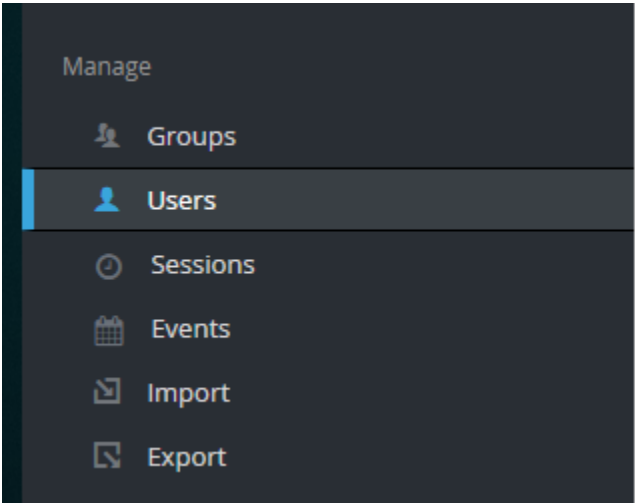


Registration. Регистрация и конфигурация пользователя

Функциональность ведения пользователей в системе соответствует меню:



Данная область позволяет просмотреть пользователей в системе. Поиск будет осуществлен по умолчанию в локальной базе Keycloak.

Для отражения пользователей из других источников потребуется предварительная синхронизация в предустановленных федерациях.


Требования по заполнению конфигурационных параметров

При регистрации пользователя в Keycloak рекомендуется задавать следующие настройки:

Details

Наименование в UI KeyCloak	Наименования по API Keycloak	Описание	Уникальность	Автозаполняется
-------------------------------	------------------------------------	----------	--------------	-----------------


ID	id	<p>уникальный идентификатор, выданный клиенту, автогенерируемое поле</p> <p>Из Active Directory всегда будут подтягиваться только активные пользователи. При синхронизации с AD "уволившиеся" будут удаляться физически (по настроенному фильтру). При синхронизации с AD для настройки групп и получения ролей, к сожалению, без удаления пользователей и повторной синхронизации мапперы по ролям корректно не обрабатываются. Идентификаторы пользователей в таком случае тоже в keusloak создаются каждый раз новые. Поэтому рекомендуется к использованию email (или другой бизнес-значимый) как уникальный идентификатор пользователя.</p>	Y	Y
Username	username	<p>Имя пользователя.</p> <p>Допустимые символы /^[a-z0-9_\. -]+)@([a-z0-9_\. -]+)\.([a-z\.] {2,6})\$/</p>	Y	N
Email	email	электронная почта	N	N
First Name	firstName	Имя	N	N
Last Name	lastName	Фамилия	N	N
User Enabled	enabled	Возможность логина.	N	Y
Email Verified	emailVerified	Признак, что почта была проверена при заведении пользователя.	N	N

<p>Required User Actions</p> <p>Важно! Следующие настройки могут быть установлены на каждом пользователе отдельно. Но к данной функции стоит прибегать в исключительных случаях.</p> <p>Данные параметры следует настраивать блоке Authentication для всех пользователей единообразно.</p>	<p>requiredActions</p>	<p>Запрашиваемые действия при логине пользователя:</p> <p>Verify Email (подтверждать почту при входе. Для пространства должен быть настроен почтовый сервер предварительно)</p> <p>Update Profile (запрос на обновление данных профайла при входе)</p> <div><h3>Update Account Information</h3><div> You need to update your user profile to activate your account.</div><div><p>Email</p><input type="text" value="vivelavie@inbox.ru"/></div><div><p>First name</p><input type="text" value="newuser2"/></div><div><p>Last name</p><input type="text" value="newuser2"/></div><div><p>Submit</p></div></div> <p>Update Password</p> <p>Требование по смене пароля</p>	<p>N</p>	<p>N</p>
--	------------------------	---	----------	----------

		Configure OTP		
		Требование по вводу QR-кода		
Impersonate user		Возможность входа Администратора под учеткой пользователя. Администратору часто бывает полезно выдавать себя за пользователя. Например, при возникновении ошибки у пользователя. Администратор может войти в систему для воспроизведения ошибки.	N	N

Помимо основных метаданных пользователя, таких как имя и адрес электронной почты, возможно хранить произвольные атрибуты пользователя.

Пример:

Johndoe 

Details

Attributes

Credentials

Role Mappings

Groups

Consents

Sessions

Key	Value	Actions
mobile	<input type="text" value="555-555-5555"/>	Delete
<input type="text"/>	<input type="text"/>	Add

Save

Cancel

User Credentials

Управление учетными данными пользователей

Наименование в UI KeyCloak	Описание	Уникальность	Автозап
New Password	Новый пароль. При заведении пользователя через админку KeyCloak необходимо задавать данные параметры	Y	
Password Confirmation			

Temporary

Параметр, позволяющий затребовать смену пароля при первом логине.

