

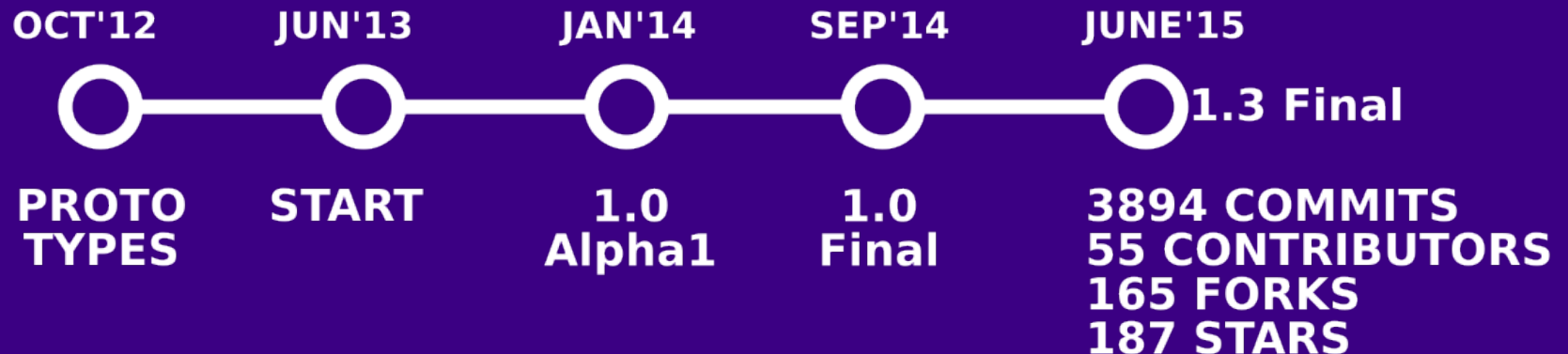
ENTERPRISE SECURITY WITH KEYCLOAK

From the Intranet to Mobile

By Divya Mehra and Stian Thorgersen



PROJECT TIMELINE



AGENDA

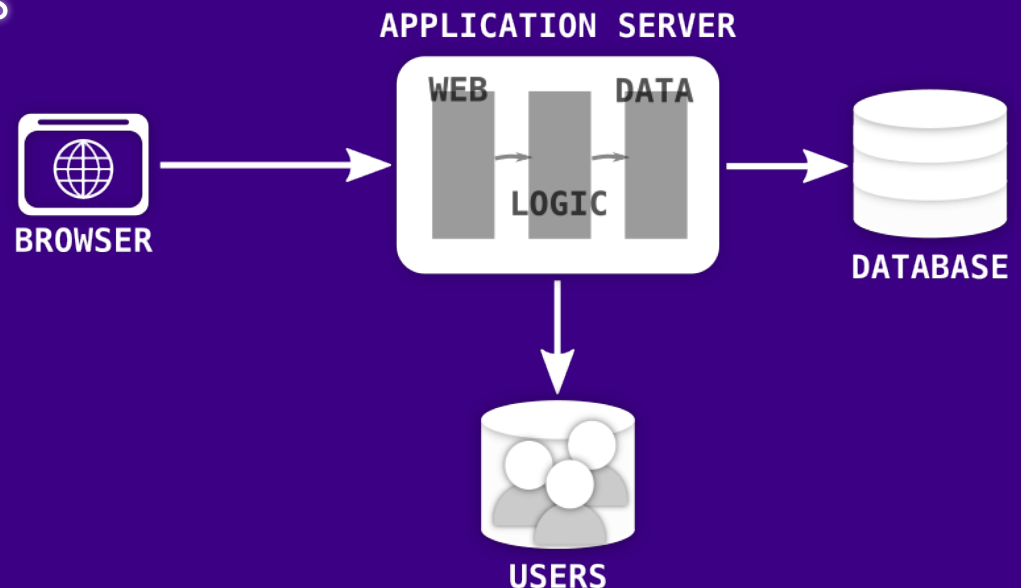




CHALLENGES

THE OLD WAY

- Securing monolithic web app relatively easy
- Username and password form
- Credentials verified against table in DB
- HTTP Session stores security context



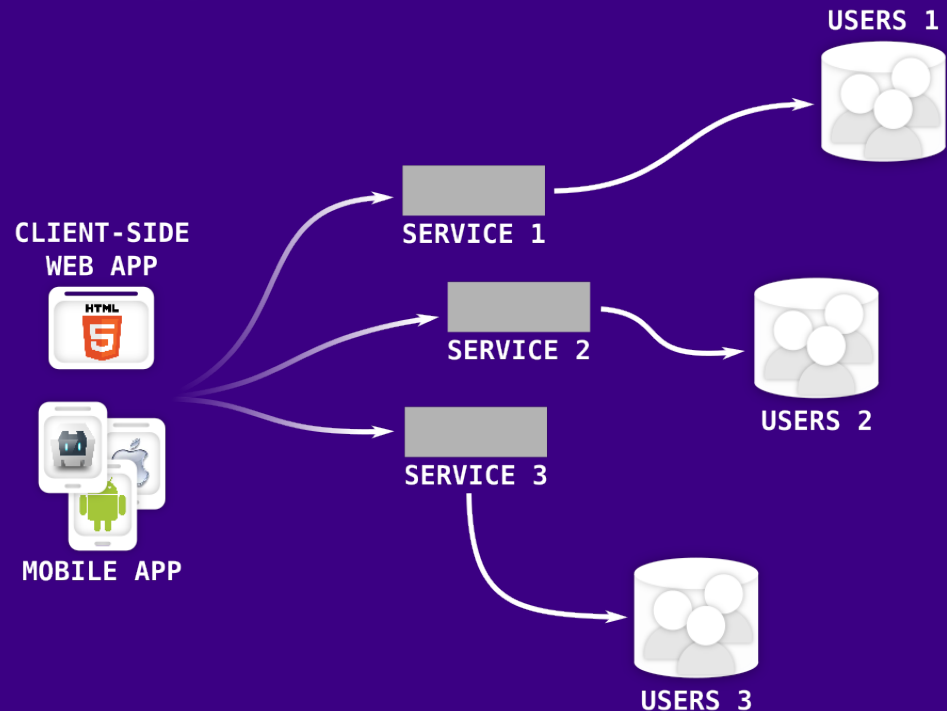
IT'S NOT JUST A FORM AND A TABLE ANYMORE

- Enterprise software has changed
- No longer one or two apps inside firewall
- Now we have many separate systems
- Exposed to mobile users and partners



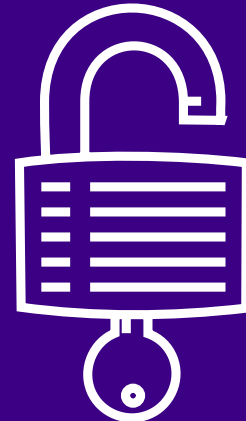
THE NEW WAY?

- Multiple apps
- Multiple variants of each app
- Multiple services
- Multiple user dbs
- Multiple logins
- Outside firewall



AUTHENTICATION

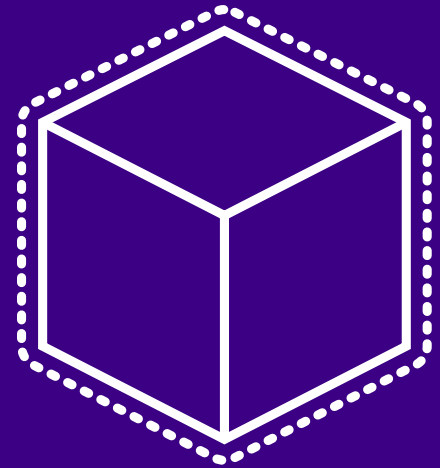
- Passwords not sufficient
- Users create bad passwords (123456 and password)
- Passwords policies help, but no guarantee
- Users reuse passwords
- Passwords can be lost
- Secure storage is required
- Need two-factor authentication



APP TYPES

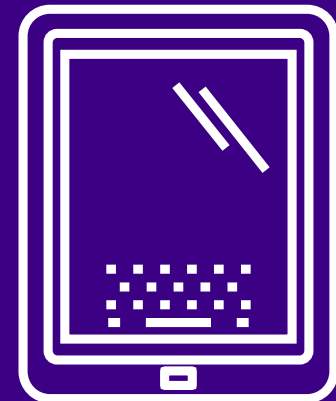
Have to deal with many app, variants & programming languages

- Client-side and server-side web
- Mobile (native and hybrid)
- APIs/Services
- ...



