Open in app ↗

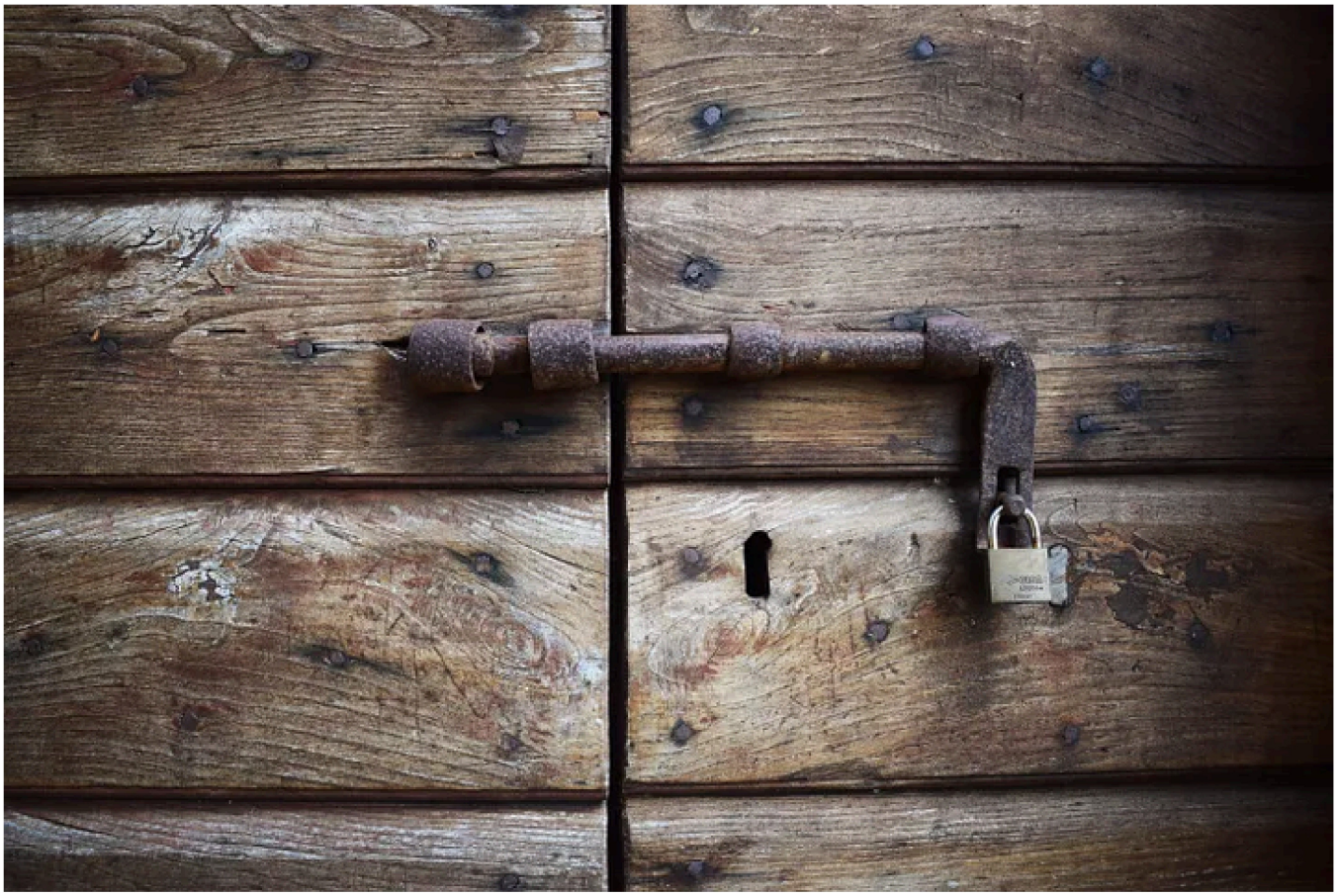
Be part of a better internet. Get 20% off membership for a limited time

# Two-Factor Authentication via Email in Keycloak (Custom Auth. SPI)

Mesut Pişkin · Follow

3 min read · Oct 27, 2022

Listen Share More



> *N.B. By default, Keycloak does not support two-factor authentication via SMS or email. Keycloak only supported two factors by default TOTP/HOTP via Google Authenticator and FreeOTP, but we may utilize 2fa Email and SMS with Service Provider Interfaces (SPI).*

• • •

Keycloak: Identity and Access Management for Modern Applications, Keycloak enables single sign-on while also managing identity and access. You can easily add authentication to applications and secure services. There is no need to manage user storage or authentication. Everything is available right away. Advanced features include user federation, identity brokering, and social login.