N

Запрашиваемые действия, которые пользователь должен выполнить, прежде чем ему будет разрешено войти в систему при сбросе настроек.

Update Password

Если настроена электронная почта, можно отправить пользователю электронное письмо с просьбой сбросить пароль. Выберите Update Password в списке Reset Actions и нажмите кнопку Send Email. Возможно дополнительно установить действительность ссылки электронной почты, которая по умолчанию устанавливается на вкладке Tokens в настройках Realms. Отправленное письмо содержит ссылку, которая приведет пользователя к экрану обновления пароля.

Update Password	Configure OTP	Verify Email	Update Profile
Пользователь должен изменить свой пароль при первом логине.	При установке пользователь должен настроить генератор одноразовых паролей на своем мобильном устройстве с помощью приложения Free OTP или Google Authenticator.	При установке пользователь должен убедиться, что у него есть действующая учетная запись электронной почты. Пользователю будет отправлено электронное письмо со ссылкой, которую он	Это обязательное действие требует от пользователя обновить информацию о своем профиле, т. е. свое имя, адрес, адрес электронной почты и/или номер телефона.

N

Reset Actions

Credential Reset

Reset Actions

✕ Configure OTP

✕ Update Profile

✕ Update Password

✕ Verify Email

Expires In

12

Hours

Reset Actions Email

Send email

			должен кликнуть. Как только этот процесс будет успешно завершен, ему будет разрешено войти в систему.			
--	--	--	--	--	--	--

Способы регистрации и конфигурации

Регистрация пользователя через панель администрирования KeyCloak

Ниже приводится описание шагов администратора, необходимых для регистрации пользователей через панель администрирования.

1. Для добавления нового пользователя необходимо выполнить действие "Add User":

Demo

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity

Providers

User Federation

Authentication

Manage

Groups

Users

Users

LookupPermissions

Search...

View all users

Unlock users

Add user

ID	Username	Email	Last Name	First Name	Actions
eedf7726-66b4-40...	user@mail.ru	user@mail.ru	User	User	EditImpersonateDelete

2. Заполнить пользовательские данные в соответствии с описанием из 1. Требования по заполнению конфигурационных параметров, блок Details.

Add user

ID	<input type="text"/>
Created At	
Username *	<input type="text" value="iiivanov@vtb.ru"/>
Email	<input type="text" value="ivanov@vtb.ru"/>
First Name	<input type="text" value="Иван"/>
Last Name	<input type="text" value="Иванов"/>
User Enabled ⓘ	<input checked="" type="checkbox"/> ON
Email Verified ⓘ	<input type="checkbox"/> OFF
Required User Actions ⓘ	<input type="text" value="Select an action..."/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

3. Создать пароль в соответствии с описанием из «Требования по заполнению конфигурационных параметров», блок User Credentials
4. Требования по запрашиваемым действиям при первом логине и сбросе настроек выставляются для всех пользователей пространства в блоке Authentication.

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"/>		

Самостоятельная регистрация пользователя с использованием формы входа сервера KeyCloak

Настраивается на уровне Realm

The screenshot shows the Keycloak Admin Console interface. On the left is a dark sidebar with a menu. The top of the sidebar has a dropdown menu labeled 'Demo'. Below it is a 'Configure' section with 'Realm Settings' highlighted. Under 'Manage', there are links for 'Groups', 'Users', 'Sessions', and 'Events'. The main content area is titled 'Demo' with a trash icon. It has several tabs: 'General', 'Login' (which is active), 'Keys', 'Email', 'Themes', 'Cache', and 'Tok'. The 'Login' tab contains several settings, each with a help icon (question mark in a circle):

- User registration**: A toggle switch set to 'ON'.
- Email as username**: A toggle switch set to 'OFF'.
- Edit username**: A toggle switch set to 'OFF'.
- Forgot password**: A toggle switch set to 'OFF'.
- Remember Me**: A toggle switch set to 'OFF'.
- Verify email**: A toggle switch set to 'OFF'.
- Login with email**: A toggle switch set to 'ON'.
- Require SSL**: A dropdown menu currently showing 'external requests'.

At the bottom of the settings are two buttons: 'Save' and 'Cancel'.

Возможна кастомизация формы регистрации. Например, добавление номера телефона при регистрации. Выполняется через шаблоны тем the template themes/_____/login/register.ftl.

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

Add 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

Параметр	Описание	Значение	Рекомендац ия 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"> • (?!.*[0-9]) - строка содержит хотя бы одно число; • (?!.*[!@#\$%^&*]) - строка содержит хотя бы один спецсимвол; • (?!.*[a-z]) - строка содержит хотя бы одну латинскую букву в нижнем регистре; • (?!.*[A-Z]) - строка содержит хотя бы одну латинскую букву в верхнем регистре; • [0-9a-zA-Z!@#\$%^&*]{10,} - 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