MOBILE

- Users don't want to login frequently
- Don't store username and password on phone
- What if device is lost?
- Sessions and cookies aren't ideal
- Requires public services



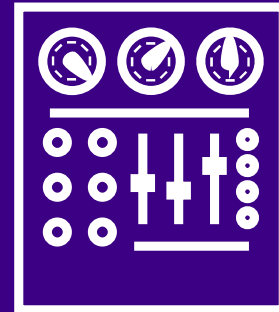
SINGLE SIGN-ON

- Not as trivial as it may seem
- Single Sign-Out can be even harder
- Need Remote Sign-Out



MANAGE

- Apps
- Services
- Users
- Devices
- Permissions
- Sessions and logs



and.. Ideally manage everything from one console

SELF SERVICE

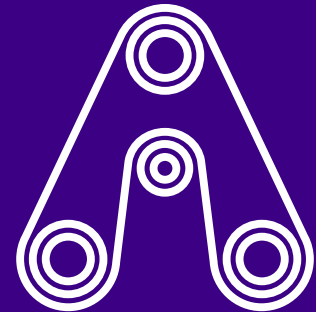
- Users can manage their own accounts
- Recover password
- Update profile
- Enable two-factor authentication
- Manage sessions
- Account history



and.. Ideally manage everything from one console

INTEGRATION

- Third party apps
- Existing Infrastructure
- New Infrastructure after acquisition
- External users
- Social networks



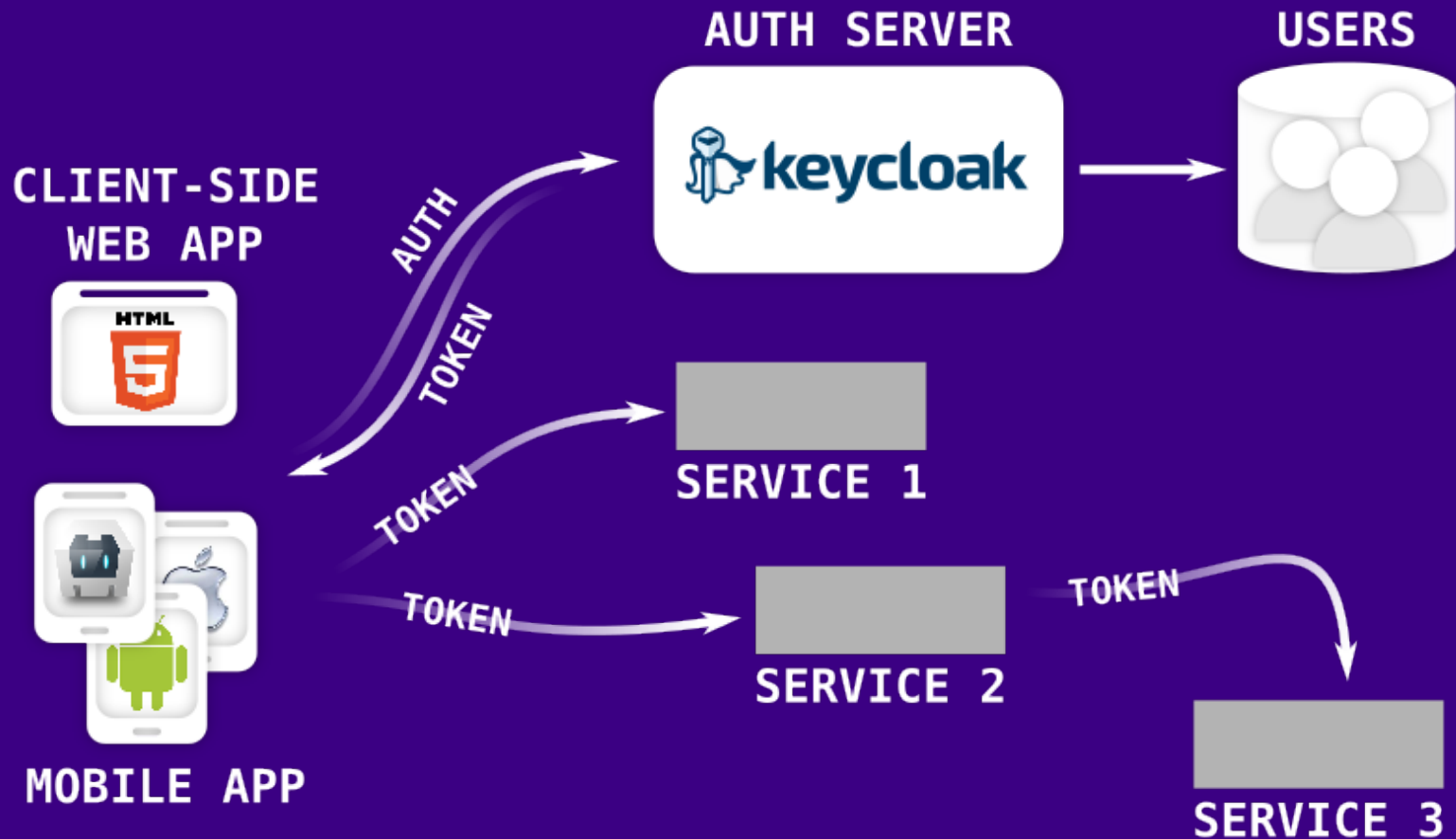
VULNERABILITIES

- Broken Authentication and Session Management is #2 on Open Web Application Security Project (OWASP) Top Ten list
- Recommendation is to not implement your own!



SOLUTION





PROTOCOLS

- OpenID Connect
- SAML 2.0

OPENID CONNECT

- Built on OAuth 2.0
- RESTful
- JSON
- Easy to use
- Less mature - final spec released last year

SAML 2.0

- XML
- Harder to use and understand
- Mature - 1.0 was adopted as an OASIS standard in 2002

TOKENS

- Decouples authentication
- Cross-domain
- Stateless
- Only sent when needed
- Standards based

AUTHENTICATION

- Authenticate with Keycloak
- Login forms provided by Keycloak
- Two-factor authentication
- Requires SSL
- Passwords are salted and hashed with PBKDF2
 - Iterations configurable

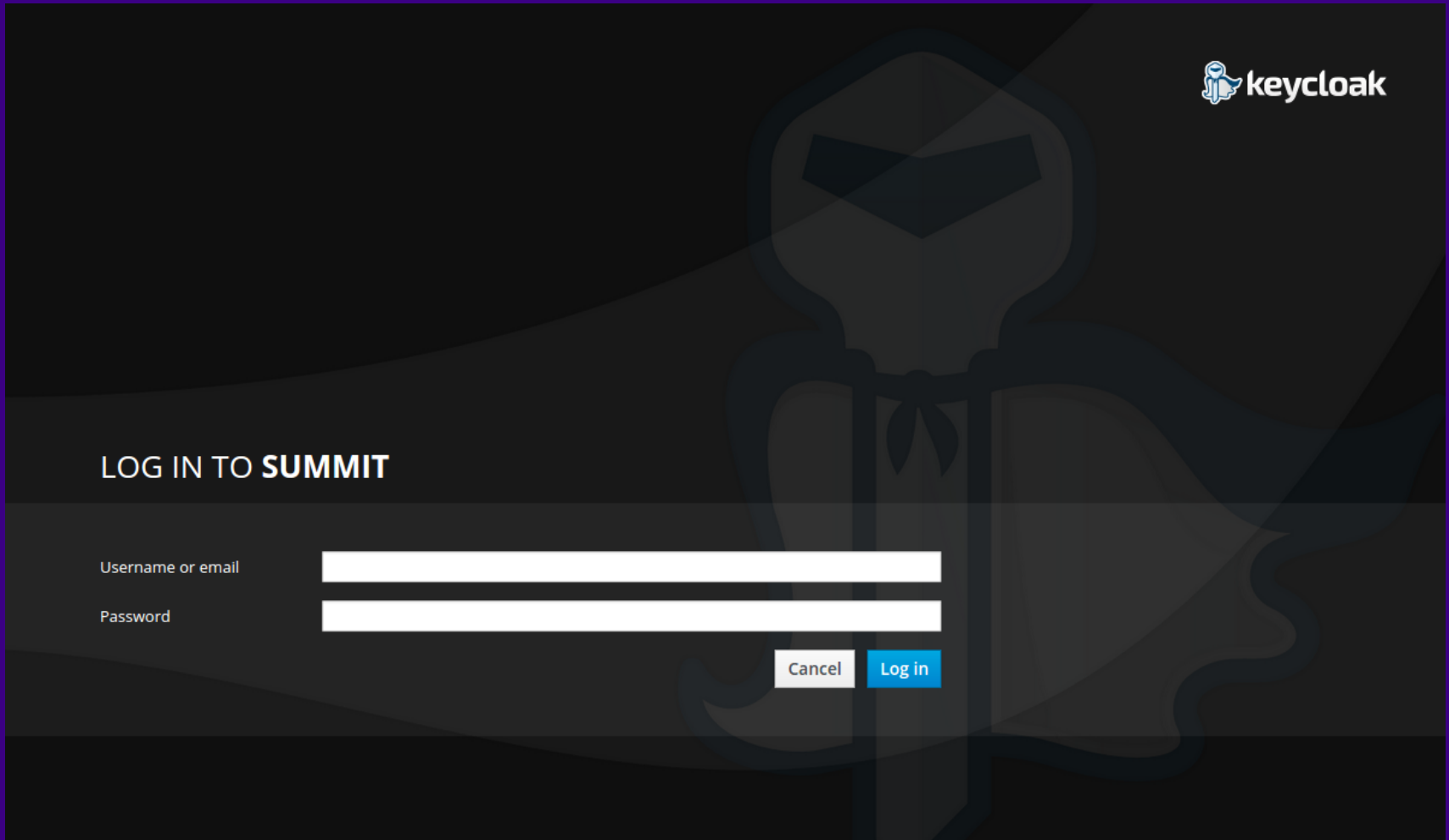
```
<button onclick="keycloak.login()">Login</button>
```