They cover everything from reviewing what Keycloak has to offer businesses, management, and identity brokering, to enabling single-sign-on, LDAP or Active Directory sync, and more. Developers and system administrators no longer have to worry about storing and protecting user passwords with this IAM tool.

### 1- Installing and Running Keycloak

Run the following command to start the Keycloak server as a Docker container:

```
docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e
KEYCLOAK_ADMIN_PASSWORD=admin quay.io/keycloak/keycloak:19.0.3
start-dev
```

Keycloak does not run with a default admin account, passing the environment variables KEYCLOAK_USER and KEYCLOAK_PASSWORD allows you to quickly create one.

If you want to run Keycloak without Docker, download the distribution from the Keycloak website. Open https://www.keycloak.org/downloads and then download the server's ZIP archive. Simply extract this archive to a suitable location after downloading it.

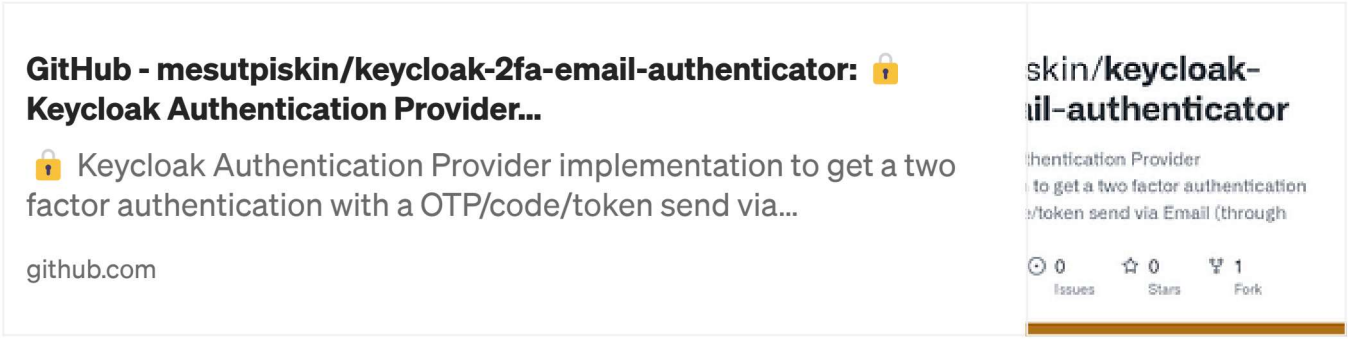
You are ready if the installation goes well. For authentication, you'll need the user, client, and realm. You are following this official tutorial; https://www.keycloak.org/docs/11.0/getting_started/#creating-a-realm-and-a-user

### 2. Custom Keycloak Email 2FA Authentication Provider

Keycloak is intended to address the majority of use cases without the need for special code, but we also want it to be adaptable. Keycloak provides several Service Provider Interfaces (SPI) through which you can implement your providers. Because Keycloak is built on SPIs, implementing a 2FA process flow yourself is not difficult. You are using the API and SMTP email protocol provided by Keycloak.

As previously said, the Authentication SPI is highly strong, but it is also the most difficult SPI in Keycloak, where you might ruin your authentication flow. If not correctly implemented, you may introduce attack vectors onto your system, making it unsafe. So, I strongly advise you to thoroughly study the server development documentation.

