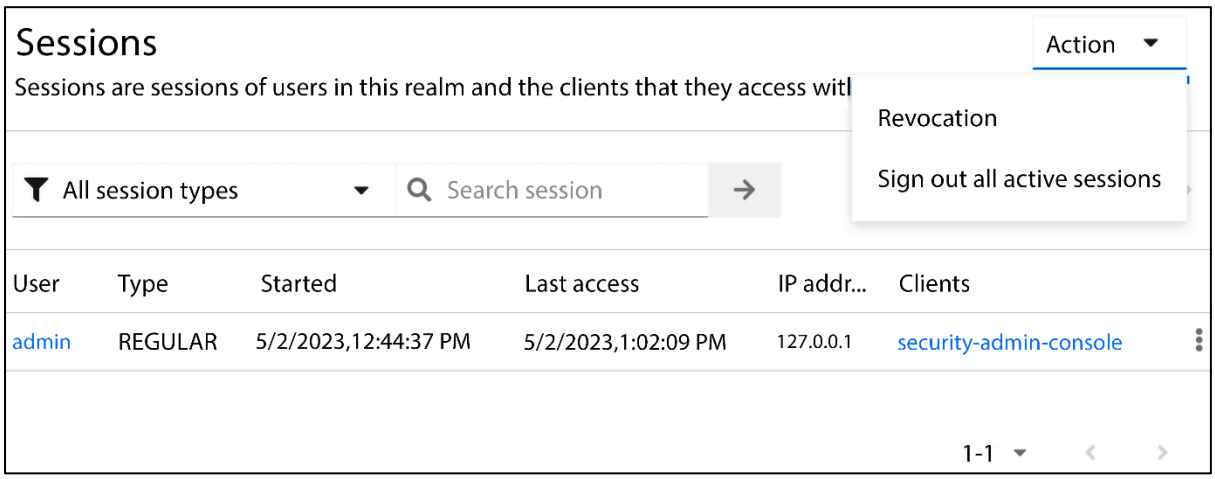


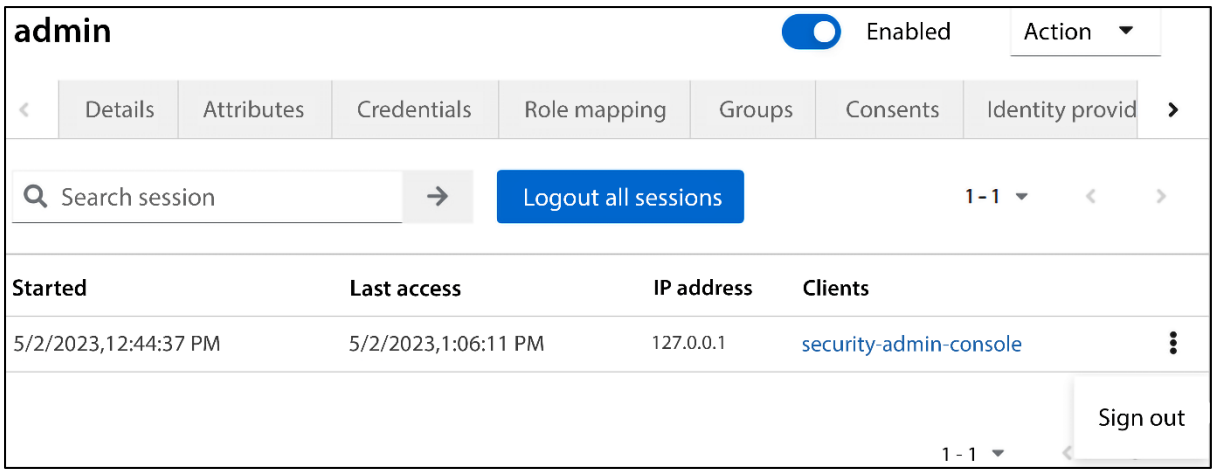


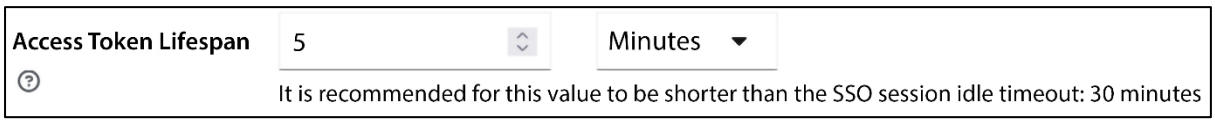


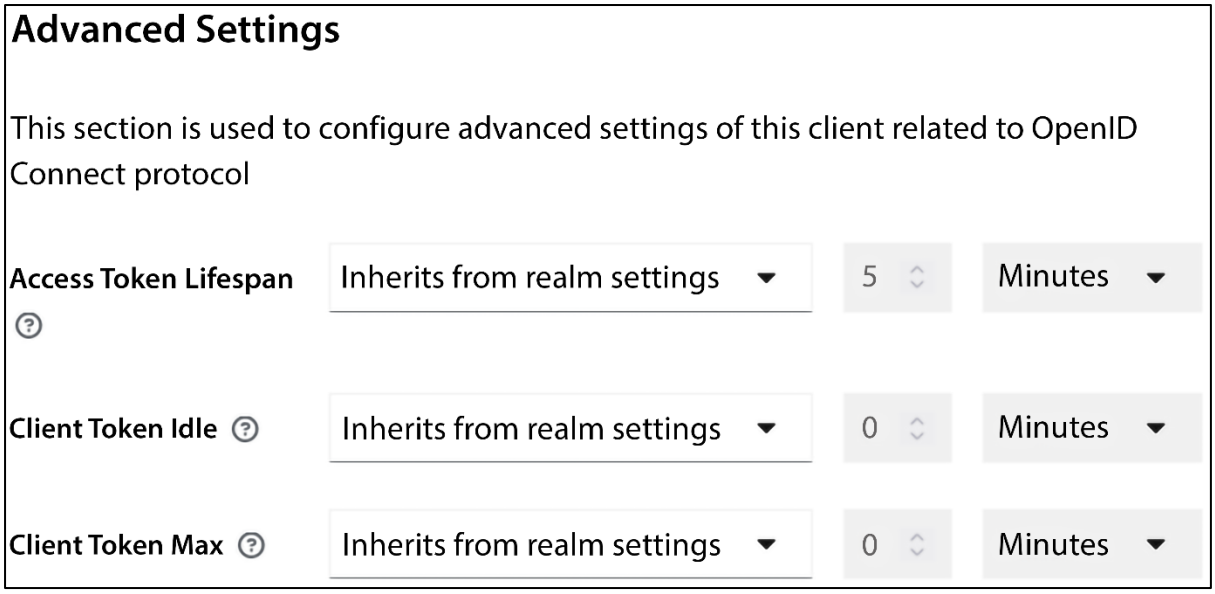

security-admin-console
OpenID Connect
Enabled
Action
Clients are applications and services that can request authentication of a user.
Settings
Roles
Client scopes
Sessions
Advanced
Search session
1 - 1
User
Type
Started
Last access
IP address
admin
Regular SSO
5/2/2023, 12:44:37 PM
5/2/2023, 12:56:43 PM
127.0.0.1
1 - 1


admin
Enabled
Action
Details
Attributes
Credentials
Role mapping
Groups
Consents
Identity provid
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 wit
Revocation
Sign out all active sessions
All session types
Search session
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
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

