

# Аутентификация OIDC

## Общие сведения

Система позволяет использовать метод аутентификации OIDC со следующими ограничениями.

- Полноценная учетная запись пользователя не может быть создана в системе со стороны провайдера аутентификации. Если аутентифицирующийся пользователь не имеет учетной записи в системе, учетная запись будет создана без ролей, принадлежности к группам и правил ограничений данных для датасетов.
- Учетная запись пользователя не может быть удалена из системы провайдером аутентификации.
- При выходе из системы сообщение о завершении сессии не отправляется провайдеру аутентификации, что в свою очередь не позволяет:
  - завершить сессию и начать новую под другим пользователем – сессия завершится по истечении срока сессии, установленного в провайдере;
  - использовать единый выход.
- При завершении сессии в провайдере аутентификации система не получает сообщения о завершении сессии.



Провайдер OIDC генерирует и сохраняет токен сессии Open ID. Данный токен по умолчанию будет использоваться при проверке прав доступа пользователя к опубликованным компонентам или встроенным пользовательским компонентам из сторонних систем, использующих тот же провайдер Open ID.

Если система устанавливается [из пакетов](#), то при настройке аутентификации OIDC необходимо внести изменения в конфигурацию веб-сервера nginx:

```
/etc/nginx/conf.d/polymatica.conf:  
  
proxy_buffer_size 4k|8k;  
proxy_busy_buffers_size 8k|16k;
```

Это позволит осуществлять аутентификацию даже при очень длинных токенах.

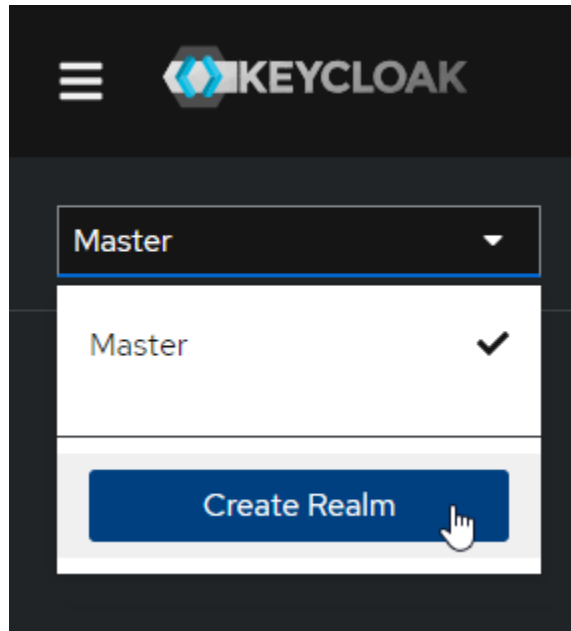
## Настройка провайдера аутентификации на примере Keycloak

Для примера настроим провайдера аутентификации Keycloak для одной системы Polymatica Dashboards (далее – система), чтобы использовать провайдера для аутентификации в системе.

Для настройки нужно иметь доступ к консоли администратора Keycloak (далее – консоль администратора). При настройке будем обращаться к документации [Keycloak](#), стандарту [RFC6749](#) и документации [OpenID Foundation](#), актуальным на момент написания.

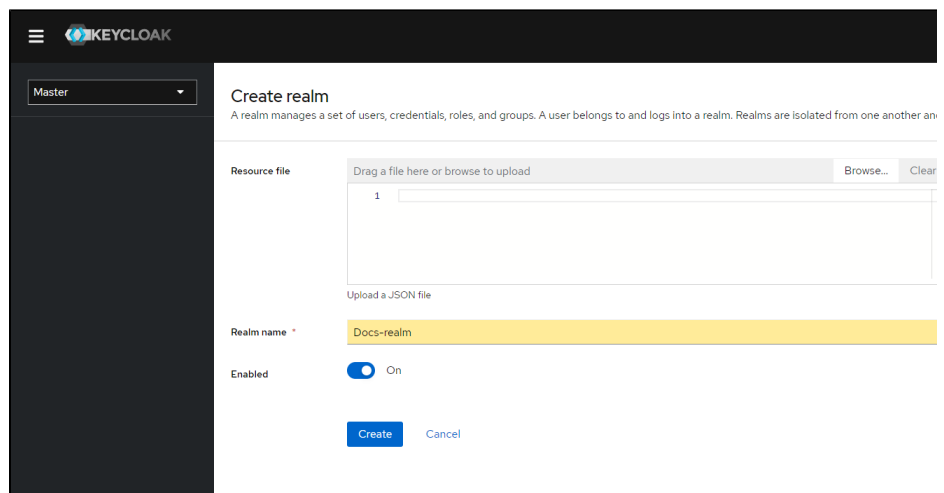
1. Создаем новую область ([realm](#)). Область определяет границы взаимодействия систем, пользователей этих систем, их права, роли и т. п.

В консоли администратора, в левом верхнем углу страницы кликаем выпадающий список и кликаем в нем кнопку **Create Realm**.



Выпадающий список областей

Далее на открывшейся справа странице Create Realm вводим в поле **Realm name** название области и кликаем кнопку **Create**.



Страница Create realm

2. Настроим область: установим название, отображаемое на странице аутентификации. А также скопируем значение для параметра "provider\_issuer", который потребуется задать позже при настройке метода аутентификации в системе.

В навигационной панели в левой части страницы кликаем вкладку **Realm settings**. На открывшейся справа странице, в поле **HTML Display name** вводим название для отображения на странице аутентификации – Polymatica. Кликаем кнопку **Save**.

The screenshot shows the Keycloak administration interface for the 'Docs-realm'. The left sidebar contains navigation links: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings (selected), Authentication, Identity providers, and User federation. The main content area is titled 'Docs-realm' and includes a sub-header 'Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. Learn more'. Below this is a tabbed interface with tabs: General, Login, Email, Themes, Keys, Events, Localization, Security defenses, Sessions, Tokens, Client policies, and User registration. The 'General' tab is active, showing fields for 'Real ID' (Docs-realm), 'Display name', 'HTML Display name' (Polymatica), 'Frontend URL', and 'Require SSL' (External requests). There is also a section for 'ACR to LoA Mapping' with 'Key' and 'Value' input fields, and a toggle for 'User-managed access' (Off). At the bottom, there are links for 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata', and 'Save' and 'Revert' buttons.

