Password Policies

- Password Policies
  - Requirement
  - How to configure Password Policies
  - Implementation
- Password Reset
  - Requirement
  - How to configure Password Recovery
  - Implementation
- 2-Factor-Auth
  - Levels of Authentication
  - Setup for Catena-X
  - How to Setup - Yubikey as 2-Fact-Auth
- OTP Policy PLANNED TO RETIRE
  - Configuration for Catena-X

Password Policies

Password Policies are restrictions and/or requirements that a user must follow to ensure that their password is strong/secure.

In Keycloak, password policies are set per realm.

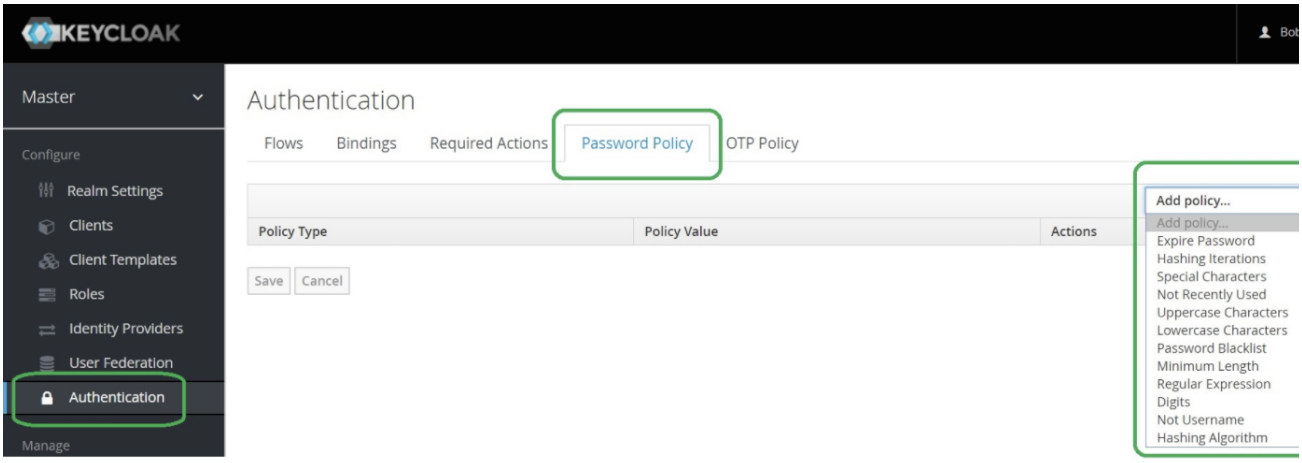
Requirement

- [ ] Default Password Policies are needed for every realm - the policies are set by Catena-X and identical for all realms
- [ ] Password refresh every 90 days
- [ ] Password length 15+ digits
- [ ] Password characters: letters + minimum 1 number is mandatory
- [ ] Password shouldn't be the same as the username or email
- [ ] If the Password is getting reset by the user and is not fitting the password policies, a error message with a detailed error code will get shown

How to configure Password Policies

Open Keycloak admin page, go to "Authentication" and open the "Password Policy" tab.

Click on the **Add policy ...** to see the list of available password policies.



Select the relevant policy and set the policy value by adding the relevant number. Important: only numbers are to be added, no letters.

After saving the policy, Keycloak login enforces the policy for new users. Existing users can still login with theire old password, but as soon as a password change request is getting triggered the new policies will take affect.

Blacklisting passwords is possible via UTF-8 file, for Catena-X no blacklisting is planned so far.

Implementation

tbd

Password Reset

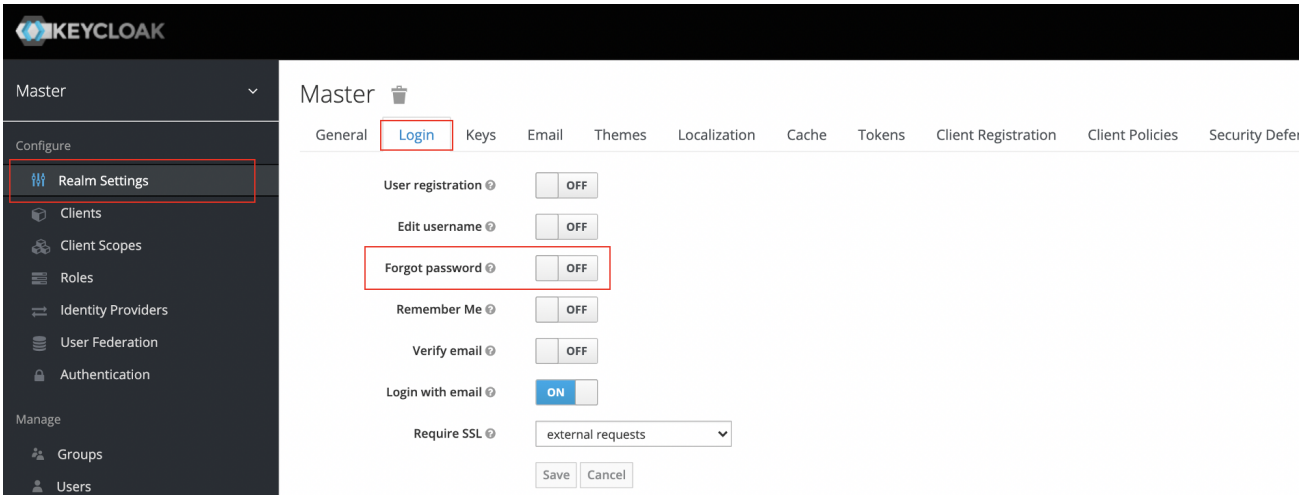
If Password reset is enabled, users are able to reset their credentials if they forget their password or lose their OTP generator.