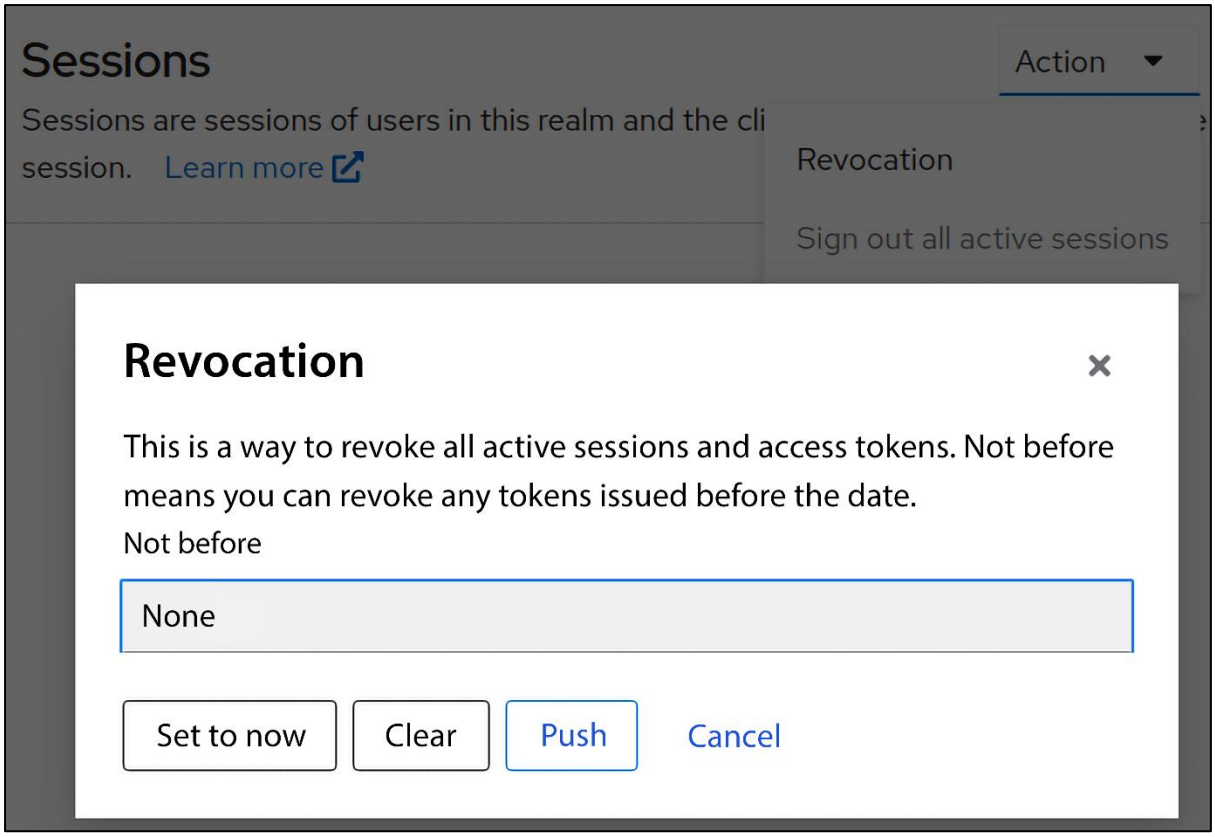
Access Token Lifespan	Inherits from realm settings	5	Minutes
Client Token Idle	Inherits from realm settings	0	Minutes
Client Token Max	Inherits from realm settings	0	Minutes

