



Инструкция по установке и настройке решения

ОГЛАВЛЕНИЕ

1 АННОТАЦИЯ.....	4
2 ВВЕДЕНИЕ.....	5
3 КОМПОНЕНТЫ.....	6
4 ИНТЕГРИРУЕМЫЕ СИСТЕМЫ.....	7
5 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ.....	8
5.1 ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ.....	8
5.2 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	8
6 УСТАНОВКА КОМПОНЕНТОВ.....	9
6.1 СУБД.....	9
6.2 INTRY FILES	9
6.3 INTRY SSO	10
6.4 INTRY API.....	11
6.5 INTRY UI.....	12
6.6 Шлюз	12
6.7 INTRY JOBS.....	13
7 НАСТРОЙКА ПАРАМЕТРОВ.....	14
7.1 Настройка INTRY SSO (KEYCLOAK).....	14
7.2 Настройка шлюза (NGINX).....	27
7.3 Настройка INTRY FILES (MINIO)	27
7.3.1 Создание бакета.....	27
7.3.2 Создание ключей доступа.....	28

СПИСОК ТАБЛИЦ

ТАБЛИЦА 1 Основные компоненты INTRY	6
ТАБЛИЦА 2 Интегрируемые системы.....	7
ТАБЛИЦА 3 ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ.....	8
ТАБЛИЦА 4 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	8

СПИСОК ИЛЛЮСТРАЦИЙ

РИСУНОК 1 Создание REALM (ОКРУЖЕНИЯ)	14
--	----

Рисунок 2 СТРАНИЦА СОЗДАНИЯ REALM (ОКРУЖЕНИЯ)	15
Рисунок 3 СТРАНИЦА СОЗДАННОГО REALM.....	15
Рисунок 4 СПИСОК КЛИЕНТОВ ДЛЯ REALM INTRY	16
Рисунок 5 Создание клиента INTRY_SPA в REALM INTRY (СТР 1)	16
Рисунок 6 Создание клиента INTRY_SPA в REALM INTRY (СТР 2)	17
Рисунок 7 Создание клиента INTRY_SPA в REALM INTRY (СТР 3).....	18
Рисунок 8 СТРАНИЦА РЕДАКТИРОВАНИЯ СОЗДАННОГО КЛИЕНТА INTRY_SPA	19
Рисунок 9 СТРАНИЦА CLIENT SCOPES	20
Рисунок 10 СТРАНИЦА СОЗДАНИЯ CLIENT SCOPE.....	20
Рисунок 11 СТРАНИЦА СПИСКА CLIENT SCOPES ПОСЛЕ СОЗДАНИЯ INTRY_API.....	21
Рисунок 12 СТРАНИЦА CLIENT SCOPE INTRY_API	21
Рисунок 13 Страница выбора типа конфигурирования для CLIENT SCOPE INTRY_API.....	22
Рисунок 14 Страница конфигурирования привязки AUDIENCE для CLIENT SCOPE INTRY_API.....	22
Рисунок 15 Добавление SCOPE INTRY_API в КЛИЕНТ INTRY_SPA (РИС 1)	23
Рисунок 16 Добавление SCOPE INTRY_API в КЛИЕНТ INTRY_SPA (РИС 2)	23
Рисунок 17 Добавленный SCOPE в СПИСКЕ	24
Рисунок 18 Создание подключения к ACTIVE DIRECTORY	24
Рисунок 19 Страница настройки LDAP подключения (часть1).....	25
Рисунок 20 Страница настройки LDAP подключения (часть2).....	26
Рисунок 21 Добавленные LDAP подключения в ФЕДЕРАЦИИ ПОЛЬЗОВАТЕЛЕЙ.....	26
Рисунок 22 Страница создания БАКЕТА	27
Рисунок 23 Страница созданного БАКЕТА.....	28
Рисунок 24 Страница списка ПОЛЬЗОВАТЕЛЕЙ	28
Рисунок 25 Страница создания ПОЛЬЗОВАТЕЛЯ.....	28
Рисунок 26 Страница списка ключей доступа для ПОЛЬЗОВАТЕЛЯ	29
Рисунок 27 Страница создания ключа доступа.....	29
Рисунок 28 ПРОВОДНИК ПО ДАННЫМ В БАКЕТЕ.....	30

1 АННОТАЦИЯ

Настоящий документ описывает процедуру установки и настройки интранет-решения Intry.

2 ВВЕДЕНИЕ

Данная инструкция предназначена для развёртывания решения Intry с использованием Docker (<https://www.docker.com>)

3 КОМПОНЕНТЫ

Таблица 1 Основные компоненты *Intry*

№	Название	Программное обеспечение	Версия	Источник
1.	Шлюз	nginx	1.23	https://nginx.org/
2.	Intry UI	Angular	11	https://angular.io/ci
3.	Intry API	.NET	6	https://github.com/dotnet/aspnetcore#readme
4.	Intry SSO	Keycloak	21.1.1	https://www.keycloak.org/
5.	Intry Jobs	.NET	6	https://github.com/dotnet/aspnetcore#readme
6.	Intry Files	MinIO	RELEASE.2023-04-07T05-28-58Z	https://min.io/
7.	СУБД	PostgreSQL	15.2	https://www.postgresql.org/

4 ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

Таблица 2 Интегрируемые системы

Название	Назначение
SMTP-сервер	Используется для отправки email-писем.
Active Directory	Используется как один из провайдеров для аутентификации. Опционально.

5 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Требования к аппаратным и программным характеристикам определяются исходя из количества одновременно действующих пользователей, их сценариям взаимодействия с решением, а также требований к отказоустойчивости.

Ниже приведены минимальные технические требования для работы продукта Intry в Docker, число пользователей системы составляет не более 100 человек, без учета отказоустойчивости.

5.1 ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ

Таблица 3 Требования к оборудованию

Компонент	ЦПУ, ядер	ОЗУ, МБ	Диск, ГБ
Шлюз	0.1	512	20
Intry UI	0.1	32	20
Intry API	0.5	1024	20
Intry SSO	1	1024	20
Intry Jobs	1	2048	20
Intry Files	2*	2048*	100*
СУБД	2	2048	50

* - Зависит от количества файлов загружаемых в систему

5.2 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

В настоящей инструкции операционной системой хост-сервера является Ubuntu 22.04.1 LTS <https://releases.ubuntu.com/jammy/>. При необходимости можно использовать любую операционную систему, поддерживающую инфраструктуру Docker <https://docs.docker.com/engine/install/>.

Таблица 4 Требования к программному обеспечению

Компонент	Образы Docker
Шлюз	Nginx 1.23
Intry UI	Angular 11, intry-ui v-2648
Intry API	.NET 6, intry-api v-2649
Intry SSO	Keycloak 21.1.1
Intry Jobs	.NET 6, intry-jobs v-2649
Intry Files	MinIO RELEASE.2023-04-07T05-28-58Z
СУБД	PostgreSQL 15.2

6 УСТАНОВКА КОМПОНЕНТОВ

6.1 СУБД

Необходим для хранения реляционных данных приложения.

Переменные окружения:

Название	Значение	Описание
POSTGRESS_PASSWORD	<пароль>	Пароль системного пользователя приложения, под которым приложение подключается к БД

Последовательность действий:

- Установить докер контейнер из образа https://hub.docker.com/_/postgres
- Включить контейнер с образом в общую сеть (`docker network connect inttry postgres`)

Пример:

```
docker run -d -p 5432:5432 --name postgres \
-e POSTGRES_PASSWORD=P@sswOrd \
postgres:15.2-alpine
```

6.2 INTTRY FILES

Необходим для хранения бинарных данных (файлы, видео, изображения). Используется последняя версия.

Размер диска и RAM сильно зависит от планируемого общего количества файлов и их размера.

Переменные окружения:

Название	Значение	Описание
MINIO_ROOT_USER	<Сгенерировать>	Имя системного пользователя для доступа к интерфейсу приложения
MINIO_ROOT_PASSWORD	<Сгенерировать>	Пароль системного пользователя
MINIO_REGION	us-east-1	Необходим для нормального функционирования библиотеки AWS по работе с S3-совместимыми хранилищами.

Последовательность действий:

- установить докер контейнер из образа quay.io/minio/minio, инструкция <https://min.io/docs/minio/container/index.html>.

- Включить контейнер в общую сеть (docker network connect intry minio)

Пример:

```
docker run -d -p 9000:9000 -p 9090:9090 --user $(id -u):$(id -g) --name minio \
-e "MINIO_ROOT_USER=admin" \
-e "MINIO_ROOT_PASSWORD=P@sswOrd" \
-e "MINIO_REGION=us-east-1" \
-v ${HOME}/minio/data:/data quay.io/minio/minio server /data --console-address ":9090"
```

6.3 INTRY SSO

Необходимо для обеспечения аутентификации пользователей.

