# Суперапп VK WorkSpace

## Запуск супераппа для Почты версии 26.1 и выше



Портал с документацией: https://biz.mail.ru/docs/on-premises/

# Оглавление


Назначение документа 3

Запуск Супераппа 3

- Предварительные действия 3
- Шаг 1. Создайте и настройте клиента в Keycloak 4
- Шаг 2. Настройте SSO в панели администратора VK WorkSpace 8
- Шаг 3. Выполните настройку в интерфейсе Keycloak 10
  - 1. Создайте нужные вам атрибуты 10
  - 2. Создайте записи для нужных вам атрибутов 12
  - 3. Завершите настройку 14
- Шаг 4. Активируйте вход через SSO в панели администратора 15
- Шаг 5. Убедитесь, что аутентификация через SSO работает 16

Где скачать суперапп? 16

Доступные функциональности после запуска Супераппа 17

Ограничения после запуска Супераппа 17

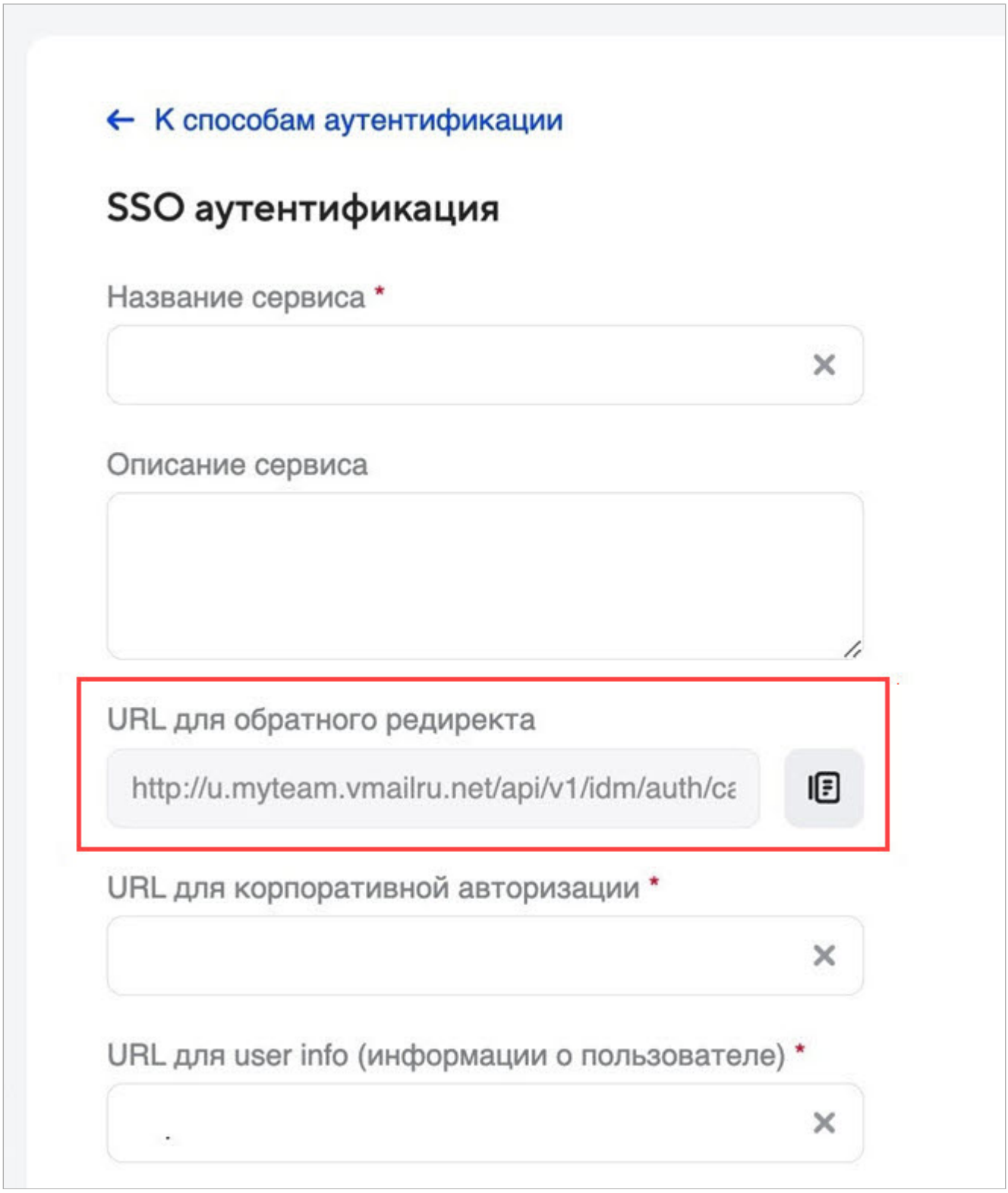
# Назначение документа

В инструкции описано, как запустить Суперапп (ранее — VK Teams) для использования Почты VK WorkSpace без функциональности мессенджера. Вы сможете пользоваться Почтой и Календарем через приложение, снизив при этом нагрузку на серверы.

