

АО «СберТех» (является дочерним обществом ПАО Сбербанк)

117105, Москва, Новоданиловская наб., д. 10

Продукт Platform V IAM SE (IAM)

Руководство по эксплуатации

Содержание

Руководство по эксплуатации компонента Keycloak.SE (KCSE)	4
Руководство по системному администрированию компонента Keycloak.SE 4	
Сценарии администрирования..... 4	
События системного журнала 148	
События мониторинга 149	
Настройка интеграции с ОСА 173	
Часто встречающиеся проблемы и пути их устранения..... 176	
Руководство оператора компонента Keycloak.SE (KCSE) 177	
Доступ к приложению 177	
Использование приложения оператором 182	
Часто встречающиеся проблемы и пути их устранения..... 203	
Параметры настройки 203	
Правила эксплуатации 207	
Детальное описание полей интерфейса 208	
Руководство прикладного разработчика компонента Keycloak.SE (KCSE) 244	
Системные требования..... 244	
Подключение и конфигурирование 245	
Миграция на текущую версию..... 245	
Быстрый старт 245	
Запуск контейнера без прав внесения изменений в корневой файловой системе.... 260	
Использование программного компонента 261	
Часто встречающиеся проблемы и пути их устранения..... 261	
Руководство по эксплуатации компонента IAM Proxy (AUTH)..... 265	
Руководство по системному администрированию компонента IAM Proxy (AUTH) 265	
Сценарии администрирования..... 265	
Параметры настройки 267	
Администрирование с помощью компонента PACMAN (CFGА) 273	
Использование приложения администратором 276	
События системного журнала 285	
События мониторинга 298	
Часто встречающиеся проблемы и пути их устранения..... 308	

Руководство прикладного разработчика компонента IAM Proxy (AUTH)	311
Системные требования.....	311
Подключение и конфигурирование	311
Миграция на текущую версию.....	323
Быстрый старт	324
Использование программного компонента	324
Часто встречающиеся проблемы и пути их устранения.....	327

Руководство по эксплуатации компонента KeyCloak.SE (KCSE)

Руководство по системному администрированию компонента KeyCloak.SE (KCSE)

Сценарии администрирования

Создание административной учетной записи

После установки KeyCloak.SE потребуется учетная запись администратора, которая может действовать как супер-администратор с полными правами на управление всеми частями KeyCloak.SE. Эта учетная запись позволит войти в консоль администратора KeyCloak.SE с возможностью создавать realms и пользователей и регистрировать приложения, защищенные KeyCloak.SE.

Примечание: Требуется выполнить задачи по установке и настройке, определенные в Руководстве по установке и настройке сервера, до того момента, когда сервер KeyCloak.SE будет запущен.

Если сервер доступен с локального хоста, выполните следующие действия:

- В веб-браузере перейдите на URL-адрес <http://localhost:8080/>.
- Введите имя пользователя и пароль.



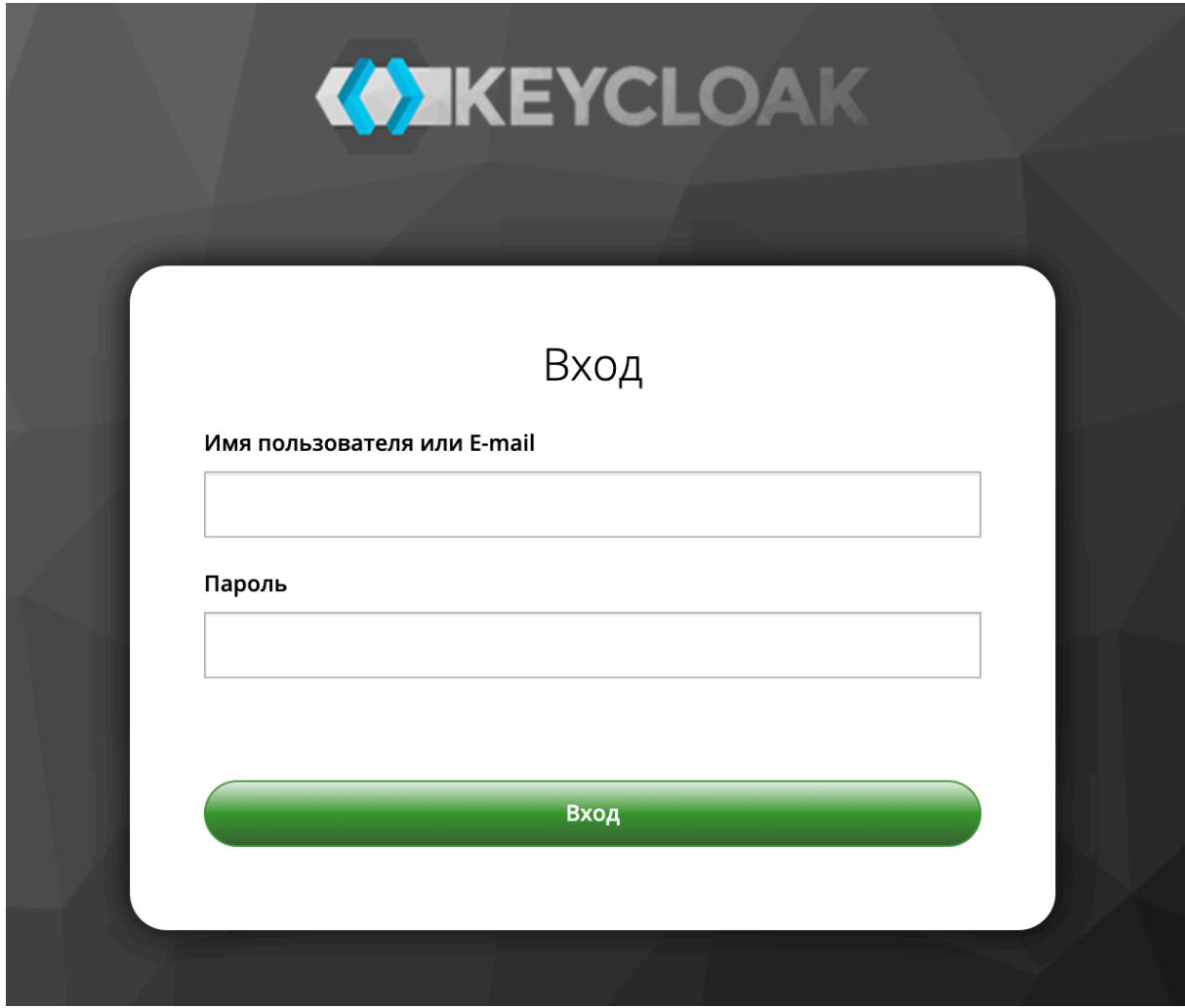
Welcome to **Keycloak**

A screenshot of the Keycloak Administration Console login interface. It features a large input field for 'Username' and 'Password', and a 'Create' button. To the right, there are three links: 'Documentation >' (with a file icon), 'Keycloak Project >' (with a gear icon), 'Mailing List >' (with an envelope icon), and 'Report an issue >' (with a bug icon). The footer of the page includes the JBoss Community logo.

После создания административной учетной записи для можно настроить realm. Realm - это пространство, в котором происходит управление объектами, включая пользователей, приложения, роли и группы. Пользователь принадлежит к realm и входит в нее. Одно развертывание KeyCloak.SE может определять, хранить и управлять столькими realm, для которых есть место в базе данных.

Настройка realms и выполнение большинства административных задач происходит в консоли администратора KeyCloak.SE (KeyCloak.SE Admin Console).

Перейдите по URL-адресу консоли администратора. Например, для localhost используйте этот URL: <http://localhost:8080/admin>



Введите имя пользователя и пароль, которые вы создали на странице приветствия. Это действие отобразит консоль администратора.

Управление Realm

Когда впервые загружается KeyCloak.SE, то создается предварительно определенная область. Это начальная область является master-realm. Realm - это область управления

объектами, включая пользователей, приложения, роли и группы. В консоли администратора существуют два типа областей:

Master-realm - это самый высокий уровень в иерархии областей. Учетные записи администраторов в этом realm имеют права на просмотр и управление любым другим realm, созданным на данном экземпляре сервера. При определении начальной учетной записи администратора, создается учетная запись в master-realm. Первоначальный вход в консоль администратора также будет осуществляться через master-realm. Прочие realms - создаются администратором в master realm. В этих областях администраторы управляют пользователями в организации и приложениями, которые им нужны. Приложения принадлежат пользователям. Realms изолированы друг от друга и могут управлять и аутентифицировать только тех пользователей, которых они контролируют. Следование этой модели безопасности помогает предотвратить случайные изменения и следует традиции предоставления учетным записям пользователей доступа только к тем привилегиям и полномочиям, которые необходимы для успешного выполнения их текущей задачи.

Не рекомендуется использовать master-realm для управления пользователями и приложениями в организации. Оставьте использование master-realm для системных администраторов для создания и управления realm в системе. Такая модель безопасности помогает предотвратить случайные изменения и следует традиции предоставления учетным записям пользователей доступа только к тем привилегиям и полномочиям, которые необходимы для успешного выполнения их текущей задачи.

Можно отключить master-realm и определить учетные записи администраторов в каждом отдельном новом realm, который создается. Каждый realm имеет свою собственную консоль администратора, в которую можно войти с помощью локальных учетных записей.

Управление Realm осуществляется через вкладку “Настройки Realm”.

Создать новый realm очень просто. Необходимо навести курсор мыши на выпадающее меню в левом верхнем углу, которое озаглавлено Master. При аутентификации в master-realm, в этом выпадающем меню перечислены все созданные realm. Последним пунктом этого выпадающего меню всегда является Добавить новый realm. Нажмите на него, чтобы добавить realm. Этот пункт меню приведет на страницу Добавления realm. Укажите имя realm и нажмите кнопку Создать. В качестве альтернативы есть возможность импортировать документ JSON, определяющий новый realm. После создания realm происходит перенаправление на главную страницу консоли администратора. Текущий realm теперь будет установлен на realm, который был только что создан. Для переключения между управлением различными realm, наведите курсор мыши на выпадающее меню в левом верхнем углу.

Главная

Основные настройки Realm

На рисунке ниже изображена форма настройки параметров realm.

The screenshot shows the Keycloak configuration interface for a 'Test' realm. The left sidebar contains navigation links for Configuration, Realm Settings (selected), Clients, Client Templates, Roles, Identity Providers, Federation, and Authentication. Under 'realm' settings, there are tabs for General, Authentication, Keys, Themes, Cache, Tokens, Client Registration, Security, and Advanced. The General tab is active, displaying fields for Name (Test), Display name, Display name in HTML, Enabled (checkbox checked), User access (checkbox checked), and Endpoints (OpenID configuration and SAML 2.0 metadata). At the bottom are 'Save' and 'Cancel' buttons.

В таблице представлено детальное описание интерфейса настройки параметров realm.

Наименование настройки	Описание	Тип настройки	Рекомендованное значение
Имя	Системное имя Realm	Текстовая	На усмотрение администратора
Отображаемое название	Отображаемое имя Realm для пользователя	Текстовая	На усмотрение администратора
Отображаемое название в HTML	Отображаемое имя Realm в коде	Текстовая	На усмотрение администратора
Включено	Статус Realm. Пользователи и клиенты могут получить доступ к Realm только если он включен	Булевая	Включен, т.к. если Realm отключен, то все пользователи/клиента будут также отключены.
Пользовательский доступ	Если включено, пользователям можно будет управлять своими ресурсами и правами, используя консоль управления учетной записью	Булевая	Выключен
Конечные точки	При нажатии на один из протоколов позволяет просмотреть все endpoint в заданном формате. Показывает конфигурацию конечных точек протокола	Grid(список)	Отсутствует

Вход

Настройки аутентификации пользователей.

Каждый realm имеет режим SSL, связанный с ним. Режим SSL определяет требования SSL/HTTPS для взаимодействия с областью. Браузеры и приложения, взаимодействующие с областью, должны соблюдать требования SSL/HTTPS, определенные режимом SSL, иначе им не будет разрешено взаимодействовать с сервером.

На рисунке ниже изображена форма настройки параметров входа.

The screenshot shows the Keycloak configuration interface for a realm named 'Test'. The left sidebar has a dark theme with white text. The 'Entry' tab is selected. The main panel displays various configuration options with checkboxes:

- Самостоятельная регистрация пользователей**: Вкл (Enabled) - checked
- E-mail как имя пользователя**: Вык (Disabled) - unchecked
- Редактируемое имя пользователя**: Вык (Disabled) - unchecked
- Сброс пароля**: Вык (Disabled) - unchecked
- Запомнить меня**: Вык (Disabled) - unchecked
- Подтверждение E-mail**: Вык (Disabled) - unchecked
- Вход по E-mail**: Вык (Disabled) - unchecked
- Дублирующиеся E-mail**: Вык (Disabled) - unchecked
- Требует SSL**: все запросы (All requests) - dropdown menu set to 'all requests'

At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

В таблице представлено детальное описание интерфейса настройки параметров входа в realm.

Наименование настройки	Описание	Тип настройки	Рекомендованное значение
Самостоятельная регистрация пользователей	Включить/выключить страницу регистрации. Ссылка для регистрации будет также показана на странице входа.	Булевая	На усмотрение администратора
E-mail как имя пользователя	Если включено, то на форме регистрации поле имени пользователя будет скрыто и в качестве имени пользователя для новых пользователей будет использоваться E-mail.	Булевая	На усмотрение администратора
Редактируемое имя пользователя	Если включено, то имя пользователя можно будет отредактировать, иначе оно будет доступным только для чтения.	Булевая	На усмотрение администратора

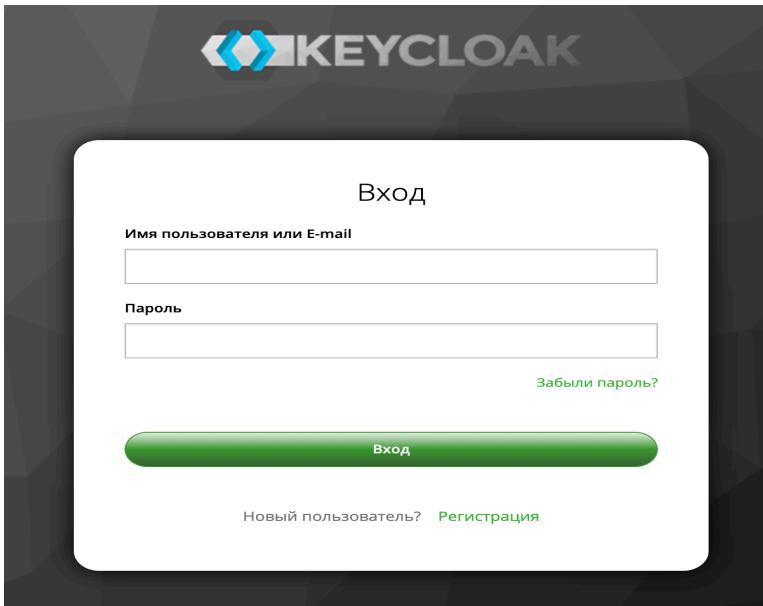
Наименование настройки	Описание	Тип настройки	Рекомендованное значение
Сброс пароля	Показывает ссылку на странице входа для пользователя, по переходу на которую пользователь сможет восстановить свои данные для входа.	Булевая	На усмотрение администратора
Запомнить меня	Показать чекбокс на странице входа, чтобы разрешить пользователю запомнить вход в учетную запись в случае если браузерная сессия устареет.	Булевая	На усмотрение администратора
Подтверждение E-mail	Требует у пользователя подтвердить свой E-mail при первом входе в учетную запись.	Булевая	На усмотрение администратора
Вход по E-mail	Позволяет включить функцию использования email вместо логина. При этом невозможна аутентификация с помощью логина.	Булевая	На усмотрение администратора
Дублирующиеся E-mail	Разрешает разным пользователям иметь один и тот же E-mail. Изменение этой настройки также очистит пользовательский кэш. После выключения поддержки дублирующихся email рекомендуется вручную почистить в базе данных ограничения по E-mail существующим пользователям.	Булевая	На усмотрение администратора
Требует SSL	Позволяет выбрать какие запросы необходимо защищать с помощью SSL.	Список с одним возможным вариантом значения	Все запросы

При включении функции “Сброс пароля”, пользователям будет доступно восстановление своих учетных данных для входа в систему (если пользователь забудет пароль или потеряет генератор OTP).

Процесс сброса пароля:

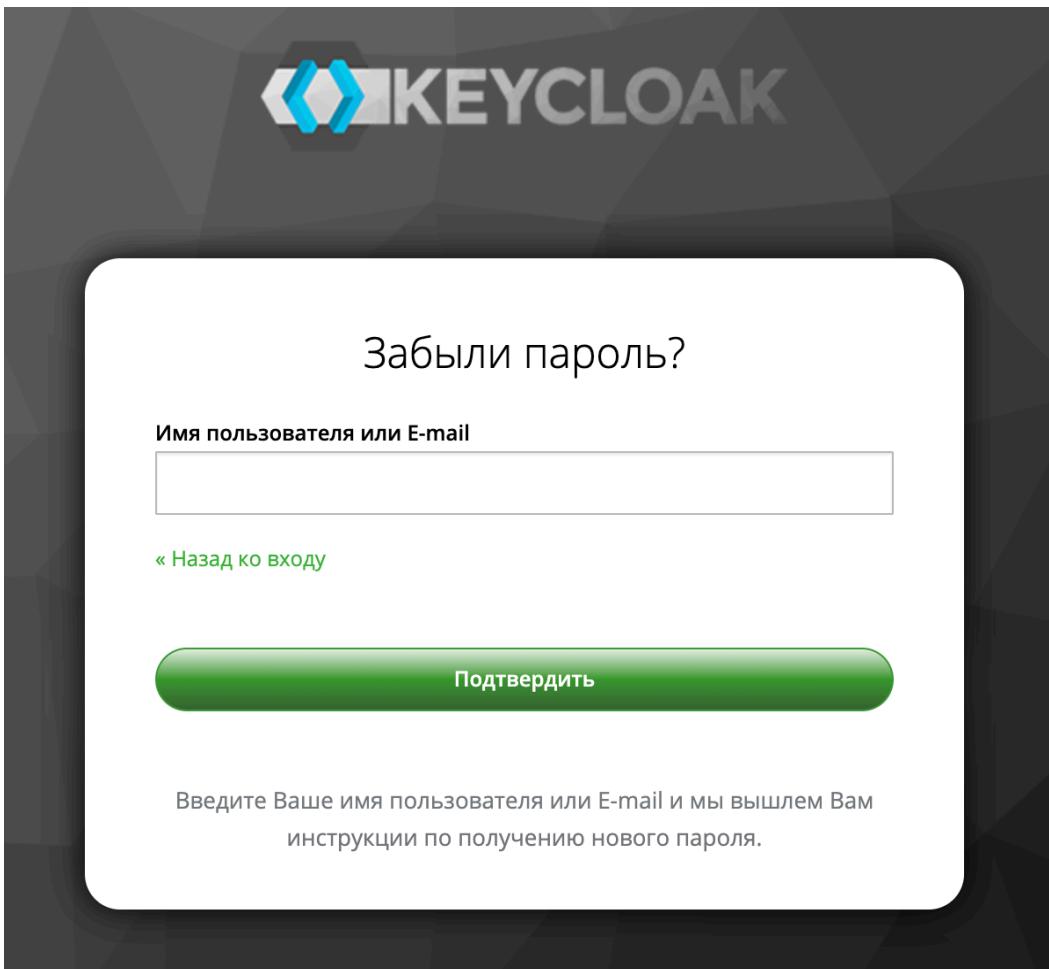
- Переключить “Сброс пароля” в настройках параметров входа realm в положение Включено.
- Ссылка на сброс пароля отображена на странице входа в систему.

На рисунке ниже изображена форма ввода логина.

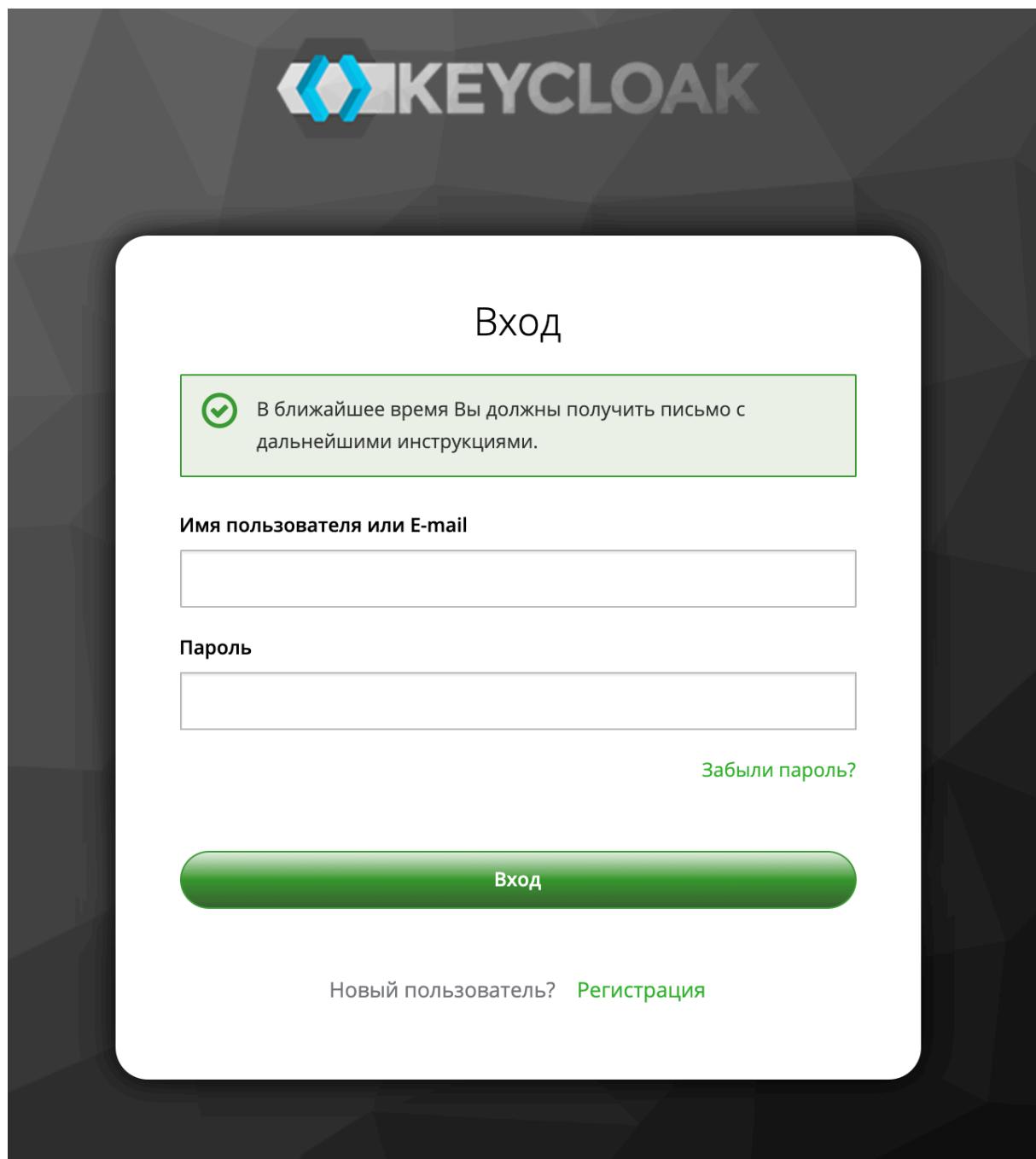


- Нажмите на эту ссылку, чтобы ввести имя пользователя или адрес электронной почты и получить электронное письмо со ссылкой для сброса своих учетных данных

На рисунке ниже изображена форма “Забыли пароль?”.



На рисунке ниже изображено окно аутентификации с информационным сообщением.



- Когда пользователи нажимают на ссылку электронной почты, Keycloak просит их обновить свой пароль, и если настроен генератор OTP, Keycloak просит их перенастроить генератор OTP. В зависимости от требований безопасности организации, возможность, чтобы пользователи сбрасывали свой генератор OTP по электронной почте, может быть ограничена.

Чтобы изменить это, требуется выполнить следующие действия:

- Выбрать пункт меню *Аутентификация*.

- Перейти на вкладку *Сценарии*.
- Выбрать сценарий сброса учетных данных.

На рисунке ниже изображено окно просмотра сценария аутентификации *Reset_credentials*.

The screenshot shows the Keycloak Platform interface with the 'Master' realm selected. The left sidebar has a 'Reset Credentials' section highlighted. The main content area is titled 'Аутентификация' (Authentication) and shows the 'Сценарии' (Scenarios) tab selected. Below it, there are tabs for 'Сопоставления' (Mappings), 'Требуемые действия' (Required Actions), 'Политики пароля' (Password Policies), 'Политики OTP' (OTP Policies), and 'WebAuthn политики' (WebAuthn Policies). A sub-tab 'Reset Credentials' is also visible. The central part of the screen displays a table for configuring the 'Reset Credentials' scenario. The table has two columns: 'Тип аутентификации' (Authentication Type) and 'Требования' (Requirements). The rows define requirements for various actions:

Тип аутентификации	Требования
Choose User	<input checked="" type="radio"/> REQUIRED
Send Reset Email	<input checked="" type="radio"/> REQUIRED
Reset Password	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED
Reset - Conditional OTP	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input checked="" type="radio"/> CONDITIONAL
Condition - User Configured	<input checked="" type="radio"/> REQUIRED <input type="radio"/> DISABLED
Reset OTP	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED

- Для отключения сброса OTP, необходимо установить для требования *Reset OTP* значение *Disabled*
- Перейти на вкладку *Требуемые действия*. Убедиться, что обновление пароля включено.

Ключи

Протоколы аутентификации требуют криптографических подписей и иногда шифрования. Для этого используются асимметричные пары ключей - Публичные и Приватные ключи.

Keycloak одновременно имеет одну активную пару ключей, но может иметь и несколько пассивных ключей. Активная пара ключей используется для создания новых подписей, а пассивные пары ключей могут использоваться для проверки предыдущих подписей. Это позволяет регулярно менять ключи без простоев и перерывов для пользователей.

При создании realm, автоматически генерируется пара ключей и самозаверяющий сертификат.

Обмен ключей

Рекомендуется регулярно менять ключи. Для этого рекомендуется начать с создания новых ключей с более высоким приоритетом, чем существующие активные ключи. Или создать новые ключи с тем же приоритетом, сделав предыдущие ключи пассивными.

После получения новых ключей все новые токены и файлы cookie будут подписываться новыми ключами. Когда пользователь аутентифицируется в приложении, cookie SSO обновляются новой подписью. При обновлении токенов OpenID Connect новые токены подписываются новыми ключами. Это означает, что со временем все cookie и токены будут использовать новые ключи, а через некоторое время старые ключи можно будет удалить.

Частота удаления старых ключей - это компромисс между безопасностью и уверенностью в том, что все файлы cookie и токены обновлены. Желательно создавать новые ключи каждые три-шесть месяцев и удалять старые ключи через один-два месяца после создания новых. Если пользователь был неактивен в период между добавлением новых и удалением старых ключей, ему придется пройти повторную аутентификацию.

Ротация ключей также применяется к автономным токенам. Чтобы убедиться, что они обновлены, приложения должны обновить токены перед удалением старых ключей.

Активные

Активные

Ниже изображено окно просмотра активных ключей шифрования.

Active encryption keys						
Search...	Algorithm	Type	KID	Priority	Provider	Public keys
	RSA	OCT	PIHBFZr4js2Q_lqxq5-ceArar_W869Y6PgFExO9Ee4o	100	rsa-generated	Public key certificate
	AES	OCT	65f7fb27-779e-4af7-9114-989cdf494ecf	100	aes-generated	
	HS256	OCT	1a792ecf-d0fe-4911-a69f-96781425d2ca	100	hmac-generated	

В таблице представлено детальное описание интерфейса просмотра активных ключей шифрования.

Наименование настройки	Описание	Тип настройки
Алгоритм	Алгоритм шифрования ключа	Текстовое значение
Тип	Тип алгоритма	Текстовое значение
Kid	Ключ	Текстовое значение
Приоритет	Приоритетность ключа (зависит от провайдера)	Текстовое значение
Поставщик	Провайдер, выпустивший ключ.	Текстовое значение
Публичные ключи	Возможность посмотреть публичные ключи, принадлежащие конкретному ключу шифрования (при наличии).	Кнопки просмотра
Поиск	Поле для поиска	Поле для поиска

Пассивные

Пассивные

Ниже изображено окно просмотра пассивных ключей шифрования.

Поиск...	Q						
Алгоритм	Тип	KID	Приоритет	Поставщик	Публичные ключи		
RS256	RSA	PiHBFZr4js2Q_lqxq5-ceArar_W869Y6PgFExO9Ee4o	100	rsa-generated	Публичный ключ	Сертификат	
AES	OCT	65f7fb27-779e-4af7-9114-989cdf494ecf	100	aes-generated			
HS256	OCT	1a792ecf-d0fe-4911-a69f-96781425d2ca	100	hmac-generated			

В таблице представлено детальное описание интерфейса просмотра пассивных ключей шифрования.

Наименование настройки	Описание	Тип настройки
Алгоритм	Алгоритм шифрования ключа	Текстовое значение
Тип	Тип алгоритма	Текстовое значение
Kid	Ключ	Текстовое значение
Приоритет	Приоритетность ключа (зависит от провайдера)	Текстовое значение
Поставщик	Провайдер, выпустивший ключ.	Текстовое значение
Публичные ключи	Возможность посмотреть публичные ключи, принадлежащие конкретному ключу шифрования (при наличии).	Кнопки просмотра
Поиск	Поле для поиска	Поле для поиска

Отключенные

Deактивированные. Ниже изображено окно просмотра отключенных ключей шифрования.

Поиск...	Q						
Алгоритм	Тип	KID	Приоритет	Поставщик	Публичные ключи		
RS256	RSA	PiHBFZr4js2Q_lqxq5-ceArar_W869Y6PgFExO9Ee4o	100	rsa-generated	Публичный ключ	Сертификат	
AES	OCT	65f7fb27-779e-4af7-9114-989cdf494ecf	100	aes-generated			
HS256	OCT	1a792ecf-d0fe-4911-a69f-96781425d2ca	100	hmac-generated			

В таблице представлено детальное описание интерфейса просмотра отключенных ключей шифрования.

Наименование настройки	Описание	Тип настройки
Алгоритм	Алгоритм шифрования ключа	Текстовое значение
Тип	Тип алгоритма	Текстовое значение
Kid	Ключ	Текстовое значение
Приоритет	Приоритетность ключа (зависит от провайдера)	Текстовое значение
Поставщик	Провайдер, выпустивший ключ.	Текстовое значение
Публичные ключи	Возможность посмотреть публичные ключи, принадлежащие конкретному ключу шифрования (при наличии).	Кнопки просмотра
Поиск	Поле для поиска	Поле для поиска

Поставщики

Провайдеры ключей шифрования.

Окно просмотра провайдеров

Ниже изображено окно просмотра провайдеров ключей шифрования.

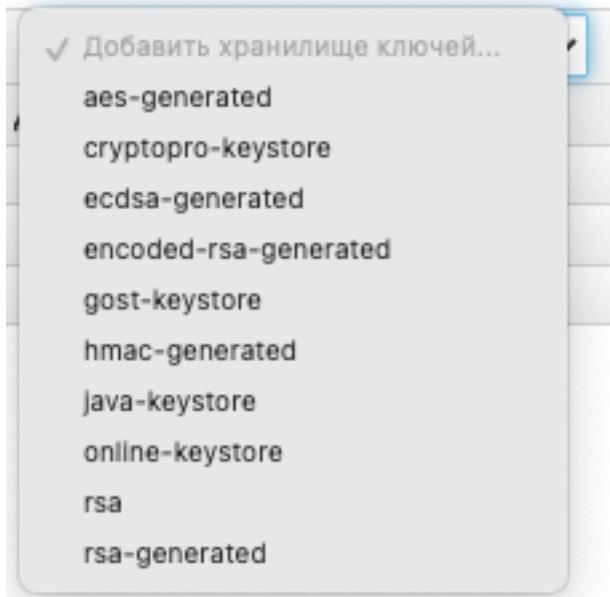
The screenshot shows a user interface for managing providers. At the top, there is a navigation bar with tabs: Главная, Вход, Ключи (selected), Е-майл, Темы, Кэш, Токены, Регистрация клиента, Защита безопасности, and Дополнительно. Below the navigation bar, there are sub-tabs: Активные, Пассивные, Отключенные, and Поставщики (selected). A search bar with a placeholder 'Поиск...' and a magnifying glass icon is located above the provider list. The provider list table has columns: Имя (Name), Поставщик (Provider), Описание поставщика (Provider description), Приоритет (Priority), and Действия (Actions). The table contains three rows:

Имя	Поставщик	Описание поставщика	Приоритет	Действия
hmac-generated	hmac-generated	Generates HMAC secret key	100	Просмотр Удалить
aes-generated	aes-generated	Generates AES secret key	100	Просмотр Удалить
rsa-generated	rsa-generated	Generates RSA keys and creates a self-signed certificate	100	Просмотр Удалить

A button 'Добавить хранилище ключей...' (Add key store...) is visible at the top right of the table area.

В таблице представлено детальное описание интерфейса просмотра провайдеров ключей шифрования.

Наименование настройки		Описание	Тип настройки
Имя		Системное наименование провайдера	Текстовое значение
Поставщик		Общее наименование провайдера	Текстовое значение
Описание поставщика		Описание провайдера	Текстовое значение
Приоритет		Приоритетность	Числовое значение
Поиск		Поле для поиска	Поле для поиска
Действия		Возможные действия с провайдером	Кнопки с возможностью нажатия
	Просмотр	Окно редактирования провайдера	Кнопка
	Удалить	Удалить поставщика	Кнопка
Добавить хранилище ключей		Позволяет добавить провайдера ключей шифрования	Список с возможными значениями



aes-generated

Ниже изображено окно добавления поставщика хранилища ключей **aes-generated**

Наименование в консоли	aes-generated
Priority	0
Enabled	<input checked="" type="checkbox"/>
Active	<input checked="" type="checkbox"/>
AES Key size	16
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **aes-generated**.

Наименование настройки	Тип настройки
Наименование в консоли	Текстовое значение
Priority	Числовое значение
Enabled	Булевая
Active	Булевая

Наименование настройки		Тип настройки
AES Key size	Размер в байтах для сгенерированного AES Key. Size 16 для AES-128, Size 24 для AES-192 и Size 32 для AES-256. ПРЕДУПРЕЖДЕНИЕ: в некоторых реализациях JDK не допускаются ключи размером более 128 бит.	Выпадающий список

cryptopro-keystore

Ниже изображено окно добавления поставщика хранилища ключей **cryptopro-keystore**

The screenshot shows the 'Postavshiki' (Providers) tab selected in the navigation bar. Below it, the 'Добавить хранилище ключей' (Add Keystore Repository) button is visible. The configuration form contains the following fields:

- Наименование в консоли: cryptopro-keystore
- Priority: 0
- Enabled: Вкл (Enabled)
- Active: Вкл (Enabled)
- Alias: admin
- Keystore Password: (redacted)

At the bottom are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **cryptopro-keystore**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Alias	Синоним (ID) keystore	Текстовое значение
Keystore Password	Пароль для keystore	Текстовое значение

ecdsa-generated

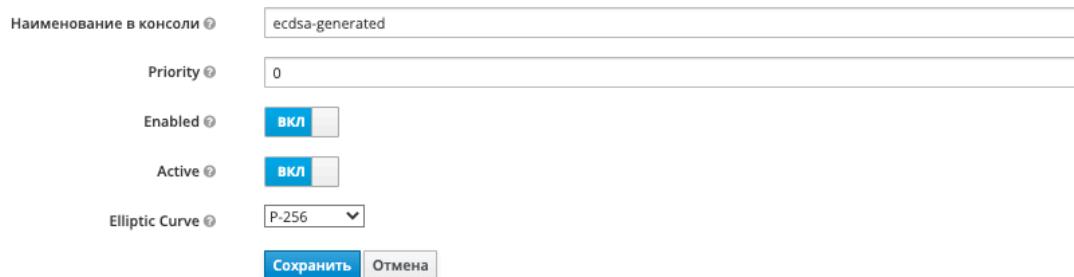
Ниже изображено окно добавления поставщика хранилища ключей **ecdsa-generated**

Test 

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Активные Пассивные Отключенные **Поставщики**

[Хранилища ключей](#) > Добавить хранилище ключей



Наименование в консоли

Priority

Enabled

Active

Elliptic Curve

Сохранить **Отмена**

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **ecdsa-generated**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Elliptic Curve	Эллиптическая кривая, используемая в ECDSA	Выпадающий список

encoded-rsa-generated

Ниже изображено окно добавления поставщика хранилища ключей **encoded-rsa-generated**

Test 

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Активные Пассивные Отключенные **Поставщики**

[Хранилища ключей](#) > Добавить хранилище ключей



Наименование в консоли

Priority

Enabled

Active

Algorithm

Key size

Сохранить **Отмена**

*В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **encoded-rsa-generated**.*

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Algorithm	Предполагаемый алгоритм для ключа	Выпадающий список
Key size	Размер для сгенерированных ключей	Выпадающий список

gost-keystore

Ниже изображено окно добавления поставщика хранилища ключей **gost-keystore**

The screenshot shows the 'Add Key Store Provider' dialog for the 'gost-keystore' provider. The provider name is 'gost-keystore'. The priority is set to 0. Both 'Enabled' and 'Active' checkboxes are checked. The sign algorithm is set to 'ГОСТ Р 34.10-2012 (256)'. The keystore path is 'admin', the type is 'PKCS12', and the password is '.....'. There are fields for 'Key Alias', 'Key Password', and 'Verify public key Alias', all of which are currently empty. At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

*В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **gost-keystore**.*

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
SignAlgorithm	Предполагаемый алгоритм для ключа	Выпадающий список
Keystore path	Путь к хранилищу ключей	Текстовое значение
Keystore type	Тип хранилища ключей	Выпадающий список
Keystore Password	Пароль для хранилища ключей	Текстовое значение
Key Alias	Псевдоним для закрытого ключа	Текстовое значение
Key Password	Пароль для ключа	Текстовое значение
Verify public key Alias	Псевдоним для подтвержденного публичного ключа	Текстовое значение

hmac-generated

Ниже изображено окно добавления поставщика хранилища ключей **hmac-generated**

The screenshot shows the 'Postavshiki' (Providers) section of the Keycloak admin interface. The 'hmac-generated' provider is selected for configuration. The configuration fields are as follows:

- Наименование в консоли: hmac-generated
- Priority: 0
- Enabled: ВКЛ (Enabled)
- Active: ВКЛ (Enabled)
- Secret size: 64
- Algorithm: HS256

At the bottom are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **hmac-generated**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение

Наименование настройки	Описание	Тип настройки
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Secret size	Размер в байтах для сгенерированного секрета	Выпадающий список
Algorithm	Предполагаемый алгоритм для ключа	Выпадающий список

java-keystore

Ниже изображено окно добавления поставщика хранилища ключей **java-keystore**

The screenshot shows the 'Postavщики' (Providers) tab selected in the navigation bar. Below it, the 'Хранилища ключей' (Key Stores) section is active. The main form is for adding a new provider:

- Наименование в консоли:** java-keystore
- Priority:** 0
- Enabled:** ВКЛ (Enabled)
- Active:** ВКЛ (Enabled)
- Algorithm:** RS256
- Keystore:** (empty input field)
- Keystore Password:** (empty input field)
- Key Alias:** (empty input field)
- Key Password:** (empty input field)

At the bottom are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **java-keystore**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая

Наименование настройки	Описание	Тип настройки
Algorithm	Предполагаемый алгоритм для ключа	Выпадающий список
Keystore	Путь к файлу ключей	Текстовое значение
Keystore Password	Пароль для ключей	Текстовое значение
Key Alias	Псевдоним для закрытого ключа	Текстовое значение
Key Password	Пароль для закрытого ключа	Текстовое значение

online-keystore

Ниже изображено окно добавления поставщика хранилища ключей **online-keystore**

The screenshot shows the 'Postavyshchi' (Providers) tab selected in the navigation bar. Below it, the 'Hraniashchi kljuchey' (Key Stores) section is active. The main area displays a form for adding a new provider:

- Naimevovanie v konsole**: online-keystore
- Priority**: 0
- Enabled**: Вкл (Enabled)
- Active**: Вкл (Enabled)
- Sign url**: (empty input field)
- Verify url**: (empty input field)
- Raw verify type**: Вык (Disabled)
- Key Alias**: (empty input field)
- Verify public key Alias**: (empty input field)
- ESIA certificate**: (empty input field)

At the bottom are two buttons: **Сохранить** (Save) and **Отмена** (Cancel).

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **online-keystore**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая

Наименование настройки	Описание	Тип настройки
Sign url	Url-адрес входа в службу DIGS. Например, http://sign-service.mycompany.ru/ufs-sign-application/v1/sign/cms/tech	Текстовое значение
Verify url	Проверьте URL-адрес службы DIGS. Например, http://sign-service.mycompany.ru/ufs-sign-application/v1/checkSign/cms	Текстовое значение
Raw verify type	Флаг для RAW типа проверки. Если флаг включен, URL-адрес проверки должен указывать на RAW URL-адрес проверки (например, http://sign-service.mycompany.ru/ufs-sign-application/v1/checkSign/raw)	Булевая
Key Alias	Псевдоним для закрытого ключа	Текстовое значение
Verify public key Alias	Псевдоним для открытого ключа	Текстовое значение
ESIA certificate	X.509 (PEM) ESIA сертификат отправляет в DIGS запрос. Например, MIIMTCCB96gAwIBAgIQY8WCANar...	Текстовое значение

rsa

Ниже изображено окно добавления поставщика хранилища ключей **rsa**

The screenshot shows the 'Добавить хранилище ключей' (Add Key Repository) dialog for the RSA provider. The tabs at the top are 'Активные' (Active), 'Пассивные' (Passive), 'Отключенные' (Disabled), and 'Поставщики' (Suppliers), with 'Поставщики' being the active tab. Below the tabs, the breadcrumb navigation shows 'Хранилища ключей > Добавить хранилище ключей'. The form fields include:

- Наименование в консоли**: rsa
- Priority**: 0
- Enabled**: Вкл (Enabled)
- Active**: Вкл (Enabled)
- Algorithm**: RS256
- Private RSA Key**: A file input field with the placeholder 'Выберите файл' (Select file).
- X509 Certificate**: A file input field with the placeholder 'Выберите файл' (Select file).

At the bottom are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **rsa**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение

Наименование настройки	Описание	Тип настройки
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Algorithm	Предполагаемый алгоритм для ключа	Выпадающий список
Private RSA Key	Закрытый ключ RSA, закодированный в формате PEM	Текстовое значение
X509 Certificate	X509 Сертификат, закодированный в формате PEM	Текстовое значение

rsa-generated

Ниже изображено окно добавления поставщика хранилища ключей **rsa-generated**

The screenshot shows the 'Postavshiki' (Providers) tab selected in the navigation bar. Below it, the 'Хранилища ключей' (Key Stores) section is active. A new provider is being created with the following settings:

- Наименование в консоли: rsa-generated
- Priority: 0
- Enabled: ВКЛ (Enabled)
- Active: ВКЛ (Enabled)
- Algorithm: RS256
- Key size: 2048

At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

В таблице представлено детальное описание интерфейса настройки поставщика хранилища ключей **rsa-generated**.

Наименование настройки	Описание	Тип настройки
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Priority	Приоритет для поставщика	Числовое значение
Enabled	Установить флаг если ключ включен	Булевая
Active	Установить, можно ли использовать ключи для подписи	Булевая
Algorithm	Предполагаемый алгоритм для ключа	Выпадающий список
Key size	Размер для сгенерированного ключа	Выпадающий список

Email

Настройки отправки email - писем от имени Keycloak.SE.

Keycloak отправляет электронные письма пользователям для проверки их адреса электронной почты, когда пользователи забывают свои пароли или когда администратору необходимо получать уведомления о событии на сервере. Чтобы разрешить Keycloak отправлять электронные письма, необходимо предоставить Keycloak настройки SMTP-сервера. Это настраивается для каждого realm. Для настройки необходимо перейти в пункт меню “Настройки realm” слева и далее на вкладку “Email”.

Ниже изображено окно настройки SMTP соединения.

В таблице представлено детальное описание интерфейса настройки SMTP соединения.

Наименование настройки	Описание	Тип настройки	Рекомендованное значение
Сервер	Хост SMTP протокола	Текстовая	
Порт	Порт SMTP протокола	Текстовая	Если не заполнен, то выставляется автоматически 25
От (имя на экране)	Понятное пользователю имя в поле “От” в письме	Текстовая	
От	E-mail отправителя	Текстовая	

Наименование настройки	Описание	Тип настройки	Рекомендованное значение
Ответить на (имя на экране)	Отображаемое имя при ответе на письмо. Позволяет настроить удобные для пользователя псевдонимы адресов электронной почты (необязательно). Если не задать обычный адрес электронной почты, он будет отображаться в почтовых клиентах.	Текстовая	
Ответить на	E-mail при ответе письма. Обозначает адрес, используемый для SMTP-заголовка ответа на отправленные письма (необязательно). Если не задано, будет использоваться обычный адрес электронной почты	Текстовая	
Письмо от. Обозначает адрес возврата, используемый для SMTP-заголовка обратного пути для отправленных писем (необязательно).	Адрес электронной почты для сообщений	Текстовая	
Включить SSL	Функция включения SSL	Булевая	
Включить StartTLS	Функция включения StartTLS	Булевая	
Включить аутентификацию	Функция включения аутентификации при отправке email	Булевая	

Поскольку электронные письма используются для восстановления имен пользователей и паролей, рекомендуется использовать SSL или TLS, особенно если SMTP-сервер находится во внешней сети. Чтобы включить SSL, требуется нажать Включить SSL или включить TLS (рекомендуется нажать Включить TLS). Скорее всего, также потребуется изменить порт (порт по умолчанию для SSL/TLS - 465).

Если SMTP-сервер требует аутентификации, то нажать Включить аутентификацию и ввести имя пользователя и пароль. Значение поля Пароля может ссылаться на значение из внешнего хранилища.

Темы

Стиль форм KeyCloak.SE

Темы позволяют изменить внешний вид и ощущение любого пользовательского интерфейса в KeyCloak.SE. Темы настраиваются для каждого realm.

Ниже изображено окно настройки стиля форм KeyCloak.SE.

В таблице представлено детальное описание интерфейса настройки стиля форм Keycloak.SE.

Наименование настройки	Описание	Тип настройки
Тема страницы входа	Выбрать тему для страниц входа, временного одноразового пароля (OTP), выдачи разрешений, регистрации и восстановления пароля.	Список с возможностью выбора
Тема учетной записи	Выбрать тему для управления учетной записью пользователя.	Список с возможностью выбора
Тема консоли администратора	Выбрать тему для консоли администратора.	Список с возможностью выбора
Тема для E-mail	Выбрать тему для E-mail, которые будут отсылаться с сервера.	Список с возможностью выбора
Интернационализация	Включение функции поддержки различных локализаций	Булевая
Поддерживаемые языки	Список поддерживаемых локализаций	Список значений
Язык по умолчанию	Базовая локализация (запускающаяся автоматически)	Список с возможностью выбора

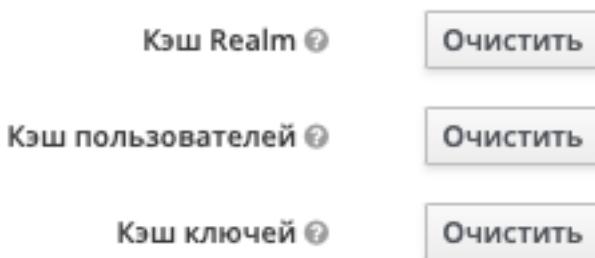
Каждый экран пользовательского интерфейса интернационализирован в Keycloak. Язык по умолчанию - английский, но если включить переключатель интернационализации на вкладке Тема, это позволит выбрать, какие языки требуется поддерживать и какой будет язык по умолчанию. В следующий раз, когда пользователь войдет в систему, он сможет выбрать язык на странице входа, который будет использоваться для экранов входа,

пользовательского интерфейса управления учетными записями пользователей и Консоли администратора.

Кэш

KeyCloak.SE кэширует в памяти все, что может, в пределах возможностей JVM и/или ограничений, на которые настроено. Если база данных KeyCloak.SE изменяется третьей стороной (например, DBA) вне рамок REST API или консоли администратора сервера, есть вероятность, что часть кэша в памяти может оказаться неактуальной.

Ниже изображено окно очистки кэша.



В таблице представлено детальное описание интерфейса очистки кэша.

Наименование настройки	Описание	Тип настройки
Кэш Realm	Очистка кэша Realm	Кнопка
Кэш пользователей	Очистка кэша пользователей	Кнопка
Кэш ключей	Очистка кэша ключей шифрования	Кнопка

Токены

Настройки формирования токена.

Keycloak включает управление тайм-аутами сессии, cookie и токенов через вкладку Токены в меню Настройки Realm.

Ниже изображен интерфейс настройки формирования токена.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

The screenshot shows the 'Tokens' configuration page in the Keycloak administration interface. The 'Tokens' tab is selected. The configuration includes:

- Стандартный алгоритм подписи:** RS256
- Одноразовые токены обновления:** Вкл.
- Максимальное повторное использование токена обновления:** 0
- Таймаут сессии SSO:** 30 минут
- Ограничение сессии SSO:** 10 часов
- Таймаут сессии SSO Remember Me:** 0 минут
- Ограничение сессии SSO Remember Me:** 0 минут
- Таймаут оффлайн сессии:** 30 дней
- Ограничение на оффлайн сессии:** Выкл.
- Время простоя клиентской сессии:** 0 минут
- Время жизни клиентской сессии:** 0 минут
- Продолжительность жизни токена доступа:** 1 минут
- Продолжительность жизни токена доступа для Implicit Flow:** 15 минут
- Таймаут авторизации клиента:** 1 минут
- Таймаут входа:** 30 минут
- Таймаут действий по входу:** 5 минут
- Время жизни пользовательского действия:** 5 минут
- Время жизни (по-умолчанию) действия администратора:** 12 часов
- Время жизни URI для запроса авторизации:** 1 минут
- Переопределить время жизни пользовательского действия:** Выберите... минут Сбросить
- OAuth 2.0 Срок службы кода устройства:** 10 минут
- OAuth 2.0 Интервал опроса:** 5

At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

В таблице представлено детальное описание интерфейса настройки формирования токена.

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
Стандартный алгоритм подписи	Стандартный алгоритм, используемый для подписи токенов реалма	Список с возможностью выбора	
Одноразовые токены обновления	Если включено, то токены обновления могут быть использованы один раз. Иначе токен отзыбаться не будет и может использоваться многократно.	Булевая	Включено
Максимальное повторное использование токена обновления	Максимальное количество раз токен обновления может быть использован повторно. Когда используется другой токен, отзыв происходит немедленно.	Числовое значение	0
Тайм-аут сессии SSO	Допустимое время бездействия сессии. По истечении этого времени токены и браузерные сессии становятся невалидными.	Число в минутах/часах/днях	15 минут

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
Ограничение сессии SSO	Максимальное время до того, как истечет сессия. По истечении этого времени токены и браузерные сессии становятся невалидными.	Число в минутах/часах/днях	
Тайм-аут сессии SSO Remember Me	Допустимое время бездействия сессии Remember Me. По истечении этого времени токены и браузерные сессии становятся невалидными. Если не установлено, используется значение тайм-аута стандартной сессии SSO	Число в минутах/часах/днях	
Ограничение сессии SSO Remember Me	Максимальное время до того, как истечет сессия с опцией Remember me. По истечении этого времени токены и браузерные сессии становятся невалидными. Если не установлено, используется значение ограничения стандартной сессии SSO	Число в минутах/часах/днях	
Тайм-аут оффлайн сессии	Допустимое время бездействия оффлайн сессии. Вам необходимо использовать оффлайн токен для обновления хотя бы раз за этот период, иначе сессия истечет.	Число в минутах/часах/днях	
Ограничение на оффлайн сессии	Функция позволяет включить ограничение максимального времени “жизни” сессии в автономном доступе.	Булевая	
Время простоя клиентской сессии	Время, в течение которого клиентской сессии разрешен простой до истечения срока ее действия. Токены становятся недействительными по истечении срока действия клиентской сессии. Если не задано, то используется стандартное SSO значение простоя сессии	Число в минутах/часах/днях	0
Время жизни клиентской сессии	Время жизни до истечения клиентской сессии. Токены становятся недействительными по истечении срока действия клиентской сессии. Если не задано, то используется стандартное SSO максимальное значение сессии.	Число в минутах/часах/днях	0
Продолжительность жизни токена доступа	Максимальное время действия токена доступа. Значение рекомендуется устанавливать как можно ближе к тайм-ауту SSO.	Число в минутах/часах/днях	5 минут
Продолжительность жизни токена доступа для Implicit Flow	Максимальное время действия токена доступа после того как сессия токена OpenID Connect Implicit Flow истекла. Это значение рекомендуется установить как можно ближе к тайм-ауту SSO. Нет возможности обновить токен во время Implicit Flow, поэтому этот тайм-аут отличается от ‘Продолжительности жизни токена доступа’	Число в минутах/часах/днях	15 минут

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
Тайм-аут авторизации клиента	Максимальное время клиента для завершения протокола access token. Обычно устанавливается равным 1-ой минуте.	Число в минутах/часах/днях	
Тайм-аут входа	Тайм-аут входа.	Число в минутах/часах/днях	5 минут
Тайм-аут действий по входу	Максимальное время, за которое пользователь должен выполнить и завершить действие после входа. Например, обновление пароля или конфигурация одноразового временного пароля.	Число в минутах/часах/днях	5 минут и более
Время жизни пользовательского действия	Максимальное время до того, как действие, отправленное пользователем (например, забыл пароль от почты), истекает. Рекомендуется устанавливать это значение небольшим, потому что ожидается, что пользователь отреагирует на собственное событие быстро.	Число в минутах/часах/днях	5 минут
Время жизни (по умолчанию) действия администратора	Максимальное время до того, как действие, отправленное пользователю администратором, истекает. Рекомендуется устанавливать это значение большим, чтобы позволить администраторам отправлять email'ы пользователям, которые находятся в офлайне. Тайм-аут по умолчанию может быть предопределен прямо перед выдачей токена	Число в минутах/часах/днях	
Время жизни URI для запроса авторизации	Число, представляющее время жизни URI запроса в минутах или часах, значение по умолчанию равно 1 минуте.	Число в минутах/часах/днях	1 минута
Переопределить время жизни пользовательского действия	Переопределить максимальное время (по умолчанию) до того, как действие отправленное пользователем (например, забыл пароль от почты), истечет для определенного действия. Рекомендуется устанавливать значение небольшим, потому что ожидается, что пользователь отреагирует на собственное событие быстро.	Число в минутах/часах/днях	
OAuth 2.0 Срок службы кода устройств	Максимальное время до истечения срока действия кода устройства и пользовательского кода. Это значение должно быть достаточно длительным, чтобы его можно было использовать (позволяя пользователю извлекать свое вторичное устройство, переходить по ссылке для верификации данных, входить в систему и т.д.), Но должно быть достаточно коротким, чтобы ограничить удобство использования кода, полученного для фишинга.	Число в минутах/часах/днях	10 минут

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
OAuth 2.0 Интервал опроса	Минимальное количество времени в секундах, которое клиент должен ожидать между запросами к endpoint токена.	Число	5

Для тайм-аутов простоя существует двухминутный промежуток времени, в течение которого сеанс активен. Например, если установлено время ожидания 30 минут, то до истечения сеанса пройдет 32 минуты.

Это действие необходимо для некоторых сценариев в средах кластеров и центров обработки данных, где токен обновляется на одном узле кластера незадолго до истечения срока действия, а другие узлы кластера ошибочно считают сеанс истекшим, поскольку они еще не получили сообщение об успешном обновлении от обновляющего узла.

Регистрация клиента

Токены первичного доступа

Позволяет создавать инициализирующие общие токены доступа для клиентов (с определенным сроком жизни). Ниже изображено окно представления токенов первичного доступа.

The screenshot shows a navigation bar with links: Главная, Вход, Ключи, E-mail, Темы, Кэш, Токены, Регистрация клиента (highlighted in blue), Защита безопасности, and Дополнительно. Below the navigation bar is a sub-navigation bar with links: Токены первичного доступа (highlighted in blue) and Политики регистрации клиента. The main content area displays a table titled 'Токены первичного доступа'. The table has columns: ID, Создано, Истекает, Счетчик, Счетчик остатка, and Действия. A search bar is located at the top left of the table. A 'Создать' button is located at the top right of the table. An example row in the table is shown: ID - 225d0e2e-4756-4f30-b9be-0feb41e77d3f, Создано - 10.11.2021 14:56:12, Истекает - (empty), Счетчик - 1, Счетчик остатка - 1, Действия - Удалить.

В таблице представлено детальное описание интерфейса представления токенов первичного доступа.

Наименование настройки	Описание	Тип настройки
ID	Идентификатор токена	Текстовое значение
Создано	Дата и время создания токена	Текстовое значение
Истекает	Дата истечения срока действия токена	Текстовое значение
Счетчик	Счетчик клиентов, которых можно создать с помощью этого токена	Текстовое значение
Счетчик остатка	Счетчик остатка клиентов, которых можно создать с помощью этого токена	Текстовое значение
Действия	Кнопка действия: Удалить - удаляет выбранный токен первичного доступа	Кнопка
Создать	Кнопка для создания токена первичного доступа	Кнопка

Создать токен первичного доступа

Ниже изображено окно добавления токена первичного доступа.

Токены первичного доступа > Добавить токен первичного доступа

Истечениe	<input type="text" value="0"/> дней
Счетчик	<input type="text" value="1"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса добавления токена первичного доступа.

Наименование настройки	Описание	Тип настройки
Истечениe	Определяет, как долго токен будет оставаться валидным	Число в секундах/минутах/часах/днях
Счетчик	Определяет, как много клиентов может быть создано с помощью этого токена	Текстовое значение

Политики регистрации клиента

Политики анонимного доступа.

Эти политики будут использоваться, когда сервис регистрации клиента вызывается неаутентифицированным запросом. Это означает, что запрос не содержит ни токена первичного доступа ни Bearer токена.

Политики аутентифицированного доступа.

Эти политики будут использоваться, когда сервис регистрации клиента вызывается аутентифицированным запросом. Это означает, что запрос содержит токен первичного доступа или Bearer токен.

Ниже изображено окно представления политик регистрации клиента.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Токены первичного доступа Политики регистрации клиента

Политики анонимного доступа

Добавить поставщика...			
Наименование политики	ID службы	Действия	
Trusted Hosts	trusted-hosts	Редактировать	Удалить
Allowed Client Scopes	allowed-client-templates	Редактировать	Удалить
Max Clients Limit	max-clients	Редактировать	Удалить
Allowed Protocol Mapper Types	allowed-protocol-mappers	Редактировать	Удалить
Full Scope Disabled	scope	Редактировать	Удалить
Consent Required	consent-required	Редактировать	Удалить

Политики аутентифицированного доступа

Добавить поставщика...			
Наименование политики	ID службы	Действия	
Allowed Protocol Mapper Types	allowed-protocol-mappers	Редактировать	Удалить
Allowed Client Scopes	allowed-client-templates	Редактировать	Удалить

В таблице представлено детальное описание интерфейса политик регистрации клиента.

Наименование настройки		Описание	Тип настройки
Наименование политики		Наименование политики	Число в секундах/минутах/часах/днях
ID службы		ID службы	Текстовое значение
Действия		Возможные действия по управлению политиками анонимного/аутентифицированного доступа	Кнопки
	Редактировать	Редактировать	Кнопка
	Удалить	Удалить	Кнопка
Добавить поставщика			Выпадающий список

Добавить поставщика

allowed-client-templates

Когда включен, то позволяет указать разрешенный список клиентских областей, которые будут доступны в представлении зарегистрированного (или обновленного) клиента.

Ниже изображено окно настройки политики регистрации клиента **allowed-client-templates**.

Разрешить шаблоны клиента 

Имя  	<input type="text"/>
Поставщик 	<input type="text" value="allowed-client-templates"/>
Разрешенные клиентские области 	<input type="button" value="selectMultiple..."/>
Области, разрешенные по умолчанию 	<input type="button" value="ВЫК"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки политики регистрации клиента *allowed-client-templates*.

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	Когда включен, то позволяет указать разрешенный список клиентских областей, которые будут доступны в представлении зарегистрированного (или обновленного) клиента. По умолчанию: allowed-client-templates По умолчанию: allowed-client-templates	Текстовое значение
Разрешенные клиентские области	Разрешенный список клиентских областей, которые могут быть использованы зарегистрированными новыми клиентами. Попытка зарегистрировать клиента с некоторыми клиентскими областями, которые отсутствуют в разрешенном списке, будет отклонена. По умолчанию, разрешенный список либо пуст или содержит лишь стандартные клиентские области (основанные на свойстве "Области, разрешенные по умолчанию")	Выпадающий список с возможностью выбора нескольких значений
Области, разрешенные по умолчанию	Если включено, то новым клиентам будет позволено клиентские области, упомянутые как клиентские области реалма по умолчанию, или optionalные клиентские области реалма.	Булевая

client-disabled

Если политика присутствует, то вновь зарегистрированный клиент будет отключен, и администратору необходимо вручную его включить.

Ниже изображено окно настройки политики регистрации клиента **client-disabled**.

Client Disabled ?

Имя *	<input type="text"/>
Поставщик	client-disabled
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **client-disabled**.

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	Если политика присутствует, то вновь зарегистрированный клиент будет отключен, и администратору необходимо вручную включить). По умолчанию: client-disabled По умолчанию: client-disabled	Текстовое значение

scope

Если присутствует, то у вновь зарегистрированного клиента не будет разрешена полная область действия. Ниже изображено окно настройки политики регистрации клиента **scope**.

Scope ?

Имя *	<input type="text"/>
Поставщик	scope
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **scope**.

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	Если присутствует, то у вновь зарегистрированного клиента не будет разрешена полная область действия. По умолчанию: scope По умолчанию: scope	Текстовое значение

max-clients

Не позволяет регистрировать клиентов больше установленного предельного значения.

Ниже изображено окно настройки политики регистрации клиента **max-clients**.

[Политики регистрации клиента](#) > Максимальное количество клиентов для Realm

Максимальное количество клиентов для Realm

Имя *	<input type="text"/>
Поставщик	<input type="text" value="max-clients"/>
Максимальное количество клиентов для Realm	<input type="text" value="200"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **max-clients**.

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	Не позволяет регистрировать клиентов больше установленного предельного значения. По умолчанию: max-clients По умолчанию: max-clients	Текстовое значение
Максимальное количество клиентов для Realm	Не позволяет регистрировать клиентов больше установленного предельного значения.	Числовое значение

allowed-protocol-mappers

Позволяет указать разрешенные шаблоны протоколов сопоставления, которые будут доступны в представлении зарегистрированного (или обновленного) клиента.

Ниже изображено окно настройки политики регистрации клиента **allowed-protocol-mappers**.

[Политики регистрации клиента](#) > Разрешенные сопоставления протокола

Разрешенные сопоставления протокола

Имя *	<input type="text"/>
Поставщик	<input type="text" value="allowed-protocol-mappers"/>
Разрешенные сопоставления протокола	<input type="button" value="selectMultiple..."/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

*В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **allowed-protocol-mappers**.*

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	Позволяет указать разрешенные шаблоны протоколов сопоставления, которые будут доступны в представлении зарегистрированного (или обновленного) клиента. По умолчанию: allowed-protocol-mappers По умолчанию: allowed-protocol-mappers	Текстовое значение
Разрешенные сопоставления протокола	Белый список разрешенных поставщиков сопоставления протокола. Если есть попытка регистрации клиента, который содержит какие-либо сопоставления протокола, которые не находятся в белом списке, то регистрация таких клиентов будет отклонена.	Выпадающий список с возможностью выбора нескольких значений

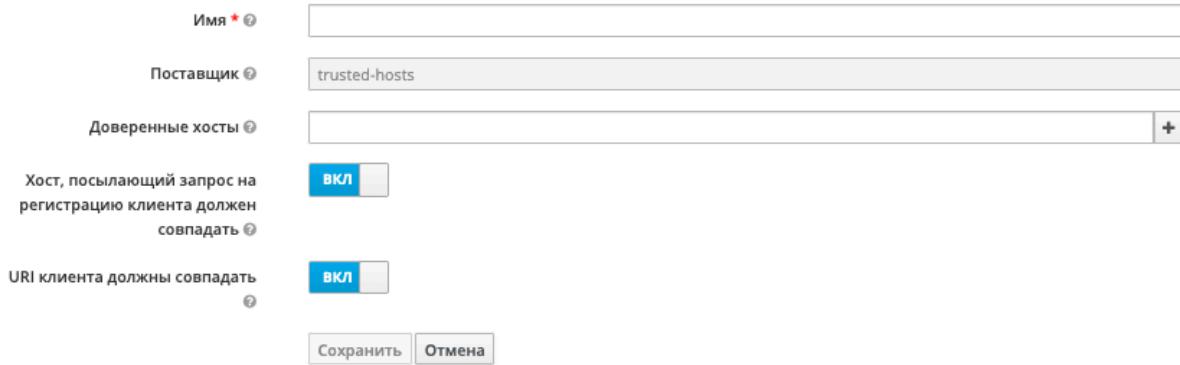
trusted-hosts

Позволяет указать, с каких хостов пользователь может зарегистрироваться, и какие URI перенаправления может использовать клиент в своей конфигурации.

Ниже изображено окно настройки политики регистрации клиента **trusted-hosts**.