Переменные окружения:

Название	Значение	Описание
KEYCLOAK_ADMIN	admin	Встроенная учётная запись администратора SSO
KEYCLOAK_ADMIN_PASSWORD	<пароль>	Пароль встроенной учётной записи администратора
KC_DB	postgres	Провайдер хранилища для SSO, используется PostgreSQL
KC_DB_URL_HOST	postgres	Хост
KC_DB_URL_PORT	5432	Порт, стандартный
KC_DB_URL_DATABASE	keycloak	Название БД SSO
KC_DB_USERNAME	keycloak_writer	Учётная запись БД SSO
KC_DB_PASSWORD	<пароль>	Пароль для подключения к БД SSO

Последовательность действий:

- Установить докер контейнер из образа `quay.io/keycloak/keycloak` согласно инструкции <https://www.keycloak.org/getting-started/getting-started-docker>
- Включить контейнер в общую сеть (docker network connect intry keycloak)

Пример:

```
docker run -p 30003:8080 --name keycloak \
-e KEYCLOAK_ADMIN=admin \
-e KEYCLOAK_ADMIN_PASSWORD="e17b67t3HOc1DPqA4ZYp" \
-e PROXY_ADDRESS_FORWARDING=true \
```

```
-e KC_PROXY=edge \
-e KC_DB=postgres \
-e KC_DB_URL_HOST=postgres \
-e KC_DB_URL_PORT=5432 \
-e KC_DB_URL_DATABASE=keycloak \
-e KC_DB_USERNAME=postgres \
-e KC_DB_PASSWORD="T9swqGps5fzpG0Wp5zey" \
-d quay.io/keycloak/keycloak:21.1.1 start
```

6.4 INTRY API

Переменные окружения:

Название	Значение	Описание
AuthConfiguration__Authority	<keycloak_url>/realms/intry	Абсолютная ссылка к сервису аутентификации.
SwaggerConfiguration__Authority	<keycloak_url>/realms/intry	Абсолютная ссылка к сервису аутентификации.
AWS__BucketName	intry	Название бакета. Можно изменять.
AWS__ServiceURL	<minio_url>:9000	Абсолютная ссылка к сервису s3-совместимого хранилища Minio.
AWS__AccessKey	<ключ>	Ключ учётной записи в Minio для внутренних коммуникаций между API и Minio
AWS__SecretKey	<секрет>	Секрет учётной записи в Minio для внутренних коммуникаций между API и Minio
ASPNETCORE_ENVIRONMENT	Production	Переменная, определяющая тип окружения (продуктивное, тестовое)
ConnectionStrings__Intry	Host=postgres;Database=intry;Username=postgres;Password=<Password>;Port=5432;	Строка подключения к БД

Последовательность действий:

- Установить докер контейнер из образа `registry.intry.net:5000/intry-api:v-2648`
- Включить контейнер в общую сеть (`docker network connect intry intry-api`)

Пример:

```
docker run -d -p 30001:80 --restart unless-stopped --name intry-api \
```

```
-e "ASPNETCORE_ENVIRONMENT= Production" \
-e
"ConnectionStrings__Intry""="Host=postgres;Database=intry;Username=postgres;
Password=P@sswOrd;Port=5432;" registry.intry.net:5000/intry-api:v-2646
```

6.5 INTRY UI

Переменные окружения:

Название	Значение	Описание
API_URL	<ссылка к API>	Абсолютная ссылка к сервису API.
AUTHORITY_URL	<keycloak_url>/realms/intry	Абсолютная ссылка к сервису аутентификации.

Последовательность действий:

- Установить докер контейнер из образа `registry.intry.net:5000/intry-ui:v-2647`
- Включить контейнер в общую сеть (`docker network connect intry intry-app`)

Пример:

```
docker run -d -p 30000:80 --restart unless-stopped --name intry-ui \
-e "environment=pg" registry.intry.net:5000/intry-ui:v-2648
```

6.6 Шлюз

Последовательность действий:

- Установить докер контейнер из образа https://hub.docker.com/_/nginx
- Включить контейнер в общую сеть (`docker network connect intry nginx`)

Пример:

```
docker run -d -p 80:80 -p 443:443 --privileged --restart unless-stopped --name nginx \
-v ./nginx/conf/:/etc/nginx/conf.d/:ro \
-v ./certbot/www:/var/www/certbot/:ro \
nginx
```

Примечания:

- В рамках развёртывания предполагается использование `certbot` для получения сертификатов для доступа по `https`.
- Публикация сервисов по небезопасному протоколу `http` не рассматривается в данной инструкции.
- Если имеются уже выпущенные собственные сертификаты, то можно использовать их и пропустить шаги для выпуска сертификатов `letsencrypt` через `certbot`.

6.7 INTRY JOBS

Переменные окружения:

Название	Значение	Описание
ConnectionStrings__Intry	Host=postgres;Database=intry;Username=postgres;Password=<Password>;Port=5432;	Строка подключения к БД
ASPNETCORE_ENVIRONMENT	Production	Переменная, определяющая тип окружения (продуктивное, тестовое)

Последовательность действий:

- Установить докер контейнер из образа **registry.intry.net:5000/intry-jobs:v-2649**
- Включить контейнер в общую сеть (`docker network connect intry intry-jobs`)

Пример:

```
docker run -d -p 30004:80 --restart unless-stopped --name intry-jobs \
-e "ASPNETCORE_ENVIRONMENT= Production" \
-e
"ConnectionStrings__Intry=""Host=postgres;Database=intry;Username=postgres;
Password=P@sswOrd;Port=5432;" registry.intry.net:5000/intry-jobs:v-2649
```

7 НАСТРОЙКА ПАРАМЕТРОВ

7.1 НАСТРОЙКА INTRY SSO (KEYCLOAK)

Для сервиса единого входа (Single Sign-On) необходимо выполнить первоначальные настройки.

1. Создать Realm

В выпадающем меню нажать кнопку «Create realm».

The screenshot shows the Keycloak administration interface. On the left, a sidebar menu is open under the 'master' realm, showing options like 'Realm roles', 'Users', 'Groups', etc. A prominent blue button labeled 'Create Realm' is highlighted. The main content area is titled 'master realm' and contains two tabs: 'Server info' (which is active) and 'Provider info'. In the 'Server info' tab, there's a 'Profile' section listing various features. Some features are marked as 'Enabled' (e.g., ACCOUNT3, ADMIN_FINE_GRAINED_AUTHZ, etc.) while others are 'Disabled' (e.g., MAP_STORAGE, OPENSHIFT_INTEGRATION, etc.). Most disabled features have a 'Preview' link next to them, except for DOCKER and FIPS which are marked as 'Supported'.

Рисунок 1 Создание Realm (окружения)

На странице создания realm указать название (**intry**) и передвинуть переключатель в **Enabled**.

Инструкция по установке и настройке решения

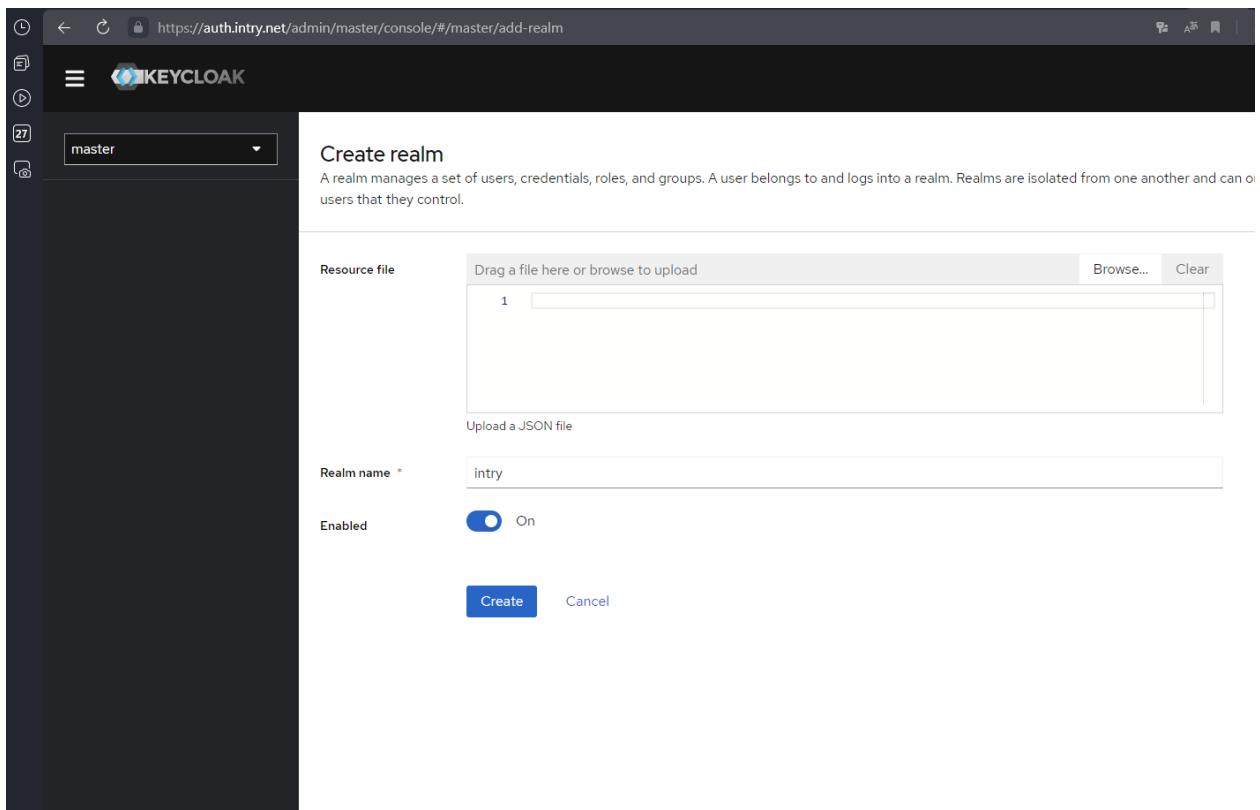


Рисунок 2 Страница создания Realm (окружения)

Созданный Realm будет отображаться в выпадающем меню.