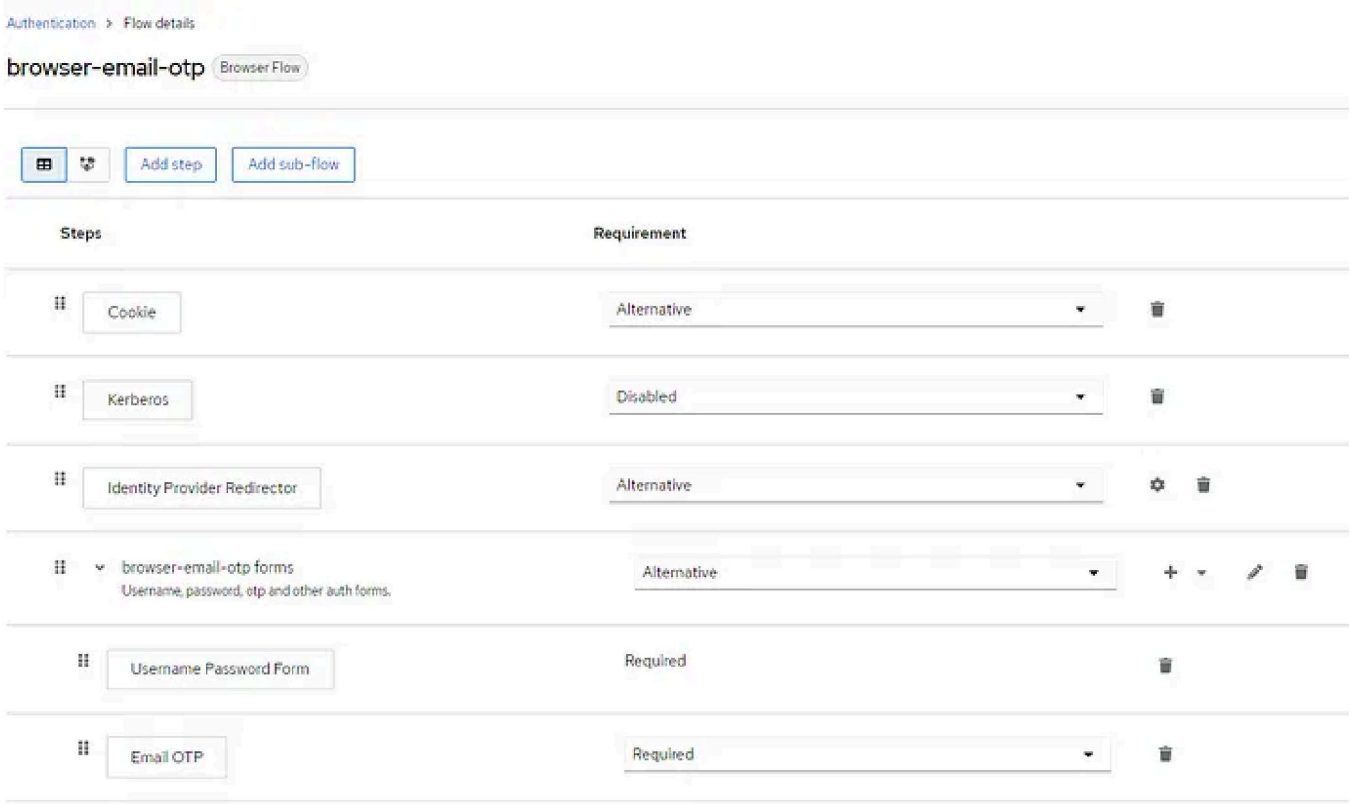
On GitHub, I've provided an example implementation of the SMTP Email Authentication SPI for Keycloak:




### 3. Configure 2FA Email Authentication Flow for SPI

After you've deployed the JAR profile to the /deployments or /provider directory, you'll need to establish and setup a Keycloak authentication flow in your realm and utilize it in a binding to use the *keycloak-2fa-email-authenticator.jar*

1. Configure Realm SMTP email settings in *Realm/Realm Settings/Email*.
2. Create (clone) a new flow for browser-based authentication and modify it to meet your requirements. Include an execution for "browser-email-otp-flow"
3. Configure the "browser-email-otp-flow" execution phase using the parameters that are most appropriate for your needs.
4. Set the newly established flow to "Browser Flow" in your realm's admin console's Authentication / Bindings tab.