Refresh tokens

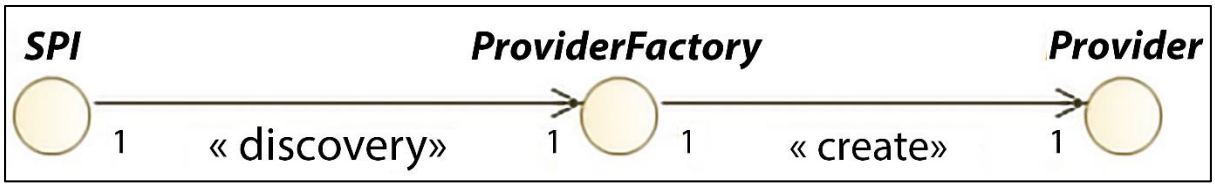
Revoke Refresh Token Enabled

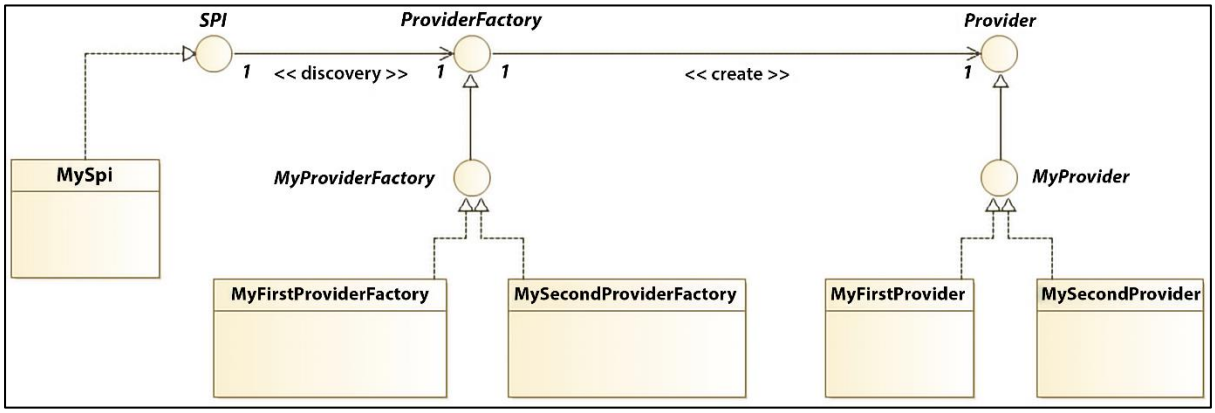
Refresh Token Max − 0 +

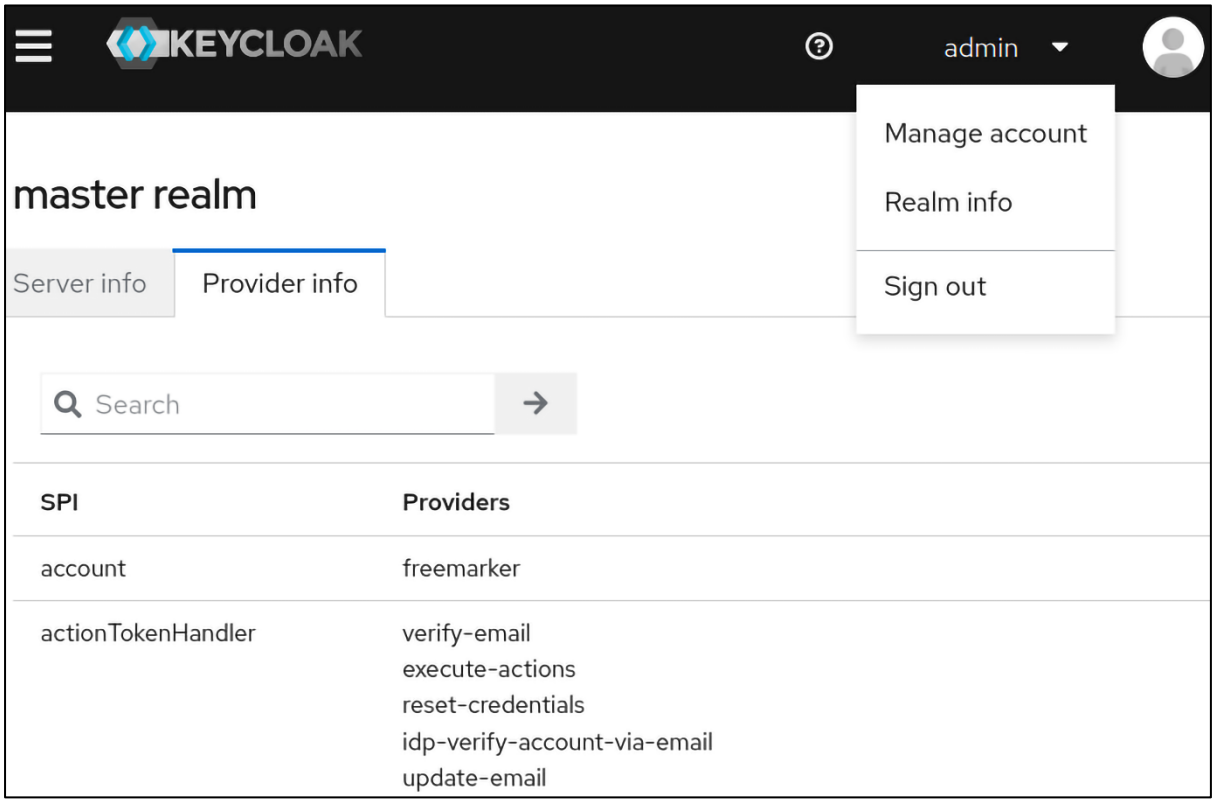
Reuse

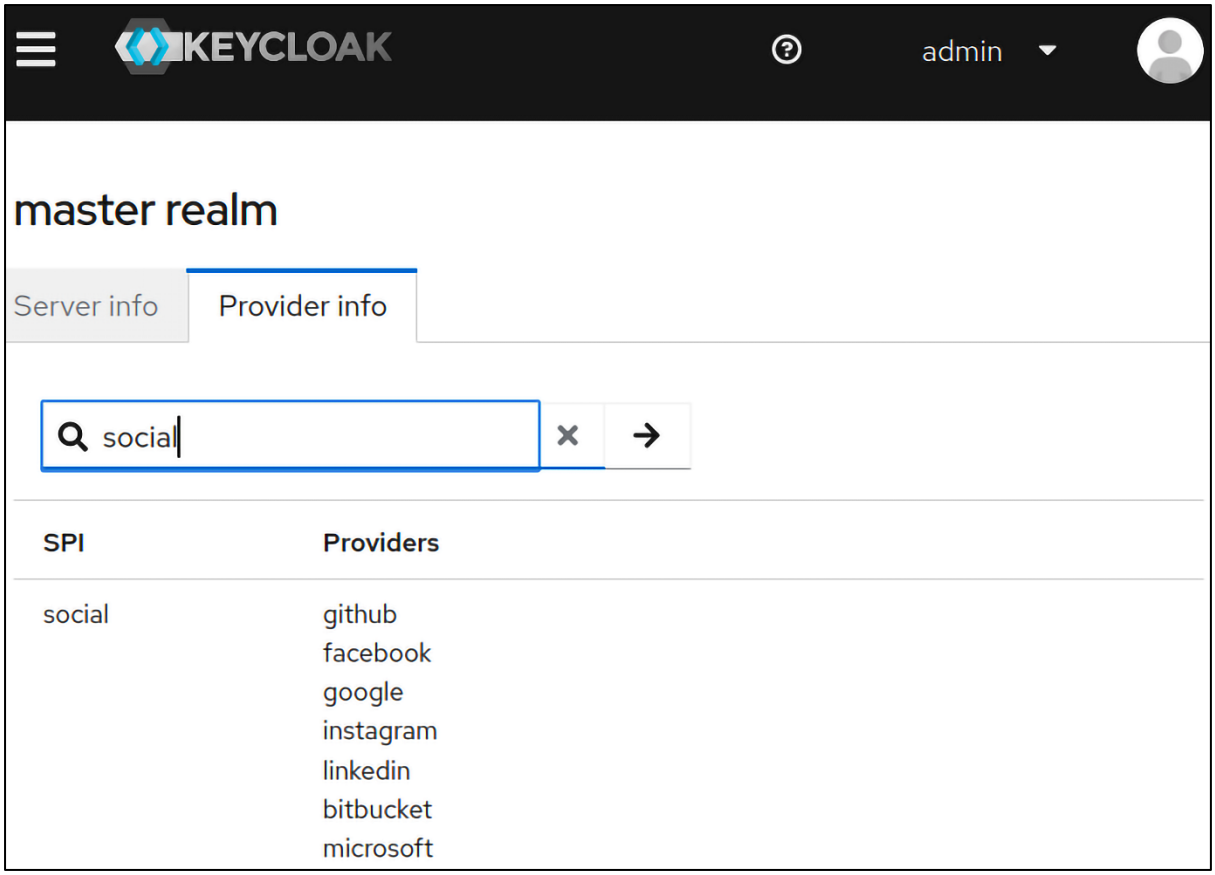

Sessions
Action
Sessions are sessions of users in this realm and the cli
session. Learn more
Revocation
Sign out all active sessions
Revocation
This is a way to revoke all active sessions and access tokens. Not before means you can revoke any tokens issued before the date.
Not before
None
Set to now
Clear
Push
Cancel

