MANGO OFFICE

8 800 555 55 22

WWW.MANGO-OFFICE.RU

Аутентификация и авторизация в рамках SSO

Руководство пользователя

v1 | 2023

MANGO OFFICE

Оглавление

MANGO OFFICE

1. Термины и определения

Keycloak – средство управления доступом и идентификации с открытым исходным кодом, которое предоставляет функциональность аутентификации, авторизации и управления пользователями для приложений и сервисов.

Realm (Область) – Realm в Keycloak представляет изолированную среду, где определяются настройки аутентификации и авторизации для пользователей и клиентов.

Front Channel Logout (Механизм выхода через передний канал) – механизм однопроходного выхода, который используется для автоматического завершения сеансов пользователя в связанных приложениях при выходе из системы.

Client Signature Required (Требуется подпись клиента) – настройка, которая обязывает клиентов предоставлять подпись в запросах к Keycloak для обеспечения безопасности и целостности данных.

Маппер (Mapper) – мапперы в Keycloak используются для преобразования и маппинга атрибутов пользователей или клиентов, чтобы предоставлять определенные атрибуты в токенах или запросах.

Роль (Role) – роль в Keycloak представляет собой определенные разрешения и привилегии, которые могут быть назначены пользователям или клиентам для управления доступом.

Атрибут (Attribute) – атрибуты в Keycloak представляют информацию о пользователе или клиенте, такую как роли, имя, адрес электронной почты и другие свойства.

MANGO OFFICE

2. Общие сведения

Технология единого входа (Single sign-on SSO) — метод аутентификации, который позволяет пользователям аутентифицироваться сразу в нескольких приложениях и сайтах, используя один набор учетных данных.

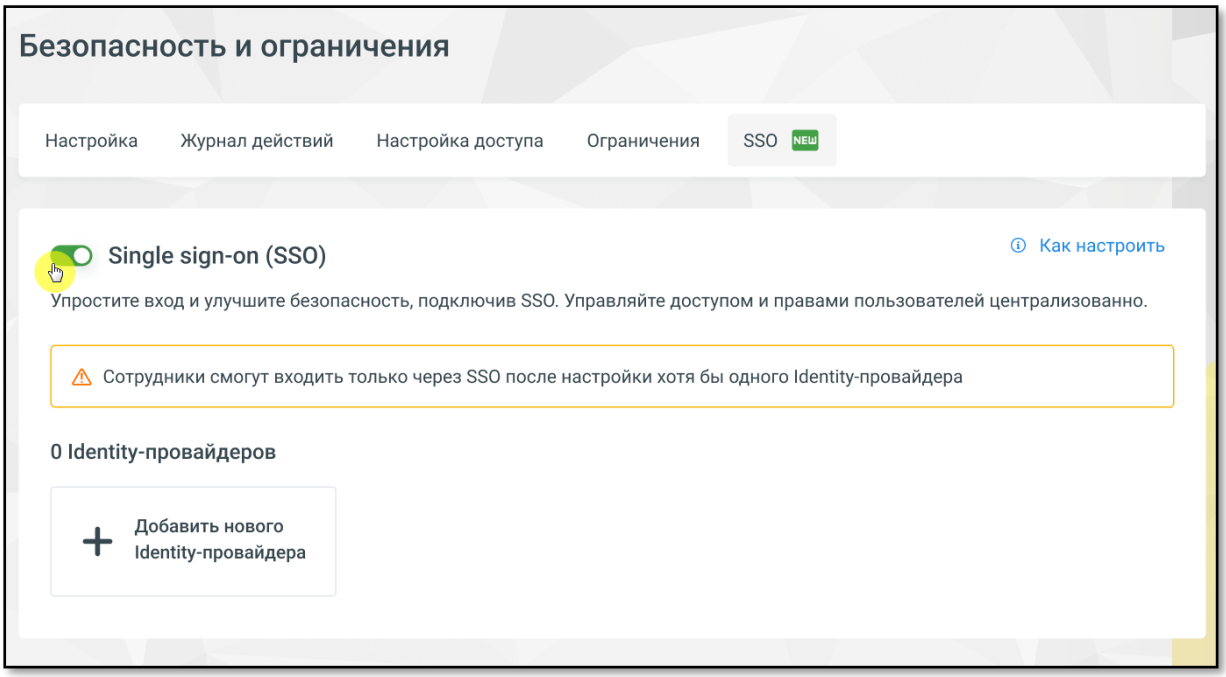
Аутентификация и авторизация в рамках SSO с алгоритмом SAMLv2 обеспечивает более безопасный и удобный способ управления доступом пользователей к множеству ресурсов, так как пользователь может пройти аутентификацию только один раз и затем автоматически получить доступ ко всем приложениям и ресурсам, интегрированным с этой системой SSO.

Порядок авторизации:

1. В разделе Identity Provider (IdP) своей системы, клиенту необходимо создать отдельные учетные записи для каждого оператора.
2. Далее перейдите в Личный кабинет ВАТС MANGO OFFICE и настройте ваш IdP. После завершения настройки вы получите специальную авторизационную ссылку, предназначенную для операторов, которые будут использовать созданные учетные записи.
3. Операторы, в свою очередь, могут получить доступ к Личному кабинету ВАТС, используя специальную ссылку, полученную в предыдущем шаге.
4. Личный кабинет инициирует запрос к форме авторизации в IdP.
5. После успешной авторизации IdP генерирует токен, содержащий информацию о пользователе (адрес электронной почты), и передает его обратно в систему SSO с помощью запроса auth-response, направленного в Личный кабинет.
6. Личный кабинет ВАТС автоматически обрабатывает этот ответ и предоставляет операторам доступ к своему функционалу. Учетная запись оператора создается и настраивается автоматически в процессе обработки.

3. Настройка IdP в ЛК ВАТС MANGO OFFICE

Для использования возможности авторизации через SSO в Личном кабинете ВАТС должна быть подключена соответствующая услуга. После подключения в ЛК в разделе **Общие настройки / Безопасность и ограничения** появится вкладка «SSO».