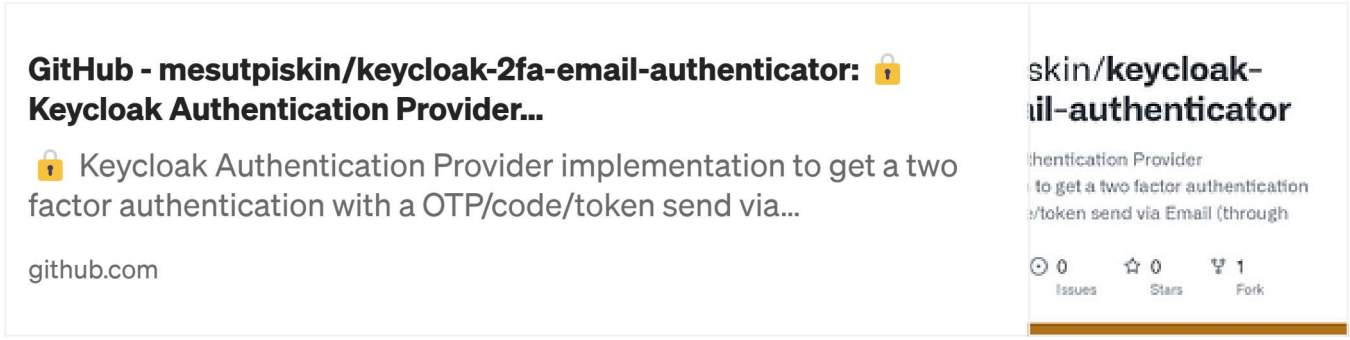



Email OTP Authentication Flow

OTP generation algorithm is very simple in generateAndSendEmailCode(). If you want to change the OTP code format then you can override this method and write custom code or use Keycloak SecretGenerator

```
private void generateAndSendEmailCode(AuthenticationFlowContext
context) {
...

int emailCode = ThreadLocalRandom.current().nextInt(99999999);
...
    }
```




Keycloak Two Factor Authentication Otp Email

Follow

## Written by Mesut Pişkin

551 Followers

Senior Software Engineer. I write about back-end development and software architecture.
https://mesutpiskin.com