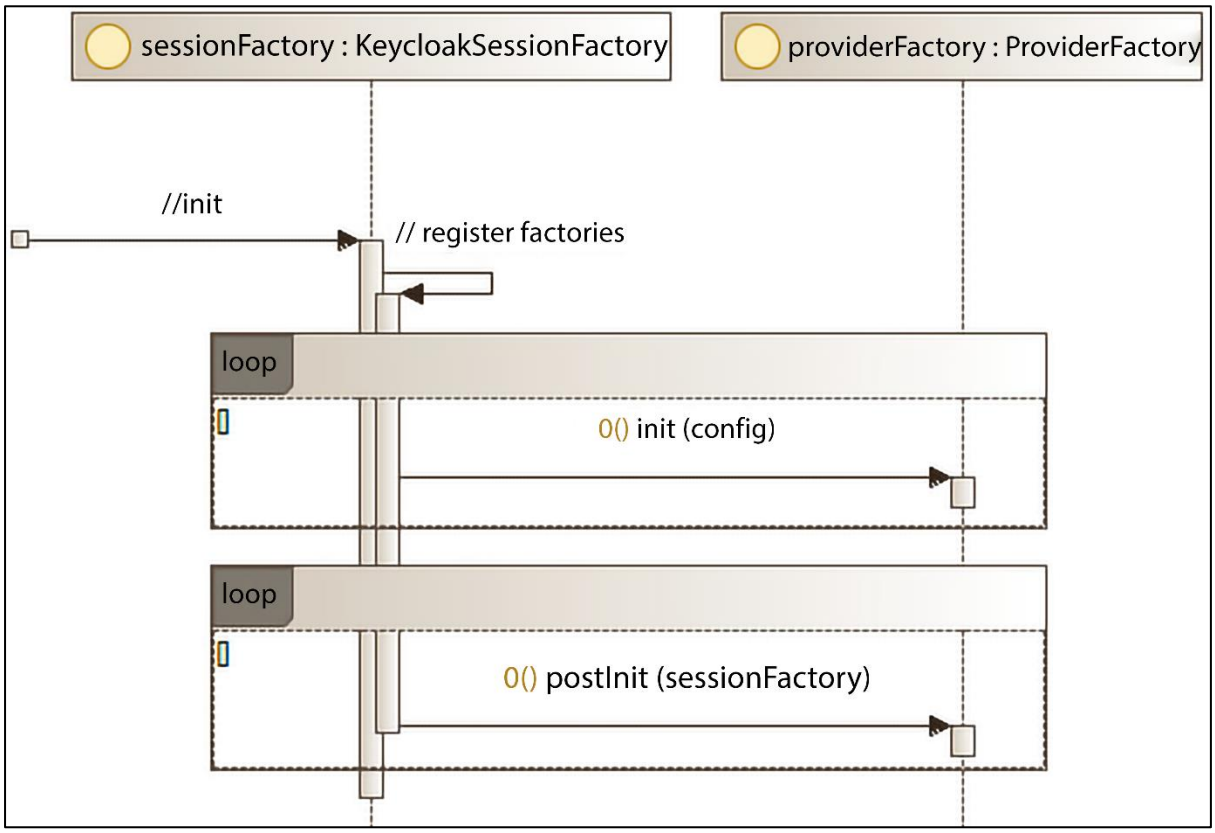
Chapter 13: Extending Keycloak

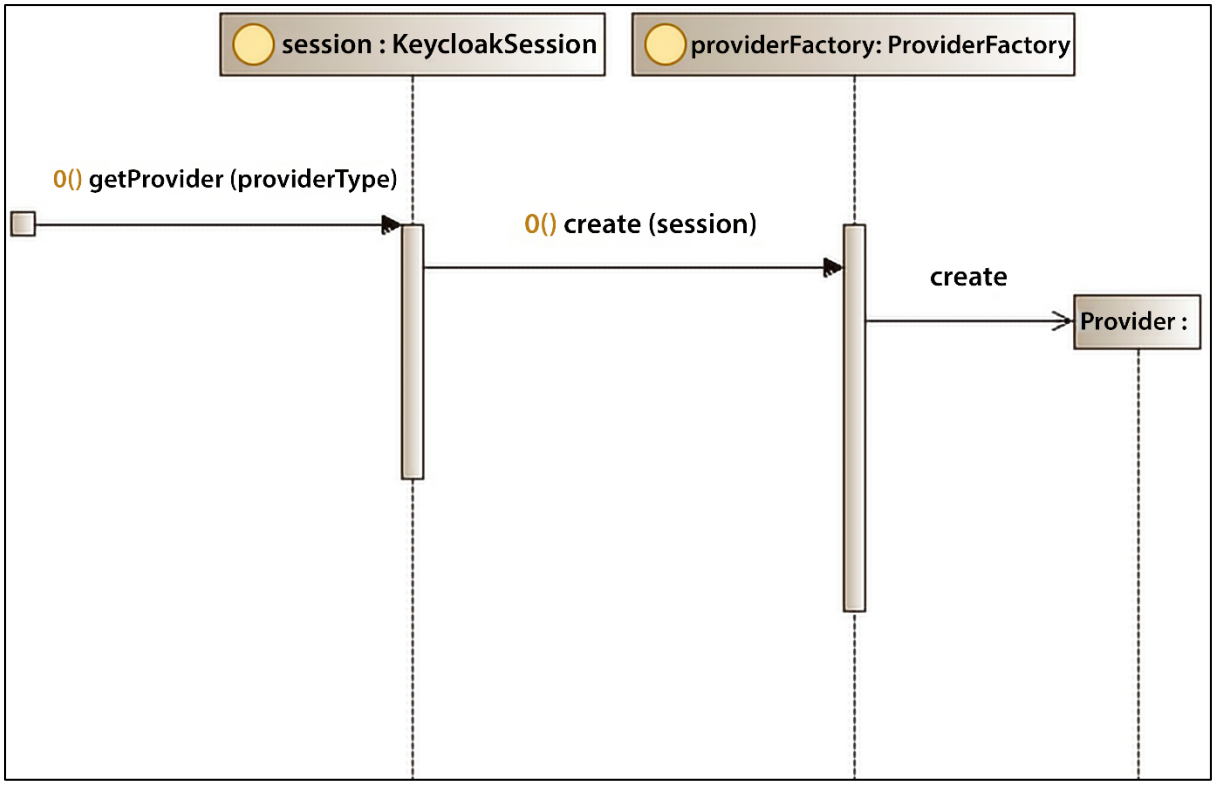


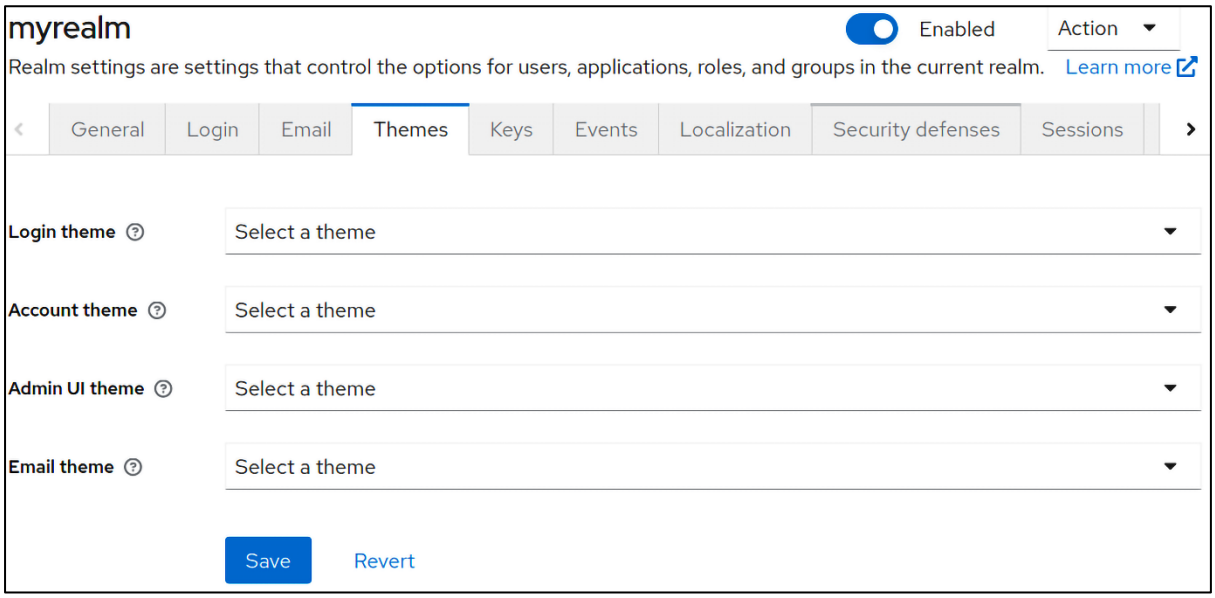


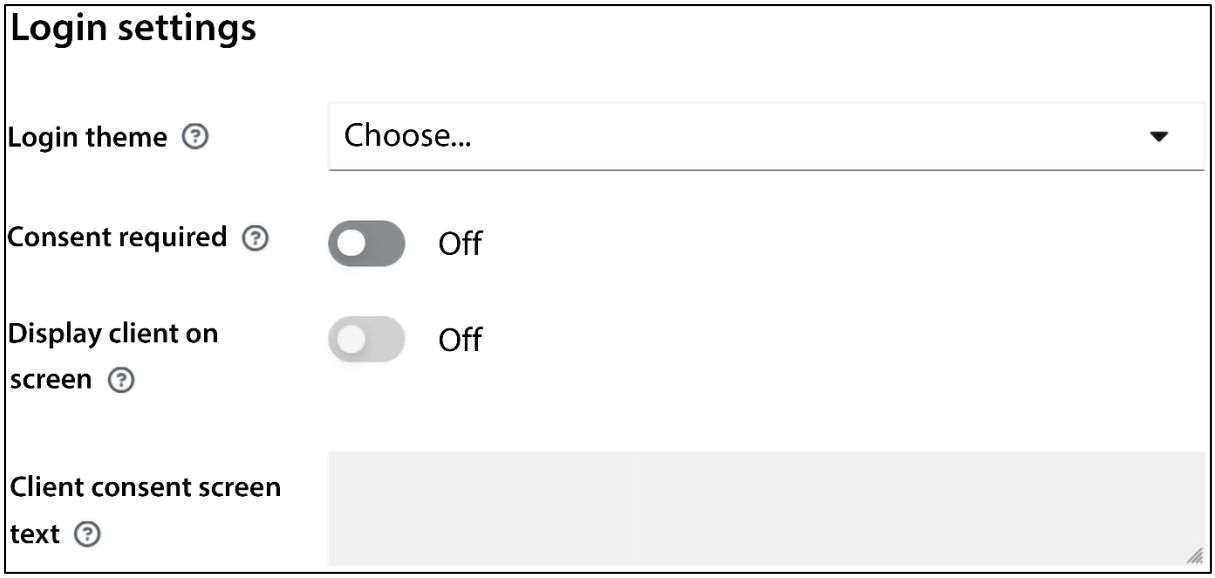


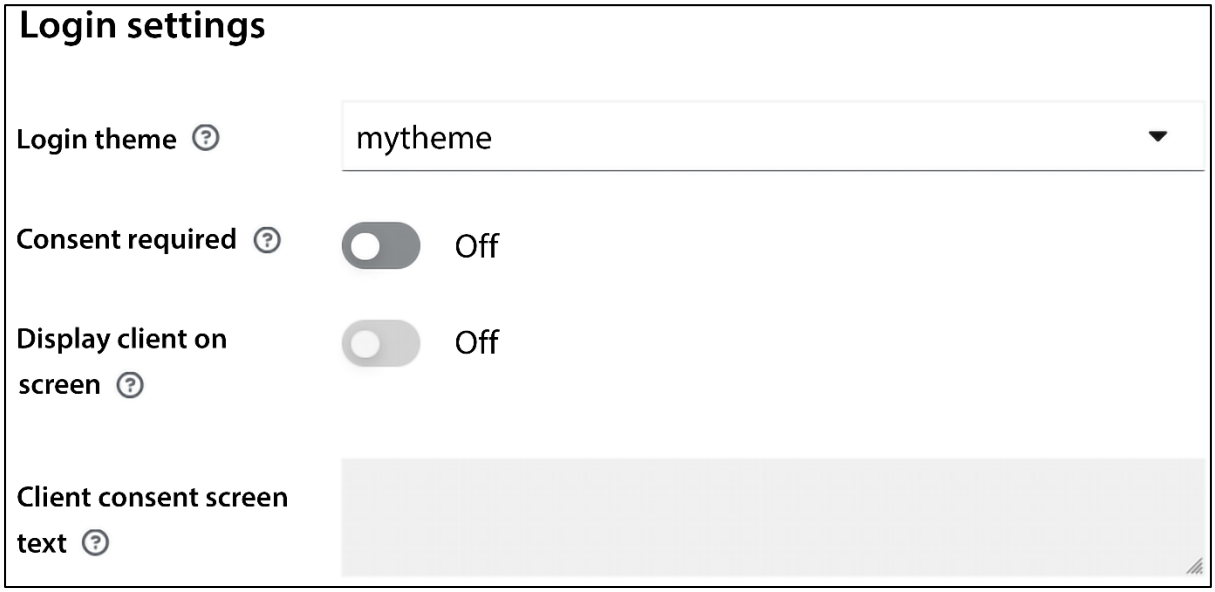

KEYCLOAK
admin
master realm
Server info
Provider info
social
SPI
Providers
social
github
facebook
google
instagram
linkedin
bitbucket
microsoft

