Enabling Two-Factor Authentication (2FA) in Keycloak

Two-Factor Authentication (2FA) adds an extra layer of security to user logins by requiring something the user knows (password) and something they have (typically an OTP via a mobile app). This guide explains how to enable and enforce OTP-based 2FA for all or specific users in Keycloak, using the Admin Console, authentication flows, and best practices.

Enabling 2FA via the Admin Console

Log in to the Admin Console

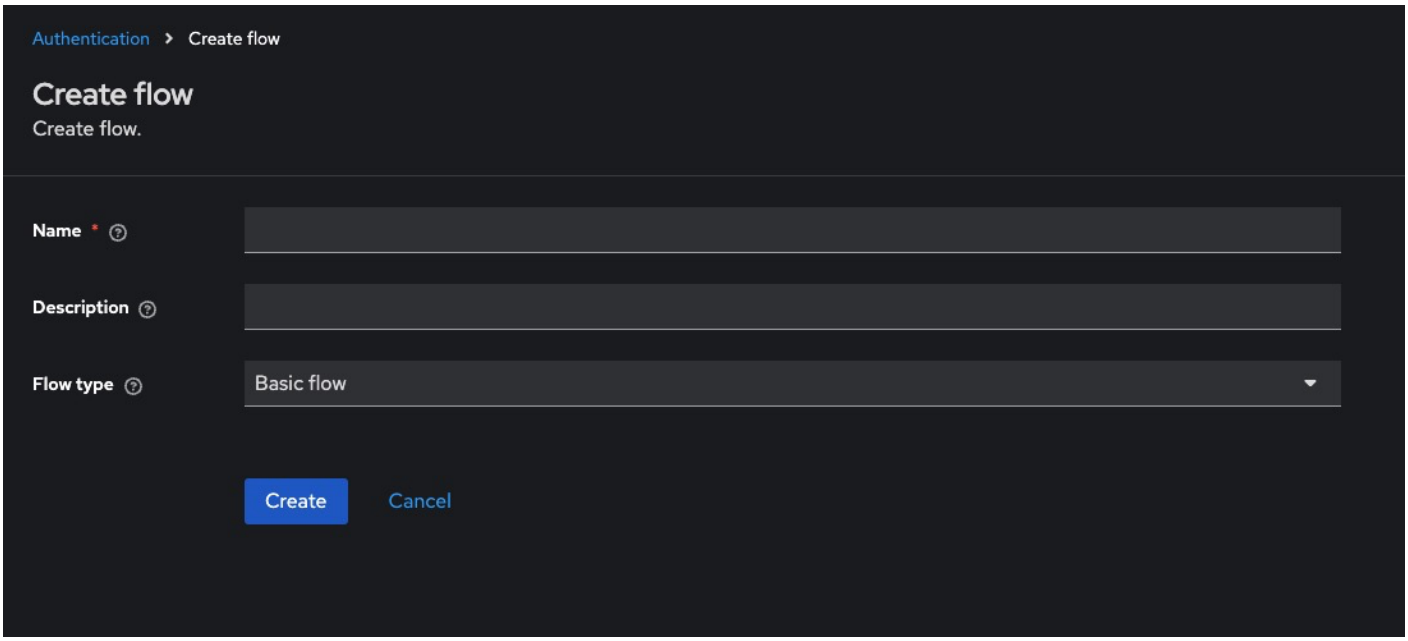
Navigate to:

```
http://<your-keycloak-domain>/admin/
```

Choose the realm where you want to enable 2FA.

Enable OTP in Authentication Flow

1. Go to **Authentication > Flows**
2. Select the **Browser** flow (or copy it if you want a custom flow)
3. Locate the **Browser** execution list:
    - Ensure that **OTP Form** is listed and set to **REQUIRED**
    - If it’s not listed:
        - Click **Add Execution**
        - Choose **OTP Form**, then set its requirement to **REQUIRED**
4. Click **Save**