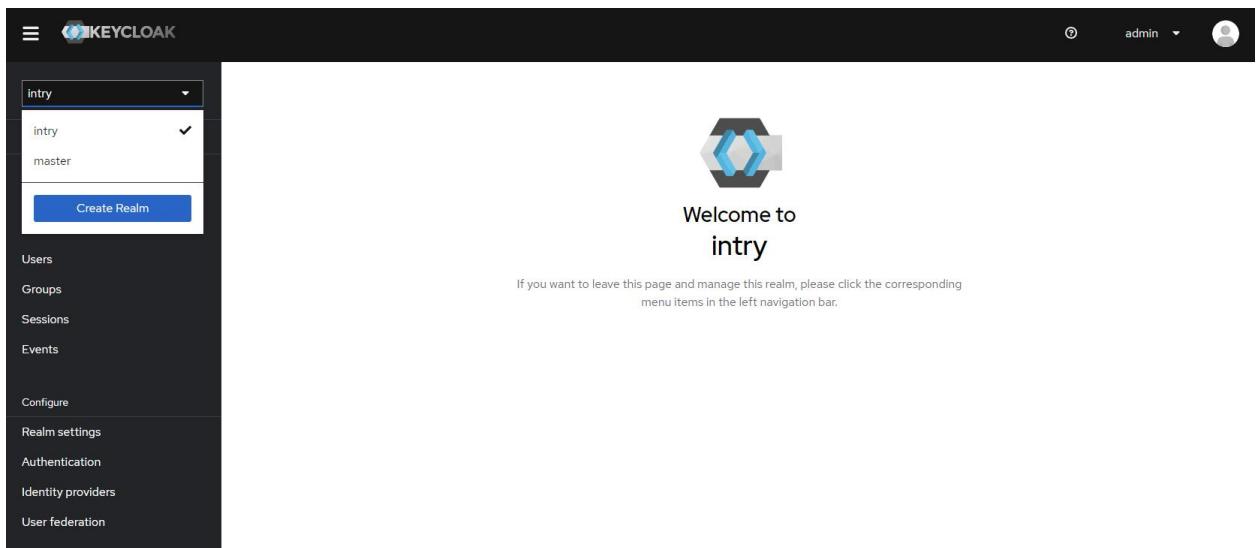
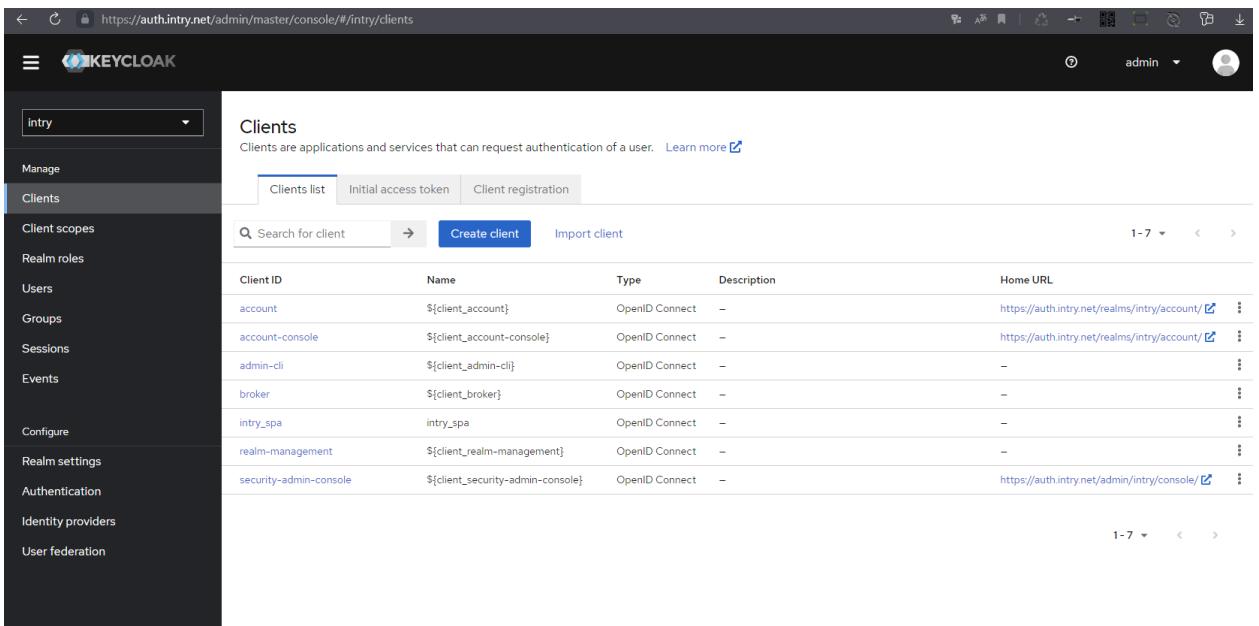


Рисунок 3 Страница созданного Realm

2. Создать и настроить клиент

Для этого необходимо перейти на страницу Clients и там нажать на кнопку Create client.

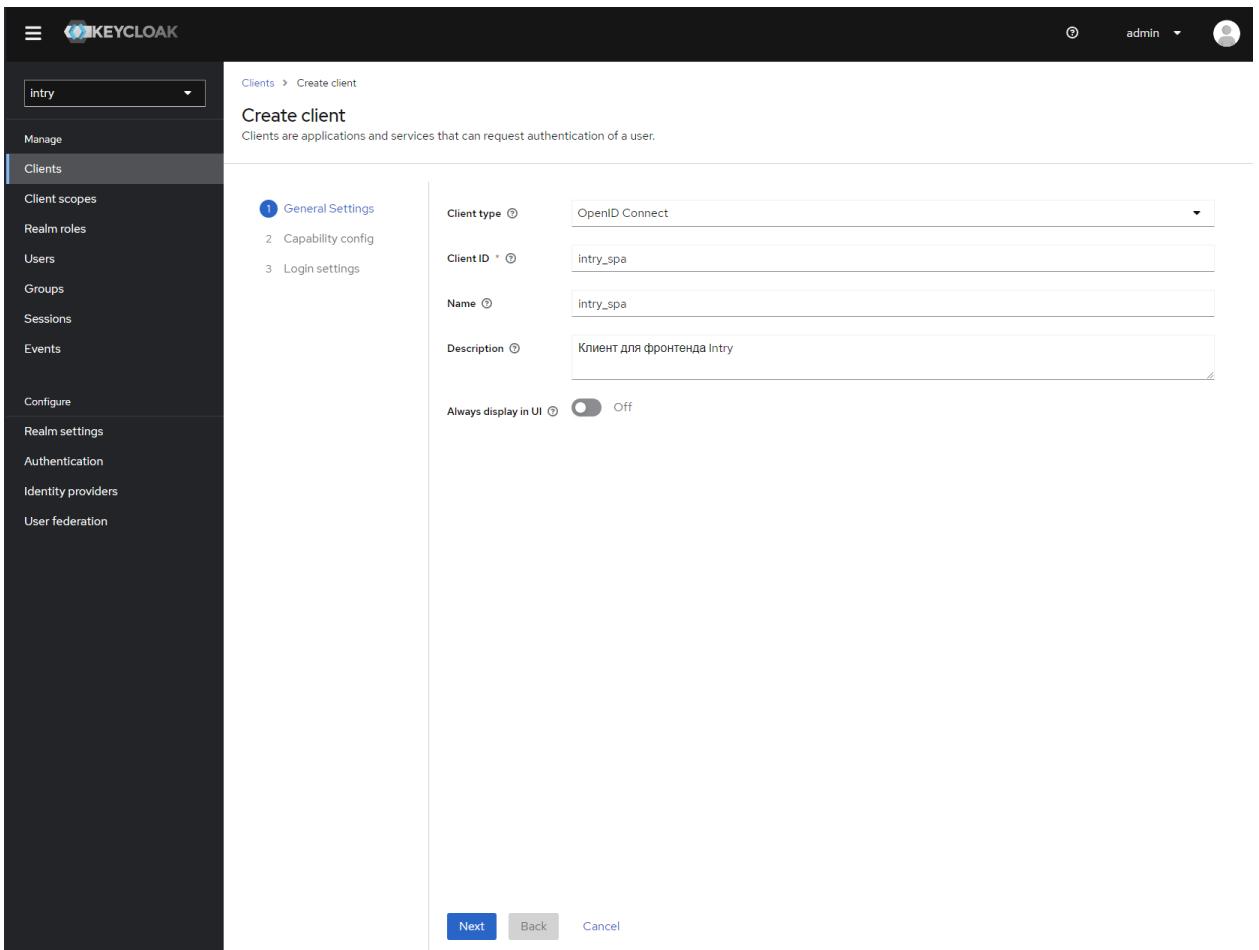
Инструкция по установке и настройке решения



The screenshot shows the Keycloak admin interface for the 'Intry' realm. The left sidebar has a 'Clients' section selected. The main area displays a table of clients with the following columns: Client ID, Name, Type, Description, and Home URL. The clients listed are:

Client ID	Name	Type	Description	Home URL
account	\${client_account}	OpenID Connect	—	https://auth.intry.net/realm/account/
account-console	\${client_account-console}	OpenID Connect	—	https://auth.intry.net/realm/intry/account/
admin-cli	\${client_admin-cli}	OpenID Connect	—	—
broker	\${client_broker}	OpenID Connect	—	—
intry_spa	intry_spa	OpenID Connect	—	—
realm-management	\${client_realm-management}	OpenID Connect	—	—
security-admin-console	\${client_security-admin-console}	OpenID Connect	—	https://auth.intry.net/admin/intry/console/

Рисунок 4 Список клиентов для realm Intry



The screenshot shows the 'Create client' form for the 'intry_spa' client. The left sidebar has a 'Clients' section selected. The right panel shows the 'General Settings' step of the wizard. The client details are as follows:

- Client type:** OpenID Connect
- Client ID:** intry_spa
- Name:** intry_spa
- Description:** Клиент для фронтенда Intry
- Always display in UI:** Off

At the bottom of the form are 'Next', 'Back', and 'Cancel' buttons.