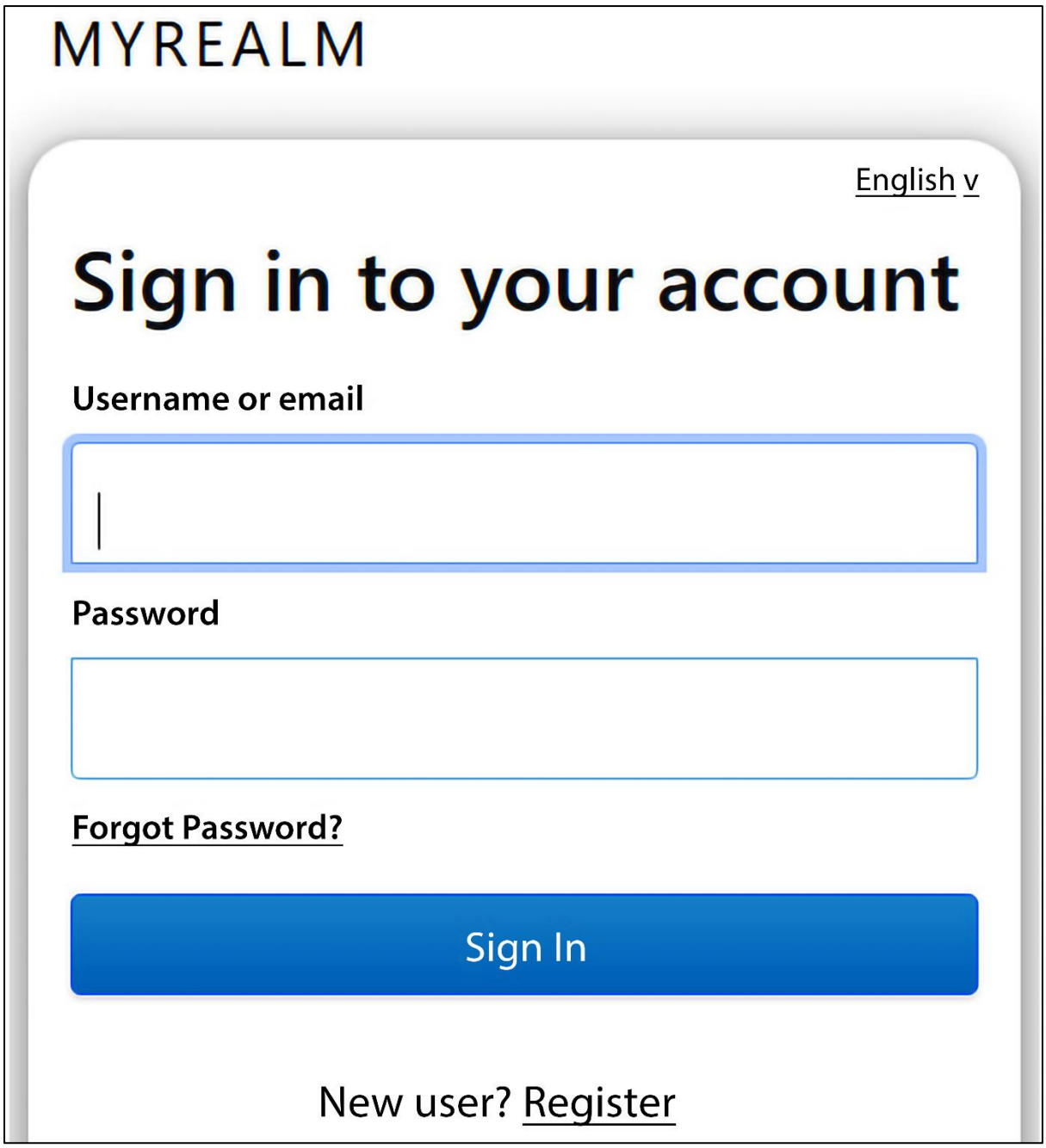

sessionFactory : KeycloakSessionFactory
providerFactory : ProviderFactory
//init
// register factories
loop
0() init (config)
loop
0() postInit (sessionFactory)


session : KeycloakSession
providerFactory: ProviderFactory
0() getProvider (providerType)
0() create (session)
create
Provider :