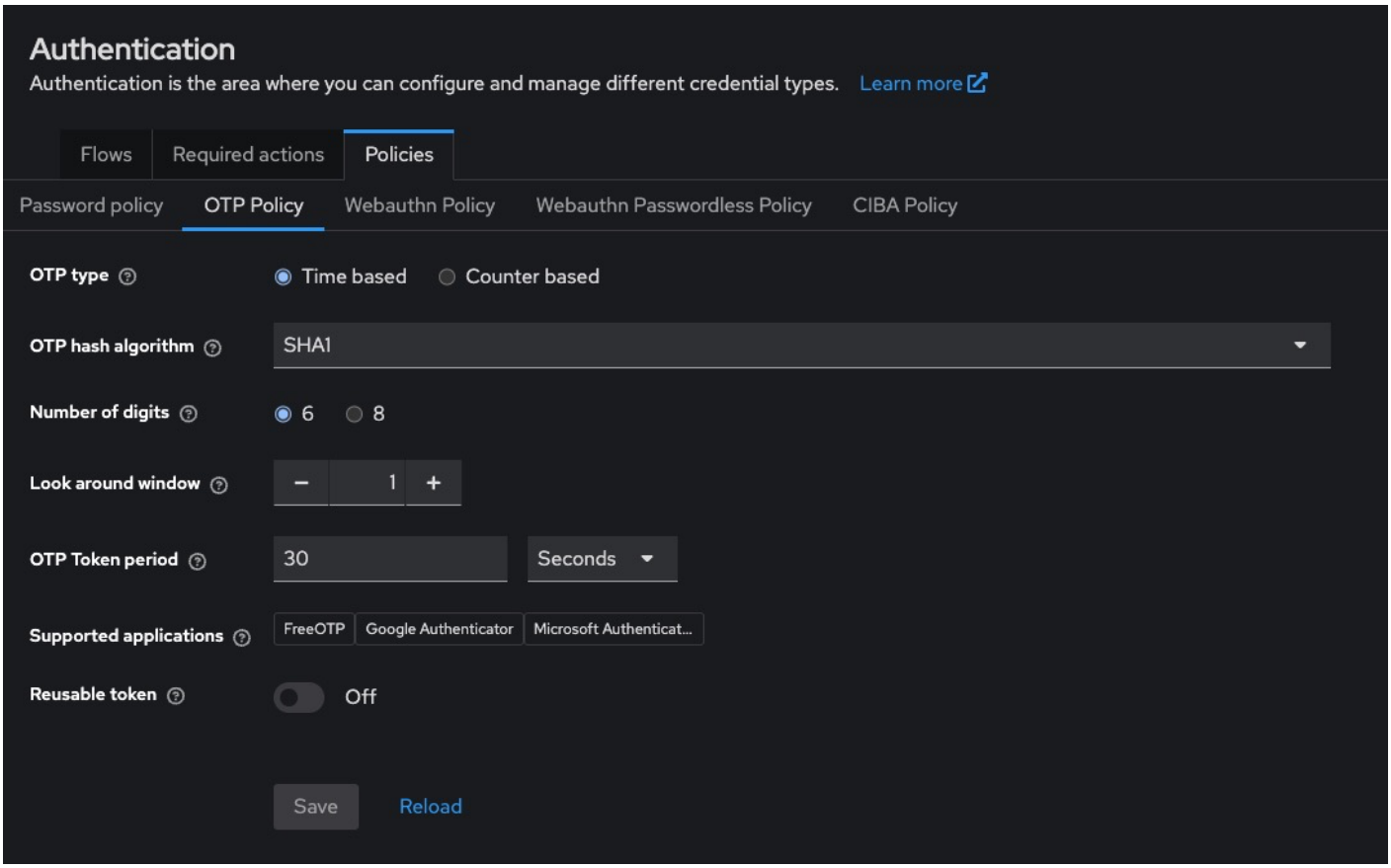


Configure OTP Policy

Go to **Realm Settings > OTP** and configure:

- **OTP Type**: TOTP (time-based, most common)
- **Period**: 30 seconds (default)
- **Digits**: 6
- **Algorithm**: SHA1
- **Look Ahead Window**: 1 or 2