Welcome App

WELCOME

LOGIN

Login to Keycloak realm



The image shows the Keycloak login interface for a realm named 'SUMMIT'. The background is dark with a faint illustration of a hooded figure. The Keycloak logo is in the top right corner. The login form is centered and includes fields for 'Username or email' and 'Password', along with 'Cancel' and 'Log in' buttons.

keycloak

LOG IN TO **SUMMIT**

Username or email

Password

Logged-in to Welcome App

HELLO
**STIAN
THORGERSEN**

LOGOUT

APP INTEGRATION

- Keycloak Client Adapters
- Keycloak Proxy
- OpenID Connect Resource Provider library
- SAML Service Provider library

CLIENT ADAPTERS

- JBoss EAP & WildFly
- JBoss Fuse
- JBoss BRMS
- JavaScript
- NodeJS
- Mobile (Apache Cordova and Native)
- Spring
- Tomcat, Jetty
- More coming (contributions welcome!)

EXAMPLE

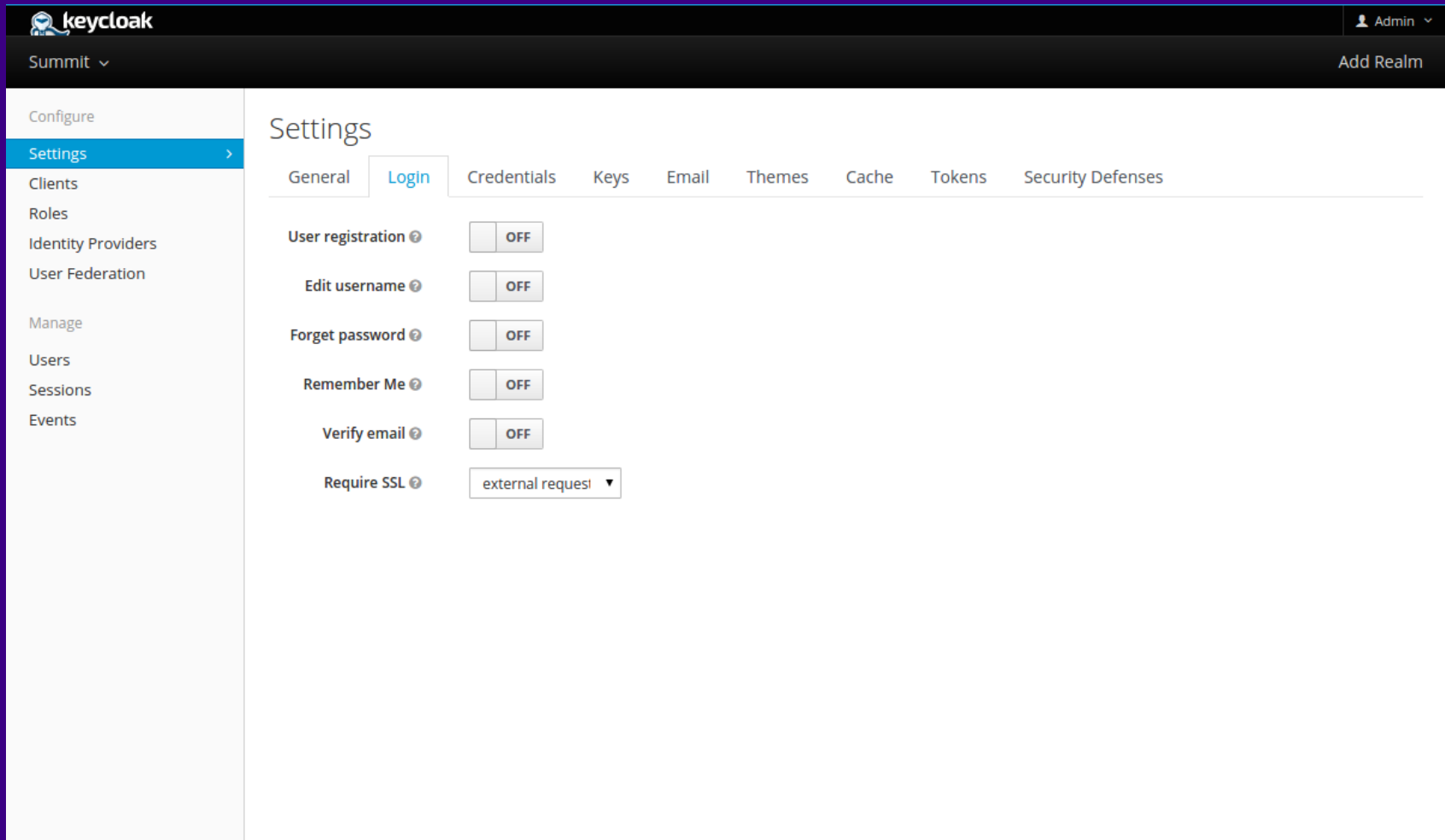
- Simple example to demonstrate features
- Two HTML5 applications
- RESTful services deployed to WildFly



ADMIN CONSOLE

- Configure and manage everything from one console
- Including settings, applications, services, users, permissions and sessions

Admin Console - Realm settings



The image shows the Keycloak Admin Console interface for realm settings. The top navigation bar includes the Keycloak logo, a 'Summit' dropdown, and an 'Admin' user profile. The left sidebar contains a 'Configure' section with 'Settings' highlighted, and other options like 'Clients', 'Roles', 'Identity Providers', 'User Federation', 'Manage', 'Users', 'Sessions', and 'Events'. The main content area is titled 'Settings' and features tabs for 'General', 'Login', 'Credentials', 'Keys', 'Email', 'Themes', 'Cache', 'Tokens', and 'Security Defenses'. The 'Login' tab is active, displaying configuration options for user registration, editing usernames, password resets, remembering users, email verification, and SSL requirements.

keycloak

Summit ▾

Admin ▾

Add Realm

Configure

Settings >

Clients

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events

Settings

General Login Credentials Keys Email Themes Cache Tokens Security Defenses

User registration ⓘ ☐ OFF

Edit username ⓘ ☐ OFF


Forget password ⓘ ☐ OFF

Remember Me ⓘ ☐ OFF

Verify email ⓘ ☐ OFF

Require SSL ⓘ external request ▾

Admin Console - Clients

 **keycloak**

Admin ▾

Summit ▾

Add Realm

Configure

Settings

Clients >

Roles

Identity Providers

User Federation


Manage

Users

Sessions

Events

Clients ?



