

Be part of a better internet. [Get 20% off membership for a limited time](#)



# Simplifying OTP Integration in Keycloak with OTP+

DOtp Plus · [Follow](#)

2 min read · Oct 5, 2023

[Open in app](#)

As the world of digital security continues to evolve, the need for robust authentication systems has become more critical than ever. Keycloak, an open-source identity and access management solution, has emerged as a powerful tool for managing authentication and authorization within applications. However, integrating One-Time Password (OTP) authentication into Keycloak can be a complex and challenging endeavor. In this article, we'll explore the current

landscape of OTP integration in the Keycloak world, highlighting the challenges developers face, and introduce our solution to simplify the process.

## The Current State of Keycloak OTP Integration

Keycloak provides support for unlimited customizability of your OTP solution through the use of Plugins. While these options are versatile, integrating them seamlessly with an external OTP providers like Twilio can be cumbersome for several reasons:

- 1. Complex Configuration:** Setting up OTP providers often involves navigating through Keycloak's extensive configuration options. This process can be time-consuming and confusing for developers, especially those new to Keycloak.
- 2. Maintenance Challenges:** Over time, maintaining and updating OTP integrations can become a significant challenge. As OTP standards evolve or security requirements change, you may need to invest considerable effort in keeping your authentication system up to date.
- 3. Finding Cost-Effective Providers:** It going to take a lot of research and testing to figure out which providers are truly the most cost-effective.

## Introducing OTP+'s keycloak

Our custom Keycloak comes with an in-built Keycloak plugin designed to simplify the integration of OTP authentication into your applications. This solution addresses the pain points developers face when connecting to OTP providers, making the process seamless and efficient.

## Key Features

- 1. Easy Configuration:** OTP+ offers an intuitive and user-friendly configuration interface within Keycloak, reducing the complexity of setting up OTP authentication. With just a few clicks, you can set up two-factor authentication on any application.
- 2. Diverse Provider Support:** Unlike the limited options provided by Keycloak, OTP+ supports a wide range of OTP providers, including SMS and email. This flexibility ensures that you can choose the method that best suits your application and user base.
- 3. Automatic Updates:** Say goodbye to the hassle of maintaining and updating your OTP integration. OTP+ automatically handles updates and security

enhancements, ensuring your authentication system remains secure and up to date.

4. **Enhanced Security:** Security is paramount when it comes to OTP authentication. OTP+ implements best practices and industry standards to safeguard your users' data, making it a reliable choice for ensuring the security of your applications.
5. **Customization Options:** While OTP+ simplifies OTP integration, it also offers advanced customization options for developers who require specific configurations or unique use cases. This balance between simplicity and flexibility sets us apart.

To try it out all you have to do is visit [OTP+](#) and follow some simple steps.

Otp Sms Service

Otp Verification

Keycloak

A circular profile picture containing a white letter 'D' on a dark green background.

Follow



## Written by Otp Plus

2 Followers

## Recommended from Medium

The screenshot shows the Kubernetes dashboard interface. On the left sidebar, under the 'Workloads' section, the following items are listed: Overview, Pods, Deployments, DaemonSets, StatefulSets, ReplicaSets, Replication Controllers, Jobs, CronJobs, Config, ConfigMaps, Secrets, Resource Quotas, Limit Ranges, HPA, Pod Disruption Budgets, Priority Classes, Runtime Classes, Leases, and Mutating Webhook. The 'Workloads' tab is currently selected.

The main content area displays a table of workloads:

Name	Namespace	Containers	Restarts	Controlled By	Node	QoS	Age	Status
keycloak-0	default	1	0	StatefulSet	10.0.10.244	BestEffort	10m	Running
keycloak-postgresql-0	default	1	0	StatefulSet	10.0.10.244	BestEffort	10m	Running
csi-oci-node-q9f55	kube-system	1	1	DaemonSet	10.0.10.244	Burstable	20d	Running
kube-proxy-pj859	kube-system	1	1	DaemonSet	10.0.10.244	BestEffort	20d	Running
proxymux-client-7wzq7	kube-system	1	1	DaemonSet	10.0.10.244	Burstable	20d	Running