Click **Save**

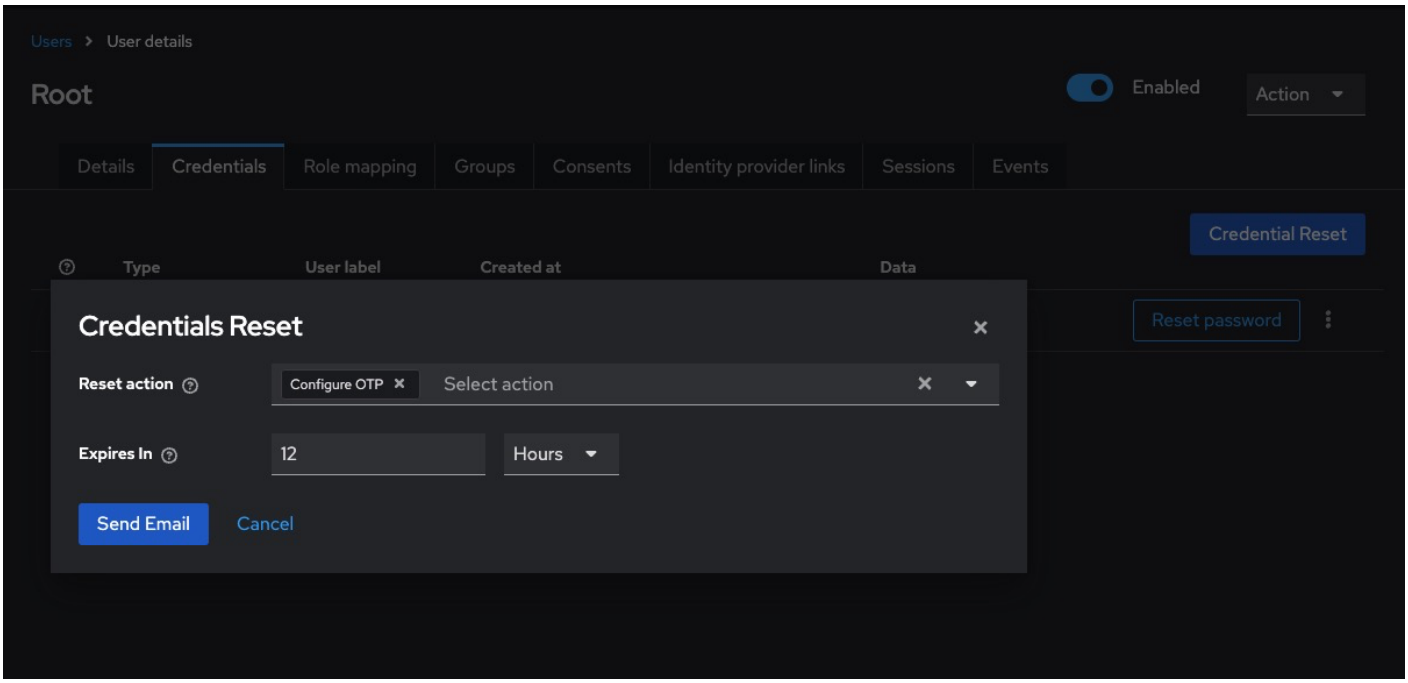


Enforcing 2FA for Specific Users

2FA is optional by default. To make it required for a specific user:

1. Go to **Users > [username]**
2. Open the **Credentials** tab
3. Click **Set Up Required Action**
4. Choose **Configure OTP** from the dropdown
5. Click **Save**

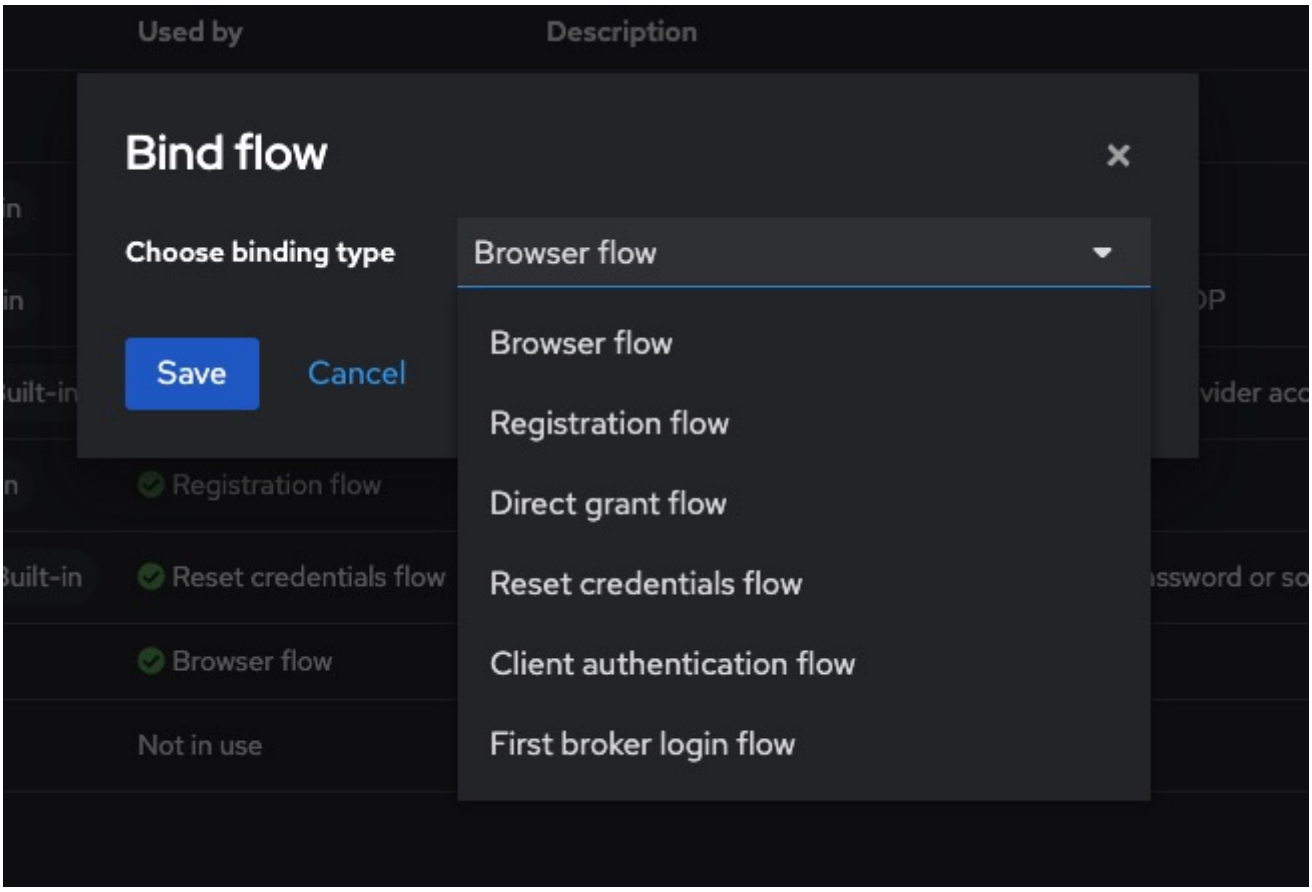
The user will be prompted to set up 2FA on their next login.



