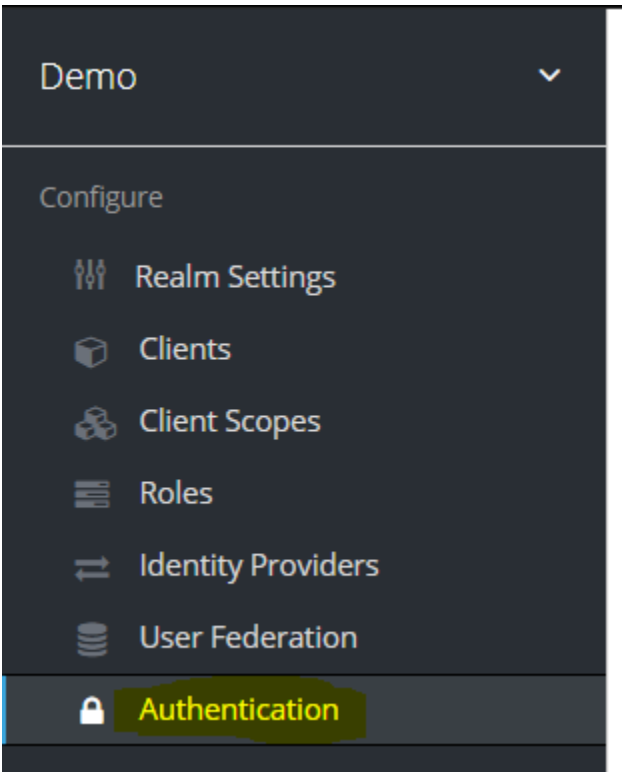


Authentication flow. Конфигурация потоков аутентификации и политик

Настройка аутентификационных потоков в системе выполняется в меню администратора.



В системе уже имеются преднастроенные потоки, которые назначаются по умолчанию. К примеру поток регистрации:

Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Registration

Auth Type		Requirement	
Registration Form		<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED
	Registration User Creation	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED
	Profile Validation	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED
	Password Validation	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED
	Recaptcha	<input type="radio"/> REQUIRED	<input checked="" type="radio"/> DISABLED

Шаги в потоках можно изменять:

1. Изменять очередность.
2. Создавать вложенности и зависимости.
3. Выставлять тип шага: Altrnative (альтернативный), Required (необходимый) или отключать (disabled).

В шаги аутентификации возможно добавлять вариант аутентификации через внешнего провайдера, форму логина/пароля, добавлять дополнительные проверки OTP –кодами или другими факторами, в случае разработки собственных провайдеров.

Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Copy Of Browser

New Copy Delete Add execution Add flow

Auth Type		Requirement				
Cookie		<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Actions	
Kerberos		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED	Actions	
Identity Provider Redirector		<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Actions	
Copy Of Browser Forms		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL Actions	
	Username Password Form	<input checked="" type="radio"/> REQUIRED			Actions	
	Copy Of Browser Browser - Conditional OTP	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL Actions	
	Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED		Actions	
	OTP Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Actions	

После создания и настройки собственного потока аутентификации его также можно задать как для всего реалма (в зависимости от сценария применимости):

Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Browser Flow ?

Copy of browser

Registration Flow ?

registration

Direct Grant Flow ?

direct grant

Reset Credentials ?

reset credentials

Client Authentication ?

clients

Save Cancel

Либо на уровне отдельно взятого клиента в общих настройках:

Root URL ?

* Valid Redirect URIs ?

*

Base URL ?

Admin URL ?

Web Origins ?

+

> Fine Grain OpenID Connect Configuration ?

> OpenID Connect Compatibility Modes ?

> Advanced Settings ?

Authentication Flow Overrides ?

Browser Flow ?

Copy of browser

Direct Grant Flow ?

Save

Cancel

Описание по заполнению конфигурационных параметров

Требования по запрашиваемым действиям при первом логине и сбросе настроек выставляются для всех пользователей пространства в блоке Authentication. Для всех пользователей Keycloak может выставляться единое требование по смене пароля.