CreateImport

Client ID	Enabled	Base URL
app	true	http://localhost:8080/app
realm-management	true	Not defined
security-admin-console	true	/auth/admin/summit/console/index.html
services	true	http://localhost:8080/services
broker	true	Not defined
app2	true	http://localhost:8080/app2
account	true	/auth/realms/summit/account

Admin Console - Client settings

The screenshot displays the Keycloak Admin Console interface. The top navigation bar includes the Keycloak logo, a 'Summit' dropdown menu, and an 'Admin' user profile. The left sidebar contains a menu with options: Configure, Settings, Clients (selected), Roles, Identity Providers, User Federation, Manage, Users, Sessions, and Events. The main content area shows the 'Clients' page for a client named 'app'. The 'Settings' tab is active, displaying various configuration fields: Client ID (app), Name (empty), Enabled (ON), Consent Required (OFF), Direct Grants Only (OFF), Client Protocol (openid-connect), Access Type (public), Valid Redirect URIs (http://localhost:8080/app/*), Base URL (http://localhost:8080/app), Admin URL (empty), and Web Origins (http://localhost:8080). The 'Valid Redirect URIs' and 'Web Origins' fields have add (+) and remove (-) buttons.

keycloak

Summit ▾

Admin ▾

Add Realm

Configure

Settings

Clients >

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events

Clients » app

App

Settings Roles Mappers ? Scope ? Revocation Sessions ? Installation ?

Client ID ? app

Name ?

Enabled ? **ON**

Consent Required ? **OFF**

Direct Grants Only ? **OFF**

Client Protocol ? openid-connect ▾

Access Type ? public ▾

* Valid Redirect URIs ?

http://localhost:8080/app/* -

+


Base URL ? http://localhost:8080/app

Admin URL ?

Web Origins ? http://localhost:8080 -

+

Admin Console - User settings

 **keycloak**

Summit ▾

Admin ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation

Manage

Users >

Sessions

Events

[Users](#) » stian

Stian

Attributes

Credentials

Role Mappings

Consents

Sessions

ID

f4fdf759-25aa-49a4-a711-fbcba4ab3dee

Username

stian

Email

stian@redhat.com

First Name

Stian

Last Name

Thorgersen

User Enabled ?

☒ ON ☐

Email verified ?

☐ OFF ☐

Required User Actions ?

Select an action...

> Contact Information ?

Delete

Admin Console - User role mappings

The screenshot displays the Keycloak Admin Console interface. The top navigation bar includes the Keycloak logo, a 'Summit' dropdown, and an 'Admin' user profile. The left sidebar contains a menu with options: Configure, Settings, Clients, Roles, Identity Providers, User Federation, Manage, Users (selected), Sessions, and Events. The main content area is titled 'Users » stian' and shows the 'Role Mappings' tab for user 'Stian'. Below this, there are two sections: 'Realm Roles' and 'Client Roles'. The 'Client Roles' section has a dropdown menu set to 'account'. Each section contains four columns: 'Available Roles', 'Assigned Roles', and 'Effective Roles'. In the 'Realm Roles' section, the 'Assigned Roles' column lists 'admin' and 'user'. In the 'Client Roles' section, the 'Assigned Roles' column lists 'view-profile' and 'manage-account', and the 'Effective Roles' column lists 'manage-account' and 'view-profile'. Buttons for 'Add selected' and 'Remove selected' are present in each section.

keycloak

Summit ▾

Admin ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation

Manage

Users >

Sessions

Events

Users » stian

Stian

Attributes

Credentials

Role Mappings

Consents

Sessions

Realm Roles

Available Roles ?

Assigned Roles ?

Effective Roles ?

admin

user

Add selected >

« Remove selected

Client Roles

account ▾

Available Roles ?

Assigned Roles ?

Effective Roles ?

view-profile

manage-account

manage-account

view-profile


Add selected >

« Remove selected

ACCOUNT MANAGEMENT

A console for users to manage their own
account

Account Management - Profile

 **keycloak**

Sign Out

Account >

Password

Authenticator

Federated Identity

Sessions

Applications

Log

Edit Account * Required fields

Username

stian

Email *

stian@redhat.com

First name *

Stian

Last name *

Thorgersen

Street

City or Locality

State, Province,
or Region


Zip or Postal
code

Country

Cancel

Save

Account Management - Password

 **keycloak**

Sign Out

Account

Password >

Authenticator

Federated Identity

Sessions

Applications

Log

Change Password

All fields required

Password


New Password

Confirmation

Cancel

Save

Account Management - Applications

keycloak

Sign Out

Account

Password

Authenticator

Federated Identity

Sessions


Applications >

Log

Applications

Application	Available Permissions	Granted Permissions	Granted Personal Info	Action
Message App	Administrator privileges , User privileges , View profile in Account , Manage account in Account	Full Access	Full Access	
Welcome App	Administrator privileges , User privileges , View profile in Account , Manage account in Account	Full Access	Full Access	
Account	View profile in Account , Manage account in Account	Full Access	Full Access	

Account Management - Account history

 **keycloak**

Sign Out

Account

Password

Authenticator

Federated Identity

Sessions

Applications

Log >

Account Log

Date	Event	IP	Client	Details
Jun 17, 2015 1:25:20 PM	login	127.0.0.1	account	auth_method = form , username = stian
Jun 17, 2015 1:20:44 PM	login	127.0.0.1	account	auth_method = form , username = stian
Jun 17, 2015 9:10:05 AM	login	127.0.0.1	app2	auth_method = form , username = stian
Jun 17, 2015 8:57:25 AM	logout	127.0.0.1		
Jun 17, 2015 8:57:21 AM	login	127.0.0.1	app2	auth_method = form , username = stian