[Политики регистрации клиента](#) > Доверенные хосты

Доверенные хосты



Имя * 

Поставщик 

Доверенные хосты  

Хост, посылающий запрос на регистрацию клиента должен совпадать 

URI клиента должны совпадать 

*В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **trusted-hosts**.*

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение

Наименование настройки	Описание	Тип настройки
Поставщик	Позволяет указать, с каких хостов пользователь может зарегистрироваться и какие URI перенаправления может использовать клиент в своей конфигурации. По умолчанию: trusted-hosts По умолчанию: trusted-hosts	Текстовое значение
Доверенные хосты	Список хостов, которые являются доверенными и которым разрешено вызывать службу регистрации клиентов и/или использоваться в качестве значений клиентских URI. Могут использоваться имена хостов или IP-адреса. Если использовать звездочку в начале (например, '*.example.com'), то доверенным будет весь домен example.com.	Текстовое поле с возможностью выбора нескольких значений
Хост, посылающий запрос на регистрацию клиента должен совпадать	Если включено, то любой запрос на сервис регистрации клиентов разрешен только если он передан из доверенного хоста или домена.	Булевая
URI клиента должны совпадать	Если включено, то все клиентские URI (URI переадресации и прочие) разрешены только если они совпадают с доверенным хостом или доменом.	Булевая

consent-required

При наличии у вновь зарегистрированного клиента всегда будет включен переключатель “Требуется согласие”.

Ниже изображено окно настройки политики регистрации клиента **consent-required**

[Политики регистрации клиента](#) > Consent Required

Consent Required ?

Имя * (*)

Поставщик

consent-required

Сохранить Отмена

В таблице представлено детальное описание интерфейса настройки политики регистрации клиента **consent-required**.

Наименование настройки	Описание	Тип настройки
Имя	Отображаемое наименование политики	Текстовое значение
Поставщик	При наличии у вновь зарегистрированного клиента всегда будет включен переключатель “Требуется согласие”. По умолчанию: consent-required	Текстовое значение

Политики клиента

Ниже изображено окно настройки Политик клиента.

Имя	Описание	Global	Действия
fapi-1-baseline	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 1: Baseline' specification.	Да	Редактировать
fapi-1-advanced	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 2: Advanced' specification.	Да	Редактировать
fapi-ciba	Client profile, which enforce clients to conform 'Financial-grade API: Client Initiated Backchannel Authentication Profile' specification (Implementer's Draft ver1'). To satisfy FAPI-CIBA, both this profile and fapi-1-advanced global profile need to be used.	Да	Редактировать

Профили

Профиль клиента позволяет установить набор исполнителей, которые применяются для различных действий, выполняемых с клиентом. Действия могут быть действиями администратора, например, создание или обновление клиента, или действиями пользователя, например, аутентификация клиента.

Form View

В таблице представлено детальное описание интерфейса профиля политик клиента Form View.

Наименование настройки	Описание
fapi-1-baseline	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 1: Baseline' specification.
fapi-1-advanced	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 2: Advanced' specification.
fapi-ciba	Client profile, which enforce clients to conform 'Financial-grade API: Client Initiated Backchannel Authentication Profile' specification (Implementer's Draft ver1'). To satisfy FAPI-CIBA, both this profile and fapi-1-advanced global profile need to be used.

Редактор JSON

```
{
  "profiles": [],
  "globalProfiles": [
    {
      "name": "fapi-1-baseline",
      "description": "Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 1: Baseline' specification."
    }
  ]
}
```

1.0 - Part 1: Baseline' specification.",

```
"executors": [
  {
    "executor": "secure-session",
    "configuration": {}
  },
  {
    "executor": "pkce-enforcer",
    "configuration": {
      "auto-configure": true
    }
  },
  {
    "executor": "secure-client-authenticator",
    "configuration": {
      "allowed-client-authenticators": [
        "client-jwt",
        "client-secret-jwt",
        "client-x509"
      ],
      "default-client-authenticator": "client-jwt"
    }
  },
  {
    "executor": "secure-client-uris",
    "configuration": {}
  },
  {
    "executor": "consent-required",
    "configuration": {
      "auto-configure": true
    }
  },
  {
    "executor": "full-scope-disabled",
    "configuration": {
      "auto-configure": true
    }
  }
],
},
{
  "name": "fapi-1-advanced",
  "description": "Client profile, which enforce clients to conform 'Financial-grade API Security Profile"
}
```

```
1.0 - Part 2: Advanced' specification.",  
  "executors": [  
    {  
      "executor": "secure-session",  
      "configuration": {}  
    },  
    {  
      "executor": "confidential-client",  
      "configuration": {}  
    },  
    {  
      "executor": "secure-client-authenticator",  
      "configuration": {  
        "allowed-client-authenticators": [  
          "client-jwt",  
          "client-x509"  
        ],  
        "default-client-authenticator": "client-jwt"  
      }  
    },  
    {  
      "executor": "secure-client-uris",  
      "configuration": {}  
    },  
    {  
      "executor": "secure-request-object",  
      "configuration": {  
        "available-period": "3600",  
        "verify-nbf": true  
      }  
    },  
    {  
      "executor": "secure-response-type",  
      "configuration": {  
        "auto-configure": true,  
        "allow-token-response-type": false  
      }  
    },  
    {  
      "executor": "secure-signature-algorithm",  
      "configuration": {  
        "default-algorithm": "PS256"  
      }  
    },  
  ],
```

```
{  
  "executor": "secure-signature-algorithm-signed-jwt",  
  "configuration": {  
    "require-client-assertion": false  
  }  
},  
{  
  "executor": "consent-required",  
  "configuration": {  
    "auto-configure": true  
  }  
},  
{  
  "executor": "full-scope-disabled",  
  "configuration": {  
    "auto-configure": true  
  }  
},  
{  
  "executor": "holder-of-key-enforcer",  
  "configuration": {  
    "auto-configure": true  
  }  
}  
]  
},  
{  
  "name": "fapi-ciba",  
  "description": "Client profile, which enforce clients to conform 'Financial-grade API: Client Initiated Backchannel Authentication Profile' specification (Implementer's Draft ver1'). To satisfy FAPI-CIBA, both this profile and fapi-1-advanced global profile need to be used.",  
  "executors": [  
    {  
      "executor": "secure-ciba-req-sig-algorithm",  
      "configuration": {  
        "default-algorithm": "PS256"  
      }  
    },  
    {  
      "executor": "secure-ciba-session",  
      "configuration": {}  
    },  
    {  
      "executor": "secure-ciba-signed-authn-req",  
    }  
  ]  
}
```

```
"configuration": {  
    "available-period": "3600"  
}  
}  
]  
}  
]  
}
```

Политики

Политика клиента позволяет привязывать профили клиентов к различным условиям, чтобы указать, когда именно принудительно выполняется поведение, указанное исполнителями конкретного профиля клиента.

Form View

Ниже изображено окно настройки политики клиента Form View.

Главная Вход Ключи Е-mail Темы Каш Токены Регистрация клиента **Политики клиента** Защита безопасности Дополнительно

Профили
Политики
Редактор JSON

Имя Описание Включено Действия

Создать

Редактор JSON

```
{  
    "policies": []  
}
```

Защита безопасности

Заголовки

Ниже изображено окно настройки определения Заголовков.

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Заголовки Определение Brute Force

X-Frame-Options	SAMEORIGIN
Content-Security-Policy	frame-src 'self'; frame-ancestors 'self'; object-src 'none';
Content-Security-Policy-Report-Only	
X-Content-Type-Options	nosniff
X-Robots-Tag	none
X-XSS-Protection	1; mode=block
HTTP Strict Transport Security (HSTS)	max-age=31536000; includeSubDomains
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки определения Заголовков.

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
X-Frame-Options	Значение по умолчанию не позволяет страницам быть включенными в iframe сторонних сайтов (перейдите по ссылке для получения дополнительной информации)	Текстовая	SAMEORIGIN
Content-Security-Policy	Значение по умолчанию не позволяет страницам быть включенными в iframe сторонних сайтов (перейдите по ссылке для получения дополнительной информации)	Текстовая	
Content-Security-Policy-Report-Only	Указывает политики безопасности с целью защиты (но без применения), позволяет тренироваться разработчикам.	Текстовая	
X-Content-Type-Options	Директива, позволяющая защитить MIME - типы. Также включает CORS для MIME - типов. Значение по умолчанию не позволяет браузерам Internet Explorer и Google Chrome вычислять тип содержимого в ответе от сервера дальше от объявленного типа содержимого (перейдите по ссылке для получения дополнительной информации)	Текстовая	nosniff
X-Robots-Tag	HTTP - заголовок, позволяющий серверу сообщать ботам поисковых систем инструкции по индексации страницы даже без загрузки содержимого самой страницы. Предотвращает страницы от появления в поисковых движках (нажмите на строку для доп. информации)	Текстовая	none

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
X-XSS-Protection	Этот заголовок настраивает Cross-site scripting (XSS) фильтр в браузере. Используя поведение по умолчанию, браузер будет предотвращать рендеринг страницы, когда обнаружится XSS атака (нажмите на строку для доп. информации)	Текстовая	
HTTP Strict Transport Security (HSTS)	Заголовок Strict-Transport-Security HTTP указывает браузеру всегда использовать HTTPS. Увидев этот заголовок однажды, браузер будет заходить на сайт через HTTPS, в течении определенного времени (1 год), включая поддомены.	Текстовая	

Определение Brute Force

Ниже изображено окно настройки определения Brute Force.

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Заголовки Определение Brute Force

Включено ВЫКЛ

Вечная блокировка ВЫКЛ

Максимальное количество неудачных попыток входа 30

Порог ожидания 1 минут

Проверка количества миллисекунд между попытками входа 1000

Минимальное ожидание быстрого входа 1 минут

Максимальное ожидание 15 минут

Время сброса неудачных попыток 12 часов

Отмена

В таблице представлено детальное описание интерфейса настройки определения Brute Force и даны рекомендуемые значения настроек.

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
Включено	Включена ли проверка Brute Force	Булевая	Включено
Вечная блокировка	Блокирует пользователя навсегда, когда пользователь достигает максимального количества неверных попыток входа	Булевая	Выключено

Наименование настройки	Описание	Тип настройки	Рекомендуемое значение
Максимальное количество неудачных попыток входа	Количество неудачных попыток входа до блокировки пользователя.	Численное значение	5
Порог ожидания	Если порог ошибок превышен, сколько времени пользователь будет заблокирован?	Число в минутах/часах/днях	30 минут
Проверка количества миллисекунд между попытками входа	Если попытки аутентификации происходят слишком часто, то пользователя необходимо заблокировать.	Численное значение	1000
Минимальное ожидание быстрого входа	Как долго ждать после неудачной попытки быстрого входа.	Число в минутах/часах/днях	1 минут
Максимальное ожидание	Максимальное время, на которое пользователь будет заблокирован.	Число в минутах/часах/днях	90 минут
Время сброса неудачных попыток	Через какое время счетчик неудачных попыток будет сброшен?	Число в минутах/часах/днях	12 часов

Дополнительно

События Аудит

Ниже изображено окно настройки модуля отправки событий KeyCloak.SE в Platform V Audit.

Test 

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

[События Аудит](#) [Настройки Syslog](#) [Настройки SOAP](#)

Список адресов kafka	
Подтверждение записи	
Максимальный размер файла буфера	
Путь каталога буфера	
Каталог с конфигурацией	
Время повторной попытки	
Список адресов zookeeper	
Пароль ключа	
Путь до хранилища ключей	
Тип хранилища ключей	Нет
Пароль хранилища ключей	
Путь до truststore	
Тип truststore	Нет
Пароль truststore	
Версия протокола SSL	
Протокол защиты обмена с kafka	

В таблице представлено детальное описание интерфейса настройки модуля отправки событий KeyCloak.SE в Platform V Audit.

Наименование настройки	Описание	Тип настройки
Список адресов kafka	Список адресов экземпляров брокера Kafka, с которым работает ТС «Аудит2». Соответствует настройке kafka.producer.bootstrap.servers	Текстовое значение
Подтверждение записи	Подтверждение записи для транспортного модуля. Возможные значения параметра: all – поставщик Kafka всегда ожидает подтверждения записи данных в минимально указанное количество реплик Kafka. Минимальное допустимое количество реплик указывается в настройках параметров сервиса Kafka. Соответствует настройке kafka.producer.acks	Текстовое значение
Максимальный размер файла буфера	Максимальный размер файла буфера (XXXX_audit.data) в байтах для каждого прикладного модуля. Соответствует настройке buffer.maxSize	Числовое значение
Путь каталога буфера	Абсолютный путь к существующему каталогу, в котором будет создан файл буфера. Соответствует настройке buffer.directory	Текстовое значение

Наименование настройки	Описание	Тип настройки
Каталог с конфигурацией	Путь до каталога с опциональными конфигурационными файлами модуля	Текстовое значение
Время повторной попытки	Время повторной попытки отправки сообщения, если была неудачная отправка (в миллисекундах)	Числовое значение
Список адресов zookeeper	Соответствует настройке zookeeper.connection.string	Текстовое значение
Пароль ключа	Соответствует настройке kafka.producer.ssl.key.password	Текстовое значение
Путь до хранилища ключей	Соответствует настройке kafka.producer.ssl.keystore.location	Текстовое значение
Тип хранилища ключей	Соответствует настройке kafka.producer.ssl.keystore.type	Выпадающий список
Пароль хранилища ключей	Соответствует настройке kafka.producer.ssl.keystore.password	Текстовое значение
Путь до truststore	Соответствует настройке kafka.producer.ssl.truststore.location	Текстовое значение
Тип truststore	Соответствует настройке kafka.producer.ssl.truststore.type	Выпадающий список
Пароль truststore	Соответствует настройке kafka.producer.ssl.truststore.password	Текстовое значение
Версия протокола SSL	Версия протокола безопасного соединения SSL. Соответствует настройке kafka.producer.ssl.protocol	Выпадающий список
Протокол защиты обмена с kafka	Сопоставляется с audit.proxy.url	Выпадающий список

События Syslog

Ниже изображено окно настройки для передачи событий в Syslog.

Test 

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

События Аудит  Настройки Syslog  Настройки SOAP 

Исключить события	<input type="text"/>
Имя хоста	<input type="text"/>
Порт хоста	<input type="text"/>
Протокол RFC	<input type="button" value="▼"/>
Работа через SSL	<input type="checkbox"/>
Резервное имя хоста	<input type="text"/>
Резервный номер порта	<input type="text"/>
Резервный протокол RFC	<input type="button" value="▼"/>
Работа через SSL (резерв)	<input type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки передачи событий в Syslog.

Наименование настройки	Описание	Тип настройки
Исключить события	Список типов событий, которые не будут отправлены в Syslog (через запятую), например REFRESH_TOKEN	Текстовое значение
Имя хоста	Имя хоста Syslog	Текстовое значение
Порт хоста	Номер порта Syslog (от 0 до 65535), стандартный 514, с SSL 6915	Числовое значение
Протокол RFC	Протокол syslog-ng для передачи данных	Выпадающий список
Работа через SSL	События будут передаваться по SSL	Чекбокс
Резервное имя хоста	Резервное имя хоста Syslog (будет задействовано в случае недоступности основного канала)	Текстовое значение
Резервный номер порта	Резервный номер порта Syslog (от 0 до 65535) (будет задействовано в случае недоступности основного канала)	Числовое значение
Резервный протокол RFC	Резервный протокол syslog-ng для передачи данных	Выпадающий список
Работа через SSL (резерв)	События будут передаваться по SSL (будет задействовано в случае недоступности основного канала)	Чекбокс

Настройки SOAP

Ниже изображено окно Настройки SOAP-интерфейса.

Test trash

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

События Аудит ? Настройки Syslog ? **Настройки SOAP ?**

CN клиентского сертификата	<input type="text"/>
Фильтр по scope ролей	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса настройки SOAP-интерфейса.

Наименование настройки	Описание	Тип настройки
CN клиентского сертификата	Список допустимых CN клиентского сертификата (при mTLS) через "", "*" - отключить проверку	Текстовое значение
Фильтр по scope ролей	Фильтр по scope ролей, попадающих под синхронизацию через API. Это префикс роли realm или клиента client_id/prefix. Пример: "platformauth, EFS, PlatformAuth-Proxy/"	Текстовое значение

Параметры сессии

Ниже изображено окно настройки ограничения числа сессий.

PLATFORM V

PlatformAuth

Конфигурация

Настройки Realm

- Клиенты
- Шаблоны клиентов
- Роли
- Поставщики идентификации

PlatformAuth

Главная Вход Ключи E-mail Темы Кэш Токены Регистрация клиента Защита безопасности Дополнительно

Настройки Syslog ? Настройки SOAP ? **Параметры сессии ?**

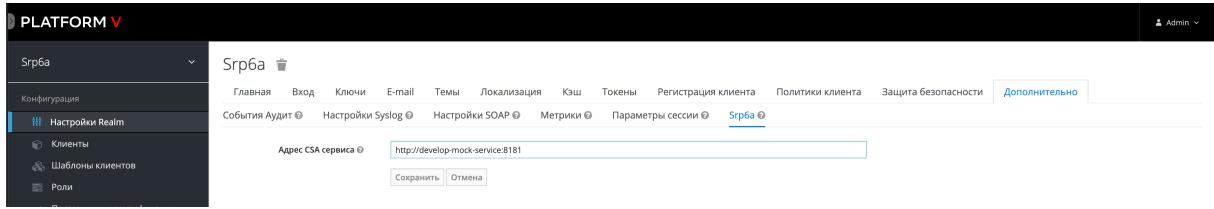
Ограничение числа сессий	<input type="text" value="10"/>
--------------------------	---------------------------------

В таблице представлено детальное описание интерфейса настройки ограничения числа сессий.

Наименование настройки	Описание	Тип настройки
Ограничение числа сессий	Этот параметр ограничивает число возможных сессий пользователя	Числовое значение

SRP6a

Ниже изображено окно настройки SRP6a.



В таблице представлено детальное описание интерфейса настройки работы по протоколу SRPБа.

Наименование настройки	Описание	Тип настройки
Адрес CSA сервиса	Адрес CSA сервиса	Текстовое значение

Управление Клиентами

Клиенты - это сущности, которые могут запросить аутентификацию пользователя. Клиенты бывают двух типов. Первый тип клиентов - это приложения, которые хотят участвовать в единой регистрации. Эти клиенты просто хотят, чтобы Keycloak.SE обеспечил безопасность для них. Другой тип клиентов - это клиенты, которые запрашивают токен доступа, чтобы иметь возможность вызывать другие службы от имени аутентифицированного пользователя.

Управление клиентом

Настройки

На рисунке ниже изображен интерфейс настройки клиента.

Тест

Настройки Роли Шаблоны клиентов Сопоставления Область Отзыв Сессии Оффлайн доступ Установка

ID клиента	Тест
Имя	
Описание	
Включено	<input checked="" type="checkbox"/>
Необходимо согласие	<input checked="" type="checkbox"/>
Отображение согласия на экране клиента	<input checked="" type="checkbox"/>
Текст согласия на экране клиента	
Тема страницы входа	
Протокол клиента	openid-connect
Тип доступа	public
Standard Flow включен	<input checked="" type="checkbox"/>
Implicit Flow включен	<input type="checkbox"/> Выкл
Direct Access Grants включен	<input checked="" type="checkbox"/>
Корневой URL	
* Валидация URI перенаправления	
Базовый URL	
URL администрирования приложения	
Web источники	

В таблице представлено детальное описание интерфейса настройки клиента.

Наименование настройки	Описание	Тип настройки
ID клиента	Задает идентификатор, указываемый в URI и в токенах. Например 'му-client'. Для SAML это также ожидаемое имя издателя для запросов аутентификации	Текстовое значение
Имя	Задает отображаемое название клиента. Например 'My Client'. Поддерживает ключи для локализованных значений. Например: \${my_client}	Текстовое значение
Описание	Задает описание клиента. Например 'Мой клиент для табеля учета времени'. Поддерживает ключи для локализованных значений. Например: \${my_client_description}	Текстовое значение
Включено	Отключенные клиенты не могут инициировать вход или иметь возможность получить токены доступа	Булевая
Необходимо согласие	Если включено, пользователи должны дать согласие на доступ клиентскому приложению	Булевая

Наименование настройки	Описание	Тип настройки
Отображение согласия на экране клиента	Применяется только в том случае, если параметр “Необходимо согласие” включен. Если этот переключатель выключен, экран согласия будет содержать только согласия, соответствующие настроенным областям клиента. Если переключатель включен, то на экране согласия будет также один пункт о самом клиенте	Булевая
Тема страницы входа	Применяется, если для данного клиента включена опция “Отображать клиента на экране согласия”. Содержит текст, который будет отображаться на экране согласия о разрешениях, относящихся только к этому клиенту	Текстовое значение
Тема страницы входа	Выберите тему для страниц входа, временного одноразового пароля (OTP), выдачи разрешений, регистрации и восстановления пароля	Выпадающий список
Протокол клиента	‘OpenID connect’ разрешает клиентам проверить личность конечного пользователя, основанного на выполнении аутентификации на Сервере Авторизации.’SAML’ включает веб-сценарии аутентификации и авторизации, включая кроссдоменные центры единого управления доступом (SSO) и использующие токены безопасности, содержащие заявления на передачу информации	Выпадающий список
Тип доступа	‘Confidential’ клиенты требуют секрет для инициализации протокола входа. ‘Public’ клиентам секрет не требуется. ‘Bearer-only’ клиенты и веб-сервисы никогда не инициализируют вход	Выпадающий список
Standard Flow включен	Включает стандартное OpenID Connect перенаправление, основанное на аутентификации с кодом авторизации. В терминах OpenID Connect или OAuth2 спецификаций включает ‘Authorization Code Flow’ для этого клиента	Булевая
Implicit Flow включен	Включает поддержку OpenID Connect перенаправления, основанного на аутентификации без кода авторизации. В терминах OpenID Connect или OAuth2 спецификаций включает поддержку ‘Implicit Flow’ для этого клиента	Булевая
Direct Access Grants включен	Включает поддержку Direct Access Grants, которая означает, что клиент имеет доступ к имени пользователя и пароля и обменивает их напрямую с сервером Keycloak на токен доступа. В терминах OAuth2 спецификации означает поддержку ‘Resource Owner Password Credentials Grant’ для этого клиента.	Булевая
Корневой URL	Корневой URL добавляется к относительным URL	Текстовое значение

Наименование настройки	Описание	Тип настройки
Валидация URI перенаправления	Валидирует паттерн URI, на который может быть перенаправлен браузер после успешного входа или выхода. Разрешены простые ссылки, напр. ‘ http://example.com/ ’. Также допускается использовать относительный путь, напр. ‘ /my/relative/path/ ’. Относительные пути необходимо указывать относительно корневого URL клиента, или, если он не специфицирован, корневого URL сервера авторизации. Для SAML необходимо задать валидный паттерн URI, если полагаться на URL сервиса потребителя, внедренного в запрос авторизации.	Текстовое значение
Базовый URL	Используемый URL по умолчанию. Используется в случае, если серверу требуется перенаправление или обратная ссылка на клиента.	Текстовое значение
URL администрирования приложения	URL для доступа к интерфейсу администратора в заданном клиенте. Необходимо установить, если клиент поддерживает адаптер REST API. Это REST API разрешает серверу авторизации сдать политики отзыва и прочие административные задачи. Обычно устанавливается значение, соответствующее базовому URL клиента.	Текстовое значение
Web источники	Разрешает CORS источникам. Чтобы разрешить всем источники с допустимыми URL-адресами переадресации, добавьте ‘+’. Чтобы разрешить все источники, добавьте ‘*’.	Текстовое значение

Тонкая настройка конфигурации OpenID Connect

На рисунке ниже изображен интерфейс тонкой настройки конфигурации OpenID Connect.

▼ Тонкая настройка конфигурации OpenID Connect ⓘ

Алгоритм подписи access-токена ⓘ	<input type="text"/>
Алгоритм подписи id-токена ⓘ	<input type="text"/>
Алгоритм подписи ответа информации о пользователе ⓘ	<input type="text" value="unsigned"/>
Алгоритм сигнатуры объекта запроса ⓘ	<input type="text" value="any"/>
Представлять объект запроса ⓘ	<input type="text" value="not required"/>

В таблице представлено детальное описание настройки конфигурации OpenID Connect.

Наименование настройки	Описание	Тип настройки
Алгоритм подписи access-токена	JWA-алгоритм, используемый для подписи access-токена	Выпадающий список

Наименование настройки	Описание	Тип настройки
Алгоритм подписи id-токена	JWA-алгоритм, используемый для подписи id-токена	Выпадающий список
Алгоритм подписи ответа информации о пользователе	JWA алгоритм используется для подписи ответа ресурса информации о пользователе. Если установлено в 'unsigned', то ответ информации о пользователе не будет подписан и будет возвращен в формате application/json.	Выпадающий список
Алгоритм сигнатурь объекта запроса	JWA алгоритм, который необходим клиенту для использования во время отсылки OIDC запроса объекта, специфицированного по 'request' или 'request_uri' параметрам. Если установлено в 'any', то объект запроса будет подписан любым алгоритмом (включая 'none').	Выпадающий список
Предоставлять объект запроса	Указывает, нужно ли клиенту предоставить объект запроса с запросом на авторизацию, и какой метод он может использовать для этого. Если установлено значение «не требуется», предоставление объекта запроса необязательно. Во всех остальных случаях предоставление объекта запроса обязательно. Если установлено значение «запрос», объект запроса должен быть предоставлен по значению. Если установлено значение «request_uri», объект запроса должен быть предоставлен по ссылке. Если установлено значение «request или request_uri», можно использовать любой метод.	Выпадающий список

Режимы совместимости OpenID Connect

На рисунке ниже изображен интерфейс настройки режима совместимости OpenID Connect.

▼ Режимы совместимости OpenID Connect

Исключить параметр session_state
из ответа аутентификации. 

В таблице представлено детальное описание интерфейса настройки режима совместимости OpenID Connect.

Наименование настройки	Описание	Тип настройки
Исключить параметр session_state из ответа аутентификации	Если включено, параметр 'session_state' не будет включен в OpenID Connect Authentication ответ.	Булевая

Это полезно если клиент использует старый OIDC / OAuth2 адаптер, который не поддерживает параметр 'session_state'.

Расширенные настройки

На рисунке ниже изображен интерфейс расширенных настроек клиента.

▼ Расширенные настройки ?

Продолжительность жизни токена доступа	<input type="text"/> минут
Включить OAuth 2.0 Mutual TLS Certificate Bound Access Tokens	<input checked="" type="checkbox"/> ВЫКЛ
Ключ подтверждения для CodeChallengeMethod обмена кодами	<input type="text"/>

В таблице представлено детальное описание интерфейса расширенных настроек клиента.

Наименование настройки	Описание	Тип настройки
Продолжительность жизни токена доступа	Максимальное время действия токена доступа. Значение рекомендуется устанавливать как можно ближе к тайм-ауту SSO.	Цифровое значение + выпадающий список
Включить OAuth 2.0 Mutual TLS Certificate Bound Access Tokens	Включает поддержку access-токенов с привязкой к сертификату OAuth 2.0 Mutual TLS, что означает, что keycloak связывает access-токен и refresh-токен с сертификатом X.509 клиента, запрашивающего токен, который обменивается mutual TLS между конечной точкой токена keycloak и этим клиентом. Эти токены могут рассматриваться как токены держателя ключа, а не токены на предъявителя.	Булевая
Ключ подтверждения для CodeChallengeMethod обмена кодами	Выберите, какой метод проверки кода для PKCE используется. Если не указано иное, keycloak не применяет PKCE к клиенту, если клиент не отправляет запрос авторизации с соответствующим запросом кода и методом обмена кода.	Выпадающий список

Переопределение потока аутентификации

На рисунке ниже изображено окно настройки переопределения потока аутентификации.

▼ Переопределения потока аутентификации ?

Сценарий браузера	<input type="text"/>
Сценарий Direct Grant Flow	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание интерфейса переопределения потока аутентификации.

Наименование настройки	Описание	Тип настройки
Сценарий браузера	Выберите сценарий, который необходимо использовать для аутентификации через браузер.	Выпадающий список
Сценарий Direct Grant Flow	Выберите сценарий, который необходимо использовать для аутентификации direct grant.	Выпадающий список
Ключ подтверждения для CodeChallengeMethod обмена кодами	Выберите, какой метод проверки кода для PKCE используется. Если не указано иное, keycloak не применяет PKCE к клиенту, если клиент не отправляет запрос авторизации с соответствующим запросом кода и методом обмена кода.	Выпадающий список

Роли

Роли клиентов – это пространства имен, предназначенные для клиентов. Каждый клиент получает свое собственное пространство имен. Роли клиентов управляются на вкладке Роли для каждого клиента. Вы взаимодействуете с этим пользовательским интерфейсом так же, как и с ролями уровня realm.

Назначьте нужные клиентские роли для возможности использования конкретной части консоли администрирования.

В таблице представлен перечень клиентских ролей и их описание.

Наименование клиентской роли	Описание роли
add-users	Позволяет создавать пользователей
allow-sync-users	запуск синхронизации УЗ с ОСА
allow-map-roles	Позволяет пользователям присваивать роли
allow-sync-data	Позволяет синхронизировать справочники с ОСА
clear-cache	Позволяет очищать кэш
create-client	Позволяет создавать клиентов
delete-account	Позволяет удалять УЗ
delete-users	Позволяет удалять пользователей
impersonation	Позволяет имперсонировать
manage-account	Позволяет управлять УЗ
manage-account-links	Позволяет управлять ссылками УЗ
manage-authorization	Позволяет управлять авторизацией

Наименование клиентской роли	Описание роли
manage-clients	Позволяет управлять клиентами
manage-consent	Позволяет управлять согласиями
manage-data-sync	Позволяет управлять синхронизацией с ОСА
manage-events	Позволяет управлять событиями
manage-identity-providers	Позволяет управлять поставщиками идентификации
manage-realm	Позволяет управлять realm
manage-realm-attributes	Позволяет управлять атрибутами realm
manage-users	Позволяет управлять пользователями
query-clients	Позволяет настраивать параметры клиентов
query-groups	Позволяет настраивать параметры групп
query-realms	Позволяет настраивать параметры realms
query-users	Позволяет настраивать параметры пользователей
read-token	Дает доступ к чтению токенов
view-applications	Позволяет просматривать параметры приложений
view-authorization	Позволяет просматривать параметры авторизации
view-clients	Позволяет просматривать клиентов
view-consent	Позволяет просматривать согласия
view-events	Позволяет просматривать события
view-groups	Позволяет просматривать группы
view-identity-providers	Позволяет просматривать поставщиков идентификации
view-profile	Позволяет просматривать профили
view-realm	Позволяет просматривать realm
view-realm-attributes	Позволяет просматривать атрибуты realm
view-users	Позволяет просматривать пользователей

Перечень ролей

На рисунке ниже изображено окно со списком ролей клиента.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Тест

Настройки Роли Шаблоны клиентов Сопоставления Область Отзыв Сессии Оффлайн доступ Установка

Наименование роли	Составная	Описание	Действия
Тестовая роль	Нет		Добавить роль Редактировать Удалить

В таблице представлено детальное описание интерфейса с представлением ролей клиента.

Наименование настройки	Описание	Тип настройки
Добавить	По нажатию открывает окно добавления роли клиента	Кнопка
Наименование роли	Отображение наименования роли	Текстовое значение
Составная	Признак составной роли	Текстовое значение
Описание	Описание роли клиента	Текстовое значение
Действия	Редактировать	Кнопка/По нажатию открывает окно редактирования роли клиента
Удалить	По нажатию удаляет роль клиента	Кнопка

Добавление роли

На рисунке ниже изображено окно добавления ролей клиента.

Добавить роль

Наименование роли *

Описание

Сохранить **Отмена**

В таблице представлено детальное описание интерфейса добавления ролей клиента.

Наименование настройки	Описание	Тип настройки
Наименование роли	Поле для ввода наименования роли клиента	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение

Редактирование роли

Детали роли

Любая роль уровня realm или клиента может стать составной ролью. Составная роль – это роль, с которой связана одна или несколько дополнительных ролей. Когда составная роль сопоставляется пользователю, пользователь получает роли, связанные с составной ролью. Это наследование является рекурсивным, поэтому пользователи также наследуют любой состав композитов. Однако не рекомендуется злоупотреблять составными ролями.

На рисунке ниже изображено окно редактирования роли клиента.

Тестовая Роль 🗑

Детали Атрибуты Пользователи с ролью

Наименование роли	Тестовая роль
Описание	
Составные роли	<input checked="" type="checkbox"/> Вкл

Сохранить Отмена

Составные роли

Роли Realm	Доступные роли Enter part of role name... Test Test1 admin create-realm default-roles-master offline_access ttt uma_authorization	Ассоциированные роли Enter part of role name...
	Добавить выбранное >	«Удалить выбранное

В таблице представлено детальное описание интерфейса редактирования роли клиента.

Наименование настройки	Описание	Тип настройки
Наименование роли	Отображение наименования роли	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение
Составные роли	Когда эта роль (не)ассоциирована с любой ролью пользователей, она (не)будет неявно ассоциирована.	Кнопка
Роли Realm		

Наименование настройки	Описание	Тип настройки
Доступные роли	Роли уровня Realm, ассоциированные с этой составной ролью.	Поле с выбором значения
Ассоциированные роли	Роли уровня Realm, ассоциированные с составными ролями.	Поле с выбором значения
Добавить выбранное	Кнопка для добавления выбранных ролей в ассоциированные роли	Кнопка
Удалить выбранное	Кнопка для удаления ролей из ассоциированных ролей	Кнопка

Пользовательский интерфейс выбора роли отображается на странице, и можно связать роли уровня realm и уровня клиента с создаваемой составной ролью.

Пользователи с ролью

На рисунке ниже изображено окно просмотра пользователей с ролью.

В таблице представлено детальное описание полей интерфейса просмотра пользователей с ролью.

Наименование настройки	Описание	Тип настройки
Пользователи с ролью	Перечисление пользователей с данной ролью	Текстовое поле

Атрибуты роли

На рисунке ниже изображено окно просмотра атрибутов роли.

В таблице представлено детальное описание полей интерфейса просмотра атрибутов роли.

Наименование настройки	Описание	Тип настройки
Ключ	Поле для ввода ключа, определяющего атрибут настройки	Текстовое поле

Наименование настройки	Описание	Тип настройки
Значение	Поле для ввода значения, задающегося атрибуту настройки	Текстовое поле
Действие. Добавить	Кнопка добавления связки ключ-значения	Кнопка

Шаблоны клиентов

Настройка клиентских областей

Разрешить настройку клиентских областей, связанных с этим клиентом.

На рисунке ниже изображен интерфейс настройки клиентских областей.

Тест

Настройки Роли Шаблоны клиентов Сопоставления Область Отзыв Сессии Оффлайн доступ Установка

Настройки Сопоставления

Области клиента по умолчанию

Доступные клиентские области

Добавить выбранное »

Назначенные клиентские области по умолчанию

web-origins
profile
roles
email

« Удалить выбранное

Необязательные клиентские области

Доступные клиентские области

Добавить выбранное »

Назначенные дополнительные клиентские области

address
phone
offline_access
microprofile-jwt

« Удалить выбранное

В таблице представлено детальное описание полей интерфейса настройки клиентских областей.

Наименование настройки	Описание	Тип настройки
Области клиента по умолчанию	Области клиента по умолчанию всегда применяются при выдаче токенов для этого клиента. Сопоставители протоколов и сопоставления областей ролей применяются всегда, независимо от значения используемого параметра области в запросе авторизации OIDC.	Поле с выбором значения
Доступные клиентские области	Области действия клиента, которые еще не назначены как области по умолчанию или дополнительные области	Поле с выбором значения
Назначенные клиентские области по умолчанию	Области действия клиента, которые будут использоваться в качестве областей действия по умолчанию при создании токенов для этого клиента.	Поле с выбором значения
Добавить выбранное	Кнопка для добавления выбранных клиентских областей в назначенные клиентские области по умолчанию	Кнопка
Удалить выбранное	Кнопка для удаления выбранных назначенных клиентских областей по умолчанию	Кнопка
Необязательные клиентские области	Необязательные клиентские области действия применяются при выдаче токенов для этого клиента, на случай, когда они запрашиваются параметром области в запросе авторизации OIDC	
Доступные клиентские области	Области действия клиента, которые еще не назначены как области по умолчанию или дополнительные области	Поле с выбором значения
Назначенные дополнительные клиентские области	Области действия клиента, которые могут использоваться как дополнительные области при генерации токенов для этого клиента	Поле с выбором значения
Добавить выбранное	Кнопка для добавления выбранных клиентских областей	Кнопка
Удалить выбранное	Кнопка для удаления выбранных клиентских областей	Кнопка

Сопоставления шаблонов клиентов

Разрешить видеть все сопоставления протоколов и сопоставления областей ролей, которые будут использоваться в токенах, выданных этому клиенту. Также разрешить создание примера access-токена на основе предоставленного параметра области.

На рисунке ниже изображен интерфейс представления и настройки сопоставления шаблонов клиентов.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

В таблице представлено детальное описание полей интерфейса представления и настройки сопоставления шаблонов клиентов.

Наименование настройки	Описание	Тип настройки
Параметр области действия	Если скопировать / вставить это значение параметра scope, то можно использовать его в начальном запросе аутентификации OpenID Connect, отправленном с этого клиентского адаптера. Области клиентов по умолчанию и выбранные дополнительные области клиентов будут использоваться при генерации токена, выпущенного для этого клиента.	Текстовое поле
Области действия клиента	Разрешить выбор дополнительных клиентских областей, которые могут использоваться при генерации токена, выпущенного для этого клиента	
Доступные дополнительные клиентские области	Содержит необязательные клиентские области, которые можно дополнительно использовать при выдаче токена доступа для этого клиента	Поле с выбором значения
Выбранные дополнительные клиентские области	Выбранные дополнительные клиентские области, которые будут использоваться при выдаче токена доступа для этого клиента. Выше указано, какое значение параметра области действия OAuth необходимо использовать, если необходимо, чтобы эти дополнительные клиентские области применялись, когда исходный запрос аутентификации OpenID Connect будет отправлен с вашего клиентского адаптера.	Поле с выбором значения
Эффективные клиентские области	Содержит все клиентские области по умолчанию и выбранные дополнительные области. Все сопоставители протоколов и сопоставления областей ролей всех этих клиентских областей будут использоваться при создании токена доступа, выданного для вашего клиента.	Поле с выбором значения

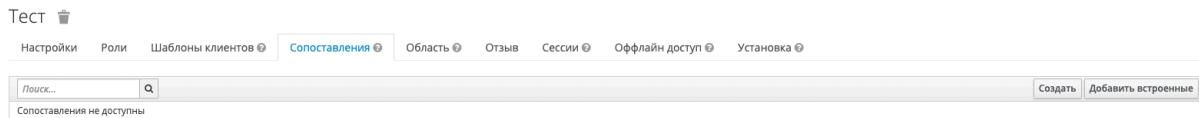
Наименование настройки	Описание	Тип настройки
Пользователь	При желании выберите пользователя, для которого будет создан пример токена доступа. Если не выбрать ни одного пользователя, то во время оценки пример токена доступа не будет сгенерирован.	Выпадающий список
Сопоставить	Применение настроек.	Кнопка

Сопоставления

Протокол сопоставлений

Протокол сопоставлений, осуществляющих преобразование в токены и документы. Могут делать такие вещи как сопоставление пользовательских данных в заявки протокола, или просто преобразовать любой запрос, происходящий между клиентом и сервером аутентификации.

На рисунке ниже изображен интерфейс представления сопоставлений протоколов для клиента.



В таблице представлено детальное описание полей интерфейса представления сопоставлений протоколов для клиента.

Наименование настройки	Описание	Тип настройки
Поисковое поле	Поле для поиска сопоставлений	Поисковое поле
Создать	Кнопка для создания сопоставлений	Кнопка
Добавить встроенные	Кнопка для добавления встроенных сопоставлений	Кнопка

Создать сопоставление протокола

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Клиенты > Тест > Сопоставления > Создать сопоставление протокола

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Добавить в токен ID

Добавить в информацию о пользователе

- Claims parameter Token
- User Realm Role
- User Session Note
- User Address
- Role Name Mapper
- User Client Role
- User Property
- Hardcoded Role
- Hardcoded claim
- Pairwise subject identifier
- User's full name
- Allowed Web Origins
- Audience
- User Attribute
- Group Membership
- Audience Resolve

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Протокол	Наименование протокола	Текстовое значение
Имя	Наименование сопоставления	Текстовое значение
Тип сопоставления	Выпадающий список	

Claims parameter Token

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Добавить в токен ID

Добавить в информацию о пользователе

Сохранить **Отмена**

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Claims parameter Token	Утверждения, указанные параметром Claims, помещаются в токены.	

Наименование настройки	Описание	Тип настройки
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

User Realm Role

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

The screenshot shows the 'Create protocol mapping' form. The fields and their current values are:

- Протокол: openid-connect
- Имя: (empty)
- Тип сопоставления: User Realm Role
- Префикс ролей Realm: (empty)
- Несколько значений: ВКЛ (Enabled)
- Имя переменной в токене: (empty)
- Тип переменной: Выбрать... (Select dropdown)
- Добавить в токен ID: ВКЛ (Enabled)
- Добавить в токен доступа: ВКЛ (Enabled)
- Добавить в информацию о пользователе: ВКЛ (Enabled)

At the bottom are two buttons: Сохранить (Save) and Отмена (Cancel).

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User Realm Role	Сопоставление роли ресурса пользователя с утверждением токена.	
Префикс ролей Realm	Префикс для каждой роли Realm (опционально).	Текстовое значение
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

User Session Note

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол ⓘ openid-connect

Имя ⓘ

Тип сопоставления ⓘ User Session Note

Заметка сессии пользователя ⓘ

Имя переменной в токене ⓘ

Тип переменной JSON ⓘ Выбрать...

Добавить в токен ID ⓘ Вкл

Добавить в токен доступа ⓘ Вкл

includeInAccessTokenResponse.label ⓘ Выкл

Сохранить **Отмена**

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User Session Note		Сопоставление сессии пользователя с записью в claim token.
Заметка сессии пользователя	Наименование процедуры заметки сессии пользователя согласованным с UserSessionModel.note.	Текстовое поле
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое поле
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
includeInAccessTokenResponse	includeInAccessTokenResponse.tooltip	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Users Address

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Имя пользовательского атрибута, обозначающего Улицу

Имя пользовательского атрибута, обозначающее Местонахождение

Имя пользовательского атрибута, обозначающее Регион

Имя пользовательского атрибута, обозначающего Почтовый индекс

Имя пользовательского атрибута, обозначающее Страна

Имя пользовательского атрибута, обозначающего Форматированный адрес

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Users Address	Сопоставляет атрибуты адреса пользователя (улица, населенный пункт, регион, почтовый индекс и страна) с утверждением OpenID Connect “адрес”	
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая
Имя пользовательского атрибута, обозначающего Улицу	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘street_address’ внутри атрибута ‘address’ токена. По умолчанию ‘street’	Текстовое значение
Имя пользовательского атрибута, обозначающего Местонахождение	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘locality’ внутри атрибута ‘address’ токена. По умолчанию ‘locality’	Текстовое значение
Имя пользовательского атрибута, обозначающего Регион	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘region’ внутри атрибута ‘address’ токена. По умолчанию ‘region’	Текстовое значение
Имя пользовательского атрибута, обозначающего Почтовый индекс	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘postal_code’ внутри атрибута ‘address’ токена. По умолчанию ‘postal_code’	Текстовое значение
Имя пользовательского атрибута, обозначающего Страну	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘country’ внутри атрибута ‘address’ токена. По умолчанию ‘country’	Текстовое значение
Имя пользовательского атрибута, обозначающего Форматированный адрес	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута ‘formatted’ внутри атрибута ‘address’ токена. По умолчанию ‘formatted’	Текстовое значение

Role Name Mapper

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Role Выберите роль

New Role Name

Сохранить **Отмена**

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Role Name Mapper	Сопоставляет назначенную роль с новым именем или позицией в токене	
Роль	Имя роли, которое необходимо изменить. Нажмите кнопку “Выбрать роль”, чтобы просмотреть роли, или просто введите ее в текстовое поле. Для ссылки на роль клиента используется синтаксис client.name.роль клиента, т.е. мой client.my роль	Текстовое значение
Новое имя роли	Новое имя роли. Новый формат имени соответствует тому, к какому токену доступа будет привязана роль. Таким образом, новое имя ‘myapp.new name’ сопоставит роль с этой позицией в маркере доступа. Новое имя “новое имя” сопоставит роль с ролями области в токене	Текстовое значение
Выберите роль	Список ролей доступных для сопоставления	Кнопка

User Client Role

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

ID клиента

Предфикс ролей клиента

Несколько значений

Имя переменной в токене

Тип переменной JSON

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User Client Role	Map a user client role to a token claim.	
ID клиента	ID клиента для сопоставления ролей	Выпадающий список с поиском
Префикс ролей клиента	Префикс для каждой роли клиента (опционально).	Текстовое значение
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая
Имя переменной в токене	Название утверждения для вставки в токен. Это может быть полное имя, например 'address.street'. В этом случае будет создан вложенный объект json. Чтобы предотвратить вложенность и использовать точку буквально, экранируйте точку обратной косой чертой (\.). Можно использовать специальный токен \${client_id}, который будет заменен фактическим идентификатором клиента. Примером использования является 'resource_access.\${client_id}.roles'. Это особенно полезно, если добавлять роли от всех клиентов (следовательно, переключатель 'ClientID' не установлен), и необходимо, чтобы роли клиентов каждого клиента хранились отдельно.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список

Наименование настройки	Описание	Тип настройки
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

User Property

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Protocol: openid-connect
Name:
Type mapping: User Property
Property:
Variable in token:
Variable type:
Add to token ID:
Add to access token:
Add to user info:

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User Property	Сопоставьте встроенное свойство пользователя (адрес электронной почты, имя, фамилия) с утверждением токена.	
Свойство	Имя свойства метода в интерфейсе UserModel. Для примера, значение 'email' будет ссылкой на метод UserModel.getEmail().	Текстовое значение

Наименование настройки	Описание	Тип настройки
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Hardcoded Role

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Protocol: openid-connect
 Имя:
 Тип сопоставления: Hardcoded Role
 Role: Выберите роль
 Сохранить Отмена

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Hardcoded Role	Жестко закодируйте роль в access token	
Роль	Роль, которую необходимо добавить к токену. Нажмите кнопку "Выбрать роль", чтобы просмотреть роли, или просто введите ее в текстовое поле. Для ссылки на роль клиента используется синтаксис client.name.роль клиента, т.е. мой client.my роль	Текстовое значение
Выберите роль	-	Кнопка

Hardcoded Claim

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Имя переменной в токене

Claim value

Тип переменной JSON

Добавить в токен ID Вкл

Добавить в токен доступа Вкл

Добавить в информацию о пользователе Вкл

includeInAccessTokenResponse.label

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Hardcoded claim	Жестко закодируйте утверждение в токене.	
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Claim value	Значение утверждения, которое необходимо жестко закодировать. 'true' и 'false' могут использоваться для логических значений.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая
includeInAccessTokenResponse.tooltip	Включить в токен доступа ответ. Всплывающая подсказка	Булевая

Pairwise subject identifier

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол	<input type="text" value="openid-connect"/>
Имя	<input type="text"/>
Тип сопоставления	<input type="text" value="Pairwise subject identifier"/>
Сектор идентификации URI	<input type="text"/>
Соль	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Pairwise subject identifier	Вычисляет попарный идентификатор субъекта, используя salted хэш sha-256. Дополнительные сведения о попарных идентификаторах субъектов см. в спецификации OpenID Connect.	
Сектор идентификации URI	Провайдеры, использующие пары вспомогательных значений и поддерживающие динамическую регистрацию клиентов ДОЛЖНЫ использовать sector_identified_uri параметр. Это обеспечивает способ для группы сайтов под общим административным контролем, чтобы иметь последовательные попарные значения независимо от индивидуальных доменных имен. Это также обеспечивает способ для клиентов для изменения redirect_uri доменов, не имеющих возможности перерегистрации всех своих пользователей.	Текстовое значение
Соль	Соль, используемая для вычисления парного субъекта идентификатора. Если поле не заполнено, то соль будет сгенерирована.	Текстовое значение

User's full name

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол	<input type="text" value="openid-connect"/>
Имя	<input type="text"/>
Тип сопоставления	<input type="text" value="User's full name"/>
Добавить в токен ID	<input checked="" type="checkbox"/>
Добавить в токен доступа	<input checked="" type="checkbox"/>
Добавить в информацию о пользователе	<input checked="" type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User's full name	Сопоставляет имя и фамилию пользователя с утверждением OpenID Connect 'name'. Формат <первый> + ' ' + <последний>	
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Allowed Web Origins

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Allowed Web Origins	Добавляет все разрешенные веб-источники к утверждению “разрешенные источники” в токене	

Audience

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Включить аудиенцию клиентов

Включить аудиенцию пользователей

Добавить в токен ID ВЫК ВКЛ

Сохранить **Отмена**

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Audience	Добавьте указанную аудиторию в поле аудитория (aud) токена	
Включить аудиенцию клиентов	Идентификатор клиента указанной аудитории будет включен в поле audience (aud) токена. Если в токене есть существующие аудиенции, указанное значение будет просто добавлено к ним. Оно не отменяет существующие аудиенции.	Выпадающий список
Включить аудиенцию пользователей	Используется только в том случае, если 'Included Client Audience' не заполнено. Указанное значение будет включено в поле audience (aud) токена. Если в токене есть существующие аудиенции, указанное значение будет просто добавлено к ним. Оно не отменяет существующие аудиенции.	Текстовое значение
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая

User Attribute

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол	<input type="text" value="openid-connect"/>
Имя	<input type="text"/>
Тип сопоставления	<input type="text" value="User Attribute"/>
Атрибут пользователя	<input type="text"/>
Имя переменной в токене	<input type="text"/>
Тип переменной JSON	<input type="button" value="Выбрать..."/>
Добавить в токен ID	<input checked="" type="checkbox"/>
Добавить в токен доступа	<input checked="" type="checkbox"/>
Добавить в информацию о пользователе	<input checked="" type="checkbox"/>
Несколько значений	<input type="checkbox"/>
Агрегированные значения атрибутов	<input type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
User Attribute	Сопоставьте пользовательский атрибут пользователя с утверждением токена.	
Атрибут пользователя	Имя сохраненного атрибута пользователя, которое является именем атрибута, согласованным с UserModel.attribute.	Текстовое значение
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая

Наименование настройки	Описание	Тип настройки
Агрегированные значения атрибутов	Указывает, следует ли агрегировать значения атрибутов с атрибутами группы. При использовании протокола OpenID Connect необходимо включить многозначную опцию, чтобы получить все значения. Дублированные значения отбрасываются, и с помощью этой опции порядок значений не гарантируется.	Булевая

Group Membership

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Имя переменной в токене

Full group path

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Сохранить **Отмена**

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Group Membership	Сопоставление пользователя с членством в группах	
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Full group path	Включает полный путь к группе т.е. /top/level 1/level 2, если выключено (false) просто укажет имя группы	Булевая
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Audience Resolve

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Создать сопоставление протокола

Протокол	openid-connect
Имя	
Тип сопоставления	Audience Resolve
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Audience Resolve	Добавляет все идентификаторы клиентов “разрешенных” клиентов в поле аудитории токена. Разрешенный клиент означает клиент, для которого пользователь имеет хотя бы одну роль клиента	

Добавить встроенное сопоставление протокола

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

Добавить встроенное сопоставление протокола

Поиск...	Категория	Тип	Добавить
zoneinfo	Token mapper	User Attribute	<input type="checkbox"/>
birthdate	Token mapper	User Attribute	<input type="checkbox"/>
family name	Token mapper	User Property	<input type="checkbox"/>
gender	Token mapper	User Attribute	<input type="checkbox"/>
Impersonator Username	Token mapper	User Session Note	<input type="checkbox"/>
phone number verified	Token mapper	User Attribute	<input type="checkbox"/>
locale	Token mapper	User Attribute	<input type="checkbox"/>
gss delegation credential	Token mapper	User Session Note	<input type="checkbox"/>
allowed web origins	Token mapper	Allowed Web Origins	<input type="checkbox"/>
middle name	Token mapper	User Attribute	<input type="checkbox"/>
nickname	Token mapper	User Attribute	<input type="checkbox"/>
updated at	Token mapper	User Attribute	<input type="checkbox"/>
email verified	Token mapper	User Property	<input type="checkbox"/>
email	Token mapper	User Property	<input type="checkbox"/>
client roles	Token mapper	User Client Role	<input type="checkbox"/>
Impersonator User ID	Token mapper	User Session Note	<input type="checkbox"/>
website	Token mapper	User Attribute	<input type="checkbox"/>
address	Token mapper	User Address	<input type="checkbox"/>
given name	Token mapper	User Property	<input type="checkbox"/>
profile	Token mapper	User Attribute	<input type="checkbox"/>
groups	Token mapper	User Realm Role	<input type="checkbox"/>
phone number	Token mapper	User Attribute	<input type="checkbox"/>
full name	Token mapper	User's full name	<input type="checkbox"/>
audience resolve	Token mapper	Audience Resolve	<input type="checkbox"/>
picture	Token mapper	User Attribute	<input type="checkbox"/>
upn	Token mapper	User Property	<input type="checkbox"/>
realm roles	Token mapper	User Realm Role	<input type="checkbox"/>
username	Token mapper	User Property	<input type="checkbox"/>

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Имя	Имя встроенного сопоставления	Текстовое значение

Наименование настройки	Описание	Тип настройки
Категория	Категория встроенного сопоставления	Текстовое значение
Тип	Тип встроенного сопоставления	Текстовое значение
Добавить	Добавить встроенное сопоставление	Чекбокс
Добавить выбранное	Добавление выбранных сопоставлений	Кнопка

Extended User Property

На рисунке ниже изображен интерфейс создания сопоставлений протоколов middleName_mapper

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование настройки	Описание	Тип настройки
Extended User Property	Передается отчество пользователя, если задано в профиле.	
Свойство	Имя свойства метода в интерфейсе ExtendedUserModel. Для примера, значение 'middleName' будет ссылкой на метод ExtendedUserModel.getMiddleName().	Текстовое значение
Имя переменной в токене	Имя переменной при добавлении ее в токен.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Область

Сопоставления ролей ограничивают роли, объявленные в токене доступа. Когда клиент запрашивает аутентификацию пользователя, получаемый им токен доступа содержит только те сопоставления ролей, которые явно указаны для области действия клиента. В результате ограничиваются полномочия каждого отдельного токена доступа вместо того, чтобы предоставить клиенту доступ ко всем полномочиям пользователей.

По умолчанию каждый клиент получает все сопоставления ролей пользователя. Сопоставления ролей доступны на вкладке Область каждого клиента.

На рисунке ниже изображено окно сопоставления областей для клиента.

Тест

Настройки Роли Шаблоны клиентов Сопоставления **Область** Отзыв Сессии Оффлайн доступ Установка

Тест Сопоставление областей

Полный доступ к областям

В таблице представлено детальное описание полей интерфейса сопоставления областей для клиента.

Наименование настройки	Описание	Тип настройки
Полный доступ к областям	Отключает все ограничения	Булевая

Отзыв

Возможность отзывать любые токены, выданные для клиента.

На рисунке ниже изображено окно отзыва токенов.

Тест

Настройки Роли Шаблоны клиентов Сопоставления Область **Отзыв** Сессии Оффлайн доступ Установка

Не ранее чем

Разослать

В таблице представлено детальное описание полей интерфейса отзыва токенов.

Наименование настройки	Описание	Тип настройки
Не ранее чем	Отозвать любые токены, выданные до указанной даты для этого клиента.	Текстовое поле, недоступное к ручному заполнению
Очистить	Очищает поле “Не ранее чем”	Кнопка
Установить на сейчас	Устанавливает в поле “Не ранее чем” значение текущей даты и времени	Кнопка
Разослать	Если URL системы администрации сконфигурирован для этого клиента, то необходимо послать политики этому клиенту.	Кнопка

Сессии

Просмотр сессий для этого клиента позволяет увидеть, какие пользователи активны и когда они вошли.

На рисунке ниже изображено окно просмотра активных сессий для клиента.

Тест



В таблице представлено детальное описание полей интерфейса просмотра активных сессий для клиента.

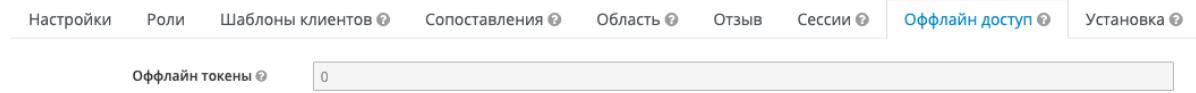
Наименование настройки	Описание	Тип настройки
Активные сессии	Общее количество активных сессий пользователей для этого клиента.	Поле, недоступное к ручному заполнению

Оффлайн доступ

Просмотр оффлайн сессий для этого клиента позволяет увидеть, какие пользователи получали оффлайн токен и когда они его получили. Чтобы выбрать все токены для этого клиента, перейдите на вкладку отзыва и установите значение в текущее время.

На рисунке ниже изображено окно просмотра оффлайн сессий для клиента.

Тест



В таблице представлено детальное описание полей интерфейса просмотра оффлайн сессий для клиента.

Наименование настройки	Описание	Тип настройки
Оффлайн токены	Общее количество оффлайн токенов для этого клиента.	Поле, недоступное к ручному заполнению

Установка

Вспомогательная утилита для генерации различных форматов конфигурации адаптера клиента, которые доступны для скачивания или копирования для конфигурации других клиентов.

На рисунке ниже изображена форма генерации различных форматов конфигурации адаптера клиента.

```
<secure-deployment name="WAR MODULE NAME.war">
<realm>master</realm>
<auth-server-url>http://localhost:18080/auth/</auth-server-url>
<public-client>true</public-client>
<ssl-required>EXTERNAL</ssl-required>
<resource>Test</resource>
</secure-deployment>
```

В таблице представлено детальное описание интерфейса генерации различных форматов конфигурации адаптера клиента.

Наименование настройки	Описание	Тип настройки
Формат	Выбор формата конфигурации адаптера клиента.	Выпадающий список
Скачать	По нажатию загружает конфигурации адаптера клиента в указанном формате	Кнопка
Поле	Конфигурации адаптера клиента	Текстовое поле

Управление Шаблонами клиентов

Если у системы много приложений, которые необходимо защитить и зарегистрировать в организации, настройка сопоставлений протоколов и ролей для каждого из этих клиентов может стать утомительной. KeyCloak.SE позволяет определить общую конфигурацию клиента в структуре, называемой клиентским шаблоном.

Клиентские шаблоны также обеспечивают поддержку параметра шаблона OAuth 2, который позволяет клиентскому приложению запрашивать больше или меньше утверждений, или ролей в токене доступа, в зависимости от потребностей приложения.

Шаблоны клиентов

Шаблоны клиентов позволяют определить основную конфигурацию, которая может быть общей между несколькими клиентами.

Чтобы создать шаблон клиента, выполните следующие действия:

- Перейдите в левый пункт меню Шаблоны клиентов. На этом начальном экране отображается список определенных в данный момент шаблонов клиентов.

- Нажмите кнопку Создать. Назовите область действия клиента и сохраните. Область клиента будет иметь вкладки, аналогичные вкладкам обычных клиентов. На вкладках можно определить сопоставления протоколов и сопоставления областей ролей, которые могут наследоваться другими клиентами, а также которые настроены для наследования от этой области клиента.

Имя	Протокол	Очередность в GUI	Действия
address	openid-connect		Редактировать Удалить
email	openid-connect		Редактировать Удалить
microprofile-jwt	openid-connect		Редактировать Удалить
offline_access	openid-connect		Редактировать Удалить
phone	openid-connect		Редактировать Удалить
profile	openid-connect		Редактировать Удалить
role_list	saml		Редактировать Удалить
roles	openid-connect		Редактировать Удалить
web-origins	openid-connect		Редактировать Удалить

Наименование настройки	Тип настройки
Поиск	Поисковое поле
Создать	Кнопка
Имя	Текстовое значение
Протокол	Текстовое значение
Очередность в GUI	Текстовое значение
Действия	Кнопки

Окно редактирования scope

Настройки

Настройки Сопоставления ? Область ?

Имя *	role_list
Описание	SAML role list
Протокол	openid-connect
Отображение на экране согласия	<input checked="" type="checkbox"/> ВКЛ
Текст Согласия	\$(samlRoleListScopeConsentText)
Включить в область действия токена	<input type="checkbox"/> ВЫК
Порядок GUI	
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Наименование настройки		Тип настройки
Имя		Текстовое значение
Описание		Текстовое значение
Протокол	Какая конфигурация протокола SSO будет поддержана шаблоном клиента	Список с возможностью выбора значений
Отображение на экране согласия	Если этот параметр включен, и эта клиентская область добавляется к какому-либо клиенту с требуемым соглашением, текст, указанный в «Текст экрана согласия», будет отображаться на экране согласия. Если выключено, эта клиентская область не будет отображаться на экране согласия	Булевая
Текст Согласия	Текст, который будет отображаться на экране согласия, когда эта клиентская область добавляется к какому-либо клиенту с требуемым соглашением. По умолчанию используется имя клиентской области, если она не заполнена	Текстовое значение
Включить в область действия токена	Если включено, имя этой клиентской области будет добавлено к свойству access_token «scope», а также к ответу от эндпойнта. Если выключено, эта клиентская область будет не будет в токене и в ответе эндпойнта.	Булевая
Порядок GUI	Укажите порядок поставщика в графическом интерфейсе (например, на странице согласия) как целое число	Текстовое значение

Сопоставления

При создании шаблона клиента необходимо выбрать сопоставления. Только клиенты, использующие те же сопоставления, могут быть связаны с этим шаблоном клиентов.

После создания нового реалма, в меню появится список предопределенных (встроенных) клиентских областей.

Для протокола SAML существует один встроенный клиентский диапазон, список ролей, который содержит один протокольный mapper для отображения списка ролей в утверждении SAML.

Для протокола OpenID Connect существуют клиентские диапазоны profile, email, address, phone, offline_access, roles, web-origins и microprofile-jwt.

Шаблон клиента offline_access полезен, когда клиент хочет получить автономные токены.

Клиентские области profile, email, address и phone также определены в спецификации OpenID Connect. Для этих клиентских областей не определены сопоставления ролей, но определены сопоставления протоколов, и эти сопоставления соответствуют утверждениям, определенным в спецификации OpenID Connect.

Общее окно с mapper scope

Поиск... 					Создать	Добавить встроенные
Имя	Категория	Тип	Priority Order	Действия		
address	Token mapper	User Address	0	Редактировать	Удалить	

Наименование настройки		Тип настройки
Поиск	Полнотекстовый поиск scope	Поисковое поле
Создать	Кнопка создания клиентского scope	Кнопка
Добавить встроенные	Добавить встроенный	Кнопка
Имя	Наименование scope	Текстовое значение (с возможностью перехода в окно редактирования)
Категория	Категория scope	Текстовое значение
Тип	Тип scope	Текстовое значение
Priority Order	Приоритетность	Текстовое значение
Действия	Возможные действия (Редактировать, Удалить)	Кнопки

Окно редактирования mapper scope

Протокол	openid-connect
ID	72273ef5-ab1e-4b94-8be9-14a51d42c44e
Имя	realm roles
Тип сопоставления	User Realm Role
Префикс ролей Realm	
Несколько значений	<input checked="" type="checkbox"/>
Имя переменной в токене	realm_access.roles
Тип переменной JSON	String
Добавить в токен ID	<input type="checkbox"/> ВЫК
Добавить в токен доступа	<input checked="" type="checkbox"/>
Добавить в информацию о пользователе	<input type="checkbox"/> ВЫК
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Наименование настройки		Тип настройки
Протокол	Протокол, под который будет создано сопоставление	Фиксированное
ID	Уникальный идентификатор	Фиксированное
Имя	Наименование сопоставления	Текстовое значение
Тип сопоставления	Тип сопоставления	Список с возможностью выбора значений
Префикс ролей Realm	Префикс для каждой роли Realm (опционально).	Текстовое значение
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Список с возможностью выбора значений
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая

Наименование настройки	Описание	Тип настройки
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Область

Сопоставление области позволяет ограничить сопоставленные роли пользователя, включаемые вместе с токеном доступа, запрошенного клиентом.

[Шаблоны клиентов](#) > [roles](#)

Roles

Настройки Сопоставления ? Область ?

roles Сопоставление областей

Роли Realm

Доступные роли ⓘ
Enter part of role name...
default-roles-test
offline_access
uma_authorization
a

Присвоенные роли ⓘ
Enter part of role name...