Requirement

- [ ] Forgot Password option should be available for all users using Shared IdP
- [ ] New Password needs to get validated against the configured Password Policies
- [ ] Config needs to get automatically set whenever a new realm is getting created

How to configure Password Recovery

Go to the `Realm Settings` left menu item, and click on the `Login` tab. Switch on the `Forgot Password` switch.



The new password will get send via email.

The email text is fully configurable. How: extend or edit the theme associated with it.

When the user clicks on the email link, they will be asked to update their password, and, if they have an OTP generator set up, they will also be asked to reconfigure this as well. Depending on the security requirements of your organization you may not want users to be able to reset their OTP generator through email. You can change this behavior by going to the `Authentication` left menu item, clicking on the `Flows` tab, and selecting the `Reset Credentials` flow.

Implementation

tbd

2-Factor-Auth

Levels of Authentication

Level 0: Authentication by username and password only. No 2-factor-auth.

Level 1: Authentication by username and password; plus additionally 2-factor-auth via Keycloak OTP

Level 2: Authentication by username and password; plus additionally 2-factor-auth via configured webauth method

Level	Username + Password	2-Factor-Method	Customization	Security Level (0 = low; 2 = high)	Support by CX
0	✅	❌	❌	0	not supported
1	✅	✅	❌	2	available
2	✅	✅	✅	2	available

Setup for Catena-X

Keycloak 2-Factor-Auth is mandatory for all users/identities which are managed by Catena-X and not federated by any company identity management system.

Config for the Master Realm

The Master realm, holding the admin accounts, is configured to

- Each User needs to mandatorily configure OTP
- Each User needs to mandatorily update the password after the first login
- Password policies as per chapter PasswordPolicies need to get followed

Config for the Catena-X Realm

tbd

Config for the Company Spec. Realm

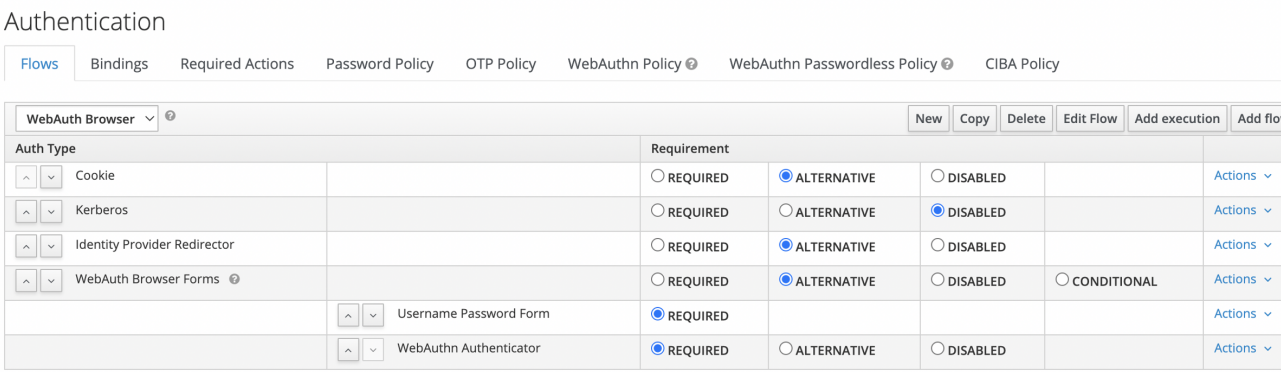
The Shared Company realm, holding the user accounts for the company, is configured as following

- Each User needs to mandatorily configure OTP
- Each User needs to mandatorily update the password after the first login
- Password policies as per chapter PasswordPolicies need to get followed