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

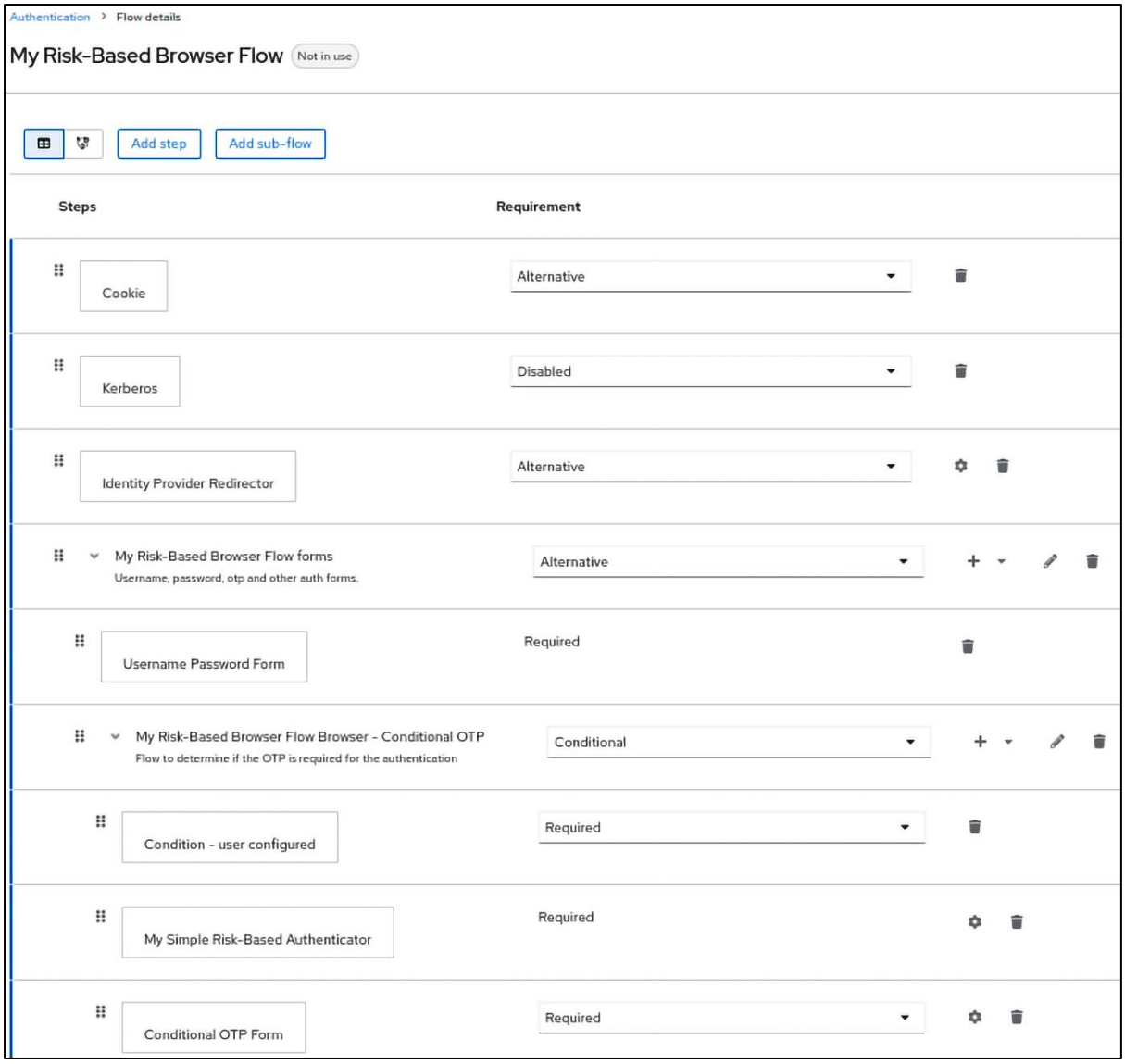
Skip OTP for Header

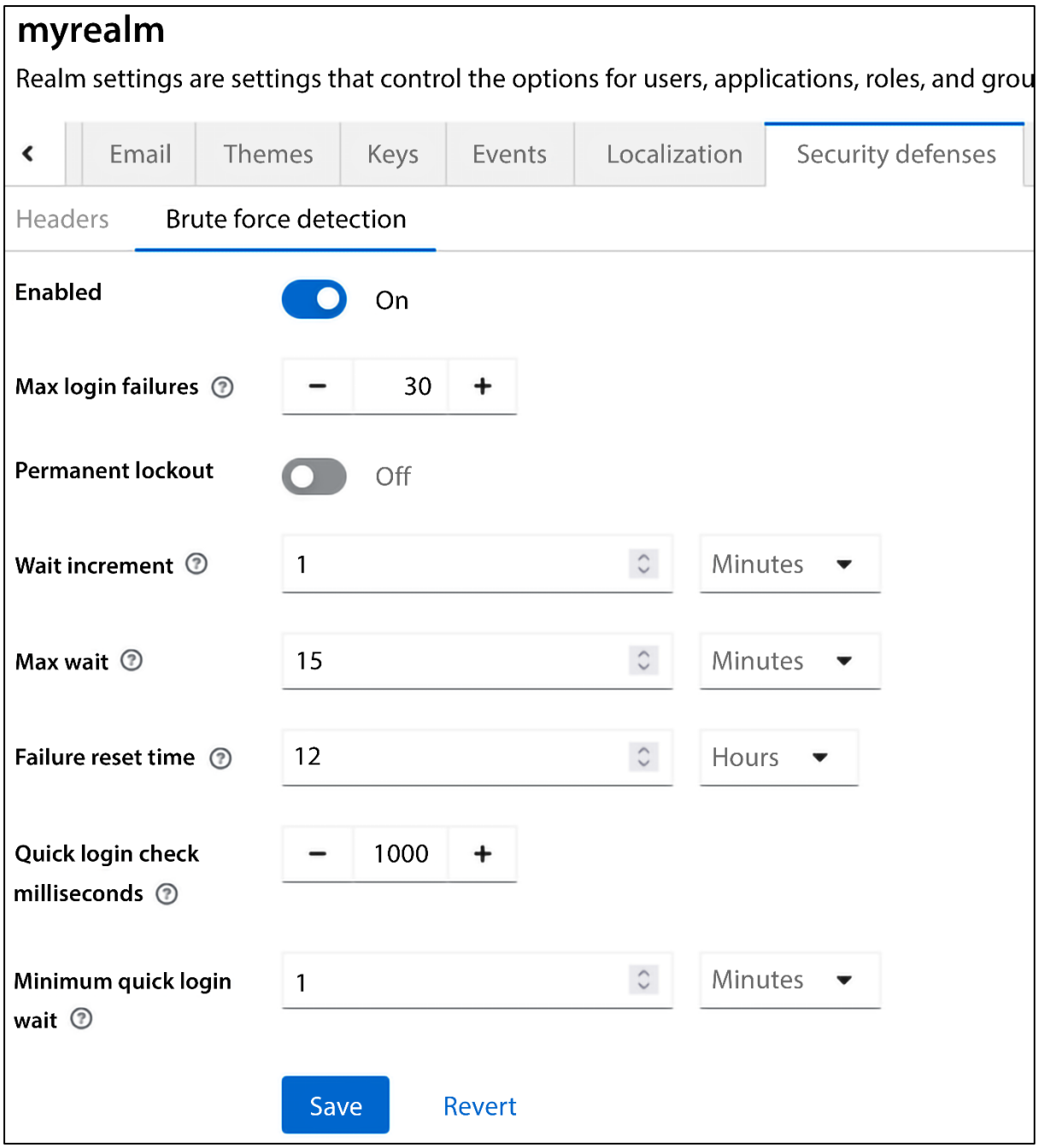
Force OTP for Header

Fallback OTP handling

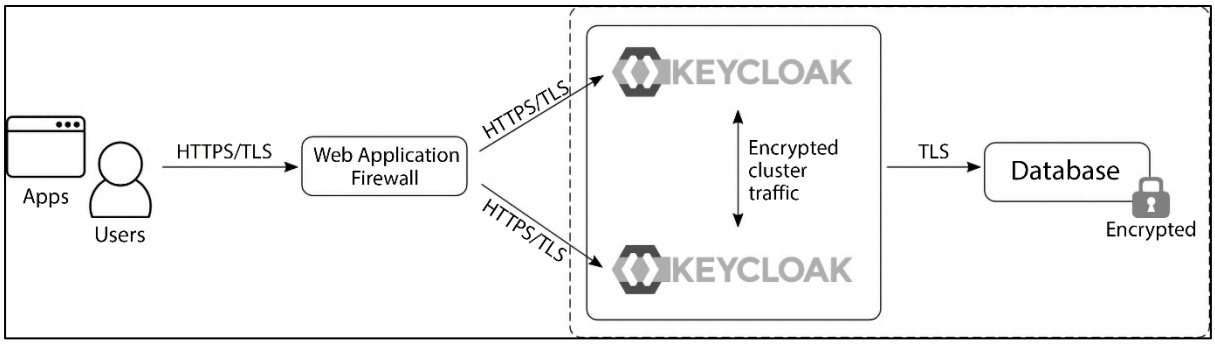
force

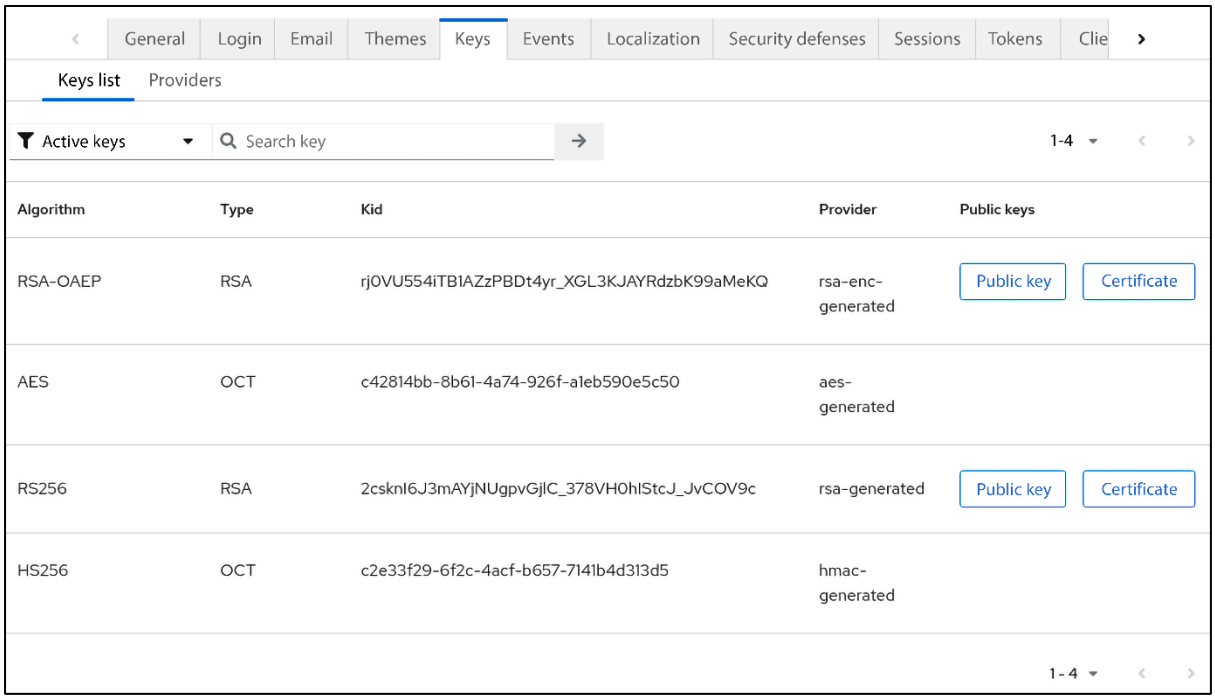
Save Cancel

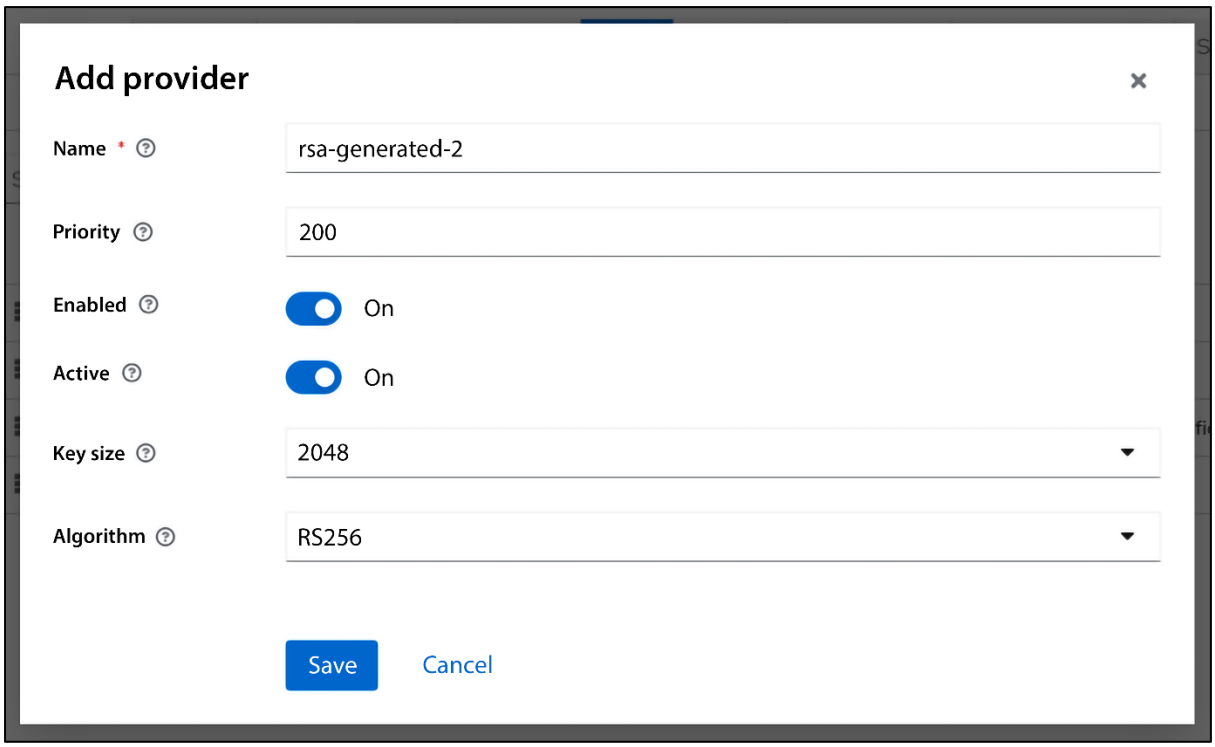

Authentication
Flow details
My Risk-Based Browser Flow
Not in use
Add step
Add sub-flow
Steps
Requirement
Cookie
Alternative
Kerberos
Disabled
Identity Provider Redirector
Alternative
My Risk-Based Browser Flow forms
Username, password, otp and other auth forms.
Alternative
