

Keycloak MFA using Mobile Authenticator Setup



Bhuvanesh Kamaraj · [Follow](#)

3 min read · Feb 28, 2024

Listen

Share

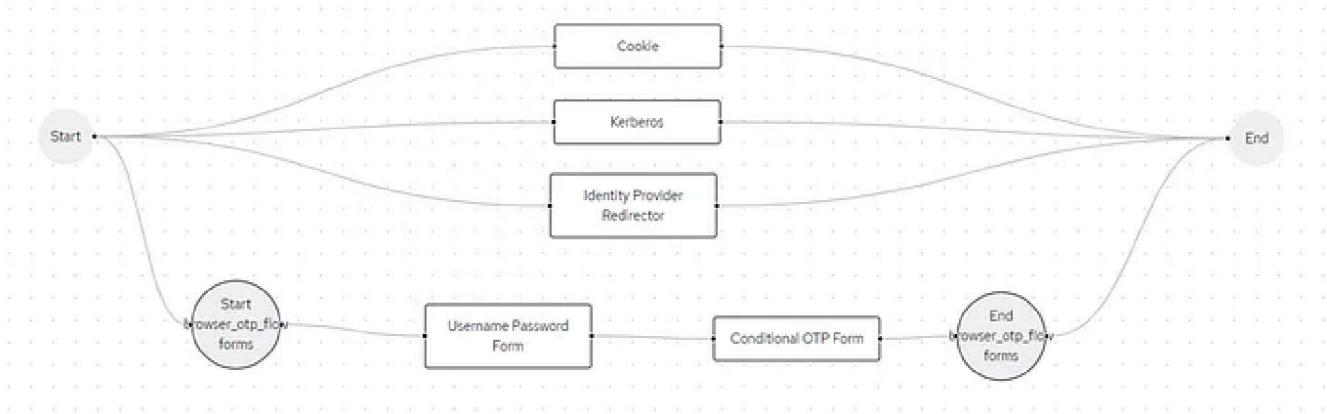
More



Introduction

This document provides a technical guide for setting up Multi-Factor Authentication (MFA) using Mobile Authenticators in Keycloak. This built-in feature supports various apps such as Google Authenticator, Microsoft Authenticator, and Free OTP. The configuration involves defining policies, enabling OTP (One-Time Password) settings, and implementing authentication flows for individual users or user groups.

Authentication Flow:



OTP Policy Configuration

1. Update OTP Policy:

- Navigate to `Realm -> Authentication -> Policies tab.`
- Configure the OTP Policy as per organizational requirements.

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 ⓘ	<input checked="" type="radio"/> Time based <input type="radio"/> Counter based	
OTP hash algorithm ⓘ	SHA1	
Number of digits ⓘ	<input checked="" type="radio"/> 6 <input type="radio"/> 8	
Look around window ⓘ	<input type="button" value="-"/> <input type="text" value="1"/> <input type="button" value="+"/>	
OTP Token period ⓘ	<input type="text" value="30"/> Seconds	
Supported applications ⓘ	FreeOTP Google Authenticator Microsoft Authenticat...	
Reusable token ⓘ	<input type="checkbox"/> Off	
Save Reload		

OTP Configuration and Authentication Flow

1. Enable OTP Configuration:

- Navigate to `Realm -> Authentication -> Required actions tab.`
- Enable “Configure OTP.”

2. Authentication for Individual User or User Group:

- Create a role named “require_otp_role” in `Realm -> Realm role/Client role`.
- Duplicate the “Browser” flow in `Realm -> Authentication -> Flows` -> click “Browser” -> Action -> Duplicate. Name it "browser_otp_flow."
- Under “browser_otp_flow”:
- Delete the “browser_otp_flow — Conditional OTP” form.