# Запуск Супераппа

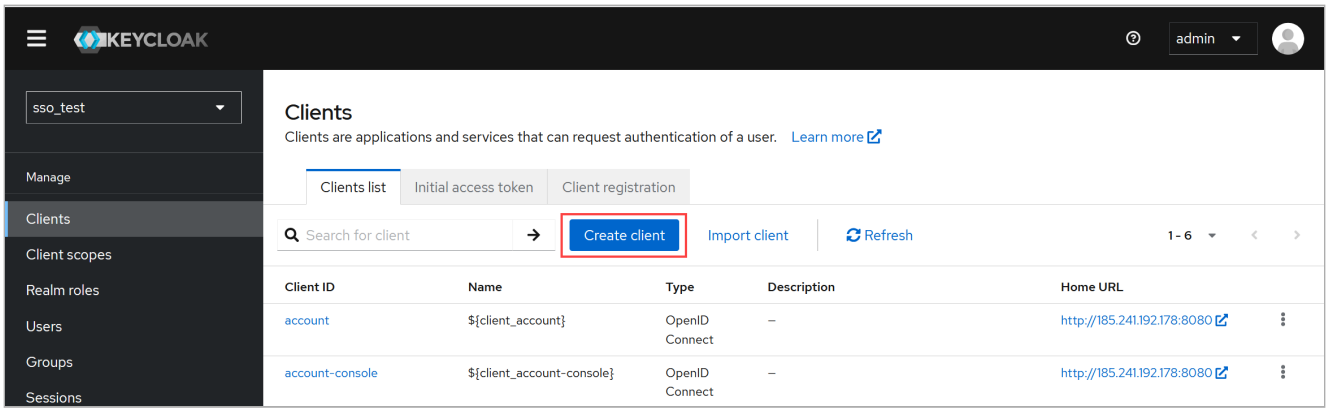
## Предварительные действия

1. Установите Почту VK WorkSpace версии 26.1 или выше по инструкции в зависимости от типа вашей инсталляции:
   - Инструкция для распределенной инсталляции
   - Инструкция для инсталляции на одну виртуальную машину
   - Инструкция для геораспределенной инсталляции
2. Откройте веб-интерфейс установщика.
3. Нажмите на кнопку  в правом верхнем углу, выберите пункт **Продукты**.
4. Перейдите на вкладку **Администрирование**.
5. Включите продукт **Single sign-on-аутентификация**.
6. Внизу страницы нажмите **Сохранить**.
7. Перейдите на главную страницу веб-интерфейса установщика и запустите автоматическую установку. Если после установки остались роли помеченные желтым, запустите автоматическую установку еще раз.
8. Перейдите в расширенную панель администратора по адресу `https://biz.<ваш_домен>/admin/features/?name=sso` и проверьте что включена фича `sso-enabled`.
9. Установите и настройте Keycloak на сервере вашей организации, создайте Realm. На уровне сетевой конфигурации необходимо разрешить входящие HTTPS-запросы.
10. Скопируйте и сохраните URL для обратного редиректа:
    a. В панели администратора VK WorkSpace перейдите в раздел **Конфигурация → Настройки → Способы аутентификации**.
    b. В блоке **SSO – технология единого входа** нажмите на кнопку **Изменить настройки**.
    c. Отобразится форма **SSO аутентификация**. Скопируйте и сохраните URL из поля **URL для обратного редиректа**. Заполнять форму пока не нужно, вы вернетесь к её заполнению позже.



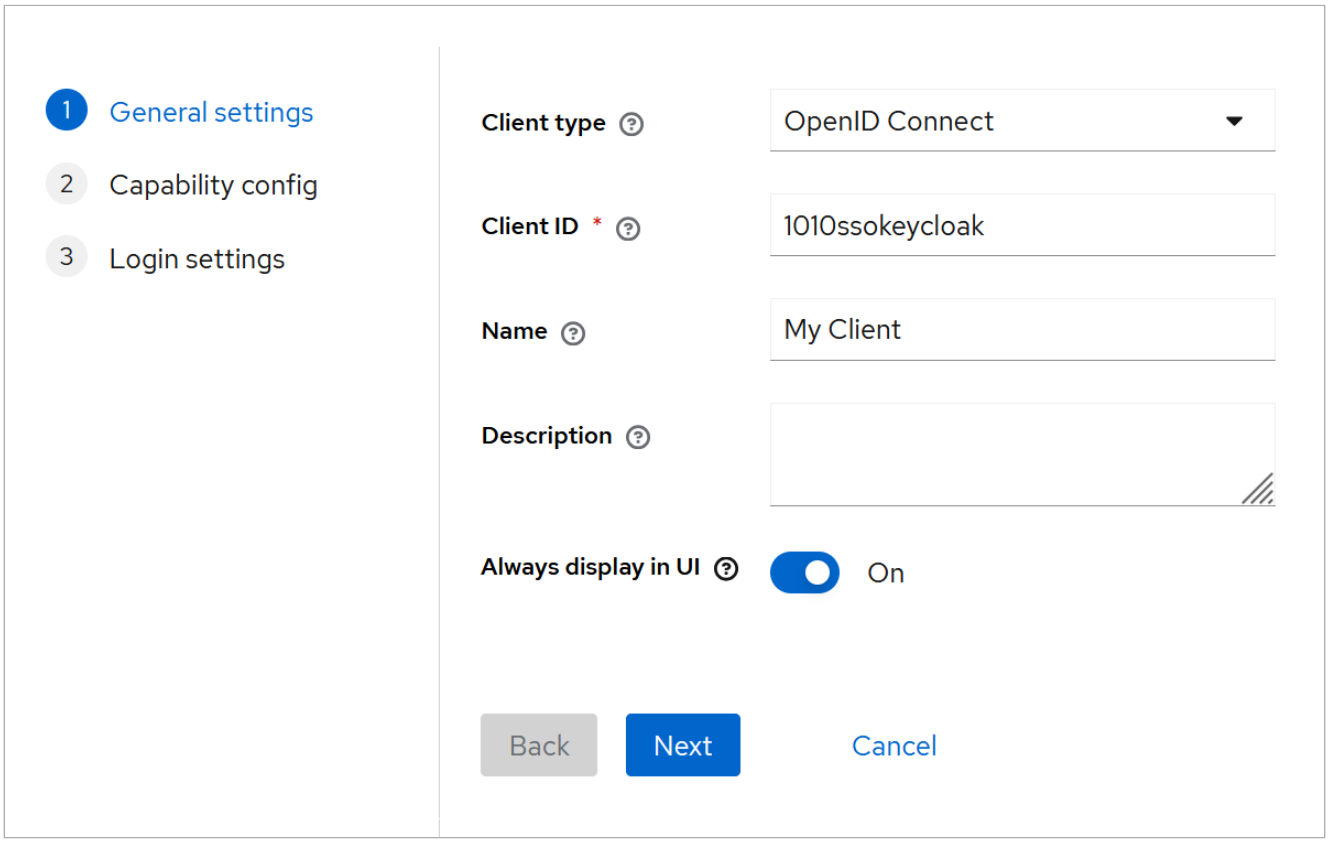

## Шаг 1. Создайте и настройте клиента в Keycloak

1. Перейдите в раздел **Clients** и нажмите на кнопку **Create client**.



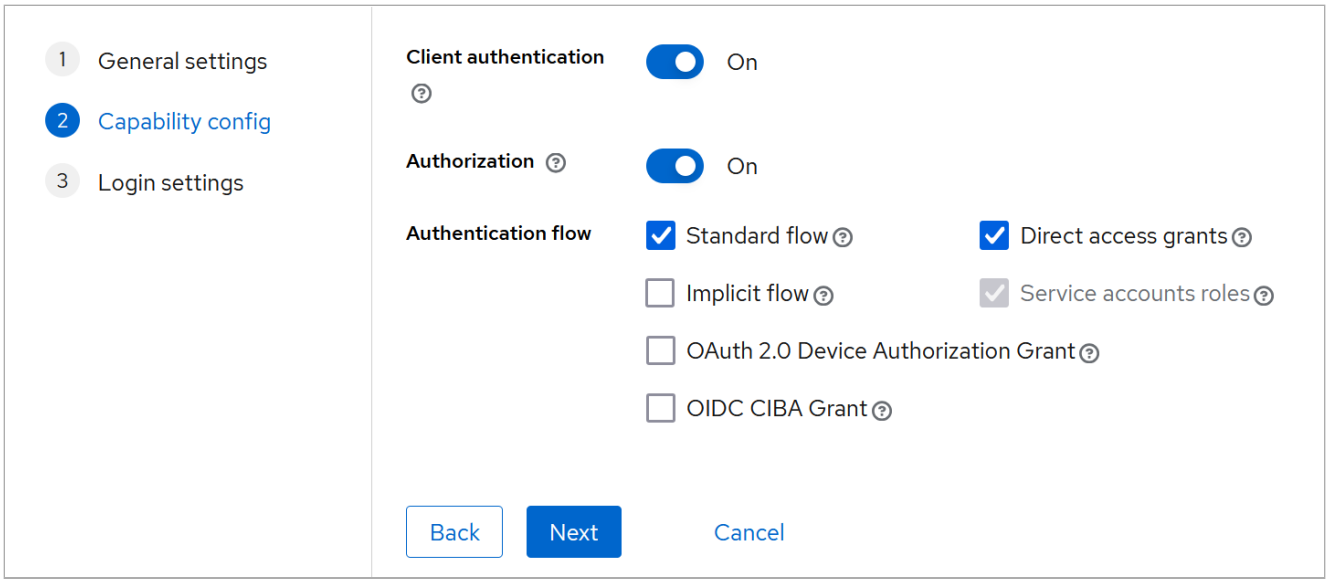

2. В поле **Client type** выберите `OpenID Connect`, в поле **Client ID** укажите любой удобный вам идентификатор.