Вкладка *Realm settings*. В заголовке вкладки отображается название области

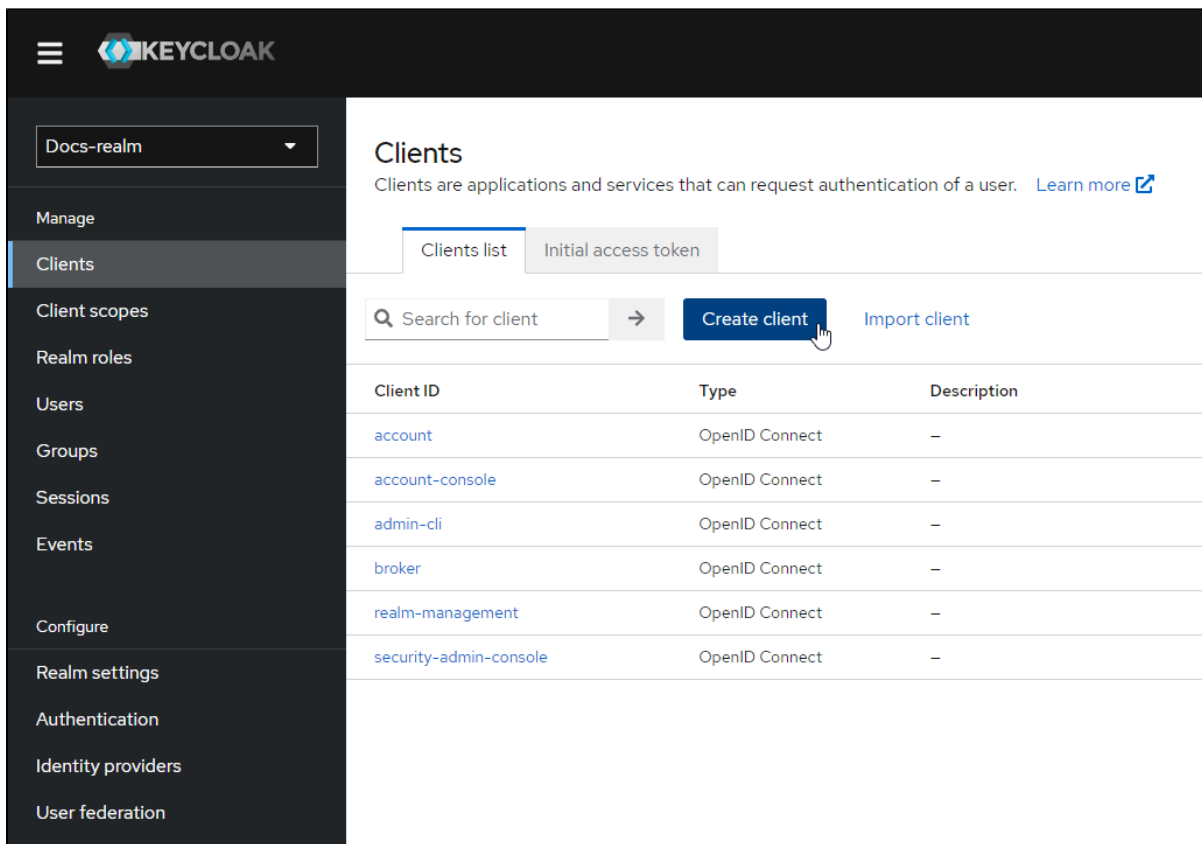
Кликаем внизу страницы ссылку **OpenID Endpoint Configuration**, чтобы открыть **метаданные провайдера**, в открывшейся вкладке браузера находим ключ **"issuer"** (обычно самый верхний после начала) и копируем значение, в нашем случае `"https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm"`.

```
1 {  
2   "issuer": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm",  
3   "authorization_endpoint": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm/pr  
4   "token_endpoint": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm/protocol/o  
5   "introspection_endpoint": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm/pr  
6   "userinfo_endpoint": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm/protoco  
7   "end_session_endpoint": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm/prot
```

Копируем значение ключа `"issuer"` для дальнейшего использования в параметре `"provider_issuer"`

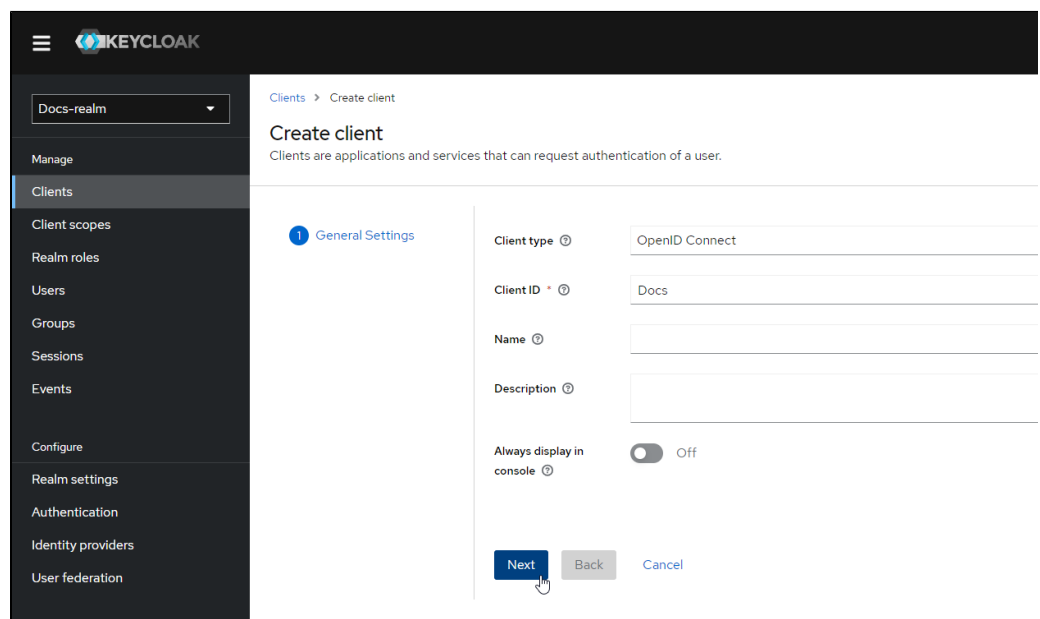
3. Добавим систему в область.

В навигационной панели в левой части страницы кликаем вкладку **Clients**. На открывшейся справа странице кликаем кнопку **Create client**.