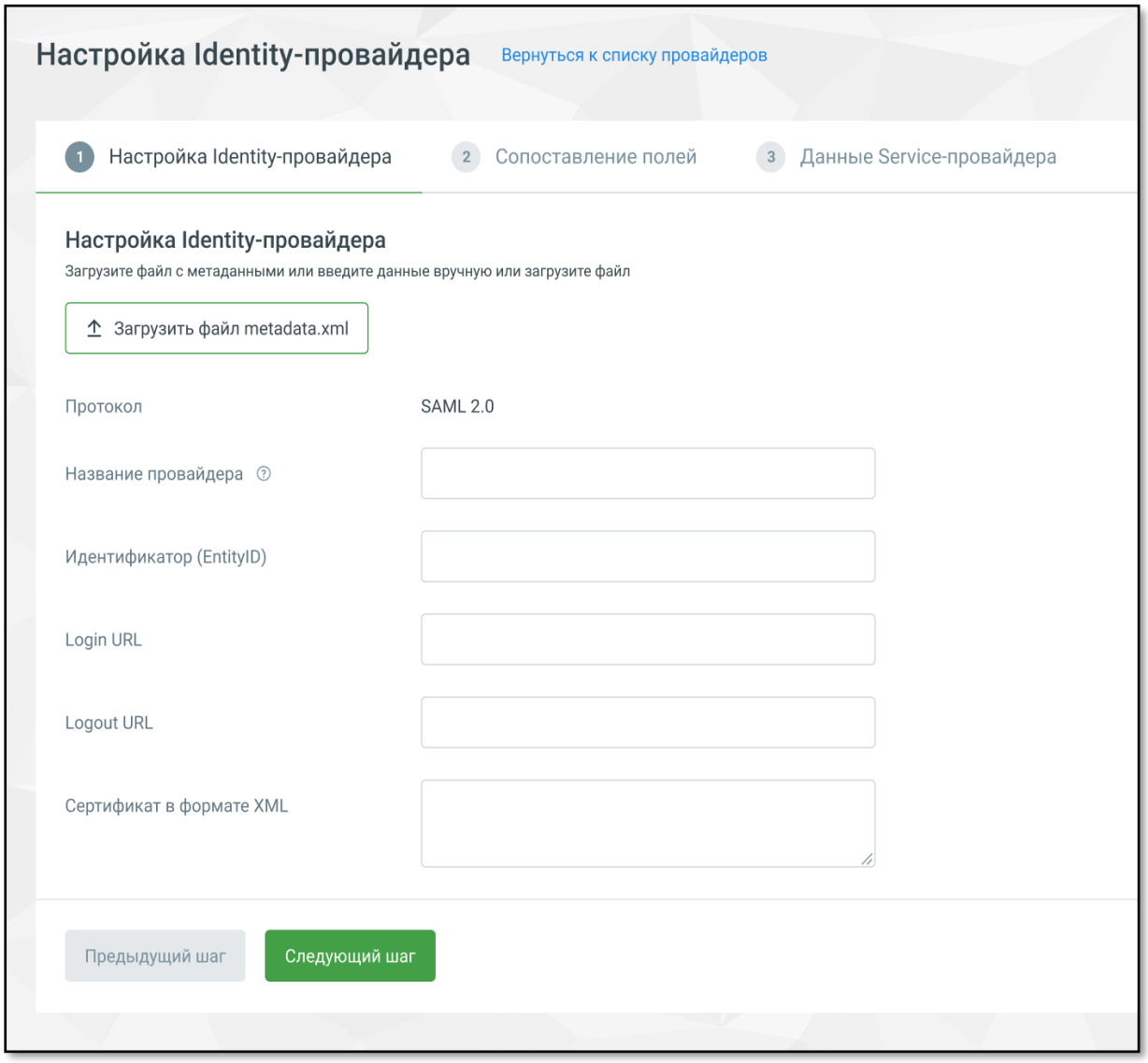


Активируйте услугу переключателем и переходите к добавлению нового провайдера.

Максимальное количество провайдеров на продукте – 5.

4. Добавление провайдера

ШАГ 1. НАСТРОЙКА IDENTITY-ПРОВАЙДЕРА (IDP).



Вы можете выбрать два способа настройки вашего Identity-провайдера: загрузить файл метаданных (metadata.xml) или ввести необходимые данные вручную.

Все поля формы являются обязательными для заполнения.

Название провайдера - название вашего Identity-провайдера (например Keycloak). Это поле помогает идентифицировать ваш IdP в системе.

Идентификатор (Entity ID) - или идентификатор сущности, уникально идентифицирует ваш Identity-провайдер в контексте SAML 2.0. Entity ID предоставляется вашим Identity-провайдером.

Login URL - URL-адрес, по которому ваш сервис-поставщик будет перенаправлять пользователей для аутентификации. Пользователи будут направлены на этот URL для ввода учетных данных в систему IdP. Login URL также предоставляется вашим Identity-провайдером.

Logout URL - URL-адрес, по которому пользователи будут перенаправляться после выхода из системы. Этот URL определяет, куда пользователи будут перенаправлены после завершения сеанса. Logout URL также предоставляется вашим Identity-провайдером.

Сертификат в формате XML - сертификат в формате XML, который используется для безопасной передачи данных между вашим сервис-поставщиком и Identity-провайдером. Этот сертификат обеспечивает защиту данных во время обмена между системами. Обратитесь к вашему Identity-провайдеру, чтобы получить этот сертификат. Вы также можете найти его в метаданных (metadata.xml), если предоставленный файл содержит эту информацию.

Загрузить файл metadata.xml - имеется возможность заполнить данную форму, используя файл с метаданными Identity-провайдера. Структура файла стандартная (соответствует спецификации SAML 2.0). Файл метаданных содержит информацию о вашем Identity-провайдере и его загрузка облегчит настройку, так как позволит автоматически получить необходимые параметры. Файл может быть предоставлен вам вашим IdP или находиться в их системе.

Пример структуры файла metadata.xml

```
<md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata»
validUntil="2023-09-30T19:48:36Z»
cacheDuration="PT604800S» entityID="https://adfs-
test.by.mgo.su/entityid">
<div id="in-page-channel-node-id» data-channel-
name="in_page_channel_jblkcP"/>
<md:SPSSODescriptor AuthnRequestsSigned="false»
WantAssertionsSigned="false»
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:p
rotocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC4jCCAcoCCQC33wnybT5QZDANBgkqhkiG9
w0BAQsFADAyMQswCQYDVQQGEwJVSzEPMA0GA1UECgwGQm94eUhRMRIwEA
YDVQQDDAlNb2NrIFNBTUwwIBcNMjIwMjI4MjE0NjM4WhgPMzAyMTA3MDE
yMTQ2MzhaMDIxCzAJBgNVBAYTAlVLMQ8wDQYDVQQKDAZCb3h5SFExEjAQ
BgNVBAMMCU1vY2sgU0FNTDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCA
QoCggEBALGfYettMsct1T6tVUwTudNJH5Pnb9GGnkXi9Zw/e6x45DD0Ru
RONbFlJ2T4RjAE/uG+AjXxXQ8o2SZfb9+GgmCHuTJFNgHoZ1nFVXCmb/H
g8Hpd4vOAGXndixaReOiq3EH5XvpMjMkJ3+8+9VYMzMZOjkgQtAqO36eA
FFfNKX7dTj3VpwLkvz6/KFCq8OAwY+AUi4eZm5J57D31GzjHwfjH9WTeX
```