Enforcing 2FA for All Users

To enforce 2FA globally:

1. Go to **Authentication > Bindings**
2. Set **Browser Flow** to a flow where **OTP Form** is REQUIRED
3. All users will be required to configure 2FA on their next login if not already done



Enabling 2FA via REST API

Get Admin Access Token

```
curl -X POST "https://<keycloak-domain>/realms/master/protocol/openid-connect/token" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "username=admin" \
  -d "password=admin-password" \
  -d "grant_type=password" \
  -d "client_id=admin-cli"
```

Assign “Configure OTP” Required Action to a User

```
curl -X PUT "https://<keycloak-domain>/admin/realms/<realm>/users/<user-id>" \
  -H "Authorization: Bearer <access_token>" \
  -H "Content-Type: application/json" \
  -d '{"requiredActions": ["CONFIGURE_TOTP"]}'
```

To get the user ID:

```
curl -H "Authorization: Bearer <access_token>" \
  https://<keycloak-domain>/admin/realms/<realm>/users?username=<username>
```

Enabling 2FA via Docker CLI

Authenticate and Set OTP Action

```
docker exec -it keycloak bash

/opt/keycloak/bin/kcadm.sh config credentials \
  --server http://localhost:8080 \
  --realm master --user admin --password admin

/opt/keycloak/bin/kcadm.sh update users/<user-id> -r <realm> \
  -s 'requiredActions=["CONFIGURE_TOTP"]'
```

Required Permissions for 2FA Management

- Requires manage-users role
- REST API calls must use a token with manage-users permission in the realm

To assign via Admin Console:

```
Users > [admin-user] > Role Mappings > Realm Roles > Add 'manage-users'
```

Best Practices for 2FA

- **Use Time-Based OTP (TOTP):** TOTP is compatible with standard apps like Google Authenticator, Authy, or FreeOTP.
- **Customize OTP Setup Page:** Modify the otp.ftl page inside your theme to reflect your brand and offer setup instructions.
- **Inform Users Before Enforcing:** Enable OTP as a required action with communication ahead of rollout to avoid login issues.

- **Use Conditional 2FA Flows:** Use **conditional executions** (e.g., only require OTP from outside a trusted network/IP range).
- **Back Up OTP Configuration:** Encourage users to back up their OTP seed or enable recovery codes for critical accounts.

Common Issues and Troubleshooting

Issue	Possible Cause	Solution
Users not prompted for 2FA	OTP Form not set to REQUIRED in flow	Set requirement to REQUIRED in the Browser flow
OTP setup skips	Configure OTP not added as required action	Manually assign it to users or enforce via default flow
“Invalid TOTP” error on login	Wrong time sync or wrong app	Ensure mobile device clock is correct and app supports TOTP
OTP works once then fails	Look-ahead window too small	Increase look-ahead window under Realm Settings > OTP
No OTP page shown after password	Flow misconfigured	Review order and requirement levels of all executions in the flow

---

Revision #1
Created 2025-06-17 13:56:30 UTC
Updated 2025-06-17 14:45:53 UTC