



MANGO
OFFICE

Аутентификация и авторизация в рамках SSO

Руководство пользователя

8 800 555 55 22

WWW.MANGO-OFFICE.RU

v2 | 2026



Содержание

v2 | 13.03.2026

1. Термины и определения	3
2. Общие сведения	4
3. Настройка IdP в ЛК ВАТС MANGO OFFICE	5
4. Добавление провайдера	6
Шаг 1. Настройка Identity-провайдера (IdP).....	6
Шаг 2. Сопоставление полей.....	8
5. Вход сотрудника в Личный кабинет ВАТС	12
6. Настройка аутентификации и авторизации на примере Keycloak.....	13

8 800 555 55 22

WWW.MANGO-OFFICE.RU



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.



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 ВАС МANGO 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 ВАС, 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 ВАС 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 BATC MANGO OFFICE

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

Безопасность и ограничения

Настройка Журнал действий Настройка доступа Ограничения SSO **NEW**

Single sign-on (SSO) [Как настроить](#)

Упростите вход и улучшите безопасность, подключив SSO. Управляйте доступом и правами пользователей централизованно.

⚠ Сотрудники смогут входить только через SSO после настройки хотя бы одного Identity-провайдера

0 Identity-провайдеров

+ Добавить нового Identity-провайдера

Активируйте услугу переключателем и переходите к добавлению нового провайдера. Максимальное количество провайдеров на продукте – 5.



4. Добавление провайдера

ШАГ 1. НАСТРОЙКА IDENTITY-ПРОВАЙДЕРА (IDP).

Настройка Identity-провайдера [Вернуться к списку провайдеров](#)

1 Настройка Identity-провайдера 2 Сопоставление полей 3 Данные Service-провайдера

Настройка Identity-провайдера
Загрузите файл с метаданными или введите данные вручную или загрузите файл

Протокол SAML 2.0

Название провайдера ?

Идентификатор (EntityID)

Login URL

Logout URL

Сертификат в формате XML

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.

8 800 555 55 22

WWW.MANGO-OFFICE.RU



```
0MyndmnNB1qV75qQR3b2/W5sGHRv+9AarggJkF+ptUkXoLtVA51wcfYm6
hILptpde5FQC8RWY1YrswBWAEZNFyrR4JeSweElNHg4NVOs4TwGjOPwWG
qzTfgTlECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAAAYR1Yf1SXAWoZpFf
wNiCQVE5d9zZ0DPzNdWhAybXcTyMf0z5mDf6FWBW5Gyoi9u3EMEDnzLcJ
NkwJAAC39Apa4I2/tml+Jy29dk8bTyX6m93ngmCgdLh5Za4khuU3AM3L6
3g7VexCu07kwkjh/+LqdcIXsVGO6XDfu2QOs1Xpe9zIzLpwm/RNYeXUjb
Sj5ce/jekpAw7qyVVL4xOyh8AtUW1ek3wIw1MJvEgEPT0d16oshWJpoS1
OT8Lr/22SvYEO3EmSGdTVGgk3x3s+A0qWAqTcyjr7Q4s/GKYRffomGwz0
TZ4Iw1ZN99Mm0eo2US1SRTV17QHRtuiuSThHpLKQQ==</ds:X509Certi
ficate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect» Location="https://ads-test.by.mgo.su/ads-
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://ads-test.by.mgo.su/ads-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>
```

8 800 555 55 22

WWW.MANGO-OFFICE.RU

ШАГ 2. СОПОСТАВЛЕНИЕ ПОЛЕЙ

На втором этапе настройки требуется указать имена атрибутов для точного сопоставления с учетной записью при процедуре авторизации, а также сопоставить роли сотрудников.

ВНИМАНИЕ

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



✓ Настройка Identity-провайдера 2 Сопоставление полей 3 Данные Service-провайдера

Сопоставление полей

Сопоставьте названия полей из assert-ов на данные сотрудника. Поля должны находиться в секции Attributes

Поля в MANGO OFFICE	Поля в вашей системе
Фамилия имя отчество	givenName
Роль сотрудника	http://schemas.xmlsoap.org/claims/Group

Настройка соответствия ролей

Настройки сопоставления

- Не использовать e-mail в качестве параметра идентификатора
- Автоматически создавать учетную запись SIP для новых сотрудников
- Автоматическое назначение групп

Настройка соответствия ролей

Роль в MANGO OFFICE	Группа доменной системы
Сотрудник	Введите соответствие роли Сотрудник
Бухгалтер	Введите соответствие роли Бухгалтер
Администратор	Администратор
Старший сотрудник	Введите соответствие роли Старший сотрудник
Руководитель группы	Введите соответствие роли Руководитель группы

ВНИМАНИЕ

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

Можно привязать несколько доменных групп к одной роли «Сотрудник» (перечислив их через запятую). Если сотрудник подходит под разные роли, система автоматически выберет ту, у которой выше приоритет.