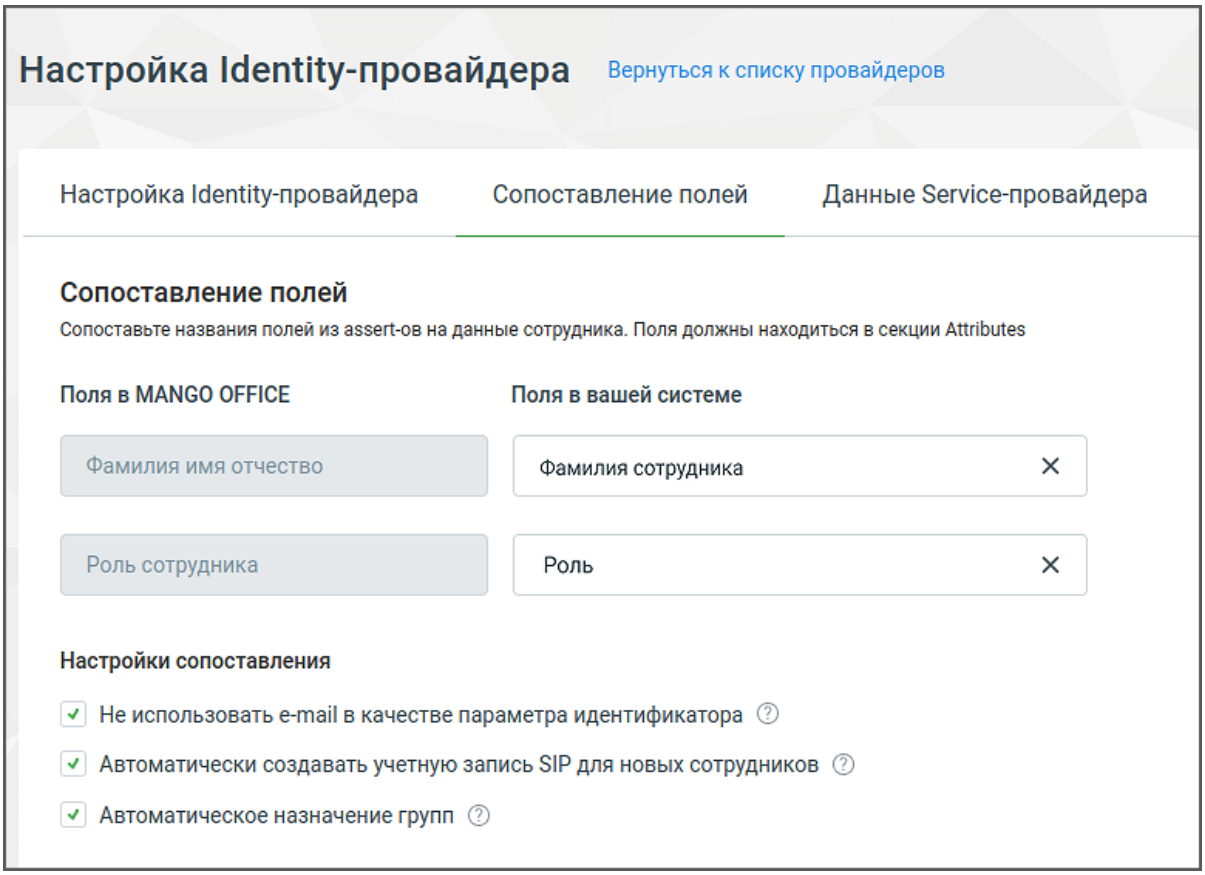
```
0MyndmnNB1qV75qQR3b2/W5sGHRv+9AarggJkF+ptUkXoLtVA51wcfYm6
hILptpde5FQC8RWY1YrswBWAEZNfyrR4JeSweElNHg4NVOs4TwGjOPwWG
qzTfgTlECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAAYRlYflSXAWoZpFf
wNiCQVE5d9zZ0DPzNdWhAybXcTyMf0z5mDf6FWBW5Gyoi9u3EMEDnzLcJ
NkwJAAc39Apa4I2/tml+Jy29dk8bTyX6m93ngmCgdLh5Za4khuU3AM3L6
3g7VexCuO7kwkjh/+LqdcIXsVGO6XDfu2QOs1Xpe9zIzLpwm/RNYeXUjb
Sj5ce/jekpAw7qyVVL4xOyh8AtUW1ek3wIw1MJvEgEPt0d16oshWJpoS1
OT8Lr/22SvYEo3EmSGdTVGgk3x3s+A0qWAqTcyjr7Q4s/GKYRFfomGwz0
TZ4Iw1ZN99Mm0eo2USlSRTVl7QHRTuiuSThHpLKQQ==</ds:X509Certi
ficate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect» Location="https://adfs-test.by.mgo.su/adfs-
logout.php"/>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST»
Location="https://adfs-test.by.mgo.su/adfs-resp-
receiver.php» index="1"/>
<md:AttributeConsumingService index="1">
<md:ServiceName xml:lang="en">SP test</md:ServiceName>
<md:ServiceDescription xml:lang="en">Test
Service</md:ServiceDescription>
<md:RequestedAttribute Name="« NameFormat="«
FriendlyName="« isRequired="false"/>