Назначенные роли ⓘ

Добавить выбранное »

« Удалить выбранное

Роли интегрированных систем

Выберите клиента для просмотра его ролей

Наименование настройки	Описание	Тип настройки
Роли Realm	Доступные роли	Поле с выбором значения
Присвоенные роли	Роли уровня Realm, присвоенные области.	Поле с выбором значения
Назначенные роли	Назначенные роли уровня realm, которые могут быть унаследованы из составной роли.	Текстовое поле
Добавить выбранное		Кнопка для добавления выбранных ролей в ассоциированные роли
Удалить выбранное		Кнопка для удаления ролей из ассоциированных ролей

Наименование настройки		Описание	Тип настройки
Роли интегрированных систем		Выбор клиента для просмотра его ролей	Выпадающий список

Клиентские области по умолчанию

Клиентские области, которые будут автоматически добавлены каждому созданному клиенту

Протокол ⓘ openid-connect

ID ⓘ 72273ef5-ab1e-4b94-8be9-14a51d42c44e

Имя ⓘ realm roles

Тип сопоставления ⓘ User Realm Role

Предфикс ролей Realm ⓘ

Несколько значений ⓘ ВКЛ

Имя переменной в токене ⓘ realm_access.roles

Тип переменной JSON ⓘ String

Добавить в токен ID ⓘ ВЫК

Добавить в токен доступа ⓘ ВКЛ

Добавить в информацию о пользователе ⓘ ВЫК

Сохранить **Отмена**

Наименование настройки		Описание	Тип настройки
Клиентские области по умолчанию		Области клиента по умолчанию всегда применяются при выдаче токенов для этого клиента. Сопоставители протоколов и сопоставления областей ролей применяются всегда, независимо от значения используемого параметра области в запросе авторизации OIDC.	
	Доступные клиентские области	Области действия клиента, которые еще не назначены как области по умолчанию или дополнительные области	Поле с выбором значения
	Назначенные клиентские области по умолчанию	Области действия клиента, которые будут использоваться в качестве областей действия по умолчанию при создании токенов для этого клиента.	Поле с выбором значения

Наименование настройки		Описание	Тип настройки
		Кнопка для добавления выбранных клиентских областей в назначенные клиентские области по умолчанию	Кнопка
		Кнопка для удаления выбранных назначенных клиентских областей по умолчанию	Кнопка
Опциональные клиентские области		Необязательные клиентские области действия применяются при выдаче токенов для этого клиента, на случай, когда они запрашиваются параметром области в запросе авторизации OIDC	
	Доступные клиентские области	Области действия клиента, которые еще не назначены как области по умолчанию или дополнительные области	Поле с выбором значения
	Назначенные дополнительные клиентские области	Области действия клиента, которые могут использоваться как дополнительные области при генерации токенов для этого клиента	Поле с выбором значения
	Добавить выбранное	Кнопка для добавления выбранных клиентских областей	Кнопка
	Удалить выбранное	Кнопка для удаления выбранных клиентских областей	Кнопка

Управление Ролями

Роли определяют тип или категорию пользователей. Администратор, пользователь, менеджер и сотрудник – все это типичные роли, которые могут существовать в организации. Приложения часто назначают доступ и разрешения конкретным ролям, а не отдельным пользователям, поскольку работа с пользователями может быть слишком детальной и сложной для управления.

Существует глобальное пространство имен для ролей, и у каждого клиента также есть свое собственное выделенное пространство имен, в котором могут быть определены роли.

Роли Realm

Роли уровня realm – это пространство имен для определения ролей на уровне realm. Для просмотра списка ролей, необходимо выбрать вкладку “Роли” в меню.

В master-realm есть две роли уровня realm. Это:

- admin;

- **create-realm.** Пользователи с ролью admin являются суперпользователями и имеют полный доступ к управлению любым realm на сервере. Пользователи с ролью create-realm могут создавать новые realms. Им будет предоставлен полный доступ к любому новому realm, который они создадут.

Пользователи-администраторы в master realm могут получить привилегии управления одним или несколькими другими realm в системе. Каждый realm в Keycloak представлен клиентом в master realm. Имя клиента - -realm. У каждого из этих клиентов определены роли клиентского уровня, которые определяют различный уровень доступа к управлению отдельным realm.

Наименование роли realm	Описание роли
admin	Суперадминистратор
create-realm	Позволяет создавать realms
default-roles-master	Позволяет управлять ролями по умолчанию
offline_access	Позволяет управлять offline-доступом
uma_authorization	Позволяет управлять авторизацией

Наименование настройки	Описание	Тип настройки
Поиск	Полнотекстовый поиск ролей	Поисковое поле
Добавить роль	Кнопка создания роли	Кнопка
Наименование роли	Наименование роли	Текстовое значение (с возможностью перехода в окно редактирования)
Составная	Признак композитной роли	Булевая
Описание	Описание роли	Текстовое значение

Наименование настройки	Описание	Тип настройки
Действия	Возможные действия (Редактировать, Удалить)	Кнопки

Добавление роли

Добавить роль

Наименование роли *

Описание

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Наименование роли	Поле для ввода наименования роли клиента	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение

Окно редактирования роли

Детали

Тестовая Роль

[Детали](#) [Атрибуты](#) [Пользователи с ролью](#)

Наименование роли	<input type="text" value="Тестовая роль"/>
Описание	<input type="text"/>
Составные роли	<input checked="" type="checkbox"/> Вкл <input type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

▼ Составные роли

Роли Realm <table border="1"> <tr> <td>Доступные роли </td> </tr> <tr> <td><input type="text" value="Enter part of role name..."/></td> </tr> <tr> <td>Test Test1 admin create-realm default-roles-master offline_access ttt uma_authorization</td> </tr> <tr> <td><input type="button" value="Добавить выбранное >"/></td> </tr> </table>	Доступные роли	<input type="text" value="Enter part of role name..."/>	Test Test1 admin create-realm default-roles-master offline_access ttt uma_authorization	<input type="button" value="Добавить выбранное >"/>	Ассоциированные роли <table border="1"> <tr> <td><input type="text" value="Enter part of role name..."/></td> </tr> <tr> <td><input type="button" value="« Удалить выбранное»"/></td> </tr> </table>	<input type="text" value="Enter part of role name..."/>	<input type="button" value="« Удалить выбранное»"/>
Доступные роли							
<input type="text" value="Enter part of role name..."/>							
Test Test1 admin create-realm default-roles-master offline_access ttt uma_authorization							
<input type="button" value="Добавить выбранное >"/>							
<input type="text" value="Enter part of role name..."/>							
<input type="button" value="« Удалить выбранное»"/>							

Наименование настройки	Описание	Тип настройки
Наименование роли	Отображение наименования роли	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение
Составные роли	Когда эта роль (не)ассоциирована с любой ролью пользователей, она (не)будет неявно ассоциирована.	Кнопка
Роли Realm		
Доступные роли	Роли уровня Realm, ассоциированные с этой составной ролью.	Поле с выбором значения
Ассоциированные роли	Роли уровня Realm, ассоциированные с составными ролями.	Поле с выбором значения
Добавить выбранное	Кнопка для добавления выбранных ролей в ассоциированные роли	Кнопка
Удалить выбранное	Кнопка для удаления ролей из ассоциированных ролей	Кнопка

Атрибуты

Возможность добавления атрибутов роли

Наименование настройки	Описание	Тип настройки
Ключ	Поле для ввода ключа, определяющего атрибут настройки	Текстовое поле
Значение	Поле для ввода значения, задающегося атрибуту настройки	Текстовое поле
Действие		
Добавить	Кнопка добавления связки ключ-значения	Кнопка

Пользователи с ролью

Позволяет посмотреть пользователей, имеющих данную роль.

Наименование настройки	Описание	Тип настройки
Пользователи с ролью	Перечисление пользователей с данной ролью	Текстовое поле

Роли по умолчанию

Позволяет выбирать стандартные роли Realm с добавлением композитных.

Роли

Роли Realm Роли по умолчанию

Роли Realm <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Доступные роли <ul style="list-style-type: none"> admin create-realm Name Test Test1 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Добавить выбранное > </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Роли интегрированных систем <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Доступные роли <ul style="list-style-type: none"> delete-account manage-account-links manage-consent Test view-applications </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Добавить выбранное > </div> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> account </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Роли Realm по умолчанию <ul style="list-style-type: none"> offline_access uma_authorization </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> «Удалить выбранное» </div>
--	---

Наименование настройки		Описание	Тип настройки
Роли Realm			
	Доступные роли	Роли уровня Realm, которые могут быть назначены.	Список с возможностью выбора значения
	Роли Realm по умолчанию	Роли уровня Realm, которые могут быть назначены новым пользователям.	Список с возможностью выбора значения
Роли интегрированных систем			Выпадающий список
	Доступные роли	Роли из этого клиента, которые могут быть назначены по умолчанию.	Список с возможностью выбора значения
	Роли клиента по умолчанию	Роли из этого клиента, назначенные как роли по умолчанию.	Список с возможностью выбора значения

Управление Поставщиками идентификации

Управление Федерацией пользователей

Управление Федерацией пользователей

Чтобы начать работу, выберите провайдера из выпадающего списка. Ниже изображено окно добавления провайдера федерации пользователей.

The screenshot shows the Keycloak administration interface with the title 'PLATFORM V'. The left sidebar is titled 'Master' and contains the following sections:

- Конфигурация**:
 - Настройки Realm
 - Клиенты
 - Шаблоны клиентов
 - Роли
 - Поставщики идентификации
 - Федерация пользователей** (highlighted with a blue border)
 - Аутентификация
- Управление**:
 - Группы
 - Пользователи
 - Сессии
 - События
 - Импорт
 - Экспорт
 - Очистить кэш
 - Синхронизация ролей и ФОС

The main content area is titled 'Федерация пользователей' and displays the following information:

- A large circular icon representing a database.
- The title 'Федерация пользователей'.
- A note: 'Keycloak can federate external user databases. Out of the box we have support for LDAP and Active Directory.'
- A sub-note: 'To get started select a provider from the dropdown below.'
- A dropdown menu labeled 'Добавить поставщика...' with a downward arrow.

kerberos

Требуемые настройки:

Требуемые настройки

Включено 

ВКЛ

Наименование в
консоли 

kerberos

Приоритет 

0

* Kerberos Realm 

* Основной сервер


* KeyTab 

Отладчик 

ВЫК

Разрешить
аутентификацию
по паролю 

ВКЛ

Режим
редактирования 

READ_ONLY



Обновить профиль
при первом входе


ВЫК

Настройки кэширования EVICT_DAILY:

Настройки кэширования

Политики
кэширования ?

EVICT_DAILY ▾

Час исключения ?

▾

Минута
исключения ?

▾

Сохранить Отмена

Настройки кэширования EVICT_WEEKLY:

Настройки кэширования

Политики
кэширования ?

EVICT_WEEKLY ▾

День исключения

?

▾

Час исключения ?

▾

Минута
исключения ?

▾

Сохранить Отмена

Настройки кэширования MAX_LIFESPAN:

Настройки кэширования

Политики кэширования **MAX_LIFESPAN**

Максимальное время жизни

Сохранить **Отмена**

Настройки кэширования NO_CACHE:

Настройки кэширования

Политики кэширования **NO_CACHE**

Сохранить **Отмена**

В таблице представлено детальное описание интерфейса настройки службы хранилища пользователей.

Наименование настройки	Описание	Тип настройки
Включено	Если поставщик отключен, он не будет учитываться для запросов, а импортированные пользователи будут отключены и доступны только для чтения до тех пор, пока поставщик снова не будет включен.	Булевая
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое значение
Приоритет	Приоритет службы при поиске пользователя. Вперед идут более низкие значения.	Текстовое значение
Kerberos Realm	Наименование kerberos realm. Например FOO.ORG	Текстовое значение
Основной сервер	Полное имя основного сервера для HTTP сервиса, включая серверное и доменное имя. Например HTTP/host.foo.org@FOO.ORG	Текстовое значение
KeyTab	Местоположение файла KeyTab в Kerberos, содержащего учетные данные основного сервера. Например /etc/krb5.keytab	Текстовое значение

Наименование настройки	Описание	Тип настройки
Отладчик	Включить/выключить отладочные логи в стандартный вывод для Krb5LoginModule.	Булевая
Разрешить аутентификацию по паролю	Включить/выключить возможность аутентификации по имени/пароля вопреки базе данных Kerberos	Булевая
Режим редактирования	READ_ONLY означает, что обновление пароля не допускается и пользователь всегда аутентифицируется с паролем Kerberos. UNSYNCED означает, что пользователь может изменить свой пароль в базе данных Keycloak и тогда он будет использован вместо пароля Kerberos	Список с возможностью выбора значений
Обновить профиль при первом входе	Обновить профиль при первом входе	Булевая
Политики кэширования	Политики кэширования для этого поставщика хранения. 'DEFAULT' представляет настройки по умолчанию для глобального пользовательского кэша. 'EVICT_DAILY' время каждого дня, после которого пользовательский кэш инвалидируется. 'EVICT_WEEKLY' день и время недели после которого пользовательский кэш инвалидируется. 'MAX-LIFESPAN' время в миллисекундах, в течение которого будет существовать жизненный цикл записи в кэше.	Список с возможностью выбора значений
EVICT_DAILY		
Час исключения	Час дня, в который запись станет недействительной.	Выпадающий список
Минута исключения	Минута дня, в которую запись станет недействительной.	Выпадающий список
EVICT_WEEKLY		
День исключения	День недели в который запись станет недействительной и будет исключена из кэша.	Выпадающий список
Час исключения	Час дня, в который запись станет недействительной.	Выпадающий список
Минута исключения	Минута дня, в которую запись станет недействительной.	Выпадающий список
MAX_LIFESPAN		
Максимальное время жизни	Максимальное время жизни записи пользовательского кэша в секундах.	Выпадающий список
NO_CACHE		

ldap

Требуемые настройки

Ниже изображен интерфейс обязательных настроек службы федерации пользователей.

Добавить службу федерации пользователей

Требуемые настройки

The screenshot shows the configuration interface for the 'ldap' service. It includes the following fields:

- Включено**: ВКЛ (Enabled) - checked.
- Наименование в консоли**: ldap
- Приоритет**: 0
- Импортировать пользователей**: ВКЛ (Enabled) - checked.
- Режим редактирования**: READ_ONLY
- Синхронизировать регистрацию**: ВЫК (Disabled) - checked.
- * Поставщик**: Active Directory
- * Атрибут Username в LDAP**: cn
- * Атрибут RDN в LDAP**: cn
- * Атрибут UUID в LDAP**: objectGUID
- * Классы объектов пользователя**: person, organizationalPerson, user
- * URL соединения**: URL соединения с LDAP
- * Пользователи DN**: Пользователи DN LDAP
- Пользовательский Фильтр LDAP пользователей**: LDAP фильтр
- Поиск области**: One Level
- * Тип аутентификации**: simple
- * Сопоставление DN**: Сопоставление DN LDAP
- * Сопоставление учетных данных**: (with a browse icon)

Buttons at the bottom right include **Тест соединения** (Test connection) and **Проверка аутентификации** (Authentication check).

В таблице представлено детальное описание интерфейса настройки службы федерации пользователей.

Наименование настройки	Описание	Тип настройки
Включено	Если поставщик отключен, он не будет учитываться для запросов, а импортированные пользователи будут отключены и доступны только для чтения до тех пор, пока поставщик снова не будет включен.	Булевая
Наименование в консоли	Отображаемое имя службы, связанное с консолью администратора.	Текстовое поле

Наименование настройки	Описание	Тип настройки
Приоритет	Приоритет службы при поиске пользователя. Вперед идут более низкие значения.	Текстовое поле
Импортировать пользователей	Если включено, пользователи LDAP будут импортированы в базу данных Keycloak и синхронизированы через сконфигурированные политики синхронизации.	Булевая
Режим редактирования	READ_ONLY означает доступ только на чтение из LDAP. WRITABLE означает, что данные будут обратно синхронизированы в LDAP по заявке. UNSYNCED означает, что данные пользователя будут импортированы, но не синхронизированы обратно в LDAP.	Выпадающий список
Синхронизировать регистрацию	Должны ли вновь созданные пользователи быть созданы в хранилище LDAP? Приоритет определяет какой из поставщиков будет выбран для синхронизации нового пользователя.	Булевая
Поставщик	LDAP поставщик (провайдер)	Выпадающий список
Атрибут Username в LDAP	Наименование LDAP атрибута, которое отображается как имя пользователя в Keycloak. Для множества серверов LDAP это может быть 'uid'. Для Active directory это может быть 'sAMAccountName' или 'cn'. Атрибут должен быть заполнен для всех LDAP записей пользователей, которые необходимо импортировать из LDAP в Keycloak.	Текстовое поле
Атрибут RDN в LDAP	Наименование атрибутов LDAP, которое используется как RDN (верхний атрибут) обычного пользователя DN. Обычно оно такое же, как атрибут имени пользователя LDAP, однако он не обязателен. Для примера, для Active directory обычно используется 'cn' как атрибут RDN, в то время как атрибут имени пользователя может быть 'sAMAccountName'.	Текстовое поле
Атрибут UUID в LDAP	Наименование LDAP атрибута, которое используется как уникальный идентификатор объектов (UUID) в LDAP. Для множества LDAP серверов это 'entryUUID' однако некоторые могут отличаться. Для примера, для Active directory он должен быть 'objectGUID'. Если LDAP сервер действительно не поддерживает понятие UUID, есть возможность использовать любой другой атрибут, который должен быть уникальным среди пользователей в дереве LDAP. Например 'uid' или 'entryDN'.	Текстовое поле
Классы объектов пользователя	Все значения из LDAP objectClass атрибутов для пользователей в LDAP, разделенные запятой. Например: 'inetOrgPerson, organizationalPerson'. Вновь созданные пользователи Keycloak будут записаны в LDAP вместе с этими классами объектов, а существующие записи пользователей LDAP будут найдены только если они содержат все эти классы объектов.	Текстовое поле
URL соединения	URL соединения с сервером LDAP	Текстовое поле
Тест соединения		Кнопка

Наименование настройки	Описание	Тип настройки
Пользователи DN	Полный DN из дерева LDAP где присутствуют пользователи. Этот DN является родителем пользователей LDAP. Он может быть, для примера 'ou=users,dc=example,dc=com' при условии, что обычный пользователь будет иметь DN похожий на 'uid=john,ou=users,dc=example,dc=com'	Текстовое поле
Пользовательский Фильтр LDAP пользователей		
Поиск области	Для одного уровня мы ищем пользователей только в DN, определенных как пользовательские DN. Для поддеревьев мы ищем полностью в их поддеревьях. Смотрите документацию LDAP для подробных деталей	Выпадающий список
Тип аутентификации	Тип LDAP аутентификации. Сейчас доступны только механизмы 'none' (анонимная аутентификация LDAP) или 'simple' (Аутентификация по сопоставленным логину и паролю)	Выпадающий список
Сопоставление DN	DN администратора LDAP, которые будут использованы Keycloak для доступа на сервер LDAP	Текстовое поле
Сопоставление учетных данных	Пароль администратора LDAP	Текстовое поле
Проверка аутентификации		Кнопка

Advanced Settings

Ниже изображен интерфейс расширенных настроек службы федерации пользователей.

Advanced Settings

Включить StartTLS ⓘ ВЫК

Enable the LDAPv3 Password Modify Extended Operation ⓘ ВЫК

Query Supported Extensions ⓘ

Validate Password Policy ⓘ ВЫК

Подтверждение E-mail ⓘ ВЫК

Использование доверенных сертификатов SPI ⓘ Only for ldaps

Таймаут соединения ⓘ Таймаут соединения

Таймаут чтения ⓘ Таймаут чтения

Постстраничный вывод ⓘ ВКЛ

В таблице представлено детальное описание расширенных настроек службы федерации пользователей.

Наименование настройки	Описание	Тип настройки
Включить StartTLS	Шифрует соединение с LDAP с помощью STARTTLS, что отключит пул соединений.	Булевая
Enable the LDAPv3 Password Modify Extended Operation	Используйте расширенную операцию изменения пароля LDAPv3 (RFC-3062). Расширенная операция изменения пароля обычно требует, чтобы у пользователя LDAP уже был пароль на сервере LDAP. Поэтому, когда это используется с “Синхронизацией регистраций”, может быть полезно добавить также “Жестко закодированный атрибут LDAP, сопоставленный” со случайно сгенерированным начальным паролем.	Булевая
Query Supported Extensions	Позволяет запросить у сервера LDAP поддерживаемые расширения, элементы управления и функции. Затем некоторые дополнительные параметры поставщика LDAP будут автоматически настроены на основе возможностей/расширений/функций, поддерживаемых сервером LDAP. Например, если расширение LDAPv3 для изменения пароля поддерживается сервером LDAP, соответствующий переключатель будет включен для поставщика LDAP.	Кнопка
Validate Password Policy	Определяет, должен ли Keycloak проверять пароль с помощью политики паролей realm перед его обновлением	Булевая
Подтверждение E-mail	Если включено, то E-mail, предоставленный этим поставщиком не будет подтвержденным даже если подтверждение включено для realm.	Булевая
Использование доверенных сертификатов SPI	Определяет, будет ли соединение с LDAP использовать хранилище доверенных сертификатов SPI вместе с сертификатами, сконфигурированными в keycloak-server.json. ‘Всегда’ означает, что они будут использоваться всегда. ‘Никогда’ означает, что они никогда не будут использованы. ‘Только для ldap’ означает, что они будут использованы вместе с настроенными соединениями к ldap серверам. Обратите внимание, что если keycloak-server.json не сконфигурирован, то по умолчанию Java будет использовать cacerts или сертификат, определенный в ‘javax.net.ssl.trustStore’.	Выпадающий список
Тайм-аут соединения	Тайм-аут соединения с LDAP в миллисекундах	Текстовое поле
Тайм-аут чтения	Тайм-аут чтения из LDAP в миллисекундах. Этот тайм-аут применяется к операциям чтения из LDAP	Текстовое поле
Постраничный вывод	Должен ли LDAP сервер поддерживать постраничный вывод.	Булевая

Пул соединений

Ниже изображен интерфейс пула соединений.

✓ Пул соединений

Пул соединений <small>?</small>	<input checked="" type="checkbox"/> Вкл
Connection Pooling Authentication <small>?</small>	none simple
Connection Pool Debug Level <small>?</small>	off
Connection Pool Initial Size <small>?</small>	1
Connection Pool Maximum Size <small>?</small>	1000
Connection Pool Preferred Size <small>?</small>	5
Connection Pool Protocol <small>?</small>	plain ssl
Connection Pool Timeout <small>?</small>	300000

В таблице представлено детальное описание интерфейса пула соединений.

Наименование настройки	Описание	Тип настройки
Включить StartTLS	Шифрует соединение с LDAP с помощью STARTTLS, что отключит пул соединений.	Булевая
Enable the LDAPv3 Password Modify Extended Operation	Используйте расширенную операцию изменения пароля LDAPv3 (RFC-3062). Расширенная операция изменения пароля обычно требует, чтобы у пользователя LDAP уже был пароль на сервере LDAP. Поэтому, когда это используется с “Синхронизацией регистраций”, может быть полезно добавить также “Жестко закодированный атрибут LDAP, сопоставленный” со случайно сгенерированным начальным паролем.	Булевая
Query Supported Extensions	Позволяет запросить у сервера LDAP поддерживаемые расширения, элементы управления и функции. Затем некоторые дополнительные параметры поставщика LDAP будут автоматически настроены на основе возможностей/расширений/функций, поддерживаемых сервером LDAP. Например, если расширение LDAPv3 для изменения пароля поддерживается сервером LDAP, соответствующий переключатель будет включен для поставщика LDAP.	Кнопка
Validate Password Policy	Определяет, должен ли Keycloak проверять пароль с помощью политики паролей realm перед его обновлением	Булевая
Подтверждение E-mail	Если включено, то E-mail, предоставленный этим поставщиком не будет подтвержденным даже если подтверждение включено для realm.	Булевая

Наименование настройки	Описание	Тип настройки
Использование доверенных сертификатов SPI	Определяет, будет ли соединение с LDAP использовать хранилище доверенных сертификатов SPI вместе с сертификатами, сконфигурированными в keycloak-server.json. ‘Всегда’ означает, что они будут использоваться всегда. ‘Никогда’ означает, что они никогда не будут использованы. ‘Только для ldap’ означает, что они будут использованы вместе с настроенными соединениями к ldap серверам. Обратите внимание, что если keycloak-server.json не сконфигурирован, то по умолчанию Java будет использовать cacerts или сертификат, определенный в ‘javax.net.ssl.trustStore’.	Выпадающий список
Тайм-аут соединения	Тайм-аут соединения с LDAP в миллисекундах	Текстовое поле
Тайм-аут чтения	Тайм-аут чтения из LDAP в миллисекундах. Этот тайм-аут применяется к операциям чтения из LDAP	Текстовое поле
Постраничный вывод	Должен ли LDAP сервер поддерживать постраничный вывод.	Булевая

Интеграция с Kerberos

Ниже изображен интерфейс настройки интеграции с Kerberos.

▼ Интеграция с Kerberos

Разрешить аутентификацию Kerberos

* Kerberos Realm

* Основной сервер

* KeyTab

Отладчик ВЫК

Использовать Kerberos для аутентификации по паролю ВЫК

В таблице представлено детальное описание интерфейса интеграции с Kerberos.

Интеграция с Kerberos		
Размер пачки	Количество пользователей LDAP, которые будут импортированы в Keycloak за одну транзакцию.	Текстовое поле

Интеграция с Kerberos		
Периодическая полная синхронизация	Должна ли быть включена полная периодическая синхронизация пользователей LDAP в Keycloak или нет	Булевая
Период полной синхронизации	Период для полной синхронизации в секундах	Текстовое поле
Периодическая синхронизация изменений пользователей	Должна ли быть включена периодическая синхронизация новых и измененных пользователей LDAP в Keycloak или нет	Булевая
Период синхронизации измененных пользователей	Период для синхронизации измененных или вновь созданных пользователей LDAP в секундах	Текстовое поле

Настройки кэширования

Настройки кэширования EVICT_DAILY:

Настройки кэширования

Политики кэширования ? EVICT_DAILY ▾

Час исключения ? 0 ▾

Минута исключения ? 0 ▾

Сохранить **Отмена**

Настройки кэширования EVICT_WEEKLY:

Настройки кэширования

Политики кэширования <small>?</small>	EVICT_WEEKLY <small>▼</small>
День исключения <small>?</small>	<input type="text"/>
Час исключения <small>?</small>	<input type="text"/>
Минута исключения <small>?</small>	<input type="text"/>
Сохранить Отмена	

Настройки кэширования MAX_LIFESPAN:

Настройки кэширования

Политики кэширования <small>?</small>	MAX_LIFESPAN <small>▼</small>
Максимальное время жизни <small>?</small>	<input type="text"/>
Сохранить Отмена	

Настройки кэширования NO_CACHE:

Настройки кэширования

Политики кэширования <small>?</small>	NO_CACHE <small>▼</small>
Сохранить Отмена	

В таблице представлено детальное описание интерфейса настройки кэширования.

Наименование настройки	Описание	
Тип настройки		
Политики кэширования	Политики кэширования для этого поставщика хранения. 'DEFAULT' представляет настройки по умолчанию для глобального пользовательского кэша. 'EVICT_DAILY' время каждого дня, после которого пользовательский кэш инвалидируется. 'EVICT_WEEKLY' день и время недели после которого пользовательский кэш инвалидируется. 'MAX-LIFESPAN' время в миллисекундах, в течение которого будет существовать жизненный цикл записи в кэше.	Список с возможностью выбора значений
EVICT_DAILY		
Час исключения	Час дня, в который запись станет недействительной.	Выпадающий список
Минута исключения	Минута дня, в которую запись станет недействительной.	Выпадающий список
EVICT_WEEKLY		
День исключения	День недели в который запись станет недействительной и будет исключена из кэша.	Выпадающий список
Час исключения	Час дня, в который запись станет недействительной.	Выпадающий список
Минута исключения	Минута дня, в которую запись станет недействительной.	Выпадающий список
MAX_LIFESPAN		
Максимальное время жизни	Максимальное время жизни записи пользовательского кэша в секундах.	Выпадающий список
NO_CACHE		

Управление Аутентификацией

Есть несколько функций, о которых следует знать при настройке аутентификации области. Во многих организациях действуют строгие политики паролей и OTP, которые можно применять с помощью настроек в консоли администратора. Могут потребоваться или не потребоваться различные типы учетных данных для аутентификации. Возможно, возникнет потребность предоставить пользователям возможность входа в систему через Kerberos или отключить или включить различные встроенные типы учетных данных.

Для управления аутентификацией перейдите в пункт меню Аутентификация, находящийся в меню слева.

Сценарии

Позволяет создавать flow и части flow(execution).

На рисунке ниже изображено окно представления сценариев и сценариев исполнения аутентификации.

Тип аутентификации	Требования		
Cookie	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED		
Kerberos	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input checked="" type="radio"/> DISABLED		
Identity Provider Redirector	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED		Действия
Forms	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input type="radio"/> CONDITIONAL		
Username Password Form	<input checked="" type="radio"/> REQUIRED		
Browser - Conditional OTP	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input checked="" type="radio"/> CONDITIONAL		
	Condition - User Configured	<input checked="" type="radio"/> REQUIRED <input type="radio"/> DISABLED	
	OTP Form	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED	

В таблице представлено детальное описание интерфейса представления сценариев и сценариев исполнения аутентификации.

Наименование настройки	Описание	Тип настройки
Выбор сценария аутентификации Browser	аутентификация на основе браузера	Выпадающий список
Выбор сценария аутентификации Registration	сценарий регистрации	Выпадающий список
Выбор сценария аутентификации Reset Credentials	Сброс учетных данных для пользователя, если он забыл свой пароль или что-то еще	Выпадающий список
Выбор сценария аутентификации Clients	Базовая аутентификация для клиентов	Выпадающий список
Выбор сценария аутентификации First Broker Login	Действия, выполняемые после первого входа в систему брокера с учетной записью поставщика удостоверений, которая еще не связана ни с одной учетной записью Keycloak	Выпадающий список

Наименование настройки	Описание	Тип настройки
Выбор сценария аутентификации Docker Auth	Используется клиентами Docker для аутентификации по IDP	Выпадающий список
Выбор сценария аутентификации Http Challenge	Поток аутентификации, основанный на схемах HTTP-аутентификации “вызов-ответ”.	Выпадающий список
Тип аутентификации	Отображение типа аутентификации	Таблица с фиксированным текстовым значением
Требования	Отображение настроек требований сценария аутентификации	Таблица с чекбоксами
Действия	Кнопки действия: Создать, Копировать, Конфигурация.	Кнопки

Required

Все необходимые элементы в потоке должны быть успешно последовательно выполнены. Поток завершается, если требуемый элемент выходит из строя.

Alternative

Когда поток содержит только Альтернативные элементы, только один элемент должен быть оценен как успешный, чтобы поток был признан успешным. Поскольку Требуемых элементов в потоке достаточно, чтобы отметить поток как успешный, любой Альтернативный элемент в потоке, который содержит Требуемые элементы потока, никогда не будет выполнен. В этом случае они функционально отключены.

Disabled

Любой элемент Disabled не оценивается и не учитывается для отметки потока как успешного.

Conditional

Этот тип требования может быть установлен только для подпотоков. Условный подпоток может содержать выполнение “Условие”. Эти исполнения “Условие” должны оцениваться как логические операторы. Если все выполнения “Условие” оцениваются как истинные, то Условный подпоток действует как Требуемый. Если нет, то Условный подпоток действует как Отключен. Если ни одно выполнение “Условие” не установлено, Условный подпоток действует как Отключен. Если поток содержит выполнение “Условие” и не установлен на Условное, то выполнение “Условие” не оценивается и может считаться функционально отключенным.

Это лучше описать на примере:

Первый тип аутентификации - Cookie. Когда пользователь успешно входит в систему в первый раз, устанавливается сессионный файл cookie. Если этот файл cookie уже был установлен, то данный тип аутентификации будет успешным. В данном случае, поскольку поставщик cookie вернул успех, а каждое выполнение на этом уровне потока является альтернативным, никакое другое выполнение не выполняется, что приводит к успешному входу в систему.

Второе выполнение потока рассматривает выполнение Kerberos. Этот аутентификатор отключен по умолчанию и будет пропущен.

Третье выполнение – это перенаправление поставщика идентификационных данных. Его можно настроить через ссылку Действия > Конфигурация для автоматического перенаправления на другой IdP для посредничества в идентификации.

Следующим выполнением является подпоток под названием Forms. Поскольку этот подпоток помечен как альтернативный, он не будет выполняться, если пройден тип аутентификации Cookie. Этот подпоток содержит дополнительный тип аутентификации, который должен быть выполнен. Выполнения для этого подпотока загружаются, и происходит та же логика обработки.

Первое выполнение в подпотоке Forms – это форма Username Password. Этот тип аутентификации отображает страницу имени пользователя и пароля. Он помечен как обязательный, поэтому пользователь должен ввести правильное имя пользователя и пароль.

Второе выполнение в подпотоке Forms – это новый подпоток: Browser - Conditional OTP. Поскольку этот подпоток является условным, его выполнение зависит от результата оценки выполнения Condition - User Configured. Если да, то загружается выполнение для этого подпотока и происходит та же логика обработки.

Следующим выполнением является Condition - User Configured. Здесь проверяется, настроены ли другие исполнения в потоке для пользователя. Это означает, что подпоток Browser - Conditional OTP будет выполнен только в том случае, если у пользователя настроена учетная запись OTP.

Последнее выполнение – это форма OTP. Она отмечена как необходимая, но из-за настройки в условном подпотоке она будет запущена только в том случае, если у пользователя настроена учетная запись OTP. В противном случае пользователь не увидит форму OTP.

Создать верхнеуровневую форму

Есть несколько вариантов создания потока:

1. Скопировать, а затем изменить существующий поток. Для этого выберите существующий поток (например, поток Browser) и нажмите кнопку Копировать. После этого вам будет предложено задать имя для нового потока, а затем создать его.

2. Создать новый поток с нуля. Для этого нажмите кнопку Создать.

При создании нового потока необходимо создать поток верхнего уровня (см. рисунок ниже).

Создать верхнеуровневую форму

Сценарии Сопоставления Требуемые действия Политики пароля Политики OTP WebAuthn Policy WebAuthn Passwordless Policy

Синоним

Описание

Top Level Flow Type

В таблице представлено детальное описание интерфейса создания потока верхнего уровня.

Наименование настройки	Описание	Тип настройки
Синоним	Задает отображаемое имя для сценария	Текстовое поле
Описание	Описание сценария	Текстовое поле
Top Level Flow Type	Какой это тип сценария верхнего уровня? Тип “клиент” используется для аутентификации клиентов (приложений), когда “общий” для пользователей и всего остального	Выпадающий список

Сопоставления

На рисунке ниже изображено окно сопоставления сценариев аутентификации.

Сценарии Сопоставления Требуемые действия Политики пароля Политики OTP WebAuthn Policy WebAuthn Passwordless Policy

Сценарий браузера

Сценарий регистрации

Сценарий Direct Grant Flow

Сбросить учетные данные

Аутентификация клиента

В таблице представлено детальное описание интерфейса сопоставления сценариев аутентификации.

Наименование настройки	Описание	Тип настройки
Сценарий браузера	Выберите сценарий, который необходимо использовать для аутентификации через браузер.	Список с возможностью выбора значений
Сценарий регистрации	Выберите сценарий, который необходимо использовать для регистрации пользователя.	Список с возможностью выбора значений
Direct Grant Flow	Выберите сценарий, который необходимо использовать для аутентификации direct grant.	Список с возможностью выбора значений
Сбросить учетные данные	Выберите сценарий, который необходимо использовать когда пользователь забыл свои учетные данные.	Список с возможностью выбора значений
Аутентификация клиента	Выберите сценарий, который необходимо использовать для аутентификации клиентов.	Список с возможностью выбора значений

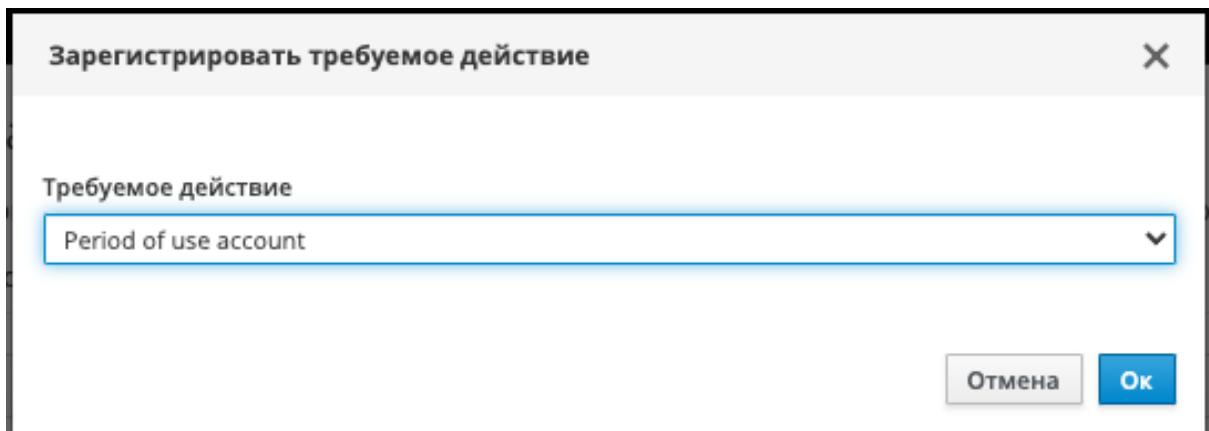
Требуемые действия

Выбор обязательных действий пользователя для создания учетной записи.

На рисунке ниже изображено окно настройки требуемых действий.

The screenshot shows the 'Required actions' configuration page. At the top, there are tabs: Сценарии (Scenarios), Сопоставления (Mappings), Требуемые действия (Required actions) (which is selected and highlighted in blue), Политики пароля (Password Policies), Политики OTP (OTP Policies), WebAuthn Policy ⓘ, and WebAuthn Passwordless Policy ⓘ. Below the tabs is a table titled 'Требуемое действие' (Required action). The table has three columns: 'Требуемое действие' (Action), 'Включено' (Enabled) with checkboxes, and 'Действие по умолчанию' (Default action) with checkboxes. The actions listed are: Configure OTP, Terms and Conditions, Update Password, Update Profile, Verify Email, Delete Account, and Update User Locale. Most actions have their 'Enabled' checkbox checked, except for 'Terms and Conditions' and 'Delete Account'. The 'Default action' checkboxes are all unchecked. A button labeled 'Регистрация' (Registration) is visible at the top right of the table area.

На рисунке ниже изображено окно регистрации требуемых действий.



В таблице представлено детальное описание интерфейса настройки требуемых действий.

Наименование настройки	Описание	Тип настройки
Требуемое действие	Требуемое действие для пользователя для создания учетной записи.	-
Кнопками можно менять порядок требуемых действий.	Текстовое поле с кнопками изменения порядка действий	-
Включено	Параметр включения/отключения требуемого действия.	Чекбокс
Действие по умолчанию	Если включено, то любому новому пользователю будет назначено требуемое действие.	Чекбокс
Регистрация	Регистрация нового требуемого действия	Кнопка

Политики пароля

Парольные политики пользователей.

Когда Keycloak создает realm, он не связывает политики паролей с областью. Установка простого пароля без ограничений по его длине, безопасности или сложности неприемлема в производственных средах. Keycloak имеет набор политик паролей, доступных через консоль администратора.

На рисунке ниже изображено окно настройки политик пароля.

Аутентификация

Добавить политику...		
Тип политики	Значение политики	Действия
Not Username		Удалить
Digits	1	Удалить
Sequence of forbidden characters in the password (separator)		Удалить

Сохранить **Отмена**

В таблице представлено детальное описание интерфейса настройки политик пароля.

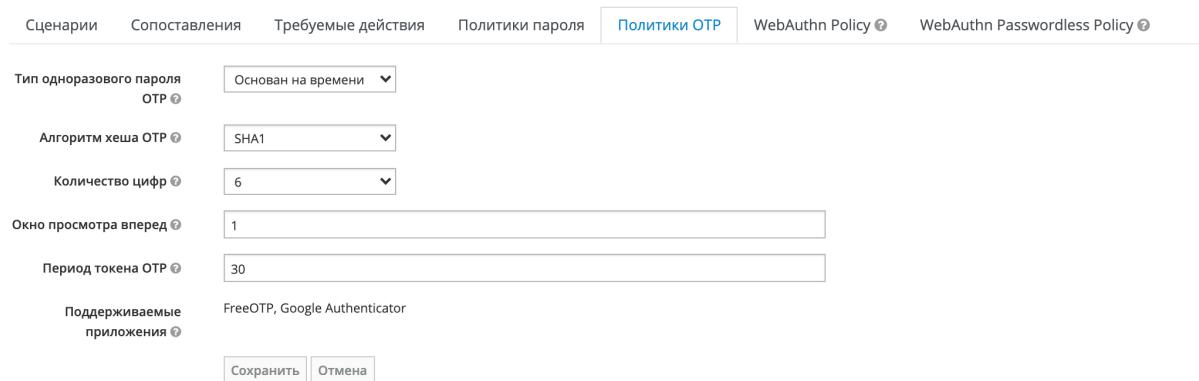
Наименование настройки	Описание	Тип настройки
Тип политики	Отображение типа парольной политики пользователя	Текстовое поле
Значение политики	Установка значения конкретной парольной политики	Текстовое поле
Действия	Удалить - удаление парольной политики	Кнопка

Наименование настройки	Описание	Тип настройки
Добавить политику	Добавление парольной политики	Выпадающий список

Политики OTP

На рисунке ниже изображено окно настройки политики OTP.

Аутентификация



Сценарии Сопоставления Требуемые действия Политики пароля Политики OTP WebAuthn Policy WebAuthn Passwordless Policy

Тип одноразового пароля OTP: Основан на времени

Алгоритм хеша OTP: SHA1

Количество цифр: 6

Окно просмотра вперед: 1

Период токена OTP: 30

Поддерживаемые приложения: FreeOTP, Google Authenticator

Сохранить Отмена

В таблице представлено детальное описание интерфейса настройки политики OTP.

Наименование настройки	Описание	Тип настройки
Тип одноразового пароля OTP	totp является временным одноразовым паролем. 'hotp' основанный на счетчике одноразовый пароль в котором сервер хранит счетчик хеша.	Список с возможностью выбора значений
Алгоритм хеша OTP	Какой алгоритм хеширования должен быть использован для генерации OTP.	Список с возможностью выбора значений
Количество цифр	Сколько цифр должен иметь OTP?	Список с возможностью выбора значений
Окно просмотра вперед	На сколько итераций вперед сервер должен попытаться сопоставить хэшпароль с тем, что предоставил пользователь. Значение по умолчанию - 1 (в реальности должно быть 10 или около того). Это случай, когда пользователь не синхронизирован с сервером по времени или привязки ко времени вообще нет.	Текстовое значение
Период токена OTP	Сколько секунд токен OTP должен быть действителен? По умолчанию 30 секунд.	Текстовое значение
Поддерживающие приложения	Приложения, которые знают, как работать с текущей политикой OTP	Список значений

WebAuthn Policy

Политика для аутентификации WebAuthn используется требуемым действием ‘WebAuthn Register’ и аутентификатором ‘WebAuthn Authenticator’. Обычно включается, когда WebAuthn используется для двухфакторной аутентификации. На рисунке ниже изображено окно настройки политики аутентификации WebAuthn.

The screenshot shows the Keycloak configuration interface with the 'Authentications' section selected in the sidebar. The main panel is titled 'Аутентификация' (Authentication) and contains several configuration fields:

- Название организации доверяющей стороны:** keycloak
- Алгоритмы подписи:** ES256, ES384, ES512, RS256
- Идентификатор доверяющей стороны:** (empty input field)
- Предпочтения передачи аттестации:** (dropdown menu)
- Подключение аутентификатора:** (dropdown menu)
- Требуется ключ резидента:** (dropdown menu)
- Требование к верификации пользователя:** (dropdown menu)
- Таймаут:** 0
- Избегать регистрации одного и того же аутентификатора:** Вык
- Допустимые AAGUIDs:** (input field)

В таблице представлено детальное описание интерфейса настройки политики аутентификации WebAuthn.

Наименование настройки	Описание	Тип настройки
Название организации доверяющей стороны	Человекочитаемое имя сервера в качестве доверяющей стороны WebAuthn	Текстовое значение
Алгоритмы подписи	Какие алгоритмы подписи следует использовать для утверждения аутентификации	Список с возможностью выбора значений
Идентификатор доверяющей стороны	Это ID как проверяющая сторона (WebAuthn Relying Party). Это должен быть эффективный домен происхождения	Текстовое значение
Предпочтения передачи аттестации	Сообщает аутентификатору о предпочтении способа генерации заявления об аттестации	Список с возможностью выбора значений
Подключение аутентификатора	Сообщает аутентификатору о приемлемой модели подключения	Список с возможностью выбора значений
Требуется ключ резидента	Сообщает аутентификатору, создавать ли учетные данные с открытым ключом как ключ резидента (Resident Key) или нет	Список с возможностью выбора значений

Наименование настройки	Описание	Тип настройки
Требование к верификации пользователя	Передается аутентификатору для подтверждения фактической верификации пользователя	Список с возможностью выбора значений
Тайм-аут	Значение тайм-аута для создания учетных данных открытого ключа пользователя в секундах. Если установлено значение 0, этот параметр тайм-аута не адаптируется.	Текстовое значение
Избегать регистрации одного и того же аутентификатора	Избегать регистрации аутентификатора, который уже был зарегистрирован	Булевая
Допустимые AAGUIDs	Список AAGUID, в которых может быть зарегистрирован аутентификатор	Текстовое значение

WebAuthn Passwordless Policy

Политика для беспарольной аутентификации WebAuthn используется требуемым действием ‘Webauthn Register Passwordless’ и аутентификатором ‘WebAuthn Passwordless Authenticator’. Типичное применение - когда WebAuthn используется в качестве первого фактора аутентификации. Наличие и ‘WebAuthn Policy’, и ‘WebAuthn Passwordless Policy’ позволяет использовать WebAuthn в качестве первого и второго фактора аутентификации в одном и том же realm.

На рисунке ниже изображено окно настройки беспарольной аутентификации WebAuthn.

The screenshot shows the Keycloak configuration interface for a realm named 'keycloak'. The left sidebar shows navigation options like 'Master', 'Конфигурация' (Configuration), 'Управление' (Management), and 'Аутентификация' (Authentication). The main panel is titled 'Аутентификация' (Authentication) and contains tabs for 'Сценарии' (Scenarios), 'Сопоставления' (Mappings), 'Требуемые действия' (Required Actions), 'Политики пароля' (Password Policies), 'Политики OTP' (OTP Policies), 'WebAuthn политики' (WebAuthn Policies), and 'WebAuthn беспарольные политики' (WebAuthn Passwordless Policies). The 'WebAuthn беспарольные политики' tab is active. The configuration form includes fields for 'Название организации доверяющей стороны' (Organization name of the relying party) set to 'keycloak', 'Алгоритмы подписи' (Signature algorithms) with 'ES256' selected, 'Идентификатор доверяющей стороны' (Identifier of the relying party), 'Предпочтения передачи аттестации' (Attestation delivery preferences), 'Подключение аутентификатора' (Authenticator connection), 'Требуется ключ резидента' (Resident key required), 'Требование к верификации пользователя' (User verification requirement), 'Таймаут' (Timeout) set to 0, 'Избегать регистрации одного и того же аутентификатора' (Avoid registration of the same authenticator) set to 'ВЫК' (OFF), and a 'Допустимые AAGUIDs' (Allowed AAGUIDs) input field with a '+' button. At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

В таблице представлено детальное описание интерфейса настройки беспарольной аутентификации WebAuthn.

Наименование настройки	Описание	Тип настройки
Название организации доверяющей стороны	Человекочитаемое имя сервера в качестве доверяющей стороны WebAuthn	Текстовое значение
Алгоритмы подписи	Какие алгоритмы подписи следует использовать для утверждения аутентификации.	Список с возможностью выбора значений
Идентификатор доверяющей стороны	Это ID как проверяющая сторона (WebAuthn Relying Party). Это должен быть эффективный домен происхождения	Текстовое значение
Предпочтения передачи аттестации	Сообщает аутентификатору о предпочтении способа генерации заявления об аттестации	Список с возможностью выбора значений
Подключение аутентификатора	Сообщает аутентификатору о приемлемой модели подключения	Список с возможностью выбора значений
Требуется ключ резидента	Сообщает аутентификатору, создавать ли учетные данные с открытым ключом как ключ резидента (Resident Key) или нет	Список с возможностью выбора значений
Требование к верификации пользователя	Передается аутентификатору для подтверждения фактической верификации пользователя	Список с возможностью выбора значений
Тайм-аут	Значение тайм-аута для создания учетных данных открытого ключа пользователя в секундах. Если установлено значение 0, этот параметр тайм-аута не адаптируется	Текстовое значение
Избегать регистрации одного и того же аутентификатора	Избегать регистрации аутентификатора, который уже был зарегистрирован	Булевая
Допустимые AAGUIDs	Список AAGUID, в которых может быть зарегистрирован аутентификатор	Текстовое значение

Управление Группами

Группы позволяют управлять общим набором атрибутов и сопоставлений ролей для группы пользователей. Пользователи могут быть членами нескольких групп. Пользователи наследуют атрибуты и сопоставления ролей, назначенные каждой группе. Для управления группами перейдите в пункт меню Группы слева.

Наименование настройки	Описание	Тип настройки
Поиск	Поле для поиска групп	Поисковое поле
Показать все группы	Отобразить все группы	Кнопка
Вырезать	Вырезать группу	Кнопка
Вставить	Вставить группу	Кнопка
Удалить	Удалить группу	Кнопка
Создать	Создать группу	Кнопка
Редактировать	Редактировать группу	Кнопка

Группы являются иерархическими. В группе может быть несколько подгрупп, но в группе может быть только один родитель. Подгруппы наследуют атрибуты и сопоставления ролей от своих родителей. Пользователи также наследуют атрибуты и сопоставления ролей от своих родителей.

Если существуют родительская группа и дочерняя группа, а пользователь принадлежит только к дочерней группе, пользователь в дочерней группе наследует атрибуты и сопоставления ролей как родительской группы, так и дочерней группы.

Создать

Создать группу

Наименование настройки	Описание	Тип настройки
Создать	Ввод наименования группы	Текстовое поле

Редактировать

Настройки

[Группы](#) > Тестовая группа

Тестовая Группа

Настройки	Атрибуты	Сопоставление ролей	Члены
<div style="border: 1px solid #ccc; padding: 5px;"> Имя * <input type="text" value="Тестовая группа"/> <input type="button" value="Сохранить"/> <input type="button" value="Отмена"/> </div>			

Наименование настройки	Описание	Тип настройки
Настройки	Ввод наименования группы	Текстовое поле

Атрибуты

[Groups](#) > Тестовая группа

Тестовая Группа

Настройки	Атрибуты	Сопоставление ролей	Члены						
<div style="border: 1px solid #ccc; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Ключ</th> <th>Значение</th> <th>Действия</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td><input type="button" value="Добавить"/></td> </tr> </tbody> </table> <input type="button" value="Сохранить"/> <input type="button" value="Отмена"/> </div>				Ключ	Значение	Действия			<input type="button" value="Добавить"/>
Ключ	Значение	Действия							
		<input type="button" value="Добавить"/>							

Наименование настройки	Описание	Тип настройки
Ключ	Поле для ввода ключа значения	Текстовое поле
Значение	Поле для ввода значения ключа	Текстовое поле
Действия	Добавить/Удалить	Кнопки

Сопоставление ролей

[Группы](#) > Тестовая группа

Тестовая Группа

Настройки	Атрибуты	Сопоставление ролей	Члены
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between;"> <div style="width: 33%;"> <p>Роли Realm</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Доступные роли ⓘ admin create-realm default-roles-master Name offline_access </div> <div style="border: 1px solid #ccc; padding: 2px; width: 100%;"> <input type="button" value="Добавить выбранное >"/> </div> </div> <div style="width: 33%;"> <p>Присвоенные роли ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px; width: 100%;"> <input type="button" value="< Удалить выбранное"/> </div> </div> <div style="width: 33%;"> <p>Назначенные роли ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px;"></div> </div> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 33%;"> <p>Роли интегрированных систем</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Доступные роли ⓘ account delete-account manage-account manage-account-links manage-consent Test </div> <div style="border: 1px solid #ccc; padding: 2px; width: 100%;"> <input type="button" value="Добавить выбранное >"/> </div> </div> <div style="width: 33%;"> <p>Присвоенные роли ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"></div> <div style="border: 1px solid #ccc; padding: 2px; width: 100%;"> <input type="button" value="< Удалить выбранное"/> </div> </div> <div style="width: 33%;"> <p>Назначенные роли ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px;"></div> </div> </div> </div>			

Наименование настройки		Описание	Тип настройки
Роли Realm		-	-
	Доступные роли	Роли уровня Realm, которые могут быть назначены.	Список с возможностью выбора значения
	Роли Realm по умолчанию	Роли уровня Realm, которые могут быть назначены новым пользователям.	Список с возможностью выбора значения
Роли интегрированных систем			Выпадающий список
	Доступные роли	Роли из этого клиента, которые могут быть назначены по умолчанию.	Список с возможностью выбора значения
	Роли клиента по умолчанию	Роли из этого клиента, назначенные как роли по умолчанию.	Список с возможностью выбора значения

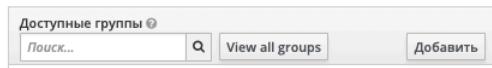
Члены

Наименование настройки	Описание	Тип настройки
Имя пользователя	Пользователь	Текстовое поле
Фамилия	Отображение фамилия пользователя	Текстовое поле
Имя	Отображение имени пользователя	Текстовое поле
E-mail	Отображение E-mail пользователя	Текстовое поле
Редактировать	Переход к редактированию пользователя	Кнопка

Группы по умолчанию

Чтобы автоматически назначать членство в группах всем пользователям, которые создаются или импортируются с помощью посредничества в идентификации используйте группы по умолчанию.

Группы пользователей

[Группы](#)[Группы по умолчанию](#)

Наименование настройки	Описание	Тип настройки
Группы по умолчанию	Вновь созданные или зарегистрированные пользователи будут автоматически добавлены к этим группам	Окно с возможностью выбора значения
Удалить	Удалить группу из групп по умолчанию	Кнопка
Доступные группы	Выберите группы, в которые пользователи будут добавляться по умолчанию.	Окно с отображением доступных групп
view All Groups	Отобразить всех пользователей	Кнопка
Добавить	Добавить группу в группы по умолчанию	Кнопка

Управление Пользователями

Пользователи – это субъекты, которые могут входить в систему. Они могут иметь связанные атрибуты, такие как электронная почта, имя пользователя, адрес, номер телефона и день рождения. Им может быть присвоено членство в группах и назначены определенные роли.

Детали

Ниже изображен интерфейс детального представления пользователя. Детали

В таблице представлено детальное описание интерфейса представления пользователя.

Наименование настройки	Описание	Тип настройки
Имя пользователя	Логин пользователя	Текстовое значение
E-mail	Почтовый адрес пользователя	Текстовое значение
Внутренний E-mail	Внутренний почтовый адрес пользователя	Текстовое значение
Имя	Имя пользователя	Текстовое значение

Наименование настройки	Описание	Тип настройки
Отчество	Отчество пользователя	Текстовое значение
Фамилия	Фамилия пользователя	Текстовое значение
Мобильный телефон	Мобильный телефон пользователя	Текстовое значение
Внутренний телефон	Внутренний телефон пользователя	Текстовое значение
Должность	Должность пользователя	Текстовое значение
Пользователь включен	Переключатель активности пользователя (выключенный пользователь считается заблокированным). Отключенные пользователи не смогут войти.	Булевая
Пользователь временно заблокирован	Переключатель временной блокировки пользователя (при использовании всех неудачных попыток входа)	Булевая
Разблокировать пользователя	Поле появляется при временной блокировке пользователя. Разблокировать пользователя, который использовал все неудачные попытки входа до истечения времени автоматической активации)	Кнопка
Подтверждение E-mail	Признак того, должен ли пользователь подтверждать свой E-mail	Булевая
Требуемые действия от пользователя	Требуемые действия от пользователя при входе: Настроить OTP (Configure OTP) - требует установить мобильное приложение генерации паролей. Обновить пароль (Update Password) - требует от пользователя ввести новый пароль. Обновить профиль (Update Profile) - требует от пользователя ввести новую персональную информацию. Подтвердить E-mail (Verify Email)- высылает письмо пользователю для подтверждения его E-mail. Обновить локаль пользователя (Update User Locale) - требует от пользователя обновить/выбрать локаль (язык). Webauthn Register Passwordless Verify Profile Webauthn Register	Выпадающий список с множественным выбором
Язык	Язык	Выпадающий список

Наименование настройки	Описание	Тип настройки
Имперсонировать	Войти как пользователь. Если пользователь в другом realm, то сессия администратора останется активной и дополнительно откроется сессия пользователя в другом realm, под которым вошел администратор. Если пользователь в том же самом realm что и администратор, то текущая сессия администратора будет разлогинена перед тем как он войдет как пользователь (т.е. останется активной только сессия пользователя).	Кнопка

Администратор с соответствующими разрешениями может выдавать себя за пользователя. Например, если пользователь обнаруживает ошибку в приложении, администратор может выдать себя за пользователя для расследования или дублирования проблемы.

Любой пользователь с ролью, допускающей имперсонирование может выдавать себя за пользователя. Для этого необходимо выбрать необходимого пользователя и нажать **Имперсонировать**.

Атрибуты

Помимо основных метаданных пользователя, таких как имя и адрес электронной почты, можно хранить произвольные пользовательские атрибуты. Для этого необходимо выбрать пользователя для управления, затем перейти на вкладку Атрибуты.

Затем ввести имя и значение атрибута в пустые поля и нажать кнопку Добавить рядом с атрибутом, чтобы добавить новое поле. Стоит обратить внимание на то, что любые изменения, внесенные на странице атрибутов, не будут сохранены, пока не нажата кнопка Сохранить. Ниже изображен интерфейс хранения и добавления произвольных пользовательских атрибутов. Атрибуты

Учетные данные

При просмотре пользователя, если перейти на вкладку Учетные данные, то есть возможность управлять учетными данными пользователя. Ниже изображен интерфейс управления учетными данными пользователя. Учетные данные

В таблице представлено детальное описание интерфейса управления учетными данными пользователя.

Наименование настройки	Описание	Тип настройки
Новый пароль	Ввести пароль пользователя	Текстовое значение
Подтверждение пароля	Повторить ввод пароля пользователя	Текстовое значение
Временный	Если включено, пользователю необходимо сменить пароль при следующем входе	Булевая

Наименование настройки	Описание	Тип настройки
Сброс учётных данных	Данный раздел появляется, если задать внутренний E-mail пользователя	
Действия сброса	Набор действий при отправке пользователю письма: - ‘Verify Email (VERIFY_EMAIL)’ - высылает пользователю письмо для подтверждения его E-mail - ‘Update Profile (UPDATE_PROFILE)’ - требует ввести пользователю новую персональную информацию - ‘Update Password (UPDATE_PASSWORD)’ - требует от пользователя ввести новый пароль - ‘Configure OTP (CONFIGURE_TOTP)’ - требует установить мобильное приложение с генератором паролей - ‘Update User Locale (update_user_locale)’ - выбрать локаль - ‘Webauthn Register (webauthn-register)’ - требует создать ключ доступа с меткой пользователя - ‘Webauthn Register Passwordless (webauthn-register-passwordless)’ - требует создать ключ доступа с меткой пользователя	Выбор из списка
Истекает в течении	Максимальное время до того, как время на разрешения истекает	Число
E-mail с действиями для сброса пароля	Отправить письмо	

Рекомендации по заданию стойких паролей

Для того чтобы пароль обладалной стойкостью, желательно задавать следующие ограничения для паролей:

- пароль должен изменяться не менее 1 раза в 80 дней с момента последнего изменения;
- пароль должен быть сложен (обязательно использование строчных и прописных букв и цифр);
- длина пароля – минимум 12 символов;
- пароль должен быть уникален, недопустимо использование одного и того же пароля для нескольких УЗ одного пользователя;
- пароль не должен содержать имя УЗ пользователя или какую-либо его часть;
- при вводе пароля символы должны быть скрыты;
- в случае компрометации пароля необходимо незамедлительно его сменить;
- пароль должен храниться в зашифрованном виде, хранение пароля в системах в незащищенном виде (в составе текстовых, конфигурационных файлов, скриптов) запрещено;
- пароль должен хешироваться алгоритмом sha512;
- в случае если хранение пароля в зашифрованном виде нереализуемо, доступ к файлам хранения должен быть ограничен только УЗ владельца.

Сопоставление ролей

Для назначения сопоставления ролей пользователю требуется перейти на вкладку *Сопоставление ролей* для этого пользователя. Ниже изображен интерфейс сопоставления (назначения и удаления) ролей пользователю. Сопоставление ролей

Согласия

Ниже изображен интерфейс отображения согласий пользователя. Согласия

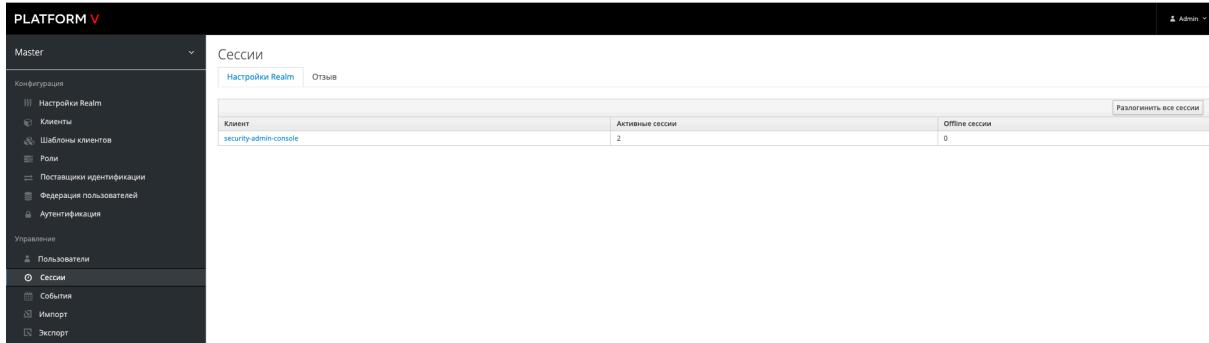
Сессии

Ниже изображен интерфейс отображения числа активных пользовательских сессий. Сессии

Управление Сессиями

Настройки Realm

Когда пользователь входит в Realm, единый вход (SSO) поддерживает сеанс пользователя для него и запоминает каждого клиента, которого посетили в рамках сеанса. Существует множество административных функций, которые администраторы области могут выполнять в этих пользовательских сеансах. Администраторы могут просматривать статистику входа в систему для всей области и погружаться в каждого клиента, чтобы узнать, кто и где вошел в систему. Или могут выйти из системы пользователя или группы пользователей из консоли администратора. Также администраторы могут отозвать токены и настроить там все тайм-ауты токенов и сеансов. Ниже изображен интерфейс отображения числа клиентских сессий в realm.



В таблице представлено детальное описание интерфейса отображения числа клиентских сессий в realm.

Наименование настройки	Описание	Тип настройки
Клиент	Ссылка на клиента	Ссылка на окно сессий клиента
Активные сессии	Количество активных сессий	Числовое значение

Наименование настройки	Описание	Тип настройки
Offline сессии	Количество Offline сессий	Числовое значение
Выйти из всех сессий	По нажатию завершает все активные сессии	Кнопка

Отзыв

Если настраиваемая система скомпрометирована, то есть возможность отзывать все активные сеансы и маркеры доступа, перейдя на вкладку *Отзыв*.

С помощью этой консоли указывается время и дата, когда сеансы или токены, выпущенные до этого времени и даты, будут недействительными. Для настройки требуется нажать Установить на сейчас, чтобы установить политику на текущее время и дату. При нажатии на кнопку Разослать, политика отзыва отправится любому зарегистрированному клиенту OIDC с помощью адаптера клиента OIDC Keycloak. Ниже изображен интерфейс отзыва токенов.

Сессии

Настройки Realm Отзыв

Не ранее чем None

Установить на сейчас Очистить Разослать

В таблице представлено детальное описание интерфейса отзыва токенов.

Наименование настройки	Описание	Тип настройки
Не ранее чем	Отозвать любые токены, выданные ранее этой даты.	Текстовое поле, недоступное для редактирования
Установить на сейчас	Установить дату отзыва токенов на сейчас	Кнопка
Очистить	Очистить дату отзыва токенов	Кнопка
Разослать	Уведомить каждого клиента, имеющего URL администратора, о новой политике отзыва токена.	Кнопка

Управление Сессиями

Настройки Realm

Когда пользователь входит в Realm, единый вход (SSO) поддерживает сеанс пользователя для него и запоминает каждого клиента, которого он посетил в рамках сеанса. Существует множество административных функций, которые администраторы области могут выполнять в этих пользовательских сеансах. Администраторы могут просматривать

статистику входа в систему для всей области и погружаться в каждого клиента, чтобы узнать, кто и где вошел в систему. Администраторы могут выйти из системы пользователя или группы пользователей из консоли администратора. Они также могут отзывать токены и настроить все тайм-ауты токенов и сеансов.

Ниже изображено окно Управления Сессиями.

В таблице представлено детальное описание интерфейса Управление Сессиями.

Наименование настройки	Описание	Тип настройки
Клиент	Ссылка на клиента	Ссылка на окно сессий клиента
Активные сессии	Количество активных сессий	Числовое значение
Offline сессии	Количество Offline сессий	Числовое значение
Разлогинить все сессии	По нажатию завершает все активные сессии	Кнопка

Отзыв

Если система скомпрометирована, то есть возможность отзывать все активные сеансы и маркеры доступа, перейдя на вкладку *Отзыв*.

С помощью данной консоли администратор может указать время и дату, когда сеансы или токены, выпущенные до этого времени и даты, будут недействительными. Для этого необходимо нажать кнопку Установить на сейчас, чтобы установить политику на текущее время и дату. Нажатие на кнопку Разослать, направит данную политику отзыва любому зарегистрированному клиенту OIDC с помощью адаптера клиента OIDC Keycloak.

Ниже изображено окно отзыва токенов.

В таблице представлено детальное описание интерфейса отзыва токенов.

Наименование настройки	Описание	Тип настройки
Не ранее чем	Отозвать любые токены, выданные ранее этой даты.	Текстовое поле, недоступное для редактирования
Установить на сейчас	Установить дату отзыва токенов на сейчас	Кнопка
Очистить	Очистить дату отзыва токенов	Кнопка
Разослать	Уведомить каждого клиента, имеющего URL администратора, о новой политике отзыва токена.	Кнопка

Управление Событиями

Каждое отдельное действие входа в систему может быть записано и сохранено в базе данных, а также рассмотрено в консоли администратора. Все действия администратора также могут быть записаны и просмотрены.

События входа в систему происходят, например, при успешном входе пользователя в систему, при вводе неверного пароля или при обновлении учетной записи пользователя. Каждое отдельное событие, происходящее с пользователем, может быть записано и просмотрено. По умолчанию события не сохраняются и не просматриваются в консоли администратора. В консоль и файл журнала сервера заносятся только события ошибок

События входа

Отображает сохраненные события для realm. События, связанные с учетными записями пользователей, например, вход пользователя. Для того чтобы включить сохранение событий, перейдите в конфигурацию.