Рисунок 5 Создание клиента *intry_spa* в realm Intry (стр 1)

Инструкция по установке и настройке решения

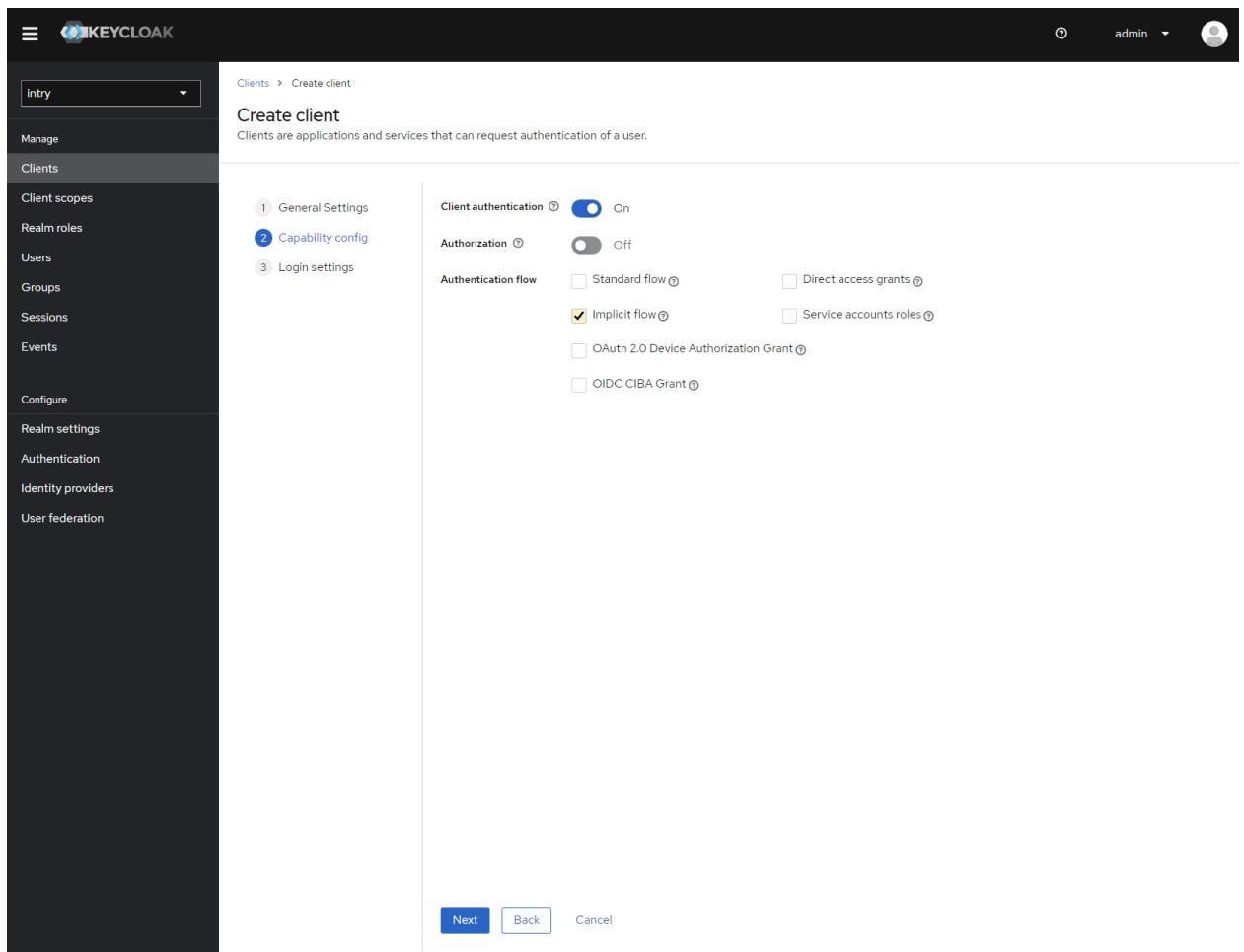


Рисунок 6 Создание клиента *intry_spa* в realm *Intry* (стр 2)

Инструкция по установке и настройке решения

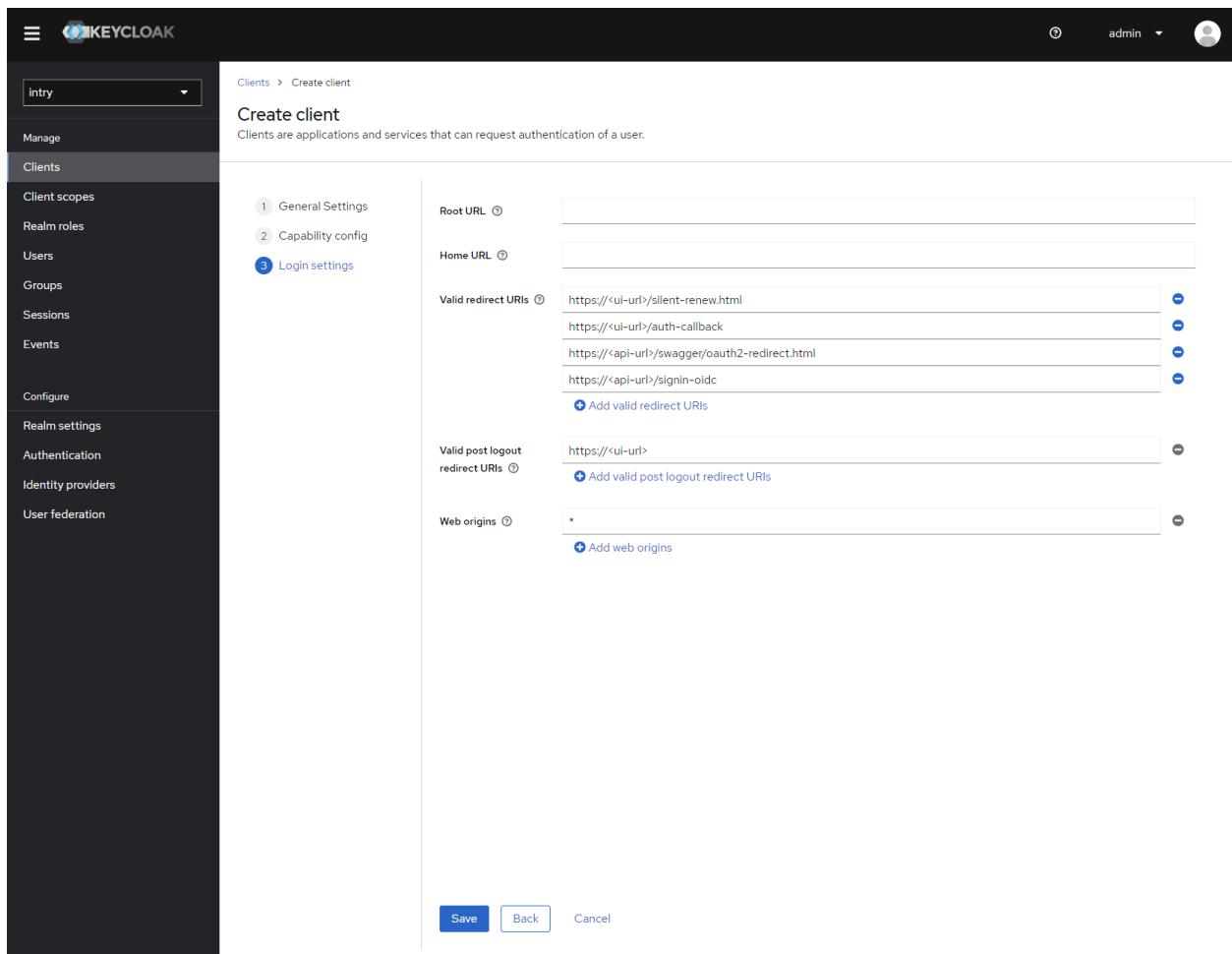


Рисунок 7 Создание клиента *intry_spa* в realm *Intry* (стр 3)

Инструкция по установке и настройке решения

The screenshot shows the Keycloak administration interface. The left sidebar is dark-themed and includes the following navigation items:

- Manage
- Clients** (selected)
- Client scopes
- Realm roles
- Users
- Groups
- Sessions
- Events
- Configure
 - Realm settings
 - Authentication
 - Identity providers
 - User federation

The main content area displays the configuration for the client 'intry_spa'. The top right shows the status as 'Enabled' and the user 'admin'. The tabs at the top of the configuration form are: Settings (selected), Keys, Credentials, Roles, Client scopes, Sessions, Advanced.

General Settings

- Client ID: intry_spa
- Name: intry_spa
- Description: Клиент для фронтенда Intry
- Always display in UI: Off

Access settings

- Root URL: (empty)
- Home URL: (empty)
- Valid redirect URIs:
 - https://pg-app.intry.net/silent-renew.html
 - https://pg-api.intry.net/swagger/oauth2-redirect.html
 - https://pg-api.intry.net/signin-oidc
 - https://pg-app.intry.net/auth-callback
- Add valid redirect URIs
- Valid post logout redirect URIs: https://pg-app.intry.net
- Add valid post logout redirect URIs
- Web origins: *
- Add web origins
- Admin URL: (empty)

At the bottom are 'Save' and 'Revert' buttons.

Рисунок 8 Страница редактирования созданного клиента *intry_spa*

Инструкция по установке и настройке решения

Name	Assigned type	Protocol	Display order	Description
acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token
address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address
email	Default	OpenID Connect	–	OpenID Connect built-in scope: email
microprofile-jwt	Optional	OpenID Connect	–	Micropattern - JWT built-in scope
offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access
phone	Optional	OpenID Connect	–	OpenID Connect built-in scope: phone
profile	Default	OpenID Connect	–	OpenID Connect built-in scope: profile
role_list	Default	SAML	–	SAML role list
roles	Default	OpenID Connect	–	OpenID Connect scope for add user roles to the access token

Рисунок 9 Страница client scopes

Create client scope

Name * intry_api

Description

Type None

Protocol OpenID Connect

Display on consent screen On

Consent screen text

Include in token scope On

Display Order

Save Cancel

Рисунок 10 Страница создания client scope

Инструкция по установке и настройке решения

The screenshot shows the Keycloak administration interface for the 'intry' realm. The left sidebar has a 'Client scopes' section selected. The main area displays a table of client scopes. One row is highlighted, showing a scope named 'intry_api' with 'None' assigned type and 'OpenID Connect' protocol. Other scopes listed include 'acr', 'address', 'email', etc.