</md:AttributeConsumingService>
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

ШАГ 2. СОПОСТАВЛЕНИЕ ПОЛЕЙ

На втором этапе настройки требуется указать имена атрибутов для точного сопоставления с учетной записью при процедуре авторизации.

ВНИМАНИЕ

Для успешной авторизации сотрудника от Identity-провайдера обязательно должны поступить указанные атрибуты. В противном случае сотрудник не сможет выполнить процедуру авторизации.



ВНИМАНИЕ

Сопоставление по полю «роль» является строгим. Таким образом, если роль в IdP не совпадет, авторизация не произойдет.

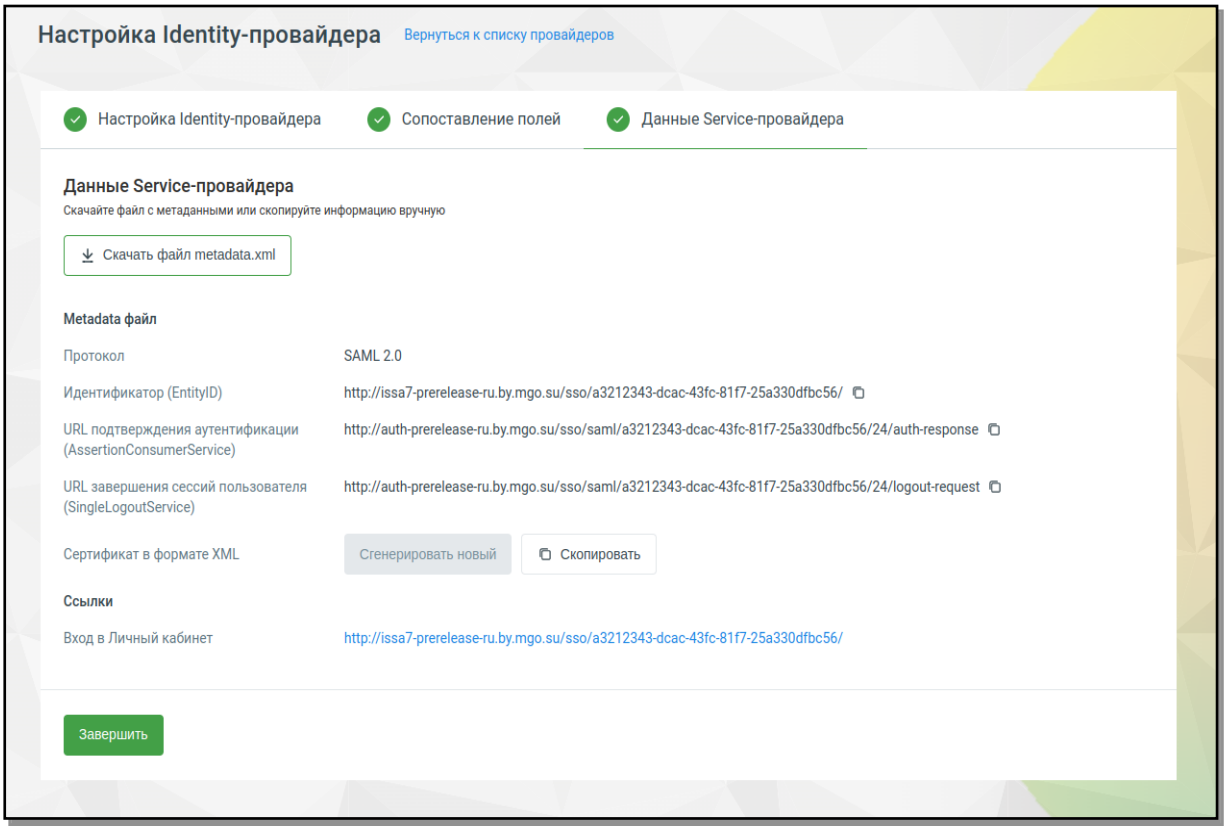
Не использовать e-mail в качестве параметра идентификатора. При включении данной опции сопоставление учетной записи будет происходить не по значению e-mail, а по тому, которое придет в nameID.

Автоматически создавать учетную запись SIP для новых сотрудников. При включении данной опции у новых сотрудников будет создаваться учетная запись SIP, которую можно использовать для звонков.

Автоматическое назначение групп. Для работы этой опции необходимо заранее добавить группы обзвона в ЛК. При включении данной опции, в момент авторизации, сотрудники будут сопоставлены с раннее созданными группами обзвона.