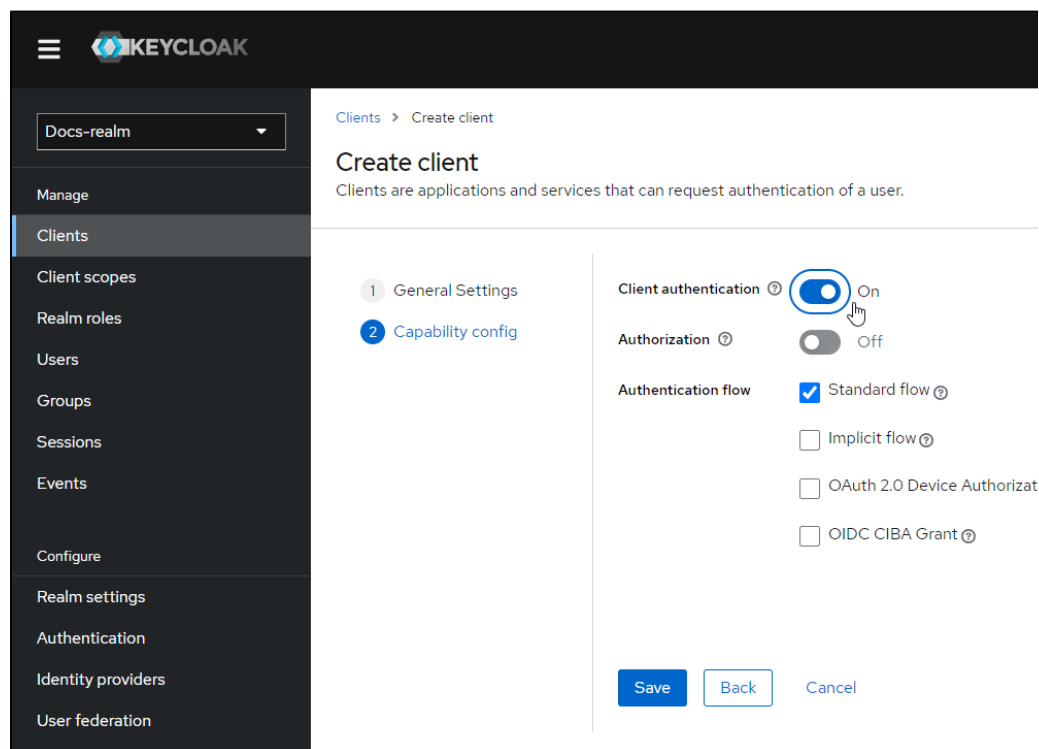
Кнопка *Create client* на странице *Clients*

На открывшейся странице заполняем произвольным значением поле **Client ID** и кликаем внизу кнопку **Next**.



Заполнили поле *Client ID* понятным нам произвольным значением

На открывшейся странице переводим переключатель **Client authentication** в положение **On** и кликаем внизу кнопку **Save**. Параметр **Client authentication** определяет используемый *тип клиента* [OpenID Connect](#).



*Перевели переключатель Client authentication в положение On*

4. Настроим добавленную систему: укажем допустимые адреса переадресации для перехода после аутентификации.

На странице системы Docs находим поле **Valid redirect URIs**. Так как мы используем тип клиента confidential, то адрес переадресации может быть любым: ставим символ «\*», что означает — любое значение. Кликаем внизу кнопку **Save**.

Docs-realm

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Clients > Client details

Docs OpenID Connect

Clients are applications and services that can request authentication of a user.

Settings Keys Credentials Roles Client scopes Sessions Advanced

General Settings

Client ID \* Docs

Name

Description

Always display in console Off

Access settings

Root URL

Home URL

Valid redirect URIs \*

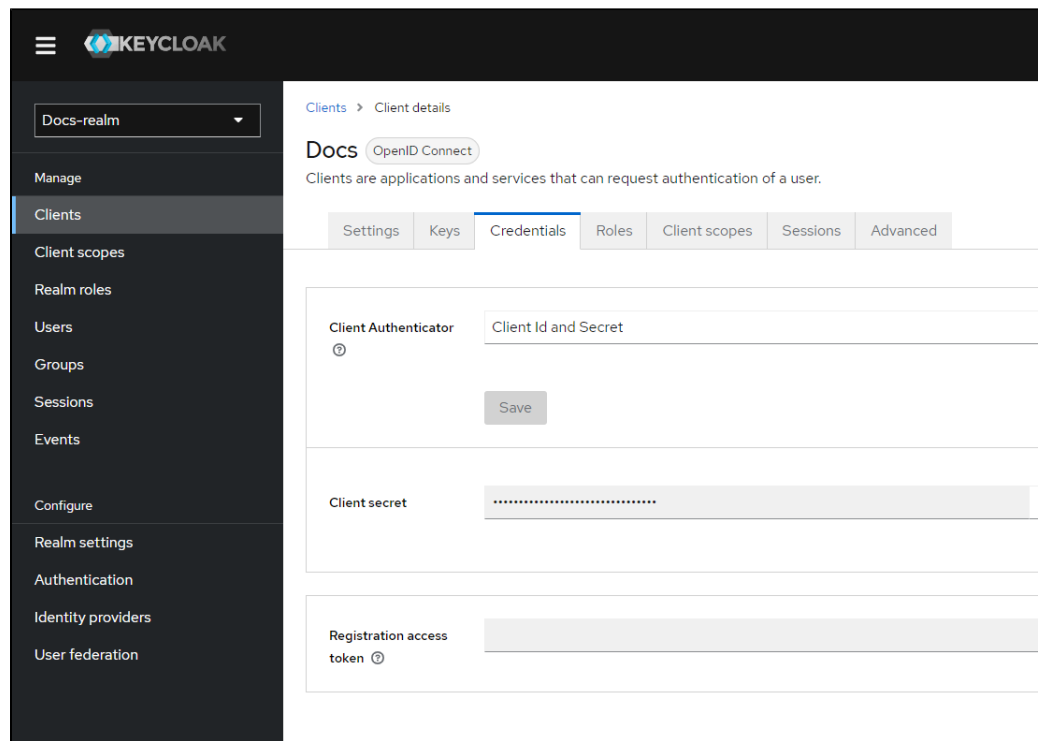
[Add valid redirect URIs](#)

Save Revert

*Добавили допустимый адрес переадресации*

5. Скопируем из добавленной системы значение для параметра "provider\_client\_secret", который потребуется задать позже при настройке метода аутентификации в системе.