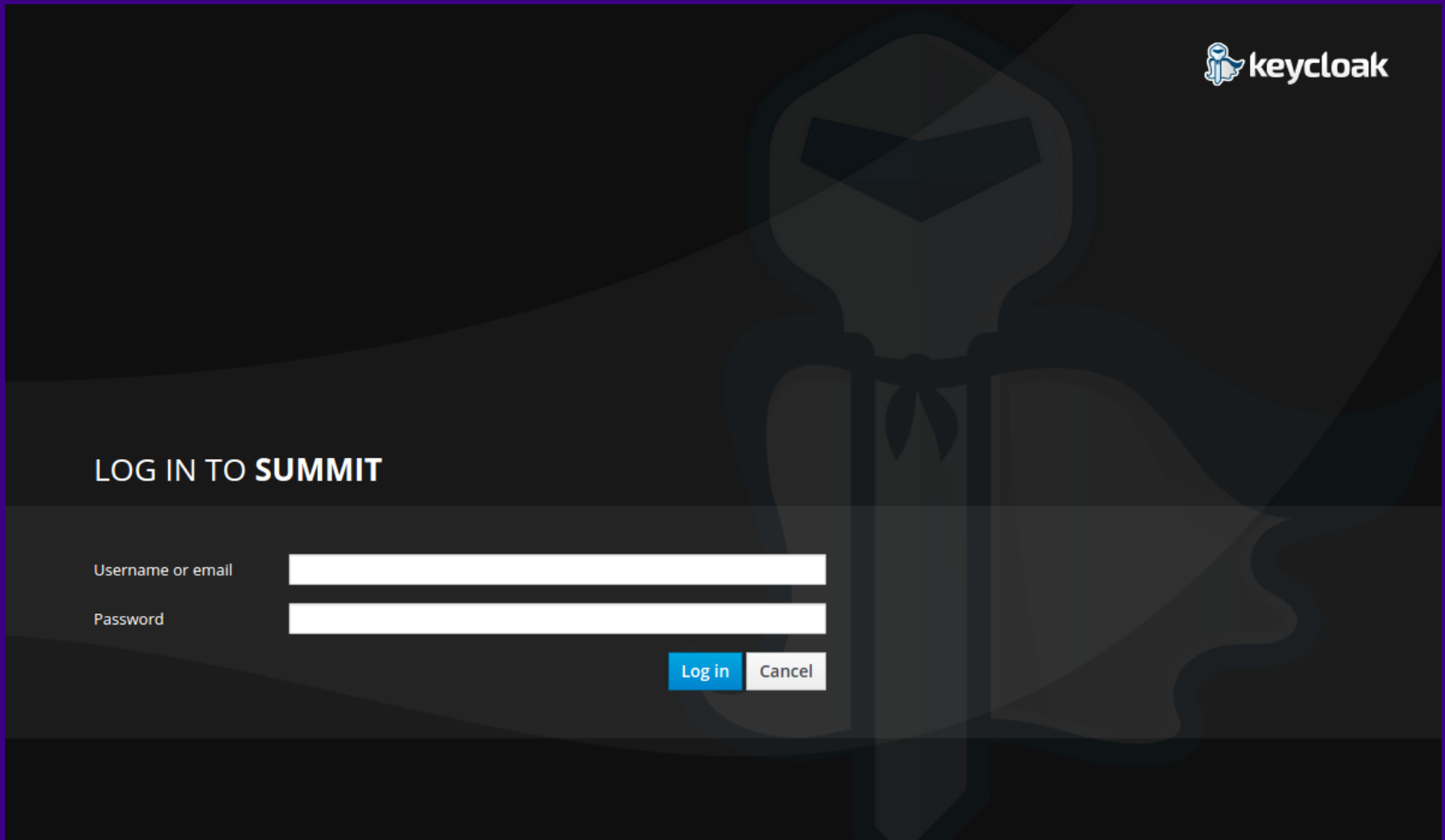
SINGLE SIGN-ON

- Web SSO
- Enterprise/Desktop SSO Bridge (Kerberos)
- Single Sign-Out
- Remote Sign-Out

THEMES

- Brand login pages and account management to integrate with your corporate brand
- HTML templates for more than just styling

Login - Default theme



The image shows the Keycloak login page with a dark theme. The background features a large, faint illustration of a hooded figure. The login form is centered and includes the following elements:

LOG IN TO **SUMMIT**

Username or email

Password

The Keycloak logo is located in the top right corner.

Admin Console - Configure theme

The screenshot displays the Keycloak Admin Console interface. At the top, there's a dark header with the 'Summit' logo and a dropdown menu, and an 'Add Realm' button on the right. The left sidebar contains a 'Configure' section with 'Settings' highlighted, and other options like 'Clients', 'Roles', 'Identity Providers', 'User Federation', 'Manage', 'Users', 'Sessions', and 'Events'. The main content area is titled 'Settings' and has several tabs: 'General', 'Login', 'Credentials', 'Keys', 'Email', 'Themes' (active), 'Cache', 'Tokens', and 'Security Defenses'. Under the 'Themes' tab, there are four theme configuration options, each with a help icon and a dropdown menu: 'Login Theme' (set to 'summit'), 'Account Theme' (set to 'Select one...'), 'Admin Console Theme' (set to 'Select one...'), and 'Email Theme' (set to 'Select one...'). Below these, there is an 'Internationalization' section with a label 'Enabled' and a toggle switch currently set to 'OFF'.

Summit

Summit ▾ Add Realm

Configure

Settings >

Clients

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events

Settings

General Login Credentials Keys Email Themes Cache Tokens Security Defenses

Login Theme ? summit ▾

Account Theme ? Select one... ▾

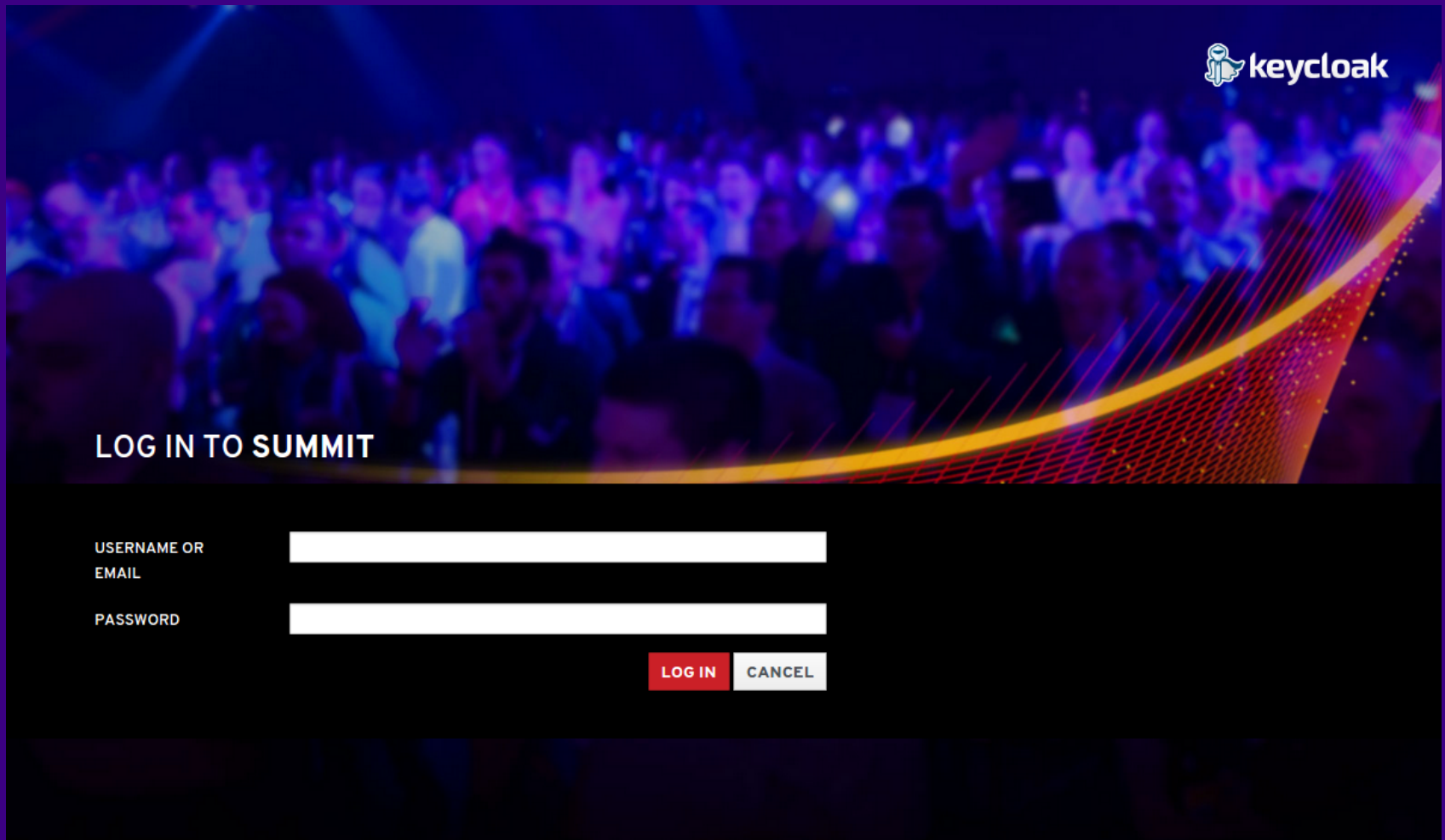
Admin Console Theme ? Select one... ▾

Email Theme ? Select one... ▾

Internationalization
Enabled

OFF

Login - Summit theme

The login page features a background image of a large crowd at a summit, with blue and purple stage lighting. A bright, curved orange and yellow light effect sweeps across the right side of the image. The Keycloak logo is in the top right corner. The text 'LOG IN TO SUMMIT' is prominently displayed in the upper left. Below this, there are two white input fields for 'USERNAME OR EMAIL' and 'PASSWORD'. At the bottom right, there are two buttons: a red 'LOG IN' button and a white 'CANCEL' button with a black border.

keycloak

LOG IN TO SUMMIT

USERNAME OR
EMAIL

PASSWORD

LOG IN CANCEL

LOGIN FLOWS

- Required actions
- Recover password
- Two factor authentication
- Registration

Admin Console - Login settings

The screenshot shows the Admin Console interface for the 'Summit' realm. The left sidebar contains a 'Configure' menu with options: Settings (selected), Clients, Roles, Identity Providers, User Federation, Manage, Users, Sessions, and Events. The main content area is titled 'Settings' and features a horizontal tab bar with 'General', 'Login', 'Credentials', 'Keys', 'Email', 'Themes' (active), 'Cache', 'Tokens', and 'Security Defenses'. Under the 'Themes' tab, there are four dropdown menus: 'Login Theme' (set to 'summit'), 'Account Theme' (set to 'Select one...'), 'Admin Console Theme' (set to 'Select one...'), and 'Email Theme' (set to 'Select one...'). At the bottom, the 'Internationalization' toggle is set to 'OFF'.