Заполните поля формы и сохраните внесенные изменения кнопкой **Сохранить**.

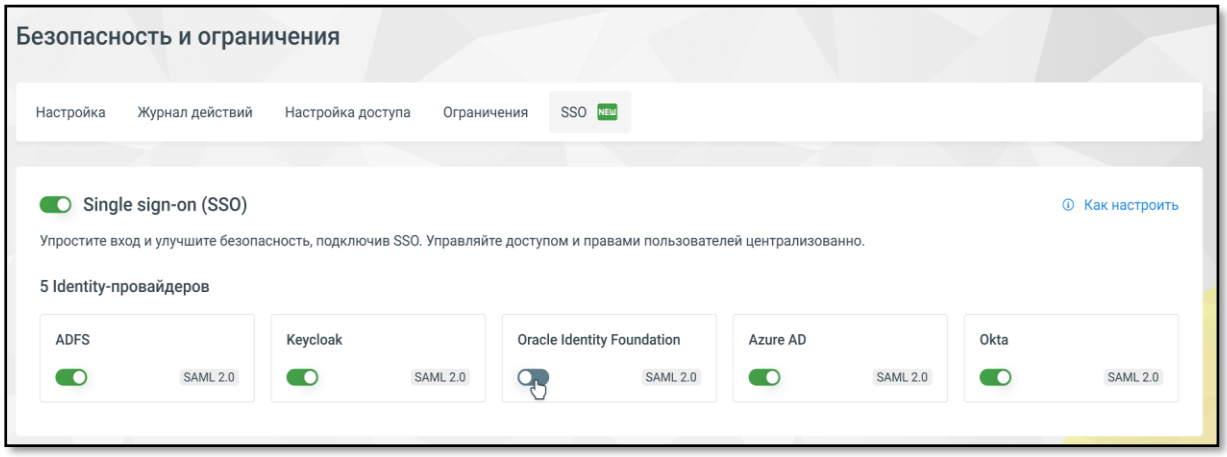
После сохранения настроек Identity-провайдера в Личном кабинете вы получите ссылку, ведущую на форму авторизации, которую и нужно будет передать своим операторам для входа в ЛК ВАТС.



Также на данной странице есть возможность скачать XML файл с настройками, для более простого импорта на стороне Identity-провайдера.

Теперь система способна обрабатывать запросы подтверждения аутентификации и завершения сессий пользователя в соответствии с SAML-спецификацией.

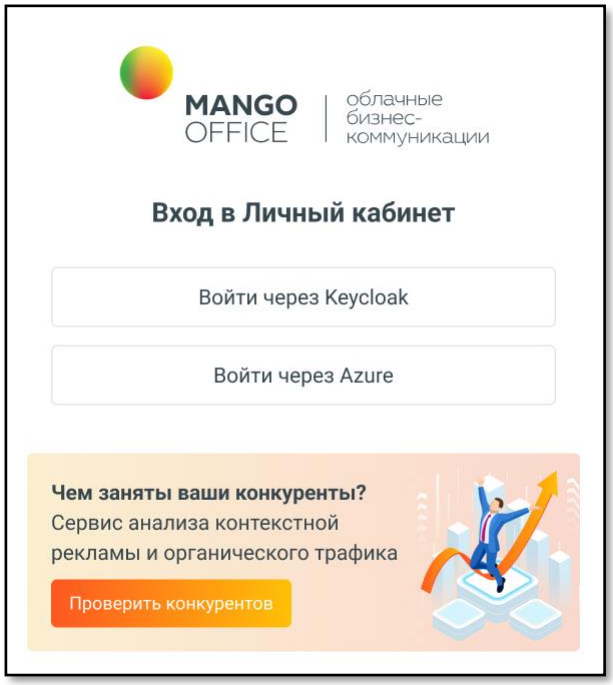
Клик по кнопке «Вернуться к списку провайдеров» открывает окно вкладки **SSO**.



Переключатель «on-off» регулирует активацию/деактивацию своего Identity-провайдера.

5. Вход сотрудника в Личный кабинет ВАТС

После перехода сотрудника по ссылке, полученной на вкладке **Данные Service-провайдера,** откроется форма выбора Identity-провайдера:



После выбора из списка нужного Identity-провайдера в новом окне будет открыта форма авторизации выбранного провайдера. После успешной авторизации на стороне IdP пользователь будет перенаправлен в Личный кабинет ВАТС MANGO OFFICE.

внимание

При обработке ответа (auth-response), полученного от IdP, важно наличие в ответе атрибута с именем «nameID", в котором должно быть передано значение e-mail сотрудника. Если этот атрибут отсутствует или значение не соответствует e-mail сотрудника, то авторизация будет невозможной, то есть сотрудник не сможет успешно войти в систему.

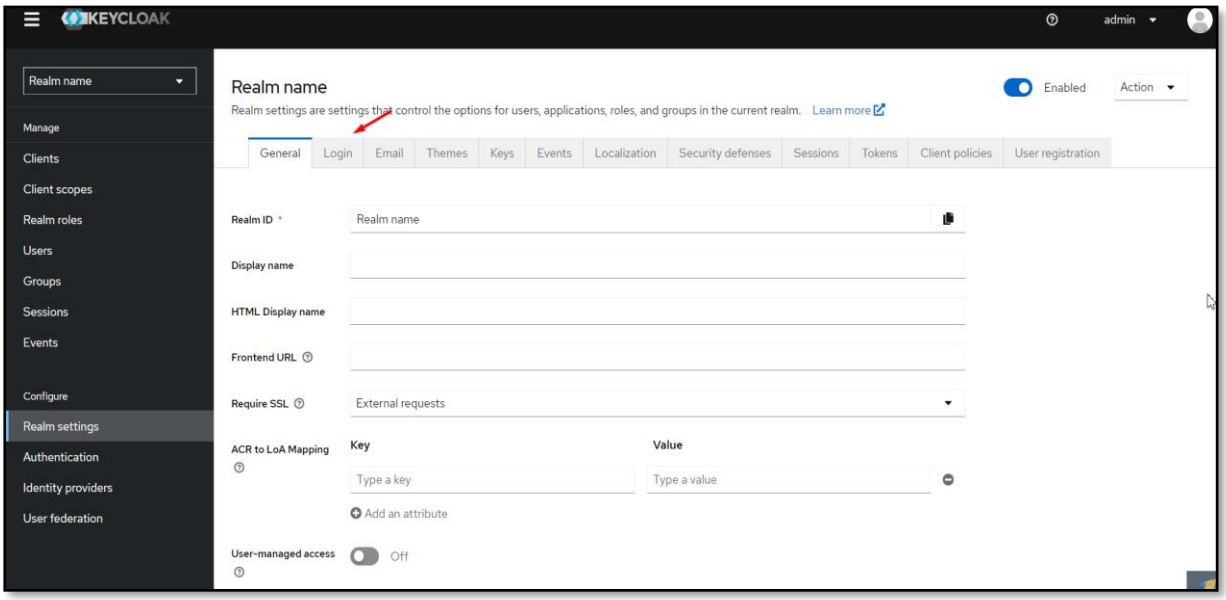
совет

Открытие всплывающих окон может быть заблокировано настройками браузера. Если после выбора IdP в списке не открывается всплывающее окно, необходимо проверить настройки отображения всплывающих окон в браузере.

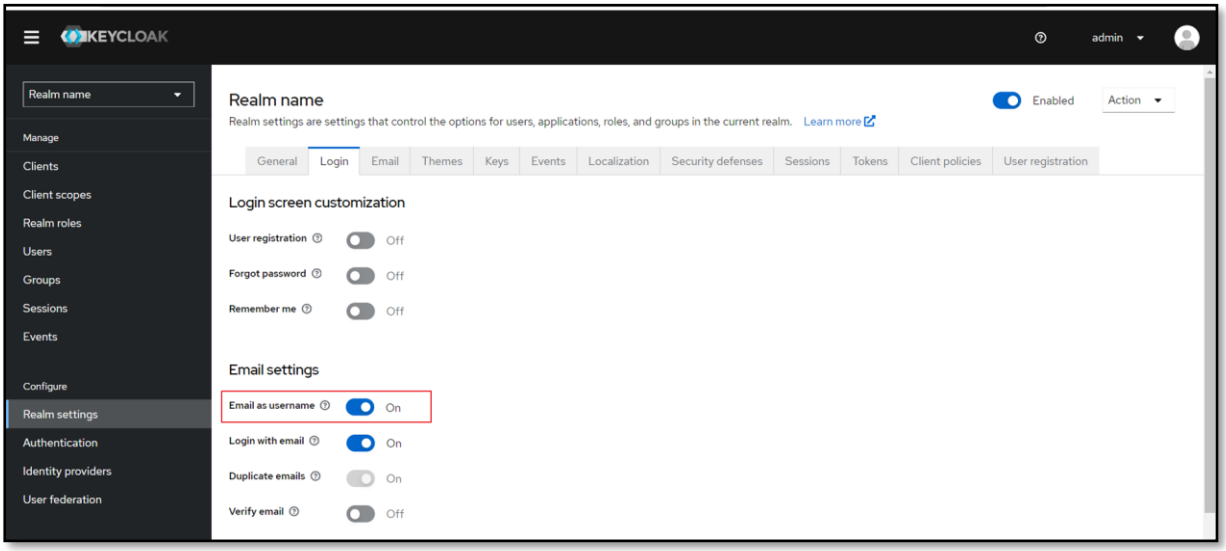
MANGO OFFICE

6. Настройка аутентификации и авторизации на примере Keycloak

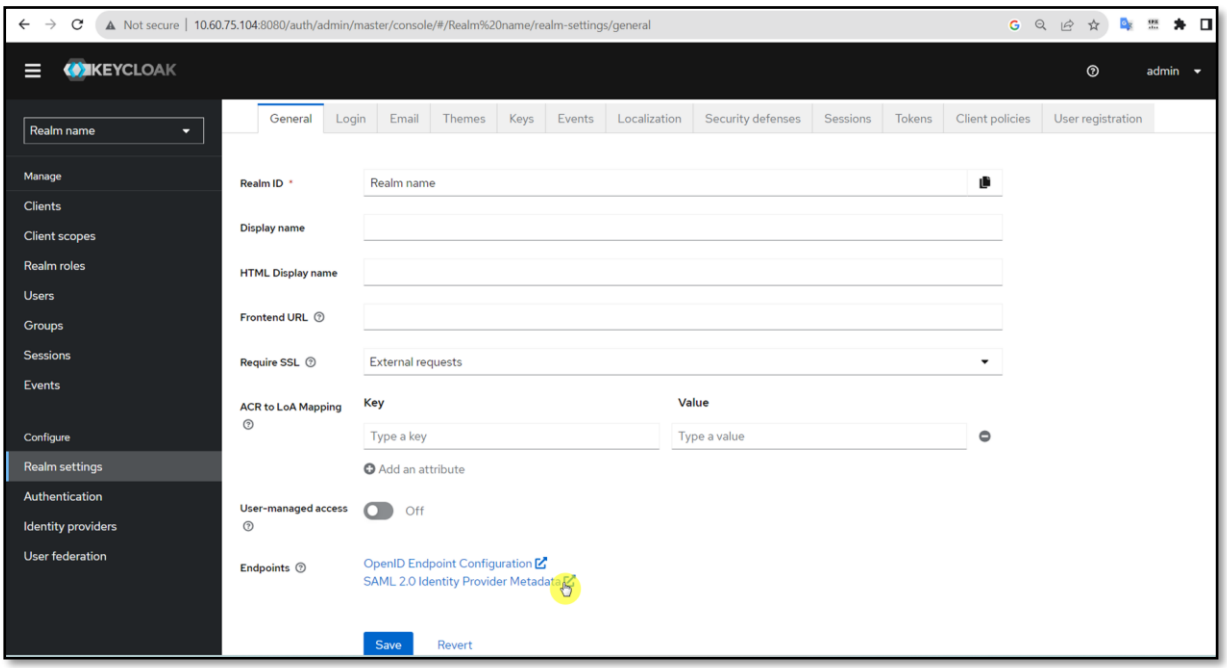
Чтобы начать настройку аутентификации и авторизации с помощью Keycloak, перейдите на вкладку «Login» в настройках вашего существующего Realm.