### More from Mesut Pişkin

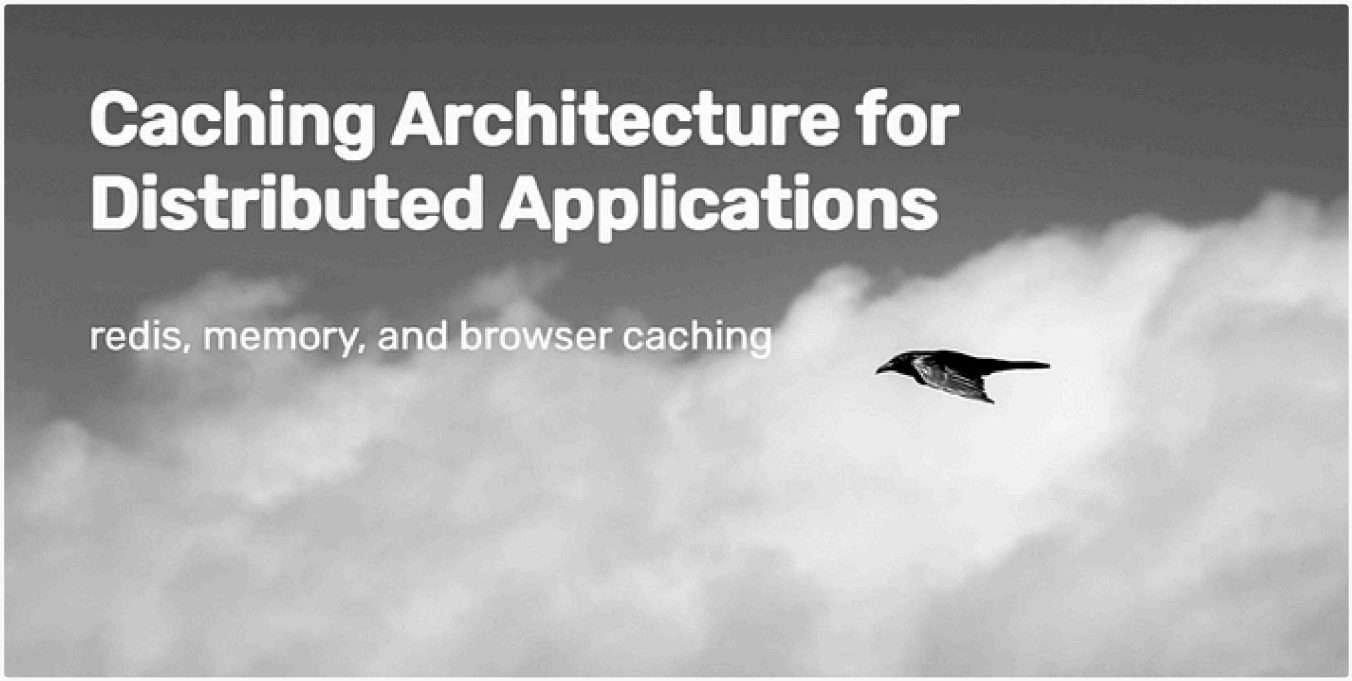

Mesut Pişkin

**Building a Distributed Job Scheduler for Microservices**

JOB Schedulers will help you automate your jobs in a standard fashion that you can configure. It can also trigger your jobs in various ways...

6 min read · Dec 7, 2022

40 4




Mesut Pişkin

## Caching Architecture for Distributed Applications

to read in Turkish

8 min read · Dec 21, 2022

86 2

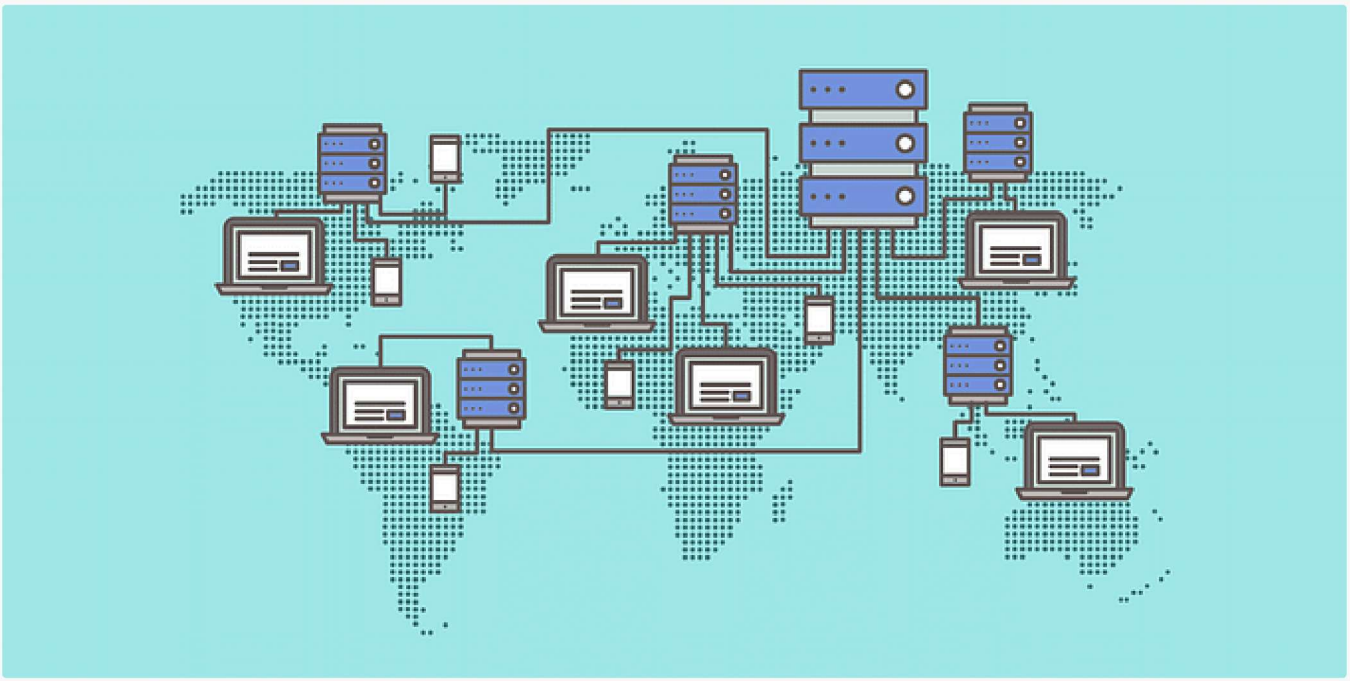

Mesut Pişkin

## Mikroservis Yaklaşımında Servisler Arası İletişim Mimarileri

Mikroservis mimaride, servisler arası iletişim yöntemleri; Event Driven, Request Driven ve Message Driven mimari...