Рисунок 11 Страница списка client scopes после создания *intry_api*

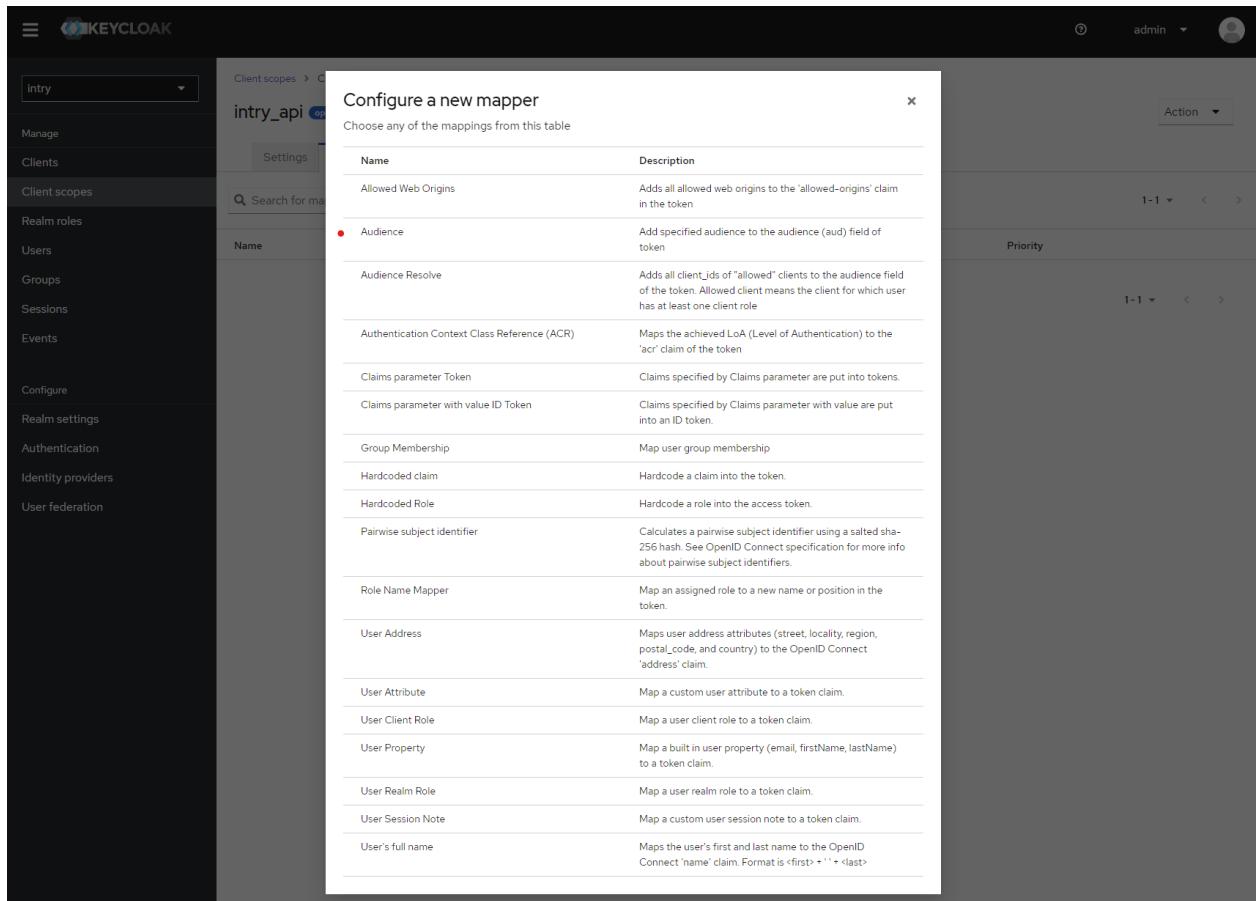
Для созданного Client Scope под названием *intry_api* необходимо создать привязку к audience. Это является необходимой защитой клиента и API – токен выданный сервисом будет валиден только для API.

The screenshot shows the 'Client scope details' page for 'intry_api'. The 'Mappers' tab is active. There is a button labeled 'Add mapper' and a table with columns 'Name', 'Category', 'Type', and 'Priority'. The table currently contains no data.

Рисунок 12 Страница client scope *intry_api*

При нажатии «Add mapper» будет открыто всплывающее окно создания конфигурации привязки для созданного client scope.

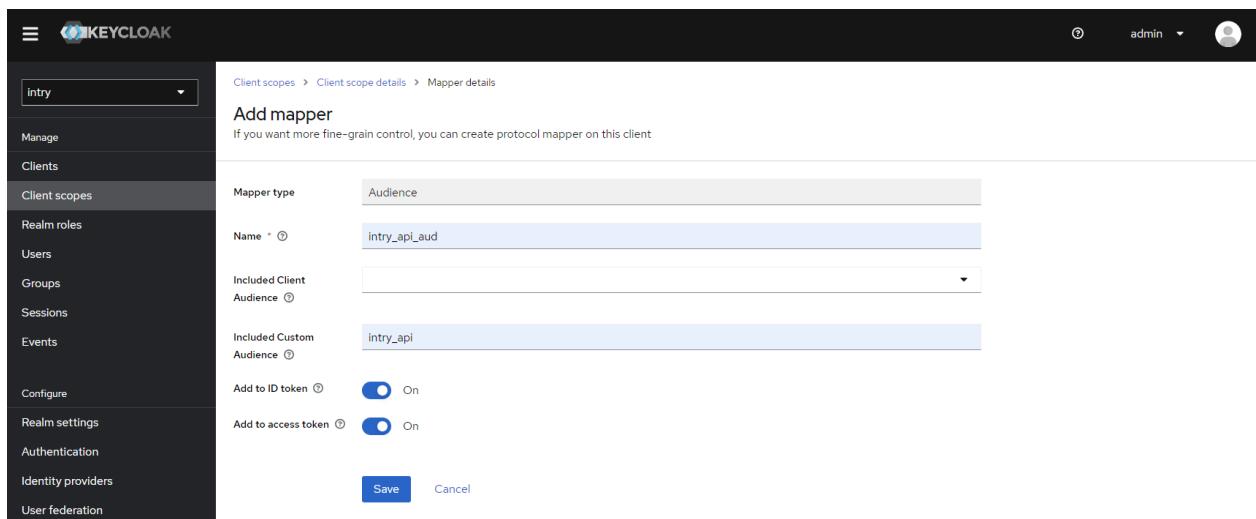
Инструкция по установке и настройке решения



The screenshot shows the Keycloak administration interface. On the left, there's a sidebar with navigation links: Manage, Clients, Client scopes (which is selected), Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. In the center, there's a search bar with 'intry' and a dropdown menu with 'intry_api'. Below it, there's a 'Settings' button. A modal window titled 'Configure a new mapper' is open, listing various mapping types with their descriptions. The 'Audience' option is highlighted with a red dot.

Рисунок 13 Страница выбора типа конфигурирования для client scope `intry_api`

Необходимо заполнить как на картинке ниже. Важный момент – это поле `Included Custom Audience`, в него необходимо внести значение `intry_api`.



The screenshot shows the 'Mapper details' configuration page for the 'intry' client. The sidebar on the left is identical to the previous screenshot. The main area shows a form for adding a mapper. The 'Mapper type' is set to 'Audience'. The 'Name' field contains 'intry_api_aud'. The 'Included Custom Audience' dropdown is set to 'intry_api'. There are two toggle switches: 'Add to ID token' is set to 'On', and 'Add to access token' is also set to 'On'. At the bottom, there are 'Save' and 'Cancel' buttons.

Рисунок 14 Страница конфигурирования привязки Audience для client scope `intry_api`

Затем необходимо добавить созданный и настроенный client scope `intry_api` в клиент `intry_spa`. Это выполняется на вкладке `Client scopes` на странице отображения клиента `intry_spa`.

Инструкция по установке и настройке решения

The screenshot shows the Keycloak administration interface. On the left, a sidebar menu is visible with items like 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', etc. The 'Clients' item is currently selected. In the main content area, the 'intry_spa' client is selected under the 'OpenID Connect' tab. The 'Client scopes' tab is active. A table lists various scopes: 'intry_spa-dedicated' (Assigned type: none), 'acr', 'address', 'email', 'micropoint-jwt', 'offline_access', 'phone', 'profile', and 'roles'. The 'intry_spa-dedicated' scope is highlighted. At the bottom right of the table, there are navigation buttons for pages 1-10.

Рисунок 15 Добавление scope *intry_api* в клиент *intry_spa* (рис 1)

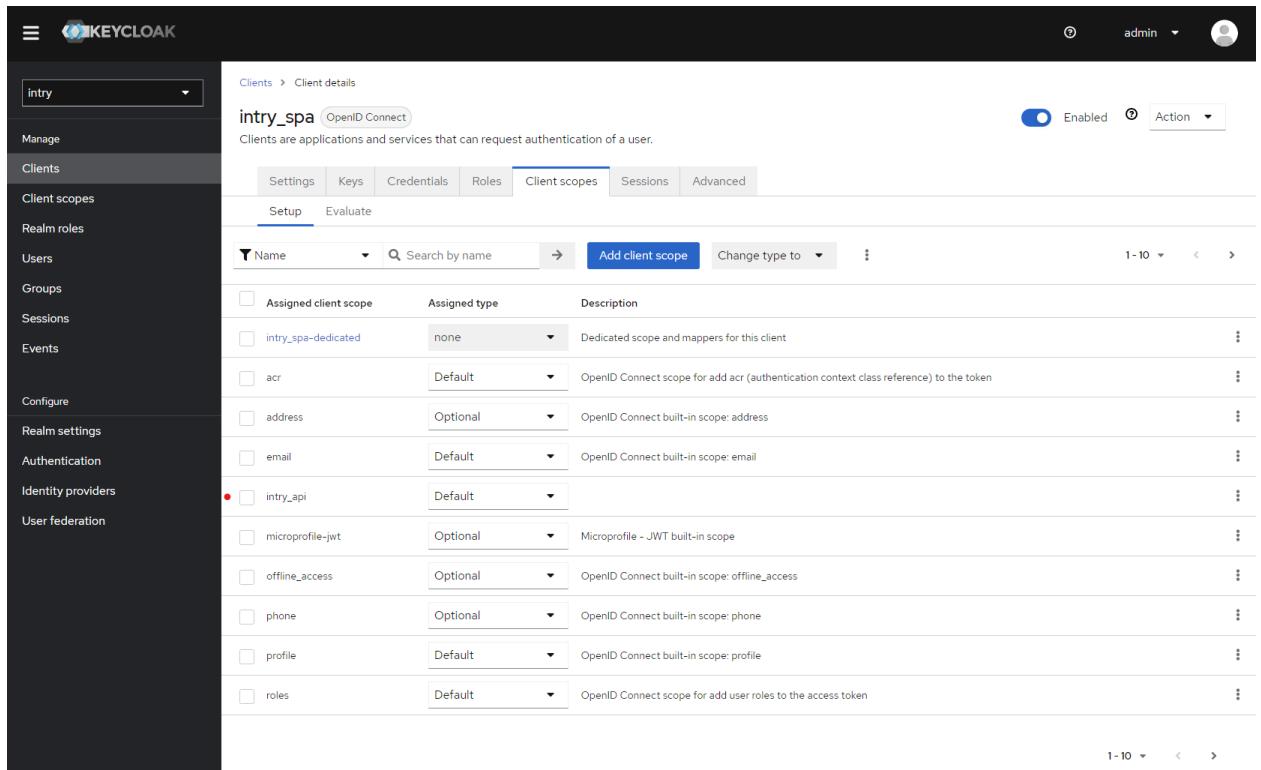
После нажатия кнопки «Add client scope», во всплывающем окне необходимо добавить требуемый scope – *intry_api*.