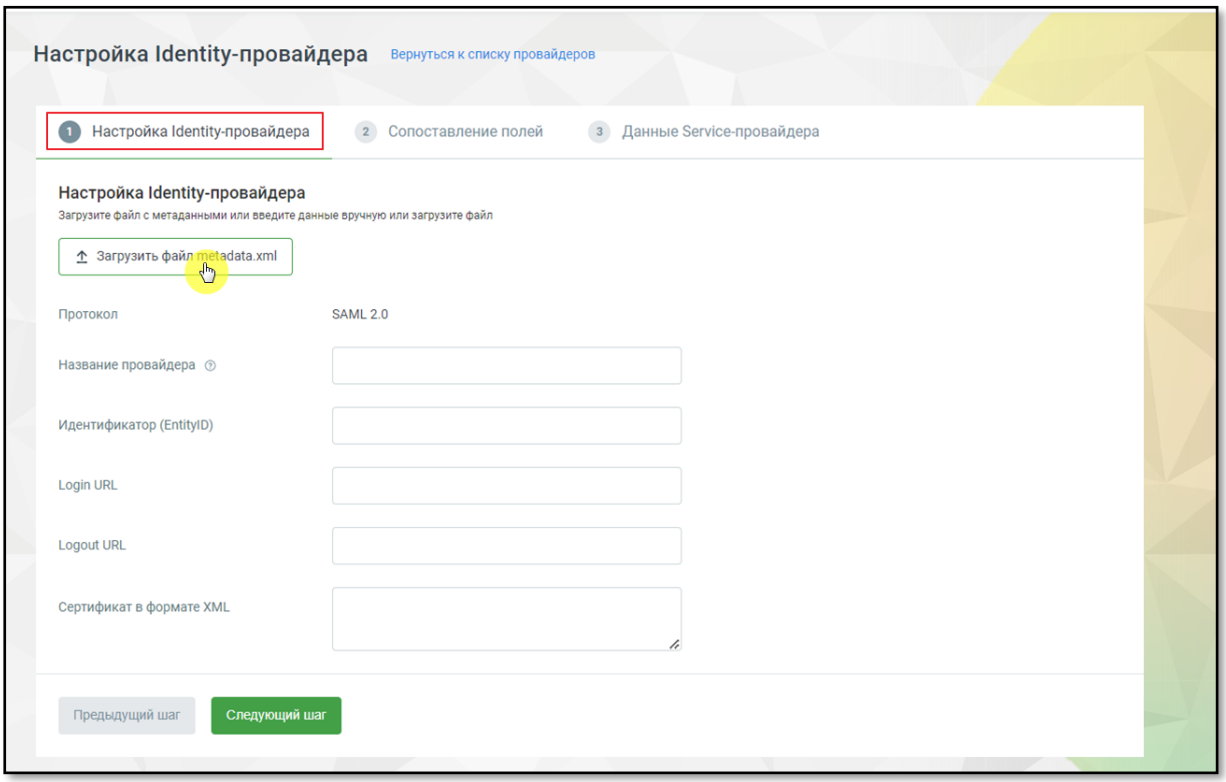
Далее установите переключатель «Email as username» («Email в качестве имени пользователя») в положение «включено». Это важно, чтобы после успешной авторизации вам предоставлялось значение адреса электронной почты в атрибуте «nameId». По умолчанию, адрес электронной почты используется как идентификатор.



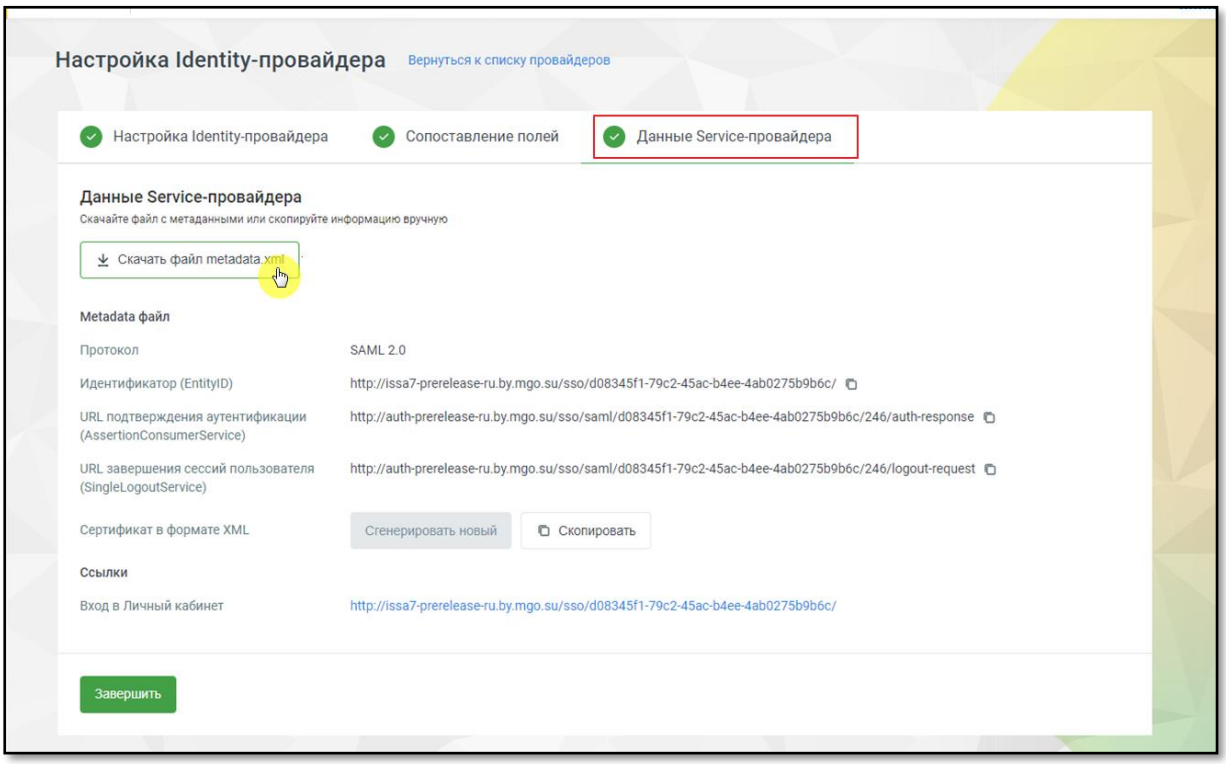
Кликнув на ссылку, экспортируйте настройки в формате XML для последующего импорта в Личный Кабинет MANGO OFFICE.



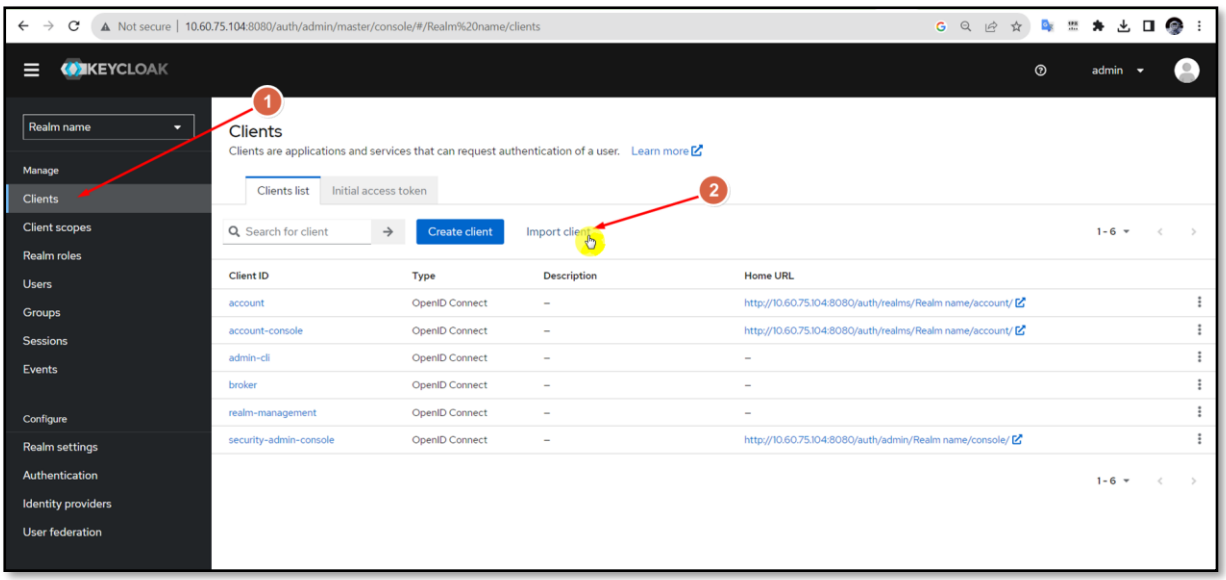
После сохранения настроек IdP (Identity Provider) в ЛК MANGO OFFICE, импортируйте полученный XML файл. Для этого нажмите на кнопку «Загрузить файл metadata.xml» на вкладке **Настройка Identity-провайдера**.



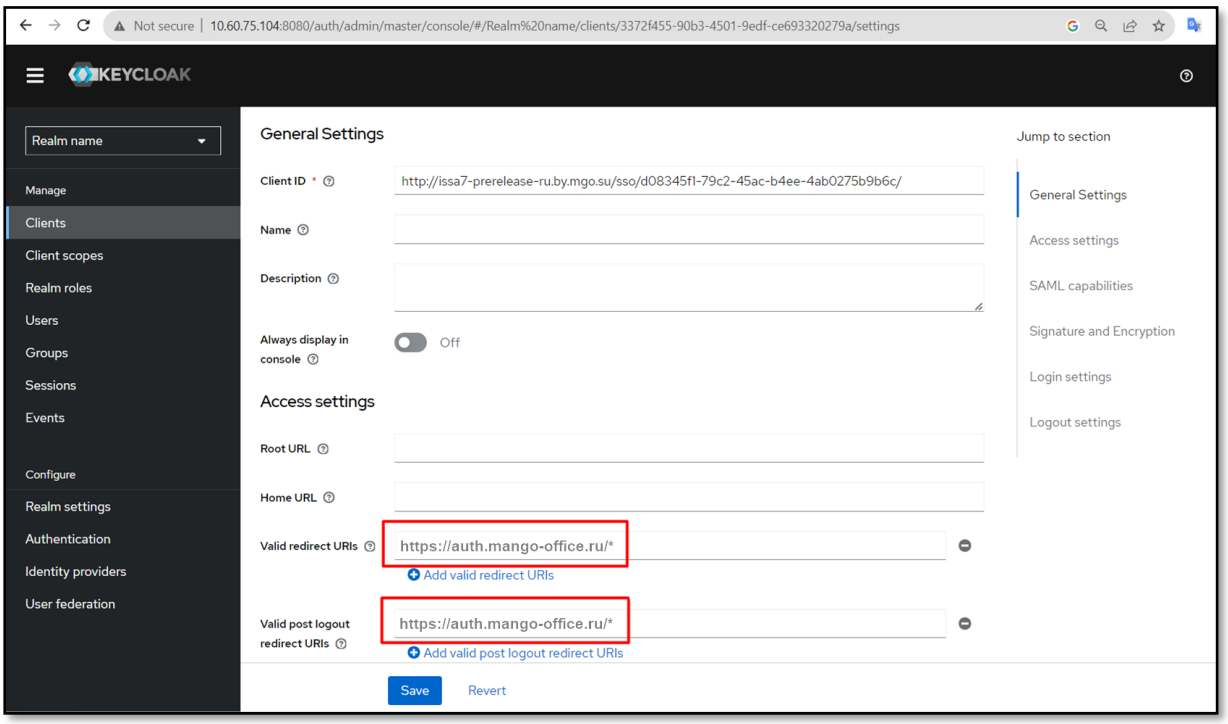
После успешного сохранения IdP в ЛК MANGO OFFICE скачайте файл с метаданными для последующего импорта в Keycloak. Для этого нажмите на кнопку «Скачать файл metadata.xml» на вкладке **Данные Service-провайдера**.



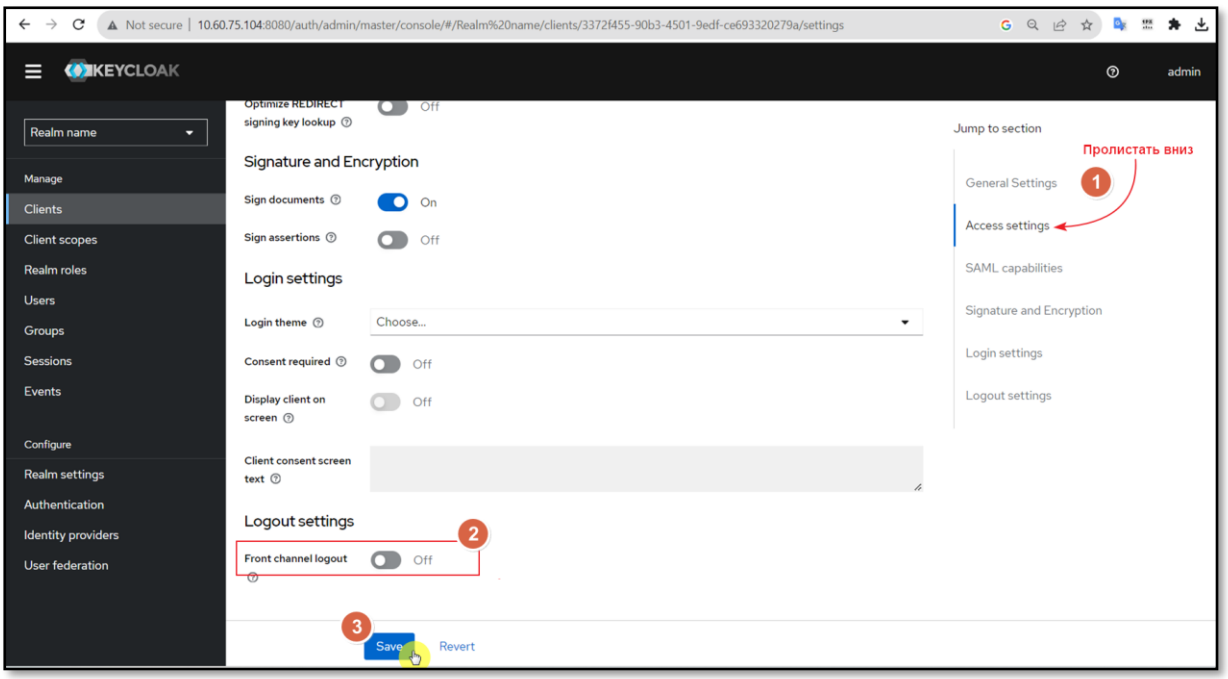