> **Примечание**
>
> Сохраните идентификатор, указанный в **Client ID**, он понадобится для дальнейшей настройки.




Остальные поля (необязательные) заполните по желанию и нажмите на кнопку **Next**.

3. Откроется раздел **Capability config**:

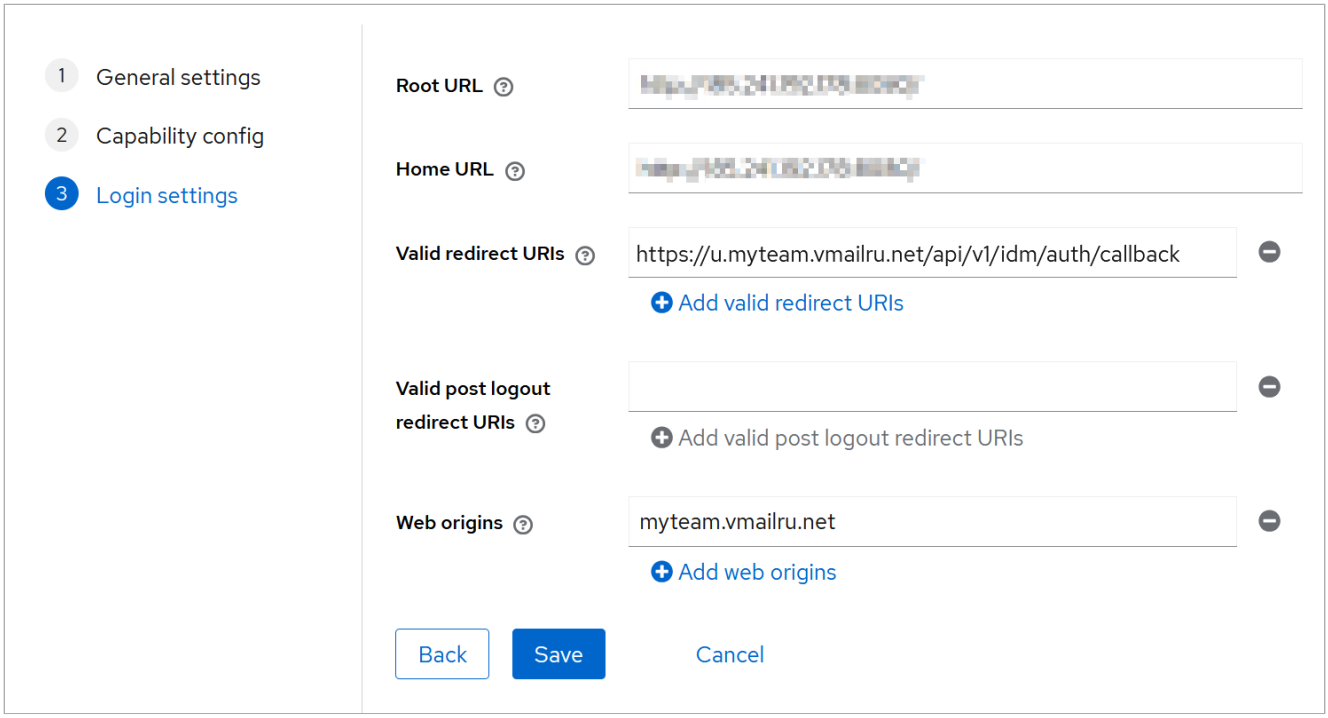



a. Включите опции **Client authentication**, **Authorization**.

b. В блоке **Authentication flow** отметьте галочками `Standard flow` и `Direct access grants`.

c. Нажмите на кнопку **Next**.

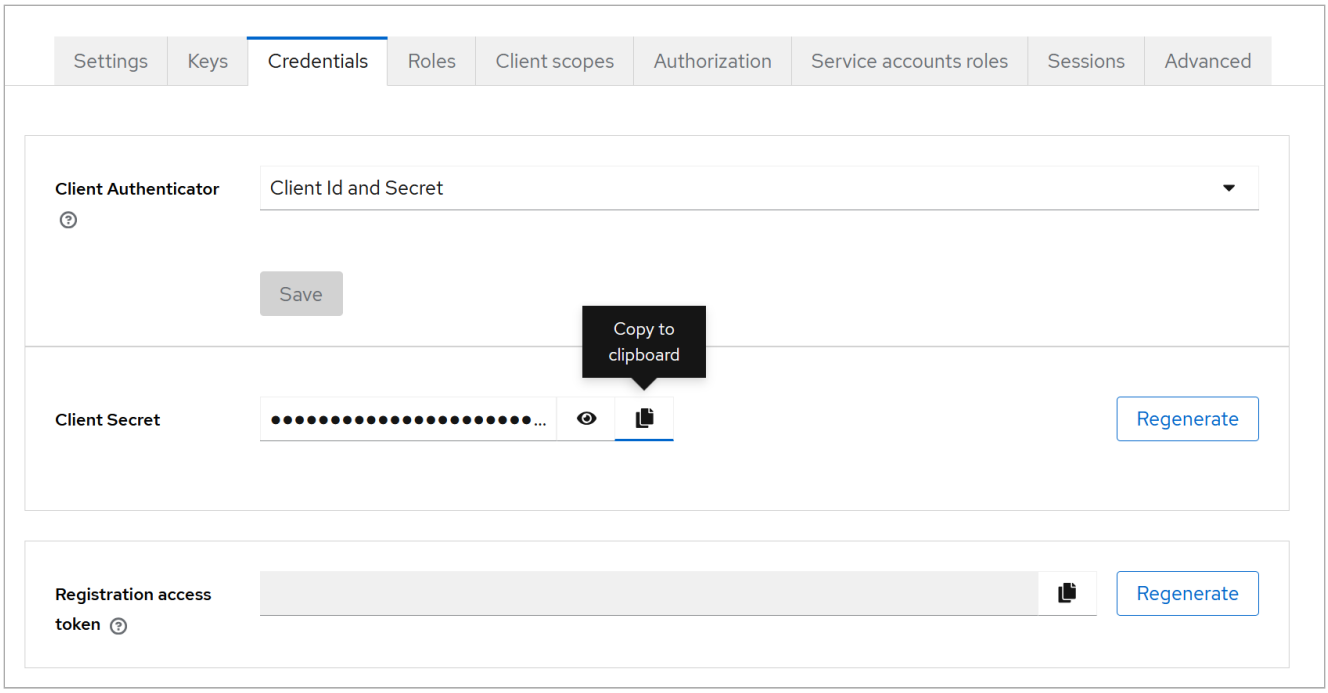
4. Откроется раздел **Login settings**:



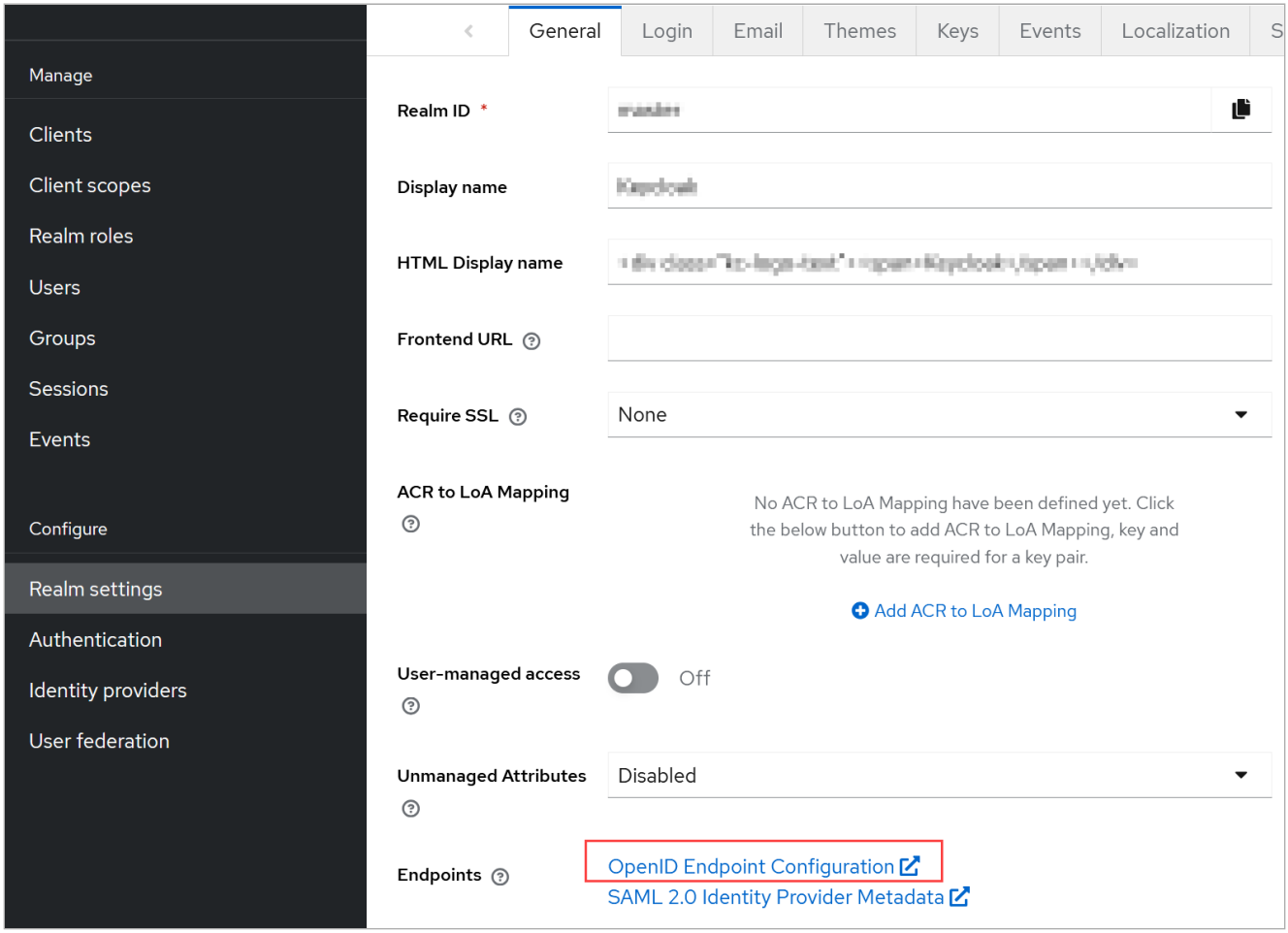

- в полях **Root URL** и **Home URL** укажите адрес сервера, на котором расположен Keycloack;
- в поле **Valid redirect URIs** укажите URL для обратного редиректа из настроек SSO в панели администратора.
- поле **Valid post logout redirect URIs** оставьте пустым;
- в поле **Web origins** укажите ваш домен для основных сервисов.

Нажмите на кнопку **Save**.

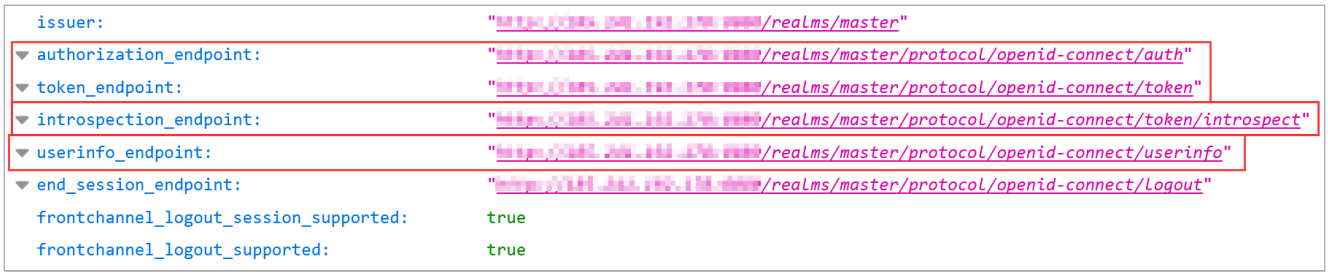
5. Перейдите на вкладку **Credentials**, скопируйте и сохраните ключ-секрет из поля **Client Secret**.




6. Перейдите в раздел **Realm settings**. На вкладке **General**, в блоке **Endpoints**, нажмите на OpenID Endpoint Configuration.