Наименование настройки	Описание	Тип настройки
Время	Время события	Текстовое окно
Тип события	Наименование типа события	Текстовое окно

Наименование настройки		Описание	Тип настройки
Детали		Детали события	Текстовое окно
Количество событий на странице		Сколько событий будет отображено на странице	Выпадающий список
Обновить		Обновить список событий	Кнопка
Сбросить		Сбросить список событий	Кнопка
Фильтр		Фильтрация списка событий	Кнопка
	Тип события	Выберите тип событий	Выпадающий список с возможностью множественного выбора значений
	Клиент	-	Текстовое поле
	Пользователь	-	Текстовое поле
	Дата (С)	-	Текстовое поле
	Дата (По)	-	Текстовое поле

События администратора

Отображает сохраненные события администратора в этом realm. События, связанные с учетной записью администратора, например создание realm. Чтобы включить сохранение событий, перейдите в конфигурацию.

Наименование настройки		Описание	Тип настройки
Время		Время события	Текстовое окно
Тип операции		Наименование типа события	Текстовое окно

Наименование настройки		Описание	Тип настройки
Тип ресурса		Тип ресурса	Текстовое окно
Путь к ресурсу		Путь к ресурсу	Текстовое окно
Детали		Детали	Текстовое окно
Количество событий на странице		Сколько событий будет отображено на странице	Выпадающий список
Обновить		Обновить список событий	Кнопка
Сбросить		Сбросить список событий	Кнопка
Фильтр		Фильтрация списка событий	Кнопка
	Типы операций	Выберите операции	Выпадающий список с возможностью множественного выбора значений
	Типы ресурсов	Выберите типы ресурсов	Текстовое поле
	Путь к ресурсу	Фильтр по пути к ресурсу. Поддерживает подстановку '*' для совпадения одной части пути и '**' совпадение нескольких частей. Например 'realms/*/clients/asbc' выберет клиента с идентификатором asbc в любом realm, в то время как 'realms/master/**' не найдет ничего в master realm.	Текстовое поле
	Дата (С)	-	Текстовое поле
	Дата (По)	-	Текстовое поле
Детали аутентификации			
	Realm	-	Текстовое поле
	Клиент	-	Текстовое поле
	Пользователь	-	Текстовое поле
	IP адрес	-	Текстовое поле

Конфигурация событий

Отображает опции конфигурации для включения сохранения событий пользователей и администратора.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Конфигурация событий

[События входа](#) [События администратора](#)

[Конфигурация](#)

Конфигурация событий

Слушатели событий 

jboss-logging

Настройки событий по входу

Сохранять события 

Сохраняемые типы событий 

LOGIN LOGIN_ERROR REGISTER REGISTER_ERROR LOGOUT LOGOUT_ERROR CODE_TO_TOKEN CODE_TO_TOKEN_ERROR
 CLIENT_LOGIN CLIENT_LOGIN_ERROR FEDERATED_IDENTITY_LINK FEDERATED_IDENTITY_LINK_ERROR REMOVE_FEDERATED_IDENTITY
 REMOVE_FEDERATED_IDENTITY_ERROR UPDATE_EMAIL UPDATE_EMAIL_ERROR UPDATE_PROFILE UPDATE_PROFILE_ERROR
 UPDATE_PASSWORD UPDATE_PASSWORD_ERROR UPDATE_TOTP UPDATE_TOTP_ERROR VERIFY_EMAIL VERIFY_EMAIL_ERROR
 VERIFY_PROFILE VERIFY_PROFILE_ERROR REMOVE_TOTP REMOVE_TOTP_ERROR GRANT_CONSENT GRANT_CONSENT_ERROR
 UPDATE_CONSENT UPDATE_CONSENT_ERROR REVOKE_GRANT REVOKE_GRANT_ERROR SEND_VERIFY_EMAIL SEND_VERIFY_EMAIL_ERROR
 SEND_RESET_PASSWORD SEND_RESET_PASSWORD_ERROR SEND_IDENTITY_PROVIDER_LINK SEND_IDENTITY_PROVIDER_LINK_ERROR
 RESET_PASSWORD RESET_PASSWORD_ERROR RESTART_AUTHENTICATION RESTART_AUTHENTICATION_ERROR
 IDENTITY_PROVIDER_LINK_ACCOUNT IDENTITY_PROVIDER_LINK_ACCOUNT_ERROR IDENTITY_PROVIDER_FIRST_LOGIN
 IDENTITY_PROVIDER_FIRST_LOGIN_ERROR IDENTITY_PROVIDER_POST_LOGIN IDENTITY_PROVIDER_POST_LOGIN_ERROR IMPERSONATE
 IMPERSONATE_ERROR CUSTOM_REQUIRED_ACTION CUSTOM_REQUIRED_ACTION_ERROR EXECUTE_ACTIONS EXECUTE_ACTIONS_ERROR
 EXECUTE_ACTION_TOKEN EXECUTE_ACTION_TOKEN_ERROR CLIENT_REGISTER CLIENT_REGISTER_ERROR CLIENT_UPDATE
 CLIENT_UPDATE_ERROR CLIENT_DELETE CLIENT_DELETE_ERROR CLIENT_INITIATED_ACCOUNT_LINKING
 CLIENT_INITIATED_ACCOUNT_LINKING_ERROR TOKEN_EXCHANGE TOKEN_EXCHANGE_ERROR OAUTH2_DEVICE_AUTH
 OAUTH2_DEVICE_AUTH_ERROR OAUTH2_DEVICE_VERIFY_USER_CODE OAUTH2_DEVICE_VERIFY_USER_CODE_ERROR
 OAUTH2_DEVICE_CODE_TO_TOKEN OAUTH2_DEVICE_CODE_TO_TOKEN_ERROR AUTHREQID_TO_TOKEN AUTHREQID_TO_TOKEN_ERROR
 PERMISSION_TOKEN DELETE_ACCOUNT DELETE_ACCOUNT_ERROR

Очистить события 

[Очистить события](#)

Истечение 

1

Настройки событий администратора

Сохранять события 

Включить представление 

Вык

Очистить события администратора 

[Очистить события администратора](#)

[Очистить изменения](#) [Сохранить](#)

Наименование настройки	Описание	Тип настройки
Слушатели событий	Настройка слушателей, получающих события для realm.	Список с возможностью выбора значений
Сохранять события	Если включено, то события будут сохранены в базу данных, что сделает их доступными администратору и консоли управления учетной записью.	Булевая
Сохраняемые типы событий	Сконфигурировать, какие типы событий следует сохранять.	Список с возможностью выбора значений
Очистить события	Удаляет все события из базы данных.	Кнопка
Истечение	Установить срок истечения для событий. Истекшие события периодически удаляются из базы данных.	Число в минутах/часах/днях
Сохранять события	Если включено, то события администратора будут сохранены в базу данных, что сделает их доступными через консоль администратора.	Булевая
Включить представление	Включить JSON представление для запросов на создание и обновление.	Булевая

Наименование настройки	Описание	Тип настройки
Очистить события администратора	Удалить все события администратора из базы данных.	Кнопка

Управление экспортом/импортом данных

Импорт

Для выполнения сценария необходимо пред назначить роль `manage-realm`.

Частичный импорт позволяет импортировать пользователей, клиентов, и другие ресурсы из ранее экспортированного json-файла.

The screenshot shows the Keycloak Platform V interface. The top navigation bar is black with the text "PLATFORM V" in white. Below it, the main header is also black with the text "Test". On the left, there is a sidebar menu with the following items:

- Конфигурация
 - Настройки Realm
 - Клиенты
 - Шаблоны клиентов
 - Роли
 - Поставщики идентификации
 - Федерация пользователей
 - Аутентификация
- Управление
 - Группы
 - Пользователи
 - Сессии
 - События
- Импорт
- Экспорт
- Очистить кэш
- Синхронизация ролей и ФОС

The "Импорт" item is highlighted with a blue bar at the bottom of the sidebar.

The main content area has a title "Частичный импорт" with a question mark icon. It contains two input fields: "Экспортированный json файл" and a button labeled "Выберите файл" with a file icon.

Экспорт

Для выполнения сценария необходимо пред назначить роль `manage-realm`.

Частичный экспорт позволяет экспортировать конфигурацию realm и других ассоциируемых ресурсов в json-файл.

The screenshot shows the Keycloak SE Platform V interface. On the left, there's a sidebar with a dropdown menu set to 'Test'. Below it are sections for 'Конфигурация' (Configuration) containing 'Настройки Realm', 'Клиенты', 'Шаблоны клиентов', 'Роли', 'Поставщики идентификации', 'Федерация пользователей', and 'Аутентификация'; and 'Управление' (Management) containing 'Группы', 'Пользователи', 'Сессии', 'События', 'Импорт', 'Экспорт' (which is highlighted in blue), 'Очистить кэш', and 'Синхронизация ролей и ФОС'. At the top right, there's a 'Частичный экспорт' (Partial Export) section with two buttons: 'Экспорт групп и ролей' (Export groups and roles) and 'Экспорт клиентов' (Export clients). A large blue button labeled 'Экспорт' (Export) is centered below them. There are also 'ВЫК' (OFF) buttons next to each export option.

Импорт и экспорт базы данных

KeyCloak.SE включает в себя возможность экспорта и импорта всей своей базы данных. Перенести возможно всю базу данных Keycloak из одной среды в другую или перенести ее в другую базу данных. Предназначение ролей компонента не требуется. Экспорт / импорт запускается во время загрузки сервера, а его параметры проходят через свойства Java.

Можно экспортить / импортировать свою базу данных в:

- Каталог в файловой системе.
- JSON-файл в файловой системе.

При импорте из каталога имена файлов должны соответствовать следующим условностям:

- -realm.json. Например, “acme-roadrunner-affairs-realm.json” для реалма с названием “acme-roadrunner-affairs”.
- -users-.json. Например, “acme-roadrunner-affairs-users-0.json” для пользователя в реалме с названием “acme-roadrunner-affairs”.

При экспорте в каталог можно указать количество пользователей, хранящихся в каждом файле JSON.

Экспорт в отдельные файлы может привести к созданию больших файлов, поэтому если используемая база данных содержит более 500 пользователей, рекомендуется экспортить ее в каталог, а не в один файл. Экспорт многих пользователей в каталог выполняется оптимально, так как поставщик каталогов использует отдельную транзакцию для каждой “страницы” (файла пользователей).

Для экспорта в незашифрованный каталог:

```
bin/standalone.sh -Dkeycloak.migration.action=export  
-Dkeycloak.migration.provider=dir -Dkeycloak.migration.dir=<DIR TO EXPORT TO>
```

Для экспорта в JSON-файл:

```
bin/standalone.sh -Dkeycloak.migration.action=export  
-Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file=<FILE TO EXPORT TO>
```

Аналогично, для импорта использовать -Dkeycloak.migration.action=import вместо export. Например:

```
bin/standalone.sh -Dkeycloak.migration.action=import  
-Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file=<FILE TO IMPORT>  
-Dkeycloak.migration.strategy=OVERWRITE_EXISTING
```

Другие параметры командной строки включают в себя:

-Dkeycloak.migration.realmName

Использовать это свойство для экспорта одной области с определенным именем. Если этот параметр не указан, экспортятся все области.

-Dkeycloak.migration.usersExportStrategy

Это свойство указывает, куда экспортируются пользователи. Возможные значения включают в себя:

- DIFFERENT_FILES - пользователи экспортируются в разные файлы в зависимости от максимального количества пользователей в файле. DIFFERENT_FILES - это значение по умолчанию для этого свойства.
- SKIP - Keycloak пропускает экспорт пользователей.
- REALM_FILE - пользователи экспортируют данные в один файл с настройками realm. Файл похож на “foo-realm.json” с данными области и пользователями.
- SAME_FILE - пользователи экспортируют в один и тот же файл, но отличный от файла realm. Результат аналогичен “foo-realm.json” с данными realm и “foo-users.json” с пользователями.

-Dkeycloak.migration.usersPerFile

Это свойство указывает количество пользователей на файл и транзакцию базы данных. По умолчанию его значение равно пятидесяти. Keycloak использует это свойство, если keycloak.migration.usersExportStrategy - DIFFERENT_FILES.

-Dkeycloak.migration.strategy

Keycloak использует это свойство при импорте. Keycloak указывает, как действовать, если область с тем же именем уже существует в базе данных.

Возможные значения:

- IGNORE_EXISTING - Не импортировать область, если область с тем же именем уже существует.
- OVERWRITE_EXISTING - Удалить существующую область и снова импортировать область с новыми данными из файла JSON. Использовать это значение для полного перехода из одной среды в другую.

Если импортировать файлы, которые не являются результатом экспорта Keycloak, то необходимо использовать опцию *keycloak.import*. Если импортировать более одного файла realm, то необходимо указать список имен файлов, разделенных запятыми. Список имен файлов подходит больше, чем в предыдущих случаях, потому что это происходит после инициализации Master Realm в Keycloak.

Примеры:

- -Dkeycloak.import=/tmp/realm1.json
- -Dkeycloak.import=/tmp/realm1.json,/tmp/realm2.json

Параметр *keycloak.import* нельзя использовать с параметрами *keycloak.migration.X*. Если использовать эти параметры вместе, то Keycloak проигнорирует параметр *keycloak.import*. Механизм игнорирует realms, которые уже существуют в Keycloak. Это удобно для целей разработки, но если требуется большая гибкость, необходимо использовать параметры *keycloak.migration.X*.

Добавление сопоставлений

При создании клиента можно добавить следующие встроенные сопоставления:

Название мэппера в Keycloak.SE	Названия поля в токене	Название поля в профиле пользователя
Встроенные	—	—
full name	name	Имя + Фамилия
gender	gender	Атрибут gender
middle name	middle_name	Атрибут middleName
allowed web origins	allowed web origins	-
address	address	-
family name	family_name	Фамилия
profile	profile	Атрибут profile
picture	picture	Атрибут picture
Client IP Address	clientAddress	-
upn	upn	Имя пользователя
updated at	updated_at	Атрибут updatedAt
birthdate	birthdate	Атрибут birthdate
phone number verified	phone_number_verified	Атрибут phoneNumberVerified
zoneinfo	zoneinfo	Атрибут zoneinfo
website	website	Атрибут website
gss delegation credential	gss_delegation_credential	-
Impersonator Username	impersonator.username	-
username	preferred_username	Имя пользователя
nickname	nickname	Атрибут nickname
given name	given_name	Имя
Client ID	clientId	-
Client Host	clientHost	-
email verified	email_verified	Подтверждение E-mail
Impersonator User ID	impersonator.id	-
locale	locale	Язык

Название мэппера в KeyCloak.SE	Названия поля в токене	Название поля в профиле пользователя
phone number	phone_number	Атрибут phoneNumber
email	email	Внутренний E-mail
audience resolve	audience resolve	-
groups	groups	-
client roles	resource_access	Роли интегрированных систем, назначенные пользователю
realm roles	realm_access	Роли реалма, назначенные пользователю

При создании клиента можно добавить следующие сопоставления:

Название мэппера в KeyCloak.SE	Названия поля в токене	Название поля в профиле пользователя
Claims parameter Token	Зависит от настройки mapper	Имя + Фамилия, Фамилия, Имя пользователя, Внутренний E-mail ("name", "given_name", "family_name", "preferred_username", "email")
User Realm Role	Зависит от настройки mapper	Пользовательские роли реалма
ESIA Info Mapper	Зависит от настройки mapper	Mapper for ESIA user info
User Session Note	Зависит от настройки mapper	Добавить user session note в SAML атрибуты (для SAML протокола) либо добавить текущую user session note в поле токен
User Address	Зависит от настройки mapper	Добавить атрибуты отвечающие за адрес пользователя (street, locality, region, postal_code, и country) в поле OpenID Connect 'address'
Role Name Mapper	Зависит от настройки mapper	Задать существующей роли новое имя в токене
User Client Role	Зависит от настройки mapper	Клиентские роли пользователя
User Property	Зависит от настройки mapper	Имя свойства в интерфейсе UserModel.class. Для примера, значение 'email' будет ссылкой на метод ExtendedUserModel.getEmail()
Hardcoded Role	Зависит от настройки mapper	Вшитая роль в access_token
Hardcoded claim	Зависит от настройки mapper	Вшитое поле в токен

Название мэппера в KeyCloak.SE	Названия поля в токене	Название поля в профиле пользователя
Pairwise subject identifier	Зависит от настройки mapper	Вычисляет попарный идентификатор субъекта, используя хэш sha-256 с солью. Смотрите спецификацию OpenID Connect для получения дополнительной информации о попарных идентификаторах объектов
User's full name	Зависит от настройки mapper	Полное имя пользователя в поле 'name' OpenID Connect 'name'. Формат + ' ' +
Allowed Web Origins	Зависит от настройки mapper	Добавить все allowed web origins в 'allowed-origins' поле токена
Audience	Зависит от настройки mapper	Add specified audience to the audience (aud) field of token
*User Attribute	Зависит от настройки mapper	Атрибуты пользователя
Group Membership	Зависит от настройки mapper	Группы, которым принадлежит пользователь
Audience Resolve	Зависит от настройки mapper	Adds all client_ids of "allowed" clients to the audience conditions in the assertion. Allowed client means any SAML client for which user has at least one client role
Extended User Property	Зависит от настройки mapper	Имя свойства в интерфейсе ExtendedUserModel.class. Для примера, значение 'email' будет ссылкой на метод ExtendedUserModel.getEmail()
Script Mapper	Зависит от настройки mapper	JavaScript код, который возвращает значение поля

При создании IDP можно задать следующие сопоставления:

Название мэппера в KeyCloak.SE	Названия поля в токене	Название поля в профиле пользователя
Advanced Claim to Group	Зависит от настройки mapper	Если все поля существуют, то добавить пользователя в конкретную группу
Hardcoded User Session Attribute	Зависит от настройки mapper	Сохранить сессию пользователя, пришедшую от провайдера в конкретный user session атрибут
Attribute Importer	Зависит от настройки mapper	Импортировать информацию о профиле пользователя, если она существует в JSON данный поставщика социальных сетей, в заданный атрибут пользователя (для OpenID Connect) либо импортировать заданные saml атрибуты, если они заданы, в заданный атрибут пользователя или свойство.

Название мэппера в KeyCloak.SE	Названия поля в токене	Название поля в профиле пользователя
External Role to Role	Зависит от настройки mapper	Сопоставить внешней роли конкретную роль клиента либо реалм
Advanced Claim to Role	Зависит от настройки mapper	Если все поля существуют, то добавить пользователю конкретную роль реалма либо клиента
Hardcoded Role	Зависит от настройки mapper	Вшить роль в конкретный атрибут access_token (для OpenID Connect) либо SAML ответ
Claim to Role	Зависит от настройки mapper	Если поле существует, то добавить пользователю конкретную роль реалма либо клиента
Hardcoded Attribute	Зависит от настройки mapper	Когда пользователь импортирует из провайдера, вшить данные в конкретный атрибут пользователя (для OpenID Connect) для либо в SAML ответ
Username Template Importer	Зависит от настройки mapper	Формат username для импорта
Extended Attribute Mapper (SberTech version)	Зависит от настройки mapper	Значение поля расширенного объекта пользователя (ExtendedUserModel.class). Например, middleName → вызовет метод ExtendedUserModel.getMiddleName(). active → вызовет метод ExtendedUserModel.isActive().

*Для передачи в токен массив атрибутов пользователя необходимо настроить созданный mapper с типом сопоставления User Attribute для OIDC клиента:

1. Тип переменной JSON - String;
2. Несколько значений - ВКЛ; Пример итоговой конфигурации:

На вкладке Атрибуты пользователя задать значение для атрибута. Для передачи массива значений в токен, необходимо использовать разделитель ##. При использовании этого разделителя, массив корректно формируется и в токене, в строке значений атрибута, отображается через запятую (для примера: "test": ["test1", "test2"]).

Провайдер JavaScript

Keycloak позволяет администраторам при помощи JavaScript скриптов добавлять новую функциональность:

- Аутентификатор.
- JavaScript Policy.
- OpenID Connect Protocol сопоставление.

В данном поле будут доступны следующие поля: ‘user’ - текущий UserModel; ‘realm’ - текущий RealmModel; ‘userSession’ - текущая пользовательская сессия; ‘keycloakSession’ - текущая KeycloakSession; ‘authenticationSession’ - текущая AuthenticationSessionModel; ‘httpRequest’ - текущая org.jboss.resteasy.spi.HttpRequest ; ‘script’ - доступ к метаданным о скрипте; ‘LOG’ - org.jboss.logging.Logger, заданный в классе ScriptBasedAuthenticator.

Пример 1. Создание аутентификатора:

```
AuthenticationFlowError = Java.type("org.keycloak.authentication.AuthenticationFlowError");

function authenticate(context) {

    LOG.info(script.name + " --> trace auth for: " + user.username);

    if ( user.username === "tester"
        && user.getAttribute("someAttribute")
        && user.getAttribute("someAttribute").contains("someValue")) {

        context.failure(AuthenticationFlowError.INVALID_USER);
        return;
    }

    context.success();
}
```

Пример 2. Создание аутентификатора:

```
AuthenticationFlowError = Java.type("org.keycloak.authentication.AuthenticationFlowError");

function authenticate(context) {

    if (authenticationSession.getRealm().getName() != "${realm}") {
        context.failure(AuthenticationFlowError.INVALID_CLIENT_SESSION);
        return;
    }

    if (authenticationSession.getClient().getclientId() != "${clientId}") {
        context.failure(AuthenticationFlowError.UNKNOWN_CLIENT);
        return;
    }

    if (authenticationSession.getProtocol() != "${authMethod}") {
        context.failure(AuthenticationFlowError.INVALID_CLIENT_SESSION);
        return;
    }
}
```

```
}

    context.success();
}
```

Пример 3. Создание сопоставления

```
'hello_' + user.username
```

Для того чтобы данная функциональность стала доступной, необходимо включить `scripts` и `upload_scripts`, следуя инструкциям в руководстве по установке (см. главу “Дополнительная функциональность”).

Подключение внешнего Infinispan

Для подключения внешнего Infinispan назначения ролей компонента не требуется, так как Infinispan входит в состав сервера приложений.

Для подключения внешнего Infinispan для поддержки режима работы НА (High Availability) Keycloak необходимо прописать в DockerFile или docker-compose следующие параметры:

```
INFINISPAN: "true"
HA_SITE: "пропишите адрес вашего service-headless"
KEYCLOAK_REMOTE_ISPN_TRUSTSTORE_PATH: /opt/jboss/ispn/keystore.jks
KEYCLOAK_REMOTE_ISPN_TRUSTSTORE_PASSWORD: some password
HA_KEYCLOAK_CONNECTIONS_INFINISPAN_DEFAULT_REMOTESTORESECURITYENABLED: "true"
```

Установка сертификата безопасности

Задайте путь к server key хранилищу, как в следующем примере:

```
$ bin/cli.sh config set truststore /home/user/my-trust-store.jks<br>
```

Задайте пароль к key store хранилищу, если необходимо, следующим образом:

```
$ bin/cli.sh config set truststore-password secret
```

Проверьте конфигурацию CLI скриптов:

```
$ bin/cli.sh config get truststore
```

```
truststore=/home/user/my-trust-store.jks
```

```
$ bin/cli.sh config get truststore-password truststore-password=secret
```

Запуск Infinispan в Cross DC режиме

В данном разделе приведены рекомендации для запуска Infinispan в режиме cross-DC:

- Когда вы запускаете сервер Keycloak внутри центра обработки данных, необходимо, чтобы база данных, указанная в источнике данных KeycloakDS, уже работала и была доступна в этом центре обработки данных. Также необходимо, чтобы сервер Infinispan, на который ссылается привязка исходящего сокета, на которую ссылается элемент удаленного хранилища кэша Infinispan, уже работал. В противном случае сервер Keycloak не запустится.
- В каждом центре обработки данных может быть больше узлов базы данных, если вы хотите поддерживать отказоустойчивость базы данных и повышать надежность. Обратитесь к документации вашей базы данных и драйвера JDBC для получения подробной информации о том, как настроить это на стороне базы данных и как нужно настроить источник данных KeycloakDS на стороне Keycloak.
- В каждом центре обработки данных может быть больше серверов Infinispan, работающих в кластере. Это полезно, если вы хотите получить отказоустойчивость и повысить отказоустойчивость. Протокол Hot Rod, используемый для связи между серверами Infinispan и серверами Keycloak, имеет функцию, заключающуюся в том, что серверы Infinispan автоматически отправляют новую топологию на серверы Keycloak об изменении в кластере Infinispan, поэтому удаленное хранилище на стороне Keycloak будет знать, на каких серверах Infinispan он можно подключиться. Прочтите документацию Infinispan и WildFly для получения более подробной информации.
- Настоятельно рекомендуется, чтобы главный сервер Infinispan работал на каждом сайте до того, как будут запущены серверы Keycloak на любом сайте. Например, сначала запустили как server1, так и server2, перед всеми серверами Keycloak. Если вам по-прежнему нужно запустить сервер Keycloak, а сайт резервного копирования отключен, рекомендуется вручную переключить сайт резервного копирования в автономный режим на серверах Infinispan на вашем сайте. Если вы не переключите недоступный сайт вручную в автономный режим, при первом запуске может произойти сбой или могут возникнуть некоторые исключения во время запуска, пока резервный сайт не будет автоматически переведен в автономный режим из-за настроенного количества неудачных операций.

Cross-DC режим может быть реализован посредством создания образа сервера Infinispan и дальнейшего развертывания на сервере Kubernetes, ссылка на официальный сайт:

<https://infinispan.org/docs/dev/titles/server/server.html>

Активация и блокировка

В консоли администратора для сущностей клиентов/пользователей/ реалмов существует флаг включения/отключения активности. Описание настроек смотрите в Руководстве по системному администрированию в соответствующих разделах Сценариев администрирования (Управление Realm, Управление Клиентами, Управление пользователями).

События системного журнала

Состояние сервиса:

```
systemctl status keycloak
```

Логи java

В среде контейнеризации при запуске KeyCloak.SE расположение логов можно задать 3 способами:

1. Через переменную окружения KC_LOG_FILE
2. Через конфигурационный файл conf/keycloak.conf (log-file)
3. Через CLI параметр –log-file Инструкция по настройке находится в Руководстве по установке

По умолчанию путь задан следующий:

```
/opt/keycloak/conf/data/log/server.log`
```

```
2020-04-09 14:27:23,362 WARN [org.keycloak.events] (default task-2) type=LOGIN_ERROR, realmId=master, clientId=security-admin-console, userId=712a734e-0750-489e-bac4-fda968d43be8, ipAddress=0.0.0.0, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://0.0.0.0:8444/auth/admin/master/console/, code_id=f30ebc76-3f9f-49d4-baff-75dc2ec55939, username=admin
```

```
2020-04-09 14:27:23,395 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user 712a734e-0750-489e-bac4-fda968d43be8 from ip 0.0.0.0
```

```
2020-04-09 14:27:26,568 WARN [org.keycloak.events] (default task-2) type=LOGIN_ERROR, realmId=master, clientId=security-admin-console, userId=712a734e-0750-489e-bac4-fda968d43be8, ipAddress=0.0.0.0, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://0.0.0.0:8444/auth/admin/master/console/, code_id=f30ebc76-3f9f-49d4-baff-75dc2ec55939, username=admin
```

```
2020-04-09 14:27:26,579 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user 712a734e-0750-489e-bac4-fda968d43be8 from ip 0.0.0.0
```

```
2020-04-09 14:30:56,725 WARN [org.keycloak.events] (default task-5) type=LOGIN_ERROR, realmId=PlatformAuth, clientId=PlatformAuth-Proxy, userId=a13c334e-b538-4706-80de-6065a68c0edc, ipAddress=0.0.0.0, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://platform-devb.mycompany.ru/openid-connect-auth/redirect_uri, code_id=89c4632a-6ada-4a3e-9d88-c1e221b28483, username=sudir-admin
```

```
2020-04-09 14:30:56,751 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user a13c334e-b538-4706-80de-6065a68c0edc from ip 0.0.0.0
```

Уровни логирования

По умолчанию используется уровень логирования INFO. Уровень логирования можно изменить:

- в профиле развертывания посредством переключения параметра `debug` в файле `proxy.yml` - для Standalone
- в переменных окружения `KC_LOG_LEVEL = DEBUG` - для среды контейнеризации

Также доступны уровни логирования: FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL, OFF. Включение уровней логирования DEBUG и TRACE не рекомендуется в промышленных инсталляциях.

При деплое в среду контейнеризации доступно одно из следующих значений уровней логирования: FATAL, ERROR, WARN, INFO.

События мониторинга

Подключение модуля сбора метрик для компонента Platform V Monitor описано в Руководстве по установке.

Метрики Keycloak.SE

Метрики Keycloak.SE разделяются на следующие типы: counter, gauge, histogram, summary.

- Counter (счетчик) - это кумулятивная метрика, представляющая собой один монотонно увеличивающийся счетчик, значение которого может только увеличиваться или обнуляться при перезапуске. Например, вы можете использовать счетчик для представления количества обслуженных запросов, выполненных задач или ошибок. Не используйте счетчик для представления значения, которое может уменьшаться. Например, не используйте счетчик для количества текущих запущенных процессов; вместо него используйте gauge.
- Gauge (датчик) - это метрика, представляющая собой одно числовое значение, которое может произвольно увеличиваться и уменьшаться. Измерители обычно используются для измеряемых величин, таких как температура или текущее использование памяти, а также для "подсчетов", которые могут увеличиваться и уменьшаться, например, количество одновременных запросов.
- Histogram (гистограмма) - отбирает данные наблюдений (обычно это такие вещи, как длительность запроса или размер ответа) и подсчитывает их в настраиваемых областях. Она также предоставляет сумму всех наблюдаемых значений.
- Summary (сводка) - подобно гистограмме, сводка делает выборку наблюдений (обычно таких, как длительность запроса и размер ответа). Хотя она также предоставляет общее количество наблюдений и сумму всех наблюдаемых значений, она рассчитывает настраиваемые квантили в скользящем временном окне.

Для каждой метрики endpoint возвращает 2 или более строк информации:

- **# HELP**: Небольшое описание, предоставленное SPI;
- **# TYPE**: Тип метрики
- В случае, если были записаны какие-либо значения, последнее из них. Если ни одно значение еще не было записано, больше строк не будет.
- В случае если одна и та же метрика имеет разные метки, для каждой из них будет своя строка. По умолчанию все метрики имеют метку realm.

Пример:

```
## HELP jvm_memory_bytes_committed Committed (bytes) of a given JVM memory area.  
## TYPE jvm_memory_bytes_committed gauge  
jvm_memory_bytes_committed{area="heap",} 2.00802304E8  
jvm_memory_bytes_committed{area="nonheap",} 2.0217856E8
```

Метрики KeyCloak.SE можно разделить на:

- Метрики JVM;
- Generic events - Все внутренние события Keycloak передаются через endpoint, с описанием Generic Keycloak User event или Generic Keycloak Admin event. С описанием событий (events) можно ознакомиться во вкладке Управление событиями в руководстве по системному администрированию.

Основные метрики Generic events:

keycloak_login_attempts_total - Этот счетчик подсчитывает каждую попытку входа в систему, выполненную пользователем, не являющимся администратором. Счетчик также различает входы от используемого провайдера идентификации с помощью метки provider и от клиента с помощью метки client_id.

```
## HELP keycloak_login_attempts_total Total number of login attempts  
## TYPE keycloak_login_attempts_total counter  
  
{realm="test",provider="keycloak",client_id="account"} 3.0  
keycloak_login_attempts_total{realm="test",provider="github",client_id="application1"} 2.0
```

keycloak_logins_total - Этот счетчик подсчитывает каждый вход в систему, выполненный пользователем, не являющимся администратором. Счетчик также различает входы от используемого провайдера идентификации с помощью метки provider и от клиента с помощью метки client_id.

```
## HELP keycloak_logins_total Total successful logins  
## TYPE keycloak_logins_total counter
```

```
keycloak_logins_total{realm="test",provider="keycloak",client_id="account"} 3.0  
keycloak_logins_total{realm="test",provider="github",client_id="application1"} 2.0
```

keycloak_failed_login_attempts_total - Этот счетчик подсчитывает каждый вход в систему, выполненный неадминистративным пользователем, который завершился неудачно, с ошибкой, описанной меткой error. Счетчик также различает входы в систему по провайдеру идентификации, используемому с помощью метки provider, и по клиенту с меткой client_id.

```
## HELP keycloak_failed_login_attempts_total Total failed login attempts  
## TYPE keycloak_failed_login_attempts_total counter  
keycloak_failed_login_attempts_total{realm="test",provider="keycloak",error="invalid_user_credentials",client_id="application1"} 6.0  
keycloak_failed_login_attempts_total{realm="test",provider="keycloak",error="user_not_found",client_id="application1"} 2.0
```

keycloak_client_logins_total - Этот счетчик подсчитывает каждый вход клиента в систему.

```
## HELP keycloak_client_logins_total Total successful client logins  
## TYPE keycloak_client_logins_total counter  
keycloak_client_logins_total{realm="test",provider="keycloak",client_id="account"} 4.0  
keycloak_client_logins_total{realm="test",provider="github",client_id="application2"} 7.0
```

keycloak_failed_client_login_attempts_total - Этот счетчик подсчитывает каждую неудачную попытку входа клиента в систему, описанную меткой error.

```
## HELP keycloak_failed_client_login_attempts_total Total failed client login attempts  
## TYPE keycloak_failed_client_login_attempts_total counter  
keycloak_failed_client_login_attempts_total{realm="test2",provider="keycloak",error="invalid_client_credentials",client_id="application2"} 5.0  
keycloak_failed_client_login_attempts_total{realm="test2",provider="keycloak",error="client_not_found",client_id="application2"} 3.0
```

keycloak_refresh_tokens_total - Этот счетчик считает каждый refresh token.

```
## HELP keycloak_refresh_tokens_total Total number of successful token refreshes  
## TYPE keycloak_refresh_tokens_total counter  
keycloak_refresh_tokens_total{realm="test3",provider="keycloak",client_id="account"} 1.0  
keycloak_refresh_tokens_total{realm="test3",provider="github",client_id="application3"} 2.0
```

keycloak_refresh_tokens_errors_total - Этот счетчик подсчитывает каждый неудачный refresh token.

```
## HELP keycloak_refresh_tokens_errors_total Total number of failed token refreshes
## TYPE keycloak_refresh_tokens_errors_total counter
keycloak_refresh_tokens_errors_total{realm="test3",provider="keycloak",error="invalid_token",client_id="application3"} 3.0
```

keycloak_registrations_total - Этот счетчик подсчитывает каждую регистрацию нового пользователя. Счетчик также различает регистрации по провайдеру идентификации, используемому с помощью метки provider, и по клиенту с меткой client_id.

```
## HELP keycloak_registrations_total Total registered users
## TYPE keycloak_registrations_total counter
keycloak_registrations_total{realm="test",provider="keycloak",client_id="application1"} 1.0
keycloak_registrations_total{realm="test",provider="github",client_id="application1"} 1.0
```

keycloak_registrations_errors_total - Этот счетчик подсчитывает каждую неудачную регистрацию нового пользователя с ошибкой, описанной меткой error. Счетчик также различает регистрации по провайдеру идентификации, используемому с помощью метки provider, и по клиенту с меткой client_id.

```
## HELP keycloak_registrations_errors_total Total errors on registrations
## TYPE keycloak_registrations_errors_total counter
keycloak_registrations_errors_total{realm="test",provider="keycloak",error="invalid_registration",client_id="application1"} 2.0
keycloak_registrations_errors_total{realm="test",provider="keycloak",error="email_in_use",client_id="application1"} 3.0
```

keycloak_code_to_tokens_total - Этот счетчик считает каждый code to token.

```
## HELP keycloak_code_to_tokens_total Total number of successful code to token
## TYPE keycloak_code_to_tokens_total counter
keycloak_code_to_tokens_total{realm="test4",provider="keycloak",client_id="account"} 3.0
keycloak_code_to_tokens_total{realm="test4",provider="github",client_id="application4"} 1.0
```

keycloak_code_to_tokens_errors_total - Этот счетчик подсчитывает каждый неудачно выполненный code to token, который является ошибкой, описанной меткой error.

```
## HELP keycloak_code_to_tokens_errors_total Total number of failed code to token
## TYPE keycloak_code_to_tokens_errors_total counter
keycloak_code_to_tokens_errors_total{realm="test4",provider="keycloak",error="invalid_client_credentials",client_id="application4"} 7.0
```

keycloak_request_duration - Эта гистограмма регистрирует время ответа на каждый метод http и помещает их в одну из девяти групп:

- Запросы, которые занимают 50 мс или меньше;

- Запросы, которые занимают 100 мс или меньше;
- Запросы, которые занимают 250 мс или меньше;
- Запросы, которые занимают 500 мс или меньше;
- Запросы, которые занимают 1 с или меньше;
- Запросы, которые занимают 2 с или меньше;
- Запросы, которые занимают 10 с или меньше;
- Запросы, которые занимают 30 с или меньше;
- Любой запрос, который занимает более 30 с.

Ответ от этого типа метрики имеет следующий формат:

```
## HELP keycloak_request_duration Request duration
## TYPE keycloak_request_duration histogram
keycloak_request_duration_bucket{method="PUT",le="50.0",} 0.0
keycloak_request_duration_bucket{method="PUT",le="100.0",} 0.0
keycloak_request_duration_bucket{method="PUT",le="250.0",} 0.0
keycloak_request_duration_bucket{method="PUT",le="500.0",} 0.0
keycloak_request_duration_bucket{method="PUT",le="1000.0",} 1.0
keycloak_request_duration_bucket{method="PUT",le="2000.0",} 2.0
keycloak_request_duration_bucket{method="PUT",le="10000.0",} 2.0
keycloak_request_duration_bucket{method="PUT",le="30000.0",} 2.0
keycloak_request_duration_bucket{method="PUT",le="+Inf",} 2.0
keycloak_request_duration_count{method="PUT",} 2.0
keycloak_request_duration_sum{method="PUT",} 3083.0
```

Это говорит о том, что было ноль запросов, которые заняли менее 500 мс. Был один запрос, который занял менее 1 с. Все остальные запросы заняли менее 2 с.

Помимо групп есть также метрики sum и count для каждого метода. В приведенном выше примере они показывают, что для этого метода http было два запроса. Сумма всех времен отклика для этой комбинации составляет 3083 мс.

Чтобы получить среднюю продолжительность запроса за последние пять минут для всего сервера, можно использовать следующий запрос Prometheus:

```
rate(keycloak_request_duration_sum[5m]) / rate(keycloak_request_duration_count[5m])
```

keycloak_response_errors_total - Этот счетчик подсчитывает количество ошибок в ответах (ответы, в которых код состояния http находится в диапазоне 400 или 500).

```
## HELP keycloak_response_errors_total Total number of error responses
## TYPE keycloak_response_errors_total counter
keycloak_response_errors_total{code="500",method="GET",} 1
```

Metrics URI

URI можно добавить в метрики, установив переменную окружения `URI_METRICS_ENABLED` в `true`. При этом в метрику будет выводиться консолидированное значение URI realm. Значение realm заменяется общим значением {realm}.

```
## HELP keycloak_request_duration Request duration
## TYPE keycloak_request_duration histogram
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="50.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="100.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="250.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="500.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="1000.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="2000.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="10000.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="30000.0",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/3p-cookies/step2.html",le="+Inf",} 2.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="50.0",} 0.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="100.0",} 0.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="250.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="500.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="500.0",} 1.0
```

```
ole",uri="admin/{realm}/console/whoami",le="1000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="2000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="10000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="30000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="admin/{realm}/console/whoami",le="+Inf",} 1.0
```

Если количество метрик слишком велико, их также можно отфильтровать до определенных значений с помощью **URI_METRICS_FILTER**, например, **token, clients**. Это разделенное запятыми значение ключевых слов для поиска и отображения необходимых URI.

```
## HELP keycloak_request_duration Request duration
## TYPE keycloak_request_duration histogram
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="50.0",} 0.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="100.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="250.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="500.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="1000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="2000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="10000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="30000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/{realm}/protocol/openid-connect/token",le="+Inf",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="50.0",} 4.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="100.0",} 5.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="250.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="500.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="1000.0",} 6.0
```

```

ole",uri="",le="1000.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="2000.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="10000.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="30000.0",} 6.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/master/console",uri="",le="+Inf",} 6.0
keycloak_request_duration_count{code="200",method="GET",resource="admin,admin/master/console",uri="",} 6.0
keycloak_request_duration_sum{code="200",method="GET",resource="admin,admin/master/console",uri="",} 274.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="50.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="100.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="250.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="500.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="1000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="2000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="10000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="30000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="+Inf",} 1.0
keycloak_request_duration_count{code="200",method="GET",resource="admin,admin/serverinfo",uri="",} 1.0

```

Чтобы удалить консолидированный URI realm, установите `URI_METRICS_DETAILED` в `true`.

```

## HELP keycloak_request_duration Request duration
## TYPE keycloak_request_duration histogram
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="50.0",} 0.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="100.0",} 0.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="250.0",} 1.0

```

```
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="500.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="1000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="2000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="10000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="30000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="POST",resource="realms,realms/master/protocol/openid-connect",uri="realms/master/protocol/openid-connect/token",le="+Inf",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="50.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="100.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="250.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="500.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="1000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="2000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="10000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="30000.0",} 1.0
keycloak_request_duration_bucket{code="200",method="GET",resource="admin,admin/serverinfo",uri="",le="+Inf",} 1.0
keycloak_request_duration_count{code="200",method="GET",resource="admin,admin/serverinfo",uri="",} 1.0
keycloak_request_duration_sum{code="200",method="GET",resource="admin,admin/serverinfo",uri="",} 19.0
```

External Access

Чтобы отключить внешний доступ к метрикам в кластере, необходимо установить переменную окружения ‘DISABLE_EXTERNAL_ACCESS’. После установки включите заголовок ‘X-Forwarded-Host’ на вашем прокси. Он включен по умолчанию в HA Proxy на Openshift.

Перечень метрик с описанием

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_response_total	counter	Общее количество ответов	
keycloak_user_event_REFRESH_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REFRESH_AUTHENTICATION_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_POST_LOGIN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_OAUTH2_DEVICE_CODE_TO_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_RESPONSE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_OAUTH2_DEVICE_CODE_TO_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_registrations_total	counter	Всего зарегистрированных пользователей	
keycloak_user_event_EXECUTE_ACTIONS_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_OAUTH2_DEVICE_AUTH_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CODE_TO_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CONSOLE_INITIATED_ACCOUNT_LINKING_ERROR_total	counter	Общее событие администратора KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_admin_event_CREATE_total	counter	Общее событие администратора KeyCloak	
keycloak_user_event_REGISTER_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_FIRST_LOGIN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_POST_LOGIN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_registrations_errors_total	counter	Общее количество ошибок при регистрации	
keycloak_user_event_CLIENT_DELETE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_DELETE_ACCOUNT_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UPDATE_PROFILE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_RESET_PASSWORD_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_PERMISSION_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_DELETE_ACCOUNT_total	counter	Общее событие пользователя KeyCloak	
keycloak_failed_login_attempts_total	counter	Всего неудачных попыток входа	
keycloak_refresh_tokens_errors_total	counter	Общее количество неудачных token refreshes	
keycloak_user_event_UPDATE_CONSENT_ERROR_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_IM_PERSONATE_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_VA_LIDATE_ACCESS_TOKEN_ERROR_total	counter	Общее событие пользователя Keycloak	
jvm_memory_bytes_used	gauge	Использованные байты данной области памяти JVM	jvm_memory_bytes_used{area="heap",} 1.23512384E8 jvm_memory_bytes_used{area="nonheap",} 2.356852E8
jvm_memory_bytes_committed	gauge	Занимаемая часть (байты) данной области памяти JVM	jvm_memory_bytes_committed{area="heap",} 1.60432128E8 jvm_memory_bytes_committed{area="nonheap",} 2.58146304E8
jvm_memory_bytes_max	gauge	Максимальное количество (в байтах) данной области памяти JVM	jvm_memory_bytes_max{area="heap",} 5.36870912E8 jvm_memory_bytes_max{area="nonheap",} 7.80140544E8
jvm_memory_bytes_init	gauge	Начальные байты данной области памяти JVM	jvm_memory_bytes_init{area="heap",} 6.7108864E7 jvm_memory_bytes_init{area="nonheap",} 7667712.0
jvm_memory_pool_bytes_used	gauge	Использованные байты данного пула памяти JVM	jvm_memory_pool_bytes_used{pool="CodeHeap 'non-nmethods'",} 1641984.0 jvm_memory_pool_bytes_used{pool="Metaspace",} 1.67686904E8 jvm_memory_pool_bytes_used{pool="CodeHeap 'profiled nmethods'",} 3.5873664E7 jvm_memory_pool_bytes_used{pool="Compressed Class Space",} 2.2100184E7 jvm_memory_pool_bytes_used{pool="G1 Eden Space",} 1.1534336E7 jvm_memory_pool_bytes_used{pool="G1 Old Gen",} 1.0883232E8 jvm_memory_pool_bytes_used{pool="G1 Survivor Space",} 3145728.0 jvm_memory_pool_bytes_used{pool="CodeHeap 'non-profiled nmethods'",} 8382464.0

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_memory_pool_bytes_committed	gauge	Распределенные байты данного пула памяти JVM	jvm_memory_pool_bytes_committed{pool="Code Heap 'non-nmethods'",} 2555904.0 jvm_memory_pool_bytes_committed{pool="Metaspace",} 1.83762944E8 jvm_memory_pool_bytes_committed{pool="Code Heap 'profiled nmethods'",} 3.5913728E7 jvm_memory_pool_bytes_committed{pool="Compressed Class Space",} 2.752512E7 jvm_memory_pool_bytes_committed{pool="G1 Eden Space",} 2.5165824E7 jvm_memory_pool_bytes_committed{pool="G1 Old Gen",} 1.32120576E8 jvm_memory_pool_bytes_committed{pool="G1 Survivor Space",} 3145728.0 jvm_memory_pool_bytes_committed{pool="Code Heap 'non-profiled nmethods'",} 8388608.0
jvm_memory_pool_bytes_max	gauge	Максимальное количество байт данного пула памяти JVM	jvm_memory_pool_bytes_max{pool="CodeHeap 'non-nmethods'",} 5832704.0 jvm_memory_pool_bytes_max{pool="Metaspace",} 2.68435456E8 jvm_memory_pool_bytes_max{pool="CodeHeap 'profiled nmethods'",} 1.22912768E8 jvm_memory_pool_bytes_max{pool="Compressed Class Space",} 2.60046848E8 jvm_memory_pool_bytes_max{pool="G1 Eden Space",} -1.0 jvm_memory_pool_bytes_max{pool="G1 Old Gen",} 5.36870912E8 jvm_memory_pool_bytes_max{pool="G1 Survivor Space",} -1.0 jvm_memory_pool_bytes_max{pool="CodeHeap 'non-profiled nmethods'",} 1.22912768E8

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_memory_pool_bytes_init	gauge	Начальные байты данного пула памяти JVM	jvm_memory_pool_bytes_init{pool="CodeHeap 'non-nmethods'",} 2555904.0 jvm_memory_pool_bytes_init{pool="Metaspace",} 0.0 jvm_memory_pool_bytes_init{pool="CodeHeap 'profiled nmethods'",} 2555904.0 jvm_memory_pool_bytes_init{pool="Compressed Class Space",} 0.0 jvm_memory_pool_bytes_init{pool="G1 Eden Space",} 2.5165824E7 jvm_memory_pool_bytes_init{pool="G1 Old Gen",} 4.194304E7 jvm_memory_pool_bytes_init{pool="G1 Survivor Space",} 0.0 jvm_memory_pool_bytes_init{pool="CodeHeap 'non-profiled nmethods'",} 2555904.0
keycloak_user_event_UPDATE_PASSWORD	counter	Общее событие пользователя KeyCloak	
keycloak_request_duration	histogram	Длительность запроса	
keycloak_admin_event_UPDATE_total	counter	Общее событие администратора KeyCloak	keycloak_admin_event_UPDATE{realm="1234",resource="REALM",} 1.0
keycloak_user_event_UPDATE_EMAIL_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_TOOKEN_EXCHANGE_total	counter	Общее событие пользователя KeyCloak	
keycloak_refresh_tokens_total	counter	Общее количество успешных token refreshes	
keycloak_user_event_REMOVE_TOTP_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_EXECUTE_ACTION_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_response_errors_total	counter	Общее число ответов на ошибки	
jvm_buffer_pool_used_bytes	gauge	Использованные байты данного буферного пула JVM	vm_buffer_pool_used_bytes{pool="mapped",} 0.0 jvm_buffer_pool_used_bytes{pool="direct",} 737350.0

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_buffer_pool_capacity_bytes	gauge	Емкость в байтах данного буферного пула JVM	jvm_buffer_pool_capacity_bytes{pool="mapped", } 0.0 jvm_buffer_pool_capacity_bytes{pool="direct", } 737350.0
jvm_buffer_pool_used_buffers	gauge	Используемые буферы данного пула буферов JVM	jvm_buffer_pool_used_buffers{pool="mapped", } 0.0 jvm_buffer_pool_used_buffers{pool="direct", } 13.0
keycloak_user_event_UNREGISTER_NODE_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_SEND_RESET_PASSWORD_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_SEND_RESET_PASSWORD_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_USER_INFO_REQUEST_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_CLIENT_INFO_total	counter	Общее событие пользователя Keycloak	
jvm_info_total	gauge	Информация о версии	jvm_info_total{runtime="OpenJDK Runtime Environment", vendor="Red Hat, Inc.", version="17.0.6+10-LTS", } 1.0
keycloak_user_event_OAUTH2_DEVICE_AUTHENTICATION_error	counter	Общее событие пользователя Keycloak	
keycloak_admin_event_ACTION_total	counter	Общее событие администратора Keycloak	
keycloak_user_event_FEDERATED_IDENTITY_LINK_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_EXECUTE_ACTIONS_ERROR_total	counter	Общее событие пользователя Keycloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_CLI_ENT_UPDATE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_logins_total	counter	Общее количество успешных входов в систему	
keycloak_user_event_SEND_VERIFY_EMAIL_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_RESET_PASSWORD_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UPDATE_CONSENT_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_RESPONSE_total	counter	Общее событие пользователя KeyCloak	
process_cpu_seconds_total	counter	Общее время работы процессора пользователя и системы в секундах	process_cpu_seconds_total 59.96
process_start_time_seconds	gauge	Время начала процесса с epoch unix в секундах	process_start_time_seconds 1.650019625844E9
process_open_fds	gauge	Количество открытых дескрипторов файлов	process_open_fds 627.0
process_max_fds	gauge	Максимальное количество открытых дескрипторов файлов	process_max_fds 1048576.0
process_virtual_memory_bytes	gauge	Размер виртуальной памяти в байтах	process_virtual_memory_bytes 1.851981824E9
process_resident_memory_bytes	gauge	Размер резидентной памяти в байтах	process_resident_memory_bytes 5.59230976E8
keycloak_user_event_CUSTOM_REQUIRED_ACTION_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REMOTE_FEDERATED_IDENTITY_ERROR_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_SE ND_RESET_PASSWORD_ ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REGISTER_NODE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_LINK_ACCOUNT_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_USER_INFO_REQUEST_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REGISTER_NODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_FEDERATED_IDENTITY_LINK_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REMOTE_TOTP_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CLI_LOGIN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_VERIFY_PROFILE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_VERIFY_PROFILE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_VERIFY_EMAIL_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_GRANT_CONSENT_ERROR_total	counter	Общее событие пользователя KeyCloak	
jvm_threads_current_threads	gauge	Текущее количество потоков в JVM	jvm_threads_current 111.0
jvm_threads_daemon_threads	gauge	Количество потоков демона в JVM	jvm_threads_daemon 60.0

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_threads_peak_threads	gauge	Максимальное количество потоков в JVM	jvm_threads_peak 171.0
jvm_threads_started_threads_total	counter	Начальное количество потоков в JVM	jvm_threads_started_total 178.0
jvm_threads_deadlocked_threads	gauge	Циклы JVM-потоков, находящихся в тупике в ожидании получения мониторов объектов или собственных синхронизаторов	jvm_threads_deadlocked 0.0
jvm_threads_deadlocked_monitor_threads	gauge	Циклы JVM-потоков, находящихся в тупике в ожидании получения мониторов объектов	jvm_threads_deadlocked_monitor 0.0
jvm_threads_states_threads	gauge	Текущее количество потоков по состоянию	jvm_threads_state{state="TERMINATED",} 0.0 jvm_threads_state{state="WAITING",} 61.0 jvm_threads_state{state="RUNNABLE",} 27.0 jvm_threads_state{state="BLOCKED",} 0.0 jvm_threads_state{state="TIMED_WAITING",} 23.0 jvm_threads_state{state="NEW",} 0.0
keycloak_user_event_IN_TROSPECT_TOKEN_ERR_OR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_GRANT_CONSENT_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CLIENT_UPDATE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UPDATE_PASSWORD_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UNREGISTER_NODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IN_VALID_SIGNATURE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IN_VALID_SIGNATURE_ERROR_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_SE_ND_IDENTITY_PROVIDER_LINK_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_LO_GOUT_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REVOKE_GRANT_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_VA_LIDATE_ACCESS_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_admin_event_DELETE_total	counter	Общее событие администратора KeyCloak	
keycloak_user_event_LO_GOUT_total	counter	Общее событие пользователя KeyCloak	
keycloak_client_logins_total	counter	Общее количество успешных входов клиентов в систему	
keycloak_user_event_IN_TROSPECT_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CLI_ENT_DELETE_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_PERMISSION_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_IDENTITY_PROVIDER_LOGIN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CLI_ENT_LOGIN_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_PU_SHED_AUTHORIZATION_REQUEST_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_AUTHREQID_TO_TOKEN_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_CLI_ENT_REGISTER_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_code_to_tokens_total	counter	Общее количество успешных code to token	
keycloak_user_event_OA_UTH2_DEVICE_VERIFY_USER_CODE_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_SE_ND_VERIFY_EMAIL_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_ID_ENTITY_PROVIDER_RETRIEVE_TOKEN_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_UP_DATE_PROFILE_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_REFRESH_GRANT_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_IM_PERSONATE_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_CLI_ENT_REGISTER_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_REFRESH_START_AUTHENTICATION_total	counter	Общее событие пользователя Keycloak	
keycloak_failed_client_login_attempts_total	counter	Всего неудачных попыток входа клиента в систему	
keycloak_user_event_REFRESH_EMAIL_total	counter	Общее событие пользователя Keycloak	
keycloak_code_to_tokens_errors_total	counter	Общее количество неудачных code to token	
keycloak_user_event_CLI_ENT_INITIATED_ACCOUNT_LINKING_total	counter	Общее событие пользователя Keycloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_memory_pool_allocated_bytes_total	counter	Общее количество байт, выделенных в данном пуле памяти JVM. Обновляется только после GC, не постоянно.	
keycloak_user_event_ID_ENTITY_PROVIDER_LINK_ACCOUNT_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_ID_ENTITY_PROVIDER_FIRS_T_LOGIN_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_UP_DATE_TOTP_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_IDENTITY_PROVIDER_RETRIEVE_TOKEN_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_PU SHED_AUTHORIZATION_REQUEST_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_CODE_TO_TOKEN_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_UP_DATE_EMAIL_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_IDENTITY_PROVIDER_LOGIN_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_SEND_IDENTITY_PROVIDER_LINK_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_CLIENT_INFO_ERROR_total	counter	Общее событие пользователя Keycloak	
keycloak_user_event_AUTHREQID_TO_TOKEN_ERROR_total	counter	Общее событие пользователя Keycloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_MOVE_FEDERATED_IDENTITY_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_REFRESH_TOKEN_total	counter	Общее событие пользователя KeyCloak	
jvm_gc_collection_seconds	summary	Время, проведенное в данном сборщике мусора JVM, в секундах	jvm_gc_collection_seconds_count{gc="G1 Young Generation",} 65.0 jvm_gc_collection_seconds_sum{gc="G1 Young Generation",} 0.519 jvm_gc_collection_seconds_count{gc="G1 Old Generation",} 0.0 jvm_gc_collection_seconds_sum{gc="G1 Old Generation",} 0.0
keycloak_user_event_EXECUTE_ACTION_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
jvm_classes_loaded_classes	gauge	Количество классов, которые в настоящее время загружены в JVM	jvm_classes_loaded 32917.0
jvm_classes_loaded_classes_total	counter	Общее количество классов, которые были загружены с момента начала выполнения JVM	jvm_classes_loaded_total 33496.0
jvm_classes_unloaded_classes_total	counter	Общее количество классов, которые были выгружены с момента начала выполнения JVM	jvm_classes_unloaded_total 579.0
keycloak_login_attempts_total	counter	Общее количество попыток входа в систему	
keycloak_user_event_OAUTH2_DEVICE_VERIFY_USER_CODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_OAUTH2_DEVICE_VERIFY_USER_CODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_TOKEN_EXCHANGE_ERROR_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_user_event_ID ENTITY_PROVIDER_LINK_ACCOUNT_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_ID ENTITY_PROVIDER_FIRS T_LOGIN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UP DATE_TOTP_ERROR_tota l	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_ID ENTITY_PROVIDER_RETR IEVE_TOKEN_ERROR_tot al	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_PU SHED_AUTHORIZATION_ REQUEST_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CO DE_TO_TOKEN_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_UP DATE_EMAIL_ERROR_tot al	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_ID ENTITY_PROVIDER_LOGI N_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_SE ND_IDENTITY_PROVIDER _LINK_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_CLI ENT_INFO_ERROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_AU THREQID_TO_TOKEN_ER ROR_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_RE MOVE_FEDERATED_IDE NTITY_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_RE FRESH_TOKEN_total	counter	Общее событие пользователя KeyCloak	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
jvm_gc_collection_seconds	summary	Время, проведенное в данном сборщике мусора JVM, в секундах	jvm_gc_collection_seconds_count{gc="G1 Young Generation",} 65.0 jvm_gc_collection_seconds_sum{gc="G1 Young Generation",} 0.519 jvm_gc_collection_seconds_count{gc="G1 Old Generation",} 0.0 jvm_gc_collection_seconds_sum{gc="G1 Old Generation",} 0.0
keycloak_user_event_EXECUTE_ACTION_TOKEN_ERROR_total	counter	Общее событие пользователя KeyCloak	
jvm_classes_loaded_total	gauge	Количество классов, которые в настоящее время загружены в JVM	jvm_classes_loaded 32917.0
jvm_classes_loaded_total	counter	Общее количество классов, которые были загружены с момента начала выполнения JVM	jvm_classes_loaded_total 33496.0
jvm_classes_unloaded_total	counter	Общее количество классов, которые были выгружены с момента начала выполнения JVM	jvm_classes_unloaded_total 579.0
keycloak_login_attempts_total	counter	Общее количество попыток входа в систему	
keycloak_user_event_OAUTH2_DEVICE_VERIFY_USER_CODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_OAUTH2_DEVICE_VERIFY_USER_CODE_total	counter	Общее событие пользователя KeyCloak	
keycloak_user_event_TOKEN_EXCHANGE_ERROR_total	counter	Общее событие пользователя KeyCloak	
agroal_available_count	gauge	Метрика показывает количество свободных соединений в пуле, доступных для получения	

Наименование метрики	Тип метрики #TYPE	Описание метрики #HELP	Дополнительно
keycloak_service_connection_count	counter	Эта метрика показывает количество успешных подключений к сервису	
vendor_cache_manager_keycloak_local_container_stats_memory_used	gauge	Объем памяти, используемый локальной JVM для хранения кэша в байтах	

Настройка интеграции с ОСА

Сервис объединенный сервис авторизации (ОСА) продукта Platform V IAM SE (AUTZ) – предназначен для авторизации доступа пользователей на основе: проверки ролей пользователей, наличия прав доступа и анализа правил атрибутов объектов и субъектов доступа. За интеграцию с данным компонентом отвечает модуль kcse-keycloak-identity-adapters.

Настройка на стороне ОСА

Дистрибутив ОСА установлен на стенде. В среде контейнеризации ОСА в Deployment Config прописаны следующие параметры:

Свойство	Значение
spas.rest.sudirEnable	true
spas.identity.basicAuthUser	например, basicAuthUser
spas.identity.basicAuthPas	например, basicAuthPas

Настройка на стороне Platform V KeyCloak.SE

1. Зайти под функциональным администратором.
2. Перейти на вкладку “Настройки Realm” -> “Дополнительно” -> “Настройки SOAP”.
3. Задать параметры:

Название переменной	Описание
CN клиентского сертификата	Список допустимых CN клиентского сертификата (при mTLS) через “ ”, “*” - отключить проверку

Название переменной	Описание
Фильтр по scope ролей	Фильтр по scope ролей, попадающих под синхронизацию через API. Это префикс роли realm или клиента client_id/prefix. Данное поле не является обязательным. Пример: “platformauth, EFS, PlatformAuth-Proxy”

4. Перейти на вкладку “Синхронизация ролей и ФОС”.

5. Заполнить параметры:

Название переменной	Описание
URL веб-сервиса *	http://{host_osa}ufs-security/identity/GenericAccountManagement2
Пользователь	Равен значению в OSE OSA spas.identity.basicAuthUser
Пароль	Равен значению в OSE OSA spas.identity.basicAuthPas
Место сохранения ролей	Роли можно сохранить в Realm или конкретному клиенту
Имя клиента	Установить имя существующего клиента

6. Сохранить конфигурацию. Если при нажатии на кнопку “Проверить подключение” выводится сообщение об успешном прохождении тестов, то настройка успешно завершена.

7. Для выполнения синхронизации нажать “Выполнить”.

Настройка планировщика

Синхронизацию с ОСА можно выполнять по расписанию. Для этого необходимо задать периодичность запуска в поле “триггер”.

<секунда (0-59)> <минута (0-59)> <час (0-23)> <день месяца (1-31)> <месяц (1-12 или JAN-DEC)> <день недели (0-7 или MON-SUN, где 0 и 7 - это SUN)>

- Допускается диапазон чисел через тире (включает крайние значения).
- Для указания всех значений можно использовать звездочку (*). Для указания дня месяца или недели можно использовать знак вопроса (?).
- Для указания дня месяца или недели можно использовать первые три буквы дня или месяца на английском языке.
- Поля день месяца или день недели может использоваться L, который означает последний. Если указывается L-n, то это означает “с n-го по последний день месяца”. В поле “день недели” L означает “последний день недели”. Если перед ним стоит цифра или название из трех букв (например, dL или DDDL), это означает “последний день недели d (или DDD) в месяце”.
- Поле “день недели” может быть d#n (или DDD#n), что означает “n-й день недели d (или DDD) в месяце”.

Например:

Триггер	Значение
0 0/1 * 1/1 * ? *	Каждую минуту, каждый день
0 0 0 1 1 *	Раз в году
0 0 0 1 * *	Раз в месяц
0 0 0 * * 0	Раз в неделю
0 0 0 * * *	Раз в день
0 0 * * * *	Раз в час
0 0 4 ? * *	В 4:00 часа

Настройка взаимодействия с ОСА через SSL/TLS

Параметр	Значение	Значение по умолчанию
spi-realm-restapi-extension-sync-spas-use-separate-keystore	Считывать доверенный сертификат и ключ для установления mTLS с ОСА из отдельного хранилища. В противном случае использует сертификат и ключ стенда	false
spi-realm-restapi-extension-sync-spas-osa-cert-file	Сертификат для установления mTLS соединения с ОСА	
spi-realm-restapi-extension-sync-spas-osa-key-file	Ключ для установления mTLS соединения с ОСА	
spi-realm-restapi-extension-sync-spas-osa-ca-cert	Корневой сертификат для установления mTLS соединения с ОСА	
spi-realm-restapi-extension-sync-spas-osa-keystore	Путь до JKS хранилища ключей для ОСА	
spi-realm-restapi-extension-sync-spas-osa-keystore-password	Пароль от JKS хранилища с сертификатом и ключом ОСА. Используется как пароль от хранилища и от ключа при работе с JKS	

Для установления mTLS соединения необходимо задать одну из следующих комбинаций:

1. Сертификат (spi-realm-restapi-extension-sync-spas-osa-cert-file) и ключ (spi-realm-restapi-extension-sync-spas-osa-key-file)
2. Сертификат (spi-realm-restapi-extension-sync-spas-osa-cert-file), ключ (spi-realm-restapi-extension-sync-spas-osa-key-file) и корневой сертификат (spi-realm-restapi-extension-sync-spas-osa-ca-cert)

3. Сконфигурированное JKS хранилище ключей с сертификатом и ключом для ОСА
(spi-realm-restapi-extension-sync-spas-osa-keystore)

Сгенерировать его можно следующим образом:

```
openssl pkcs12 -export -chain -inkey <путь к ключу> \
-in <путь к сертификату> -name "osa" -CAfile <путь к корневому сертификату> \
-out <путь к файлу с расширением p12> -password pass:<пароль>
```

```
keytool -importkeystore -noprompt \
-srcalias "osa" -destalias "osa" \
-srckeystore <путь к файлу с расширением p12> \
-srcstoretype pkcs12 \
-destkeystore <путь к файлу с расширением jks> \
-storepass <пароль> -srcstorepass <пароль>
```

Необходимо добавить сертификат в доверенные по инструкции в Руководстве по установке -> Настройка сети -> Добавление сертификатов в доверенные.

Часто встречающиеся проблемы и пути их устранения

KeyCloak.SE кэширует в памяти все, что может, в пределах возможностей JVM и/или ограничений, на которые настроено. Если база данных Keycloak была изменена третьей стороной (например, DBA) вне рамок REST API или консоли администратора сервера, есть вероятность, что часть кэша в памяти может быть устаревшей. Доступна очистка кэша realm, кэша пользователей или кэша внешних открытых ключей (открытые ключи внешних клиентов или поставщиков идентификационных данных, которые Keycloak обычно использует для проверки подписей конкретной внешней сущности) из консоли администратора, для этого необходимо перейти в левый пункт меню Настройки realm и на вкладку Кэш.