Authentication

Flows	Bindings	Required Actions	Password Policy	OTP Policy
Required Action		Enabled	Default Action ?	
Configure OTP		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Terms and Conditions		<input type="checkbox"/>	<input type="checkbox"/>	
Update Password		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Update Profile		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Verify Email		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Требования к паролям пользователей необходимо настраивать в области Authentication

Authentication

Flows

Bindings

Required Actions

Password Policy

OTP Policy

Policy Type	Policy Value

Save

Cancel

Add policy...

Add policy...

Expire Password

Hashing Iterations

Special Characters

Not Recently Used

Uppercase Characters

Lowercase Characters

Password Blacklist

Minimum Length

Regular Expression

Digits

Not Username

Hashing Algorithm

Рекомендуемые требования к паролям (Password Policy):

Flows

Bindings

Required Actions

Password Policy

OTP Policy

Policy Type	Policy Value	Actions
Expire Password	90	Delete
Hashing Iterations	15000	Delete
Special Characters	1	Delete
Not Recently Used	3	Delete
Uppercase Characters	1	Delete
Lowercase Characters	1	Delete
Minimum Length	10	Delete
Digits	1	Delete
Not Username		Delete

Save

Cancel

Add policy...

Параметр	Описание	Значение	Рекомендация к установке
Expire Password	Количество дней, в течение которых действителен пароль. По истечении указанного количества дней пользователь должен изменить свой пароль.	90	Y

Hashing Iterations	Это значение указывает, сколько раз пароль будет хэшироваться перед сохранением или проверкой. Значение по умолчанию-20 000. Получив доступ к базе данных, хакеры могут перепроектировать пароли пользователей. Рекомендуемое значение этого параметра меняется каждый год по мере повышения мощности процессора. Более высокое значение итераций хэширования требует большей мощности процессора и может повлиять на производительность.	15000	Y
HashAlgorithm	Пароли не хранятся в виде открытого текста. Вместо этого они хэшируются с использованием стандартных алгоритмов хэширования, прежде чем они будут сохранены или проверены. Единственным встроенным и стандартным алгоритмом является PBKDF2. Переопределение возможно, но требует разработки.	-	N
Digits	Количество цифр, необходимых для ввода пароля.	1	Y
Lowercase Characters	Количество строчных букв, необходимых для ввода пароля.	1	Y
Uppercase Characters	Количество прописных букв, необходимых для ввода пароля.	1	Y
Special Characters	Количество специальных символов, таких как '?!# % \$ 'необходимых для ввода пароля.	1	Y
Not Username	При установке пароль не должен совпадать с именем пользователя.		Y

Regular Expression	Определите один или несколько шаблонов регулярных выражений, которым должны соответствовать пароли.	<pre>(?=.*[0-9])(?=.*[!@#\$%^&*])(?=.*[a-z])(?=.*[A-Z])[0-9a-zA-Z!@#\$%^&*]{10,}</pre> <p>Пояснение:</p> <ul style="list-style-type: none"> • <code>(?=.*[0-9])</code> - строка содержит хотя бы одно число; • <code>(?=.*[!@#\$%^&*])</code> - строка содержит хотя бы один спецсимвол; • <code>(?=.*[a-z])</code> - строка содержит хотя бы одну латинскую букву в нижнем регистре; • <code>(?=.*[A-Z])</code> - строка содержит хотя бы одну латинскую букву в верхнем регистре; • <code>[0-9a-zA-Z!@#\$%^&*]{10,}</code> - строка состоит не менее, чем из 10 вышеупомянутых символов. 	N
Not Recently Used	Эта политика сохраняет историю предыдущих паролей. Количество сохраненных старых паролей настраивается. Когда пользователь меняет свой пароль, он не может использовать сохраненные пароли.	3	Y
Password Blacklist	Черные списки паролей	-	N
Minimum Length	Минимальное число символов в пароле	10	Y