A terminal window is open at the bottom, showing the command output for deploying the Keycloak chart:

```
admin@Admins-MacBook-Pro ~ % helm install keycloak oci://registry-1.docker.io/bitnami/charts/keycloak
Pulled: registry-1.docker.io/bitnami/charts/keycloak:19.3.3
Digest: sha256:c3b7734f7181b0307bb6aa6a5209e1b628899004dc33df19c68d888bc919eeff5
NAME: keycloak
LAST DEPLOYED: Sat Mar 16 00:02:48 2024
NAMESPACE: default
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: keycloak
CHART VERSION: 19.3.3
APP VERSION: 23.0.7

** Please be patient while the chart is being deployed **

Keycloak can be accessed through the following DNS name from within your cluster:
  keycloak.default.svc.cluster.local (port 80)

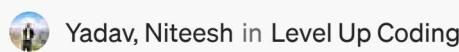
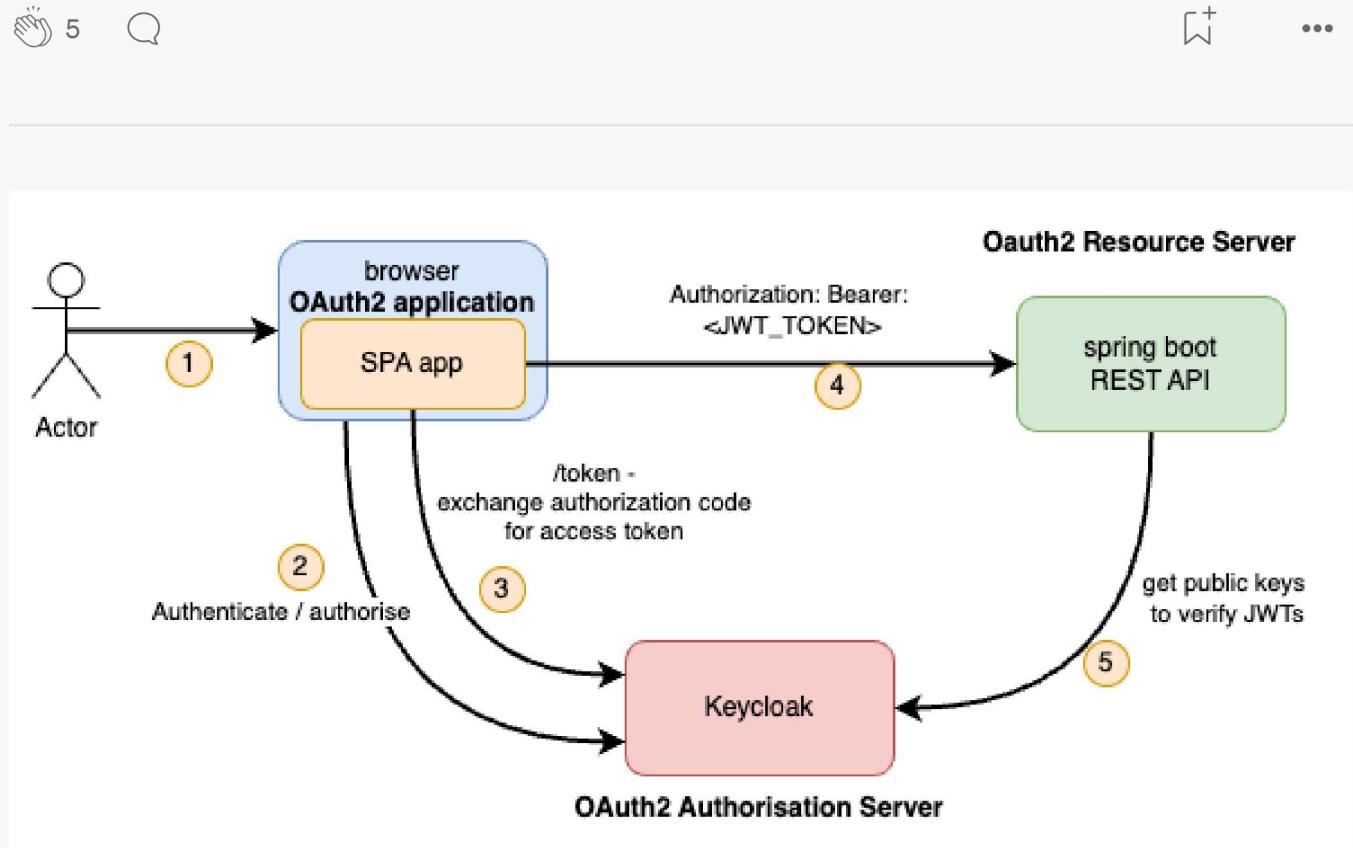
To access Keycloak from outside the cluster execute the following commands:
1. Get the Keycloak URL by running these commands:
  export HTTP_SERVICE_PORT=$([kubectl get --namespace default -o jsonpath='{.spec.ports[?(@.name=="http")].port}' services keycloak])
  kubectl port-forward --namespace default svc/keycloak $([HTTP_SERVICE_PORT]):$([HTTP_SERVICE_PORT]) &
  echo "http://127.0.0.1:$([HTTP_SERVICE_PORT])"
```



# OpenVPN Authentication via Keycloak

OpenVPN is a system that creates secure tunnels between networks. Imagine a secret passage for your data to travel. It uses strong...

★ · 10 min read · Mar 16, 2024



# OpenID Connect (OIDC) Authentication in a React application

## Just a Basic Example

★ · 3 min read · Jan 26, 2024

109



...

### Lists



#### Staff Picks

673 stories · 1092 saves



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

19 stories · 667 saves



#### Self-Improvement 101

20 stories · 2187 saves



#### Productivity 101

20 stories · 1947 saves



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

...

## Clients

Clients are applications and services that can request authentication of a user. [Learn more](#) 

[Clients list](#)[Initial access token](#)[Client registration](#) Search for client[Create client](#)[Import client](#)

1 - 6

Client ID

[account](#)

Name

[\\${client\\_account}](#)

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

 127

...



Benjamin Buffet

## Keycloak Essentials: OpenID Connect

Need to quickly set up a Keycloak server for OIDC? Overwhelmed? Don't fret. Let's simplify to get you started pronto !

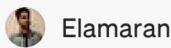
12 min read · May 24, 2024

👏 3    💬 1

Bookmark · More

The screenshot shows the Keycloak admin interface under the 'Session' tab. It displays 'SSO Session Settings' and 'Client session settings' with various configuration fields for session timeout and maximum age.

Setting	Value	Unit
SSO Session Idle	30	Minutes
SSO Session Max	1	Days
SSO Session Idle Remember Me		Minutes
SSO Session Max Remember Me		Minutes
Client Session Idle		Minutes
Client Session Max		Minutes



Elamaran

## Keycloak Session Configuration: Best Practices and Principles

In this article, we delve into the intricacies of Keycloak session and token configuration, focusing on timeouts and optimal settings for...

3 min read · Feb 23, 2024

👏 26



...

See more recommendations