В случае, если настройки в консоли администратора не применяются даже после обновления страницы, то рекомендуется очистить кэш. Для этого необходимо перейти на вкладку *Очистить кэш*:

- Кнопка *Кэш Realm* - Удалить все записи в кэше realm (удалит все записи для всех realm).
- Кнопка *Кэш пользователей* - Очистить все записи в пользовательском кэше (это удалит записи для всех realm).
- Кнопка *Кэш ключей* - Очистить все записи в кэше внешних публичных ключей. Это ключи внешних ключей или провайдеров идентификации (это очистит все записи для всех realm).

The screenshot shows the Keycloak SE (KCSE) application interface. At the top, there is a dark header bar with the text "PLATFORM V". Below it, the main window has a dark sidebar on the left and a light-colored main content area on the right.

Sidebar (Left):

- Section: Конфигурация
 - Настройки Realm
 - Клиенты
 - Шаблоны клиентов
 - Роли
 - Поставщики идентификации
 - Федерация пользователей
 - Аутентификация
- Управление
 - Группы
 - Пользователи
 - Сессии
 - События
 - Импорт
 - Экспорт
- Очистить кэш
- Синхронизация ролей и ФОС

Main Content Area (Right):

Очистка кэша Test

Кэш Realm ? Очистить

Кэш пользователей ? Очистить

Кэш ключей ? Очистить

Руководство оператора компонента Keycloak.SE (KCSE)

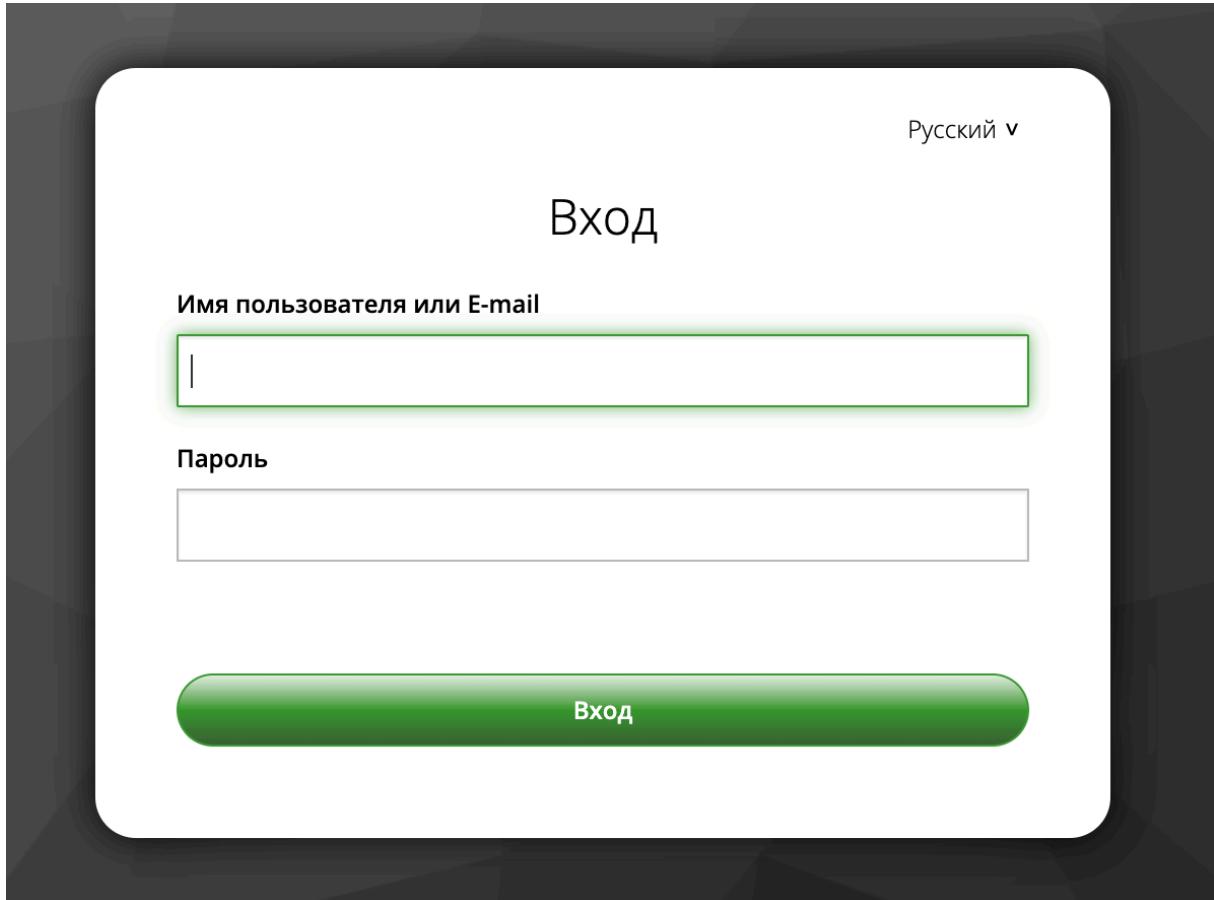
Доступ к приложению

Вход в приложение как пользователь

Вход пользователя в Keycloak.SE используется редко, т.к. данный продукт обычно выступает в качестве провайдера идентификации (IDP) для других приложений. В случае, если продукт внедрен в систему, базовый сценарий выглядит следующим образом:

1. Пользователю необходимо войти в приложение, использующее продукт в качестве провайдера идентификации (IDP);
2. Пользователь нажимает войти с помощью провайдера идентификации (IDP);

3. Пользователь перенаправляется на форму аутентификации Keycloak.SE;
4. Пользователь вводит учетные данные для входа.



5. В случае необходимости пользователь проходит дополнительные шаги аутентификации, например, OTP;
6. В случае успешного входа пользователь перенаправляется обратно в приложение;
 1. Тем временем приложение получает токен доступа для запроса информации о пользователе от провайдера идентификации (IDP).

Для доступа в консоль администратора у пользователя должна быть роль реалма - `platformauth_admin`.

Приложение поддерживает браузеры, указанные в требованиях к стороннему ПО.

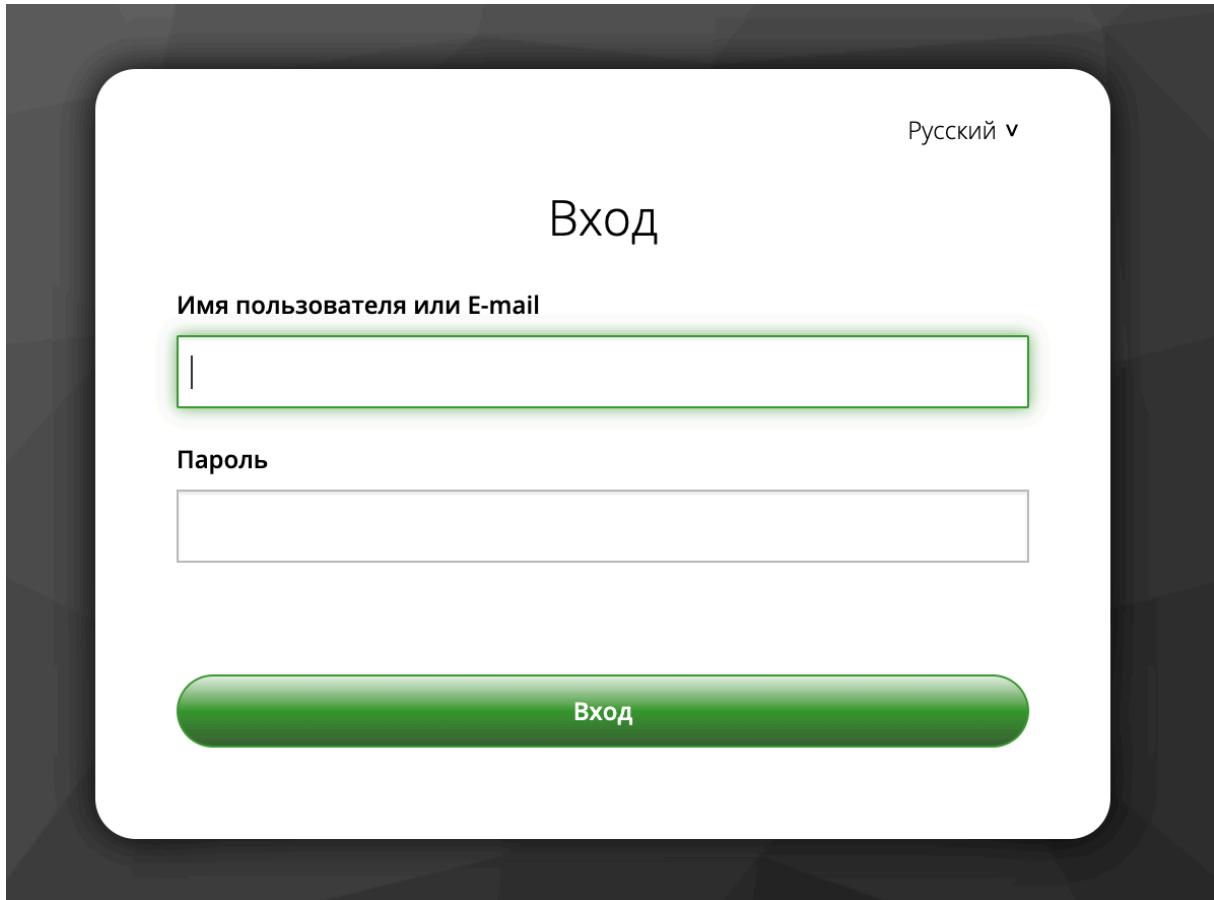
Вход в приложение как администратор

Для доступа в консоль администратора у пользователя должна быть административная роль реалма - `platformauth_admin`.

Приложение поддерживает браузеры, указанные в требованиях к стороннему ПО.

Для того чтобы выполнить вход под администратором, необходимо:

1. Перейти по ссылке, которая указана в настройках конфигурации (endpoint);
2. Ввести учетные данные (логин/пароль) администратора;



3. В случае успешной аутентификации отобразится консоль администратора.

Вход в Account console

KeyCloak.SE имеет встроенную службу учетных записей, к которой имеет доступ каждый пользователь - Личный кабинет (Account console). Этот сервис позволяет пользователям управлять своей учетной записью, изменять учетные данные, обновлять свой профиль, изменять пароль и просматривать сеансы входа в систему. URL-адрес этого сервиса: /realms/{realm-name}/account. Для доступа в личный кабинет у пользователя должна быть роль клиента account (роль интегрированных систем) - manage-account.

Приложение поддерживает браузеры, указанные в требованиях к стороннему ПО.

Учетная запись

Учетная запись – это профиль пользователя. В данном разделе указаны данные о пользователе. Редактирование данных пользователя через личный кабинет недоступно. Изменить данные может администратор через консоль администратора.

Пароль

В данном разделе пользователю доступна смена пароля.

The screenshot shows the 'Password' configuration page. On the left sidebar, 'Пароль' (Password) is selected. The main area is titled 'Смена пароля' (Change Password). It contains three input fields: 'Текущий пароль' (Current password), 'Новый пароль' (New password), and 'Подтверждение пароля' (Confirm password). A note at the top right says 'Все поля обязательны' (All fields are mandatory). A blue 'Сохранить' (Save) button is located at the bottom right. Below the form, there is a section titled 'Правила парольной политики:' (Password policy rules) with a bulleted list of requirements.

- Максимальный срок действия пароля – **42 дня**
- Пароль должен быть отличен от **3 последних паролей**
- Минимальная длина пароля **8 символов**
- Пароль должен содержать **минимум 1 букву в нижнем регистре, 1 букву в верхнем регистре, и одну не букву**
- Пароль должен содержать **6 уникальных символов**
- Не допускается в пароле **3 и более рядом расположенных на клавиатуре символов**
- Пароль не должен совпадать с логином пользователя

Сессии

В данном разделе отображаются активные сессии. Для каждой сессии предоставляется информация об устройстве, с которого был выполнен вход, времени начала сессии, под каким клиентом выполнен вход.

The screenshot shows the 'Sessions' list page. On the left sidebar, 'Сессии' (Sessions) is selected. The main area is titled 'Сессии'. It displays a table with one row, showing a session for IP 172.23.0.1, started on 29.08.2022 08:53:10 GMTZ, last accessed on 29.08.2022 09:01:11 GMTZ, and set to expire on 29.08.2022 18:53:10 GMTZ. The 'Подсистемы' (Subsystems) column shows 'security-admin-console account'. A blue 'Выйти из всех сессий' (Logout from all sessions) button is located at the bottom left of the table.

IP	Начата	Последний доступ	Истекает	Подсистемы
172.23.0.1	29.08.2022 08:53:10 GMTZ	29.08.2022 09:01:11 GMTZ	29.08.2022 18:53:10 GMTZ	security-admin-console account

Приложения

В данном разделе отображается список приложений, к которым есть доступ у пользователя.

The screenshot shows the 'Applications' list page. On the left sidebar, 'Приложения' (Applications) is selected. The main area is titled 'Приложения'. It displays a table with five rows, each representing an application and its available roles and consent status. The columns are 'Приложение' (Application), 'Available Roles' (Available Roles), 'Согласованные разрешения' (Granted permissions), 'Дополнительные соглашания' (Additional agreements), and 'Действие' (Action).

Приложение	Available Roles	Согласованные разрешения	Дополнительные соглашания	Действие
Учетная запись	Доступ оффлайн, Управление учетной записью в Учетная запись , Manage account links в Учетная запись , Просмотр профиля в Учетная запись	Полный доступ		
Account Console	Доступ оффлайн, Управление учетной записью в Учетная запись , Manage account links в Учетная запись	Полный доступ		
Командный интерфейс администратора	Доступ оффлайн	Полный доступ		
Консоль администратора безопасности	Доступ оффлайн	Полный доступ		

Использование приложения оператором

Сценарии Использования

В консоли администрирования Keycloak.SE существует несколько основных вариантов использования:

п/п	сценарий	Ролевая модель для выполнения сценариев использования Keycloak.SE оператором
1	Создание пользователя (Create User)	add-users + manage-users
2	Управление ролями пользователя (manage users role)	allow-map-roles + view-users
3	Блокировка/разблокировка пользователя	manage-users + query-realm + query-users
4	Создание Client (Create Client)	create-client или manage-clients + view-clients
5	Управление Client (manage Client)	manage-clients + view-clients
6	Создание и управление Группами (Create and manage Groups)	query-groups + manage-users

Для доступа ко всем разделам администрирования может быть предназначена роль `realm-admin`.

Возможности оператора:

1. Управление ролями (Manage Roles);
2. Управление пользователями(Manage Users);
3. Управление клиентами (Manage Clients);
4. Управление группами (Manage Groups).

Главное отличие оператора от администратора - администратору доступны настройки `realm`, провайдеров, аутентификации и прочее.

Ограничение действий, доступных оператору, регулируется либо отсутствием разделов/кнопок (разделы становятся доступны при назначении отдельных ролей, например роль `allow-sync-users` предоставляет доступ к вкладке “Синхронизация ролей и ФОС” для запуска синхронизации УЗ с ОСА), либо блокировкой элементов (например, роль `allow-map-roles` делает активным раздел “Сопоставление ролей” в профиле пользователя, при отсутствии этой роли страница назначения ролей неактивна/кнопки некликабельны)

Создание пользователя оператором

Создание пользователя (user) происходит в рамках конкретного Realm, созданного системным администратором или оператором (в зависимости от вашей ролевой модели), т.е. учетная запись пользователя будет в рамках конкретного Realm и в других Realm поддерживаться не будет.

Для создания пользователя необходимо выполнить следующие действия:

- Перейти на вкладку “Пользователи” и нажать “Добавить пользователя”.

ID	Имя пользователя	E-mail	Фамилия	Имя	Действия
7bb6fa82-3f67-4d51-8215-ed73d2b11967	admin	test@test.ru	namefamily	Умка	Редактировать Имперсонировать Удалить Редактировать Имперсонировать Удалить Редактировать Имперсонировать Удалить
ca52e974-bd7c-413e-a254-578fe51905ff					
7bd632f2-9418-4ffc-a64d-01a834cbfc59	тест				

- Заполнить необходимые поля (Поле: Имя пользователя - обязательно) и нажать кнопку “Сохранить”.

Добавить пользователя

ID

Создан

Имя пользователя *

E-mail

Внутренний E-mail

Имя

Отчество

Фамилия

Мобильный телефон

Внутренний телефон

Должность

Пользователь включен Вкл Выкл

Подтверждение E-mail

Группы Выберите существующую группу...
Группа не выбрана

Требуемые действия от пользователя Выберите действие...

Язык Выберите...

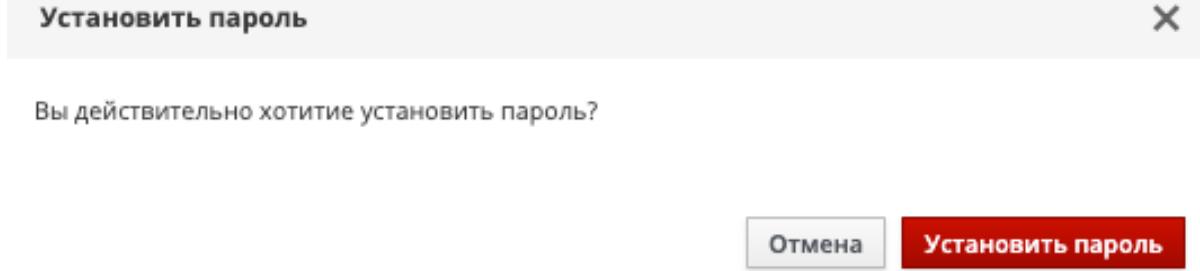
Для установки пароля необходимо перейти во вкладку “Учетные данные” и установить пароль пользователя:

1. Ввести пароль в поле “Новый пароль”;
2. Повторить введенный пароль в поле “Подтверждение пароля”;
3. При необходимости установить переключатель временного пароля в нужное положение;
4. Нажать кнопку “Установить пароль”.

The screenshot shows the Keycloak administration interface. On the left, a sidebar menu includes sections like 'Master', 'Конфигурация' (with sub-options like 'Настройки Realm', 'Клиенты', etc.), 'Управление' (with sub-options like 'Группы', 'Пользователи'), and 'Сессии'. The main content area is titled 'Тест' and shows the 'Учетные данные' tab selected. A sub-section titled 'Управление паролями' contains fields for 'Новый пароль' and 'Подтверждение пароля', which are both highlighted with a red border.

5. Подтвердить установку пароля для пользователя:

1. Нажать кнопку “Установить пароль”.



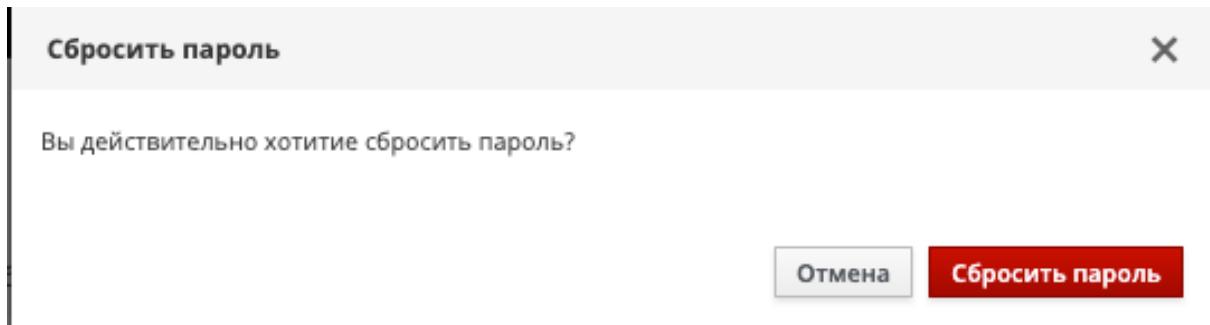
Для сброса пароля необходимо перейти во вкладку “Учетные данные” и совершить следующие действия:

1. Ввести пароль в поле “Пароль”;
2. Повторить введенный пароль в поле “Подтверждение пароля”;
1. Нажать кнопку “Сбросить пароль”.

The screenshot shows the Keycloak Platform interface. The left sidebar is titled 'PLATFORM V' and contains sections for Configuration (Настройки Realm, Клиенты, Шаблоны клиентов, Роли, Поставщики), Identity (идентификации, Федерация), Users (пользователей, Аутентификация), and Management (Группы, Пользователи, Сессии, События, Импорт, Экспорт, Очистить кэш, Синхронизация ролей и ФОС). The 'Пользователи' section is currently selected. The main content area shows a user named 'Тест' with tabs for Details, Attributes, Account Data (highlighted in blue), Role Mappings, Groups, Consents, Sessions, and Additional. The 'Account Data' tab displays a 'Password Management' section with fields for 'Password' and 'Confirm password', both of which are enclosed in a red rectangular box. Below these fields are 'Temporary' and 'On' buttons for password expiration, and a 'Reset Password' button.

3. Подтвердить сброс пароля для пользователя;

1. Нажать кнопку “Сбросить пароль”.



Можно установить требуемые действия от пользователя при входе:

1. Необходимо в разделе “Пользователи” на вкладке “Детали”, выбрать одно или несколько значений из выпадающего списка “Требуемые действия от пользователя”:

The screenshot shows the Keycloak Platform interface. On the left, there's a sidebar with 'Master' selected. Under 'Configuration', 'Настройки Realm' is highlighted. Under 'Управление', 'Пользователи' is selected. The main area shows a user named 'Тест' with various details like ID, creation date, and email. A red box highlights a dropdown menu titled 'Требуемые действия от пользователя' (Actions required from user) which contains several options.

Для добавления пользователя в группу, необходимо в поле “Группы” найти и выбрать требуемое название. Созданному пользователю будут назначены все роли, присутствующие у группы.

Удаление пользователя

Для удаления пользователя необходимо наличие роли `delete-users`

Для удаления пользователя необходимо выполнить следующие действия:

- Перейти на вкладку “Пользователи”, найти нужного пользователя и нажать “Удалить”.

The screenshot shows the 'Users' list in the Keycloak Platform. The 'Overview' tab is selected. A red box highlights the 'Delete' button in the 'Actions' column for a user row. The table lists various users with their IDs, names, emails, and other details.

ID	Имя пользователя	Внутренний E-mail	Фамилия	Имя	Действия
3424120	superman2@kael.com	4021132	3424120	Редактировать	Удалить
4121130api-test	4121130api-test@kael.com	2550151	4121130	Редактировать	Удалить
4125133api-test	4125133api-test@kael.com	1204135	4125133	Редактировать	Удалить
4222142api-test	4222142api-test@kael.com	4200123	4222142	Редактировать	Удалить
4504141api-test	1522153@test.ru	1253141	1522153	Редактировать	Удалить
4555134api-test	3110132@test.ru	4413130	3110132	Редактировать	Удалить

- Подтвердить удаление пользователя в модальном окне.

The screenshot shows the Keycloak Platform V interface. On the left, there's a sidebar with sections like 'Настройки Realm', 'Клиенты', 'Шаблоны клиентов', 'Роли', 'Поставщики идентификации', 'Федерация пользователей', and 'Аутентификация'. Under 'Управление', there are 'Группы', 'Пользователи', 'Сессии', 'События', 'Импорт', and 'Экспорт'. The 'Пользователи' section is selected. A modal dialog titled 'Удалить User' is open, asking 'Вы действительно хотите навсегда удалить user 32b6ba2b-de19-482f-b157-27edab369305?'. It has 'Отмена' and 'Удалить' buttons. Below the modal is a table listing users with columns: ID, Имя пользователя, Внутренний E-mail, Фамилия, Имя, and Действия. One row is highlighted.

Управление ролями пользователя

Роли пользователя - сущность, в рамках которой определяется тип и категория пользователя. В отличие от назначения конкретного доступа, в компоненте Keycloak.SE продукта Platform V IAM SE доступ и разрешение на выполнение операций назначается определенной роли, которая в свою очередь привязывается к пользователю.

Для создания роли необходимо выполнить следующие шаги:

1. Необходимо перейти во вкладку - Роли и выбрать - Добавить роль

The screenshot shows the Keycloak Platform V interface. The 'Roles' section is selected in the sidebar. A modal dialog titled 'Добавить роль' is open, with a red box around the 'Добавить роль' button. The main table lists existing roles with columns: Наименование роли, Составная, Описание, and Действия. One row is highlighted.

2. Заполнить необходимые поля (Поле: Наименование роли - обязательное)

- После создания роли откроется окно управления ролью. В нем можно установить признак составной роли, заполнить дополнительные атрибуты и внести прочие изменения:

В настройках пользователя также можно осуществить сопоставление ролей Realm/клиентов:

- Перейти во вкладку – Пользователи, выбрать необходимого пользователя и нажать - Редактировать

ID	Имя пользователя	E-mail	Фамилия	Имя	Действия
7be6fa82-39a7-4d51-8215-e073d2b11947	admin	test@test.ru		Илья	Редактировать
ca52e974-94f5-413e-a254-578fe419056f	namefamily				Имперсонировать
7be6fa82-9418-4fc4-a64d-01a834bcfd59	тест				Удалить
deab07b1-7fc7-4b74-810a-0e72eaf6d51d	тесттест				Имперсонировать

2. Открыть вкладку – Сопоставление ролей

1. Для добавления ролей - выделить необходимые роли Realm из окна - Доступные роли и нажать кнопку - Добавить выбранное, после чего выбранные роли будут перемещены в окно Присвоенных ролей. Также можно выбрать из выпадающего списка – Роли клиентов.

2. Для удаления ролей пользователю - выделить необходимые роли Realm из окна - Присвоенные роли и нажать кнопку - Удалить выбранное, после чего выбранные роли будут перемещены в окно Доступных ролей. Также можно выбрать из выпадающего списка – Роли клиентов.

1 Сопоставление ролей

2 Available Roles

3 Granted Roles

Для удаления роли необходимо выполнить следующие шаги:

1. Необходимо перейти во вкладку - Роли, выбрать роль и нажать - Удалить

Roles

Удалить Role

Вы действительно хотите навсегда удалить роль 3505144?

Отмена Удалить

2. В модальном окне подтвердить удаление роли

Успех! Роль успешно удалена

3. После удаления роли появится модальное окно подтверждения

Успех! Роль успешно удалена

Блокировка/разблокировка пользователя

Блокировка/разблокировка пользователя служит для проставления признака (включения/отключения) возможности авторизоваться и входить в систему под учетными данными пользователя.

Для блокировки/разблокировки пользователя необходимо выполнить следующие действия:

1. Необходимо перейти во вкладку “Пользователи”, выбрать необходимого пользователя и нажать “Редактировать”.

2. Перевести в нужное положение переключатель - Пользователь включен (вкл - если пользователь активен, т.е. разблокирован, выкл - если пользователь не активен, т.е. заблокирован) и нажать “Сохранить”.

Создание клиента

Создание клиента

Создание клиента (client) происходит в рамках конкретного Realm, созданного системным администратором или оператором (в зависимости от вашей ролевой модели), т.е. клиент будет в рамках конкретного Realm и в других Realm поддерживаться не будет.

Для создания клиента необходимо выполнить следующие действия:

- Перейти на вкладку “Клиенты” и нажать “Создать”.

ID клиента	Включено	Базовый URL	Действия
account	Да	http://localhost:18080/auth/realm/master/account/	Редактировать Экспорт Удалить
account-console	Да	http://localhost:18080/auth/realm/master/account/	Редактировать Экспорт Удалить
admin-cli	Да	Не задан	Редактировать Экспорт Удалить
broker	Да	Не задан	Редактировать Экспорт Удалить
master-realm	Да	Не задан	Редактировать Экспорт Удалить
q1w2e3r4	Да	Не задан	Редактировать Экспорт Удалить
security-admin-console	Да	http://localhost:18080/auth/admin/master/console/	Редактировать Экспорт Удалить
Test	Да	Не задан	Редактировать Экспорт Удалить
Test-realm	Да	Не задан	Редактировать Экспорт Удалить
Тестик	Да	Не задан	Редактировать Экспорт Удалить

- Заполнить необходимые поля (Поле: ID клиента - обязательное) и нажать кнопку “Сохранить”.

Добавить клиента

Импорт	Выберите файл
ID клиента *	<input type="text"/>
Тенант	ВыК
Протокол клиента	openid-connect
Корневой URL	
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Вторым способом создания клиента является импорт из файла в формате JSON.

Для импорта клиента из файла необходимо:

- Перейти на вкладку “Клиенты” и нажать “Создать”.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

ID клиента	Включено	Базовый URL	Действия
account	Да	http://localhost:18080/auth/realm/master/account/	Редактировать Экспорт Удалить
account-console	Да	http://localhost:18080/auth/realm/master/account/	Редактировать Экспорт Удалить
admin-cli	Да	Не задан	Редактировать Экспорт Удалить
broker	Да	Не задан	Редактировать Экспорт Удалить
master-realm	Да	Не задан	Редактировать Экспорт Удалить
q1w2e3r4	Да	Не задан	Редактировать Экспорт Удалить
security-admin-console	Да	http://localhost:18080/auth/admin/master/console/	Редактировать Экспорт Удалить
Test	Да	Не задан	Редактировать Экспорт Удалить
Test-realm	Да	Не задан	Редактировать Экспорт Удалить
Тестик	Да	Не задан	Редактировать Экспорт Удалить

- Нажать кнопку “Выбрать файл” в строке “Импорт”. Выбрать файл в формате JSON и нажать кнопку “Открыть”. Поля заполняются автоматически.

- Нажать кнопку “Сохранить”.

Пример файла:

```
{
  "clientId": "test_client",
  "description": "Описание",
  "rootUrl": "${authAdminUrl}",
  "baseUrl": "/realms/test/account/",
  "surrogateAuthRequired": false,
  "enabled": true,
  "alwaysDisplayInConsole": false,
  "clientAuthenticatorType": "client-secret",
  "secret": "burnANqd4V5pNyX7pHFyE6BfOiOVshLS",
  "redirectUris": [
    "http://localhost:8080/auth/realms/test/protocol/openid-connect/auth"
  ]
}
```

```
        "/realms/test/account/*"
    ],
    "webOrigins": [],
    "notBefore": 0,
    "bearerOnly": false,
    "consentRequired": false,
    "standardFlowEnabled": true,
    "implicitFlowEnabled": false,
    "directAccessGrantsEnabled": true,
    "serviceAccountsEnabled": true,
    "authorizationServicesEnabled": true,
    "publicClient": false,
    "frontchannelLogout": false,
    "protocol": "openid-connect",
    "attributes": {
        "saml.assertion.signature": "false",
        "id.token.as.detached.signature": "false",
        "client.secret.creation.time": "1681205796",
        "saml.multivalued.roles": "false",
        "saml.force.post.binding": "false",
        "saml.encrypt": "false",
        "oauth2.device.authorization.grant.enabled": "true",
        "saml.server.signature": "false",
        "backchannel.logout.revoke.offline.tokens": "false",
        "saml.server.signature.keyinfo.ext": "false",
        "use.refresh.tokens": "true",
        "exclude.session.state.from.auth.response": "false",
        "oidc.ciba.grant.enabled": "false",
        "saml.artifact.binding": "false",
        "backchannel.logout.session.required": "true",
        "client_credentials.use_refresh_token": "false",
        "saml_force_name_id_format": "false",
        "saml.client.signature": "false",
        "tls.client.certificate.bound.access.tokens": "false",
        "require.pushed.authorization.requests": "false",
        "saml.authnstatement": "false",
        "display.on.consent.screen": "false",
        "saml.onetimeuse.condition": "false"
    },
    "authenticationFlowBindingOverrides": {},
    "fullScopeAllowed": true,
    "nodeReRegistrationTimeout": -1,
    "protocolMappers": [
    {
```

```
"name": "Client IP Address",
"protocol": "openid-connect",
"protocolMapper": "oidc-usersessionmodel-note-mapper",
"consentRequired": false,
"config": {
    "user.session.note": "clientAddress",
    "id.token.claim": "true",
    "access.token.claim": "true",
    "claim.name": "clientAddress",
    "jsonType.label": "String"
},
{
    "name": "Client ID",
    "protocol": "openid-connect",
    "protocolMapper": "oidc-usersessionmodel-note-mapper",
    "consentRequired": false,
    "config": {
        "user.session.note": "clientId",
        "id.token.claim": "true",
        "access.token.claim": "true",
        "claim.name": "clientId",
        "jsonType.label": "String"
    }
},
{
    "name": "Esia_info",
    "protocol": "openid-connect",
    "protocolMapper": "esia-user-info-mapper",
    "consentRequired": false,
    "config": {
        "esia.attributes.filter": "PLV",
        "id.token.claim": "true",
        "access.token.claim": "true",
        "claim.name": "esia.attributes.info",
        "userinfo.token.claim": "true"
    }
},
{
    "name": "Client Host",
    "protocol": "openid-connect",
    "protocolMapper": "oidc-usersessionmodel-note-mapper",
    "consentRequired": false,
    "config": {
```

```
"user.session.note": "clientHost",
"id.token.claim": "true",
"access.token.claim": "true",
"claim.name": "clientHost",
"jsonType.label": "String"
}
},
],
"defaultClientScopes": [
"web-origins",
"acr",
"openid",
"profile",
"roles",
"https://api.sberbank.ru/sendSMS",
"email"
],
"optionalClientScopes": [
"address",
"phone",
"offline_access",
"microprofile-jwt"
],
"access": {
"view": true,
"configure": true,
"manage": true
}
}
```

Управление клиентом

Редактирование клиента

1. После создания клиента (client) откроется окно редактирования клиента. В нем можно заполнить данные клиента и применить различные настройки управления клиентом.

The screenshot shows the Keycloak configuration interface for a client named 'Тест'. The 'Настройки' tab is selected. The configuration includes:

- ID клиента: Тест
- Имя: (empty)
- Описание: (empty)
- Включено: ВКЛ (Enabled)
- Необходимо согласие: ВЫК (Consent Required)
- Тенант: ВЫК (Tenant)
- Тема страницы входа: (empty)
- Протокол клиента: openid-connect
- Тип доступа: public
- Standard Flow включен: ВКЛ (Enabled)
- Implicit Flow включен: ВЫК (Disabled)
- Direct Access Grants включен: ВКЛ (Enabled)
- Корневой URL: (empty)
- * Валидация URI перенаправления: (empty)
- Базовый URL: (empty)
- URL администрирования приложения: (empty)
- Web источники: (empty)

2. Клиенту можно задать определенную роль/ряд ролей:

1. Необходимо перейти во вкладку “Роли” и нажать “Добавить роль”.

The screenshot shows the 'Роли' tab for the 'Тест' client. A new role named 'Тестовая роль' has been added. The table shows:

Назначение роли	Составная	Описание	Действия
Тестовая роль	Нет	Описание тестовой роли	Редактировать Удалить

2. Заполнить необходимые поля (Поле: Наименование роли - обязательное) и нажать кнопку “Сохранить”.

3. После создания роли можно дополнить ее необходимыми атрибутами или установить к ней составные роли.
4. Перевести в положение вкл. кнопку “Составные роли”, выделить необходимые “роли Realm” из окна “Доступные роли” и нажать кнопку “Добавить выбранное”, после чего выбранные роли будут перемещены в окно “Ассоциированных ролей”.

Удаление клиента

Для удаления клиента необходимо выполнить следующие действия:

1. Перейти на вкладку “Клиенты”, найти нужного клиента и нажать “Удалить”.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

The screenshot shows the 'Клиенты' (Clients) section of the Keycloak Platform. A modal window titled 'Удалить Client' (Delete Client) is open, asking 'Вы действительно хотите навсегда удалить client test?' (Do you really want to permanently delete client test?). The 'Удалить' (Delete) button is highlighted with a red border.

ID клиента	Включено	Базовый URL	Действия
account	Да	https://kcse-pub2-tribe-sc-kcse-ift-2.apps.ocp.devpub.solution.sbt/auth/realm/test/account/	Редактировать Экспорт Удалить
account-console	Да	https://kcse-pub2-tribe-sc-kcse-ift-2.apps.ocp.devpub.solution.sbt/auth/realm/test/account/	Редактировать Экспорт Удалить
admin-cli	Да	Не задан	Редактировать Экспорт Удалить
broker	Да	Не задан	Редактировать Экспорт Удалить
client_osa	Да	Не задан	Редактировать Экспорт Удалить
realm-management	Да	Не задан	Редактировать Экспорт Удалить

2. Подтвердить удаление клиента в модальном окне.

The screenshot shows the 'Клиенты' (Clients) section after deletion. A modal window titled 'Удалить Client' (Delete Client) is open, displaying the confirmation message 'Вы действительно хотите навсегда удалить client test?' (Do you really want to permanently delete client test?). The 'Удалить' (Delete) button is highlighted with a red border.

3. После удаления клиента появится модальное окно подтверждения.

The screenshot shows the 'Клиенты' (Clients) section after successful deletion. A green success message 'Успех! Клиент успешно удален' (Success! Client successfully deleted) is displayed at the top. The 'realm-management' client is no longer listed in the table.

ID клиента	Включено	Базовый URL	Действия
account	Да	https://kcse-pub2-tribe-sc-kcse-ift-2.apps.ocp.devpub.solution.sbt/auth/realm/test/account/	Редактировать Экспорт Удалить
account-console	Да	https://kcse-pub2-tribe-sc-kcse-ift-2.apps.ocp.devpub.solution.sbt/auth/realm/test/account/	Редактировать Экспорт Удалить
admin-cli	Да	Не задан	Редактировать Экспорт Удалить
broker	Да	Не задан	Редактировать Экспорт Удалить
client_osa	Да	Не задан	Редактировать Экспорт Удалить
realm-management	Да	Не задан	Редактировать Экспорт Удалить

Создание и Управление группами

Группы (Groups) – это сущность, позволяющая управлять общим набором атрибутов, присущих данной группе. Пользователь может входить в любое количество групп или не входить в них вовсе. При этом пользователи наследуют атрибуты и роли, присвоенные данной группе. Также группы могут иметь иерархию, т.е. у каждой группы может быть n - количество подгрупп, но при этом у каждой группы может быть только один родитель.

Создание группы

Для создания групп необходимо:

1. Перейти во вкладку “Группы”, нажать кнопку “Создать”

2. Ввести наименование группы в поле “Имя”, нажать на кнопку “Сохранить”

Создать группу

Имя *	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Добавление пользователей в группу

Для добавления пользователей в группу, необходимо:

1. Перейти на страницу “Пользователи”, выбрать необходимого пользователя и нажать “Редактировать”.

ID	Имя пользователя	E-mail	Фамилия	Имя	Действия
7be0fa62-3e7-4d51-8215-ed73d2b119d7	admin				<input type="button" value="Редактировать"/> <input type="button" value="Интересоваться"/> <input type="button" value="Удалить"/>
ca52e974-9df5-413e-a254-578fe19056f	namefamily	test@test.ru	Фамилия	Имя	<input type="button" value="Редактировать"/> <input type="button" value="Интересоваться"/> <input type="button" value="Удалить"/>
7be6d12f-9418-4fc-a640-01a834cb5c59	test				<input type="button" value="Редактировать"/> <input type="button" value="Интересоваться"/> <input type="button" value="Удалить"/>
d0d207b1-7fc7-4b74-810a-0e72eaaf6d51	тест				<input type="button" value="Редактировать"/> <input type="button" value="Интересоваться"/> <input type="button" value="Удалить"/>

2. Перейти на вкладку “Группы”. В окне “Доступные группы” должны отобразиться все имеющиеся группы (или при нажатии кнопки “Показать все группы”).

1. Для добавления пользователя в группу необходимо выделить в окне “Доступные группы” необходимую группу и нажать “Присоединиться”

- Для того, чтобы исключить пользователя из группы, необходимо в окне “Членство в группах” выделить необходимую группу и нажать кнопку “Покинуть”.

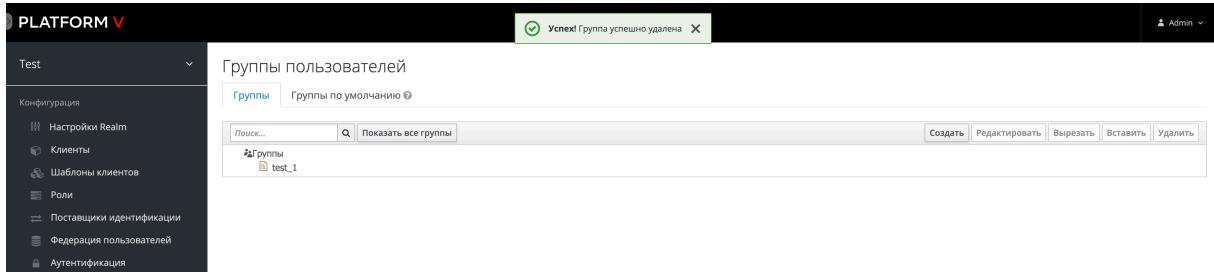
Удаление группы

Для удаления групп необходимо:

- Перейти на вкладку “Группы”, выделить необходимую группу и нажать кнопку “Удалить”.

- Подтвердить удаление группы в модальном окне.

- После удаления группы появится модальное окно подтверждения.



Часто встречающиеся проблемы и пути их устранения

База проблем нарабатывается и для текущего релиза частых проблем не выявлено.

Параметры настройки

Оператору доступны настройки параметров безопасности в части идентификации и аутентификации:

1. Flow (Сценарии) - позволяет настраивать необходимый сценарий аутентификации и его исполнение;
2. Сопоставления - позволяет установить сценарий, который необходимо использовать для аутентификации;
3. Требуемые действия - возможность установки обязательных действий пользователя для создания учетной записи;
4. Политики пароля - установка пароля с ограничениями по длине, безопасности или сложности, в зависимости от требований производственных сред;
5. Политики OTP - возможность задать параметры одноразового пароля. OTP - это пароль, действительный только для одного сеанса аутентификации.

Для изменения параметров оператору должна быть назначена роль `manage-realm`.

Flow (Сценарии)

1. Для построения нового Flow необходимо перейти во вкладку - Аутентификация и нажать кнопку - Создать.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

The screenshot shows the Keycloak SE platform interface. The left sidebar is titled 'PLATFORM' and contains sections for 'Master', 'Конфигурация' (Configuration) with items like 'Настройки Realm', 'Клиенты', 'Шаблоны клиентов', 'Роли', 'Поставщики идентификации', 'Федерация пользователей', and 'Аутентификация' (1), which is selected. Below these are 'Управление' (Management) sections for 'Группы', 'Пользователи', 'Сессии', 'События', 'Импорт', 'Экспорт', 'Очистить кеш', and 'Синхронизация ролей и ФОС'. The main content area is titled 'Аутентификация' and shows a table of authentication scenarios. The table has columns for 'Тип аутентификации' (Authentication Type), 'Требования' (Requirements), and 'Действия' (Actions). A red box highlights the 'Создать' (Create) button at the top right of the table.

2. В открывшемся окне необходимо заполнить имеющиеся поля и нажать - Сохранить.

The screenshot shows the 'Create top-level flow' form. The left sidebar is identical to the previous screenshot. The main form has a title 'Создать верхнеуровневую форму' (Create top-level flow). It includes fields for 'Синоним' (Alias), 'Описание' (Description), and 'Top Level Flow Type' (Type, set to 'общий' - general). At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons. A red box highlights the 'Сохранить' button.

3. Для добавления необходимых исполнений нужно нажать на кнопку - Добавить исполнение, после чего выбрать из выпадающего списка интересующее значение и нажать Сохранить.

Создать исполнение а

The screenshot shows a dropdown menu with the following items:

- Allow Access
- Automatically Set Existing User
- Basic Auth Challenge
- Basic Auth Password+OTP
- Browser Redirect/Refresh** (highlighted in blue)
- Choose User
- Condition - User Configured
- Condition - User Role
- Conditional OTP Form
- Confirm Link Existing Account
- Cookie
- Create User If Unique
- Deny Access
- Detect Existing Broker User
- Docker Authenticator
- HTTP Basic Authentication
- Identity Provider Redirector
- Kerberos
- OTP
- OTP Form
- Password
- Password Form
- Reset OTP
- Reset Password
- Review Profile
- Send Reset Email
- Username Form
- Username Password Challenge
- Username Password Form
- Username Password Form For Identity Provider Reauthentication
- Username Validation
- Verify Existing Account By Email
- WebAuthn Authenticator
- WebAuthn Passwordless Authenticator
- X509/Validate Username
- X509/Validate Username Form

- Добавленные исполнения можно конфигурировать, менять их требования, менять их местами в иерархии, удалять и совершать прочие операции.

Сопоставления

- На странице Аутентификация во вкладке Сопоставления (Bindings) можно выбрать flow, который требуется к исполнению для конкретной цели:

The screenshot shows the 'Authentications' configuration page with the 'Bindings' tab selected. On the left, there is a sidebar with the following sections:

- Настройки Realm
- Клиенты
- Шаблоны клиентов
- Роли
- Поставщики идентификации
- Федерация пользователей
- Аутентификация** (highlighted with a red border)

The main area displays the 'Bindings' configuration. A red box highlights the dropdown menu for the 'User Agent' binding, which is set to 'browser'. Other dropdowns include 'registration', 'direct grant', 'reset credentials', and 'clients'.

- Выбрать значения из выпадающих списков:

- Сценарий браузера - Выберите flow, который вы хотите использовать для проверки подлинности браузера.
- Сценарий регистрации - Выберите flow, который вы хотите использовать для регистрации.

3. Сценарий Direct Grant Flow - Выберите flow, который вы хотите использовать для прямой проверки подлинности grant.
4. Сбросить учетные данные - Выберите flow, который вы хотите использовать, когда пользователь забыл свои учетные данные.
5. Аутентификация клиента - Выберите flow, который вы хотите использовать для аутентификации клиентов.

Требуемые действия

1. На странице Аутентификация во вкладке Требуемые действия можно выбрать обязательные действия пользователя для создания учетной записи.

Требуемое действие	Включено	Действие по умолчанию
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 type="checkbox"/>
Update Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Verify Email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete Account	<input type="checkbox"/>	<input type="checkbox"/>
Update User Locale	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Webauthn Register Passwordless	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Verify Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Webauthn Register	<input checked="" type="checkbox"/>	<input type="checkbox"/>

1. Можно менять местами в иерархии последовательности требуемых действий, включать/отключать, устанавливать, как действие по умолчанию.

Парольные политики

1. Для добавления парольных политик необходимо перейти на страницу Аутентификация, выбрать вкладку Политики пароля:
2. Выбрать из выпадающего списка - Добавить политику.

✓ Добавить политику

- Number of unique characters
- Expire Password
- Hashing Iterations
- How often the password can be changed (days)
- Not Password
- Password Blocklist
- Minimum Length
- Regular Expression
- Sequence of forbidden characters in the password (separator ||)
- Not Username
- Not Email
- Time period account before disabling a user
- Date to lock changing password after expire password
- Special Characters
- Uppercase Characters
- Lowercase Characters
- Distance for new password by X symbols
- Digits
- Hashing Algorithm

3. У добавленных парольных политик можно выбрать определенное значение.

Тип политики	Значение политики	Действия
Expire Password	365	Удалить
Password Blacklist		Удалить
Not Email		Удалить
Hashing Iterations	27500	Удалить
Not Recently Used	3	Удалить
Minimum Length	8	Удалить
Regular Expression		Удалить
Not Username		Удалить
Special Characters	1	Удалить
Uppercase Characters	1	Удалить
Lowercase Characters	1	Удалить
Digits	1	Удалить
Hashing Algorithm	pbkdf2-sha256	Удалить

Сохранить Отмена

Политики OTP

- Для добавления политик OTP необходимо на странице Аутентификация перейти во вкладку Политики OTP.
- На вкладке Политики OTP можно выбрать значения и конфигурации следующих политик:

Тип одноразового пароля OTP	Основан на времени
Алгоритм хеша OTP	SHA1
Количество цифр	6
Окно просмотра вперед	1
Период токена OTP	30

Поддерживаемые приложения: FreeOTP, Google Authenticator

Сохранить Отмена

Приведенные настройки направлены на обеспечение безопасности сервисов потребителей, с которыми интегрируется сервис провайдер аутентификации.

Правила эксплуатации

- Взаимодействие KeyCloak.SE с компонентами продукта Platform V Pangolin должно осуществляться на основе протокола TLS;
- Взаимодействие с компонентами продукта Platform V Audit должно осуществляться на основе протокола TLS;

3. Взаимодействия с компонентами продукта Platform V Monitor должно осуществляться на основе протокола TLS.
4. Формат экспорта/импорта данных скачиваемых конфигураций является json. Механизмы безопасности обеспечиваются ролевой моделью, опция доступна администратору.

Детальное описание полей интерфейса

Детальное описание вкладки Клиенты

Клиенты – это сущности, которые могут запросить аутентификацию пользователя.

Клиенты бывают двух видов:

- Первый тип клиентов – это приложения, которые хотят участвовать в единой регистрации. Эти клиенты просто хотят, чтобы KeyCloak.SE обеспечил безопасность для них.
- Другой тип клиентов – это клиенты, которые запрашивают токен доступа, чтобы иметь возможность вызывать другие службы от имени аутентифицированного пользователя.

Управление клиентом

Настройки

На рисунке ниже изображен интерфейс настройки клиента.

The screenshot shows the Keycloak SE configuration interface. On the left, there's a sidebar with sections like 'Master', 'Конфигурация', 'Настройки Realm', 'Клиенты', 'Шаблоны клиентов', 'Роли', 'Поставщики идентификации', 'Федерация пользователей', and 'Аутентификация'. Under 'Управление', there are links for 'Группы', 'Пользователи', 'Сессии', 'События', 'Импорт', 'Экспорт', 'Очистить кеш', and 'Синхронизация ролей и ФОС'. The main area is titled 'Тест' and has tabs for 'Настройки', 'Роли', 'Шаблоны клиентов', 'Сопоставления', 'Область', 'Отзыв', 'Сессии', 'Оффлайн доступ', and 'Установка'. The 'Настройки' tab is active. It contains fields for 'ID клиента' (Test), 'Имя' (Name), 'Описание' (Description), 'Включено' (Enabled) (set to 'Вкл'), 'Необходимо согласие' (Consent Required) (set to 'Выкл'), 'Тенант' (Tenant) (set to 'Выкл'), 'Тема страницы входа' (Theme), 'Протокол клиента' (Protocol) (set to 'openid-connect'), 'Тип доступа' (Access Type) (set to 'public'), 'Standard Flow включен' (Standard Flow Enabled) (set to 'Вкл'), 'Implicit Flow включен' (Implicit Flow Enabled) (set to 'Выкл'), 'Direct Access Grants включен' (Direct Access Grants Enabled) (set to 'Вкл'), 'Корневой URL' (Root URL), 'Валидация URI перенаправления' (URI Validation for Redirects) (with a '+' button), 'Базовый URL' (Base URL), 'URL администрирования приложения' (Application Admin URL), and 'Web источники' (Web Origins) (with a '+' button).

В таблице представлено детальное описание интерфейса настройки клиента.

Наименование настройки	Описание	Тип настройки
ID клиента	Задает идентификатор, указываемый в URI и в токенах. Например 'my-client'. Для SAML это также ожидаемое имя издателя для запросов аутентификации	Текстовое значение
Имя	Задает отображаемое название клиента. Например 'My Client'. Поддерживает ключи для локализованных значений. Например: \${my_client}	Текстовое значение
Описание	Задает описание клиента. Например 'Мой клиент для табеля учета времени'. Поддерживает ключи для локализованных значений. Например: \${my_client_description}	Текстовое значение
Включено	Отключенные клиенты не могут инициализировать вход или иметь возможность получить токены доступа.	Булевая
Необходимо согласие	Если включено, пользователи должны дать согласие на доступ клиентскому приложению.	Булевая
Отображение согласия на экране клиента	Применяется только в том случае, если параметр "Необходимо согласие" включен. Если этот переключатель выключен, экран согласия будет содержать только согласия, соответствующие настроенным областям клиента. Если переключатель включен, то на экране согласия будет также один пункт о самом клиенте.	Булевая

Наименование настройки	Описание	Тип настройки
Тема страницы входа	Применяется, если для данного клиента включена опция “Отображать клиента на экране согласия”. Содержит текст, который будет отображаться на экране согласия о разрешениях, относящихся только к этому клиенту.	Текстовое значение
Тема страницы входа	Выберите тему для страниц входа, временного одноразового пароля (OTP), выдачи разрешений, регистрации и восстановления пароля.	Выпадающий список
Протокол клиента	‘OpenID connect’ разрешает клиентам проверить личность конечного пользователя, основанного на выполнении аутентификации на Сервере Авторизации.’SAML’ включает веб-сценарии аутентификации и авторизации, включая кроссдоменные центры единого управления доступом (SSO) и использующие токены безопасности, содержащие заявления на передачу информации.	Выпадающий список
Тип доступа	‘Confidential’ клиенты требуют секрет для инициализации протокола входа. ‘Public’ клиентам секрет не требуется. ‘Bearer-only’ клиенты и веб-сервисы никогда не инициализируют вход.	Выпадающий список
Standard Flow включен	Включает стандартное OpenID Connect перенаправление, основанное на аутентификации с кодом авторизации. В терминах OpenID Connect или OAuth2 спецификаций включает ‘Authorization Code Flow’ для этого клиента.	Булевая
Implicit Flow включен	Включает поддержку OpenID Connect перенаправления, основанного на аутентификации без кода авторизации. В терминах OpenID Connect или OAuth2 спецификаций включает поддержку ‘Implicit Flow’ для этого клиента.	Булевая
Direct Access Grants включен	Включает поддержку Direct Access Grants, которая означает, что клиент имеет доступ к имени пользователя и пароля и обменивает их напрямую с сервером Keycloak на токен доступа. В терминах OAuth2 спецификации означает поддержку ‘Resource Owner Password Credentials Grant’ для этого клиента.	Булевая
Корневой URL	Корневой URL добавляется к относительным URL	Текстовое значение
Валидация URI перенаправления	Валидирует паттерн URI, на который может быть перенаправлен браузер после успешного входа или выхода. Разрешены простые ссылки, напр. ‘http://example.com/*’. Также допускается использовать относительный путь, напр. ‘/my/relative/path/*’. Относительные пути необходимо указывать относительно корневого URL клиента, или, если он не специфицирован, корневого URL сервера авторизации. Для SAML Вы должны задать валидный паттерн URI, если Вы полагаетесь на URL сервиса потребителя, внедренного в запрос авторизации.	Текстовое значение
Базовый URL	Используемый URL по умолчанию. Используется в случае, если серверу требуется перенаправление или обратная ссылка на клиента.	Текстовое значение

Наименование настройки	Описание	Тип настройки
URL администрирования приложения	URL для доступа к интерфейсу администратора в заданном клиенте. Необходимо установить, если клиент поддерживает адаптер REST API. Это REST API разрешает серверу авторизации сдать политики отзыва и прочие административные задачи. Обычно устанавливается значение, соответствующее базовому URL клиента.	Текстовое значение
Web источники	Разрешает CORS источникам. Чтобы разрешить всем источники с допустимыми URI-адресами переадресации, добавьте '+'. Чтобы разрешить все источники, добавьте '*'.	Текстовое значение

Тонкая настройка конфигурации OpenID Connect

На рисунке ниже изображен интерфейс тонкой настройки конфигурации OpenID Connect.

▼ Тонкая настройка конфигурации OpenID Connect 

Алгоритм подписи access-токена 	<input type="text"/>
Алгоритм подписи id-токена 	<input type="text"/>
Алгоритм подписи ответа информации о пользователе 	<input type="text" value="unsigned"/>
Алгоритм сигнатуры объекта запроса 	<input type="text" value="any"/>
Предоставлять объект запроса 	<input type="text" value="not required"/>

В таблице представлено детальное описание настройки конфигурации OpenID Connect.

Наименование Настройки	Описание	Тип Настройки
Алгоритм Подписи Access-Токена	JWA-Алгоритм, Используемый Для Подписи Access-Токена	Выпадающий Список
Алгоритм Подписи Id-Токена	JWA-Алгоритм, Используемый Для Подписи Id-Токена	Выпадающий Список
Алгоритм Подписи Ответа Информации О Пользователе	JWA Алгоритм Используется Для Подписи Ответа Ресурса Информации О Пользователе. Если Установлено В 'Unsigned', То Ответ Информации О Пользователе Не Будет Подписан И Будет Возвращен В Формате Application/json.	Выпадающий Список
Алгоритм Сигнатурь Объекта Запроса	JWA Алгоритм, Который Необходим Клиенту Для Использования Во Время Отсылки OIDC Запроса Объекта, Специфицированного По 'Request' Или 'Request_uri' Параметрам. Если Установлено В 'Any', То Объект Запроса Будет Подписан Любым Алгоритмом (включая 'None').	Выпадающий Список

Наименование Настройки	Описание	Тип Настройки
Предоставлять Объект Запроса	Указывает, Нужно Ли Клиенту Предоставить Объект Запроса С Запросом На Авторизацию, И Какой Метод Он Может Использовать Для Этого. Если Установлено Значение «не Требуется», Предоставление Объекта Запроса Необязательно. Во Всех Остальных Случаях Предоставление Объекта Запроса Обязательно. Если Установлено Значение «запрос», Объект Запроса Должен Быть Предоставлен По Значению. Если Установлено Значение «request_uri», Объект Запроса Должен Быть Предоставлен По Ссылке. Если Установлено Значение «gequest Или Request_uri», Можно Использовать Любой Метод.	Выпадающий Список

Режимы совместимости OpenID Connect

На рисунке ниже изображен интерфейс настройки режима совместимости OpenID Connect.

▼ Режимы совместимости OpenID Connect ?

Исключить параметр session_state
из ответа аутентификации.



ВЫК

В таблице представлено детальное описание интерфейса настройки режима совместимости OpenID Connect.

Наименование Настройки	Описание	Тип Настройки
Исключить Параметр Session_state Из Ответа Аутентификации	Если Включено, Параметр ‘Session_state’ Не Будет Включен В OpenID Connect Authentication Ответ. Это Полезно Если Клиент Использует Старый OIDC / OAuth2 Адаптер, Который Не Поддерживает Параметр ‘Session_state’.	Булевая

Расширенные настройки

На рисунке ниже изображен интерфейс расширенных настроек клиента.

▼ Расширенные настройки ?

Продолжительность жизни токена доступа
 минут



минут



Включить OAuth 2.0 Mutual TLS Certificate Bound Access Tokens



ВЫК

Ключ подтверждения для CodeChallengeMethod обмена кодами

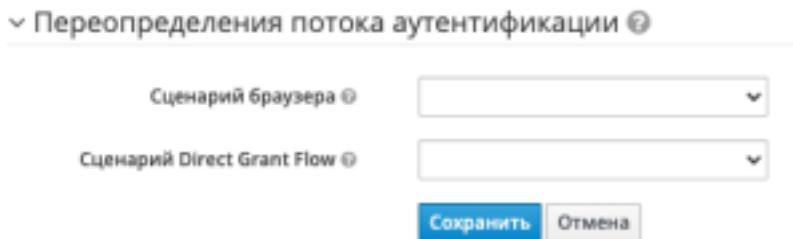


В таблице представлено детальное описание интерфейса расширенных настроек клиента.

Наименование Настройки	Описание	Тип Настройки
Продолжительность Жизни Токена Доступа	Максимальное Время Действия Токена Доступа. Значение Рекомендуется Устанавливать Как Можно Ближе К тайм-ауту SSO.	Цифровое Значение + Выпадающий Список
Включить OAuth 2.0 Mutual TLS Certificate Bound Access Tokens	Включает Поддержку Access-Токенов С Привязкой К Сертификату OAuth 2.0 Mutual TLS, Что Означает, Что KeyCloak.SE Связывает Access-Токен И Refresh-Токен С Сертификатом X.509 Клиента, Запрашивающего Токен, Который Обменивается Mutual TLS Между Конечной Точной Токена KeyCloak.SE И Этим Клиентом. Эти Токены Могут Рассматриваться Как Токены Держателя Ключа, А Не Токены На Предъявителя.	Булевая
Ключ Подтверждения Для CodeChallengeMethod Обмена Кодами	Выберите, Какой Метод Проверки Кода Для PKCE Используется. Если Не Указано Иное, KeyCloak.SE Не Применяет PKCE К Клиенту, Если Клиент Не Отправляет Запрос Авторизации С Соответствующим Запросом Кода И Методом Обмена Кода.	Выпадающий Список

Переопределение потока аутентификации

На рисунке ниже изображено окно настройки переопределения потока аутентификации.



В таблице представлено детальное описание интерфейса переопределения потока аутентификации.

Наименование Настройки	Описание	Тип Настройки
Сценарий Браузера	Выберите Сценарий, Который необходим Использовать Для Аутентификации Через Браузер.	Выпадающий Список
Сценарий Direct Grant Flow	Выберите Сценарий, Который необходим Использоваться Для Аутентификации Direct Grant.	Выпадающий Список
Ключ Подтверждения Для CodeChallengeMethod Обмена Кодами	Выберите, Какой Метод Проверки Кода Для PKCE Используется. Если Не Указано Иное, KeyCloak.SE Не Применяет PKCE К Клиенту, Если Клиент Не Отправляет Запрос Авторизации С Соответствующим Запросом Кода И Методом Обмена Кода.	Выпадающий Список

Роли

Перечень ролей

На рисунке ниже изображено окно со списком ролей клиента.

Наименование роли	Составная	Описание	Действия
Тестовая роль	Нет		<button>Добавить роль</button> <button>Редактировать</button> <button>Удалить</button>

В таблице представлено детальное описание интерфейса с представлением ролей клиента.

Наименование Настройки	Описание	Тип Настройки
Update Tenant Clients	По Нажатию Отправляется Запрос В ОСА На Получение Ролей Клиента (функциональность SCIM)	Кнопка
Добавить Роль	По Нажатию Открывает Окно Добавления Роли Клиента	Кнопка
Наименование Роли	Отображение Наименования Роли	Текстовое Значение
Составная	Признак Составной Роли	Текстовое Значение
Описание	Описание Роли Клиента	Текстовое Значение
Действия	Редактировать	По Нажатию Открывает Окно Редактирования Роли Клиента
Удалить	По Нажатию Удаляет Роль Клиента	Кнопка

Описание полей вкладки Роли находится в разделе Детальное описание вкладки Роли клиента.

Шаблоны клиентов

Настройка клиентских областей

Разрешить настройку клиентских областей, связанных с этим клиентом. На рисунке ниже изображен интерфейс настройки клиентских областей.

Тест

The screenshot shows the 'Client Areas' section of the Keycloak configuration. It includes four main sections:

- Default Client Areas (Default):** A list box containing 'web-origins', 'profile', 'roles', and 'email'. Below it is a button 'Добавить выбранное >' (Add selected).
- Available Client Areas (Available):** An empty list box with a button 'Добавить выбранное >' (Add selected) at the bottom.
- Assigned Client Areas (Assigned):** A list box containing 'address', 'phone', 'offline_access', and 'microprofile-jwt'. Below it is a button '< Удалить выбранное' (Delete selected).
- Optional Client Areas (Optional):** An empty list box with a button 'Добавить выбранное >' (Add selected) at the bottom.

В таблице представлено детальное описание полей интерфейса настройки клиентских областей.

Наименование Настройки	Описание	Тип Настройки
Области Клиента По Умолчанию	Области Клиента По Умолчанию Всегда Применяются При Выдаче Токенов Для Этого Клиента. Сопоставители Протоколов И Сопоставления Областей Ролей Применяются Всегда, Независимо От Значения Используемого Параметра Области В Запросе Авторизации OIDC.	
Доступные Клиентские Области	Области Действия Клиента, Которые Еще Не Назначены Как Области По Умолчанию Или Дополнительные Области	Поле С Выбором Значения
Назначенные Клиентские Области По Умолчанию	Области Действия Клиента, Которые Будут Использоваться В Качестве Областей Действия По Умолчанию При Создании Токенов Для Этого Клиента.	Поле С Выбором Значения
Добавить Выбранное	Кнопка Для Добавления Выбранных Клиентских Областей В Назначенные Клиентские Области По Умолчанию	Кнопка
Удалить Выбранное	Кнопка Для Удаления Выбранных Назначенных Клиентских Областей По Умолчанию	Кнопка

Наименование Настройки	Описание	Тип Настройки
Необязательные Клиентские Области	Необязательные Клиентские Области Действия Применяются При Выдаче Токенов Для Этого Клиента, На Случай, Когда Они Запрашиваются Параметром Области В Запросе Авторизации OIDC	
Доступные Клиентские Области	Области Действия Клиента, Которые Еще Не Назначены Как Области По Умолчанию Или Дополнительные Области	Поле С Выбором Значения
Назначенные Дополнительные Клиентские Области	Области Действия Клиента, Которые Могут Использоваться Как Дополнительные Области При Генерации Токенов Для Этого Клиента	Поле С Выбором Значения
Добавить Выбранное	Кнопка Для Добавления Выбранных Клиентских Областей	Кнопка
Удалить Выбранное	Кнопка Для Удаления Выбранных Клиентских Областей	Кнопка

Сопоставления шаблонов клиентов

Разрешить видеть все сопоставления протоколов и сопоставления областей ролей, которые будут использоваться в токенах, выданных этому клиенту. Также разрешить создание примера access-токена на основе предоставленного параметра области. На рисунке ниже изображен интерфейс представления и настройки сопоставления шаблонов клиентов.

The screenshot shows the 'Clients' section of the Keycloak interface. Under 'Clients', 'Test' is selected. In the top navigation bar, 'Client Templates' is highlighted. Below the tabs, there are sections for 'Parameter of action scope' (set to 'openid'), 'Available client areas' (listing 'address', 'micropublic-jwt', 'offline_access', 'phone'), 'Selected additional client areas' (empty), and 'Effective client areas' (listing 'acr', 'email', 'profile', 'roles', 'weborigins'). Buttons for 'Add selected' and 'Delete selected' are located between the 'Available' and 'Selected' areas. At the bottom, there are sections for 'User' and 'Score'.