This screenshot shows the 'Add client scopes to intry_spa' dialog box. It contains a table with columns 'Name', 'Protocol', and 'Description'. Two scopes are listed: 'intry_api' (Protocol: OpenID Connect) and 'acr'. Below the table, there are dropdown menus for 'Default' and 'Optional', and a large blue 'Add' button. The background shows the same Keycloak interface as in Figure 15, with the 'Client scopes' tab still active for the 'intry_spa' client.

Рисунок 16 Добавление scope *intry_api* в клиент *intry_spa* (рис 2)

Инструкция по установке и настройке решения

Добавленный scope **intry_api** обязательно будет отображаться на странице списка scope для клиента **intry_spa**.

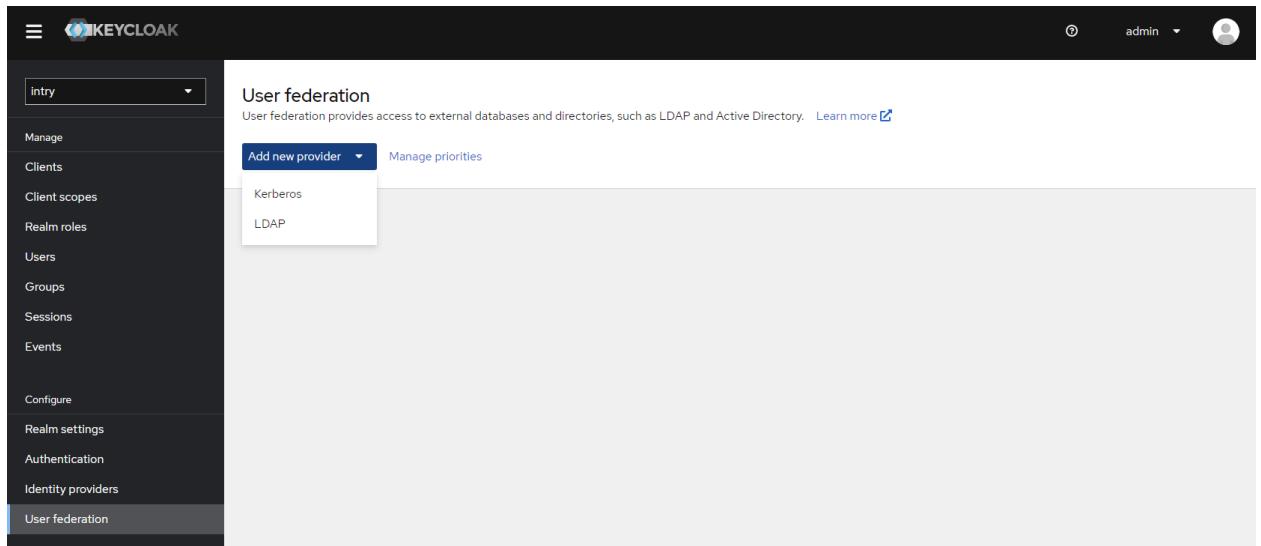


The screenshot shows the Keycloak administration interface. On the left, a sidebar menu is open with the 'Clients' section selected. In the main content area, the 'Client details' page for 'intry_spa' is displayed. The 'Client scopes' tab is active. A table lists various client scopes, including 'intry_api' which is highlighted with a red dot. Other scopes listed include 'intry_spadev-dedicated', 'acr', 'address', 'email', 'micropfile-jwt', 'offline_access', 'phone', 'profile', and 'roles'. Each row in the table includes columns for 'Name', 'Assigned type', and 'Description'.

Рисунок 17 Добавленный scope в списке

3. Добавление подключения к Active Directory (опционально)

При наличии служб Active Directory в компании, либо любой иной службы директорий, поддерживающих LDAP протокол, возможно подключить федерацию для синхронизации данных по пользователям.



The screenshot shows the Keycloak administration interface with the 'User federation' tab selected in the sidebar. A dropdown menu labeled 'Add new provider' is open, showing options like 'Kerberos' and 'LDAP'. The 'LDAP' option is highlighted with a red dot. The main content area displays information about user federation, mentioning external databases and directories like LDAP and Active Directory.

Рисунок 18 Создание подключения к Active Directory

Инструкция по установке и настройке решения

Пользователи, синхронизированные из LDAP, смогут входить на портал без дополнительных настроек и создания их вручную.

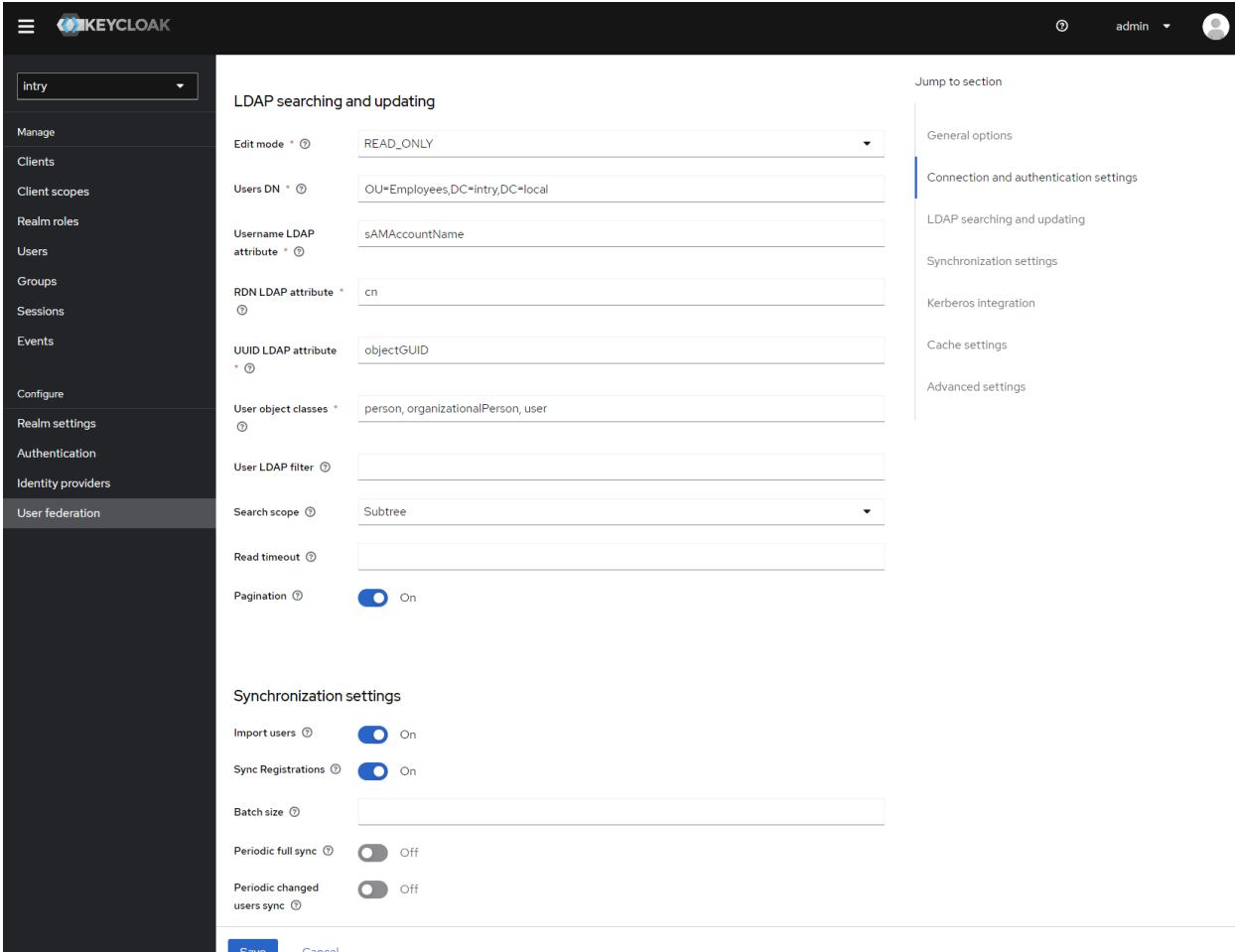
На странице создания LDAP подключения заполняются необходимые параметры. Протоколы используются стандартные, поэтому примеры настройки можно найти в общем доступе, в том числе и на сайте open source поставщика (<https://www.keycloak.org/documentation.html>).

Рабочий пример, также, указан ниже на скриншотах.