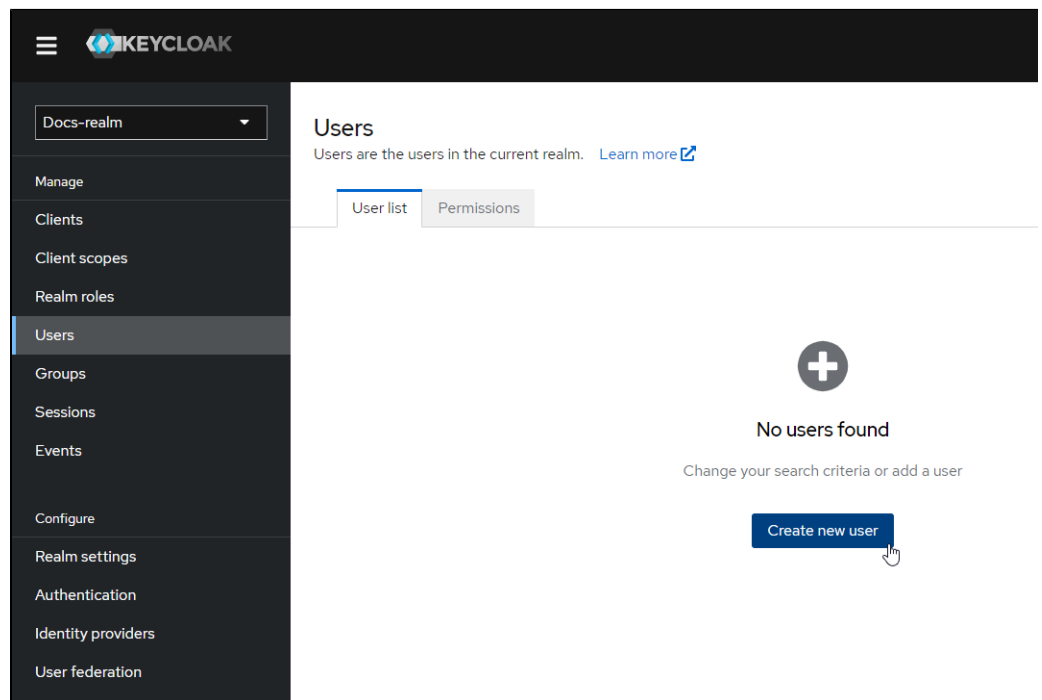
Переходим на странице системы Docs в секцию **Credentials**. Находим поле **Client secret** и в правой его части кликаем кнопку **Copy to clipboard**. Сохраняем скопированное значение в файл, чтобы не потерять (например, в блокнот).



Скопировали Client secret

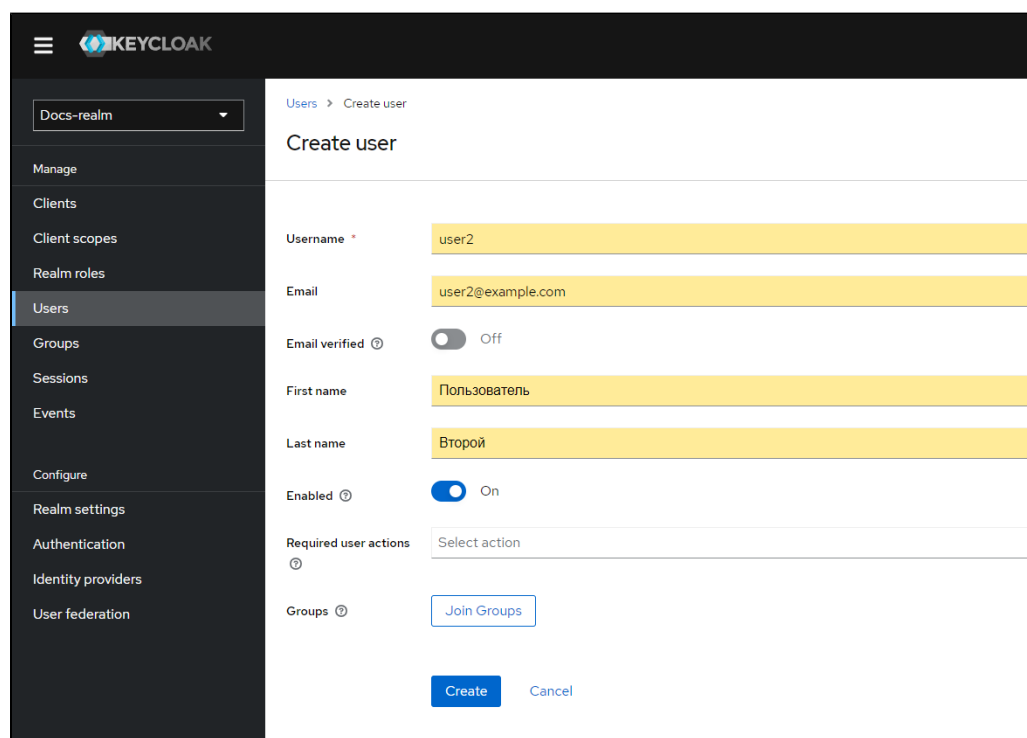
6. Добавим учетную запись пользователя системы. Если учетная запись не существует в системе, она автоматически создается с ограничениями: заполняются только поля «Логин» и «E-mail», учетная запись не имеет ролей.

В навигационной панели в левой части страницы кликаем вкладку **Users**. На открывшейся справа странице Users кликаем кнопку **Create new user**.



Кликаем кнопку Create new user

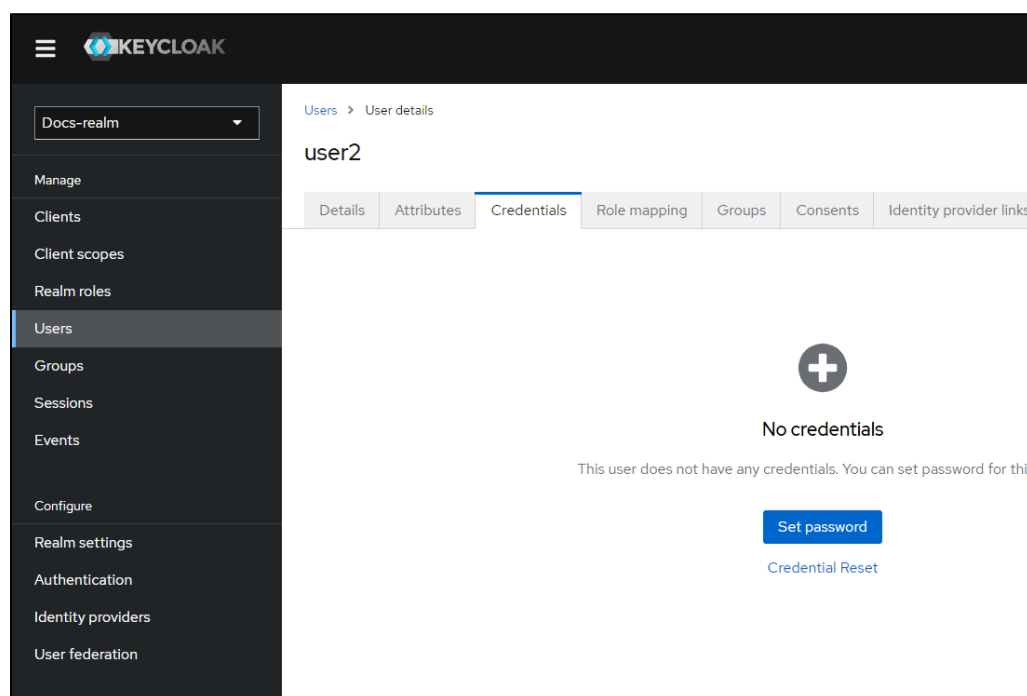
На открывшейся странице Create user заполняем все поля формы, в том числе поля First name и Last name, что позволит, когда поддержка передаваемых полей будет доработана, не возвращаться к заполнению этих полей. После заполнения полей кликаем внизу кнопку **Create**.