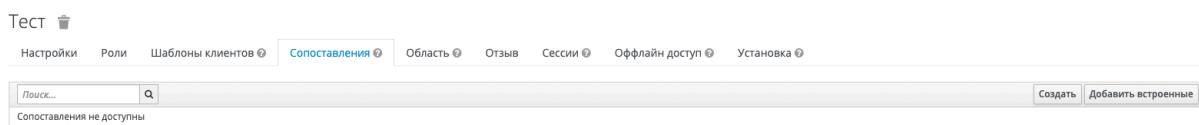
Наименование Настройки	Описание	Тип Настройки
Параметр области действия	Скопировать / Вставить это значение параметра scope и использовать его в начальном запросе аутентификации OpenID Connect, отправленном с этого клиентского адаптера. Области клиентов по умолчанию и выбранные дополнительные области клиентов будут использоваться при генерации токена, выпущенного для этого клиента.	Текстовое поле

Наименование Настройки	Описание	Тип Настройки
Области действия клиента	Разрешить выбор дополнительных клиентских областей, которые могут использоваться при генерации токена, выпущенного для этого клиента	
Доступные дополнительные клиентские области	Содержит необязательные клиентские области, которые можно дополнительно использовать при выдаче токена доступа для этого клиента	Поле с выбором значения
Выбранные дополнительные клиентские Области	Выбранные дополнительные клиентские области, которые будут использоваться при выдаче токена доступа для этого клиента. Можно увидеть выше, какое значение параметра области действия OAuth необходимо использовать, если необходим, чтобы эти дополнительные клиентские области применялись, когда исходный запрос аутентификации OpenID Connect будет отправлен с вашего клиентского адаптера.	Поле с выбором значения
Эффективные клиентские области	Содержит все клиентские области по умолчанию и выбранные дополнительные области. Все сопоставители протоколов и сопоставления областей ролей всех этих клиентских областей будут использоваться при создании токена доступа, выданного для вашего клиента.	Поле с выбором значения
Пользователь	При желании выберите пользователя, для которого будет создан пример токена доступа. Если не выбрать ни одного пользователя, то во время оценки пример токена доступа не будет сгенерирован.	Выпадающий список
Оценка	Нажав на эту кнопку, можно увидеть все сопоставления протоколов и ролей, которые будут использоваться при выдаче токена доступа для этого клиента. Также дополнительно будет сгенерирован пример токена доступа в случае, если был выбран какой-либо пользователь	Кнопка

Сопоставления

Протокол сопоставлений

Протокол сопоставлений, осуществляющих преобразование в токены и документы. Могут делать такие вещи как сопоставление пользовательских данных в заявки протокола, или просто преобразовать любой запрос, происходящий между клиентом и сервером аутентификации. На рисунке ниже изображен интерфейс представления сопоставлений протоколов для клиента.



Наименование Настройки	Тип Настройки
Поисковое Поле	Поле Для Поиска Сопоставлений
Создать	Кнопка Для Создания Сопоставлений
Добавить Встроенные	Кнопка Для Добавления Встроенных Сопоставлений

Создать сопоставление протокола

На рисунке ниже изображен интерфейс создания сопоставлений протоколов.

В таблице представлено детальное описание полей интерфейса создания сопоставлений протоколов.

Наименование Настройки	Описание	Тип Настройки
Протокол	Наименование Протокола	Текстовое Значение
Имя	Наименование Сопоставления.	Текстовое Значение
Тип Сопоставления	Выпадающий Список	

Описание полей вкладки Сопоставления в зависимости от типа сопоставления находится в разделе Детальное описание вкладки Сопоставления клиента.

Добавить встроенное сопоставление протокола

На рисунке ниже изображен интерфейс добавления встроенных сопоставлений протоколов.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Добавить встроенное сопоставление протокола

Поиск...	Категория	Тип	Добавить
zoneinfo	Token mapper	User Attribute	<input type="checkbox"/>
birthdate	Token mapper	User Attribute	<input type="checkbox"/>
family_name	Token mapper	User Property	<input type="checkbox"/>
gender	Token mapper	User Attribute	<input type="checkbox"/>
Impersonator Username	Token mapper	User Session Note	<input type="checkbox"/>
phone_number_verified	Token mapper	User Attribute	<input type="checkbox"/>
locale	Token mapper	User Attribute	<input type="checkbox"/>
gss_delegation_credential	Token mapper	User Session Note	<input type="checkbox"/>
allowed_web_origins	Token mapper	Allowed Web Origins	<input type="checkbox"/>
middle_name	Token mapper	User Attribute	<input type="checkbox"/>
nickname	Token mapper	User Attribute	<input type="checkbox"/>
updated_at	Token mapper	User Attribute	<input type="checkbox"/>
email_verified	Token mapper	User Property	<input type="checkbox"/>
email	Token mapper	User Property	<input type="checkbox"/>
client_roles	Token mapper	User Client Role	<input type="checkbox"/>
Impersonator User ID	Token mapper	User Session Note	<input type="checkbox"/>
website	Token mapper	User Attribute	<input type="checkbox"/>
address	Token mapper	User Address	<input type="checkbox"/>
given_name	Token mapper	User Property	<input type="checkbox"/>
profile	Token mapper	User Attribute	<input type="checkbox"/>
groups	Token mapper	User Realm Role	<input type="checkbox"/>
phone_number	Token mapper	User Attribute	<input type="checkbox"/>
full_name	Token mapper	User's full name	<input type="checkbox"/>
audience_resolve	Token mapper	Audience Resolve	<input type="checkbox"/>
picture	Token mapper	User Attribute	<input type="checkbox"/>
upn	Token mapper	User Property	<input type="checkbox"/>
realm_roles	Token mapper	User Realm Role	<input type="checkbox"/>
username	Token mapper	User Property	<input type="checkbox"/>

[Добавить выбранное](#)

Наименование Настройки	Тип Настройки
Поисковое Поле	Поисковое Поле
Имя	Имя Встроенного Сопоставления
Категория	Категория Встроенного Сопоставления
Тип	Тип Встроенного Сопоставления
Добавить	Добавить Встроенное Сопоставление
Добавить Выбранное	Добавление Выбранных Сопоставлений

Область

Сопоставление области позволяет вам ограничить сопоставленные роли пользователя, включаемые вместе с токеном доступа, запрошенного клиентом. На рисунке ниже изображено окно сопоставления областей для клиента.

Тест 

[Настройки](#) [Роли](#) [Шаблоны клиентов](#) [Сопоставления](#) [Область](#) [Отзыв](#) [Сессии](#) [Оффлайн доступ](#) [Установка](#)

Тест Сопоставление областей

Полный доступ к областям

[Вкл](#)

В таблице представлено детальное описание полей интерфейса сопоставления областей для клиента.

Наименование Настройки	Тип Настройки
Полный Доступ К Областям	Отключает Все Ограничения

Отзыв

На рисунке ниже изображено окно отзыва токенов.

Test 📁

Настройки Роли Шаблоны клиентов Сопоставления Область Отзыв Сессии Оффлайн доступ Установка

Не ранее чем None

Очистить Установить на сейчас Разослать

Наименование Настройки	Тип Настройки
Не Ранее Чем	Отозвать Любые Токены, Выданные До Указанной Даты Для Этого Клиента.
Очистить	Очищает Поле “Не Ранее Чем”
Установить На Сейчас	Устанавливает В Поле “Не Ранее Чем” Значение Текущей Даты И Времени
Разослать	Если URL Системы Администрации Сконфигурирован Для Этого Клиента, То Необходимо Послать Политики Этому Клиенту.

Сессии

Просмотр сессий для этого клиента. Позволяет увидеть, какие пользователи активны и когда они вошли. На рисунке ниже изображено окно просмотра активных сессий для клиента.

Test 📁

Настройки Роли Шаблоны клиентов Сопоставления Область Отзыв Сессии Оффлайн доступ Установка

Активные сессии 0

В таблице представлено детальное описание полей интерфейса просмотра активных сессий для клиента.

Наименование Настройки	Описание	Тип Настройки
Активные Сессии	Общее Количество Активных Сессий Пользователей Для Этого Клиента.	Поле, Недоступное К Ручному Заполнению

Оффлайн доступ

Просмотр оффлайн сессий для клиента. Позволяет увидеть, какие пользователи получали оффлайн токен и когда они его получили. Чтобы выбрать все токены для этого клиента, необходимо перейти на вкладку отзыва и установить значение в текущее время. На рисунке ниже изображено окно просмотра оффлайн сессий для клиента.

Тест

Наименование Настройки	Описание	Тип Настройки
Оффлайн Токены	Общее Количество Оффлайн Токенов Для Этого Клиента.	Поле, Недоступное К Ручному Заполнению

Установка

Вспомогательная утилита для генерации различных форматов конфигурации адаптера клиента, которые доступны к скачиванию или копированию для конфигурации клиентов. На рисунке ниже изображено окно генерации различных форматов конфигурации клиента.

Тест

```
<secure-deployment name="WAR MODULE NAME.war">
<realm>master</realm>
<auth-server-url>http://localhost:18080/auth/</auth-server-url>
<public-client>true</public-client>
<ssl-required>EXTERNAL</ssl-required>
<resource>Test</resource>
</secure-deployment>
```

В таблице представлено детальное описание интерфейса генерации различных форматов конфигурации адаптера клиента.

Наименование Настройки	Описание	Тип Настройки
Формат	Выбор Формата Конфигурации Адаптера Клиента.	Выпадающий Список
Скачать	По Нажатию Загружает Конфигурации Адаптера Клиента В Указанном Формате	Кнопка

Наименование Настройки	Описание	Тип Настройки
Поле	Конфигурации Адаптера Клиента	Текстовое Поле

Детальное описание вкладки Пользователи

Описание полей вкладки Пользователи

Детали

На рисунке ниже изображен интерфейс детального представления пользователя.

The screenshot shows the 'User Details' page for a user named 'test_1'. The page includes fields for ID, creation date, name, email, mobile phone, and other personal details. It also features sections for 'User Enabled' (status), 'Temporary Locked' (status), and 'Email Confirmation' (status). At the bottom, there are buttons for 'Select Action...', 'Language', and 'Impersonate'.

Наименование настройки	Описание	Тип настройки
E-mail	Почтовый адрес пользователя	Текстовое значение
Имя	Имя пользователя	Текстовое значение
Фамилия	Фамилия пользователя	Текстовое значение
Пользователь включен	Переключатель активности пользователя (выключенный пользователь считается заблокированным). Отключенные пользователи не смогут войти.	Булевая

Наименование настройки	Описание	Тип настройки
Подтверждение E-mail	Признак того, должен ли пользователь подтверждать свой E-mail	Булевая
Требуемые действия от пользователя	Требуемые действия от пользователя при входе: Настроить OTP (Configure OTP) - требует установить мобильное приложение генерации паролей. Обновить пароль (Update Password) - требует от пользователя ввести новый пароль. Обновить профиль (Update Profile) - требует от пользователя ввести новую персональную информацию. Подтвердить E-mail (Verify Email)- высылает письмо пользователю для подтверждения его E-mail. Обновить локаль пользователя (Update User Locale) - требует от пользователя обновить/выбрать локаль (язык). Webauthn Register Passwordless Verify Profile Webauthn Register	Выпадающий список с множественным выбором
Язык	Язык	Выпадающий список
Имперсонировать	Войти как этот пользователь. Если пользователь в том же самом realm что и вы, то ваша текущая сессия будет разлогинена перед тем как вы войдете как этот пользователь.	Кнопка

Атрибуты

Помимо основных метаданных пользователя, таких как имя и адрес электронной почты, можно хранить произвольные пользовательские атрибуты. Для этого необходимо выбрать пользователя для управления, затем перейти на вкладку Атрибуты.

Далее ввести имя и значение атрибута в пустые поля и нажать кнопку “Добавить” рядом с атрибутом, чтобы добавить новое поле. Стоит обратить внимание на то, что любые изменения, внесенные на странице атрибутов, не будут сохранены, пока не нажата кнопка Сохранить. На рисунке ниже изображено окно настройки и добавления пользовательских атрибутов.

Ключ	Значение	Действия
employeeNumber		Удалить
locale	ru	Удалить
orgCode		Удалить
startDate		Удалить
		Добавить

Сохранить Отмена

Учетные данные

При просмотре пользователя, если перейти на вкладку Учетные данные, то есть возможность управлять паролем. На рисунке ниже изображено окно настройки и управления учетными данными пользователя.

Pользователи > test_1

Test_1

Детали Атрибуты Учетные данные Сопоставление ролей Группы Согласия Сессии Дополнительно

Manage Credentials

Position	Тип	User Label	Data	Действия
<input type="button" value="▲"/>	password		Show data...	Удалить Сохранить

Сброс пароля

Пароль
Подтверждение пароля
Временный Сброс пароля

Наименование настройки	Описание	Тип настройки
Новый пароль	Ввести пароль пользователя	Текстовое значение
Подтверждение пароля	Повторить ввод пароля пользователя	Текстовое значение
Временный	Если включено, пользователю необходимо сменить пароль при следующем входе	Булевая

Сопоставление ролей

Для назначения сопоставления ролей пользователю требуется перейти на вкладку *Сопоставление ролей* для этого пользователя. На рисунке ниже изображено окно сопоставления ролей пользователя.

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Пользователи > test_1

Test_1

Детали Атрибуты Учетные данные Сопоставление ролей Группы Согласия Сессии Дополнительно

Роли Realm Доступные роли ⓘ Enter part of role name... AS_EDITOR offline_access test uma_authorization

Присвоенные роли ⓘ Enter part of role name... default-roles-test

Назначенные роли ⓘ default-roles-test offline_access uma_authorization

Добавить выбранное >

« Удалить выбранное

Роли интегрированных систем realm-management

Доступные роли ⓘ Enter part of role name... add-users allow-map-roles allow-sync-data clear-cache create-client delete-users impersonation manage-authorization manage-clients manage-data-sync manage-events manage-identity-providers manage-realm manage-realm-attributes manage-users

Присвоенные роли ⓘ Enter part of role name...

Назначенные роли ⓘ

Добавить выбранное >

« Удалить выбранное

Группы

Определенные конфигурированием атрибуты и сопоставления ролей наследуются группами и пользователями, которые являются членами группы. Для управления членством в группах, требуется перейти на вкладку *Группы*.

На рисунке ниже изображен интерфейс управления членством в группах.

Пользователи > test_1

Test_1

Детали Атрибуты Учетные данные Сопоставление ролей Группы Согласия Сессии Дополнительно

Членство в группах ⓘ Поиск... Показать все группы Покинуть

Доступные группы ⓘ Поиск... Показать все группы Присоединиться

Наименование настройки	Описание	Тип настройки
Членство в группах	Пользователь является членом группы. Выберите в списке группу и нажмите кнопку Покинуть, чтобы покинуть группу	-

Руководство по эксплуатации компонента Keycloak.SE (KCSE)

Наименование настройки	Описание	Тип настройки
Поиск	Поиск	Текстовое поле
Показать все группы	-	Кнопка
Покинуть	-	Кнопка
Доступные группы	Группы, к которым пользователь может присоединиться	-
Поиск	Поиск	Текстовое поле
Показать все группы	-	Кнопка
Покинуть	-	Кнопка

Согласия

На рисунке ниже изображено окно согласий пользователя.

The screenshot shows the 'Согласия' (Consents) tab selected in the user profile navigation bar. Below the tabs, there is a table with columns: Клиент (Client), Предоставленные клиентские области (Granted client areas), Дополнительные полномочия (Additional permissions), Создано (Created), Обновлено (Updated), and Действие (Action). There is one row in the table representing a consent named 'Test_1'.

Сессии

На рисунке ниже изображено окно активных сессий пользователя.

The screenshot shows the 'Сессии' (Sessions) tab selected in the user profile navigation bar. Below the tabs, there is a table with columns: IP адрес (IP address), Начало (Start), Последний доступ (Last access), Клиенты (Clients), and Действие (Action). A button 'Выйти из всех сессий' (Logout from all sessions) is located at the top right of the table area.

Дополнительно

На вкладке Дополнительно задаются кадровые атрибуты пользователя.

На рисунке ниже изображено окно дополнительных кадровых атрибутов пользователя.

Test_1 

Детали Атрибуты Учетные данные Сопоставление ролей Группы Согласия Сессии Дополнительно

Кадровые атрибуты

Внешний GUID * 	<input type="text"/>
Имя 	<input type="text"/>
Отчество 	<input type="text"/>
Логин в Sigma 	<input type="text"/>
Код организации * 	<input type="text"/>
Код подразделения * 	<input type="text"/>
Имя подразделения * 	<input type="text"/>
Должность 	<input type="text"/>
Табельный номер * 	<input type="text"/>
Структурные подразделения 	<input type="text"/>
Тип пользователя 	<input type="button" value="Пользователь"/>
Коды ФОС 	<input type="text"/>
Время последней аутентификации 	<input type="text"/>
Администратор последних изменений УЗ 	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Кадровые атрибуты

Атрибуты, необходимые для использования методов ОСА/СПАС (по SOAP).

Наименование настройки	Описание	Тип настройки
Внешний GUID	Внешний GUID	Текстовое поле
Имя	Имя пользователя	Текстовое поле
Отчество	Отчество пользователя	Текстовое поле
Логин в Sigma	Логин в Sigma пользователя	Текстовое поле
Логин в Sigma	Логин в Sigma пользователя	Текстовое поле
Код организации	Код организации	Текстовое поле
Код подразделения	Код подразделения	Текстовое поле
Имя подразделения	Имя подразделения	Текстовое поле
Должность	Должность пользователя	Текстовое поле

Наименование настройки	Описание	Тип настройки
Табельный номер	Табельный номер в КИ	Текстовое поле
Структурные подразделения	Идентификаторы структурных подразделений, к которым привязан пользователь (можно несколько, через запятую без пробелов)	Текстовое поле
Тип пользователя	Тип пользователя	Выпадающий список
Коды ФОС	Идентификаторы узлов ФОС, к которым привязан пользователь (можно несколько, через запятую без пробелов)	Текстовое поле
Время последней аутентификации	Время последней успешной аутентификации пользователя	Текстовое поле нередактируемое
Администратор последних изменений УЗ	Логин Администратора который последний вносил изменения в учетную запись	Текстовое поле нередактируемое
Сохранить	-	Кнопка
Отмена	-	Кнопка

Детальное описание вкладки Роли клиента

Для того чтобы создать Роль клиента, необходимо:

- Перейти на вкладку Клиенты;
- Выбрать клиента;
- Перейти на вкладку Роли и нажать кнопку создания.

Добавление роли

Добавить роль

Наименование роли *	<input type="text"/>
Описание	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Наименование настройки	Описание	Тип настройки
Наименование роли	Поле для ввода наименования роли клиента	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение

Редактирование роли

Детали роли

Тестовая Роль

[Детали](#)[Атрибуты](#)[Пользователи с ролью](#)

Наименование роли

Тестовая роль

Описание

Составные роли

Вкл

[Сохранить](#) [Отмена](#)

Составные роли

Роли Realm

Доступные роли

Enter part of role name...

Test
Test1
admin
create-realm
default-roles-master
offline_access
ttt
uma_authorization

[Добавить выбранное »](#)

Ассоциированные роли

Enter part of role name...

[« Удалить выбранное](#)

Наименование настройки	Описание	Тип настройки
Наименование роли	Отображение наименования роли	Текстовое значение
Описание	Поле для ввода описания роли клиента	Текстовое значение
Составные роли	Когда эта роль (не)ассоциирована с любой ролью пользователей, она (не)будет неявно ассоциирована.	Кнопка
Роли Realm	Доступные роли	Поле с выбором значения
Ассоциированные роли	Роли уровня Realm, ассоциированные с составными ролями.	Поле с выбором значения
Добавить выбранное	Кнопка для добавления выбранных ролей в ассоциированные роли	Кнопка

Наименование настройки	Описание	Тип настройки
Удалить выбранное	Кнопка для удаления ролей из ассоциированных ролей	Кнопка

Атрибуты роли

Тестовая Роль

Детали Атрибуты Пользователи с ролью

Ключ	Значение	Действия
		Добавить

Сохранить Отмена

Наименование настройки	Описание	Тип настройки
Ключ	Поле для ввода ключа, определяющего атрибут настройки	Текстовое поле
Значение	Поле для ввода значения, задающегося атрибуту настройки	Текстовое поле
Действие	Добавить	Кнопка добавления связки ключ-значения

Пользователи с ролью

Тестовая Роль

Детали Атрибуты Пользователи с ролью

No role members

Наименование настройки	Описание	Тип настройки
Пользователи с ролью	Перечисление пользователей с данной ролью	Текстовое поле

Детальное описание вкладки Сопоставления клиента

Для того чтобы создать Сопоставление клиента, необходимо:

1. Перейти на вкладку Клиенты.
2. Выбрать клиента.
3. Перейти на вкладку Сопоставления и нажать кнопку создания.

Поля заполняются в зависимости от выбора типа сопоставления.

Тип сопоставления Claims parameter Token

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Добавить в токен ID

Добавить в информацию о пользователе

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Claims parameter Token	Утверждения, указанные параметром Claims, помещаются в токены.	
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления User Realm Role

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол ? openid-connect

Имя ?

Тип сопоставления ? User Realm Role

Префикс ролей Realm ?

Несколько значений ? ВКЛ

Имя переменной в токене ?

Тип переменной JSON ? Выбрать...

Добавить в токен ID ? ВКЛ

Добавить в токен доступа ? ВКЛ

Добавить в информацию о пользователе ? ВКЛ

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
User Realm Role	Сопоставление роли realm пользователя с утверждением токена.	
Префикс ролей Realm	Префикс для каждой роли Realm (опционально).	Текстовое значение
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение

Наименование настройки	Описание	Тип настройки
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления User Session Note

На рисунке ниже изображено окно создания сопоставления протокола.

The screenshot shows the 'Create protocol mapping' dialog box. At the top, it says 'Создать сопоставление протокола'. Below that, there are several input fields and dropdown menus:

- 'Протокол' (Protocol) dropdown: openid-connect
- 'Имя' (Name) input field: empty
- 'Тип сопоставления' (Mapping Type) dropdown: User Session Note
- 'Заметка сессии пользователя' (User Session Note) input field: empty
- 'Имя переменной в токене' (Token Variable Name) input field: empty
- 'Тип переменной JSON' (JSON Variable Type) dropdown: Выбрать... (Select)
- 'Добавить в токен ID' (Add to token ID) button: ВКЛ (Enabled)
- 'Добавить в токен доступа' (Add to access token response) button: ВКЛ (Enabled)
- 'Add to access token response' (Add to access token response) button: ВЫКЛ (Disabled)

At the bottom right are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

Наименование настройки	Описание	Тип настройки
User Session Note	Сопоставление пользовательской сессии с утверждением токена.	
Заметка сессии пользователя	Наименование процедуры заметки сессии пользователя согласованным с UserSessionModel.note.	Текстовое поле
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое поле
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая

Наименование настройки	Описание	Тип настройки
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Add to access token response	Включить в access token всплывающую подсказку	Булевая

Тип сопоставления Users Address

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Имя пользователя атрибута, обозначающего Улицу

Имя пользователя атрибута, обозначающего Местонахождение

Имя пользователя атрибута, обозначающего Регион

Имя пользователя атрибута, обозначающего Почтовый индекс

Имя пользователя атрибута, обозначающего Страна

Имя пользователя атрибута, обозначающего Форматированный адрес

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Users Address	Сопоставляет атрибуты адреса пользователя (улица, населенный пункт, регион, почтовый индекс и страна) с утверждением OpenID Connect “адрес”.	
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Наименование настройки	Описание	Тип настройки
Имя пользовательского атрибута, обозначающего Улицу	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'street_address' внутри атрибута 'address' токена. По умолчанию 'street' .	Текстовое значение
Имя пользовательского атрибута, обозначающего Местонахождение	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'locality' внутри атрибута 'address' токена. По умолчанию 'locality' .	Текстовое значение
Имя пользовательского атрибута, обозначающего Регион	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'region' внутри атрибута 'address' токена. По умолчанию 'region' .	Текстовое значение
Имя пользовательского атрибута, обозначающего Почтовый индекс	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'postal_code' внутри атрибута 'address' токена. По умолчанию 'postal_code' .	Текстовое значение
Имя пользовательского атрибута, обозначающего Страну	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'country' внутри атрибута 'address' токена. По умолчанию 'country' .	Текстовое значение
Имя пользовательского атрибута, обозначающего Форматированный адрес	Имя пользовательского атрибута, которое будет использоваться для сопоставления атрибута 'formatted' внутри атрибута 'address' токена. По умолчанию 'formatted' .	Текстовое значение

Тип сопоставления Role Name Mapper

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Protocol: openid-connect
 Имя:
 Тип сопоставления: Role Name Mapper
 Role: Выберите роль
 New Role Name:
 Сохранить Отмена

Наименование настройки	Описание	Тип настройки
Role Name Mapper	Сопоставьте назначенную роль с новым именем или позицией в токене.	

Наименование настройки	Описание	Тип настройки
Роль	Имя роли, которое необходимо изменить. Нажмите кнопку “Выбрать роль”, чтобы просмотреть роли, или просто введите ее в текстовое поле. Для ссылки на роль клиента используется синтаксис client name.роль клиента, т.е. myclient.myrole	Текстовое значение
Новое имя роли	Новое имя роли. Новый формат имени соответствует тому, к какому токену доступа будет привязана роль. Таким образом, новое имя ‘myapp.new name’ сопоставит роль с этой позицией в маркере доступа. Новое имя “новое имя” сопоставит роль с ролями области в токене.	Текстовое значение
Выберите роль	Кнопка	

Тип сопоставления User Client Role

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

ID клиента

Предфикс ролей клиента

Несколько значений

Имя переменной в токене

Тип переменной JSON

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Наименование настройки	Описание	Тип настройки
User Client Role	Сопоставьте клиентскую роль пользователя с утверждением токена.	
ID клиента	ID клиента для сопоставления ролей	Выпадающий список с поиском
Предфикс ролей клиента	Предфикс для каждой роли клиента (опционально).	Текстовое значение
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая

Наименование настройки	Описание	Тип настройки
Имя переменной в токене	Название утверждения для вставки в токен. Это может быть полное имя, например 'address.street'. В этом случае будет создан вложенный объект json. Чтобы предотвратить вложенность и использовать точку буквально, экранируйте точку обратной косой чертой (.). Можно использовать специальный токен \${client_id}, который будет заменен фактическим идентификатором клиента. Примером использования является 'resource_access.\${client_id}.roles'. Это особенно полезно, когда требуется добавить роли от всех клиентов (следовательно, переключатель 'ClientID' не установлен), и чтобы роли клиентов каждого клиента хранились отдельно.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления User Property

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол openid-connect

Имя

Тип сопоставления User Property

Свойство

Имя переменной в токене

Тип переменной JSON Выбрать...

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Наименование настройки	Описание	Тип настройки
User Property	Сопоставьте встроенное свойство пользователя (адрес электронной почты, имя, фамилия) с утверждением токена	
Свойство	Имя свойства метода в интерфейсе UserModel. Для примера, значение 'email' будет ссылкой на метод UserModel.getEmail().	Текстовое значение
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления Hardcoded Role

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления ▼

Role Выберите роль

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Hardcoded Role	Жестко закодировать роль в токене доступа (access token).	
Роль	Роль, которую необходимо добавить к токену. Нажмите кнопку "Выберите роль", чтобы просмотреть роли, или просто введите ее в текстовое поле. Для ссылки на роль клиента используется синтаксис: имя клиента.роль клиента, т.е.. myclient.myrole	Текстовое значение
Выберите роль	Кнопка	

Тип сопоставления Hardcoded Claim

На рисунке ниже изображено окно создания сопоставления протокола.

Наименование настройки	Описание	Тип настройки
Hardcoded claim	Жестко закодируйте утверждение в токене.	
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Claim value	Значение утверждения, которое необходимо жестко закодировать. 'true' и 'false' могут использоваться для логических значений.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, и String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая
Add to access token response	Включить в access token всплывающую подсказку	Булевая

Тип сопоставления Pairwise subject identifier

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол	<input type="text" value="openid-connect"/>
Имя	<input type="text"/>
Тип сопоставления	<input type="text" value="Pairwise subject identifier"/>
Сектор идентификации URI	<input type="text"/>
Соль	<input type="text"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Наименование настройки	Описание	Тип настройки
Pairwise subject identifier	Вычисляет попарный идентификатор субъекта, используя соленый хэш sha-256. Дополнительную информацию о попарном подключении см. в спецификации OpenID Connect.	
Сектор идентификации URI	Провайдеры, использующие пары вспомогательных значений и поддерживающие динамическую регистрацию клиентов ДОЛЖНЫ использовать sector_identified_uri параметр. Это обеспечивает способ для группы сайтов под общим административным контролем, чтобы иметь последовательные попарные значения независимо от индивидуальных доменных имен. Это также обеспечивает способ для клиентов для изменения redirect_uri доменов, не имеющих возможности перерегистрации всех своих пользователей.	Текстовое значение
Соль	Соль, используемая для вычисления парного субъекта идентификатора. Если поле не заполнено, то соль будет сгенерирована.	Текстовое значение

Тип сопоставления User's full name

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол	<input type="text" value="openid-connect"/>
Имя	<input type="text"/>
Тип сопоставления	<input type="text" value="User's full name"/>
Добавить в токен ID	<input checked="" type="checkbox"/>
Добавить в токен доступа	<input checked="" type="checkbox"/>
Добавить в информацию о пользователе	<input checked="" type="checkbox"/>
<input type="button" value="Сохранить"/> <input type="button" value="Отмена"/>	

Наименование настройки	Описание	Тип настройки
User's full name	Сопоставляет имя и фамилию пользователя с утверждением OpenID Connect “имя”. Формат ‘первый’ + ‘ ’ + ‘последний’>	
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления Allowed Web Origins

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол ⓘ openid-connect

Имя ⓘ

Тип сопоставления ⓘ Allowed Web Origins

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Allowed Web Origins	Добавляет все разрешенные веб-источники к утверждению “разрешенные источники” в токене	

Тип сопоставления Audience

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол ⓘ openid-connect

Имя ⓘ

Тип сопоставления ⓘ Audience

Включить аудиенцию клиентов ⓘ Выбрать.....

Включить аудиенцию пользователей ⓘ

Добавить в токен ID ⓘ ВЫК

Добавить в токен доступа ⓘ ВКЛ

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Audience	Добавьте указанную аудиторию в поле аудитория (aud) токена	
Включить аудиенцию клиентов	Идентификатор клиента указанной аудитории будет включен в поле audience (aud) токена. Если в токене есть существующие аудиенции, указанное значение будет просто добавлено к ним. Оно не отменяет существующие аудиенции.	Выпадающий список
Включить аудиенцию пользователей	Используется только в том случае, если 'Included Client Audience' не заполнено. Указанное значение будет включено в поле audience (aud) токена. Если в токене есть существующие аудиенции, указанное значение будет просто добавлено к ним. Оно не отменяет существующие аудиенции.	Текстовое значение
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая

Тип сопоставления User Attribute

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Атрибут пользователя

Имя переменной в токене

Тип переменной JSON

Добавить в токен ID

Добавить в токен доступа

Добавить в информацию о пользователе

Несколько значений

Агрегированные значения атрибутов

Наименование настройки	Описание	Тип настройки
User Attribute	Сопоставьте пользовательский атрибут пользователя с утверждением токена.	

Наименование настройки	Описание	Тип настройки
Атрибут пользователя	Имя сохраненного атрибута пользователя, которое является именем атрибута, согласованным с UserModel.attribute.	Текстовое значение
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например 'address.street'. В таком случае будет создан вложенный json объект.	Текстовое значение
Тип переменной JSON	Тип переменной в JSON, который должен использоваться при добавлении ее в токен. Допустимые значения long, int, boolean, или String.	Выпадающий список
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая
Несколько значений	Отображается, если атрибут поддерживает несколько значений. Если включен, то список всех значений будет претендовать на этот атрибут. В противном случае выбираться будет только первое значение	Булевая
Агрегированные значения атрибутов	Указывает, следует ли агрегировать значения атрибутов с атрибутами группы. При использовании протокола OpenID Connect необходимо включить многозначную опцию, чтобы получить все значения. Дублированные значения отбрасываются, и с помощью этой опции порядок значений не гарантируется.	Булевая

Тип сопоставления Group Membership

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол: openid-connect

Имя:

Тип сопоставления: Group Membership

Имя переменной в токене:

Full group path:

Добавить в токен ID:

Добавить в токен доступа:

Добавить в информацию о пользователе:

Сохранить **Отмена**

Наименование настройки	Описание	Тип настройки
Group Membership	Сопоставление групп пользователя с членством в группах	
Имя переменной в токене	Имя переменной при добавлении ее в токен. Может быть полное имя, например ‘address.street’. В таком случае будет создан вложенный json объект.	Текстовое значение
Full group path	Укажите полный путь к группе, т.е. /top/level 1/level2, false просто укажет имя группы	Булевая
Добавить в токен ID	Должно ли значение быть добавлено в токен ID?	Булевая
Добавить в токен доступа	Должно ли значение быть добавлено в токен доступа?	Булевая
Добавить в информацию о пользователе	Должно ли требование быть добавлено в информацию о пользователе?	Булевая

Тип сопоставления Audience Resolve

На рисунке ниже изображено окно создания сопоставления протокола.

Создать сопоставление протокола

Протокол

Имя

Тип сопоставления

Наименование настройки	Описание	Тип настройки
Audience Resolve	Добавляет все идентификаторы клиентов “разрешенных” клиентов в поле аудитории токена. Разрешенный клиент означает клиент, для которого пользователь имеет хотя бы одну роль клиента	

Руководство прикладного разработчика компонента KeyCloak.SE (KCSE)

Системные требования

Системные требования описаны в Руководстве по установке.

Подключение и конфигурирование

Описано в руководстве по установке KeyCloak.SE Руководство по установке.

Миграция на текущую версию

Миграция на актуальную версию осуществляется путем получения актуального дистрибутива у поставщика. Автоматическая миграция на текущую версию в данный момент не поддерживается. В случае изменения схемы базы данных миграция осуществляется автоматически при запуске дистрибутива. Для настройки отправки событий в Platform V Audit с использованием REST API необходимо изменить слушателя событий с `send-events-to-audit` на `send-events-to-audit-by-rest` в настройке конфигурации событий в Административной консоли (Панель Управление/События/Конфигурация).

Быстрый старт

Предусловие для запуска проекта

Для того чтобы использовать KeyCloak.SE, необходимо выполнить несколько простых манипуляций:

1. Необходимо запустить продукт с помощью выбранного метода (локальный старт / установка в среде контейнеризации);
2. Перейти к консоли администратора по порту, который конфигурируется в deployment конфигурации (более подробно описано в Руководстве по установке);
3. Далее необходимо выполнить параллельные манипуляции для пользователя и приложения, осуществляющего доступ к информации о пользователе:
 1. Для приложения:
 1. Необходимо реализовать backend на основе REST - контроллеров для аутентификации и получения информации о пользователе на основе API, описанных в KeyCloak.SE. Документация REST API.
 2. Необходимо создать клиента в KeyCloak.SE с определенным набором ролей и scope, позволяющих получать доступ о будущих пользователях (описано в Руководстве оператора.)
 2. Для пользователя:
 1. Необходимо создать учетную запись пользователя (описано в Руководстве оператора.)
4. Далее пользователь, используя учетную запись, пытается произвести аутентификацию в продукт с помощью KeyCloak.SE, дает согласие на получение

продуктом информации из KeyCloak.SE и входит в систему - поток описан в Детальной архитектуре.

Запуск проекта для разработчика. Запуск в режиме Standalone

В этом руководстве объясняются методы настройки KeyCloak.SE, а также способы запуска и применения предпочтительной конфигурации.

KeyCloak.SE загружает конфигурацию из четырех различных источников конфигурации:

1. параметры командной строки
2. переменные среды
3. созданный пользователем файл .conf
4. файл keycloak.conf, расположенный в каталоге conf.

Источники конфигурации имеют приоритет по убыванию: параметры командной строки имеют приоритет над переменными среды. Переменные среды имеют приоритет над параметрами, заданными с помощью определенного файла конфигурации. Параметры из определенного конфигурационного файла имеют приоритет над параметрами, определенными в conf/keycloak.conf. Когда один и тот же ключ конфигурации найден в нескольких источниках конфигурации, применяемое значение берется из источника конфигурации с наивысшим порядком приоритета.

Необходимо развернуть скомпилированные модули в директорию /providers:

Обязательные модули:

- kcse-common-security.jar;
- kcse-commons-lib.jar;
- kcse-commons-runnable.jar;
- kcse-core.jar;
- kcse-keycloak-attribute-manager.jar;
- kcse-keycloak-rest-module.jar;
- com.google.code.gson:gson:2.8.6;
- org.json:json:20210307;
- org.apache.commons:commons-text:1.8;
- org.glassfish:jakarta.json:1.1.6.

Остальные модули также должны быть размещены в этой папке.

При первом запуске необходимо добавить хотя бы одного пользователя при помощи скрипта add-user-keycloak.sh (add-user-keycloak.bat) в папке bin.

Порт сервиса для доступа к UI настраивается в конфигурационных файлах kc.sh.

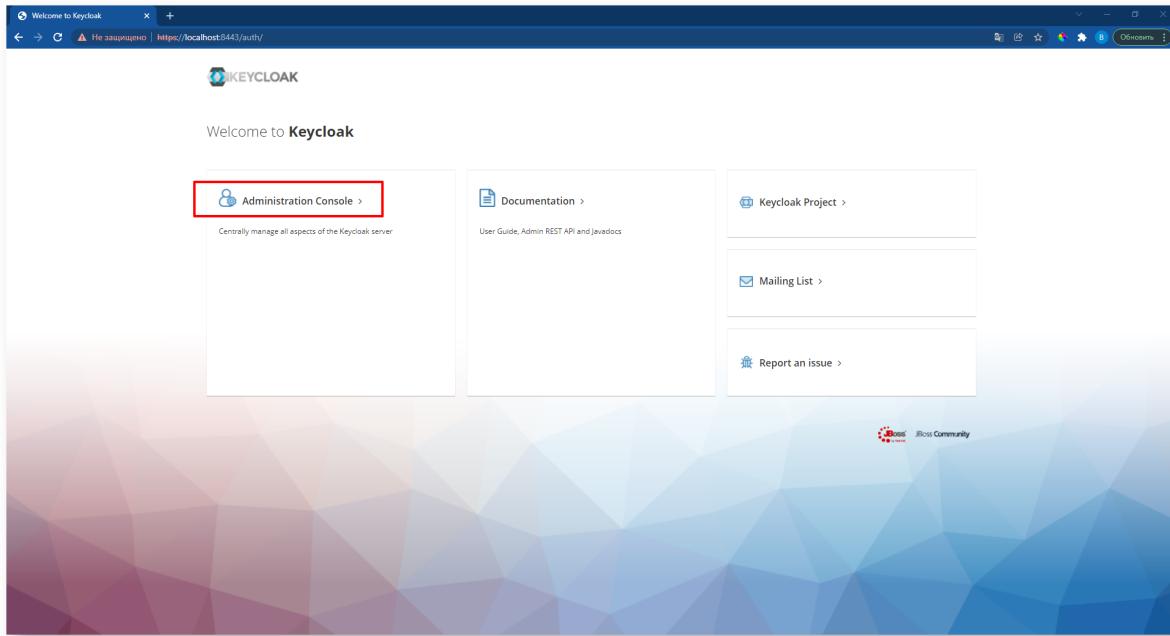
Запуска сервиса осуществляется стартовым скриптом bin/kc.sh (kc.bat)

Пример запуска: bin/kc.[sh|bat] start

В случае успешного старта в консоли будет сообщение следующего содержания:

```
16:18:12,106 INFO [io.quarkus] (main) Keycloak 18.0.2 on JVM (powered by Quarkus 2.7.5.Final)  
started in 7.871s. Listening on: http://0.0.0.0:8080 and https://0.0.0.0:8443
```

Теперь в браузере можно перейти к UI сервиса по ссылке http://localhost:8443 (порт ранее настраивается в конфигах kc.sh)



Запуск проекта для разработчика. Запуск в Docker

Для запуска приложения в docker необходимо написать Dockerfile, пример которого с комментариями ниже:

```
FROM host/path/to/keycloak:20.0.1          # то, откуда берется образ KeyCloak.SE  
  
COPY --chown=1000:jboss conf/ /opt/keycloak/conf      # добавляет файл  
конфигурации  
COPY --chown=1000:jboss dependencies/common-dependencies/ /opt/keycloak/providers #  
копирует зависимости  
  
COPY --chown=1000:jboss dependencies/modules/ /opt/keycloak/providers      # добавляем  
внешние(кастомные) модули приложения
```

...

EXPOSE 7600

указание порта и запуск

Разработка backend

Разработка/доработка KeyCloak.SE помимо основных действий (например: Добавление расширение Admin REST API) требует ряда обязательных действий:

- Подключение к разработанной/доработанной функциональности событий (events);
- Написание документации - JavaDoc;
- Проведение тестирования разработчиками на этапе кодирования приложения - UnitTesting;
- Проведение разработки с использованием SonarQube.

JS Аутентификаторы

JS Scripts в KeyCloak.SE позволяются осуществлять доработку продукта с целью создания аутентификаторов без пересборки исходного дистрибутива.

Включение проверки СНИЛС из клиентского сертификата при аутентификации через ЕСИА

Для того чтобы использовать функциональность JS скриптов для аутентификации в первую очередь необходимо включить их поддержку (базово она отключена).

Для этого необходимо перейти по \keycloak\standalone\configuration\profile.properties и в этом файле добавить следующий блок кода (если файл отсутствует - его необходимо создать):

profile.properties

```
## Enable JavaScript
feature.scripts=enabled
## Enable editing JavaScript based Components via Admin-Console
feature.upload_scripts=enabled
```

Далее необходимо разработать необходимый JS скрипт аутентификатора. В рамках указанной задачи прикладываем готовый скрипт:

Проверка СНИЛС из клиентского сертификата при аутентификации через ЕСИА

```
AuthenticationFlowError = Java.type("org.keycloak.authentication.AuthenticationFlowError");
```

```
HEADER_PARAM = "X-Test"; // параметр HTTP хедера, где передаются данные о кл. сертификате. Заменить на свое значение!!
```

```
EMAIL_KEY_PARAM = "S.E=";
SNILS_KEY_PARAM = "S.SNILS=";
DELIMETER = "; ";
// параметр разделителя данных кл. сертификата. Заменить на свое значение!!
KEY_VALUE_DELIMETER = '=';

function authenticate(context) {
    var clientCertData = httpRequest.getHttpHeaders().getHeaderString(H HEADER_PARAM) || "";
    LOG.debug(script.name + " trace auth: http header value = " + clientCertData);
    var certParams = clientCertData.split(DELIMETER);

    if (certParams) {
        var foundUser = getUserBySnils(certParams); // аутентификация по СНИЛС из клиентского сертификата.
        //var foundUser = getUserByEmail(certParams); // аутентификация по email из клиентского сертификата.

        if (foundUser) {
            LOG.debug(script.name + " trace auth: found user id = " + foundUser.id);

            var username = foundUser ? foundUser.username : "anonymous";
            LOG.debug(script.name + " trace auth: username of found user: " + username);

            context.success();
            LOG.info(script.name + ": SNILS authentication from client certificate is PASSED");
            return;
        }
    }

    context.failure(AuthenticationFlowError.INVALID_USER);
}

function getUserBySnils(clientCertData) {
    var snils = clientCertData.filter(function(x) {
        return x.startsWith(SNILS_KEY_PARAM);
    }).toString().split(KEY_VALUE_DELIMETER)[1];
    LOG.debug(script.name + " trace auth: extracted snils from client certificate = " + snils);

    var foundedUsers = session.users().searchForUserByUserAttribute("snils", snils, realm);
}
```

```
var count = foundedUsers ? foundedUsers.length : 0;

if (count > 0) {
    return foundedUsers[0]; // возвращаем первого пользователя из списка найденных
пользователей с указанным СНИЛС.
}

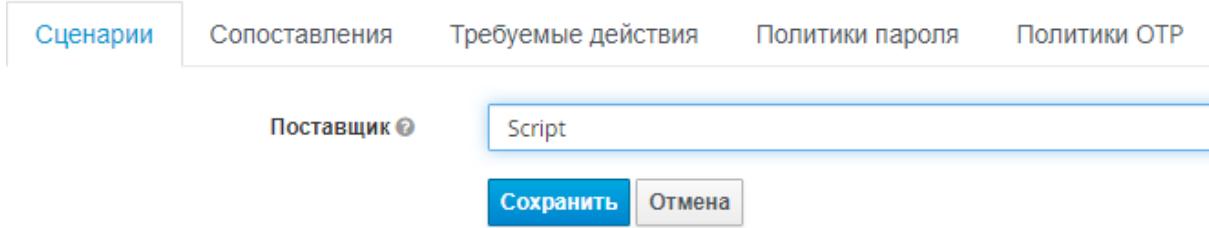
return undefined;
}

function getUserByEmail(clientCertData) {
    var email = clientCertData.filter(function(x) {
        return x.startsWith(EMAIL_KEY_PARAM);
    }).toString().split(KEY_VALUE_DELIMETER)[1];
    LOG.debug(script.name + " trace auth: extracted email from client certificate = " + email);

    return session.users().getUserByEmail(email, realm);
}
```

Далее рассмотрим процесс настройки указанной функциональности. Для этого необходимо открыть Admin Console и отредактировать flow постлогина через ЕСИА, после чего добавить JS аутентификатор (нажать “добавить исполнение”, выбрать поставщик “Script”)

Создать исполнение аутентификатора



Затем необходимо заполнить обязательные поля и вставить скрипт аутентификатора.
Сохранить.

ID	9d4416d8-8bfe-4907-9592-6da0c13d1fb
Синоним	http-auth
Script Name	Аутентификация по HTTP заголовкам
Script Description	
Script Source	<pre> 1 AuthenticationFlowError = Java.type("org.keycloak.authentication.AuthenticationFlowError"); 2 3 HEADER_PARAM = "X-Test"; 4 EMAIL_KEY_PARAM = "S.E="; 5 SNILS_KEY_PARAM = "S.SNILS="; 6 DELIMETER = "; "; 7 KEY_VALUE_DELIMETER = '='; </pre>

Выставить первый порядок у JS аутентификатора, требование в REQUIRED.

Аутентификация

Сценарии	Сопоставления	Требуемые действия	Политики пароля	Политики OTP
Esia Post Login				
Тип аутентификации				Требования
<input type="checkbox"/> Script (http-auth)				<input checked="" type="radio"/> REQUIRED
<input type="checkbox"/> Get ESIA User Info (getUserInfo)				<input checked="" type="radio"/> REQUIRED
<input type="checkbox"/> ESIA Organization List (getOrgList)				<input checked="" type="radio"/> REQUIRED
<input type="checkbox"/> ESIA Organization Choice (orgChoice)				<input checked="" type="radio"/> REQUIRED
<input type="checkbox"/> Get ESIA User Roles (getUserRoles)				<input checked="" type="radio"/> REQUIRED

После этой настройки при каждой аутентификации через ЕСИА будет дополнительно сверяться СНИЛС из клиентского сертификата, переданного в HTTP заголовке с данными из УЗ Keycloak.SE.

Добавление/расширение Admin Rest API

Написание нового модуля

Для доработки или добавления функциональности в Keycloak.SE существуют SPI (Service Provider Interfaces). Он состоит из интерфейсов ProviderFactory и Provider, а так же конфигурационного файла.

При реализации функциональности следует использовать существующие SPI (например, RealmResourceSPI) или реализовывать SPI самостоятельно. Чтобы создать собственный SPI, необходимо наследоваться от Spi класса.

RealmResourceSPI.java

```
public class RealmResourceSPI implements Spi {
```

```
@Override
```

```
public boolean isInternal() {
    return true;
}

@Override
public String getName() {
    return "realm-restapi-extension";
}

@Override
public Class<? extends Provider> getProviderClass() {
    return RealmResourceProvider.class;
}

@Override
public Class<? extends ProviderFactory> getProviderFactoryClass() {
    return RealmResourceProviderFactory.class;
}
```

Затем его следует прописать в конфигурационном файле с полным наименованием родительского класса (полный путь с пакетом), а в файл org.keycloak.provider.SPI записать полный путь с пакетом самого класса org.keycloak.services.resource.RealmResourceSPI. Также следует прописать ProviderFactory.

resources/META-INF/services/org.keycloak.services.resource.RealmResourceProviderFactory
org.keycloak.examples.rest.HelloResourceProviderFactory

Provider будет инициализироваться из фабрики.

HelloResourceProviderFactory.java

```
public class HelloResourceProviderFactory implements RealmResourceProviderFactory {

    public static final String ID = "hello";

    @Override
    public String getId() {
        return ID;
    }

    @Override
    public RealmResourceProvider create(KeycloakSession session) {
        return new HelloResourceProvider(session);
    }
}
```

```
}

@Override
public void init(Scope config) {
}

@Override
public void postInit(KeycloakSessionFactory factory) {
}

@Override
public void close() {
}

}
```

В Provider реализуется необходимая функциональность REST API.

HelloResourceProvider.java

```
public class HelloResourceProvider implements RealmResourceProvider {

    private KeycloakSession session;

    public HelloResourceProvider(KeycloakSession session) {
        this.session = session;
    }

    @Override
    public Object getResource() {
        return this;
    }

    @GET
    @Produces("text/plain; charset=utf-8")
    public String get() {
        String name = session.getContext().getRealm().getDisplayName();
        if (name == null) {
            name = session.getContext().getRealm().getName();
        }
        return "Hello " + name;
    }

    @Override
```

```
public void close() {  
}  
}
```

Подключение модуля

После написания и компиляции модуля его необходимо подключить к Keycloak.SE:

1. Скопировать через Modules

```
COPY --chown=1000:jboss dependencies/modules/ /opt/keycloak/providers
```

2. Установить переменные окружения.
3. Запустить kc.sh.

События (events)

Для создания собственного обработчика событий необходимо:

1. Создать кастомный CustomEventListenerProvider, который будет имплементировать org.keycloak.events.EventListenerProvider EventListenerProvider.java

```
public class CustomEventListenerProvider implements EventListenerProvider {  
  
    @Override  
    public void onEvent(Event event) {  
        log.info("Example caught event", EventUtils.toString(event));  
    }  
  
    @Override  
    public void onEvent(AdminEvent adminEvent, boolean b) {  
        log.info("Example caught admin event {}", EventUtils.toString(adminEvent));  
    }  
  
    @Override  
    public void close() {  
    }  
}
```

2. У данного интерфейса необходимо определить три метода:

1. *onEvent* метод, перехватывающий обычные события в системе, такие как событие неправильного ввода пароля;

2. *onAdminEvent* перехватывает события администратора, например: событие сброса пароля пользователя через консоль администратора Keycloak;
3. *close* своего рода деструктор, вызывается при удалении текущего провайдера.
3. Создать собственную фабрику CustomEventListenerProviderFactory, которая имплементирует org.keycloak.events.EventListenerProviderFactory

CustomEventListenerProviderFactory.java

```
public class CustomEventListenerProviderFactory implements EventListenerProviderFactory {

    private static final String LISTENER_ID = "event-listener-extension";

    @Override
    public EventListenerProvider create(KeycloakSession session) {
        return new CustomEventListenerProvider();
    }

    @Override
    public void init(Config.Scope scope) {

    }

    @Override
    public void postInit(KeycloakSessionFactory keycloakSessionFactory) {

    }

    @Override
    public void close() {

    }

    @Override
    public String getId() {
        return LISTENER_ID;
    }

}
```

Здесь необходимо переопределить пять методов:

- *create* будет возвращать наш кастомный провайдер CustomEventListenerProvider. Вызывается при каждом новом событии в системе.
- *init* срабатывает только один раз при первом создании фабрики.

- *postInit* вызывается один раз после инициализации всех фабрик провайдеров в системе.
- *close* выполняется при завершении работы Keycloak.
- *getId* устанавливает название нашего расширения при создании фабрики.

Здесь описано только минимальное расширение для отлавливания событий в Keycloak, вы же можете делать с ними все, что вам необходимо.

JavaDoc

Javadoc – это инструмент, который поставляется с JDK и используется для создания документации кода Java в формате HTML из исходного кода Java, для чего требуется документация в заранее определенном формате.

Javadoc генерируется с помощью так называемого «доклета». Различные докледы могут по-разному анализировать аннотации Java и создавать разные выходные данные. Но по большому счету почти каждая документация по Java использует стандартный доклед.

При документировании приложения необходима поддержка документации программы. Если документация и код разделены, то непроизвольно создаются сложности, связанные с необходимостью внесения изменений в соответствующие разделы сопроводительной документации при изменении программного кода: javadoc - решение этой проблемы.

Unit testing

Unit Testing – это тип тестирования программного обеспечения, при котором тестируются отдельные модули или компоненты программного обеспечения. Его цель заключается в том, чтобы проверить, что каждая единица программного кода работает должным образом. Данный вид тестирование выполняется разработчиками на этапе кодирования приложения. Модульные тесты изолируют часть кода и проверяют его работоспособность. Единицей для измерения может служить отдельная функция, метод, процедура, модуль или объект.

Документация по одному из самых популярных фреймворком JUnit:

<https://junit.org/junit5/docs/current/user-guide/>

Sonarqube

SonarQube - это платформа с открытым исходным кодом, разработанная SonarSource, для непрерывной оценки качества кода путем статического анализа, сканирования кода. Завершив это сканирование, SonarQube формирует отчет, который можно посмотреть в GUI через браузер. Все обнаруженные проблемы представляют собой “интерактивные тикеты”, позволяющие писать к ним комментарии, делегировать их другим пользователям, открывать или закрывать и т. д.

Инструмент предоставляет систематизированный отчет о качестве кода, безопасности и общий Quality Gate Status. Он поддерживает контроль версий, каждая из которых фиксирует конкретный коммит или слияние веток в проекте.

Этот инструмент отлично подходит для командного взаимодействия, поскольку позволяет всем участникам совместно работать над качеством кода в проектах. SonarQube можно интегрировать в конвейеры и веб-сайты, например GitHub, а GitLab поддерживает его по умолчанию.

Разработка frontend (FTL)

Построение тем keycloak основано на шаблонизаторе FreeMarker + AngularJS.

Шаблоны FreeMarker имеют расширение **.ftl**. Синтаксис разметки фактически является синтаксисом html расширенным новыми тегами и конструкциями. Freemarker интегрируется с java и позволяет использовать интерполяцию java переменных.

Темы

Создание темы

За кастомные темы Keycloak отвечает модуль kcse-platform-v-theme.

Принцип создания новой темы - переопределение файлов базовой темы.

Переопределенные компоненты содержатся в директории theme/mytheme по аналогии с темой platform-v. Кроме того кастомную тему необходимо объявить в файле META-INF/keycloak-theme.json в массиве themes

```
{  
  "themes": [  
    {"name": "platform-v",  
     "types": [  
       "admin",  
       "account",  
       "login",  
       "email",  
       "welcome"  
     ]  
   }]  
}
```

Добавление органов управления на страницу

Кроме кастомной стилизации темы могут содержать графические органы управления с расширенной функциональностью. Добавление новой функциональности на страницу осуществляется переопределением соответствующей html-страницы стандартной темы.

Так, например, для добавления новых блоков на страницу Роли > Роли по умолчанию (Roles > Default roles) следует скопировать из базовой темы страницу realm-default-roles.html и положить в папку кастомной темы по аналогичному оригиналу пути theme/admin/resources/partials. Теперь страницу можно отредактировать. Затем пересобрать модуль. Для просмотра изменений необходимо помнить о кэшировании страниц в браузере.

Частые ошибки

Если изменения не отображаются

- Отключите или сбросьте кэш браузера
- Для standalone-версии приложения убедитесь, что тема развернулась. Рядом с собранным .jar в папке /standalone/deployments должен появиться файл с расширением .deployed
- Убедитесь, что в настройках реалма тема выбрана для соответствующего раздела UI (например, консоль администратора) и вход также произведен именно в этот реалм.

Локализация

При реализации кастомной темы также следует уделить внимание локализации, то есть адаптации интерфейса к языку конечного пользователя. Существуют различные варианты работы с данными файлами в разных языках программирования.

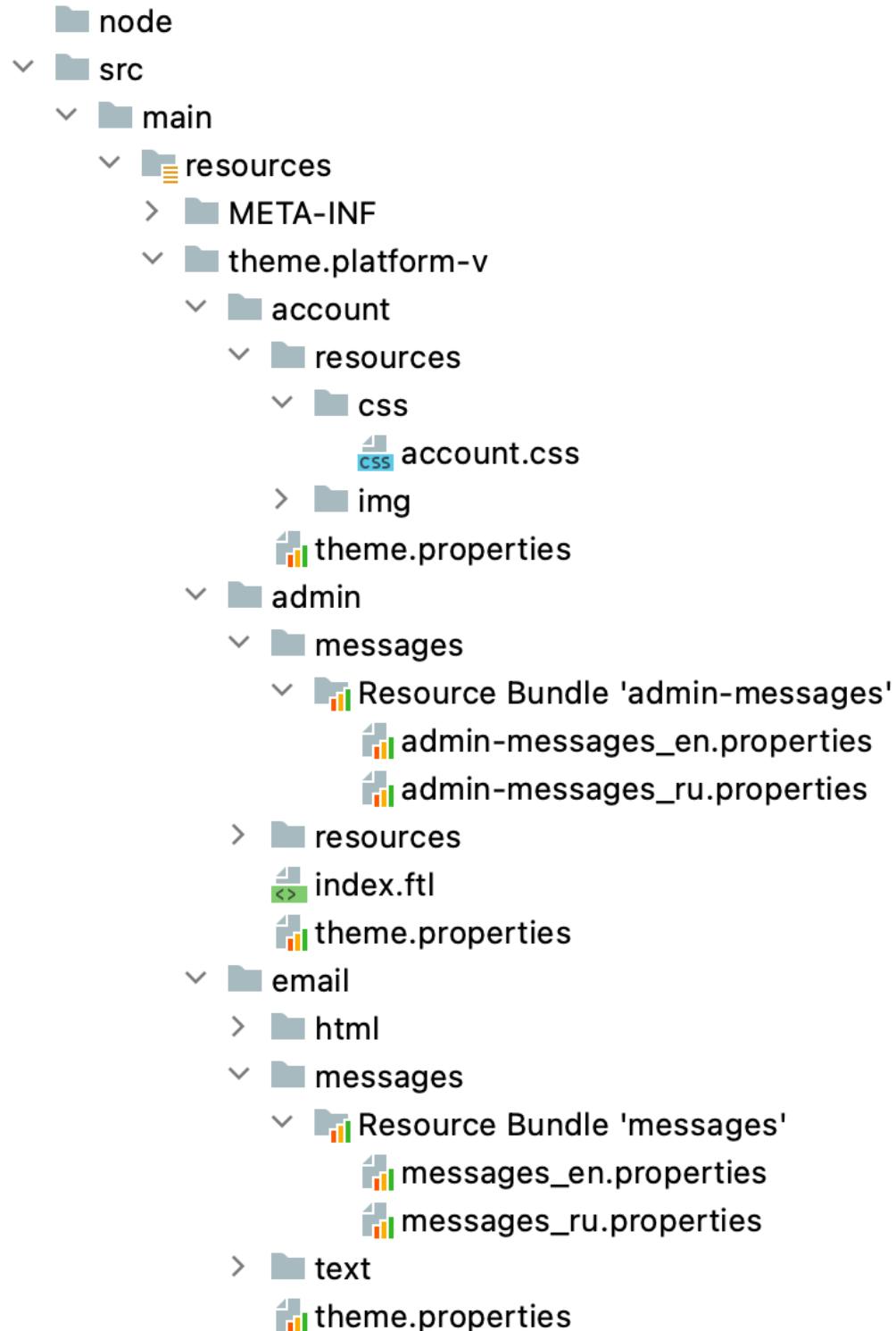
Необходимо получать соответствующую настройку локализации (язык), а затем по ключу доставать из файла необходимый текст и использовать его в интерфейсе.

messages_en.properties

```
## custom messages
readFromTM_domain_label=Domain for read TM
```

В Keycloak.SE реализована данная возможность при помощи соответствующих файлов:

kcse-platform-v-theme



Запуск контейнера без прав внесения изменений в корневой файловой системе

В данном режиме запрещено запускать контейнер с правами внесения изменений в корневой файловой системе. При активации этого режима злоумышленник не сможет записать посторонние исполняемые файлы на диск в корневую файловую систему. Режим настраивается в приложении и активируется настройками в скриптах запуска контейнера. В переменной окружения WRITABLE_PATH задается директория, в которую монтируется директория с правом записи файлов. По умолчанию данная переменная принимает значение “/tmp/kcse”. Контейнер определяет режим запуска автоматически.

При запуске приложения в Docker при помощи утилиты docker-compose необходимо при определении сервиса указать параметр “read_only: true” и примонтировать том (см. volumes) в директорию заданную в переменной WRITABLE_PATH.

```
#docker-compose.yml
services:
  keycloak:
    image: keycloak.se:1.0
    read_only: true
    container_name: keycloak
    environment:
      KEYCLOAK_LOGLEVEL: "INFO"
...
volumes:
  - ./tmp:/tmp
```

При запуске приложения в Kubernetes/OpenShift необходимо при определении сервиса указать параметр “readOnlyRootFilesystem: true” и примонтировать том (см. volumeMounts) в директорию, заданную в переменной WRITABLE_PATH. Пример запуска в OpenShift:

```
## pod_READONLY.yml
apiVersion: v1
kind: DeploymentConfig
metadata:
  name: keycloak
  labels:
    name: keycloak
spec:
  containers:
    - name: keycloak
      image: <image_link>
      env:
```

```
...
securityContext:
  readOnlyRootFilesystem: true
  runAsNonRoot: true
ports:
  - containerPort: 80
volumeMounts:
  - mountPath: /tmp
    name: tmp
    readonly: false
  - name: shared-logs
    mountPath: /opt/keycloak/log/
volumes:
  - name: tmp
    emptyDir: {}
  - name: shared-logs
    emptyDir: {}
```

При запуске в Kubernetes следует вместо DeploymentConfig указать Deployment.

Использование программного компонента

Основной кейс использования KeyCloak.SE – использование продукта в качестве IDP провайдер для осуществления управления учетными записями пользователей, клиентов (приложений), а также контроль их аутентификации и предоставление доступа к различным ресурсам.

Часто встречающиеся проблемы и пути их устранения

В случае падения приложения cache данных по сессиям удаляется, что приводит к обрыву активных сессий пользователей и их “выбросу” из приложений, использующих KeyCloak.SE

Сертификат

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. SSL-сертификат содержит следующую информацию:

- доменное имя, на которое оформлен SSL-сертификат;
- юридическое лицо, которое владеет сертификатом;
- физическое местонахождение владельца сертификата (город, страна);
- срок действия сертификата;
- реквизиты компании-поставщика SSL-сертификата.

Протокол HTTPS, поддерживающий технологию шифрования TLS/SSL, использует сертификаты для проверки принадлежности открытого ключа его реальному владельцу. Он создает безопасный канал в незащищенной сети. Это обеспечивает достаточную защиту от перехватчиков и атак типа «человек посередине» при условии, что используются адекватные наборы шифров и что сертификат сервера проверен и доверен.

Способы получения SSL-сертификата:

- Использовать сертификат, выданный CA (Certification authority), то есть центром сертификации или удостоверяющим центром;
- Использовать самоподписанный сертификат;
- Использовать «пустой» сертификат.

Самоподписанный сертификат — сертификат, созданный самим пользователем — в этом случае издатель сертификата совпадает с владельцем сертификата. «Пустой» сертификат — сертификат, содержащий фиктивную информацию, используемую в качестве временной для настройки SSL и проверки его функциональности в данной среде.

Для получения самоподписанного сертификата необходимо:

ssl.conf

```
[req]
default_bits = 4096
distinguished_name = req_distinguished_name
req_extensions = req_ext

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = RU
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Moscow
localityName = Locality Name (eg, city)
localityName_default = Moscow
organizationName = Organization Name (eg, company)
organizationName_default = Sberbank
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_max = 64
commonName_default = apps.dev-gen.my.company.ru

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = *.apps.dev-gen.my.company.ru
```

get_selfsigned_cert.sh

```
openssl req -newkey rsa:4096 -x509 -days 3654 -nodes \
-config ssl.conf \
-keyout ca.key -out ca.crt

## Создание сертов под сервер\стенд
name=proxy-server
openssl req -new -newkey rsa:4096 -sha256 -nodes \
-keyout $name.key -out $name.csr \
-config ssl.conf

openssl x509 -req -CAcreateserial -days 1000 -sha256 \
-CA ca.crt -CAkey ca.key \
-extensions req_ext \
-extfile ssl.conf \
-in $name.csr -out $name.crt
```

Уязвимости

Неиспользуемые зависимости

Для того чтобы используемые модули были максимально безопасными, рекомендуется исключать из зависимостей неиспользуемые зависимости. Эти неиспользуемые зависимости по-прежнему доступны в вашей программе и могут содержать уязвимые места. В целом, независимо от того, используется зависимость или нет, разработчики должны проверить, безопасно ли включать ее в свою систему.

Maven помогает определить неиспользуемые зависимости:

pom.xml

```
<build>
  <plugins>
    <plugin>
      <artifactId>maven-dependency-plugin</artifactId>
      <version>3.1.2</version>
    </plugin>
  </plugins>
</build>
```

Необходимо запустить в командной строке:

```
mvn dependency:analyze
```

IntelliJ IDEA так же позволяет найти уязвимости в используемых зависимостях.

XSS

XSS (межсайтовый скриптинг) – одна из разновидностей атак на веб-системы, которая подразумевает внедрение вредоносного кода на определенную страницу сайта и взаимодействие этого кода с удаленным сервером злоумышленников при открытии страницы пользователем.