The screenshot shows the 'User federation > Add LDAP provider' screen in the Keycloak interface. The left sidebar is dark with white text, showing the 'intry' realm selected. The main panel has a light background. It displays the 'General options' section with 'UI display name' set to 'ldap' and 'Vendor' set to 'Active Directory'. Below this is the 'Connection and authentication settings' section, which includes fields for 'Connection URL' (set to 'LDAP://<domain>:389'), 'Enable StartTLS' (set to 'Off'), 'Use Truststore SPI' (set to 'Only for ldaps'), 'Connection pooling' (set to 'Off'), and 'Connection timeout'. There are 'Test connection' and 'Test authentication' buttons. On the right side, there's a sidebar with a tree view: 'General options' (selected), 'Connection and authentication settings', 'LDAP searching and updating', 'Synchronization settings', 'Kerberos integration', 'Cache settings', and 'Advanced settings'.

Рисунок 19 Страница настройки LDAP подключения (часть1)

Инструкция по установке и настройке решения



The screenshot shows the 'User federation' configuration page in Keycloak. On the left, a sidebar lists various management options like 'Clients', 'Groups', and 'Events'. The 'User federation' option is selected. The main panel is titled 'LDAP searching and updating' and contains several configuration fields:

- 'Edit mode': READ_ONLY
- 'Users DN': OU=Employees,DC=intry,DC=local
- 'Username LDAP attribute': sAMAccountName
- 'RDN LDAP attribute': cn
- 'UUID LDAP attribute': objectGUID
- 'User object classes': person, organizationalPerson, user
- 'User LDAP filter': (empty)
- 'Search scope': Subtree
- 'Read timeout': (empty)
- 'Pagination': On (switch is turned on)

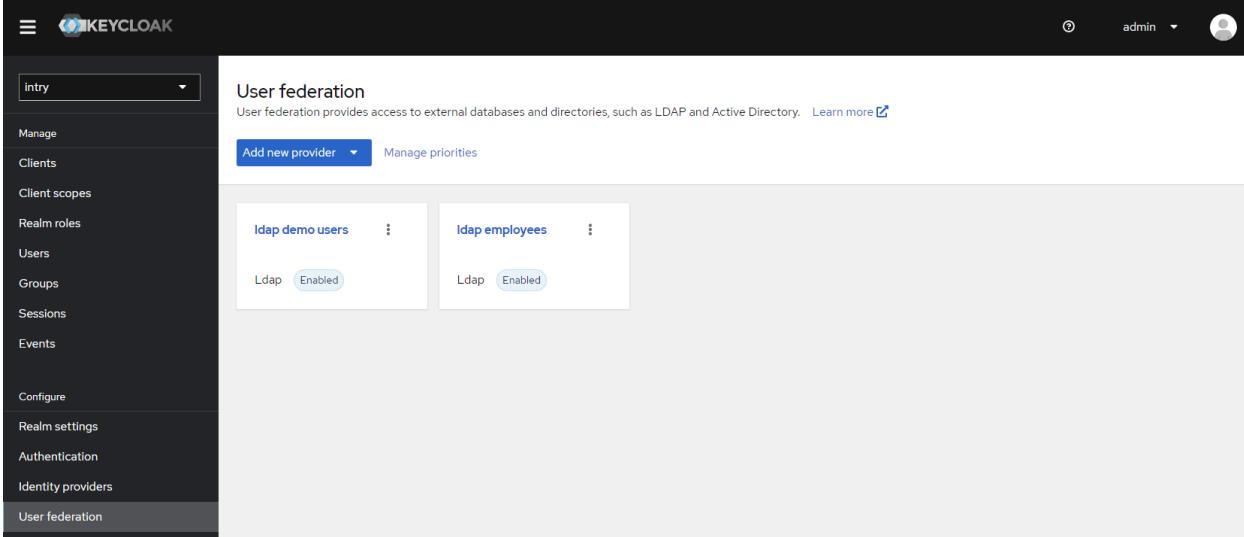
Below this, under 'Synchronization settings', there are five toggle switches:

- 'Import users': On
- 'Sync Registrations': On
- 'Batch size': (empty input field)
- 'Periodic full sync': Off
- 'Periodic changed users sync': Off

At the bottom are 'Save' and 'Cancel' buttons.

Рисунок 20 Страница настройки LDAP подключения (часть2)

После добавления LDAP провайдера – он будет отображаться на странице **User federation**.



The screenshot shows the 'User federation' page. The sidebar is identical to the previous one. The main area has a title 'User federation' with a subtitle explaining it provides access to external databases and directories. It includes a 'Learn more' link. Below this are two cards representing LDAP providers:

- 'ldap demo users': Ldap, Enabled
- 'ldap employees': Ldap, Enabled

At the top of this section are buttons for 'Add new provider' and 'Manage priorities'.

Рисунок 21 Добавленые LDAP подключения в федерации пользователей

7.2 НАСТРОЙКА ШЛЮЗА (NGINX)

Для успешного маршрутизации запросов необходимо выполнить настройки для службы nginx.

1. Необходимо скопировать настройки для сайтов в папку /nginx/conf
2. Выпустить ssl-сертификат или использовать имеющийся

7.3 НАСТРОЙКА INTRY FILES (MINIO)

Для выполнения настроек необходимо перейти на сайт MinIO. По умолчанию это <minio_url>:9090

7.3.1 Создание бакета

Далее следует создать бакет и назвать его **intry**.

Для этого необходимо нажать «**Create bucket**»

The screenshot shows the MinIO Object Browser interface. On the left, there is a dark sidebar with various navigation options: User (Object Browser, Access Keys, Documentation), Administrator (Buckets, Policies, Identity, Monitoring, Events, Tiering, Site Replication, Settings). The main area is titled 'Object Browser' and contains a 'Buckets' section. It includes a brief description: 'MinIO uses buckets to organize objects. A bucket is similar to a folder or directory in a filesystem, where each bucket can hold an arbitrary number of objects.' Below this is a link 'To get started, [Create a Bucket](#)'. At the bottom of the main area, there is a small circular progress bar icon.

Рисунок 22 Страница создания бакета

На следующей странице ввести в **BucketName** значение «**intry**», включить версионность и нажать «**Create bucket**».

The screenshot shows the 'Create Bucket' page within the MinIO Object Browser. The sidebar on the left is identical to the previous screenshot. The main form has a title 'Create Bucket'. It contains a 'Bucket Name*' field with the value 'intry'. Below it is a 'Features' section with four toggle switches: 'Versioning' (ON), 'Object Locking' (OFF), 'Quota' (OFF), and 'Retention' (OFF). At the bottom right of the form are two buttons: 'Clear' and 'Create Bucket' (in a dark blue button). To the right of the form is a 'Buckets' sidebar with the same descriptive text and 'Create a Bucket' link as the previous screenshot. Below the sidebar, there are three detailed descriptions: 'Versioning', 'Object Locking', and 'Retention'.

Инструкция по установке и настройке решения

Рисунок 23 Страница созданного бакета

7.3.2 Создание ключей доступа

Приложение API подключается к MinIO по 9000 порту с использованием access_key_id и secret_access_key, что является типичными подключением к S3-совместимому хранилищу.

Ключ доступа можно создать глобально либо привязанными к конкретному пользователю. Мы рекомендуем создать «системного пользователя», выдать ему права и затем сгенерировать ключ.

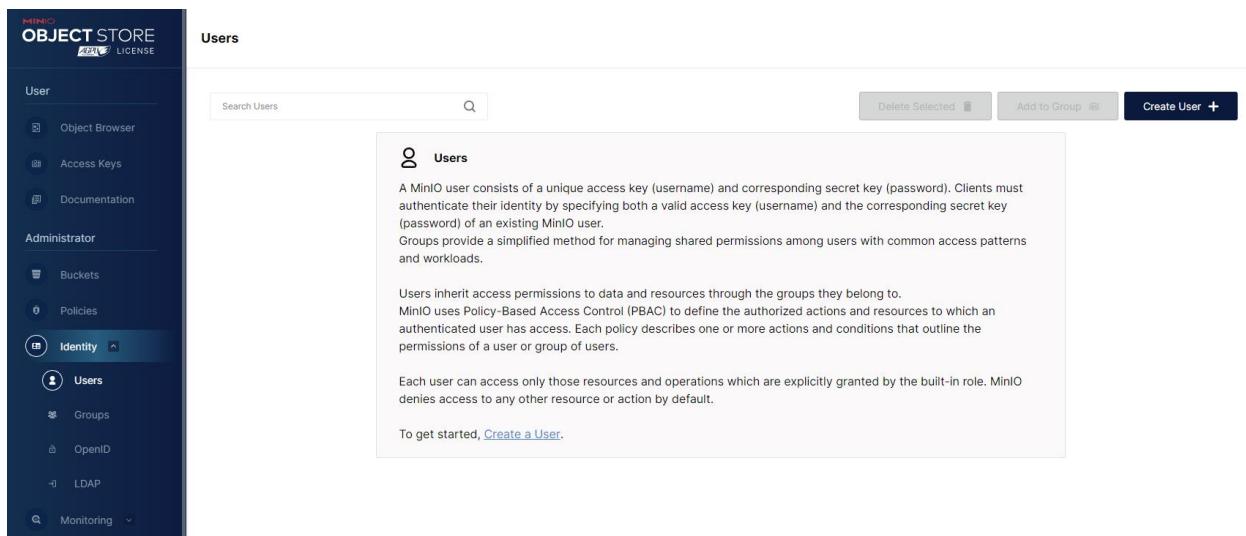


Рисунок 24 Страница списка пользователей

На странице создания пользователя указать User Name (имя), Password (пароль) и отметить права **readwrite**.