Username Password Form
Required
My Risk-Based Browser Flow 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

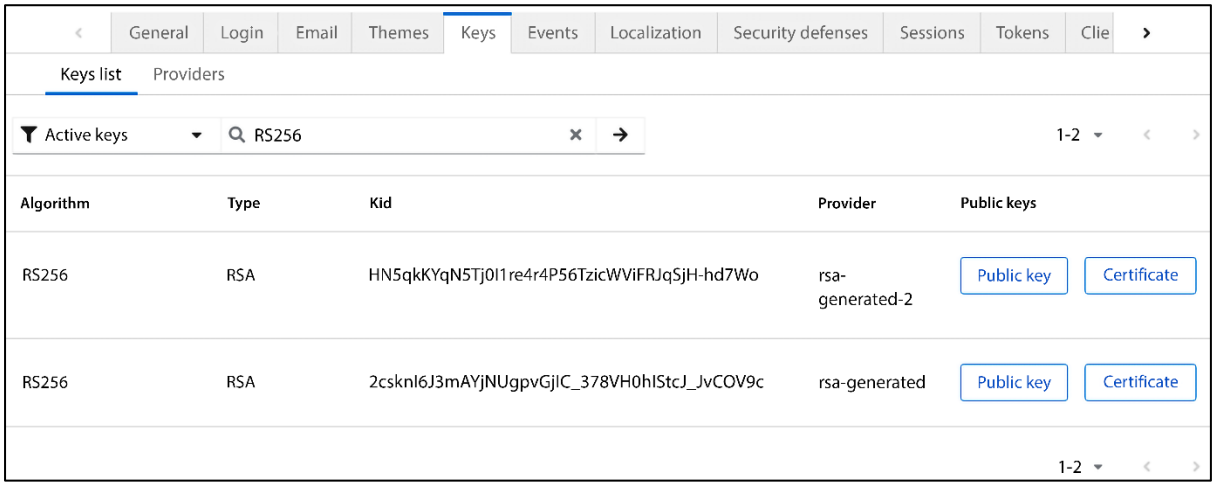

myrealm
Realm settings are settings that control the options for users, applications, roles, and grou
Email
Themes
Keys
Events
Localization
Security defenses
Headers
Brute force detection
Enabled
On
Max login failures
30
Permanent lockout
Off
Wait increment
1
Minutes
Max wait
15
Minutes
Failure reset time
12
Hours
Quick login check milliseconds
1000
Minimum quick login wait
1
Minutes
Save
Revert

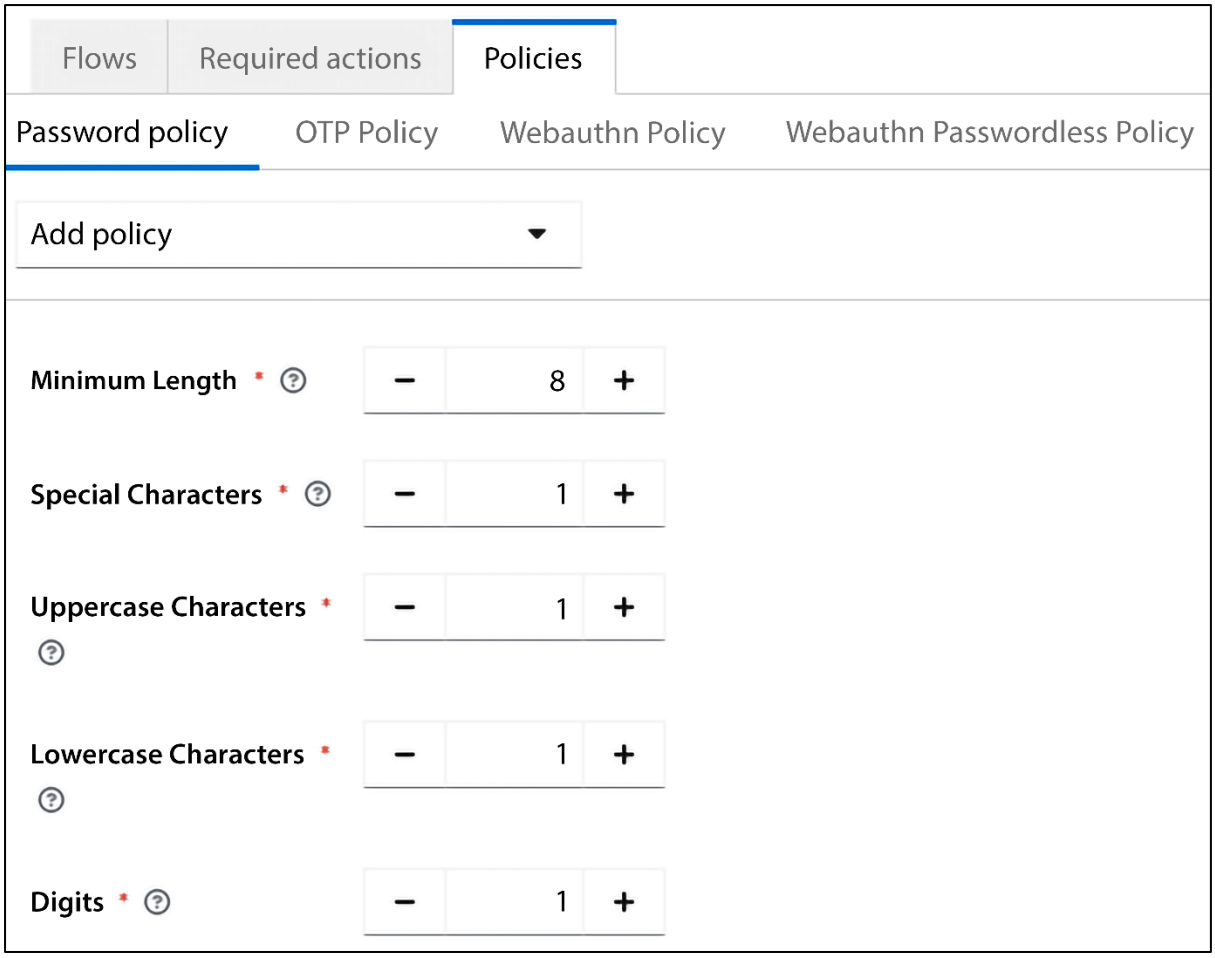
Chapter 14: Securing Keycloak and Applications