Основная цель межсайтового скриптинга – кража cookies пользователей при помощи встроенного на сервере скрипта с дальнейшей выборкой необходимых данных и использованием их для последующих атак и взломов. Злоумышленник осуществляет атаку пользователей не напрямую, а с использованием уязвимостей веб-сайта, который посещают жертвы, и внедряет специальный JavaScript. В браузере у пользователей этот код отображается как единая часть сайта. При этом посещаемый ресурс по факту является соучастником XSS-атаки.

Необходимо экранировать входящие и исходящие строковые параметры.

EscapeHtml.java

```
org.apache.commons.lang.StringEscapeUtils.escapeHtml("example_with_vulnerability");
```

Либо заменять специальные символы (&,<,>,“,’), которые используются для записи скрипта, на html entities name.

Руководство по эксплуатации компонента IAM Proxy (AUTH)

Руководство по системному администрированию компонента IAM Proxy (AUTH)

Сценарии администрирования

Этот документ содержит названия переменных одинаково применимых для различных сред контейнеризации, указанных в системных требованиях. Имя переменной не определяет конкретную среду контейнеризации.

Введение

Данный раздел содержит описание сценариев администрирования IAM Proxy.

Варианты администрирования

Администрирование IAM Proxy осуществляется преимущественно через изменение конфигурации 3 способами:

1. Использование компонента PACMAN (CFGА). Данный способ является целевым и рекомендуется для использования.
2. Использование yaml-файла конфигурации формата компонента PACMAN (CFGА).
3. Использование yaml-файла параметров inventory-ansible, при установке с помощью Ansible. Подходит для версий IAM Proxy без развернутого RDS-Server.

Администрирование с использованием компонента Расман (CFGА)

Компонент Расман (CFGА) представляет собой централизованный инструмент управления параметрами и конфигурациями. Компонент Расман (CFGА) используется для изменения конфигурации без повторного развертывания.

Использование компонента Расман (CFGА) описано в разделе Администрирование с помощью компонента PACMAN (CFGА).

Для корректной работы в компоненте PACMAN (CFGА), администратор должен ознакомится с параметрами настроек.

При работе с компонентом Расман (CFGА), администратор должен руководствоваться правилами эксплуатации.

Типовые сценарии администрирования компонента IAM Proxy

Типовыми сценариями администрирования являются:

- Добавление/удаление/изменение ответвлений.
- Контроль событий системного журнала. Описан в разделе События системного журнала.
- Контроль событий мониторинга. Описан в разделе События мониторинга.

Добавление нового ответвления (junction)

Для создания нового ответвления, выполнить следующие действия:

- При использовании PACMAN (CFGА):
 1. Открыть UI PACMAN (CFGА), выбрать раздел артефакта `rds-server` относящийся к текущему контуру.
 2. Создать новое ответвление. Нажать кнопку **Добавить** в строке содержащей `JunctionConfig` и заполнить обязательные параметры. При создании ответвления для нескольких контуров (`Zone`) добавить новую секцию `Junction` входящее в этот контур (`Zone`) (подробнее в разделе Параметры настройки).
 3. Нажать кнопку **Сохранить**.
- При использовании yaml-файла формата PACMAN (CFGА):
 1. Открыть в режиме редактирования конфигурационный файл предназначенный для настройки IAM Proxy.
 2. Создать новое ответвление. Добавить новую секцию `JunctionConfig` и заполнить обязательные параметры. При создании ответвления для нескольких контуров (`Zone`) добавьте новую секцию `Junction` входящее в этот контур (`Zone`) (подробнее в разделе Параметры настройки).
 3. Сохраните измененный файл.

Изменение параметров ответвления (junction)

Для изменения существующего ответвления, выполнить следующие действия:

- При использовании PACMAN (CFGА):
 1. Открыть UI PACMAN (CFGА), выбрать раздел артефакта `rds-server` относящийся к текущему контуру.
 2. Выбрать необходимое ответвление в `JunctionConfig` и заполнить параметры требующие изменения.

3. Нажать кнопку **Сохранить**.

- При использовании yaml-файла формата PACMAN (CFGА):
 1. Открыть в режиме редактирования конфигурационный файл предназначенный для настройки IAM Proxy.
 2. Найти необходимое ответвление в секции **JunctionConfig** и заполнить параметры требующие изменения.
 3. Сохраните измененный файл.

Удаление параметров ответвления (junction)

Для удаления ответвления, выполнить следующие действия:

- При использовании PACMAN (CFGА):
 1. Открыть UI PACMAN (CFGА), выбрать раздел артефакта **rds-server** относящийся к текущему контуру.
 2. Удалить необходимое ответвление. Нажать кнопку **Удалить**. При наличии ответвления в нескольких контурах (Zone) удалить ответвление во всех разделах контуров (Zone) (подробнее в разделе Параметры настройки).
 3. Нажать кнопку **Сохранить**.
- При использовании yaml-файла формата PACMAN (CFGА):
 1. Открыть в режиме редактирования конфигурационный файл, предназначенный для настройки IAM Proxy.
 2. Найти необходимое ответвление в секции **JunctionConfig** и удалить раздел с этим ответвлением. При наличии ответвления в нескольких контурах (Zone) удалить ответвление во всех разделах контуров (Zone).
 3. Сохраните измененный файл.

Параметры настройки

Примечание

Данный раздел содержит описание параметров конфигурационного файла для настройки IAM Proxy.

Группа ZoneConfig

Данная группа содержит основные параметры конфигурации IAM Proxy.

JunctionConfig

Группа основных параметров ответвления (junction) IAM Proxy. Название ответвления, отображается только на стартовой странице IAM Proxy.

На стартовой странице допускается объединять ответвления в группы. Это позволяет упорядочить список внешне на UI и не влияет на процесс проксирования.

Для объединения в группу этого необходимо сначала указать название группы, затем, через / название самого ответвления. Пример: **Группа ответвлений / мое ответвление** - на стартовой странице IAM Proxy в списке появиться раскрываемая строка с названием “Группа ответвлений”. При раскрытии в списке появятся “мое ответвление”.

Параметр	Значение по умолчанию	Описание	Пример
junctionName	Отсутствует	Название ответвления, отображается и существует только на стартовой странице IAM Proxy. На стартовой странице также можно объединять ответвления в группы, это никак не влияет на процесс проксирования, лишь позволяет внешне на UI упорядочить список. Для этого необходимо сначала указать название группы, затем, через / название самого ответвления, например: Группа ответвлений / мое ответвление . На стартовой странице IAM Proxy в списке появиться раскрываемая строчка с названием “Группа ответвлений”. После раскрытия в списке появятся строчки с ответвлениями из развернутой группы, в нашем примере, появится “мое ответвление”	Контур “Компания”/Страница администрирования контура “Компания”
description	Отсутствует	Описание ответвления, отображается и существующее только на стартовой странице IAM Proxy	Страница предназначен а для администриро вания контура “Компания”

Параметр	Значение по умолчанию	Описание	Пример
junctionPoint *	Отсутствует	<p>Параметр, определяющий абстрактные директории на уровне IAM Proxy. Формирует URL вида: https://proxy.com/myJunctionPoint. При HTTP Request на данный URL пользователь получит HTTP Answer корневого каталога Backend. Этот параметр позволяет определить принадлежность запроса к конкретному сервису, конкретному Backend. Также по нему станет доступен какой-либо подкаталог из Backend, например: https://proxy.com/myJunctionPoint/index.html - в качестве ответа пользователь получит файл index.html лежащий в корневой директории Backend. Возможно также создать ответвление в “корень” сервиса IAM Proxy. В качестве значения необходимо указать /. Стартовая страница пропадет, и запросы с proxy.com/ будут идти напрямую на указанный Backend</p>	/company
indexUrl	Отсутствует	<p>Параметр предназначен для формирования ссылки на стартовой странице IAM Proxy и не влияющий на процесс проксирования. Пример: требуется настроить проксирование со страницы IAM Proxy testpage/index.html на страницу Backend:1. При значении false параметра transperent:</p> <p>https://backend.com/junctionPoint/index.html - корневая страница Backend</p> <p>https://backend.com/junctionPoint/testpage/index.html - страница, на которую хотелось бы попадать со стартовой страницы IAM Proxy2. При значении true параметра transperent:</p> <p>https://backend.com/index.html - корневая страница Backend, https://backend.com/testpage/index.html - страница, на которую хотелось бы попадать со стартовой страницы IAM Proxy. В случае указания в данном параметре /testpage/index.html будет производиться редирект со стартовой страницы IAMProxy SE на эту страницу</p> <p>https://backend.com/junctionPoint/testpage/index.html или https://backend.com/testpage/index.html, хотя корневой контекст Backend будет другим</p> <p>https://backend.com/junctionPoint/index.html или https://backend.com/testpage/index.html. Если оставить данный параметр пустым, либо указать «-», то ссылка на данное ответвление не будет отображаться на стартовой странице IAM Proxy. Для того чтобы попадать на корневую страницу Backend, необходимо в данный параметр указать “/”</p>	/admin

Параметр	Значение по умолчанию	Описание	Пример
transparent *	False	<p>Тождество (“прозрачность” или “одинаковость”), равенство той части URL, в которой содержится директория до ресурса. Параметр определяет, будет ли передаваться junctionPoint внутри URL на Backend и обратно. True - при проксировании запросы будут проходить без изменения URL на каком либо этапе. URL отправленный в сервис IAM Proxy (к примеру, введенный пользователем в адресной строке браузера) будет совпадать с URL который придет на backend (на сервер приложения). В обратном случае: URL ответа от Backend будет совпадать с URL пришедшем пользователю от IAM Proxy. Например: Отправлений HTTP Request от пользователя → IAM Proxy → Полученный HTTP Request на Backend https://proxy.com/junctionPoint/index.html → IAM Proxy → https://backend.com/junctionPoint/index.html. Полученный HTTP Answer к пользователю ← IAM Proxy ← Отправлений HTTP Answer от Backend https://proxy.com/junctionPoint/page.html ← IAM Proxy ← https://backend.com/junctionPoint/page.html. False - значение из junctionPoint будет вырезано из URL запросов, и вставлено в URL в контента ответов. Из URL отправленной в сервис IAM Proxy (к примеру, введенный пользователем в адресной строке браузера) будет вырезан junctionPoint из URL который придет на Backend (на сервер приложения). И наоборот: в URL ответа от Backend будет добавлен параметр junctionPoint. Отправлений HTTP Request от пользователя → IAM Proxy → Полученный HTTP Request на Backend https://proxy.com/junctionPoint/index.html → IAM Proxy → https://backend.com/index.html. Полученный HTTP Answer к пользователю ← IAM Proxy ← Отправлений HTTP Answer от Backend https://proxy.com/junctionPoint/page.html ← IAM Proxy ← https://backend.com/page.html</p>	True
https *	True	Параметр, для определения типа запросов подключения к Backend. True – на Backend используется SSL для доступа к сервису, False – на Backend не используется SSL для доступа к сервису	False
sslCommonName	.mycompany.ru	Шаблон\значение имени из CN сертификата backend-серверов, используется при соединении с backend по HTTPS. Значение * (звездочка) отключает проверку SSL	.ourcompany.ru

Параметр	Значение по умолчанию	Описание	Пример
serverAddresse s[]	Отсутствует	Параметр принимающий на вход список Backends, для осуществления проксирования запросов и ответов в рамках данного ответвления с помощью IAM Proxy. Минимальное количество: 1 Backend. Указывается в формате: address:port	10.X.X.1:9443 abs- 4.mycompany. mycompany.ru: 8080
applyJctReques tFilter	Отсутствует	Применить фильтр(конфигурацию) для запросов на этот junction. можно задать набор из следующих значений (через запятую): common/oidc-unauth-access.location.conf - отключение функциональности по аутентификации\авторизации на ответвлении; common/rds-set-header-host-to-backend.location.conf - переопределение заголовка Host в сторону backend с указанием первого сервера из пула балансировки (необходимо использовать при проксировании в сторону OpenShift); common/rds-ssl-sni-on.server.conf - разрешает передачу имени сервера по SNI, fqdn-имя сервера обязательно задается в proxy_ssl_name (необходимо использовать при проксировании в сторону OpenShift при routes с типом passthrough)	common/set-authz-by-role-admin.location.conf

Примечание:

* - параметр обязательный к заполнению (при создании конфигурации вручную, данные параметры обязательны к наличию в файле).

Полный набор значений для applyJctRequestFilter в разделе Файлы дополнительных опций для ответвлений.

Группа ZoneConfig

Группа параметров для всех возможных зон (default, standIn, offline).

Параметр	Значение по умолчанию	Описание	Пример
zoneNameStandin *	standin	Параметр предназначен для задания кастомизированного имени зоны StandIn	zone1
zoneNameOffline *	offline	Параметр предназначен для задания кастомизированного имени зоны offline. Данная зона используется при недоступности основной и StandIn зоны (например идет переключение на StandIn)	zone2

Примечание:

* - параметр обязательный к заполнению (при создании конфигурации вручную, данные параметры обязательны к наличию в файле).

Группа ZoneConfig/Zone (standin/offline)

Группа предназначена для настроек конкретной зоны.

Параметр	Значение по умолчанию	Описание	Пример
applyRequestFilter	Отсутствует	Применить фильтр(конфигурацию) ко всем запросам всех перечисленных ответвлений(junctions)	common/rewrite-response-is-offline.server.conf

Группа ZoneConfig/Zone[]/Junction[]

Группа предназначена для настроек конкретного ответвления(junction) в рамках указанной зоны.

Параметр	Значение по умолчанию	Описание	Пример
serverAddresses[]	Отсутствует / serverAddresses[]	Каждый end-point должен быть описан строкой следующего вида: адрес узла[:порт] . Где: адрес узла – IP-адрес узла кластера или его DNS-имя; порт – порт, по которому происходит перенаправление (по умолчанию 443)	abs-5.mycompany.ru:4444

Параметры в корневом контексте

Данная группа содержит основные параметры конфигурации работы RDS-Server.

Параметр	Значение по умолчанию	Описание	Пример
checkConfigurationFrequency *	60	Частота проверки изменений в конфигурации (задается в секундах)	1
checkStandInFrequency *	10	Частота проверки флагов состояния контуров StandIn в ПЖ (задается в секундах)	35
httpClientMaxPoolSize *	1	Максимальное количество соединений в пуле REST-клиента	10
manualMode *	false	Включение режима ручного переключения на необходимый контур (true- разрешение смены контура вручную, false - запрет смены контура вручную)	true

Параметр	Значение по умолчанию	Описание	Пример
transportRequestTimeo ut *	9	Время ожидания ответа от ММТ (задается в секундах)	15
usePlatformSemaphore *	false	Флаг использования платформенного семафора (true - использовать платформенный семафор, false - использовать прикладной семафор)	true

Примечание:

* - параметр обязательный к заполнению (при создании конфигурации вручную, данные параметры обязательны к наличию в файле).

Администрирование с помощью компонента PACMAN (CFGА)

Предусловие

Перед началом использования компонента PACMAN (CFGА), ознакомьтесь с документацией на компонент PACMAN (CFGА).

Введение

Данное руководство предназначено для описания администрирования компонента IAM proxy с помощью компонента PACMAN (CFGА). Для использования компонента PACMAN (CFGА) необходимо иметь развернутый RDS-Server (подробнее в разделе Чек-лист валидации установки RDS-Server) и настроенную интеграцию RDS-server с компонента PACMAN (CFGА), подробнее в разделе Настройка получения конфигурации)

Для доступа в UI RDS, необходимо получить роль platformauth_admin (данная роль задается на стороне “Platform V IAM Keycloak.SE”). Роль platformauth_admin обладает правами на чтение статуса.

Доступ к приложению

Для получения доступа к настройкам приложения IAM Proxy, в компоненте PACMAN (CFGА), выполните следующие действия:

1. Перейдите на точку входа заданную на этапе развертывания IAM Proxy (подробнее в разделе Установка).
 - Если на IAM Proxy настроено корневое ответвление, то перейдите на /proxy/index.html. > Откроется форма аутентификации пользователя.
2. Пройдите аутентификацию, введя имя учетной записи и пароль, затем нажмите кнопку OK. > Если данные корректны, то откроется стартовая страница IAM Proxy.

3. На стартовой странице IAM Proxy выберите Platform V Starting Manager и нажмите кнопку **OK**.
4. Пройдите аутентификацию, введя имя учетной записи и пароль, затем нажмите кнопку **OK**. > Если данные корректны, то откроется окно компонента Platform V Starting Manager.

Главное окно компонента «Platform V Starting Manager».

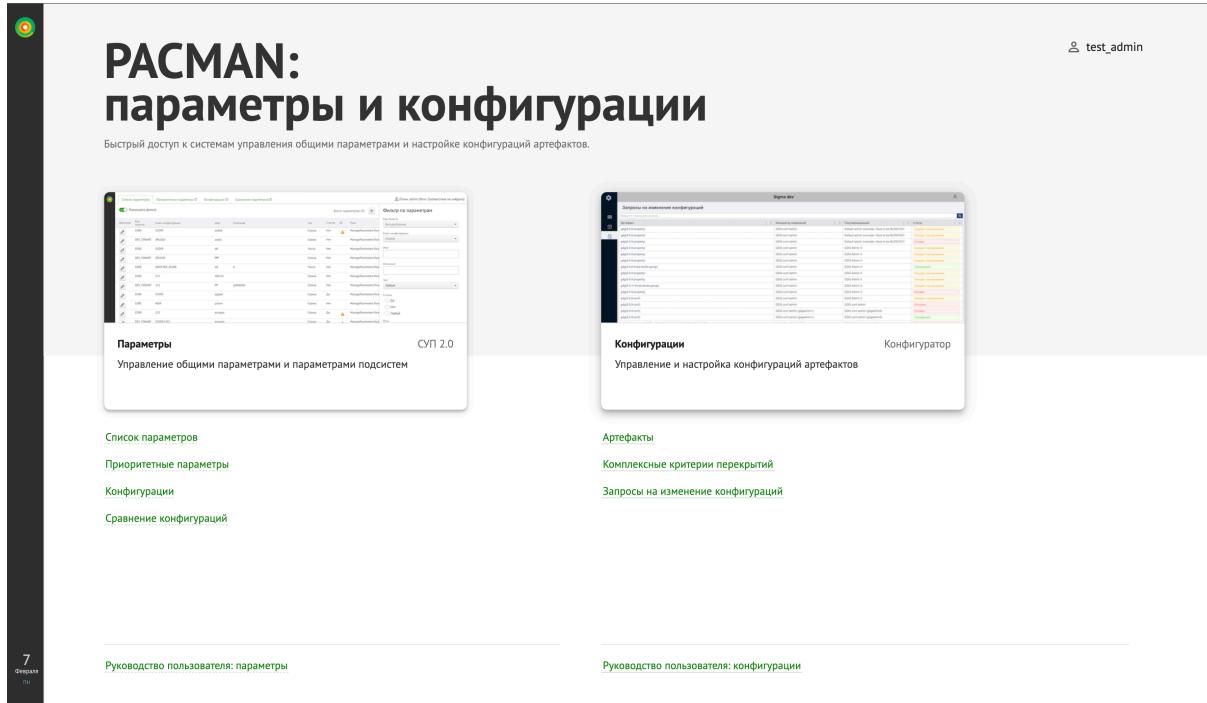


5. Нажать кнопку Управление параметрами 2.0. > Откроется единое окно «PACMAN (CFGА): параметры и конфигурации»

Управление параметрами 2.0

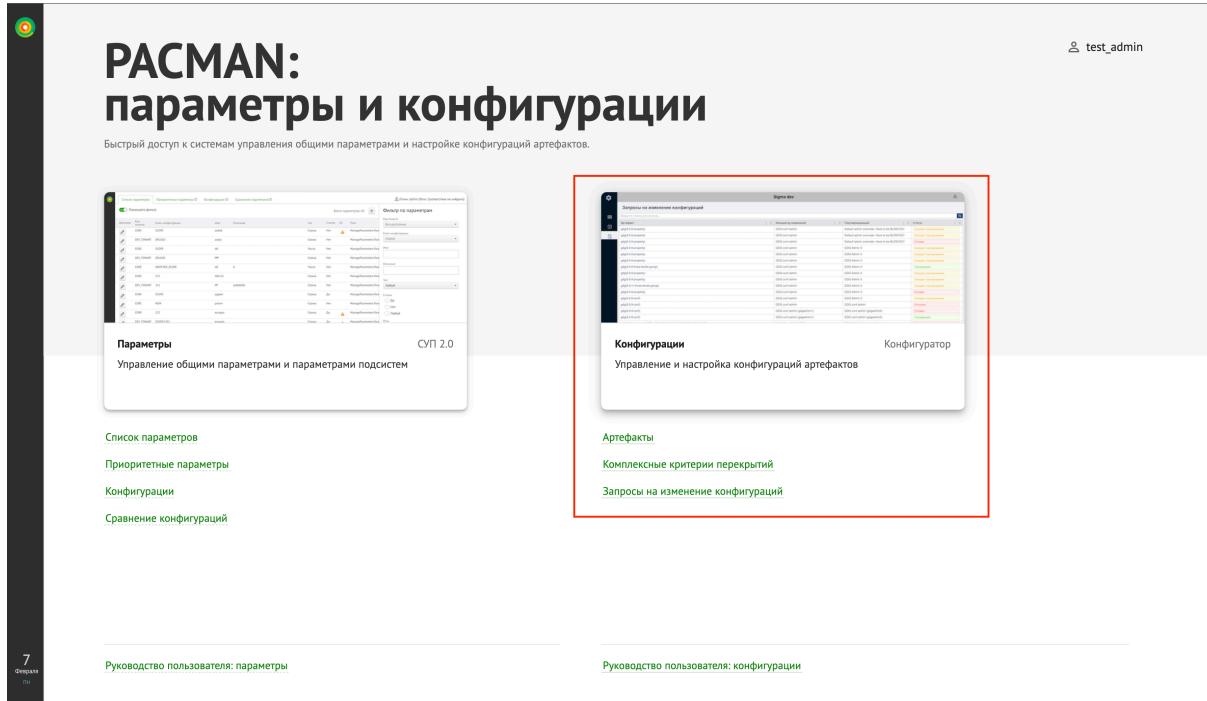


Единое окно управления параметрами и конфигурациями



6. Выберите модуль Конфигурации. Управление и настройка конфигураций артефактов. > Откроется АРМ компонента Platform V Configuration.

Конфигурации. Управление и настройка конфигураций артефактов

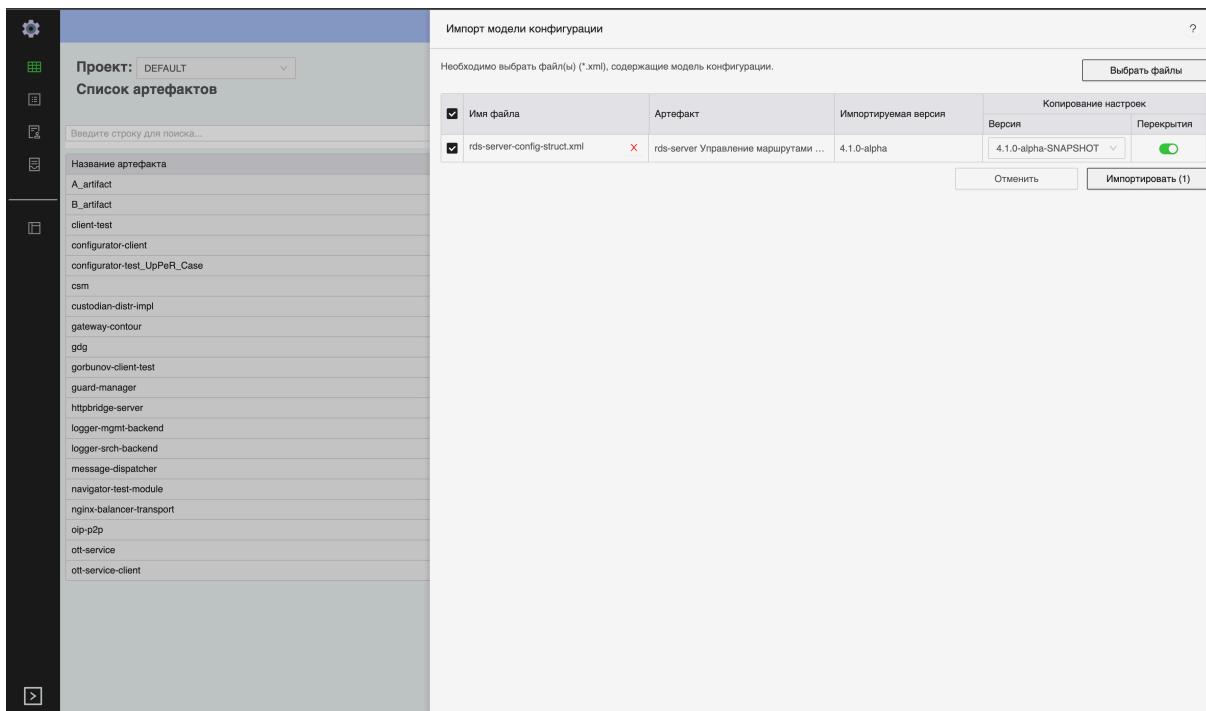


Использование приложения администратором

Загрузка модели конфигурации артефакта

Для загрузки модели конфигурации артефакта IAM Proxy, необходимо обладать правами не ниже администратора. Для загрузки модели конфигурации артефакта IAM Proxy, выполните следующие действия:

1. Пройдите авторизацию. > Откроется главная страница.
2. Нажать кнопку **Импорт модели**. > Откроется окно импорта моделей.
3. Нажать кнопку **Выбрать файлы**. > Откроется окно выбора файлов для импорта.
4. Укажите в файловой системе путь к xml-файлу модели конфигурации:(Расположение файла в дистрибутиве: /config/rds-server-configuration-struct.xml).
5. Нажать кнопку **Импортировать**. > Выполнится импорт указанного артефакта. > При импорте существующего артефакта, выполнится его обновление до новой версии. > При повторном импорте уже существующей версии артефакта с заполненными настройками, отобразится сообщение о > необходимости удаления перекрытия.



Описание полей таблицы с файлами для импорта:

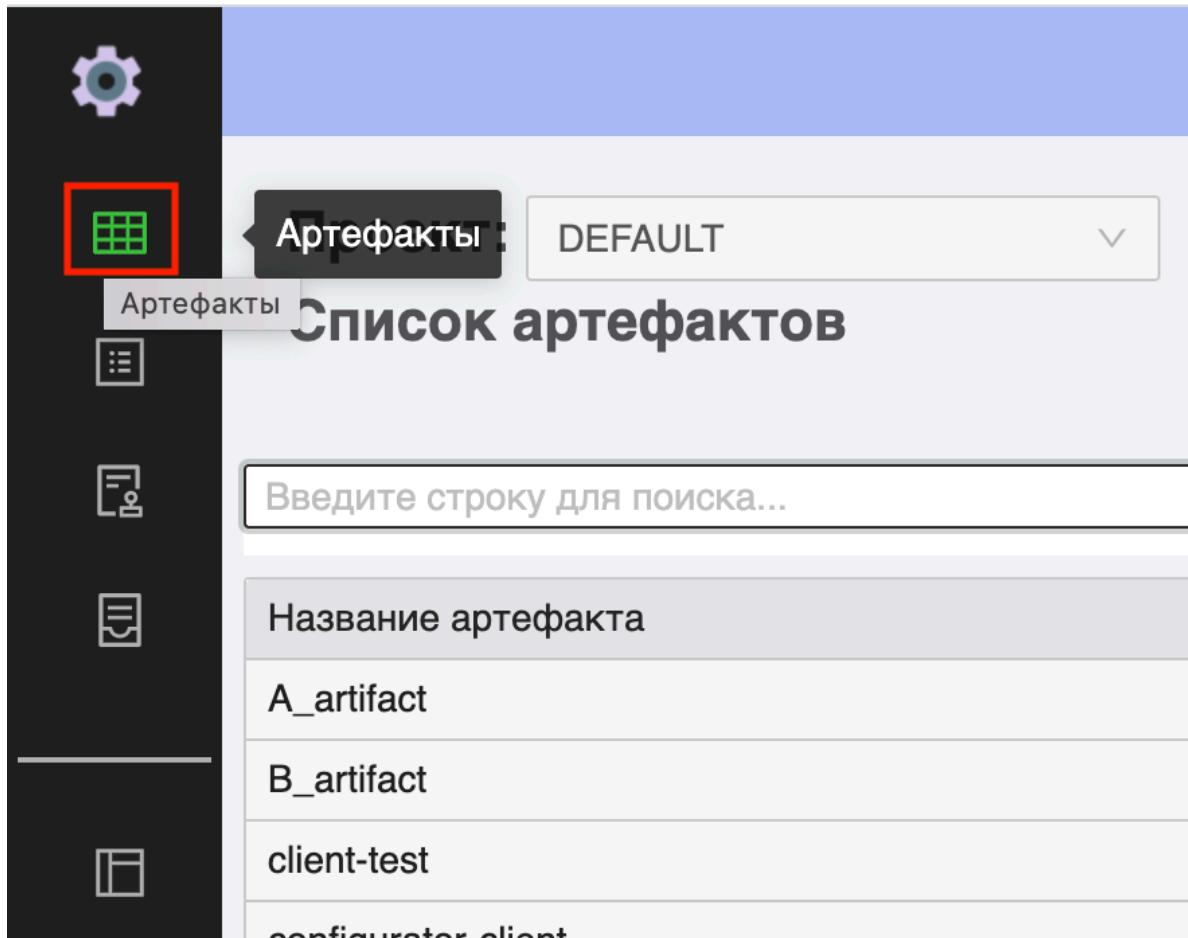
Наименование поля	Описание
Имя файла	Содержит наименование выбранного для импорта файла и кнопку для удаления файла из списка

Наименование поля	Описание
Артефакт	Содержит название артефакта и оригинальное имя артефакта
Импортируемая версия	Содержит название версии артефакта
Копируемая версия	Содержит элементы управления, обеспечивающие копирование настроек из выбранной версии в импортируемую с дополнительной возможностью копирования всех перекрытий из указанной версии

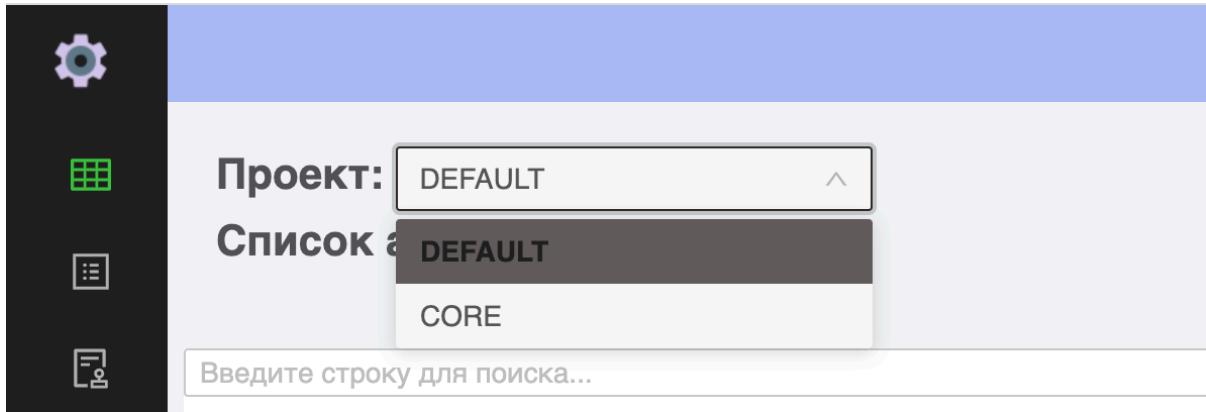
Изменение значений параметров конфигураций с помощью интерфейса

Для изменения значение настройки, выполните следующие действия:

- Нажмите на иконку “Артефакты”. > Откроется окно артефактов.



- Откройте всплывающие меню “Проект” и выберите проект default.



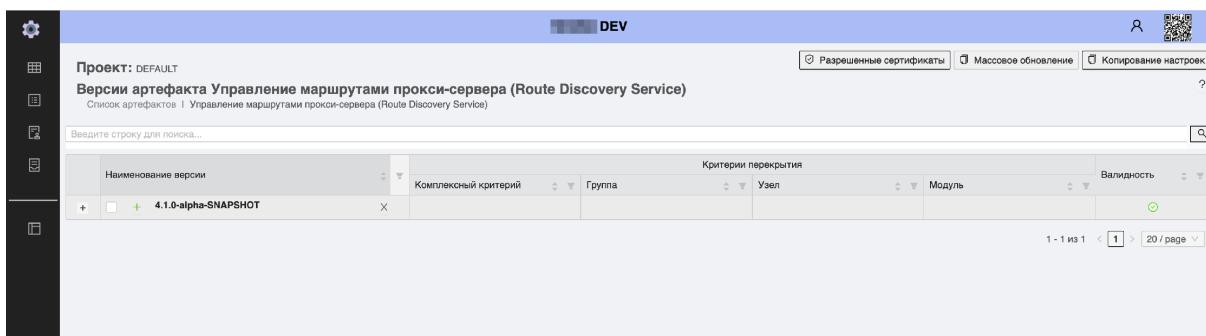
- В поисковой строке, введите **rds-server** и нажмите иконку “Поиск” > На экран будут выведены результаты поиска по заданным параметрам.



- Выберите артефакт из полученных результатов поиска, соответствующий параметрам:
 - название артефакта: Управление маршрутами прокси-сервера (Route Discovery Service);
 - оригинальное имя артефакта: rds-server.
> Откроется окно выбранного артефакта



- Выберите необходимую версию артефакта, нажав на нее. > Откроется окно выбранной версии артефакта.



- Раскройте дерево конфигурации выбранной версии, нажав на нее. > Раскроется дерево конфигурации.

The screenshot shows the configuration interface for the IAM Proxy component. The top navigation bar indicates the project is 'DEFAULT' and the environment is 'DEV'. The main area displays a hierarchical tree of configuration elements under '4.1.0-alpha-SNAPSHOT'. The tree includes nodes for 'Root', 'ZoneConfig', and various 'JunctionConfig' sub-nodes like '1-Configurator' and '1-Configurator-PACMAN'. Each node has associated properties listed in a table, such as 'junctionName', 'junctionPoint', and 'serverAddresses'. A search bar at the top allows for filtering the tree. Buttons for saving changes and performing a full search are visible in the top right.

Пример работы с деревом конфигурации: Создание нового узла дерева конфигурации

Для избежания ошибок имя узла дерева (группы) должно быть уникально, например: GROUP123

Для создания нового узла дерева конфигурации, выполните следующие действия:

1. Нажмите на иконку “Добавить узел дерева” > Откроется окно создания нового узла.

This screenshot shows the configuration interface with a modal dialog box titled 'Добавить узел дерева' (Add tree node) overlaid on the configuration tree. The dialog box contains a single input field for the new node name. A red box highlights the '+' icon next to the input field, which is used to trigger the creation of a new node. The background configuration tree remains visible, showing existing nodes like 'Root', 'ZoneConfig', and various junction configurations.

2. Заполнить значения параметров в соответствующих полях (например: junctionPoint).

The screenshot shows the configuration interface for the IAM Proxy component. The 'junctionPoint' field under the 'GROUP123' group is highlighted, showing its current value as '/snoop'. This indicates that the configuration has been updated but not yet saved.

3. Нажать кнопку Сохранить все. > Изменения сохранятся, созданный узел дерева будет добавлен в общий список.

The screenshot shows the configuration interface after the changes have been saved. The 'junctionPoint' field under the 'GROUP123' group now displays '/snoop'. The 'Save All' button is highlighted, indicating the action that triggered the save operation.

Примечание: Любые изменения конфигурации без щелчка по кнопке Сохранить все не сохраняются. При сохранении выполняется итоговая проверка конфигурации в

соответствии с моделью. При неуспешной валидации выводится предупреждающее сообщение о причине.

Загрузка значений параметров конфигураций

Загрузка значений параметров конфигураций IAM Proxy предназначена для быстрого изменения значений параметров с помощью файла *.properties. Данный файл создается с помощью операции экспорта конфигурации в файл.

Загрузить значения параметров конфигурации артефакта можно следующими способами:

- через дерево конфигурации; -с помощью кнопки **Импорт настроек** ;

Пример файла *.properties:

```
#@artifact=rds-server
#@artifact_version=4.1.0-alpha-SNAPSHOT
#@version.crit=[;;]
#Tue Feb 08 09:35:46 MSK 2022

rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-
Configurator]/applyJctRequestFilter=common/rds-set-header-host-to-backend.location.conf
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/authorizeByRoleTemplate=
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/https=false
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-
Configurator]/indexUrl=/pacman/sup/#%7B%22data%22:%7B%22appLocation%22:%22/%22%7D%
7D
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/junctionName=#BD/Platform V
Configuration OSE
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/description=Расширенное
описание #BD/Platform V Configuration OSE
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/junctionPoint=/pacman
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-
Configurator]/serverAddresses=ingressgateway-pacman-ui-unver.pacman.apps.dev-
gen.mycompany.ru:80;
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/sslCommonName=*
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator]/transparent=true
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-
PACMAN]/applyJctRequestFilter=
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-
PACMAN]/authorizeByRoleTemplate=
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-PACMAN]/https=true
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-PACMAN]/indexUrl=/ufs-
config-manager/pacman/configurator/
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-
```

```
PACMAN]/junctionName=#BD/Platform V Configuration  
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-  
PACMAN]/description=Расширенное описание #BD/Platform V Configuration  
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-PACMAN]/junctionPoint=/cfg  
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-  
PACMAN]/serverAddresses=127.0.0.1:9444;  
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-PACMAN]/sslCommonName=*  
rds-server@ZoneConfig[ZoneConfig]/JunctionConfig[1-Configurator-PACMAN]/transparent=true  
...
```

Загрузка значений параметров конфигураций через дерево конфигурации

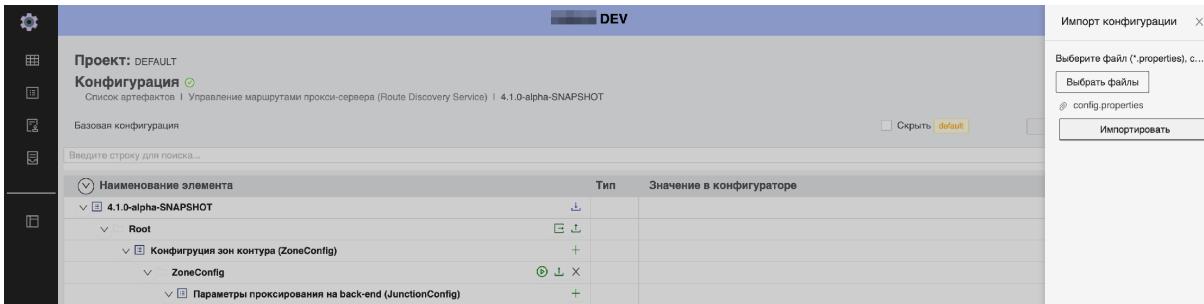
Перед загрузкой значений параметров конфигураций необходимо обязательно выполнить загрузку модели конфигурации артефакта.

Для загрузки параметров конфигурации артефакта, через дерево конфигурации, необходимо в окне просмотра параметров конкретной конфигурации:

1. Перейдите в окно просмотра параметров конфигурации. > Откроется окно просмотра параметров.
2. Нажмите на иконку , на уровне конфигурационного элемента. > Откроется окно импорта конфигураций.
3. Нажать кнопку **Выбрать файлы**. > Откроется окно выбора файлов.
4. Укажите путь к файлу *.properties в файловой системе. > Наименование файла отобразится под кнопкой **Выбрать файлы**.
5. Нажать кнопку **Импортировать**. > Начнется импорт выбранного файла.

При загрузке конфигурации выполняется проверка конфигурации в соответствии с моделью. При неуспешной валидации выводится предупреждающее сообщение о причине. При этом сохранение в базу выполняется независимо от результата валидации. Из файла не загружаются поля с признаком запрета миграции значения – **transient**. После импорта необходимо заполнить такие поля вручную и сохранить конфигурацию.

6. Дождитесь окончания импорта и заполните оставшиеся поля.
7. Нажать кнопку **Сохранить**. > Параметры конфигурации сохранены.



С помощью кнопки «Импорт настроек»

Предусловие

При импорте конфигураций для компонента обязательно должны быть выполнены условия:

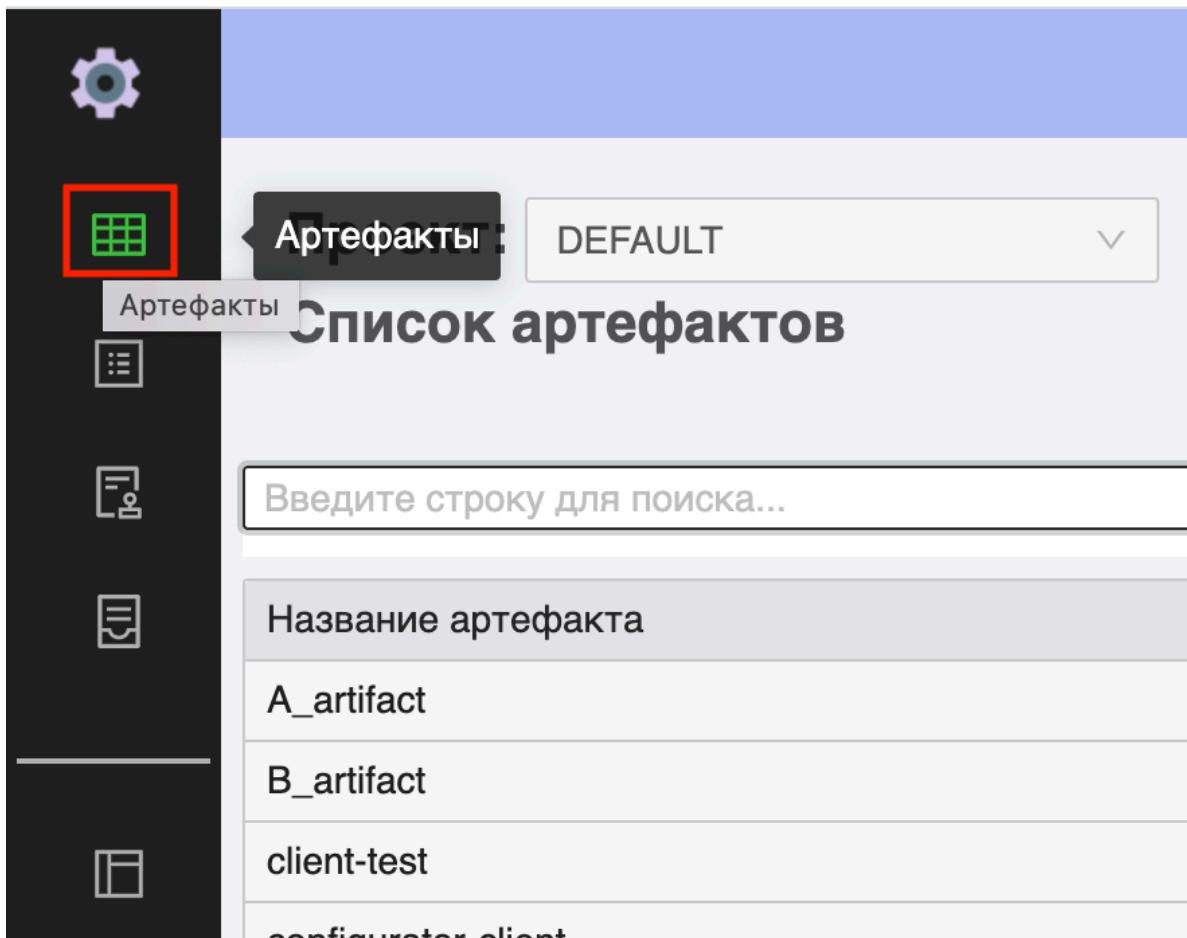
- Перед загрузкой значений параметров конфигураций необходимо обязательно выполнить загрузку модели конфигурации артефакта.
- В импортируемом файле обязательно наличие разделов:
 - `#@artifact=;`
 - `#@artifact_version=.`
- Для значений параметров применяются следующие ограничения:
 - при использовании DNS-имен в `serverAddresses` они должны успешно разрешаться в IP на DNS-сервере, который используется на IAM Proxy (иначе конфигурация не будет применена);
 - `applyJctRequestFilter` должен содержать пути к существующим файлам на IAM Proxy;
 - при `https = true` необходимо обеспечить наличие сертификатов ЦС в `TrustStore` IAM Proxy;
 - параметр `junctionPoint` должен быть уникален и не должен заканчиваться на `"/"`;
 - в случае наличия у всех запросов на приложение одного базового корневого контекста, рекомендуется использовать `transparent = true`;
 - использовать в `applyJctRequestFilter` опции `common/rds-set-header-host-to-backend.location.conf` и\или `common/rds-ssl-sni-on.server.conf` при проксировании в k8s\OS.

Импорт настроек

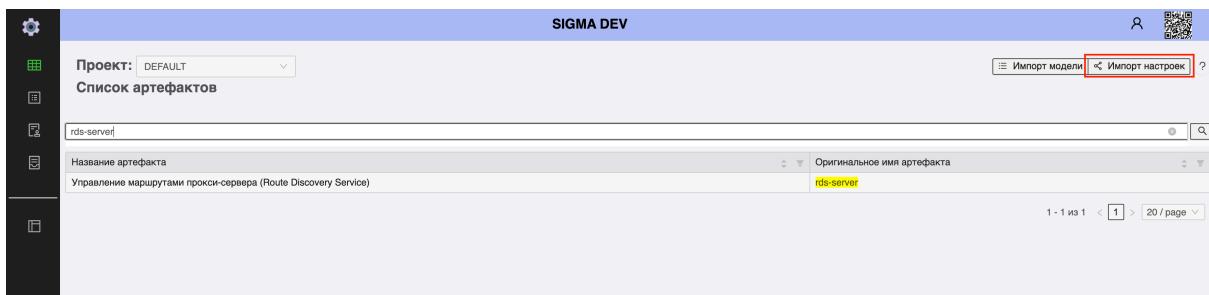
«Импорт настроек» позволяет импортировать любые значения конкретной указанной версии.

Для загрузки значений параметров конфигурации артефакта с помощью импорта настроек, выполните следующие действия:

1. Нажмите на иконку “Артефакты”. > Откроется окно артефактов.



2. На главной странице нажать кнопку Импорт настроек. > Откроется окно импорта настроек.



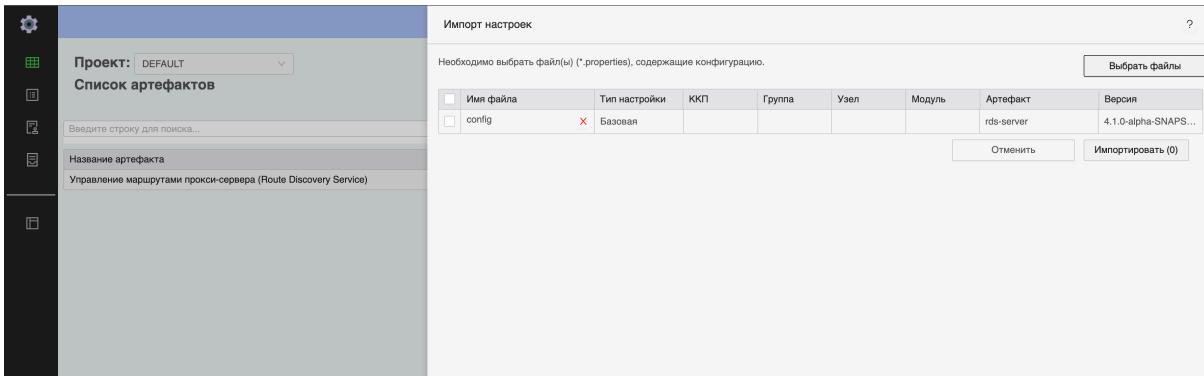
3. Нажать кнопку Выбрать файлы. > Откроется окно выбора файлов для импорта.
4. Выберите файлы *.properties со значениями параметров конфигурации.

Файлы с настройками должны соответствовать требованиям к структуре файла (поля должны соответствовать загруженной ранее схеме артефакта `rds-server`), при этом обязательно наличие следующих разделов:

```
#@artifact=rds-server
#@artifact_version=....
```

При необходимости файлы можно удалить из списка загрузки.

5. Нажать кнопку **Импортировать**. > При успешном импорте окно закроется автоматически. > При возникновении ошибки система выведет на экран соответствующее сообщение.



События системного журнала

Прокси сервер (Nginx)

Состояние сервиса:

```
systemctl status nginx
```

Логи запросов к IAM Proxy

```
/usr/local/openresty/nginx/logs/access.log
```

```
[09/Apr/2020:17:36:03 +0300] 10.x.x.63:36350 -> 10.x.x.178:45406 -> 10.x.x.162:10444 -> - - - "GET /sps-st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788 HTTP/1.1" 302 153 "https://platform-devb.mycompany.ru/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:03 +0300] 10.x.x.63:36350 -> 10.x.x.178:45406 -> 10.x.x.162:10444 -> - - - "GET /openid-connect-auth/redirect_uri?state=901af43b699cc0936418a48ce27c2bec&session_state=89c4632a-6ada-4a3e-9d88-c1e221b28483&code=07e81bac-73d7-482e-be05-68a4f7310e78.89c4632a-6ada-4a3e-9d88-c1e221b28483.e330def0-182f-4d93-8887-97928f014dc4 HTTP/1.1" 302 142 "https://platform-devb.mycompany.ru/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:04 +0300] 10.x.x.63:36350 -> 10.x.x.178:45406 -> 10.x.x.162:10444 -> 10.x.x.149:8443 - sudir-admin "GET /sps-st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788 HTTP/1.1" 200 8357 "https://platform-devb.mycompany.ru/" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 YaBrowser/19.x.x.281
```

```
Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:04 +0300] 10.x.x.63:36350 -> 10.x.x.178:45406 -> 10.x.x.162:10444 ->
10.x.x.149:8443 - sudir-admin "GET /sps-st/sps/ext/resources/css/as.css HTTP/1.1" 200 33128
"https://platform-devb.mycompany.ru/sps-
st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788"
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:04 +0300] 10.x.x.63:36350 -> 10.x.x.178:45406 -> 10.x.x.162:10444 ->
10.x.x.149:8443 - sudir-admin "GET /sps-st/sps/ext/resources/ext-theme-neptune/ext-theme-
neptune-all.css HTTP/1.1" 200 318552 "https://platform-devb.mycompany.ru/sps-
st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788"
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:04 +0300] 10.x.x.63:36362 -> 10.x.x.178:45436 -> 10.x.x.162:10444 ->
10.x.x.149:8443 - sudir-admin "GET /sps-st/sps/ext/App/Api.js HTTP/1.1" 200 3210
"https://platform-devb.mycompany.ru/sps-
st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788"
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
[09/Apr/2020:17:36:04 +0300] 10.x.x.63:36368 -> 10.x.x.178:45448 -> 10.x.x.162:10444 ->
10.x.x.149:8443 - sudir-admin "GET /sps-st/sps/ext/App/ux/UX_DateTimeField.js HTTP/1.1" 200
1367 "https://platform-devb.mycompany.ru/sps-
st/sps/admin/index;jsessionid=7pthWVu2FYn5OxeP3GokVZaSem7ST5bvT4tmvyGW.tkli-ppr2788"
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 YaBrowser/19.x.x.281 Yowser/2.5 Safari/537.36" "-"
```

Логи ошибок и других диагностических сообщений (детализация зависит от уровня логирования в nginx.conf)

/usr/local/openresty/nginx/logs/error.log

```
2020/04/09 17:15:43 [warn] 2090#2090: the "user" directive makes sense only if the master process
runs with super-user privileges, ignored in /usr/local/openresty/nginx/conf/nginx.conf:2
2020/04/09 17:15:47 [warn] 2322#2322: the "user" directive makes sense only if the master process
runs with super-user privileges, ignored in /usr/local/openresty/nginx/conf/nginx.conf.rds:2
2020/04/09 17:15:47 [warn] 2356#2356: the "user" directive makes sense only if the master process
runs with super-user privileges, ignored in /usr/local/openresty/nginx/conf/nginx.conf.rds:2
2020/04/09 17:36:03 [error] 2385#2385: send() failed (111: Connection refused)
2020/04/09 17:36:04 [crit] 2385#2385: *7 SSL_do_handshake() failed (SSL: error:140944E7:SSL
routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client:
10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2385#2385: *9 SSL_do_handshake() failed (SSL: error:140944E7:SSL
routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client:
10.x.x.178, server: 0.0.0.0:10444
```

```
2020/04/09 17:36:04 [crit] 2384#2384: *8 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2385#2385: *10 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2384#2384: *11 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2384#2384: *19 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2385#2385: *18 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2385#2385: *20 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:04 [crit] 2385#2385: *22 SSL_do_handshake() failed (SSL: error:140944E7:SSL routines:ssl3_read_bytes:reason(1255):SSL alert number 255) while SSL handshaking, client: 10.x.x.178, server: 0.0.0.0:10444
2020/04/09 17:36:05 [error] 2385#2385: send() failed (111: Connection refused)
```

Изменение уровня логирования на самый подробный производится опцией в nginx.conf
error_log logs/error.log debug;

Клиент по конфигурированию маршрутов (rds-client)

состояние сервиса:

```
systemctl status rds-client
```

логи работы приложения /usr/local/openresty/nginx/rds-client/logs/log-2020-04-10.log

```
16:35:15.096 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:15.105 INFO | [pool-3-thread-1]: Response received.
16:35:20.097 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:20.116 INFO | [pool-3-thread-1]: Response received.
16:35:25.097 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:25.104 INFO | [pool-3-thread-1]: Response received.
16:35:29.823 INFO | [main]: RDS-client is started
```

```
16:35:30.287 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/last-conf.json
16:35:30.375 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.498 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/index.html
16:35:30.537 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.546 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/sps-st.upstream.conf
16:35:30.550 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.552 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/spsSt.upstream.conf
16:35:30.556 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.558 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/prb-st.upstream.conf
16:35:30.562 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.566 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/prb-st2.upstream.conf
16:35:30.567 INFO | [pool-1-thread-1]: Name for resulting file is empty. Skip.
[/usr/local/openresty/nginx/rds-client/templates/jct.name-upstream.upstream.jinja2 , jct]
16:35:30.571 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.574 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/aud-st.upstream.conf
16:35:30.576 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.578 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/logger-st.upstream.conf
16:35:30.581 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.583 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/rds-for-proxy.upstream.conf
16:35:30.586 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.589 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/jct-snoop.upstream.conf
16:35:30.591 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.595 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/snoop.upstream.conf
```

```
16:35:30.597 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.600 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/stub.upstream.conf
16:35:30.602 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.604 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/test-sutb2.upstream.conf
16:35:30.607 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.613 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/sps-st.server.conf
16:35:30.615 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.618 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/spsSt.server.conf
16:35:30.626 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.628 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/prb-st.server.conf
16:35:30.631 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.634 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/prb-st2.server.conf
16:35:30.641 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.643 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/logger-st.server.conf
16:35:30.648 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.651 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/aud-st.server.conf
16:35:30.653 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.656 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/logger-st.server.conf
16:35:30.659 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.661 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/rds-for-proxy.server.conf
16:35:30.664 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.667 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/jct-snoop.server.conf
```

```
16:35:30.669 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.672 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/snoop.server.conf
16:35:30.674 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.678 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/stub.server.conf
16:35:30.680 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.682 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/results/test-sutb2.server.conf
16:35:30.685 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/context.log
16:35:30.687 INFO | [pool-1-thread-1]: Write to file: /usr/local/openresty/nginx/rds-client/cache/reload-nginx.sh
16:35:30.792 INFO | [pool-1-thread-1]: --- SCRIPT OUTPUT BEGIN ---
16:35:30.793 INFO | [pool-1-thread-1]: nginx: [warn] the "user" directive makes sense only if the master process runs with super-user privileges, ignored in /usr/local/openresty/nginx/conf/nginx.conf.rds:2
16:35:30.793 INFO | [pool-1-thread-1]: OK - Тест новой конфигурации пройден
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/test-sutb2.server.conf -> /usr/local/openresty/nginx/conf/jct/test-sutb2.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/stub.server.conf -> /usr/local/openresty/nginx/conf/jct/stub.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/sps-st.upstream.conf -> /usr/local/openresty/nginx/conf/jct/sps-st.upstream.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/spsSt.upstream.conf -> /usr/local/openresty/nginx/conf/jct/spsSt.upstream.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/logger-st.server.conf -> /usr/local/openresty/nginx/conf/jct/logger-st.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/aud-st.upstream.conf -> /usr/local/openresty/nginx/conf/jct/aud-st.upstream.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/snoop.server.conf -> /usr/local/openresty/nginx/conf/jct/snoop.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/snoop.upstream.conf -> /usr/local/openresty/nginx/conf/jct/snoop.upstream.conf
```

```
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/jct-snoop.server.conf -> /usr/local/openresty/nginx/conf/jct/jct-snoop.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/prb-st2.upstream.conf -> /usr/local/openresty/nginx/conf/jct/prb-st2.upstream.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.793 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/aud-st.server.conf -> /usr/local/openresty/nginx/conf/jct/aud-st.server.conf
16:35:30.793 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/rds-for-proxy.server.conf -> /usr/local/openresty/nginx/conf/jct/rds-for-proxy.server.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/stub.upstream.conf -> /usr/local/openresty/nginx/conf/jct/stub.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/sps-st.server.conf -> /usr/local/openresty/nginx/conf/jct/sps-st.server.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/logger-st.upstream.conf -> /usr/local/openresty/nginx/conf/jct/logger-st.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/jct-snoop.upstream.conf -> /usr/local/openresty/nginx/conf/jct/jct-snoop.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/prb-st.server.conf -> /usr/local/openresty/nginx/conf/jct/prb-st.server.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/prb-st.upstream.conf -> /usr/local/openresty/nginx/conf/jct/prb-st.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/rds-for-proxy.upstream.conf -> /usr/local/openresty/nginx/conf/jct/rds-for-proxy.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/test-sutb2.upstream.conf -> /usr/local/openresty/nginx/conf/jct/test-sutb2.upstream.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/spsSt.server.conf -> /usr/local/openresty/nginx/conf/jct/spsSt.server.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: /usr/local/openresty/nginx/rds-client/results/prb-st2.server.conf -> /usr/local/openresty/nginx/conf/jct/prb-st2.server.conf
16:35:30.794 INFO | [pool-1-thread-1]: ok
16:35:30.794 INFO | [pool-1-thread-1]: '/usr/local/openresty/nginx/rds-client/results/index.html' -
```

```
> '/usr/local/openresty/nginx/conf/../html/index.html'
16:35:30.794 INFO | [pool-1-thread-1]: Успешно запущен reload nginx [31147]
16:35:30.794 INFO | [pool-1-thread-1]: --- SCRIPT OUTPUT END ---
16:35:30.796 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:30.945 INFO | [pool-3-thread-1]: *** SSL *** Force set private key with alias: platform-
devb.mycompany.ru
16:35:31.076 INFO | [pool-3-thread-1]: Response received.
16:35:35.796 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:35.812 INFO | [pool-3-thread-1]: Response received.
16:35:40.797 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:40.812 INFO | [pool-3-thread-1]: Response received.
16:35:45.797 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:45.809 INFO | [pool-3-thread-1]: Response received.
16:35:50.797 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:50.811 INFO | [pool-3-thread-1]: Response received.
16:35:55.797 INFO | [pool-3-thread-1]: Trying to send GET request to https://mycompany-auth-svc-
idp1-dev2.mycompany.ru:7443/rds-for-proxy/active-conf-json
16:35:55.809 INFO | [pool-3-thread-1]: Response received.
```

При использовании nginx как программного балансировщика

Состояние сервиса:

```
systemctl status lb-nginx
```

Расположение логов:

/usr/local/openresty/nginx/lb-logs/access-lb-nginx.log

/usr/local/openresty/nginx/lb-logs/error-lb-nginx.log

Сервер аутентификации (Keycloak)

Состояние сервиса:

```
systemctl status keycloak
```

Логи java

/opt/keycloak-4.8.3.Final/standalone/log/server.log

```
2020-04-09 14:27:23,362 WARN [org.keycloak.events] (default task-2) type=LOGIN_ERROR, realmId=master, clientId=security-admin-console, userId=712a734e-0750-489e-bac4-fda968d43be8, ipAddress=10.x.x.63, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://10.x.x.178:8444/auth/admin/master/console/, code_id=f30ebc76-3f9f-49d4-baff-75dc2ec55939, username=admin
2020-04-09 14:27:23,395 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user 712a734e-0750-489e-bac4-fda968d43be8 from ip 10.x.x.63
2020-04-09 14:27:26,568 WARN [org.keycloak.events] (default task-2) type=LOGIN_ERROR, realmId=master, clientId=security-admin-console, userId=712a734e-0750-489e-bac4-fda968d43be8, ipAddress=10.x.x.63, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://10.x.x.178:8444/auth/admin/master/console/, code_id=f30ebc76-3f9f-49d4-baff-75dc2ec55939, username=admin
2020-04-09 14:27:26,579 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user 712a734e-0750-489e-bac4-fda968d43be8 from ip 10.x.x.63
2020-04-09 14:30:56,725 WARN [org.keycloak.events] (default task-5) type=LOGIN_ERROR, realmId=PlatformAuth, clientId=PlatformAuth-Proxy, userId=a13c334e-b538-4706-80de-6065a68c0edc, ipAddress=10.x.x.180, error=invalid_user_credentials, auth_method=openid-connect, auth_type=code, redirect_uri=https://platform-devb.mycompany.ru/openid-connect-auth/redirect_uri, code_id=89c4632a-6ada-4a3e-9d88-c1e221b28483, username=sudir-admin
2020-04-09 14:30:56,751 WARN [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: login failure for user a13c334e-b538-4706-80de-6065a68c0edc from ip 10.x.x.180
```

Сервер обработки логов (Syslog-NG)

Посмотреть состояние сервиса, команда:

```
systemctl status syslog-ng
```

логи сервиса в /var/log/messages

Логи модуля java

```
/var/log/syslog-ng/java.log
```

```
2020-04-03 01:47:29,387 INFO [root] - sendToAudit: logMessage=org.syslog_ng.LogMessage@41cae424
2020-04-03 01:47:29,390 DEBUG [root] - doAudit r=com.sbt.ppr.platformauth.syslogng.audit2.AuditDestination$$Lambda$58/99663809@11419d1a
2020-04-03 01:47:29,391 DEBUG [root] - sendToAudit: fieldValues={action=[keycloak,authn,oidc]
Аутентификация пользователя, fullhost=mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru, isodate=2020-04-02T22:47:29+00:00, authn.realmId=master, authn.event_type=LOGIN, authn.userId=712a734e-0750-489e-bac4-fda968d43be8, authn.userName=admin, authn.ipAddress=10.x.x.63, authn.oidc.clientId=security-admin-console, authn.oidc.auth_method=openid-connect / code,
```

```
authn.oidc.redirect_uri=https://10.x.x.178:8444/auth/admin/master/console/#/realms/PlatformAuth/identity-provider-settings}
2020-04-03 01:47:29,391 DEBUG [root] - doAudit
r=com.sbt.ppr.platformauth.syslogng.audit2.AuditDestination$$Lambda$52/500746777@20e1d564
2020-04-03 01:47:29,393 DEBUG [root] - doAudit OK,
operation=com.sbt.audit2.OperationHandlerImpl@c77d85
2020-04-03 01:47:29,393 DEBUG [root] - sendToAudit: calling auditUserEvent with
pars=[UserEventParam{name='action', value='[keycloak,authn,oidc] Аутентификация пользователя',
linkedEntityID=null}, UserEventParam{name='fullhost', value='mycompany-auth-svc-idp1-
devb.vm.mos.cloud.mycompany.ru', linkedEntityID=null}, UserEventParam{name='isodate',
value='2020-04-02T22:47:29+00:00', linkedEntityID=null}, UserEventParam{name='authn.realmId',
value='master', linkedEntityID=null}, UserEventParam{name='authn.event_type', value='LOGIN',
linkedEntityID=null}, UserEventParam{name='authn.userId', value='712a734e-0750-489e-bac4-
fda968d43be8', linkedEntityID=null}, UserEventParam{name='authn.userName', value='admin',
linkedEntityID=null}, UserEventParam{name='authn.ipAddress', value='10.x.x.63',
linkedEntityID=null}, UserEventParam{name='authn.oidc.clientId', value='security-admin-console',
linkedEntityID=null}, UserEventParam{name='authn.oidc.auth_method', value='openid-connect /
code', linkedEntityID=null}, UserEventParam{name='authn.oidc.redirect_uri',
value='https://10.x.x.178:8444/auth/admin/master/console/#/realms/PlatformAuth/identity-
provider-settings', linkedEntityID=null}]
2020-04-03 01:47:29,393 DEBUG [root] - sendToAudit: called auditUserEvent, committing
2020-04-03 01:47:29,393 DEBUG [root] - doAudit OK,
operation=com.sbt.audit2.OperationHandlerImpl@c77d85
2020-04-03 01:47:29,393 DEBUG [root] - sendToAudit delay=6.372634ms
2020-04-03 01:47:30,365 INFO [root] - sendToAudit:
logMessage=org.syslog_ng.LogMessage@16ba527d
2020-04-03 01:47:30,365 DEBUG [root] - doAudit
r=com.sbt.ppr.platformauth.syslogng.audit2.AuditDestination$$Lambda$58/99663809@b0ea4fd
2020-04-03 01:47:30,365 DEBUG [root] - sendToAudit: fieldValues={action=[keycloak,authn,oidc]
Аутентификация пользователя, fullhost=mycompany-auth-svc-idp1-devb.vm.mos.mycompany.ru,
isodate=2020-04-02T22:47:30+00:00, authn.realmId=master, authn.event_type=CODE_TO_TOKEN,
authn.userId=712a734e-0750-489e-bac4-fda968d43be8, authn.userName=admin,
authn.ipAddress=10.x.x.63, authn.oidc.clientId=security-admin-console, authn.oidc.auth_method= / ,
authn.oidc.redirect_uri=}
2020-04-03 01:47:30,365 DEBUG [root] - doAudit
r=com.sbt.ppr.platformauth.syslogng.audit2.AuditDestination$$Lambda$52/500746777@256a0a0d
2020-04-03 01:47:30,366 DEBUG [root] - doAudit OK,
operation=com.sbt.audit2.OperationHandlerImpl@1e7a6070
2020-04-03 01:47:30,366 DEBUG [root] - sendToAudit: calling auditUserEvent with
pars=[UserEventParam{name='action', value='[keycloak,authn,oidc] Аутентификация пользователя',
linkedEntityID=null}, UserEventParam{name='fullhost', value='mycompany-auth-svc-idp1-
devb.vm.mos.cloud.mycompany.ru', linkedEntityID=null}, UserEventParam{name='isodate',
value='2020-04-02T22:47:30+00:00', linkedEntityID=null}, UserEventParam{name='authn.realmId',
value='master', linkedEntityID=null}, UserEventParam{name='authn.event_type',
```

```
value='CODE_TO_TOKEN', linkedEntityID=null}, UserEventParam{name='authn.userId',
value='712a734e-0750-489e-bac4-fda968d43be8', linkedEntityID=null},
UserEventParam{name='authn.userName', value='admin', linkedEntityID=null},
UserEventParam{name='authn.ipAddress', value='10.x.x.63', linkedEntityID=null},
UserEventParam{name='authn_oidc.clientId', value='security-admin-console', linkedEntityID=null},
UserEventParam{name='authn_oidc.auth_method', value=' / ', linkedEntityID=null},
UserEventParam{name='authn_oidc.redirect_uri', value='', linkedEntityID=null}]
2020-04-03 01:47:30,366 DEBUG [root] - sendToAudit: called auditUserEvent, committing
2020-04-03 01:47:30,366 DEBUG [root] - doAudit OK,
operation=com.sbt.audit2.OperationHandlerImpl@1e7a6070
2020-04-03 01:47:30,366 DEBUG [root] - sendToAudit delay=1.952938ms
```