Вернитесь в Keycloak и перейдите на вкладку **Clients**. Затем импортируйте скачанный в шаге 5 файл с метаданными, нажав на кнопку «Import client».



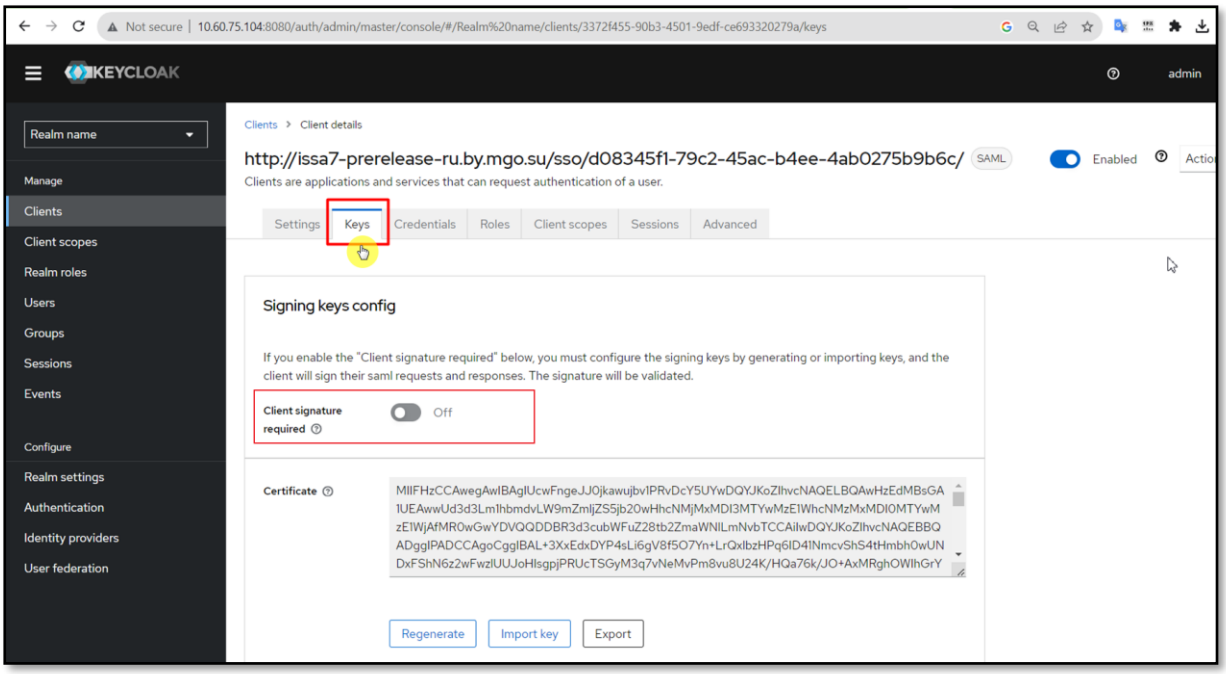
После импорта настроек, заполните параметры «Valid Redirect URIs» и «Valid Post Logout Redirect URIs» значением https://auth.mango-office.ru/*.



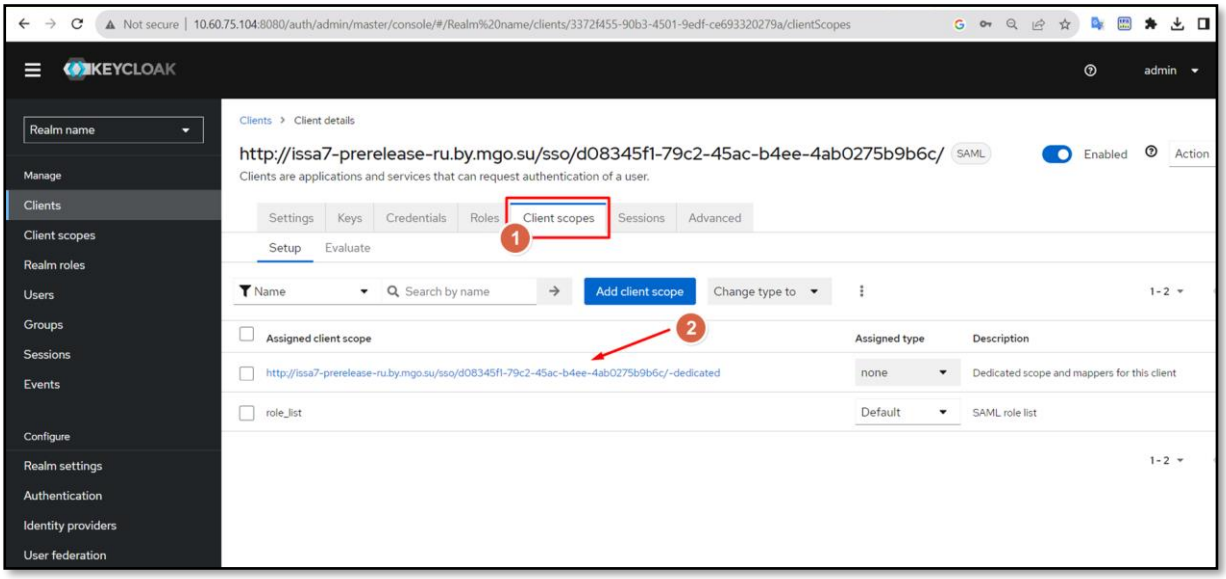
Пролистайте окно вкладки «Clients» вниз до подраздела ***Access setting***. Переведите переключатель «Front Channel Logout» в положение «выключено», чтобы Keycloak не инициировал автоматический выход пользователя из приложений. Сохраните внесенные изменения.



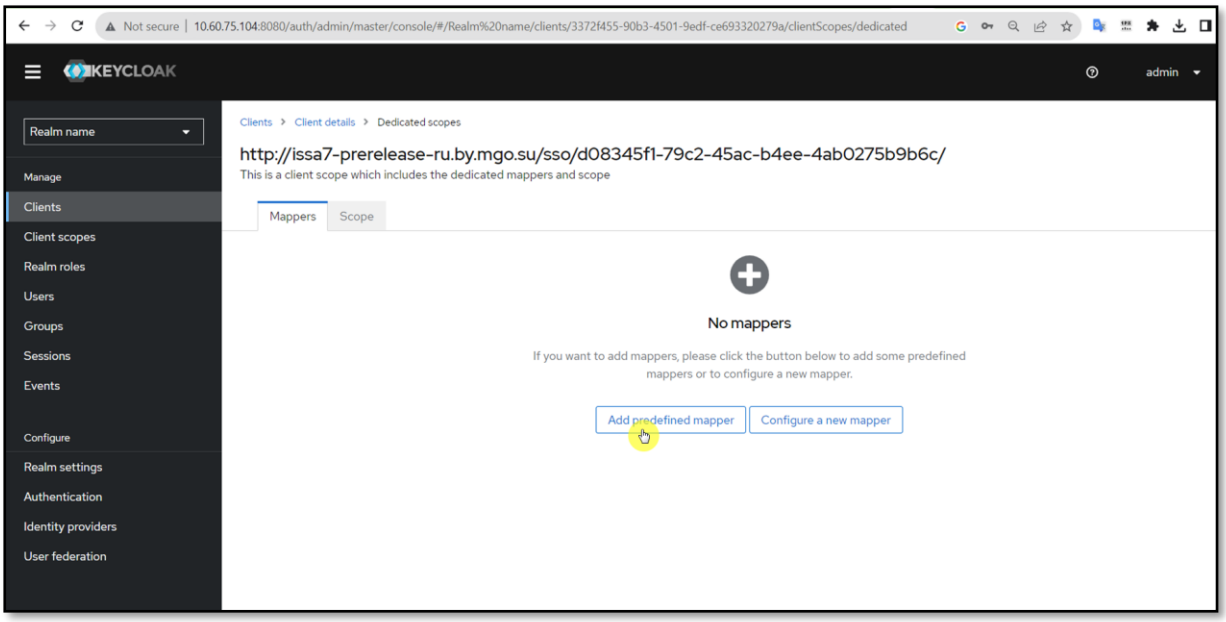
Перейдите на вкладку **Keys** и отключите переключатель «Client Signature Required».



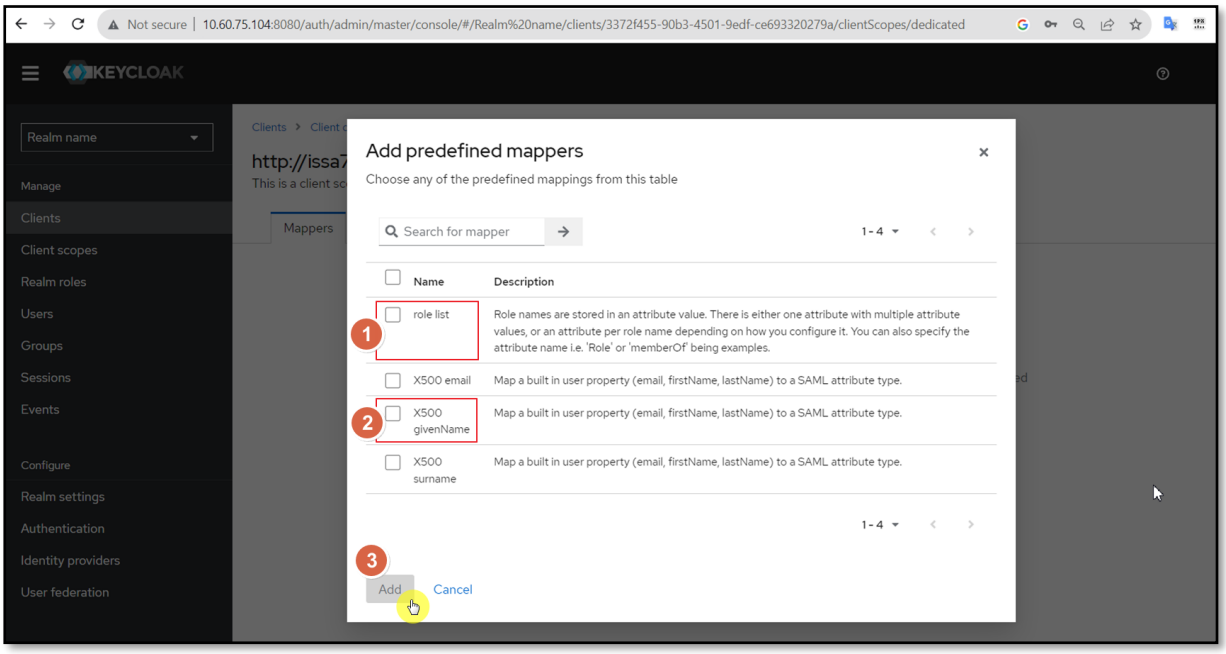
Перейдите на вкладку **Client Scopes** и добавьте новый маппер для сопоставления полей, настроенных в [Шаге 2](#) настройки IdP в ЛК MANGO OFFICE.



Нажмите кнопку «Add predefined mapper», чтобы добавить новый маппер.



Добавьте мапперу атрибуты (Роль и Имя).



Далее, на вкладке «Advanced», скопируйте URL-адреса, как показано на скриншотах, и сохраните изменения.