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 ранее 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.

Настройка Identity-провайдера [Вернуться к списку провайдеров](#)

✓ Настройка Identity-провайдера ✓ Сопоставление полей ✓ Данные Service-провайдера

Данные Service-провайдера
Скачайте файл с метаданными или скопируйте информацию вручную

↓ Скачать файл metadata.xml

Metadata файл

Протокол	SAML 2.0
Идентификатор (EntityID)	http://issa7-prerelease-ru.by.mgo.su/sso/a3212343-dcac-43fc-81f7-25a330dfbc56/
URL подтверждения аутентификации (AssertionConsumerService)	http://auth-prerelease-ru.by.mgo.su/sso/saml/a3212343-dcac-43fc-81f7-25a330dfbc56/24/auth-response
URL завершения сессий пользователя (SingleLogoutService)	http://auth-prerelease-ru.by.mgo.su/sso/saml/a3212343-dcac-43fc-81f7-25a330dfbc56/24/logout-request

Сертификат в формате XML

Ссылки

Вход в Личный кабинет <http://issa7-prerelease-ru.by.mgo.su/sso/a3212343-dcac-43fc-81f7-25a330dfbc56/>

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**.



Безопасность и ограничения

Настройка | Журнал действий | Настройка доступа | Ограничения | SSO NEW

Single sign-on (SSO) 🔗 Как настроить

Упростите вход и улучшите безопасность, подключив SSO. Управляйте доступом и правами пользователей централизованно.

5 Identity-провайдеров

ADFS <input checked="" type="checkbox"/> SAML 2.0	Keycloak <input checked="" type="checkbox"/> SAML 2.0	Oracle Identity Foundation <input type="checkbox"/> SAML 2.0	Azure AD <input checked="" type="checkbox"/> SAML 2.0	Okta <input checked="" type="checkbox"/> SAML 2.0
--	--	---	--	--

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

8 800 555 55 22

WWW.MANGO-OFFICE.RU



5. Вход сотрудника в Личный кабинет ВАТС

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

облачные
бизнес-
коммуникации

Вход в Личный кабинет

Войти через Keycloak

Войти через Azure

Чем заняты ваши конкуренты?
Сервис анализа контекстной
рекламы и органического трафика

Проверить конкурентов

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.

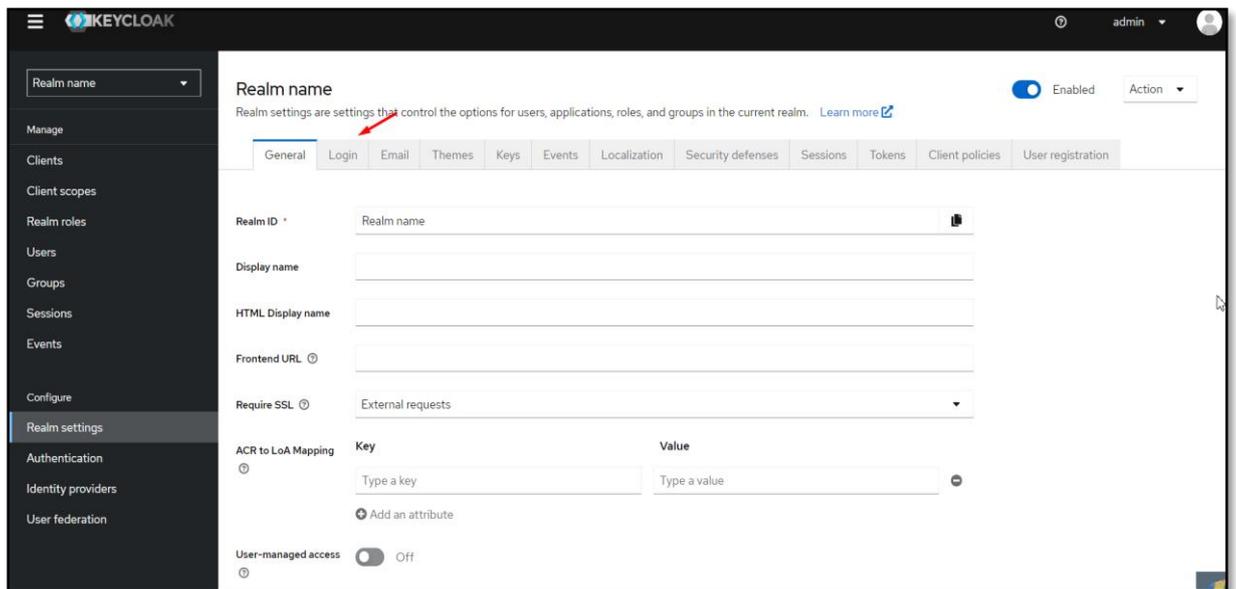
СОВЕТ

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.