The screenshot shows the 'Create user' page in the Keycloak administration console. The left sidebar contains a menu with options like Manage, Clients, Client scopes, Realm roles, Users (selected), Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'Create user' and contains several input fields: Username (filled with 'user2'), Email (filled with 'user2@example.com'), Email verified (toggle switch set to 'Off'), First name (filled with 'Пользователь'), Last name (filled with 'Второй'), Enabled (toggle switch set to 'On'), Required user actions (dropdown menu set to 'Select action'), and Groups (button labeled 'Join Groups'). At the bottom right, there are two buttons: 'Create' (highlighted in blue) and 'Cancel'.

*Заполнили поля формы учетными данными пользователя*

На открывшейся странице с логином пользователя в заголовке перейдем в секцию **Credentials** и кликнем на ней кнопку **Set password**.

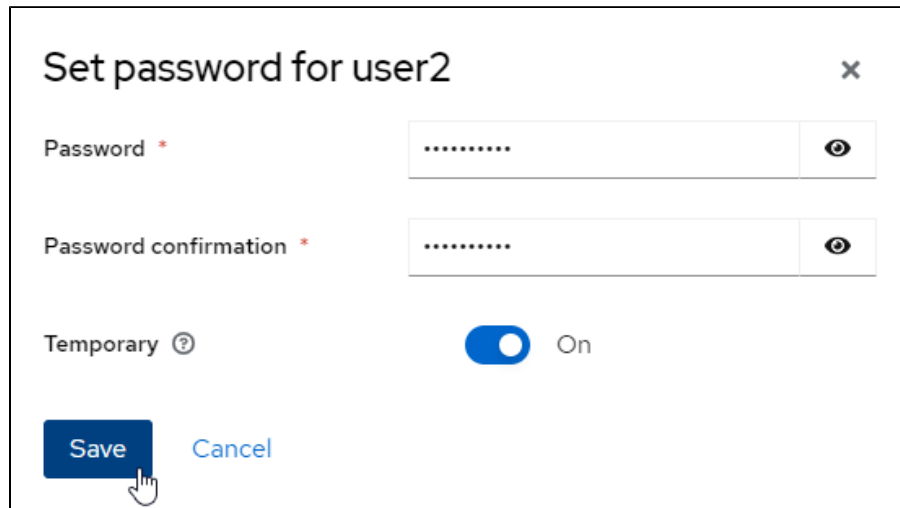


The screenshot shows the 'User details' page for 'user2' in the Keycloak administration console. The left sidebar is the same as in the previous screenshot. The main content area has a breadcrumb 'Users > User details' and the username 'user2'. Below this is a tabbed interface with tabs for Details, Attributes, Credentials (selected), Role mapping, Groups, Consents, and Identity provider links. The 'Credentials' tab displays a large plus icon in a circle, the text 'No credentials', and a message: 'This user does not have any credentials. You can set password for this'. Below the message is a blue button labeled 'Set password' and a link labeled 'Credential Reset'.

*Секция Credentials страницы пользователя*

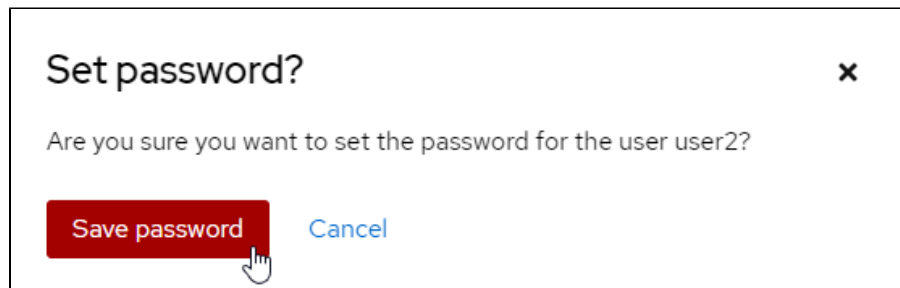
В открывшемся окне **Set password** укажем в обоих полях временный пароль учетной записи для входа в систему и нажмем кнопку **Save**.

Чтобы использовать установленный пароль в качестве постоянного, следует выключить параметр **Temporary**.



Окно установки пароля учетной записи

Подтвердим установку пароля – нажмем кнопку **Save password**.



Учетная запись пользователя готова. При первой аутентификации пользователю будет предложено сменить временный пароль, если параметр **Temporary** был оставлен включенным.

На этом шаге мы завершили настройку провайдера аутентификации Keycloak для системы. Далее необходимо настроить метод аутентификации OIDC в системе.

## Настройка метода аутентификации OIDC в системе

Чтобы включить в системе метод аутентификации OIDC, выполните следующие действия.

1. Добавьте SSL-сертификат провайдера аутентификации.

- Для системы, установленной с использованием пакетов:

- i. Добавьте сертификат в директорию `/usr/local/share/ca-certificates/` операционной системы окружения.
- ii. Выполните команду:

```
update-ca-certificates
```

- Для системы, установленной с использованием Docker:

- i. Добавьте сертификат в скрипт:

```
#!/bin/bash

echo "inserting certificate"

cat << EOF >> /usr/local/share/ca-certificates/.cert
-----BEGIN CERTIFICATE-----
_
-----END CERTIFICATE-----
EOF

echo "updating CA"
update-ca-certificates

exit 0
```

где сертификат – файл, в который следует записать сертификат;

тело\_сертификата – содержимое сертификата.