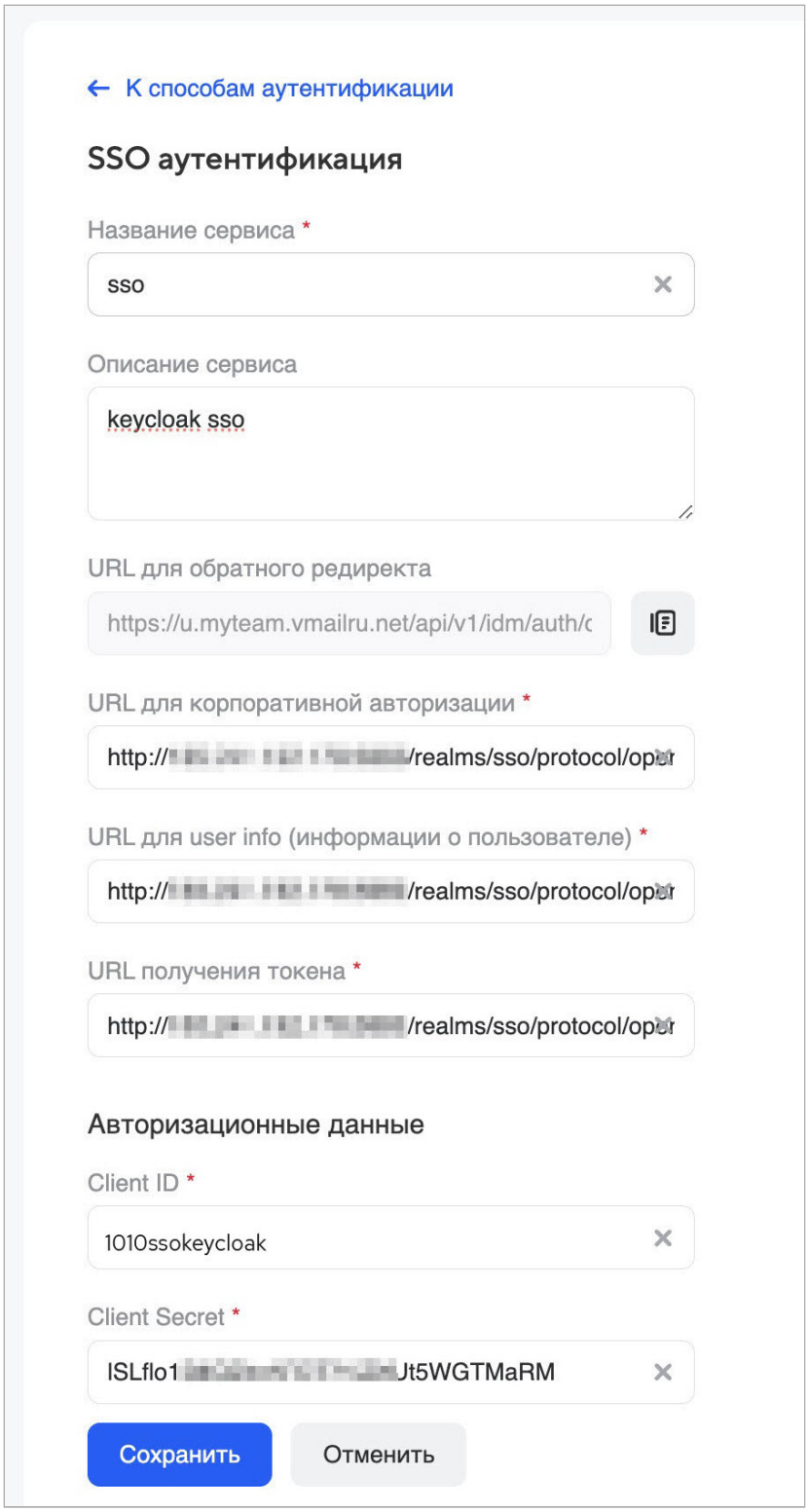



7. Откроется страница с конфигурационными данными. Скопируйте и сохраните следующие URL-адреса: `authorization_endpoint`, `token_endpoint`, `introspection_endpoint` и `userinfo_endpoint`.




## Шаг 2. Настройте SSO в панели администратора VK WorkSpace

Перейдите в раздел настройки SSO в панели администратора (**Конфигурация → Настройки → Способы аутентификации**) и заполните форму. В полях укажите данные, а также URL-адреса и идентификаторы, которые вы сохранили на предыдущих шагах:




- **URL для корпоративной авторизации** — `authorization_endpoint` из конфигурационных данных в Keycloak.
- **URL для user info** — `userinfo_endpoint` из конфигурационных данных в Keycloak.
- **URL получения токена** — `token_endpoint` из конфигурационных данных в Keycloak.
- **URL для валидации токена (token introspection)** — `introspection_endpoint` из конфигурационных данных в Keycloak.
- **Client ID** — идентификатор, который вы придумали и сохранили при создании клиента в Keycloak.
- **Client Secret** — ключ-секрет из интерфейса Keycloak.

# Шаг 3. Выполните настройку в интерфейсе Keycloak

Вернитесь в интерфейс администрирования Keycloak.

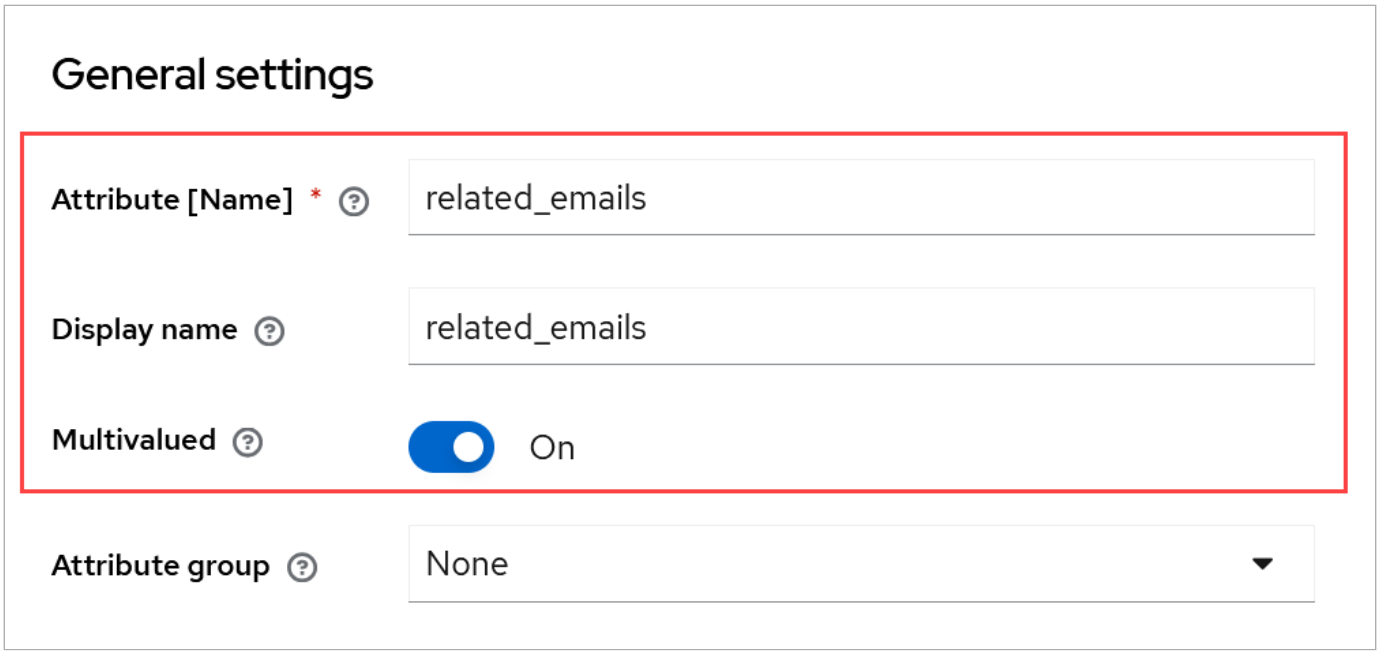
## 1. Создайте нужные вам атрибуты

Если нужно, чтобы в системе и адресной книге отображалась дополнительная информация о пользователе, создайте соответствующие атрибуты в Keycloak. Все доступные атрибуты перечислены в таблице:

| **Название атрибута** | **Описание** | **Включить опцию Multivalued** |
|---|---|---|
| related_emails | Связанные почтовые ящики | да |
| job_title | Должность | нет |
| department | Подразделение | нет |
| company | Организация | нет |
| phone | Рабочий номер телефона | да |
| phone_fax | Факс | да |
| phone_home | Домашний номер телефона | да |
| phone_mobile | Мобильный номер телефона | да |
| phone_other | Дополнительный номер телефона | да |
| address | Адрес<br><br>Данный атрибут может быть передан как с типом `string`, так и с типом `object`, со следующим набором параметров:<br>- country (страна)<br>- postal_code (индекс)<br>- region (регион)<br>- locality (город)<br>- street_address (улица, дом, офис)<br>При передаче атрибута с типом `object` происходит | нет |

| Название атрибута | Описание | Включить опцию Multivalued |
|---|---|---|
| | склейка параметров в строку в следующем порядке: postal_code, country, region, locality, street_address. | |
| comment | Примечание / комментарий | нет |
| boss | ФИО руководителя | нет |

Перейдите в раздел **Realm settings**, на вкладке **User profile** нажмите на кнопку **Create attribute** и заполните форму:




- в полях **Attribute [Name]** и **Display name** введите название нужного атрибута, например `related_emails`;
- если нужно, включите опцию **Multivalued** (см. в таблице выше);
- остальные настройки/поля оставьте без изменений;

Нажмите на кнопку **Create**. Повторите действия и создайте все нужные атрибуты.

**Внимание**

При создании атрибута `related_emails` обратите внимание на блок **Permission** (следует за блоком **General settings** со скриншота выше). Предоставление рядовому пользователю права на редактирование атрибута `related_emails` (путем установки галочки **User** в блоке **Who can edit?**) может привести к атаке с подменой личности (impersonation attack). Злоумышленник может временно добавить email-почту любого сотрудника или администратора и получить несанкционированный доступ к ресурсам.

## 2. Создайте записи для нужных вам атрибутов

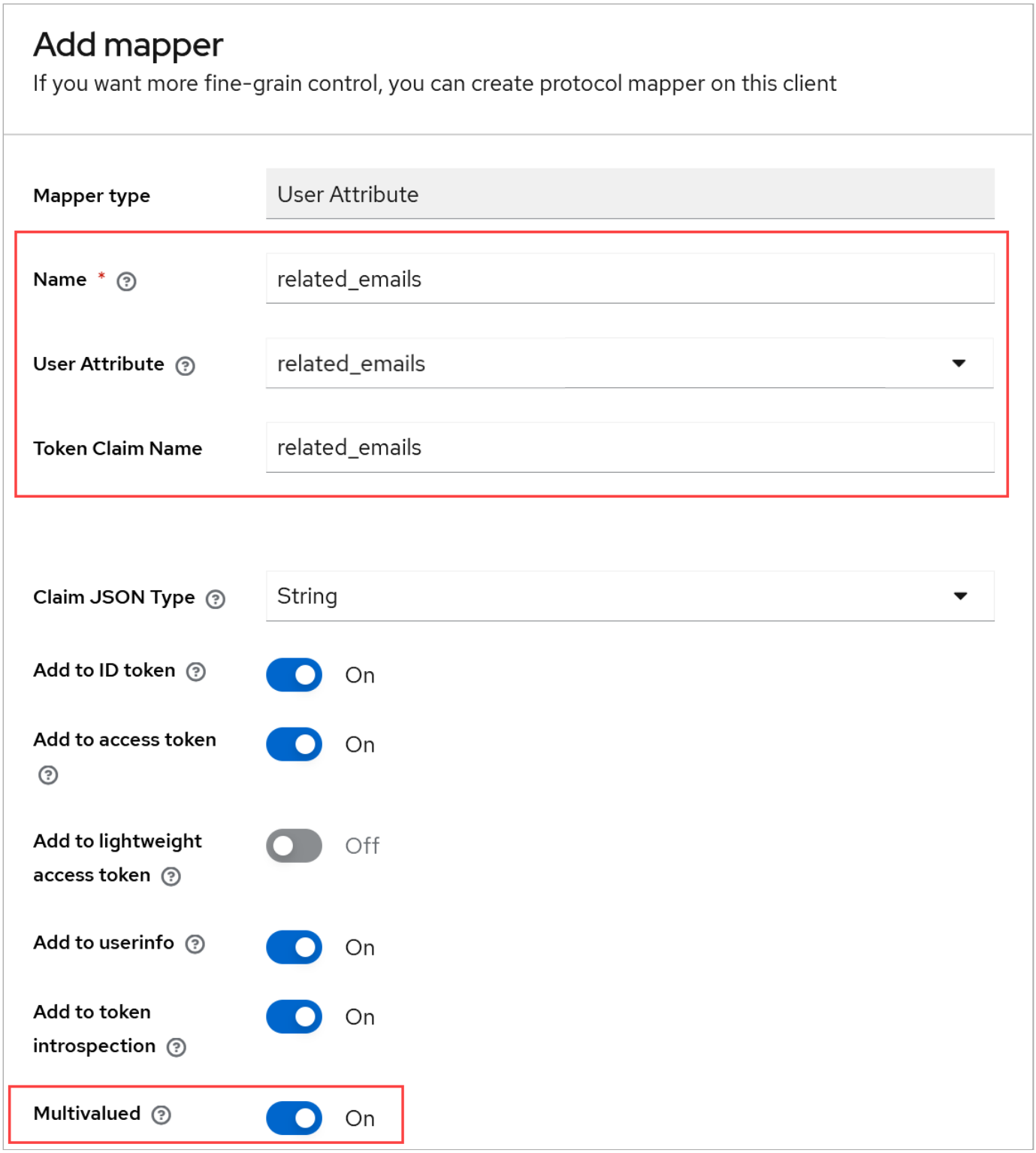
В разделе **Client scopes** заведите записи для созданных атрибутов.

2.1. Нажмите на кнопку **Create client scope** и заполните форму:

- в полях **Name** и **Description** укажите название нужного атрибута, например `related_emails`;
- в поле **Type** выберите `default`;
- в поле **Protocol** выберите `OpenID Connect`;

Нажмите на кнопку **Save**.