Summit ▾ Add Realm

Configure

Settings >

Clients

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events

Settings

General Login Credentials Keys Email Themes Cache Tokens Security Defenses

Login Theme ⓘ summit ▾

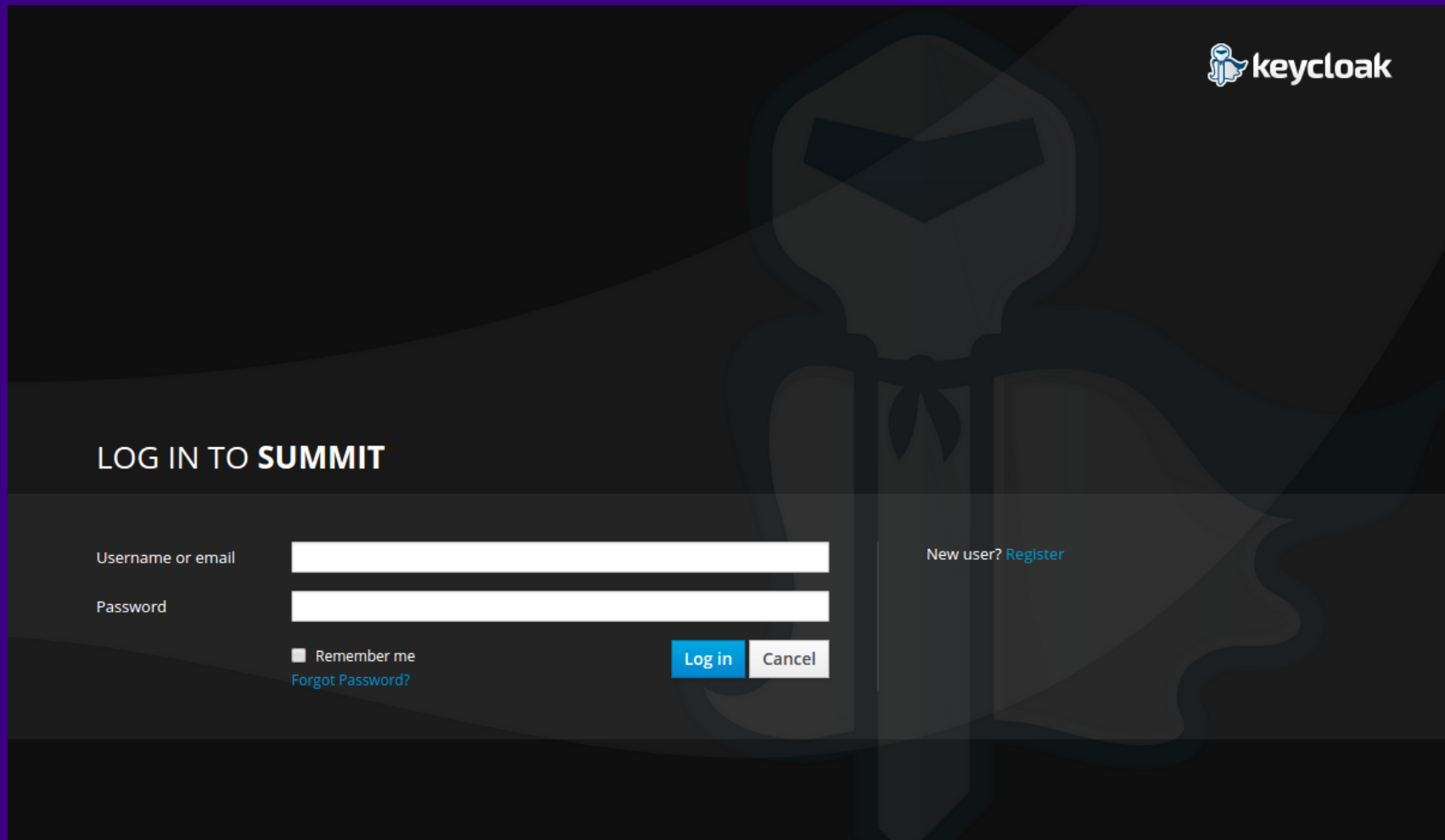
Account Theme ⓘ Select one... ▾


Admin Console Theme ⓘ Select one... ▾

Email Theme ⓘ Select one... ▾

Internationalization Enabled OFF

Login - Extra features enabled



 keycloak

LOG IN TO **SUMMIT**

Username or email


Password

☐ Remember me


[Forgot Password?](#)

New user? [Register](#)

Login - Configure two factor authentication

 keycloak


MOBILE AUTHENTICATOR SETUP

 You need to set up Mobile Authenticator to activate your account.

One-time code

Submit

1. Install [FreeOTP](#) or Google Authenticator on your mobile. Both applications are available in [Google Play](#) and Apple App Store.
2. Open the application and scan the barcode or enter the key



G5QW IT2U OB3U KVKF KNGE CTRT MIZW C6SJ

3. Enter the one-time code provided by the application and click Submit to finish the setup

Login - Update profile



UPDATE ACCOUNT INFORMATION



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

Email

First name

Last name

PASSWORD POLICIES

- Set required complexity for passwords
- Prevent reuse of old passwords
- Require regular updating of passwords
- Set hashing intervals

Admin Console - Password policies

Summit ▾

Add Realm

Configure

Settings >

Clients

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events

Settings

GeneralLoginCredentialsKeysEmailThemesCacheTokensSecurity Defenses

Realm Credentials Settings ?

Required User Credentials

✖ password

Realm Password Policy ?

Add policy... ▾

Policy Type	Policy Value	Actions
Hash Iterations	10000	
Length	8	
Force Expired Password Change	365	
Password History	3	

Login - invalid password update



UPDATE PASSWORD



Invalid password: must not be equal to any of last 3 passwords.

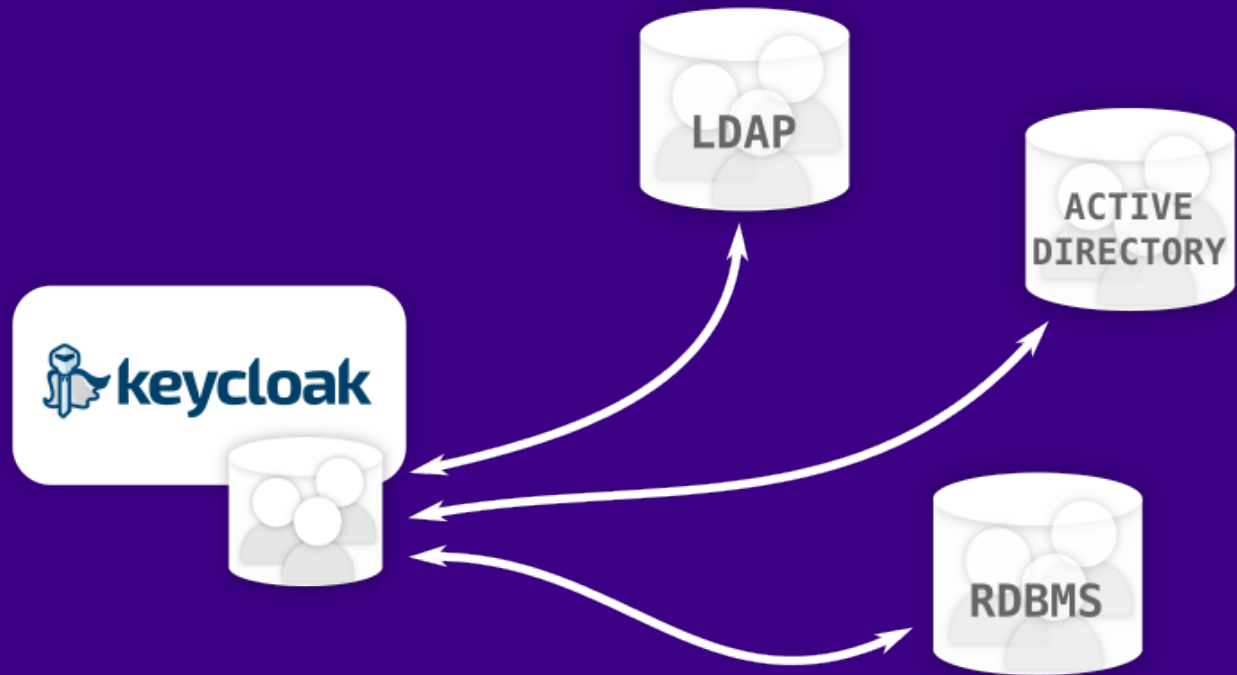
New Password

Confirm password


Submit

USER FEDERATION

- Sync users with external directories
- Read-only or read-write



Admin Console - Add LDAP user federation

keycloak

Admin ▾

Summit ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation >

Manage

Users

Sessions

Events

User Federation > Add User Federation Provider

Add LDAP User Federation Provider

Required Settings

Console display name ?

defaults to id

Priority ?