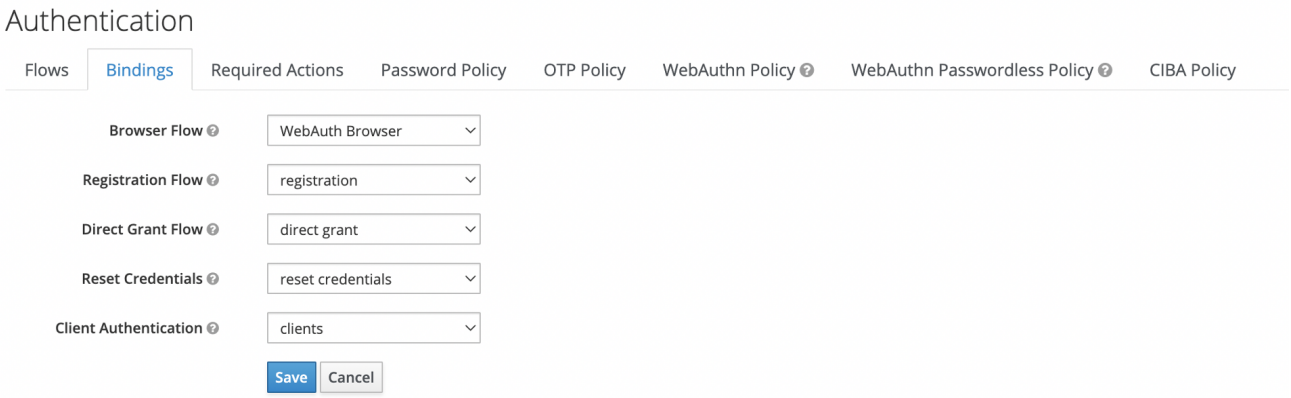
How to Setup - Yubikey as 2-Fact-Auth

The IdP, where the user is stored/created (for SharedIdP Companies its the SharedIdP; for CX Operators its the CentralIdP as well as the SharedIdP) an authentication flow need to get configured.

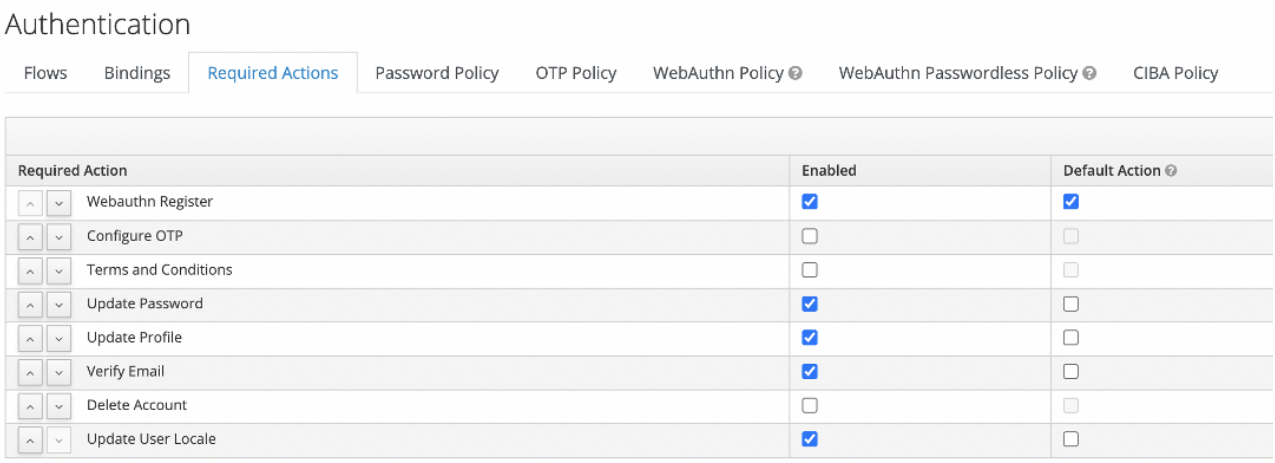
#1 Create New Auth Flow as shown below



#2 Set the Auth Flow as browser flow



#3 Update the Required Actions



OTP Policy PLANNED TO RETIRE

Any policies you set under OTP Policies will be used to validate one-time passwords. When configuring OTP, FreeOTP and Google Authenticator can scan a QR code that is generated on the OTP set up page that Keycloak has. The bar code is also generated from information configured on the `OTP Policy` tab.

OTP Type

Select between Time Based and Counter Based; Time Based is the more secure solution.

OTP Hash Algorithm

Default is SHA1, more secure options are SHA256 and SHA512.

Number of Digits

How many characters is the OTP? Short means more user friendly as it is less the user has to type. More means more security.

Look Ahead Window

How many intervals ahead should the server try and match the hash? This exists so just in case the clock of the TOTP generator or authentication server get out of sync. The default value of 1 is usually good enough. For example, if the time interval for a new token is every 30 seconds, the default value of 1 means that it will only accept valid tokens in that 30 second window. Each increment of this config value will increase the valid window by 30 seconds.

OTP Token Period

Time interval in seconds a new TOTP will be generated by the token generator. And, the time window the server is matching a hash.

Configuration for Catena-X

- OTP Type: Time Based
- OTP Hash Algorithm: SHA256
- Number of digits: 6
- Look Ahead Window: 1
- Token Period: 30