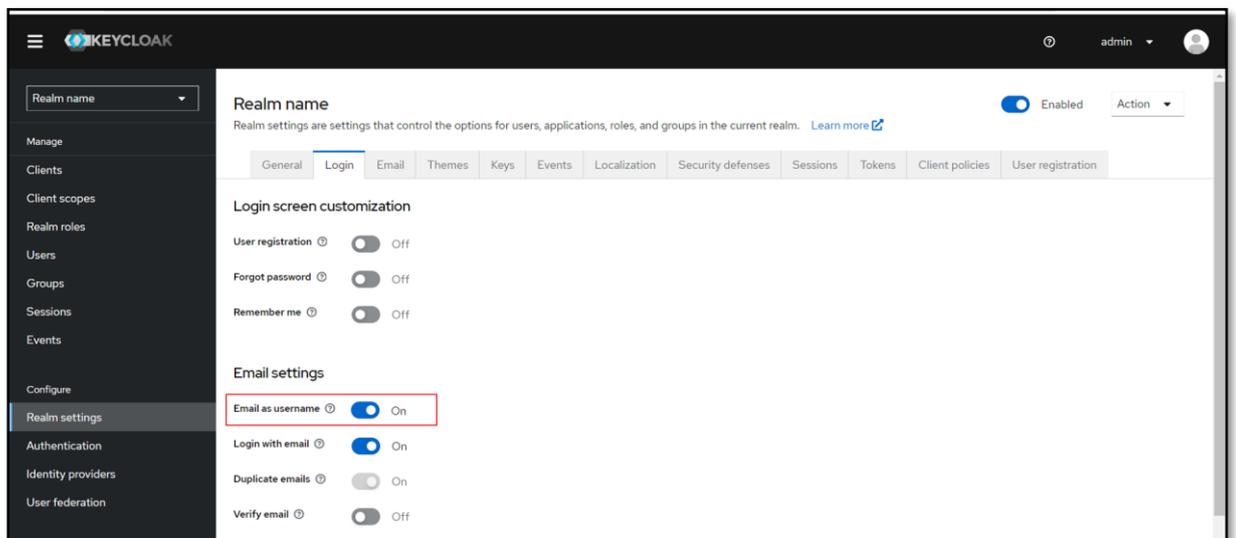


6. Настройка аутентификации и авторизации на примере Keycloak

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.





MANGO
OFFICE

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

The screenshot shows the Keycloak Admin Console interface. The left sidebar contains a menu with 'Realm settings' highlighted. The main content area shows the 'General' tab of the 'Realm settings' page. The 'SAML 2.0 Identity Provider Metadata' link is highlighted with a yellow circle and a hand cursor. A red circle highlights the 'Realm settings' menu item in the left sidebar.

8 800 555 55 22

WWW.MANGO-OFFICE.RU



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**.

Настройка Identity-провайдера [Вернуться к списку провайдеров](#)

1 Настройка Identity-провайдера 2 Сопоставление полей 3 Данные Service-провайдера

Настройка Identity-провайдера
Загрузите файл с метаданными или введите данные вручную или загрузите файл

↑ Загрузить файл metadata.xml

Протокол SAML 2.0

Название провайдера

Идентификатор (EntityID)