0

Edit mode ?

▾

Sync Registrations ?

☐ OFF

* Vendor ?

Active Directory

▾

* Username LDAP attribute ?

cn

* RDN LDAP attribute ?

cn

* UUID LDAP attribute ?

objectGUID

* User Object Classes ?


person, organizationalPerson, user

* Connection URL ?

ldap

Test connection

Admin Console - User federation

 **keycloak**

Admin ▾

Summit ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation >

Manage

Users

Sessions

Events

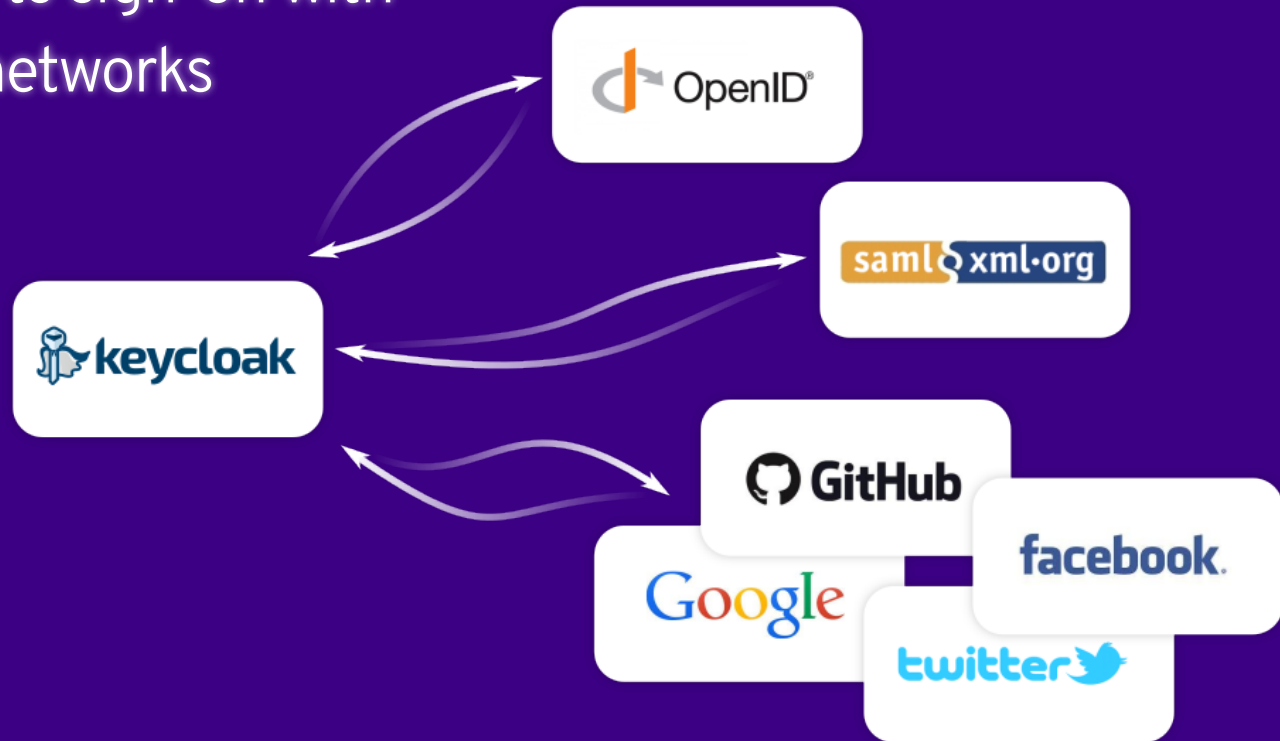
User Federation Summit

Add provider... ▾

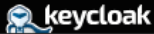
ID	Provider Name	Priority
3e49a3ae-9f6d-49d4-9d5c-b49c103c4d65	Ldap	0
eeffc4a3-884f-4d2f-a81c-61beb5cead03	Kerberos	0

IDENTITY BROKERING

- Allow external users to sign-on
- Supports sign-on with social networks



Admin Console - Add SAML Identity Provider

keycloak

Admin ▾

Summit ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation

Manage

Users

Sessions

Events


Identity Providers > saml

Identity Provider Saml

Redirect URI ?

http://localhost:8180/auth/realms/summit/broker/saml/endpoint

* Alias ?

saml 

Enabled ?

☒ ON ☐

Authenticate By Default ?

☐ OFF

Store Tokens ?

☐ OFF

Stored Tokens Readable ?

☐ OFF

Update Profile on First Login ?

Off ▾

Trust email ?

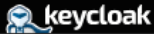
☐ OFF

GUI order ?

⌵ SAML Config ?

* Single Sign-On Service Url ?

Admin Console - Identity Providers

keycloak

Admin ▾

Summit ▾

Add Realm

Configure

Settings

Clients

Roles

Identity Providers >

User Federation

Manage

Users

Sessions

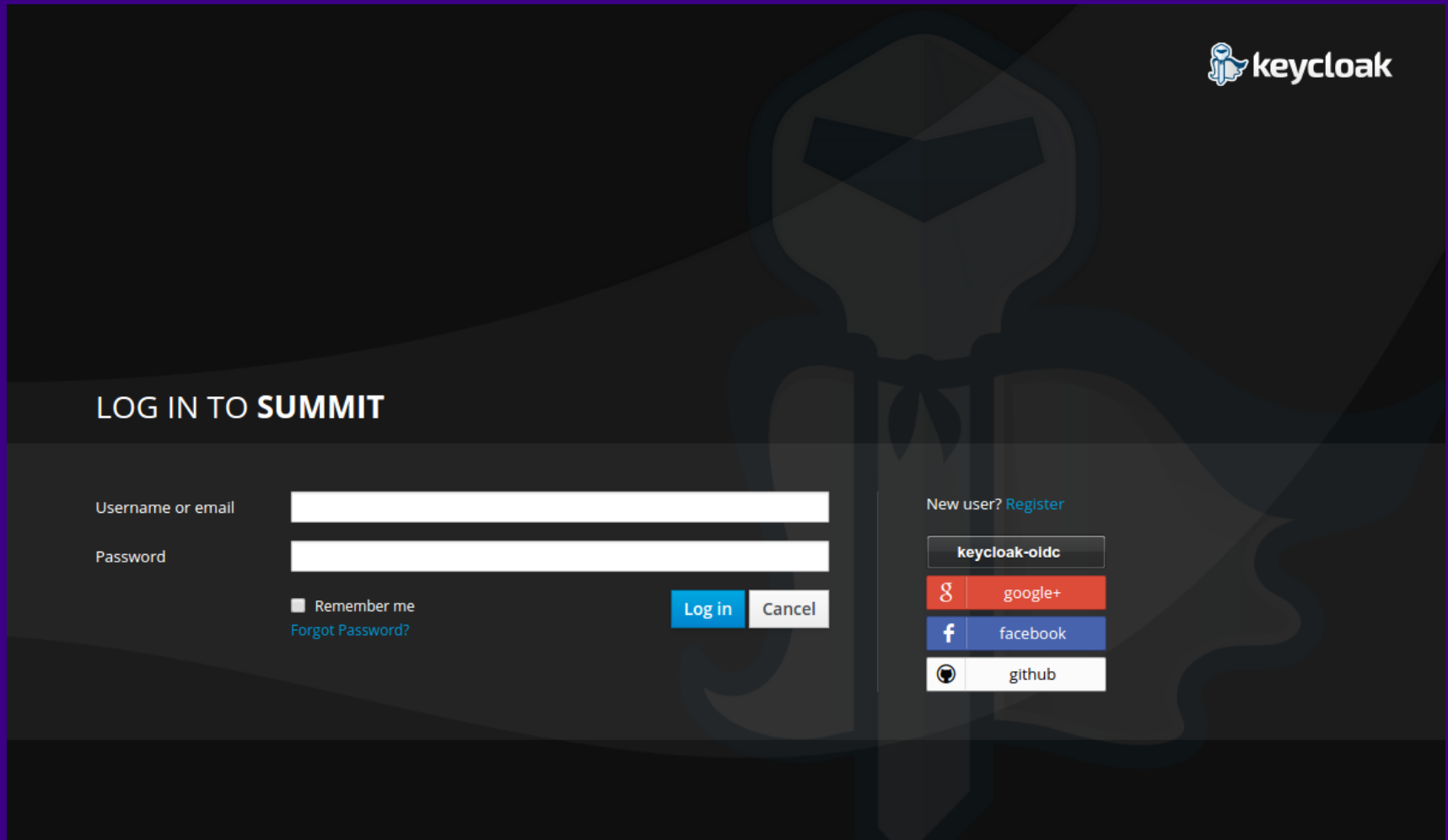
Events

Identity Providers Summit

Add provider... ▾

Name	Provider	Enabled	GUI order
saml	saml	true	
oidc	oidc	true	
github	github	true	
twitter	twitter	true	
facebook	facebook	true	
google	google	true	
linkedin	linkedin	true	
stackoverflow	stackoverflow	true	