- ii. Добавьте скрипт для выполнения в контейнер сервиса manager (см. [Приложение В. Выполнение скрипта в контейнере сервиса при запуске контейнера](#)).

2. Укажите параметры метода аутентификации OIDC в конфигурации системы в файле oidc-providers.json (см. [Параметры конфигурации](#)). Требуется указать следующие параметры и их значения.

```
[
  {
    "auth_method_active": true,
    "provider_issuer": "https://dev-keycloak.polymatica.ru/auth/realms/Docs-realm",
    "provider_redirect_url": "https://stage-docs.platform.polymatica.ru/auth/oidc-callback",
    "provider_client_id": "Docs",
    "provider_client_secret": "jmMEby8L9Jo0TNweolgSiLaXR4AEGNna",
    "provider_scope": "openid profile email",
    "provider_name": "keycloak_OP",
    "provider_type": "keycloak",
    "provider_claims": {
      "preferred_username_key": "preferred_username",
      "email_key": "email",
      "first_name_key": "firstName",
      "middle_name_key": "middle_name",
      "last_name_key": "lastName"
    }
  }
]
```

где "provider\_name" – произвольно выбранное наименование провайдера аутентификации;  
 "provider\_type" – тип провайдера;  
 "provider\_issuer" – значение ключа **issuer** в [метаданных провайдера](#);  
 "provider\_redirect\_url" – адрес клиента для перенаправления после успешной аутентификации в провайдере, должен иметь вид `https://  
 /auth/oidc-callback`;  
 "provider\_scope" – запрашиваемые системой доступы;  
 "provider\_client\_id" – **Client ID**, заданный при настройке провайдера;  
 "provider\_client\_secret" – **Client secret**, полученный при настройке провайдера;  
 "preferred\_username\_key" – параметр, определяющий логин пользователя системы, в который передаем значение ключа **preferred\_username** из токена;  
 "email\_key" – параметр, определяющий e-mail пользователя системы, в который передаем значение ключа **email** из токена;  
 "first\_name\_key" – параметр, определяющий имя пользователя системы, в который передаем значение ключа **given\_name** из токена;  
 "last\_name\_key" – параметр, определяющий фамилию пользователя системы, в который передаем значение ключа **family\_name** из токена;  
 "middle\_name\_key" – параметр, определяющий отчество пользователя системы, в который передаем значение ключа **middle\_name** из токена.

### 3. Перезапустите систему.

- Для системы, установленной с использованием пакетов, выполните команду:

```
systemctl restart polymatica-platform-manager
```

- Для системы, установленной с использованием Docker, выполните команду:

```
cd /srv/platform && docker compose up -d --remove-orphans || docker-compose up -d --remove-orphans
```

При правильно выполненной настройке на странице входа в систему должна отображаться вкладка «OpenID»:



Вкладка «OpenID» слева от вкладки «Стандартный»

По клику вкладки выполняется переадресация на страницу аутентификации OIDC-провайдера.

## Настройка нескольких провайдеров

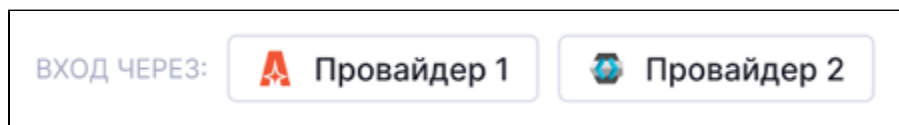
Система позволяет настроить несколько провайдеров (см. [Руководство пользователя Polymatica Dashboards](#) - "Вход в систему" - "Вход по Open ID" - "Несколько провайдеров"). Все параметры задаются в файле [oidc-providers.json](#) для каждого провайдера, как показано в примере ниже:

Пример файла `oidc-providers.json` при настройке нескольких провайдеров

```
[
  {
    "auth_method_active": true,
    "insecure_override_issuer": false,
    "provider_issuer": "https://keycloak.example.ru/realms/platform",
    "provider_actual_issuer": "",
    "provider_redirect_url": "http://host.docker.internal:4300/auth/oidc-callback",
    "provider_logout_url": "https://keycloak.example.ru/realms/platform/protocol/openid-connect/logout",
    "provider_client_id": "Client1",
    "provider_client_secret": "",
    "provider_scope": "openid profile email",
    "provider_type": "keycloak",
    "provider_name": "Keycloak",
    "provider_icon": "/static/oidc-providers/keycloak.svg",
    "provider_claims": {
      "preferred_username_key": "preferred_username",
      "email_key": "email",
      "first_name_key": "firstName",
      "middle_name_key": "middleName",
      "last_name_key": "lastName"
    }
  },
  {
    "auth_method_active": true,
    "insecure_override_issuer": false,
    "provider_issuer": "https://avanpost.example.ru/realms/platform",
    "provider_actual_issuer": "",
    "provider_redirect_url": "http://host.docker.internal:4300/auth/oidc-callback",
    "provider_logout_url": "https://avanpost.example.ru/realms/platform/protocol/openid-connect/logout",
    "provider_client_id": "Client2",
    "provider_client_secret": "",
    "provider_scope": "openid profile email",
    "provider_type": "avanpost",
    "provider_name": "Avanpost",
    "provider_icon": "/static/oidc-providers/avanpost.svg",
    "provider_claims": {
      "preferred_username_key": "preferred_username",
      "email_key": "email",
      "first_name_key": "firstName",
      "middle_name_key": "middleName",
      "last_name_key": "lastName",
      "group_key": "sia_groups",
      "role_key": "sia_role"
    },
    "provider_auto_create_user": false,
    "provider_groups_whitelist": ""
  }
]
```

Текст на кнопке входа задается параметром `"provider_name"`. Если заданный текст не помещается на кнопке, он сокращается многоточием.

Кроме того, на кнопку можно добавить логотип, который будет отображаться слева от текста:



Логотипы на кнопках входа

В системе есть два предустановленных логотипа (для Keycloak и Avanpost). Чтобы выбрать один из них, нужно задать в параметре `"provider_icon"` значение `"/static/oidc-providers/keycloak.svg"` или `"/static/oidc-providers/avanpost.svg"` соответственно. Также система позволяет загрузить пользовательский логотип. Для этого нужно в директорию `/usr/share/polymatica/platform/file-storage/assets/oidc-providers` положить выбранный файл в формате SVG и задать значение параметра `"/static/oidc-providers/<FILE_NAME_EXAMPLE>.svg"`.