Логи принятых сообщений от keycloak

/var/log/syslog-ng/keycloak_logs_tls.log

```
Dec 13 11:41:57 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=LOGIN_ERROR, realmId=PlatformAuth, clientId=PlatformAuth-Proxy, userId=,
ipAddress="10.x.x.180", error=invalid_redirect_uri, redirect_uri="https://10.x.x.59:32826/openid-
connect-auth/redirect_uri"
Dec 13 15:07:58 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=LOGIN, realmId=master, clientId=security-admin-console, userId=712a734e-0750-489e-
bac4-fda968d43be8, ipAddress="10.x.x.60", auth_method=openid-connect, auth_type=code,
redirect_uri="https://10.x.x.178:8444/auth/admin/master/console/", consent=no_consent_required,
code_id=5a3f03bb-d8eb-4280-85bc-ac4ab182f335, username=admin
Dec 13 15:09:27 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=REFRESH_TOKEN, realmId=master, clientId=security-admin-console, userId=712a734e-
0750-489e-bac4-fda968d43be8, ipAddress="10.x.x.60", token_id=1cbe88c9-d34e-4546-ad37-
248334c1c2b2, grant_type=refresh_token, refresh_token_type=Refresh,
updated_refresh_token_id=da2531ff-0631-4175-9258-06f893098cd2, scope="openid profile email",
refresh_token_id=891c6ac6-d238-46d7-b386-e716dfc1a0a6, client_auth_method=client-secret
Dec 13 15:12:36 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=REFRESH_TOKEN, realmId=master, clientId=security-admin-console, userId=712a734e-
0750-489e-bac4-fda968d43be8, ipAddress="10.x.x.60", token_id=25d1f35b-450d-41df-a74d-
e392fbe0b171, grant_type=refresh_token, refresh_token_type=Refresh,
updated_refresh_token_id=4ae520b1-ef77-42a7-b2f3-214210b56ba7, scope="openid profile email",
refresh_token_id=da2531ff-0631-4175-9258-06f893098cd2, client_auth_method=client-secret
Dec 13 15:13:13 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: operationType=UPDATE, realmId=master, clientId=97944ae7-2b78-41c5-91d2-85a8a04bb1b0,
userId=712a734e-0750-489e-bac4-fda968d43be8, ipAddress="10.x.x.60",
resourcePath="clients/e330def0-182f-4d93-8887-97928f014dc4", data="{"id": "e330def0-182f-
4d93-8887-97928f014dc4", "clientId": "PlatformAuth-Proxy", "name": "Platform V (Сервис
автентификации)", "description": "Аутентификация на прокси сервере сервиса аутентификации
платформы", "baseUrl": "https://platform-
```

```

devb.mycompany.ru/",\"surrogateAuthRequired\":false,\"enabled\":true,\"clientAuthenticatorType
\":\"client-secret\",\"redirectUris\":[\"https://platform-
devb.mycompany.ru/*\",\"https://10.x.x.180:10443/*\",\"https://10.x.x.162:10443/*\",\"https://1
0.x.x.59:*\"],\"webOrigins\":[\"+\"]},\"notBefore\":0,\"bearerOnly\":false,\"consentRequired\":false,
\"standardFlowEnabled\":true,\"implicitFlowEnabled\":false,\"directAccessGrantsEnabled\":false,\"s
erviceAccountsEnabled\":false,\"publicClient\":false,\"frontchannelLogout\":false,\"protocol\\"\\"op
enid-
connect\",\"attributes\":{\"saml.assertion.signature\":\"false\",\"saml.force.post.binding\\"\\"false\"
\",\"saml.multivalued.roles\\"\\"false\",\"saml.encrypt\\"\\"false\",\"access.token.signed.response.alg
\\"\\"\",\"saml.server.signature\\"\\"false\",\"saml.server.signature.keyinfo.ext\\"\\"false\",\"exclude.s
ession.state.from.auth.response\\"\\"false\",\"id.token.signed.response.alg\\"\\"\",\"saml_force_name
_id_format\\"\\"false\",\"saml.client.signature\\"\\"false\",\"tls.client.certificate.bound.access.tokens
\\"\\"false\",\"saml.authnstatement\\"\\"false\",\"display.on.consent.screen\\"\\"false\",\"saml.oneti
meuse.condition\\"\\"false\"},\"authenticationFlowBindingOverrides\\"\{}\",\"fullScopeAllowed\\":false,
\"nodeReRegistrationTimeout\\":-1,\"protocolMappers\":[{\\"id\\"\":\"425503f1-a623-4308-b50a-
2cec5694b445\",\"name\\"\":\"Платформа, сервис авторизации (sps)\\",\"protocol\\"\\"openid-
connect\",\"protocolMapper\\"\\"oidc-audience-
mapper\",\"consentRequired\\":false,\"config\\"\":{\\"id.token.claim\\"\\"true\",\"access.token.claim\\"\"
\"false\",\"included.custom.audience\\"\\"PlatformAuthZ\",\"userinfo.token.claim\\"\\"true\"}},{\\"id\"
\\"\":\"29eb2905-b9b8-4f1e-a67a-a51c439e69ee\",\"name\\"\":\"Платформа,
Азимут\",\"protocol\\"\\"openid-connect\",\"protocolMapper\\"\\"oidc-audience-
mapper\",\"consentRequired\\":false,\"config\\"\":{\\"id.token.claim\\"\\"true\",\"access.token.claim\\"\"
\"false\",\"included.custom.audience\\"\\"PlatformAzimuth\",\"userinfo.token.claim\\"\\"true\"}},{\\"id\"
\\"\":\"e12309a3-a723-49a7-a06c-da101d4f88b4\",\"name\\"\":\"Платформа,
BGP\",\"protocol\\"\\"openid-connect\",\"protocolMapper\\"\\"oidc-audience-
mapper\",\"consentRequired\\":false,\"config\\"\":{\\"id.token.claim\\"\\"true\",\"access.token.claim\\"\"
\"false\",\"included.custom.audience\\"\\"PlatformBGP\",\"userinfo.token.claim\\"\\"true\"}},\"defaul
tClientScopes\\"\":[\\"role_list\",\"login\"],\"optionalClientScopes\\"\":[\\"address\",\"phone\",\"roles\",\"l
profile\",\"email\"],\"access\\"\":{\\"view\\"\":true,\"configure\\"\":true,\"manage\\"\":true}}}
Dec 13 15:16:05 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=REFRESH_TOKEN, realmId=master, clientId=security-admin-console, userId=712a734e-
0750-489e-bac4-fda968d43be8, ipAddress="10.x.x.60", token_id=b815c211-7ddb-49e1-9f42-
7f01ef380594, grant_type=refresh_token, refresh_token_type=Refresh,
updated_refresh_token_id=2a098ba7-905f-43d9-9f31-465f27fd8970, scope="openid profile email",
refresh_token_id=4ae520b1-ef77-42a7-b2f3-214210b56ba7, client_auth_method=client-secret
Dec 13 15:18:55 mycompany-auth-svc-idp1-devb.vm.mos.cloud.mycompany.ru send-events-to-
syslog: type=LOGIN, realmId=PlatformAuth, clientId=PlatformAuth-Proxy, userId=eeaac123-b027-
4cb9-af14-cb86363ed921, ipAddress="10.x.x.180", auth_method=openid-connect, auth_type=code,
redirect_uri="https://10.x.x.59:32826/openid-connect-auth/redirect_uri",
consent=no_consent_required, code_id=e66694ac-7a10-4866-bf16-0b88ad5c74f8, username=test_user

```

Логи принятых сообщений от nginx

/var/log/syslog-ng/nginx_logs.log

Apr 3 03:12:22 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /openid-connect-auth/redirect_uri?state=2b39050bb5e25eb2a00ee177e2784e35&session_state=5389fb52-917d-4fef-9ffc-75de77d7c805&code=be0a89c7-fb9f-4506-b4a2-5516be0165f1.5389fb52-917d-4fef-9ffc-75de77d7c805.e330def0-182f-4d93-8887-97928f014dc4 HTTP/1.1" TS:2020-04-03T03:12:22+03:00 M:GET URL:"/openid-connect-auth/redirect_uri?state=2b39050bb5e25eb2a00ee177e2784e35&session_state=5389fb52-917d-4fef-9ffc-75de77d7c805&code=be0a89c7-fb9f-4506-b4a2-5516be0165f1.5389fb52-917d-4fef-9ffc-75de77d7c805.e330def0-182f-4d93-8887-97928f014dc4" CA:10.x.x.178[10.x.x.63] F:0.078 ST:302 B:142 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:- T:87f28b015aaa9f0ea953d1ba5d9f3b42 Apr 3 03:12:22 mycompany-auth-svc-proxy1-devb nginx: BR:"GET / HTTP/1.1" TS:2020-04-03T03:12:22+03:00 M:GET URL:"/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:200 B:12336 CTRESP:"text/html; charset=utf-8" SI:001b5df6de8c4bcfaa9d02d1dba01e72 SU:admin LA:10.x.x.162 JN: S:- T:5ce4caf9f943d8ffa66623d94547a04 Apr 3 03:12:30 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /jwt/ HTTP/1.1" TS:2020-04-03T03:12:30+03:00 M:GET URL:"/jwt/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:200 B:6771 CTRESP:"text/html" SI:001b5df6de8c4bcfaa9d02d1dba01e72 SU:admin LA:10.x.x.162 JN: S:- T:201d2b6039b159003d5d1e6d87cb49bc Apr 3 03:20:24 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /openid-connect-auth/logout HTTP/1.1" TS:2020-04-03T03:20:24+03:00 M:GET URL:"/openid-connect-auth/logout" CA:10.x.x.178[10.x.x.63] F:0.000 ST:302 B:142 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:- T:b56fb7dce5807f4b1feb3175990bb3d8 Apr 3 03:20:25 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /openid-connect-auth/logoutSuccessful.html HTTP/1.1" TS:2020-04-03T03:20:25+03:00 M:GET URL:"/openid-connect-auth/logoutSuccessful.html" CA:10.x.x.178[10.x.x.63] F:0.000 ST:200 B:510 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:- T:e3246061ca14f1b25da15652bf43a7d6 Apr 3 03:20:29 mycompany-auth-svc-proxy1-devb nginx: BR:"GET / HTTP/1.1" TS:2020-04-03T03:20:29+03:00 M:GET URL:"/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:302 B:142 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:- T:a18e7c2881d65928053d5d01d79f68e2 Apr 3 03:20:46 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /openid-connect-auth/redirect_uri?state=77f388928a7d5be3284b653d8d14bc6e&session_state=d1ac9d67-1b00-4386-9b2e-f2d862700dc2&code=f5ed3d18-bfe4-40fe-bf19-05a3abe586b6.d1ac9d67-1b00-4386-9b2e-f2d862700dc2.e330def0-182f-4d93-8887-97928f014dc4 HTTP/1.1" TS:2020-04-03T03:20:46+03:00 M:GET URL:"/openid-connect-auth/redirect_uri?state=77f388928a7d5be3284b653d8d14bc6e&session_state=d1ac9d67-1b00-4386-9b2e-f2d862700dc2&code=f5ed3d18-bfe4-40fe-bf19-05a3abe586b6.d1ac9d67-1b00-4386-9b2e-f2d862700dc2.e330def0-182f-4d93-8887-97928f014dc4" CA:10.x.x.178[10.x.x.63] F:0.059 ST:302 B:142 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:- T:305e43d6582f9e47794bb15e610042e5 Apr 3 03:20:46 mycompany-auth-svc-proxy1-devb nginx: BR:"GET / HTTP/1.1" TS:2020-04-03T03:20:46+03:00 M:GET URL:"/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:200 B:12336 CTRESP:"text/html; charset=utf-8" SI:2295f5938fea1f4bdfd8fa8d910aecb9 SU:admin LA:10.x.x.162 JN: S:- T:ece0ff5632c2402a532e96fc4cae345a Apr 3 03:20:49 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /jwt/ HTTP/1.1" TS:2020-04-03T03:20:49+03:00 M:GET URL:"/jwt/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:200 B:6771

```
CTRESP:"text/html" SI:2295f5938fea1f4bdfd8fa8d910aecb9 SU:admin LA:10.x.x.162 JN: S:-  
T:636548d2dfc8e30178e7024ec761c5c9  
Apr 3 03:25:30 mycompany-auth-svc-proxy1-devb nginx: BR:"GET /openid-connect-auth/logout  
HTTP/1.1" TS:2020-04-03T03:25:30+03:00 M:GET URL:"/openid-connect-auth/logout"  
CA:10.x.x.178[10.x.x.63] F:0.000 ST:302 B:142 CTRESP:"text/html" SI:- SU:- LA:10.x.x.162 JN: S:-  
T:6af6beffc9b3e950452d31874f42b954  
Apr 3 03:25:59 mycompany-auth-svc-proxy1-devb nginx: BR:"GET / HTTP/1.1" TS:2020-04-  
03T03:25:59+03:00 M:GET URL:"/" CA:10.x.x.178[10.x.x.63] F:0.000 ST:302 B:142 CTRESP:"text/html"  
SI:- SU:- LA:10.x.x.162 JN: S:- T:dc478f3d488cd2749298bcc452b66f24
```

Уровни логирования

Можно настроить следующие уровни логирования: `warn`, `debug`. По умолчанию используется уровень логирования `warn`. Уровень логирования `debug` включается в профиле развертывания посредством переключения параметра `debug` в файле `proxy.yml`. Использование уровня логирования `debug` в штатном режиме не рекомендуется из-за больших ресурсозатрат и падения производительности.

Примечание

При установке на ПРОМ среду(тип стенда `prom`), средствами Platform V DevOps Tools (CDJE), возможность задания уровня логирования в `debug` отсутствует (отключено по соображениям безопасности).

События мониторинга

Сервис аутентификации не оперирует бизнес-операциями, но позволяет следить за метриками в формате Prometheus.

Предусловия

Для получения метрик в формате Prometheus необходимо настроить параметр `PROXY_METRICS_ENABLE` в значение `True` (подробнее в разделе Параметры основной функциональности компонента IAM Proxy) . Метрики публикуются на отдельном порту в открытом виде, для просмотра метрик ролевая модель не применяется. Метрики в формате Prometheus доступны в браузере по адресу `http://<host>:10080/metrics/` (подробнее в разделе Параметры основной функциональности компонента IAM Proxy) .

Проверка доступности метрик

Для проверки доступности метрик на виртуальной машине необходимо:

1. Открыть ssh-терминал VM по адресу папки (адрес задается на этапе развертывания, подробнее в разделе Установка), где установлен IAM Proxy.
2. Выполнить запрос: `curl http://<host>:10080/metrics/`.

3. Убедиться, что метрики отдаются в ответе в формате Prometheus (смотрите пример ниже).

Пример выполнения запроса curl http://<host>:10080/metrics/ (пояснения к представленным в примере метрикам, приведены в подразделе “Выводимые метрики и их описание”):

```
## HELP auth_counters Счетчик запросов аутентификации и авторизации
## TYPE auth_counters counter
auth_counters{state="error_302"} 3
auth_counters{state="oidc_authenticated"} 1
auth_counters{state="oidc_created"} 2
auth_counters{state="success"} 2
## HELP http_connections Число HTTP соединений в настоящий момент
## TYPE http_connections gauge
http_connections{state="active"} 4
http_connections{state="reading"} 0
http_connections{state="waiting"} 2
http_connections{state="writing"} 2
## HELP http_durations Backend, гистограмма времени обработки HTTP запросов разрезе
upstream+upstream_server (в секундах)
## TYPE http_durations histogram
http_durations_bucket{upstream="",upstream_addr="",le="0.005"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.01"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.02"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.03"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.05"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.075"} 4
http_durations_bucket{upstream="",upstream_addr="",le="0.1"} 4
http_durations_bucket{upstream="",upstream_addr="",le="0.2"} 5
http_durations_bucket{upstream="",upstream_addr="",le="0.3"} 6
http_durations_bucket{upstream="",upstream_addr="",le="0.4"} 6
http_durations_bucket{upstream="",upstream_addr="",le="0.5"} 6
http_durations_bucket{upstream="",upstream_addr="",le="0.75"} 6
http_durations_bucket{upstream="",upstream_addr="",le="1"} 6
http_durations_bucket{upstream="",upstream_addr="",le="1.5"} 6
http_durations_bucket{upstream="",upstream_addr="",le="2"} 6
http_durations_bucket{upstream="",upstream_addr="",le="3"} 6
http_durations_bucket{upstream="",upstream_addr="",le="4"} 6
http_durations_bucket{upstream="",upstream_addr="",le="5"} 6
http_durations_bucket{upstream="",upstream_addr="",le="10"} 6
http_durations_bucket{upstream="",upstream_addr="",le="+Inf"} 6
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.005"} 2
```

```

http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.01"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.02"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.03"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.05"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.075"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.1"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.2"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.3"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.4"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.75"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="1"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="1.5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="2"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="3"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="4"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="10"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="+Inf"} 2
http_durations_count{upstream="",upstream_addr=""} 6
http_durations_count{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080"} 2
http_durations_sum{upstream="",upstream_addr=""} 0.426
http_durations_sum{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080"} 0.005
## HELP http_requests_backend Backend, счетчик HTTP запросов в разрезе
host+upstream+upstream_server+код_ответа
## TYPE http_requests_backend counter
http_requests_backend{host="platform-ift2.sc.dev.mycompany",upstream="",upstream_addr:"",status="200"} 3
http_requests_backend{host="platform-ift2.sc.dev.mycompany",upstream="",upstream_addr:"",status="302"} 3
http_requests_backend{host="platform-"

```

```
ift2.sc.dev.mycompany",upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",status="200"} 2
## HELP http_requests Frontend, счетчик HTTP запросов в разрезе host+ответвление+код_ответа
## TYPE http_requests counter
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="",status="200"} 3
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="",status="302"} 1
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="/metrics",status="200"} 2
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="/metrics",status="302"} 2
http_requests{host="platformauth-ift2.sc.dev.mycompany",jctroot="",status="200"} 4
## HELP nginx_metric_errors_total Number of nginx-lua-prometheus errors
## TYPE nginx_metric_errors_total counter
nginx_metric_errors_total 0
```

Для проверки доступности метрик в OpenShift необходимо:

1. Открыть терминал контейнера `iamproxy` в pod IAM Proxy, заданным на этапе развертывания.
2. Выполнить запрос: `curl http://<host>:10080/metrics/`.
3. Убедиться что метрики отдаются в ответе в формате Prometheus

Пример выполнения запроса `curl http://<host>:10080/metrics/` (пояснения к представленным в примере метрикам, приведены в подразделе “Выводимые метрики и их описание”):

```
## HELP auth_counters Счетчик запросов аутентификации и авторизации
## TYPE auth_counters counter
auth_counters{state="error_302"} 3
auth_counters{state="oidc_authenticated"} 1
auth_counters{state="oidc_created"} 2
auth_counters{state="success"} 2
## HELP http_connections Число HTTP соединений в настоящий момент
## TYPE http_connections gauge
http_connections{state="active"} 4
http_connections{state="reading"} 0
http_connections{state="waiting"} 2
http_connections{state="writing"} 2
## HELP http_durations Backend, гистограмма времени обработки HTTP запросов разрезе
upstream+upstream_server (в секундах)
## TYPE http_durations histogram
http_durations_bucket{upstream="",upstream_addr="",le="0.005"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.01"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.02"} 3
http_durations_bucket{upstream="",upstream_addr="",le="0.03"} 3
```

```
http_durations_bucket{upstream="",upstream_addr:"",le="0.05"} 3
http_durations_bucket{upstream="",upstream_addr:"",le="0.075"} 4
http_durations_bucket{upstream="",upstream_addr:"",le="0.1"} 4
http_durations_bucket{upstream="",upstream_addr:"",le="0.2"} 5
http_durations_bucket{upstream="",upstream_addr:"",le="0.3"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="0.4"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="0.5"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="0.75"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="1"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="1.5"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="2"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="3"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="4"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="5"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="10"} 6
http_durations_bucket{upstream="",upstream_addr:"",le="+Inf"} 6
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.005"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.01"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.02"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.03"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.05"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.075"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.1"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.2"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.3"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.4"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="0.75"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="1"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="1.5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="2"} 2
```

```

http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="3"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="4"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="5"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="10"} 2
http_durations_bucket{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",le="+Inf"} 2
http_durations_count{upstream="",upstream_addr=""} 6
http_durations_count{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080"} 2
http_durations_sum{upstream="",upstream_addr=""} 0.426
http_durations_sum{upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080"} 0.005
## HELP http_requests_backend Backend, счетчик HTTP запросов в разрезе
host+upstream+upstream_server+код_ответа
## TYPE http_requests_backend counter
http_requests_backend{host="platform-
ift2.sc.dev.mycompany",upstream="",upstream_addr="",status="200"} 3
http_requests_backend{host="platform-
ift2.sc.dev.mycompany",upstream="",upstream_addr="",status="302"} 3
http_requests_backend{host="platform-
ift2.sc.dev.mycompany",upstream="backend_jct_metrics",upstream_addr="127.0.0.1:10080",status=
"200"} 2
## HELP http_requests Frontend, счетчик HTTP запросов в разрезе host+ответвление+код_ответа
## TYPE http_requests counter
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="",status="200"} 3
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="",status="302"} 1
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="/metrics",status="200"} 2
http_requests{host="platform-ift2.sc.dev.mycompany",jctroot="/metrics",status="302"} 2
http_requests{host="platformauth-ift2.sc.dev.mycompany",jctroot="",status="200"} 4
## HELP nginx_metric_errors_total Number of nginx-lua-prometheus errors
## TYPE nginx_metric_errors_total counter
nginx_metric_errors_total 0

```

Выводимые метрики и их описание

Метрики событий аутентификации

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Аутентификация	После выполнения операции	auth_counters	Счетчик	Количество событий “получения ошибок с кодом XXX”	{state=“error_302”} 5
Аутентификация	После выполнения операции	auth_counters	Счетчик	Количество событий “успешной аутентификации”	{state=“oidc_authenticate_d”} 2

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Аутентификация	После выполнения операции	auth_counters	Счетчик	Количество событий “создания сессии”	{state=“oidc_created”} 3
Аутентификация	После выполнения операции	auth_counters	Счетчик	Количество событий “обновления токена”	{state=“oidc_regeneration”} 4
Проксирование и аутентификация	После выполнения операции	auth_counters	Счетчик	Количество событий “обращение аутентифицированного пользователя”	{state=“success”} 1705

Метрики событий подключений

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Проксирование и аутентификация	При выполнении запроса	http_connections	Счетчик	Количество активных подключений	{state=“active”} 1
Проксирование и аутентификация	При выполнении запроса	http_connections	Счетчик	Количество подключений чтения	{state=“reading”} 0
Проксирование и аутентификация	При выполнении запроса	http_connections	Счетчик	Количество подключений ожидания	{state=“waiting”} 0
Проксирование и аутентификация	При выполнении запроса	http_connections	Счетчик	Количество подключений записи	{state=“writing”} 1

Гистограмма времени обработки HTTP запросов разрезе upstream+upstream_server (в секундах)

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Проксирование	После выполнения операции	http_durations_bucket	Счетчик	Заполнение bucket upstream ответвления	{upstream=“backend_jct_распределение”, upstream_addr=“10.x.x.102:80”, le=“4”} 45

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Проксирование	После выполнения операции	http_durations_count	Счетчик	Количество обращений в пространстве	{upstream="backend_jct_nexus",upstream_addr="10.x.x.136:443"} 819
Проксирование	После выполнения операции	http_durations_sum	Счетчик	Сумма обращений в пространстве	{upstream="backend_jct_nexus",upstream_addr="10.x.x.15:443"} 12.639

Счетчик HTTP запросов в разрезе host+upstream+upstream_server+код_ответа

Наименование операции	Частота сбора метрик	Название метрики	Тип метрик и	Описание метрики	Описание результатов выполнения операций
Проксирование	После выполнения операции	http_requests_backend	Счетчик	Количество обращений к backend	{host="platform-devb.mycompany.ru",upstream="backend_jct_nexus",upstream_addr="10.x.x.15:443",status="202"} 1

Счетчик HTTP запросов в разрезе host+ответвление+код_ответа

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Проксирование	После выполнения операции	http_requests	Счетчик	Количество обращений к ответвлению	{host="platform-devb.mycompany.ru",jctroot="/nexus",status="204"} 945

Метрики ядра Nginx

Наименование операции	Частота сбора метрик	Название метрики	Тип метрики	Описание метрики	Описание результатов выполнения операций
Проксирование	При возникновении	nginx_metric_errors_total	Счетчик	Количество ошибок Nginx	0

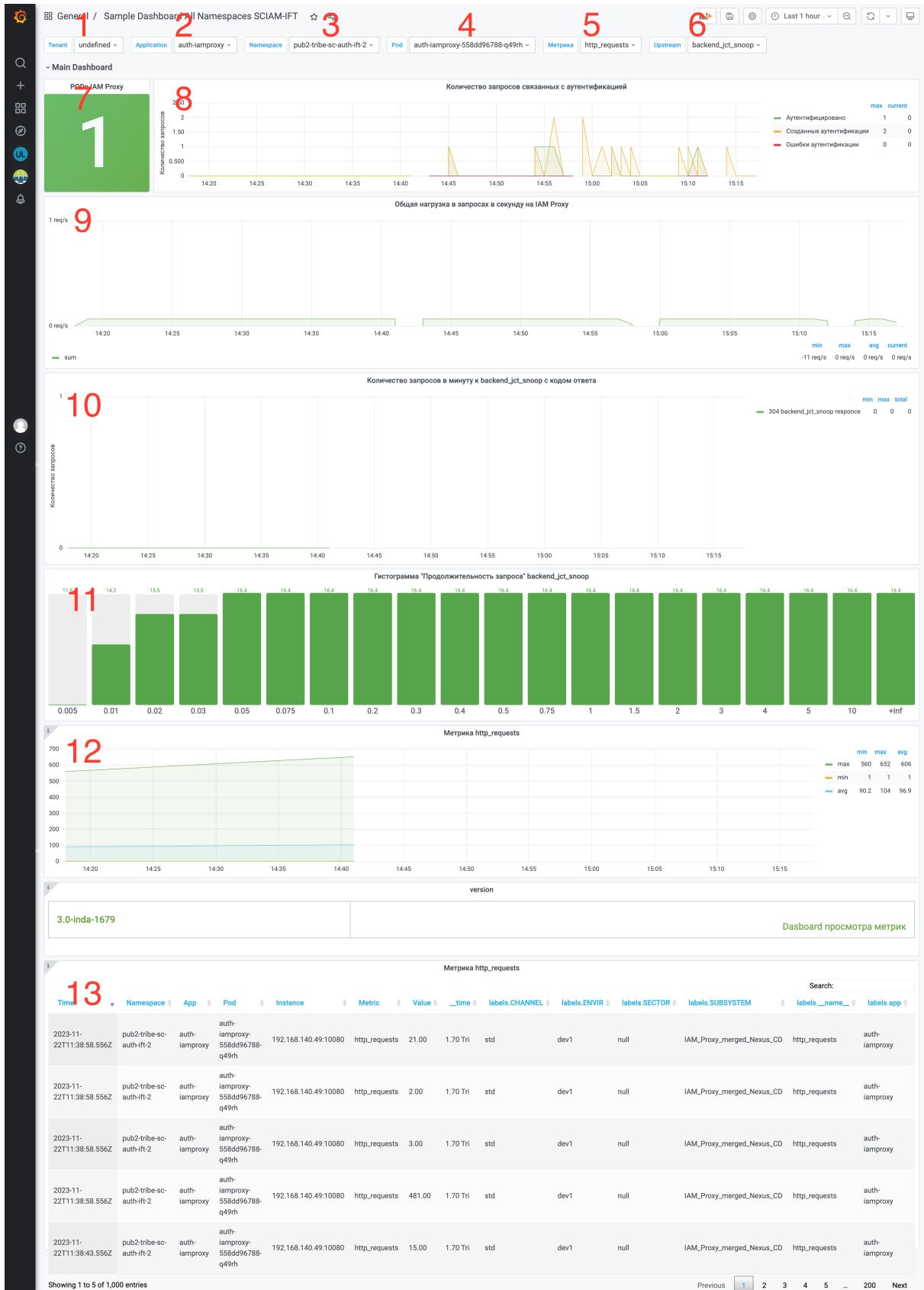
Стандартный дашборд IAM Proxy

В состав дистрибутива входит Дашборд, который позволяет осуществлять мониторинг ключевых точек отказа IAM Proxy и сервисов защиты которых он осуществляет. Дашборд представляет из себя файл в формате json для импорта в Platform V Monitor, который

располагается в дистрибутиве с бинарными артефактами -
package/deploy/monitoring/pvm-dashboard-for-iamproxy-v1.json

После успешного импорта в интерфейс Platform V Monitor для просмотра будет предоставлено несколько панелей:

Руководство по эксплуатации компонента IAM Proxy (AUTH)



1. Кнопка выбора Теннанта - этот параметр определяется в параметрах установки MONA для CDJE в файле `ort_unimon.unimon-agent.conf`;
2. Кнопка выбора приложения, определяется лейблом app сервиса из которого извлекаются метрики при помощи unimon-agent ;
3. Кнопка выбора namespace в которое установлено приложение;
4. Кнопка выбора POD;
5. Кнопка выбора метрики, которую отдает приложение;
6. Кнопка выбора проксируемого приложения;
7. Панель отображения количества запущенных POD IAM Proxy;
8. Панель, отображающая количество Аутентификаций на IAM Proxy (успешные аутентификации, созданные аутентификации и ошибки аутентификации);
9. Панель отображающая нагрузку на Proxy в запросах в секунду;
10. Панель отображающая количество запросов к проксируемому сервису в минуту, с кодом ответа полученным от этого сервиса, выбрать сервис для отображения можно при помощи кнопки 6;
11. Гистограмма отражающая статистику по скорости выполнения запроса к проксируемому сервису в секундах. Значение снизу отражает время выполнения запроса к сервису, верхнее количество запросов которое попало в промежуток равный или ниже времени обозначенном на шкале внизу;
12. Информационная панель, которая показывает графическое значение выбранной метрики по кнопке 5;
13. Информационная панель, которая показывает общую сводку по выбранной, кнопкой 5, метрике, в виде таблицы.

Часто встречающиеся проблемы и пути их устранения

Проблема	Причины возникновения проблем	Пути устранения
Не получается посмотреть конфигурацию	1. У пользователя нет прав для просмотра конфигурации	1. В удаленном компоненте авторизации проверить импортированную ролевую модель Пользователя. 2. Сверить список привилегий, выданных пользователю со списком основных групп пользователей, описанных в разделе «Ролевая модель» руководства по безопасности компонента PACMAN (CFGА)

Проблема	Причины возникновения проблем	Пути устранения
Не загружается модель артефактов	1. Загруженный файл с моделью не прошел валидацию. 2. Версия артефакта уже существует	1. Провалидировать файл модели на наличие ошибок. 2. Удалить существующий артефакт, либо изменить версию артефакта в модели
Не загружаются настройки из файла	1. Загруженный файл .properties не прошел валидацию	1. Проверить файл .properties на наличие ошибок
Не подтверждается запрос на изменение	1. Пользователь является автором запроса. 2. У пользователя нет привилегии на изменение настроек данного артефакта. 3. При подтверждении запроса заполнены не все обязательные поля	1. Обратитесь к другому администратору, имеющему права на работу с данным артефактом (в целях безопасности, отключена возможность подтверждать свои собственные запросы). 2. Обратитесь к администратору, имеющему привилегии. Если в удаленный компонент авторизации была импортирована некорректная ролевая модель для текущего пользователя и текущий пользователь должен иметь возможность редактировать настройки артефакта, то необходимо проверить ролевую модель в удаленном компоненте авторизации и при необходимости добавить недостающие привилегии Configurator.ArtifactManager.Edit , Configurator.ArtifactManager.Edit.All . 3. Заполнить все обязательные поля

Работы по восстановлению

В случае сбоев проанализируйте логи на наличие ошибок

Прокси сервер (Nginx)

Состояние сервиса:

```
systemctl status nginx
```

/usr/local/openresty/nginx/logs/access.log

/usr/local/openresty/nginx/logs/error.log

При использовании nginx как программного балансировщика

/usr/local/openresty/nginx/lb-logs/access-lb-nginx.log

/usr/local/openresty/nginx/lb-logs/error-lb-nginx.log

Клиент по конфигурированию маршрутов (rds-client)

/usr/local/openresty/nginx/rds-client/logs/log-*.*.log

Сервер обработки логов (Syslog-NG)

/var/log/messages

/var/log/syslog-ng/java.log

Проверить наличие свободных ресурсов на проблемных серверах (disk/cpri/mem)

Наличие свободных системных ресурсов должно отслеживаться в рамках используемых систем мониторинга.

Вручную сделать это можно так - зайти под системной учетной записью на сервера по SSH, и убедиться, что ресурсы disk/cpri/mem не исчерпаны.

Проверить свободное место на диске, команда: `df -h`

Проверить свободную память, команда: `vmstat -s`

Проверить загрузку сри, команда: `top`

Перезапустить сервисы

Для перезапуска используются команды из ssh-консоли:

`sudo systemctl restart nginx`

`sudo systemctl restart lb-nginx`

`sudo systemctl restart rds-client`

`sudo systemctl restart keycloak`

`sudo systemctl restart syslog-ng`

Предоставление доступа к логам

Чтобы иметь возможность просмотра логов/конфигурационных файлов без использования sudo, нужно дать доступ для рабочей системной непривилегированной учетной записи linux (например ivanov-ii). Для этого на серверах необходимо включить непривилегированную учетную запись в группы сервисов.

Сделать это можно под root-ом такой командой (пример для логина ivanov-ii):

```
usermod ivanov-ii -a -G nginx
```

группа keycloak

```
usermod ivanov-ii -a -G keycloak
```

группа nginx (сервисы nginx, lb-nginx, rds-client)

```
usermod ivanov-ii -a -G nginx
```

```
группа syslog-ng
usermod ivanov-ii -a -G syslog-ng
```

После этого директории, журналы и большинство файлов, потенциально не содержащих секреты, станут доступны под учетной записью ivanov-ii .

Также будут права на перезапуск служб ТС, для членов групп сервисов (т.е. под ivanov-ii можно, например будет сделать перезапуск nginx - sudo systemctl restart nginx).

*Identity provider - СУДИР

Руководство прикладного разработчика компонента IAM Proxy (AUTH)

Системные требования

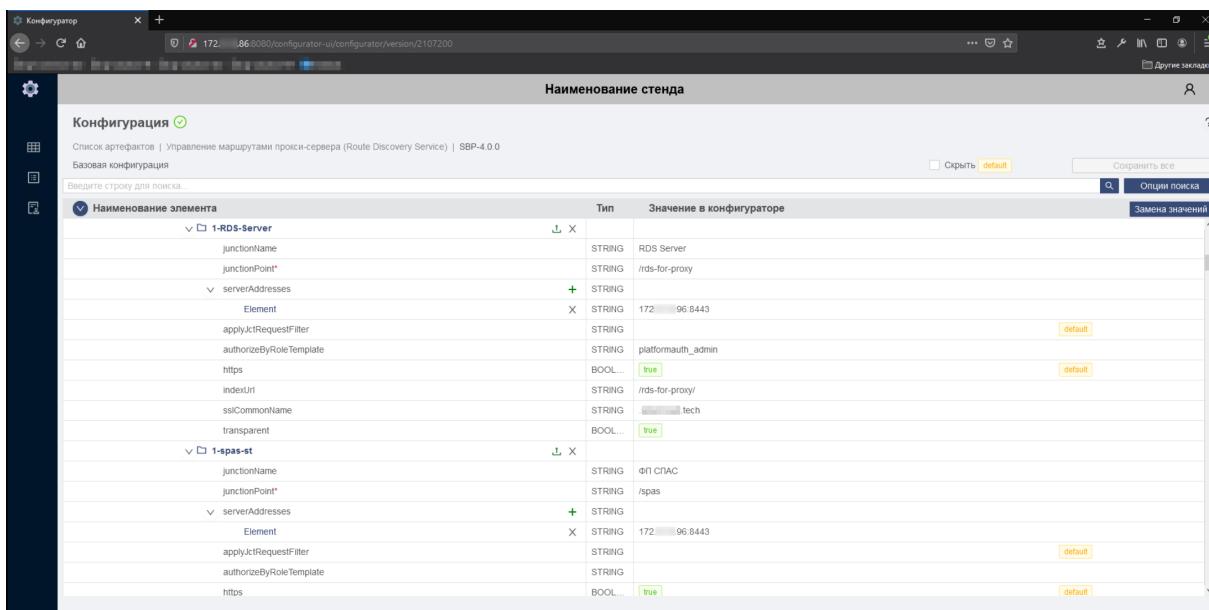
Системные требования приведены в документе *Руководство по установке* в разделе Системные требования.

Подключение и конфигурирование

Настройка интеграции с Platform V IAM с использованием проксирования

При интеграции с использованием прокси сервера, клиентская часть аутентификации по Open ID Connect (Relay Party) выполняется на стороне прокси Platform V IAM.

Для осуществления проксирования на конкретное приложение/backend, необходимо на новом или уже существующем прокси сервиса аутентификации добавить “ответвление”. Делается это в компоненте PACMAN (CFGА), администраторами сервисов платформы.



При добавлении указывается базовый контекст (по которому определяется на какой backend будет осуществляться проксирование), необходимость вставки в URL базового контекста, адреса и порты серверов приложений, и др.

После применения изменений в компоненте PACMAN (CFGА) (нажатие кнопки с зеленым треугольником в круге), в течение ~5 секунд, изменения должны попасть на прокси-сервера.

При первом переходе из браузера на прокси, будет запрошена аутентификация у пользователя, и только после успешной аутентификации будет осуществляться проксирование на сервера приложений.

После проксирования ко всем запросам в backend добавляются http-заголовки:

iv-user - логин пользователя (обратная совместимость с **webseal**);

iv-groups - группы пользователя (обратная совместимость с **webseal**);

Auth-Svc-User - логин пользователя;

Authorization - аутентификационный токен OIDC (**id_token**) в формате **Authorization: Bearer id_token**.

Если Сервер приложений (СП) использует для авторизации Объединенный сервис авторизации (ОСА), то необходимо на СП брать из http-заголовка полученный от прокси **jtw-token** (**id_token** или **access_token**) и использовать его при вызове методов Объединенного сервиса авторизации (ОСА) (при получении **ticket**). Объединенный сервис авторизации (ОСА) умеет самостоятельно валидировать токен от Platform V IAM, и на основе него будет определен пользователь приложения при выдаче авторизационного решения. Так же Объединенный сервис авторизации (ОСА) имеет методы возврата различной информации о пользователе, такой как логин, ФИО, табельный номер, код подразделения и т.п.

В тестовых целях, на стендах тестирования, текущий **id_token**/**access_token**/**refresh_token** можно посмотреть на endpoint **/jwt/** прокси (доступен только на стенах тестирования).

Пример url - <https://mycompany-auth-svc-proxy-dev2.mycompany.ru/jwt/>

Настройка интеграции с сервисом аутентификации без использования проксирования

Описание

Для использования сервиса аутентификации, система должна иметь поддержку клиентской части аутентификации по стандарту Open Id Connect v1 (Relay Party), с использованием **code-flow**.

Для наиболее распространенных платформ есть готовые реализации open-source адаптеров от Keycloak.SE.

WILDFLY_HOME - ниже данное значение замените на каталог в который установлен WildFly

Системные требования

WildFly Application Server 10 или выше. Java 8.0 (Java SDK 1.8) or later and Maven 3.1.1 or later.

Настройка на WildFly

На WildFly необходимо распаковать архив с адаптером `keycloak-wildfly-adapter-${project.version}.zip` в `WILDFLY_HOME`. Используем файл Server Keycloak версии 4.3.8.

Установка на WildFly 9 или новее

Предварительно необходимо остановить сервер WildFly.

```
$ cd $WILDFLY_HOME $ unzip keycloak-wildfly-adapter-dist-4.8.3.Final.zip
```

Установить адаптер keycloak на WildFly, для использования аутентификации по Open Id Connect

WildFly 10 или старше

```
$ ./bin/jboss-cli.sh --file=bin/adapter-install-offline.cli
```

WildFly 11 или новее

```
$ ./bin/jboss-cli.sh --file=bin/adapter-elytron-install-offline.cli
```

Настройка. Метод 1

Настройка приложения

Создать файл конфигурации адаптера `WEB-INF/keycloak.json` в вашем веб-приложении (WAR). Актуальный формат файла можно посмотреть на сайте Keycloak.SE в разделе документация.

Пример `keycloak.json`: `WEB-INF/keycloak.json`

```
{  
    "realm": "PlatformAuth",  
    "auth-server-url": "https://platform-devb:8443/auth",  
    "ssl-required": "external",  
    "resource": "app-jsp",  
    "credentials": {  
        "secret": "5bad43ac-0dac-4272-a723-ab7a3cef49b9"  
    }  
}
```

Установить auth-method = KEYCLOAK в файле web.xml . Пример: WEB-INF/web.xml

```
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd"
  version="3.0">

  <module-name>application</module-name>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Admins</web-resource-name>
      <url-pattern>/admin/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>admin</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Customers</web-resource-name>
      <url-pattern>/customers/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>user</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>

  <login-config>
    <auth-method>KEYCLOAK</auth-method>
    <realm-name>this is ignored currently</realm-name>
  </login-config>

  <security-role>
    <role-name>admin</role-name>
  </security-role>
  <security-role>
```

```
<role-name>user</role-name>
</security-role>
</web-app>
```

Настройка. Метод 2

Настройка аутентификации на WildFly без изменения WAR (использование Adapter Subsystem).

В standalone.xml добавляются разделы: standalone.xml

```
<extensions>
<extension module="org.keycloak.keycloak-adapter-subsystem"/>
</extensions>

<profile>
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
<realm name="PlatformAuth">
<auth-server-url>https://platform-devb:8443/auth</auth-server-url>
<ssl-required>external</ssl-required>
</realm>
<secure-deployment name="WAR MODULE NAME.war">
<realm>PlatformAuth</realm>
<resource>customer-portal</resource>
<credential name="secret">password</credential>
</secure-deployment>
<secure-deployment name="customer-portal.war">
<realm>PlatformAuth</realm>
<resource>customer-portal</resource>
<credential name="secret">password</credential>
</secure-deployment>
<secure-deployment name="product-portal.war">
<realm>PlatformAuth</realm>
<resource>product-portal</resource>
<credential name="secret">password</credential>
</secure-deployment>

</subsystem>
</profile>
```

Использование в EJB

Чтобы распространить контекст безопасности на уровень EJB, требуется настроить его на использование домена безопасности KeyCloak.SE:

```
import org.jboss.ejb3.annotation.SecurityDomain;  
...  
  
@Stateless  
@SecurityDomain("keycloak")  
public class CustomerService {  
  
    @RolesAllowed("user")  
    public List<String> getCustomers() {  
        return db.getCustomers();  
    }  
}
```

Использование в Spring Boot

Чтобы использовать Keycloak Spring Boot starter необходимо добавить зависимость: pom.xml

```
<dependency>  
    <groupId>org.keycloak</groupId>  
    <artifactId>keycloak-spring-boot-starter</artifactId>  
</dependency>
```

Добавить зависимость Keycloak Adapter BOM: pom.xml

```
<dependencyManagement>  
    <dependencies>  
        <dependency>  
            <groupId>org.keycloak.bom</groupId>  
            <artifactId>keycloak-adapter-bom</artifactId>  
            <version>4.8.3.Final</version>  
            <type>pom</type>  
            <scope>import</scope>  
        </dependency>  
    </dependencies>  
</dependencyManagement>
```

Spring Boot Adapter Configuration

В файле application.properties указать настройки адаптера. Актуальные настройки можно посмотреть на сайте Keycloak. SE в разделе документация: application.properties

```
keycloak.realm = PlatformAuth  
keycloak.auth-server-url = https://platform-devb:8443/auth  
keycloak.ssl-required = external
```

```
keycloak.resource = demoapp
keycloak.credentials.secret = 11111111-1111-1111-1111-111111111111
keycloak.use-resource-role-mappings = true
```

Spring Boot Adapter установит login-method в KEYCLOAK и настроит security-constraints при запуске. Пример конфигурации security-constraints : application.properties

```
keycloak.securityConstraints[0].authRoles[0] = admin
keycloak.securityConstraints[0].authRoles[1] = user
keycloak.securityConstraints[0].securityCollections[0].name = insecure stuff
keycloak.securityConstraints[0].securityCollections[0].patterns[0] = /insecure
keycloak.securityConstraints[1].authRoles[0] = admin
keycloak.securityConstraints[1].securityCollections[0].name = admin stuff
keycloak.securityConstraints[1].securityCollections[0].patterns[0] = /admin
```

Spring Security Adapter

Установка адаптера

Для установки адаптера Spring Security достаточно добавить зависимость: pom.xml

```
<dependency>
  <groupId>org.keycloak</groupId>
  <artifactId>keycloak-spring-security-adapter</artifactId>
  <version>4.8.3.Final</version>
</dependency>
```

Конфигурация Spring Security в java

Реализуем WebSecurityConfigurer (KeycloakWebSecurityConfigurerAdapter). При этом будет использоваться конфигурация из файла **keycloak.json**, который нужно создать в ресурсном каталоге:

```
@KeycloakConfiguration
public class SecurityConfig extends KeycloakWebSecurityConfigurerAdapter
{
    /**
     * Registers the KeycloakAuthenticationProvider with the authentication manager.
     */
    @Autowired
    public void configureGlobal(AuthenticationManagerBuilder auth) throws Exception {
        auth.authenticationProvider(keycloakAuthenticationProvider());
    }

    /**

```

```

 * Defines the session authentication strategy.
 */
@Bean
@Override
protected SessionAuthenticationStrategy sessionAuthenticationStrategy() {
    return new RegisterSessionAuthenticationStrategy(new SessionRegistryImpl());
}

@Override
protected void configure(HttpSecurity http) throws Exception
{
    super.configure(http);
    http
        .authorizeRequests()
        .antMatchers("/customers*").hasRole("USER")
        .antMatchers("/admin*").hasRole("ADMIN")
        .anyRequest().permitAll();
}
}

```

При необходимости можно организовать маппинг ролей, org.keycloak.adapters.springsecurity.authentication.KeycloakAuthenticationProvider имеет поддержку маппинга через org.springframework.security.core.authority.mapping.GrantedAuthoritiesMapper.

Конфигурация через XML

```

<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:security="http://www.springframework.org/schema/security"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
           http://www.springframework.org/schema/beans
           http://www.springframework.org/schema/beans/spring-beans.xsd
           http://www.springframework.org/schema/context
           http://www.springframework.org/schema/context/spring-context.xsd
           http://www.springframework.org/schema/security
           http://www.springframework.org/schema/security/spring-security.xsd">

    <context:component-scan base-package="org.keycloak.adapters.springsecurity" />

    <security:authentication-manager alias="authenticationManager">
        <security:authentication-provider ref="keycloakAuthenticationProvider" />
    </security:authentication-manager>

```

```
<bean id="adapterDeploymentContext"
class="org.keycloak.adapters.springsecurity.AdapterDeploymentContextFactoryBean">
    <constructor-arg value="/WEB-INF/keycloak.json" />
</bean>

<bean id="keycloakAuthenticationEntryPoint"
class="org.keycloak.adapters.springsecurity.authentication.KeycloakAuthenticationEntryPoint" />
    <bean id="keycloakAuthenticationProvider"
class="org.keycloak.adapters.springsecurity.authentication.KeycloakAuthenticationProvider" />
        <bean id="keycloakPreAuthActionsFilter"
class="org.keycloak.adapters.springsecurity.filter.KeycloakPreAuthActionsFilter" />
            <bean id="keycloakAuthenticationProcessingFilter"
class="org.keycloak.adapters.springsecurity.filter.KeycloakAuthenticationProcessingFilter">
                <constructor-arg name="authenticationManager" ref="authenticationManager" />
            </bean>

        <bean id="keycloakLogoutHandler"
class="org.keycloak.adapters.springsecurity.authentication.KeycloakLogoutHandler">
            <constructor-arg ref="adapterDeploymentContext" />
        </bean>

        <bean id="logoutFilter"
class="org.springframework.security.web.authentication.logout.LogoutFilter">
            <constructor-arg name="logoutSuccessUrl" value="/" />
            <constructor-arg name="handlers">
                <list>
                    <ref bean="keycloakLogoutHandler" />
                    <bean
class="org.springframework.security.web.authentication.logout.SecurityContextLogoutHandler" />
                </list>
            </constructor-arg>
            <property name="logoutRequestMatcher">
                <bean class="org.springframework.security.web.util.matcher.AntPathRequestMatcher">
                    <constructor-arg name="pattern" value="/sso/logout**" />
                    <constructor-arg name="httpMethod" value="GET" />
                </bean>
            </property>
        </bean>

        <security:http auto-config="false" entry-point-ref="keycloakAuthenticationEntryPoint">
            <security:custom-filter ref="keycloakPreAuthActionsFilter" before="LOGOUT_FILTER" />
            <security:custom-filter ref="keycloakAuthenticationProcessingFilter"
before="FORM_LOGIN_FILTER" />
```

```
<security:intercept-url pattern="/customers**" access="ROLE_USER" />
<security:intercept-url pattern="/admin**" access="ROLE_ADMIN" />
<security:custom-filter ref="logoutFilter" position="LOGOUT_FILTER" />
</security:http>

</beans>
```

Настройка logout пользователя

С целью предотвращения несанкционированного доступа к данным конечного пользователя в защищаемом приложении, существуют функции деактивации пользовательской сессии и инвалидации JWT-токена, доступные в IAM Proxy. Данные механизмы являются частью стандарта **OpenID Connect**, что позволяет использовать их практически с любым провайдером идентификации. При рассмотрении данного раздела следует учесть, что IAM Proxy не используется для защиты в межсервисных взаимодействиях, а предназначен для использования в сценариях работы пользователя с конечными сервисами. Например, с **web UI**. Для осуществления выхода пользователя (**logout**) из защищаемого приложения, необходимо на фронте (браузер, мобильное приложение или устройство) вызвать сервис завершения сессии пользователя в IAM Proxy: **GET: /openid-connect-auth/logout**. В результате вызова сервиса IAM Proxy вернет сообщение с перенаправлением (**redirect**), который должен быть корректно обработан фронтом (браузером, мобильным приложением или устройством), для перенаправления пользователя на веб-страницу сервиса завершения сессии пользователя провайдера идентификации. В ходе разработки приложения необходимо учитывать определенные особенности реализации механизма завершения сессии пользователя, накладываемые спецификацией **OpenID Connect** и текущей реализацией компонента IAM Proxy.

Обратите внимание:

- URL страницы или сервиса завершения сессии пользователя (или **logout**) должен быть настраиваемым в вашем приложении, т.к. конкретные значения могут быть изменены в зависимости от настроек IAM Proxy;
- при проектировании приложения и встраивании страницы или сервиса завершения сессии пользователя необходимо учесть, что используемый протокол **OpenID** и текущая реализация решения предполагает работу с компонентом IAM Proxy конечных пользователей (например, физически существующих людей, использующих браузеры или мобильные устройства), а не межсервисные взаимодействия, для аутентификации которых используются другие средства. В связи с этим, необходимо избежать использования программных решений, которые позволяют имитировать или автоматизировать выполнение запросов к сервису завершения пользовательской сессии. Примером, такого нежелательного решения может являться использование AJAX, который позволяет вызывать сервис с помощью **JS**, но при этом непосредственно браузер не обрабатывает результат вызова, а такие вызовы браузером считаются небезопасными из-за возможности **XSS**, вследствие чего будут применены политики CORS, что в итоге может не

позволить обработать перенаправления на IDP провайдера (потребуется разрешения CORS на IDP). Вызов сервиса завершения пользовательской сессии должен выполняться браузером - это позволит осуществить корректное перенаправление для инвалидации всех, связанных с текущей сессией, объектов.

*Identity provider - СУДИР

Опции logout пользователя

Есть возможность переопределить заданные по умолчанию при развертывании опции revoke токенов и выход на IDP через параметры URI при logout.

- Параметр `revoke` отвечает за включение/выключение `revoke` токенов при `logout`;
- Параметр `logout_idp` отвечает за `logout` из IDP.

Пример: `/openid-connect-auth/logout?revoke=true&logout_idp=false`.

При таких параметрах будет выполнен `revoke` токенов и `logout` на IDP выполнен не будет, ограничившись лишь выходом из клиента/AC, соответствующего отозванным токенам.

Описание стандартных опций `logout` можно посмотреть в демо-профиле развертывания (`oidc_revoke_tokens_on_logout` и `oidc_disable_logout_in_idp`).

Настройка дизайна стартовой страницы IAM Proxy

IAM Proxy позволяет использовать свой шаблон дизайна стартовой страницы. Для этого необходимо заменить файл `jinja2`-шаблона стартовой `html`-страницы `template.index_html.jinja2` на свой (предварительно потребуется создать свой файл, на основе стандартного). Пример измененной страницы можно [скачать](#).

Для виртуальной машины (ВМ)

Замена шаблона стартовой страницы на виртуальной машине с использованием профиля развертывания

1. При расположении файлов шаблона стартовой страницы и ресурсов для нее, необходимо в профиле развертывания соблюсти следующую структуру каталогов (относительно директории профиля развертывания):
 - расположение шаблона стартовой страницы: `files/proxy/nginx/rds-client/templates/template.index_html.jinja2`;
ВАЖНО! имя файла шаблона должно соответствовать оригинальному имени файла: `template.index_html.jinja2`.
 - ресурсы используемые стартовой страницей (опционально) размещаются по пути `files/proxy/nginx/html/`, например: `files/proxy/nginx/html/smartzlp_logo.png`.
2. Применить изменения внесенные в профиль развертывания и запустить Jenkins Job.

Замена шаблона стартовой страницы на виртуальной машине вручную

Данный способ применим только при использовании RDS Server, стартовая страница при этом генерируется средствами rds-client.

Для замены шаблона стартовой страницы, выполните следующие действия:

1. Скопируйте на виртуальную машину персонализированный шаблон и перенесите в директорию назначения `/usr/local/openresty/nginx/rds-client/templates/`.
 - Персонализированный шаблон размещен по пути `/usr/local/openresty/nginx/rds-client/templates/`.
2. Измените владельца и группу владельцев файла персонализированного шаблона на nginx.
 - Владелец и группа владельцев успешно изменена.
3. Скопируйте файлы ресурсов (изображения, css и т.п., опционально), используемые персонализированным шаблоном, в директорию `/usr/local/openresty/nginx/html/`.
 - Файлы ресурсов скопированы в директорию `/usr/local/openresty/nginx/html/`.
4. Измените владельца и группу владельцев на скопированных файлах на nginx.
 - Владелец и группа владельцев успешно изменена.
5. Перезапустите службы rds-client (`sudo systemctl restart rds-client`).
 - Служба rds-client (`sudo systemctl restart rds-client`) перезапущена.

Для OpenShift

Замена шаблона стартовой страницы в контейнере (в OpenShift)

1. Подготовка ConfigMap. Подготавливаем файл персонализированного шаблона. Для подключения статических бинарных ресурсов, используемых персонализированным шаблоном (опционально), необходимо выполнить конвертацию подключаемого бинарного файла в формат base64 (например командой `base64 smartnlp_logo.png`). Пример формата: `iVBORw0KGgoAAAANSUhE....AAACXBIWXMAABYlAAAWJQFJUiTwAAAA`. Полученный формат изображения используем на следующем шаге.
2. Создание OSE ConfigMap. Используя OSE UI или шаблон OSE ConfigMap по умолчанию, приводим манифест ConfigMap к следующему виду:

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: iamproxy.custom.template
data:
  template.index.html.jinja2: |
    # Содержимое персонализированного шаблона (полученный на предыдущем шаге)
binaryData:
```

```
smartnlp_logo.png: |  
    # бинарный файл изображения в формате base64 (полученный на предыдущем шаге)
```

3. Подготовка OSE Deployment IAM Proxy. Подключаем созданный в пункте 2 ConfigMap к контейнеру IAM Proxy в качестве volume, для чего приводим Deployment IAM Proxy к следующему виду:

```
...  
spec:  
...  
template:  
...  
spec:  
volumes:  
- name: iamproxy-custom-template-volume  
configMap:  
    name: iamproxy.custom.template  
    defaultMode: 0400 #Права только на чтение  
...  
containers:  
...  
volumeMounts:  
- name: iamproxy-custom-template-volume  
  mountPath: /usr/local/openresty/nginx/rds-client/templates/template.index.html.jinja2  
  subPath: template.index.html.jinja2  
- name: iamproxy-custom-template-volume  
  mountPath: /usr/local/openresty/nginx/html/smartnlp_logo.png  
  subPath: smartnlp_logo.png  
...
```

Миграция на текущую версию

Для миграции на текущую версию продукта необходимо выполнить следующие действия:

1. Ознакомьтесь с разделом “Руководство по установке”.
2. Проверьте соответствие требованиям изложенным в разделе “Системные требования”.
3. Выполните действия описанные в разделе “Установка” (для установки на виртуальную машину) или в разделе “Руководство по установке в среде контейнеризации” (для установки в среде контейнеризации).

Быстрый старт

IAM Proxy имеет базовую конфигурацию которая донастраивается при установке компонента.

Использование программного компонента

Как правило, разработчик не использует проксирование непосредственно при разработке и интеграции с сервисом идентификации и аутентификации, но может использовать некоторые артефакты аутентификации и идентификации, производимые провайдером идентификации и используемые IAM Proxy в ходе своего нормального функционирования. При использовании проксирования через IAM Proxy и при использовании mTLS на подключениях к серверам приложения, проверка подписи JWT-токена и его срока действия не является необязательной. Однако данную проверку рекомендуется производить. Разработчику приложения следует ориентироваться на состав JWT-токена с конкретного региона (могут быть небольшие отличия в зависимость от региона) при проектировании механизмов аутентификации и авторизации своего приложения. Ниже приводится пример передаваемого JWT-токена и описание его полей.

```
{  
    "alg": "RS256",  
    "typ": "JWT",  
    "kid": "QQQGMpFRIhaR1HDeJNIVRrEmUK14AgR_sz_rg-5kjvU"  
}  
{  
    "exp": 1623917687,  
    "iat": 1623917387,  
    "jti": "b986ddb6-d96e-400d-8b09-64f217ea98a6",  
    "iss": "https://auth.my.company.ru/auth/realmCustomerA",  
    "aud": [  
        "CustomerA:Project1",  
        "CustomerA:Project2"  
    ],  
    "sub": "6608179f-9f7f-4154-922f-f541c7448e6e",  
    "typ": "Bearer",  
    "azp": "CustomerA:IAMProxy",  
    "session_state": "aed58344-610d-4d09-b241-5db0193e2ad5",  
    "acr": "1",  
    "resource_access": {  
        "CustomerA:Project1": {  
            "roles": [  
                "JustUser"  
            ]  
        },  
        "CustomerA:Project2": {  
            "roles": [  
                "JustUser"  
            ]  
        }  
    }  
}
```

```

"roles": [
    "AppRoleC",
    "AppRoleB"
]
},
"scope": "email profile",
"email_verified": false,
"preferred_username": "ivanov-ii"
}

```

Содержимое токена приведено в качестве примера, и может не соответствовать по наполнению с реальными токенами.

Блок	Параметр	Описание	Пример
Header	alg	Алгоритм, который использовался для подписания токена HS256 (HMAC с SHA-256) - это симметричный алгоритм шифрования с одним (секретным) ключом, который разделяется между авторизационным сервисом и клиентским сервисом. Поскольку один и тот же ключ используется как для генерации подписи, так и для проверки подписи, необходимо следить за тем, чтобы ключ не был скомпрометирован. RS256 (подпись RSA с SHA-256) является симметричный алгоритм, использует пару открытый/закрытый ключ: сервис авторизации имеет закрытый ключ, используемый для генерации подписи, а клиентские сервисы хранят открытый ключ, используемый для проверки подписи. Поскольку открытый ключ, в отличие от закрытого ключа, не должен быть защищен, большинство поставщиков удостоверений делают его доступным для потребителей для получения и использования (обычно через URL метаданных). Возможны также данные алгоритмы с размером ключа в 384 и 512 бит (RS512 ...).	RS256
	typ	Тип формата токена	JWT
	kid	ID открытого ключа для проверки подписи	QQQGMpFRIhaR1HDeJNIVRrEmUK14AgR_sz_rg-5kjvU
Payload	jti	JWT ID Claim - уникальный идентификатор токена	9d4cd7be-320a-4ee7-b8b8-15623c0ba4dd
	typ	Тип токена	ID

Блок	Параметр	Описание	Пример
	exp	Срок действия токена (тип NumericDate)	1586514237
	nbf	Not Before Claim – Срок, до которого токен НЕ может быть использован (тип NumericDate)	0
	iat	Not Before Claim – Время выдачи токена (тип NumericDate)	1586513637
	iss	Issuer Claim - идентификатор издателя токена	https://mycompany-auth.mycompany.ru/auth/realms/PlatformAuth
	azp	Получатель, сторона которая запросила токен (содержит client id)	PlatformAuth-Proxy
	sub	Subject Claim - идентификатор назначения токена, содержит ID УЗ пользователя	739edb6e-b9b5-4ec5-9731-2e37de8d6327
	aud[]	Audience Claim - определяет получателей, для которых предназначен токен	["PlatformAuth-Proxy", "PlatformAuthZ"]
	nonce	Строковое значение, используемое для связывания сеанса клиента с TokenID	64ac9d64d2b2b31167ab02015ae75d4e
	auth_time	Время когда была произведена аутентификация (тип NumericDate)	1586513637
	session_state	Идентификатор сессии пользователя	e281c489-b28b-4213-95a5-e6985071b69c
	acr	Уровень, достаточный для идентификации	1

Блок	Параметр	Описание	Пример
	realm_access.roles[]	Набор разрешений для работы с консолью	"roles" : ["EFS_APPLICATION_ADMIN","platform_uth_admin","uma_authorization"]
	preferred_username	Логин пользователя	test_admin
Sign		Подпись токена на закрытом ключе с использованием алгоритма из поля <code>alg</code> , в формате <code>base64</code> . <code>EncodeToBase64(SHA256withRSA(unsignedToken, SECRET_KEY))</code>	Zwbmz3zMqixJMbuuG9FS9OTqThG1FWHND1.....

Примечание: *NumericDate* - количество секунд с 1 января 1970 года 00:00:00 UTC

проверка токена при авторизации

1. Проверка подписи по открытому ключу `kid`;
2. Выдан доверенной стороной `iss`;
3. Валидность по времени `iat/exp`;
4. Наличия имени/`id` проверяющей системы в поле `aud`.

Часто встречающиеся проблемы и пути их устранения

Этот документ содержит названия переменных одинаково применимых для различных сред контейнеризации, указанных в системных требованиях. Имя переменной не определяет конкретную среду контейнеризации.

Проблемы при конфигурировании клиентского модуля Сервиса Аутентификации

Несовпадение логинов в сессионных параметрах и поставщике пользовательских данных

Текст ошибки в логах:

Caused by: ru.mycompany.ufs.platform.core.auth.UfsAuthenticationForbiddenException: Ошибка аутентификации -
неидентичные логины в сессионных параметрах и поставщике пользовательских данных

Описание:

При конфигурации клиентского модуля Сервиса Аутентификации для платформенных приложений на **Spring Boot** по умолчанию включена проверка на соответствие логина из токена и логина из сервиса сессионных данных. Если сервис сессионных данных не используется, то проверка не требуется и ее необходимо выключить (возможность выключения добавлена начиная с версии `authentication-spring-boot-starter 7.4.8` и выше). За включение/выключение этой проверки отвечает атрибут `secureByLogin`(по умолчанию он имеет значение `true`). Чтобы выключить, необходимо установить атрибуту `secureByLogin` значение `false`. Делается это в части конфигурирования, а именно:

```
@IamProvider(  
    pathsConfiguration = @PathsSecuredByLoginConfiguration(  
        secureByLogin = false)  
)
```