Add step to browser_otp_flow forms

The screenshot shows a configuration interface for adding steps to a flow. At the top, there is a search bar and navigation controls (1-10, <, >). Below the search bar, there is a list of options:

- Allow access: Authenticator will always successfully authenticate. Useful for example in the conditional flows to be used after satisfying the previous conditions.
- Automatically set existing user: Automatically set existing user to authentication context without any verification.
- Choose User: Choose a user to reset credentials for.
- Conditional OTP Form: Validates a OTP on a separate OTP form. Only shown if required based on the configured conditions.

- Add a step: “Conditional OTP Form” to “browser_otp_flow forms.”
- Mark “Conditional OTP Form” as required.



- Configure settings:
- Provide an appropriate alias name.
- Force OTP for Role: Select Role as “require_otp_role.”
- Save the settings.

Conditional OTP Form config

Alias * ⓘ
browser_otp

OTP control User Attribute ⓘ
[empty input field]

Skip OTP for Role ⓘ
Select Role

Force OTP for Role ⓘ
require_otp_role ✖ Select Role

Skip OTP for Header ⓘ
[empty input field]

Force OTP for Header ⓘ
[empty input field]

Fallback OTP handling ⓘ
skip

Save **Cancel** **Clear**

3. Bind Flow to Action:

Open in app ↗



- Choose Binding Type: “Browser flow” and save.
- “browser_otp_flow” becomes the default browser flow.

Authentication > Flow details

browser_otp_flow Default Action ▾

Add step Add sub-flow

Steps	Requirement
Cookie	Alternative
Kerberos	Disabled
Identity Provider Redirector	Alternative
browser_otp_flow forms Username, password, otp and other auth forms.	Alternative
Username Password Form	Required
Conditional OTP Form	Required

4. Role Assignment:

- Assign “require_otp_role” to the desired user or user group.

5. User Authentication:

- Users with the “require_otp_role” will be prompted to enter OTP for authentication.
- Note: Remove required actions like “Configure OTP” from the user, as the role dictates the authentication flow in this case.

6. Initial Login Setup:

- When a user logs in for the first time after this change, they will go through the initial OTP setup.

English v

Mobile Authenticator Setup

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

- Install one of the following applications on your mobile:
 - Google Authenticator
 - Microsoft Authenticator
 - FreeOTP
- Open the application and scan the barcode:



Unable to scan?

- 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

7. Subsequent Logins:

- After the initial setup, subsequent logins will require the user to enter a new OTP for authentication.

English v

UserName

One-time code

Sign In

This comprehensive setup ensures that MFA using Mobile Authenticators is configured with specific policies and tailored authentication flows for enhanced

security. Adjust the configurations based on organizational needs and security considerations.

[Follow](#)

Written by Bhuvanesh Kamaraj

8 Followers

Tech aficionado turning complexities into solutions. A coding wizard and innovation enthusiast ready to shape the digital future. Let's create magic!

More from Bhuvanesh Kamaraj



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



...



Bhuvanesh Kamaraj

Okta to Keycloak Single Sign On Implementation

Okta and Keycloak are both identity and access management (IAM) solutions that provide Single Sign-On (SSO) capabilities, allowing users to...

5 min read · Mar 8, 2024



...

Click a feature name for more information.

- Windows Performance Toolkit
- Debugging Tools for Windows
- Application Verifier For Windows
- .NET Framework 4.8 Software Development Kit
- Windows App Certification Kit
- Windows IP Over USB
- MSI Tools
- Windows SDK Signing Tools for Desktop Apps
- Windows SDK for UWP Managed Apps
- Windows SDK for UWP C++ Apps
- Windows SDK for UWP Apps Localization
- Windows SDK for Desktop C++ x86 Apps
- Windows SDK for Desktop C++ amd64 Apps
- Windows SDK for Desktop C++ arm Apps

MSI Tools

Size: 8.6 MB

Tools for creating and editing MSI installer packages.

Estimated disk space required:

8.6 MB

22.6 GB

 Bhuvanesh Kamaraj

How to remove “Repair” option of an MSI File using ORCA Editor

Description: Disable/Remove “Repair” feature from .msi

3 min read · Jan 17, 2024

 3



...