Рекомендации к загружаемому изображению:

- максимальный размер файла — не более 100 КБ;
- рекомендуемые размеры — 24×24 px или 32×32 px;
- соотношение сторон — 1:1 (квадрат);
- фон — прозрачный или нейтральный;
- изображение должно сохранять читаемость при масштабировании.

## Аутентификация OIDC по умолчанию

Перед использованием метода аутентификации OIDC по умолчанию убедитесь, что метод настроен.

Чтобы установить метод аутентификации OIDC выбранным по умолчанию, в конфигурации системы укажите параметр со значением:

```
POLYMATICA_CORE_AUTH_DEFAULT_METHOD=openIDConnect
```

В случае, когда в системе настроено сразу несколько OIDC-провайдеров, необходимо также выбрать провайдер, который будет использоваться по умолчанию. Для этого нужно дополнительно заполнить параметр конфигурации POLYMATICA\_CORE\_AUTH\_DEFAULT\_PROVIDER, указав для него то же значение, которое указано в параметре "provider\_type" из [файла oidc-providers.json](#):

```
POLYMATICA_CORE_AUTH_DEFAULT_METHOD=openIDConnect  
POLYMATICA_CORE_AUTH_DEFAULT_PROVIDER=<provider_type>
```

После этого нужно перезапустить систему.

При правильно выполненной настройке страница входа в систему должна открываться на вкладке "OpenID", после чего автоматически выполняется переадресация на страницу аутентификации OIDC-провайдера.



Можно отключить появление страницы аутентификации провайдера, задав в [файле oidc-providers.json](#) параметры "provider\_skip\_token\_check" и "provider\_use\_token\_auth". Тогда при переходе из сторонней системы сразу будет открываться окно авторизации Polymatica Dashboards.

## Авторизация при переходе по внешней ссылке

Система позволяет настроить автоматическую авторизацию через провайдера OpenID Connect при переходе пользователем по ссылке на проект или слой проекта. Для этого к адресу ссылки необходимо добавить query-параметр, содержащий идентификатор одного из настроенных провайдеров, через которого должна произойти авторизация.

Например:

<https://example.polymatica.dashboards.server/dashboard/project/177938?provider=avanpost>

<https://example.polymatica.dashboards.server/dashboard/project/177938/layer/2?provider=avanpost>

В качестве значения query-параметра передается значение, которое указано в параметре "provider\_type" из [файла oidc-providers.json](#).

## Настройка атрибутов пользователя на примере Keycloak

Атрибут пользователя — это параметр, описывающий конкретное свойство пользователя в системе. Атрибуты используются для идентификации, классификации, персонализации и управления взаимодействием с пользователем. В Polymatica Dashboards атрибуты используются в атрибутивных правилах для быстрой настройки доступа к данным датасета. Атрибуты в системе делятся на автоматически синхронизируемые атрибуты и атрибуты с ручной настройкой. Автосинхронизируемые атрибуты связаны с ключом IAM, передаваемым в токене пользователя при авторизации через IAM-провайдера. Подробнее о работе атрибутов в системе см. в [руководстве пользователя](#) в разделах "Пользователи" - "Создание пользователя" и "Датасеты" - "Настройка датасета" - "Функции рабочей области" - "Ограничение данных".

Для настройки автоатрибута на стороне Keycloak нужно выполнить следующее:

1. Перейти в **Realm settings**.

platform

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

platform

Realm settings are settings that control the options for users, applications, roles, and groups in the cur

GeneralLoginEmailThemesKeysEventsLocalizationSecurity defe

Realm ID \*

platform

Display name

HTML Display name

Frontend URL ?

Require SSL ?

External requests

ACR to LoA Mapping ?

No ACR to LoA Mapping have been defined yet. Click the below button to add ACR to LoA Mapping. (Email and Password value are required for a key pair.)

+ Add ACR to LoA Mapping

User-managed access ?

Off

Unmanaged Attributes ?

Disabled

Раздел Realm settings

2. Перейти на вкладку **User profile**.

platform

platform

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Attributes

Attributes Group

JSON editor

All groups

Create attribute

|   | Attribute [Name] | Display name  | Attribute group |
|---|------------------|---------------|-----------------|
| ⋮ | username         | \${username}  |                 |
| ⋮ | email            | \${email}     |                 |
| ⋮ | firstName        | \${firstName} |                 |
| ⋮ | lastName         | \${lastName}  |                 |
| ⋮ | new_attr         |               |                 |
| ⋮ | new_attr_1       | new_attr_1    |                 |
| ⋮ | sia_groups       | sia_groups    |                 |

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Переход в User profile

3. Нажать на кнопку **Create attribute**.

4. Заполнить следующие поля и настроить параметры:

- **Attribute [Name]**. Имя, используемое при создании score. Значение, введенное в поле, должно совпадать со значением IAM-ключа атрибута в Polymatica Dashboards.
- **Display name**. Имя атрибута, которое будет отображаться в Keycloak.
- **Multivalued**. Включить переключатель.
- **Permission**. Проставить отметки на всех чекбоксах.

KEYCLOAK

platform

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Realm settings > User profile > Create attribute

Create attribute

Create a new attribute

General settings

Attribute [Name] \* create\_attr

Display name create\_attr

Multivalued ☒ On

Attribute group None

Enabled when ☒ Always  
☐ Scopes are requested

Required field ☐ Off

Permission

Who can edit? ☒ User ☒ Admin

Who can view? ☒ User ☒ Admin

Пример заполнения полей

5. Нажать на кнопку **Create**.