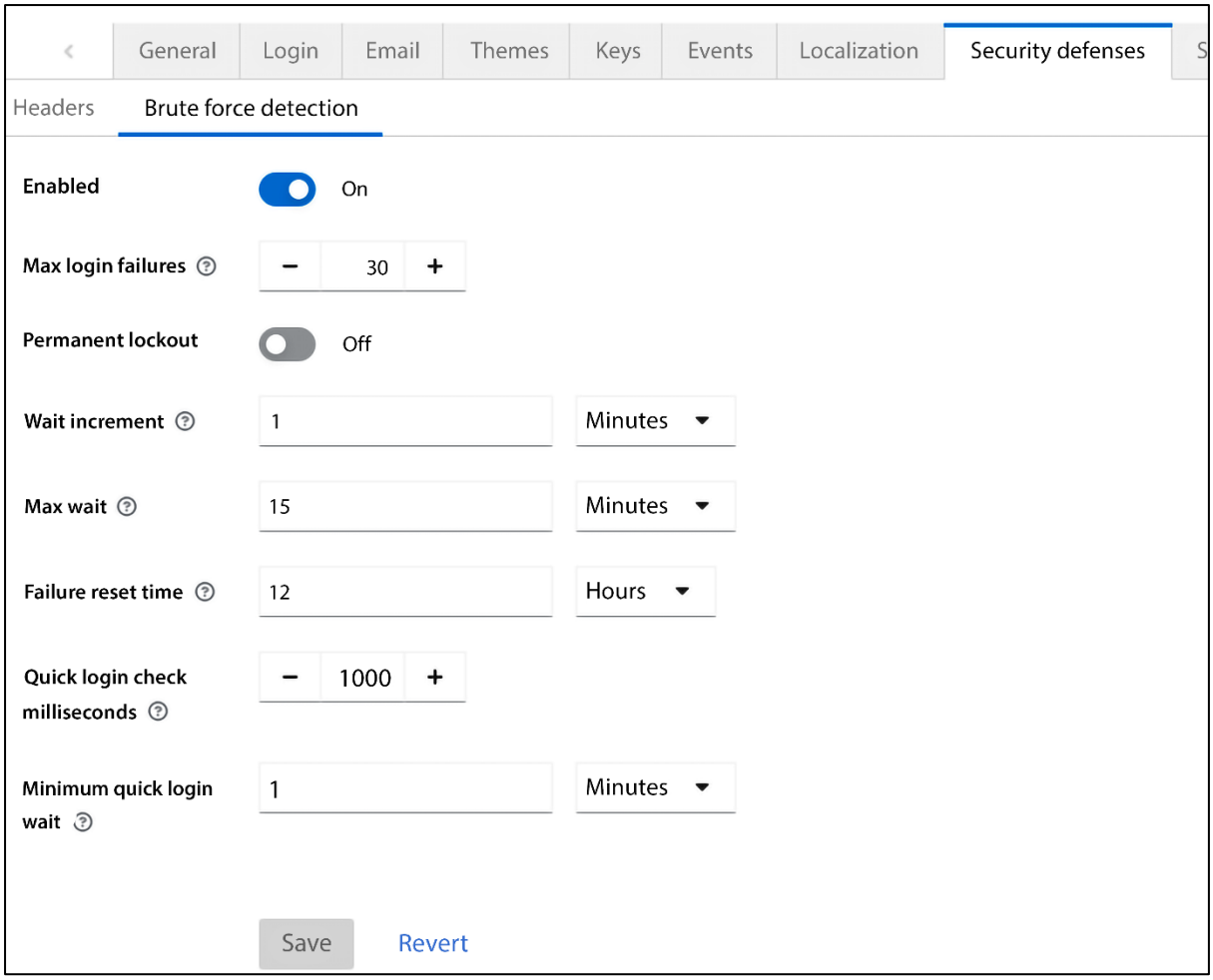


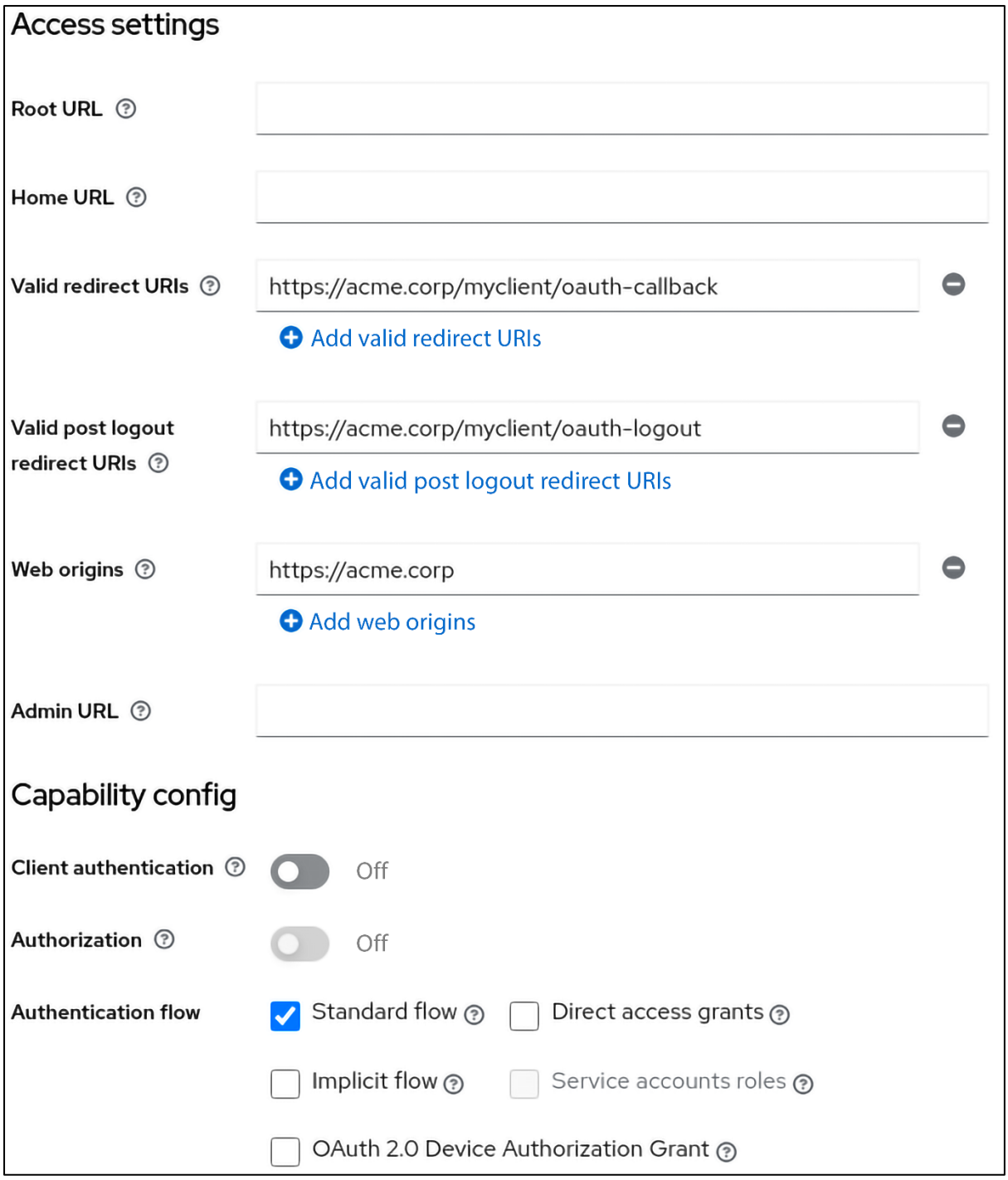



Add provider
Name *
rsa-generated-2
Priority
200
Enabled
On
Active
On
Key size
2048
Algorithm
RS256
Save
Cancel


General
Login
Email
Themes
Keys
Events
Localization
Security defenses
Sessions
Tokens
Clie
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
2csknI6J3mAYjNUgpvGjIC_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
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
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