5 min read · Apr 15, 2020

328



Mesut Pişkin in Inside Architecht

## Dağıtık Uygulamalar İçin Önbellekleme (Distributed Caching) Mimarisi

Önbellek (Cache), kullanıcı isteklerine daha hızlı cevap verebilmek, uygulama performansını arttırmak, oluşabilecek dar boğazları önlemek...

6 min read · Feb 10, 2021

72 1

See all from Mesut Pişkin

## Recommended from Medium

Daniel Craciun in Level Up Coding

### 3 Reasons to Use NoSQL over SQL

The Merits of Using NoSQL

✦ · 3 min read · May 29, 2024

195 8

Zhimin Wen

# Implement SAML based SSO with KeyCloak

Let's explore SAML integration with KeyCloak.

· 4 min read · May 6, 2024

4

## Lists

**Staff Picks**

673 stories · 1092 saves

**Stories to Help You Level-Up at Work**

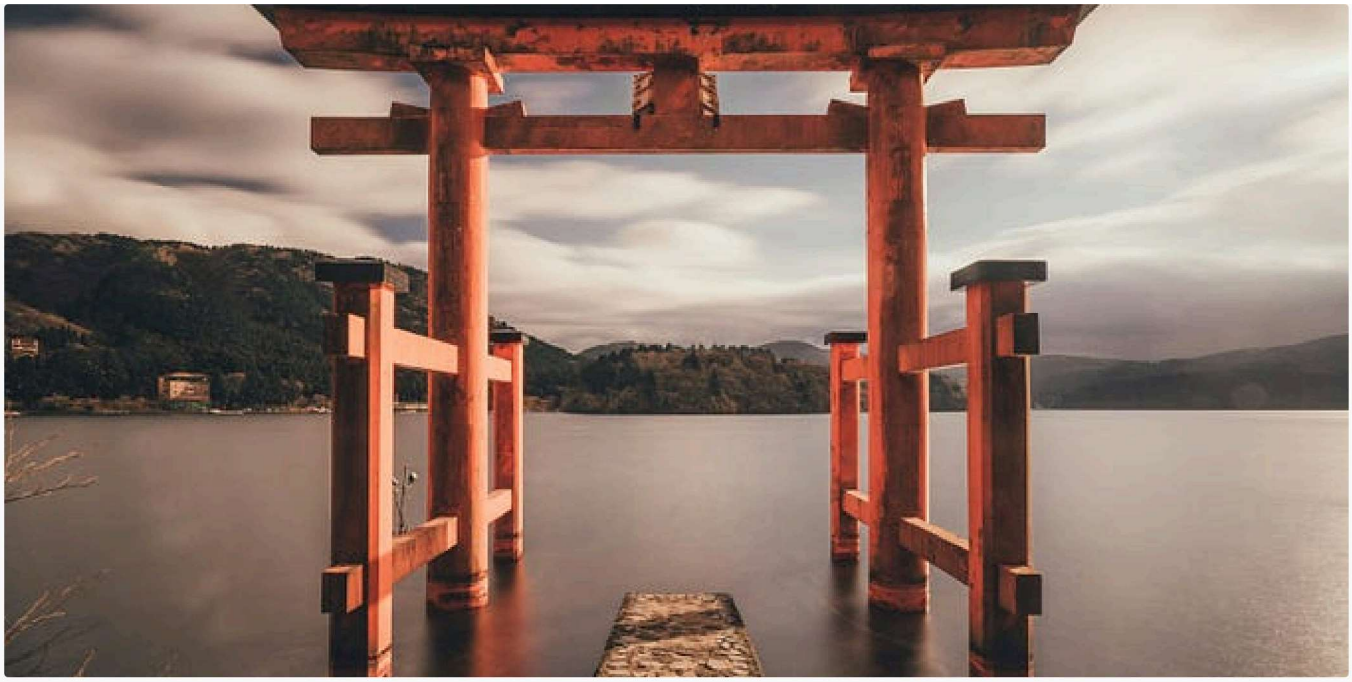
19 stories · 666 saves

**Self-Improvement 101**

20 stories · 2186 saves

**Productivity 101**

20 stories · 1946 saves



Ivan Franchin in ITNEXT

## Exploring Keycloak Admin REST API

Manage realms, clients, users, and more using Keycloak Admin REST API

· 10 min read · May 30, 2024

80 1

Nagarjun Nagesh

## Custom Filters and Handlers in Spring Boot

In this article, we will explore the power of custom filters and handlers in Spring Boot applications. Custom filters allow you to add...