6. Перейти в **Client scopes**.

platform

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

### Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between multiple clients. [Learn more](#)

Name

Search for client scope

→

Create client scope

Change type to

Refresh

| <input type="checkbox"/> | Name             | Assigned type | Protocol       | Display order | Description                 |
|--------------------------|------------------|---------------|----------------|---------------|-----------------------------|
| <input type="checkbox"/> | acr              | Default       | OpenID Connect | –             | OpenID Connect scope        |
| <input type="checkbox"/> | address          | Optional      | OpenID Connect | –             | OpenID Connect built-in     |
| <input type="checkbox"/> | basic            | Default       | OpenID Connect | –             | OpenID Connect scope        |
| <input type="checkbox"/> | email            | Default       | OpenID Connect | –             | OpenID Connect built-in     |
| <input type="checkbox"/> | microprofile-jwt | Optional      | OpenID Connect | –             | Microprofile - JWT built-in |
| <input type="checkbox"/> | offline_access   | Optional      | OpenID Connect | –             | OpenID Connect built-in     |
| <input type="checkbox"/> | phone            | Optional      | OpenID Connect | –             | OpenID Connect built-in     |
| <input type="checkbox"/> | profile          | Default       | OpenID Connect | –             | OpenID Connect built-in     |
| <input type="checkbox"/> | region           | Default       | OpenID Connect | –             | region                      |
| <input type="checkbox"/> | role_list        | Default       | SAML           | –             | SAML role list              |

Раздел Client scopes

7. Выбрать требуемую строку (scope).

|                    |                                           |          |                |   |
|--------------------|-------------------------------------------|----------|----------------|---|
| platform           | <input type="checkbox"/> address          | Optional | OpenID Connect | – |
|                    | <input type="checkbox"/> basic            | Default  | OpenID Connect | – |
| Manage             | <input type="checkbox"/> email            | Default  | OpenID Connect | – |
| Clients            | <input type="checkbox"/> microprofile-jwt | Optional | OpenID Connect | – |
| Client scopes      | <input type="checkbox"/> offline_access   | Optional | OpenID Connect | – |
| Realm roles        | <input type="checkbox"/> phone            | Optional | OpenID Connect | – |
| Users              | <input type="checkbox"/> profile          | Default  | OpenID Connect | – |
| Groups             | <input type="checkbox"/> region           | Default  | OpenID Connect | – |
| Sessions           | <input type="checkbox"/> role_list        | Default  | SAML           | – |
| Events             | <input type="checkbox"/> roles            | Default  | OpenID Connect | – |
| Configure          | <input type="checkbox"/> sasha            | Default  | OpenID Connect | – |
| Realm settings     | <input type="checkbox"/> test             | Default  | OpenID Connect | – |
| Authentication     | <input type="checkbox"/> Test123          | Default  | OpenID Connect | – |
| Identity providers | <input type="checkbox"/> web-origins      | Default  | OpenID Connect | – |
| User federation    |                                           |          |                |   |

Пример выбора scope Test123

8. Перейти на вкладку **Mappers**.

|               |                     |              |                        |
|---------------|---------------------|--------------|------------------------|
| platform      | Settings            | Mappers      | Scope                  |
| Manage        | Q Search for mapper | →            | Add mapper             |
| Clients       | Name                | Category     | Type                   |
| Client scopes | sub                 | Token mapper | Subject (sub)          |
| Realm roles   | address             | Token mapper | User Address           |
| Users         | acr loa level       | Token mapper | Authentication Context |
| Groups        | upn                 | Token mapper | User Attribute         |
| Sessions      | nickname            | Token mapper | User Attribute         |
| Events        | var                 | Token mapper | User Attribute         |
|               | full name           | Token mapper | User's full name       |
|               | phone number        | Token mapper | User Attribute         |

Вкладка Mappers

9. Нажать на кнопку **Add mapper** и в выпадающем списке выбрать опцию **By configuration**.

10. Прокрутить содержимое вниз и выбрать опцию **User Attribute**.

## Configure a new mapper



Choose any of the mappings from this table

|                               |                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Membership              | Map user group membership                                                                                                                                                               |
| Hardcoded claim               | Hardcode a claim into the token.                                                                                                                                                        |
| Hardcoded Role                | Hardcode a role into the access token.                                                                                                                                                  |
| Nonce backwards compatible    | Adds the nonce claim to Access, Refresh and ID token                                                                                                                                    |
| Pairwise subject identifier   | Calculates a pairwise subject identifier using a salted sha-256 hash and adds it to the 'sub' claim. See OpenID Connect specification for more info about pairwise subject identifiers. |
| Role Name Mapper              | Map an assigned role to a new name or position in the token.                                                                                                                            |
| Session State (session_state) | Add Session State (session_state) claim                                                                                                                                                 |
| Subject (sub)                 | Add Subject (sub) claim                                                                                                                                                                 |
| User Address                  | Maps user address attributes (street, locality, region, postal_code, and country) to the OpenID Connect 'address' claim.                                                                |
| <b>User Attribute</b>         | Map a custom user attribute to a token claim.                                                                                                                                           |
| User Client Role              | Map a user client role to a token claim.                                                                                                                                                |
| User Property                 | Map a built in user property (email, firstName, lastName) to a token claim.                                                                                                             |
| User Realm Role               | Map a user realm role to a token claim.                                                                                                                                                 |
| User Session Note             | Map a custom user session note to a token claim.                                                                                                                                        |
| User's full name              | Maps the user's first and last name to the OpenID Connect 'name' claim. Format is <first> + ' ' + <last>                                                                                |

Выбор опции User Attribute

11. В поле **User attribute** выбрать атрибут, который создавался на шагах 4-5.

12. Заполнить следующие поля:

- **Name.**
- **Token Claim Name.**
- **Claim JSON Type.** Выбрать из выпадающего списка опцию **JSON**.
- Включить все переключатели.

platform

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Mapper type

User Attribute

Name \*

create\_attr

User Attribute

create\_attr

Token Claim Name

create\_attr

Claim JSON Type

JSON

Add to ID token

On

Add to access token

On

Add to lightweight access token

On

Add to userinfo

On

Add to token introspection

On

Multivalued

On

Aggregate attribute values

On

Save

Cancel

Пример заполнения полей

13. Нажать на кнопку **Save**.

14. Перейти в **Users**.

platform

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

## Users

Users are the users in the current realm. [Learn more](#)

User list

Default search

Search user

| <input type="checkbox"/> | Username              |
|--------------------------|-----------------------|
| <input type="checkbox"/> | akushnyr              |
| <input type="checkbox"/> | kkadmin               |
| <input type="checkbox"/> | new_test              |
| <input type="checkbox"/> | new_user_default_pass |
| <input type="checkbox"/> | oidc_user             |
| <input type="checkbox"/> | piter                 |
| <input type="checkbox"/> | platform              |
| <input type="checkbox"/> | popov-test            |
| <input type="checkbox"/> | proverka              |
| <input type="checkbox"/> | ...                   |

Раздел Users

15. Выбрать пользователя.

16. Прокрутить содержимое страницы вниз и убедиться, что новый атрибут добавлен.

create\_attr

+

Add create\_attr

Save

Revert

17. Для добавления значений атрибута нужно нажать на кнопку **+ Add <название атрибута>** и ввести в поле значения через запятую, заключив все заданные значения в квадратные скобки. Каждое строковое значение при этом заключается в кавычки. Например: ["HR","Finance","IT"], [1,2,3].