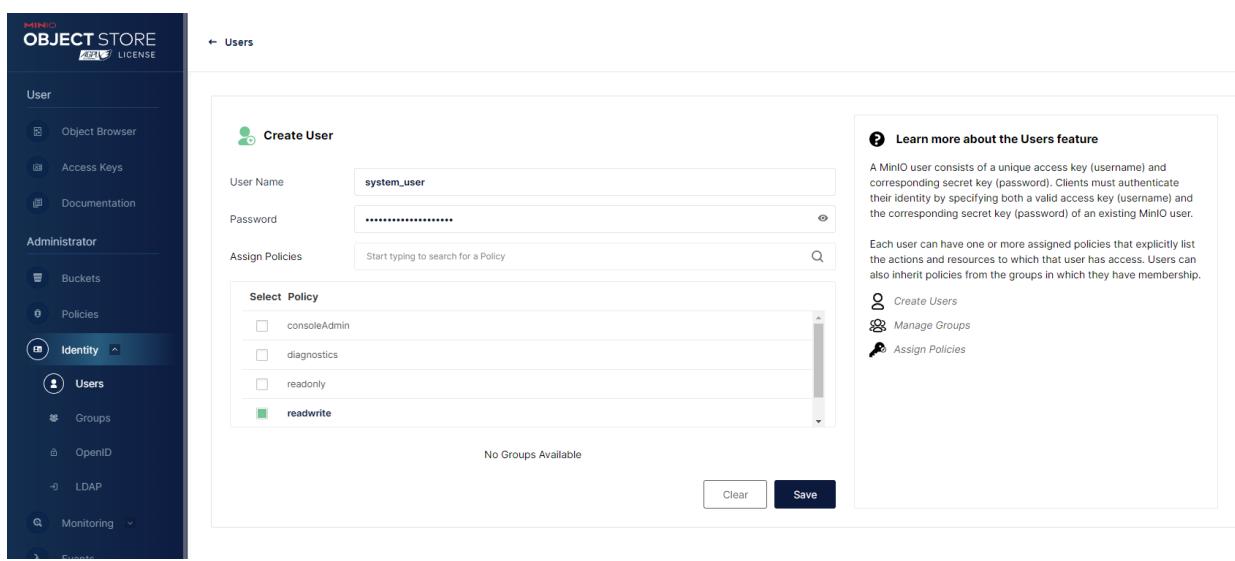


Рисунок 25 Страница создания пользователя

После создания пользователя необходимо в него перейти и выбрать Service Accounts. На данной странице нажать Create Access Key.

Инструкция по установке и настройке решения

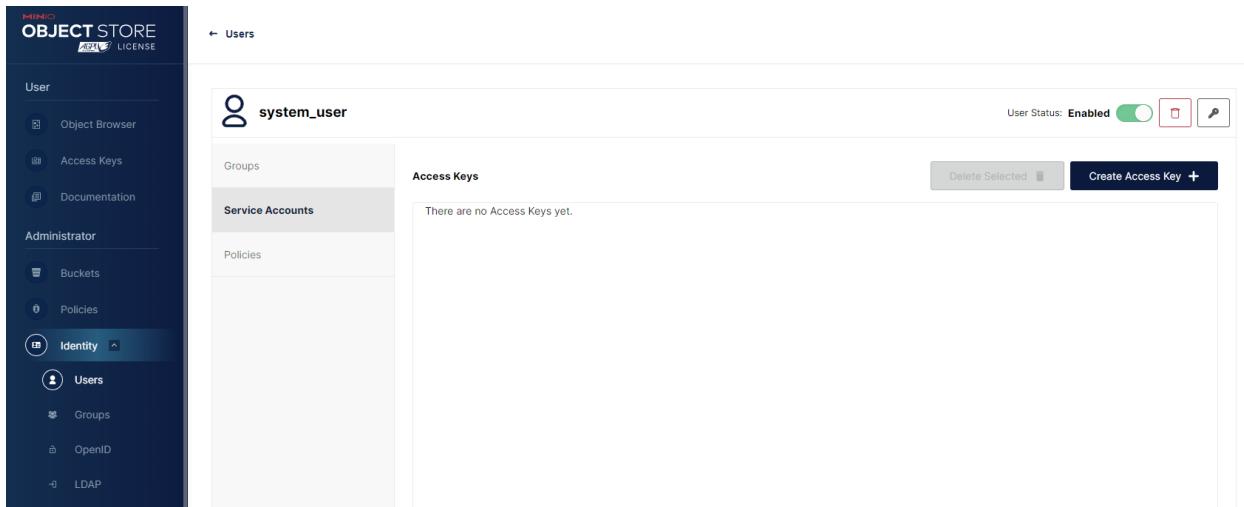


Рисунок 26 Страница списка ключей доступа для пользователя

Ключ и секрет сгенерируются автоматически. Их необходимо будет записать, т. к. секрет после создания посмотреть невозможно.

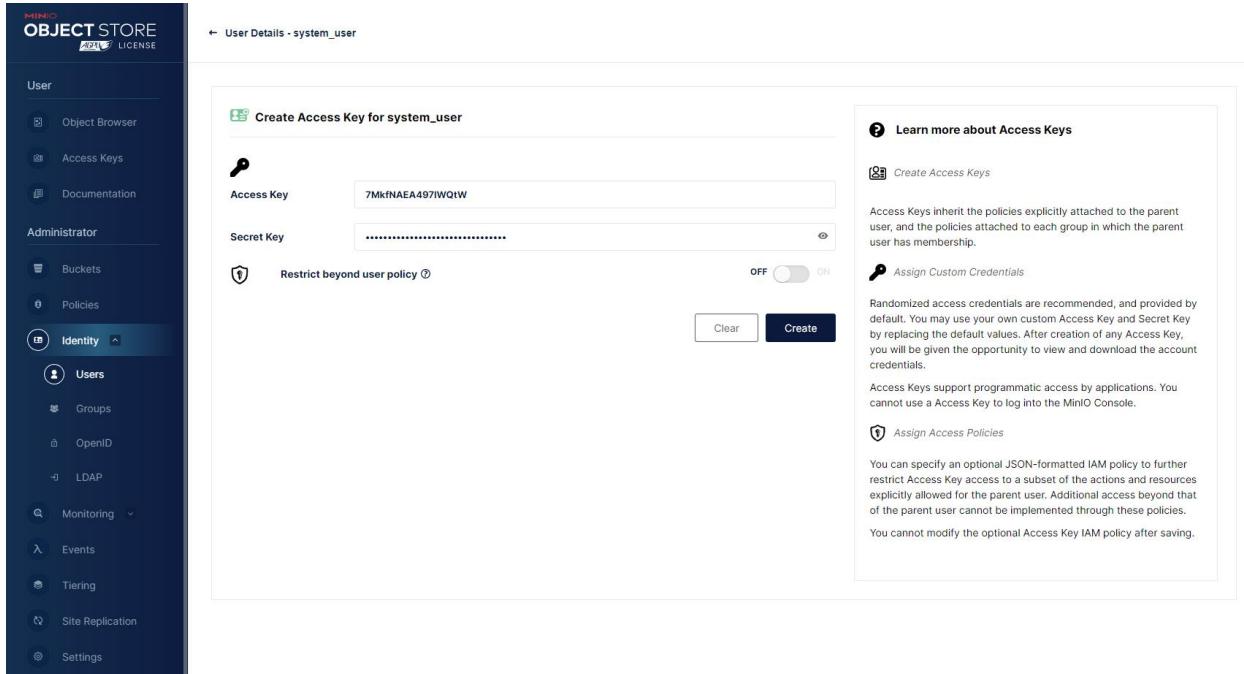


Рисунок 27 Страница создания ключа доступа

В дальнейшем можно просматривать и администрировать файлы через данный интерфейс.

Инструкция по установке и настройке решения

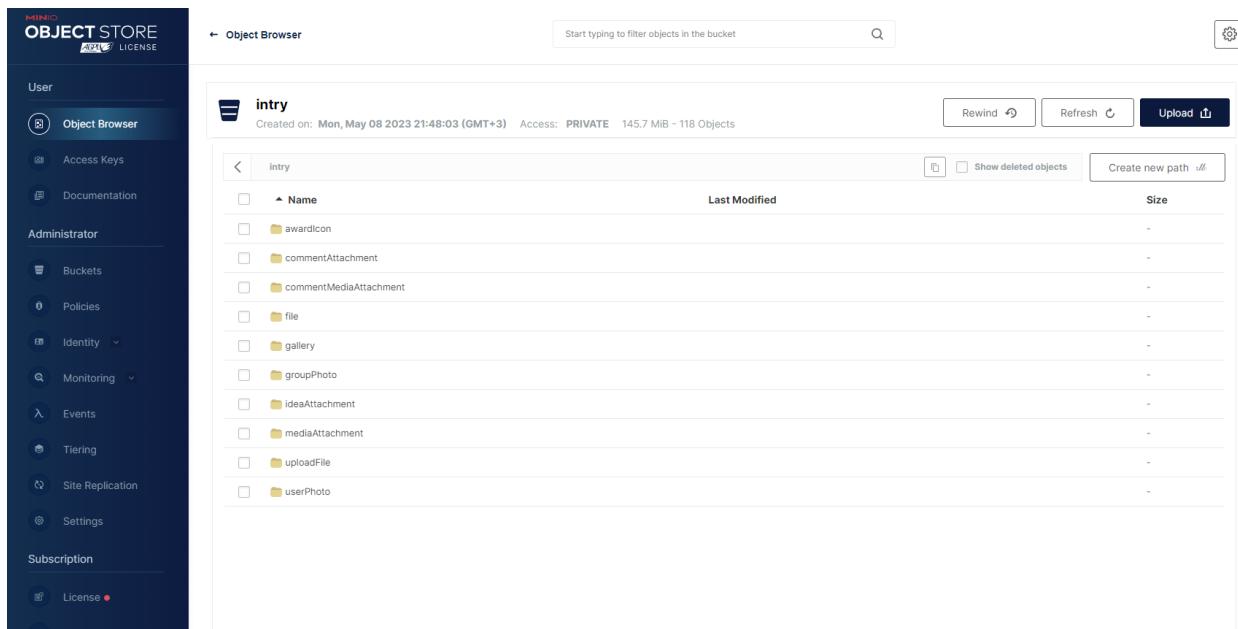


Рисунок 28 Проводник по данным в бакете