· 3 min read · Feb 20, 2024

6

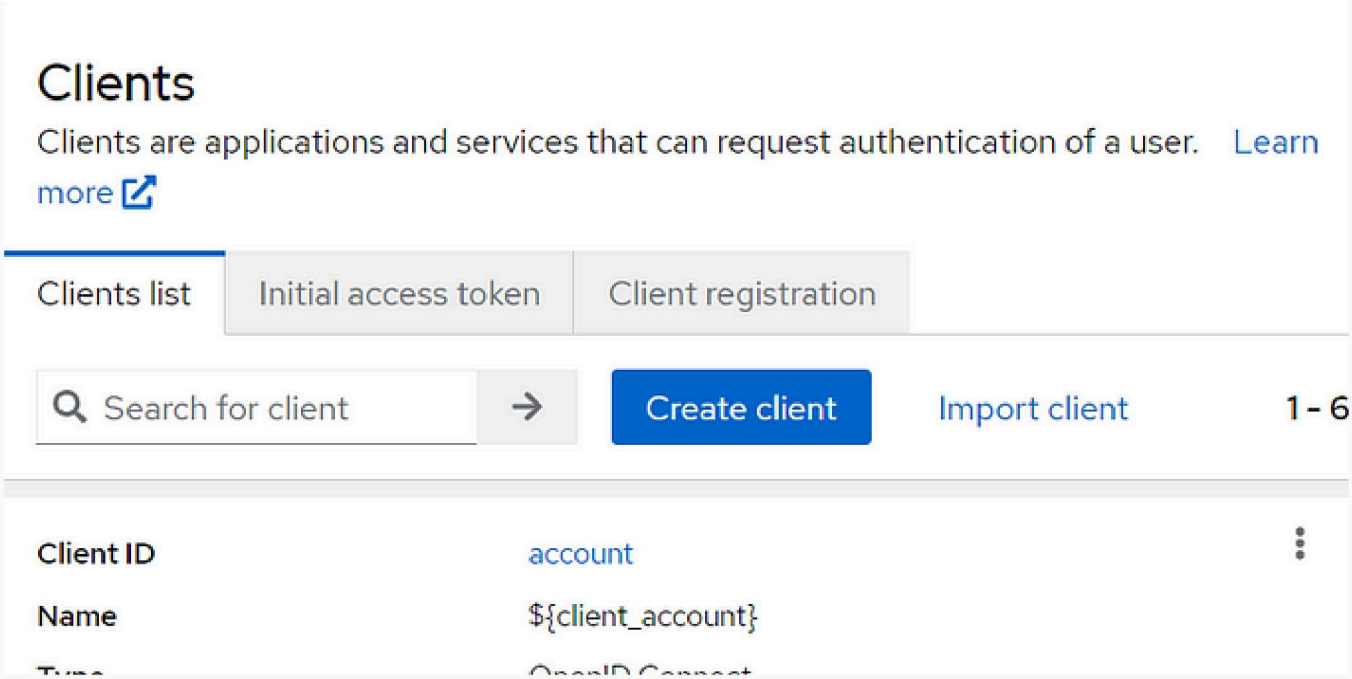
Bhuvanesh Kamaraj

## Implementing MFA using SMS OTP in Keycloak

In this document, we will outline the steps to implement Multi-Factor Authentication (MFA) using SMS One-Time Password (OTP) in Keycloak...

3 min read · Feb 29, 2024

3 2




Akalanka Dissanayake

## Effortless Authentication with Docker: Deploying Keycloak and PostgreSQL

Unlock the Power of Centralized User Management and Secure Single Sign-On for Your Applications

4 min read · Feb 17, 2024

77

See more recommendations