Login - Identity Brokering



The image shows a Keycloak login page with a dark theme. In the top right corner is the Keycloak logo. The main heading is "LOG IN TO SUMMIT". Below this are two input fields for "Username or email" and "Password". To the right of the password field is a "Remember me" checkbox and a "Forgot Password?" link. At the bottom of the form are "Log in" and "Cancel" buttons. On the right side of the page, there is a "New user? Register" link and a list of social login providers: "keycloak-oidc", "google+", "facebook", and "github". The background features a faint illustration of a person in a hooded cloak.

keycloak

LOG IN TO SUMMIT




Username or email

Password

☐ Remember me [Forgot Password?](#)

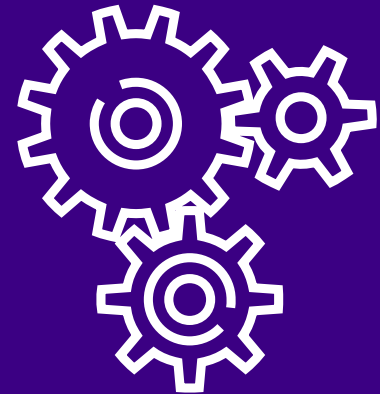
[Log in](#) [Cancel](#)

New user? [Register](#)

- keycloak-oidc
-  google+
-  facebook
-  github

MAPPERS

- Customize tokens
- Map claims and attributes from external tokens
- Map attributes and groups from LDAP

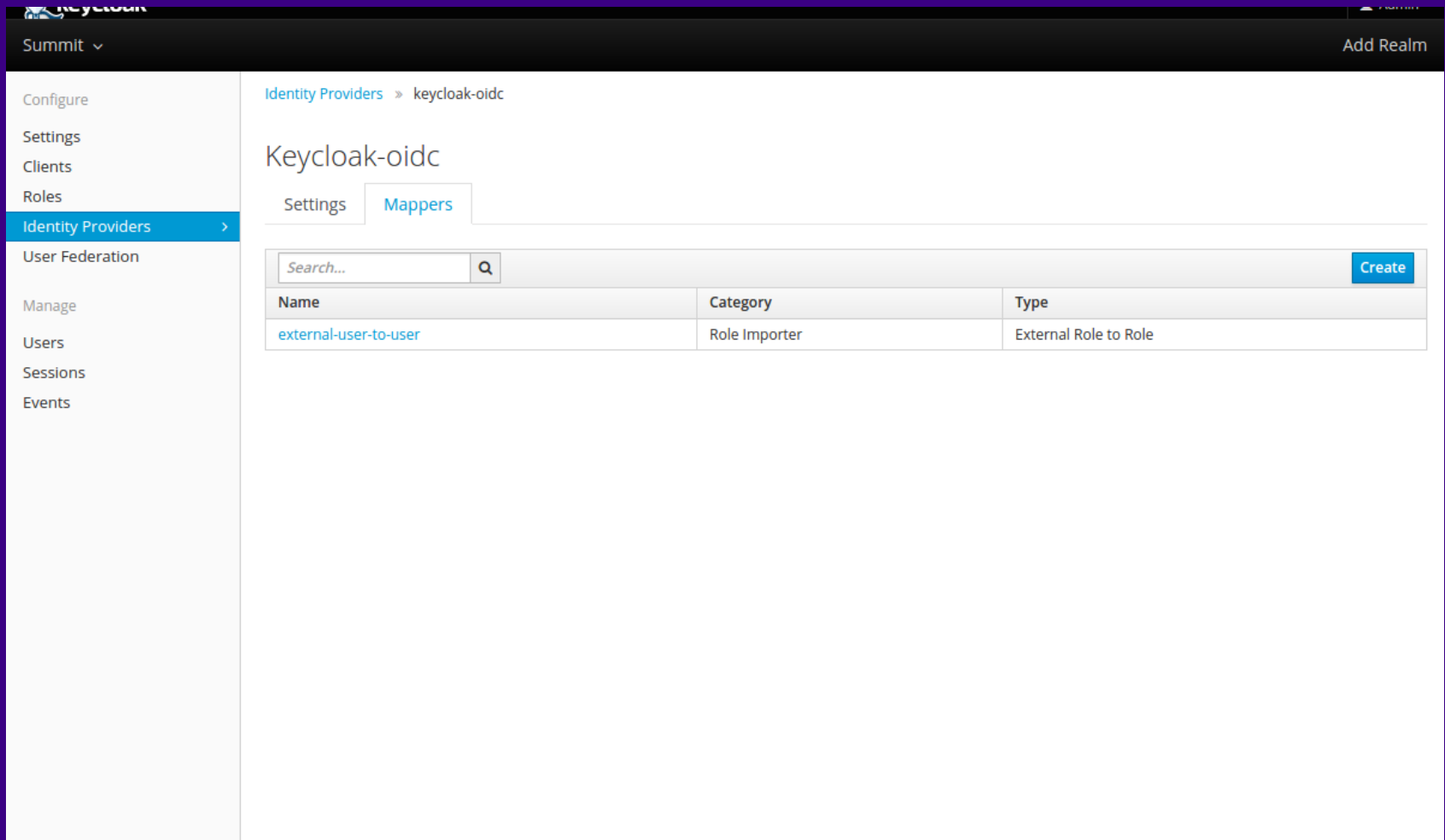


Admin Console - Token mappers

The screenshot shows the Keycloak Admin Console interface. On the left is a navigation sidebar with options: Configure, Settings, Clients (selected), Roles, Identity Providers, User Federation, Manage, Users, Sessions, and Events. The top header includes the 'Summit' logo and an 'Add Realm' button. The main content area is titled 'Clients » app' and 'App'. Below this, there are tabs for 'Settings', 'Roles', 'Mappers' (active), 'Scope', 'Revocation', 'Sessions', and 'Installation'. A search bar and 'Create'/'Add Built-in' buttons are present above a table of mappers.

Name	Category	Type
email	Token mapper	User Property
given name	Token mapper	User Property
full name	Token mapper	User's full name
username	Token mapper	User Property
family name	Token mapper	User Property

Admin Console - Identity Provider mappers



Summit ▼ Add Realm

Configure
Settings
Clients
Roles
Identity Providers >
User Federation
Manage
Users
Sessions
Events


Identity Providers » keycloak-oidc

Keycloak-oidc

Settings **Mappers**

Name	Category	Type
external-user-to-user	Role Importer	External Role to Role

Admin Console - LDAP mappers

 Summit ▼ Add Realm

Configure

Settings

Clients

Roles

Identity Providers

User Federation >

Manage

Users


Sessions

Events

User Federation > 2adea638-8ff4-40b2-9f90-4f0460015390 > User Federation Mappers

LDAP

Settings Mappers

 Create

Name	Category	Type
creation date	Attribute Mapper	User Attribute
email	Attribute Mapper	User Attribute
first name	Attribute Mapper	User Attribute
last name	Attribute Mapper	User Attribute
modify date	Attribute Mapper	User Attribute
username	Attribute Mapper	User Attribute

VULNERABILITIES

- Standard Protocols
- Built-in Brute Force protection
- Integrate with Intrusion Detection
- Protected against known attacks
- Patches



redhat®