2.2. Перейдите на вкладку **Mappers** и нажмите на кнопку **Configure a new mapper**. Откроется окно со списком — найдите в списке `User attribute` и нажмите на него. Заполните форму:



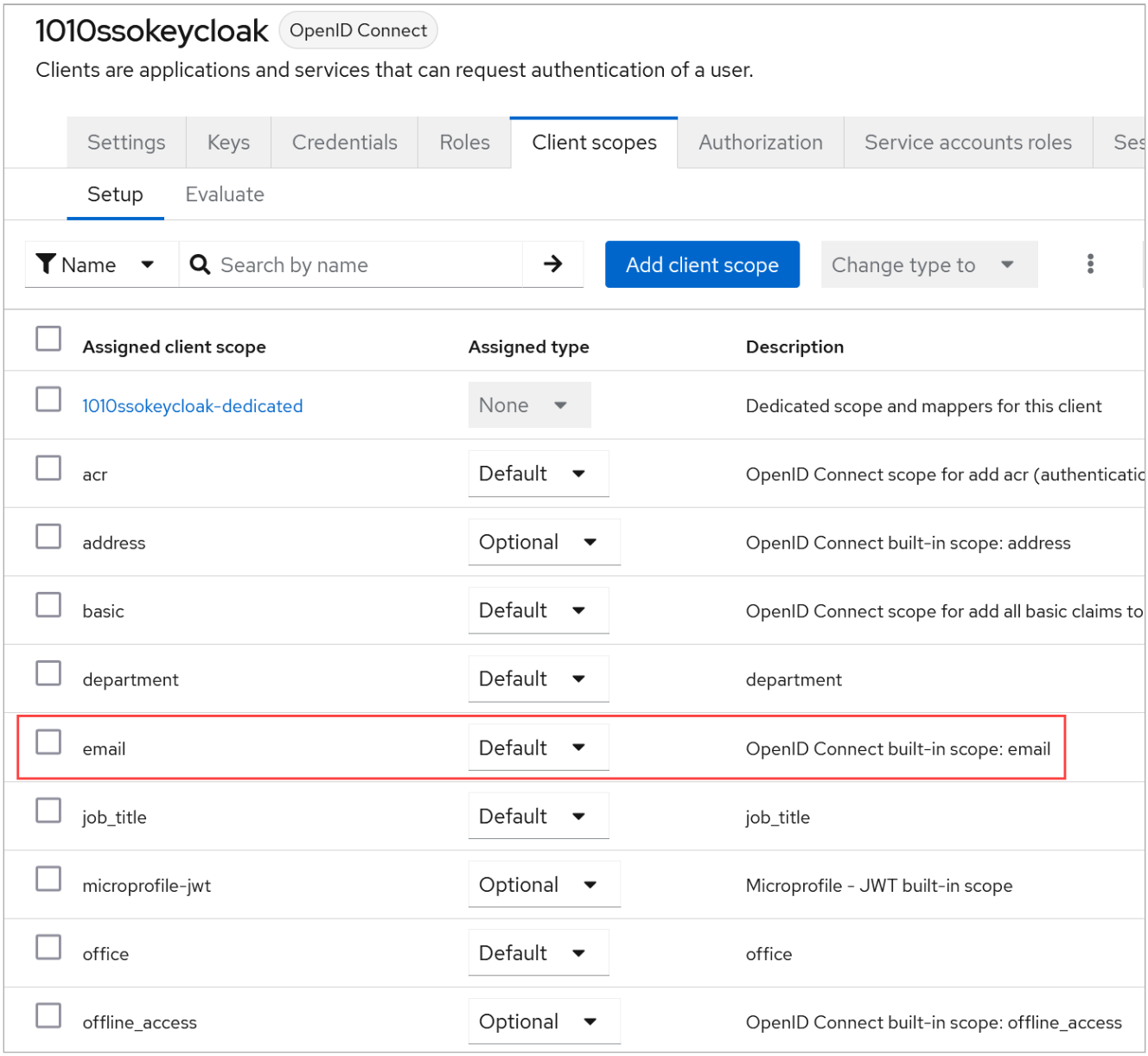

- в полях **Name** и **Token Claim Name** укажите название нужного атрибута, например `related_emails`;
- в поле **User attribute** выберите из списка соответствующее название атрибута, например `related_emails`;
- если нужно, включите опцию **Multivalued** (см. в таблице выше).

Остальные настройки оставьте без изменений. Нажмите на кнопку **Save**. Повторите действия для всех нужных вам атрибутов.