 Bhuvanesh Kamaraj

Docker basic commands

What is Docker ?

2 min read · Mar 8, 2024



...

[See all from Bhuvanesh Kamaraj](#)

Recommended from Medium



Zhimin Wen

Implement SAML based SSO with KeyCloak

Let's explore SAML integration with KeyCloak.



· 4 min read · May 6, 2024



4



...



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



...

Lists



Staff Picks

673 stories · 1092 saves



Stories to Help You Level-Up at Work

19 stories · 667 saves



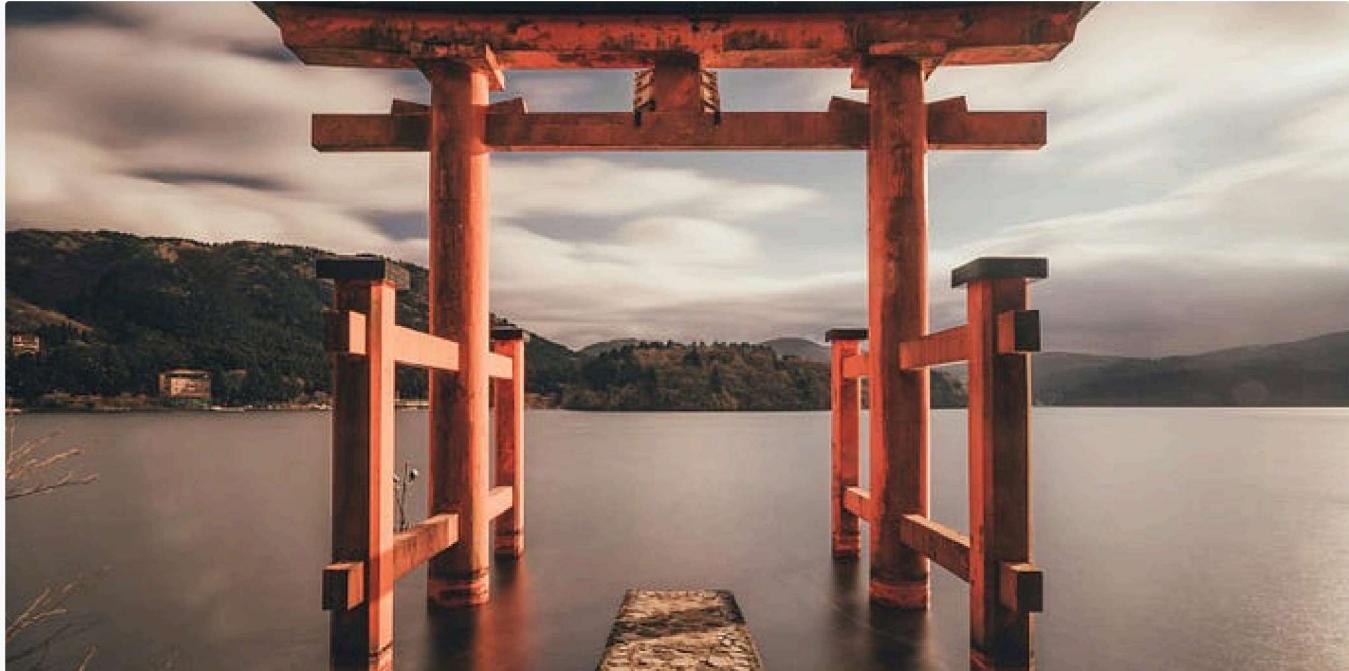
Self-Improvement 101

20 stories · 2187 saves



Productivity 101

20 stories · 1947 saves



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



...

Azure

Create Keycloak
project folder

Docker Hub



Anji Keesari

Setup Keycloak in a Docker Container

Introduction

9 min read · Feb 4, 2024

17 1



...

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}

Type

OpenID Connect

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 1



...



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



...

See more recommendations