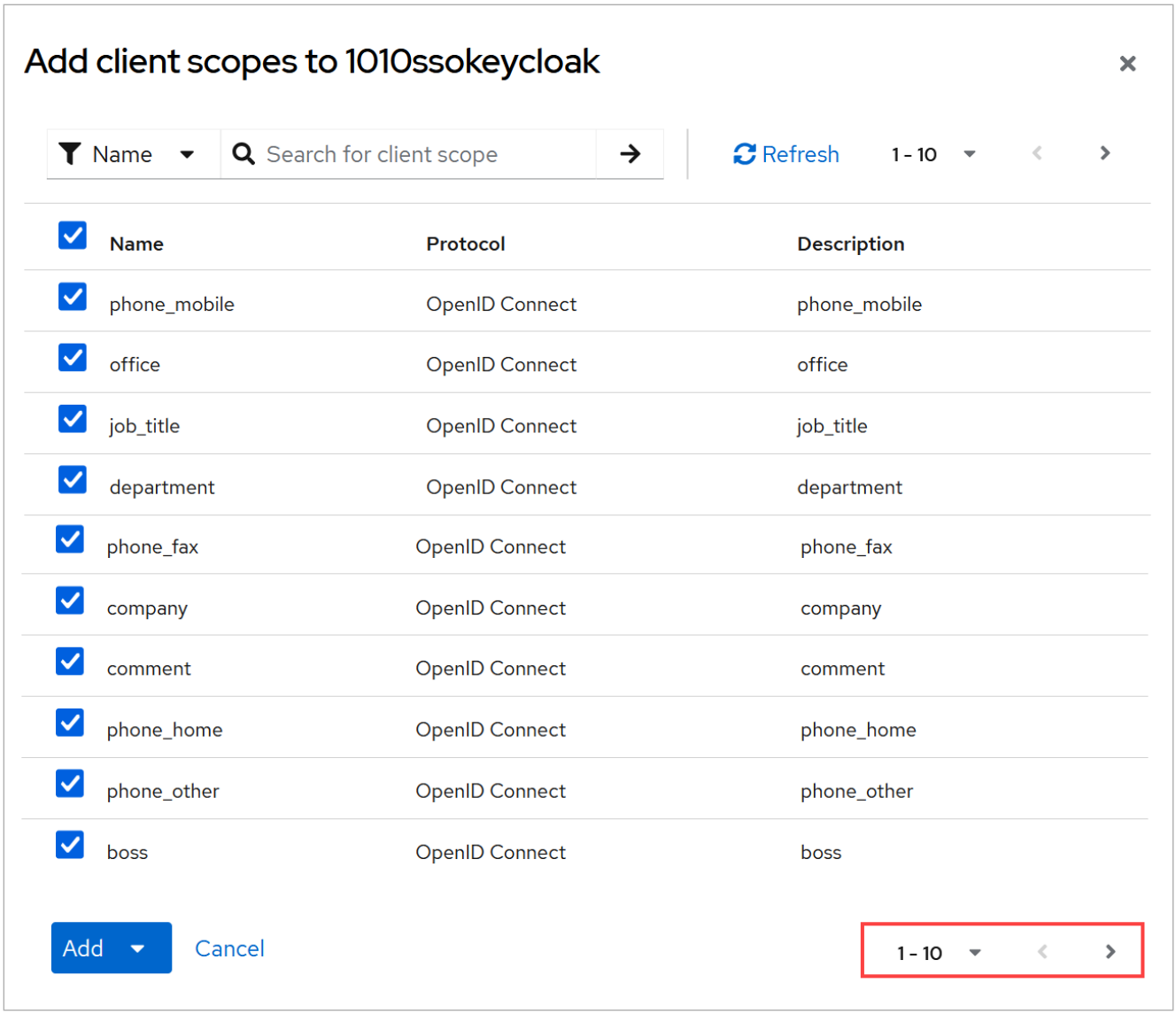
# 3. Завершите настройку

Перейдите в раздел **Clients** и выберите ранее созданного клиента. На вкладке **Client scopes** выполните следующие действия:

- Найдите в списке параметр `email` и убедитесь, что у него задан тип `Default` и указано `OpenID Connect built-in scope: email`.



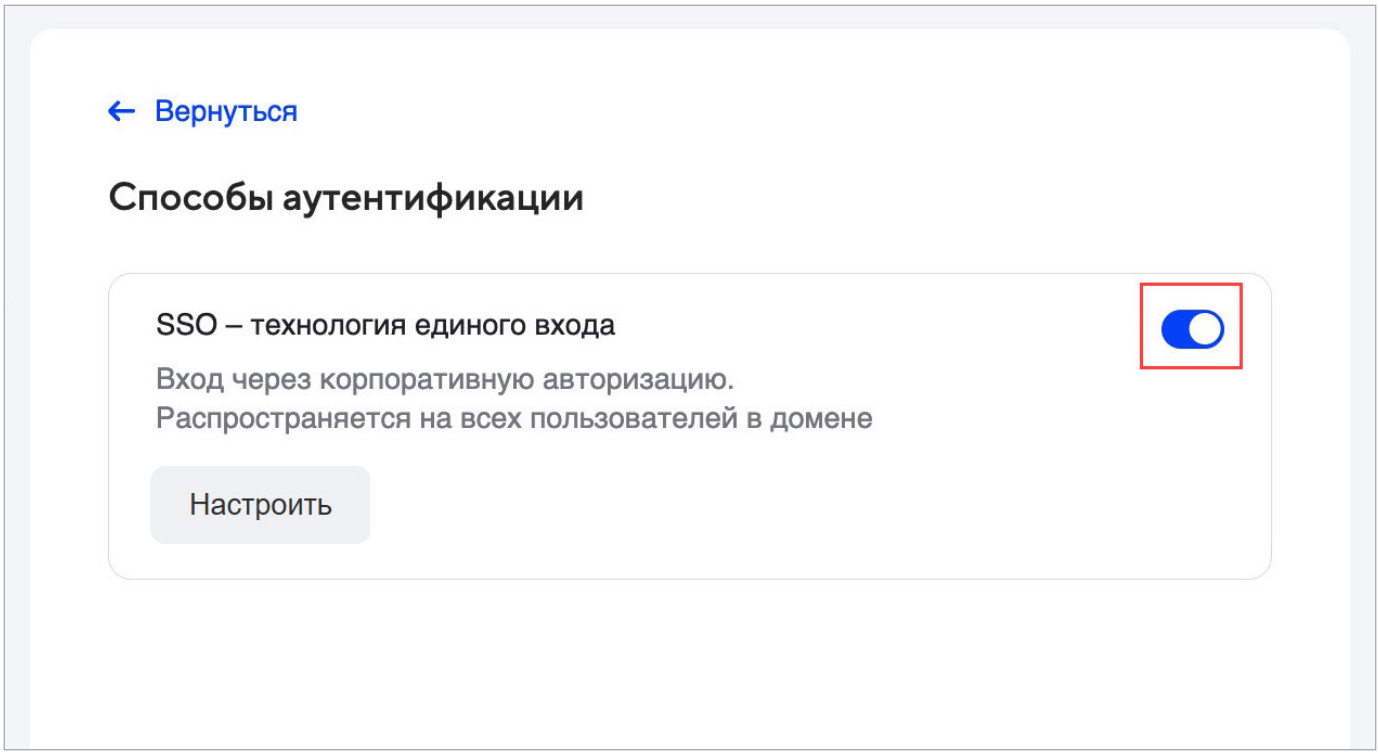

- Нажмите на кнопку **Add client scope** и в открывшемся окне отметьте галочками все созданные атрибуты. По умолчанию в окне отображается 10 записей, поэтому если вы создали больше десяти атрибутов, воспользуйтесь опцией перехода, чтобы отметить все атрибуты. Затем нажмите **Add → Default**.




На этом настройка SSO в Keycloak завершена.

## Шаг 4. Активируйте вход через SSO в панели администратора

Перейдите в интерфейс настроек SSO в панели администратора VK Workspace (**Конфигурация → Настройки → Способы аутентификации**) и включите вход через SSO:




## Шаг 5. Убедитесь, что аутентификация через SSO работает

- Авторизуйтесь в любом сервисе VK WorkSpace через учетную запись, заведенную в панели администратора.
- Авторизуйтесь в любом сервисе VK WorkSpace через учетную запись, заведенную в Keycloack и отсутствующую в панели администратора. Проверьте, что сотрудник появился в списке пользователей после успешной авторизации (раздел **Пользователи** в меню панели администратора).

**Примечание**

Новые сотрудники создаются в VK WorkSpace автоматически в момент первой авторизации через SSO. В случае блокировки пользователя в Keycloak все его сессии в VK WorkSpace будут завершены, и он больше не сможет войти в сервисы, но его статус в разделе **Пользователи** в панели администратора при этом не изменится. Изменить статус пользователя на «Заблокирован» надо будет вручную через интерфейс панели администратора.

# Где скачать суперапп?

Суперапп будет доступен для скачивания на лендинге по адресу `https://dl.<сайт_компании>`.

# Доступные функциональности после запуска Супераппа

После запуска Супераппа вы можете управлять безопасностью Супераппа для мобильных устройств — контролировать, защищать и управлять мобильными приложениями, установленными на устройствах сотрудников, обеспечивая безопасность корпоративных данных и предотвращая несанкционированный доступ.

Управление осуществляется через файл конфигурации **/opt/mailOnPremise/dockerVolumes/superapp-nginx1/public/myteam-config.json**.

# Ограничения после запуска Супераппа

Начиная с версии 26.1 Суперапп может работать без инсталляции Мессенджера VK WorkSpace, но в таком случае групповые политики не будут доступны. Если вам необходимы групповые политики — запустите Суперапп по инструкции.

Технический писатель: Белова Ирина

5 мая 2026 г.