Login URL

Logout URL

Сертификат в формате XML

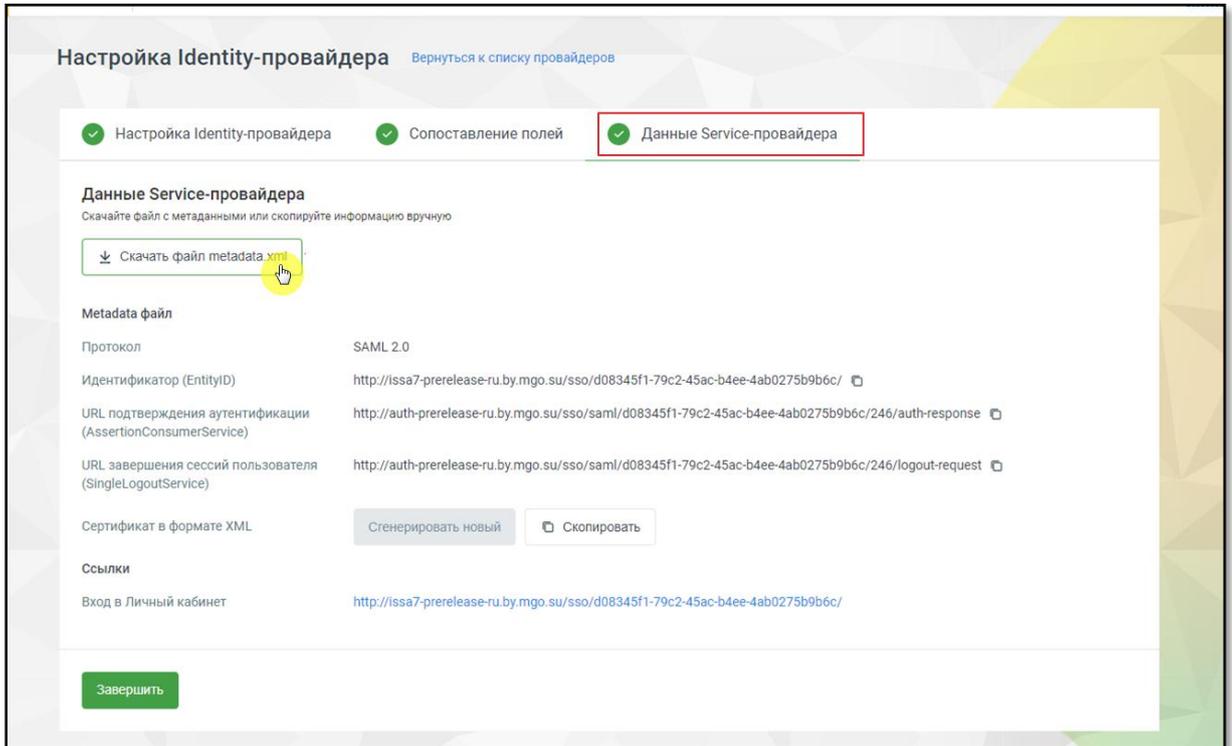
Предыдущий шаг Следующий шаг

Поле «Название провайдера» заполните самостоятельно, остальные поля подтянутся из файла metadata.xml.

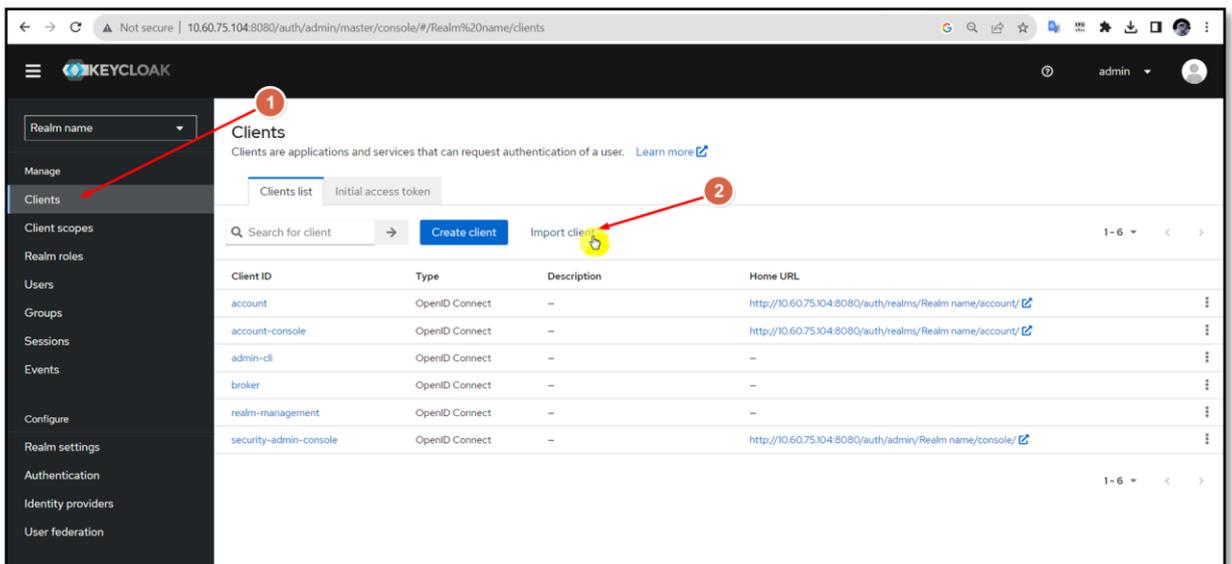
В ЛК ВАТС произведите сопоставление полей в соответствии с [Шагом 2](#).



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**.

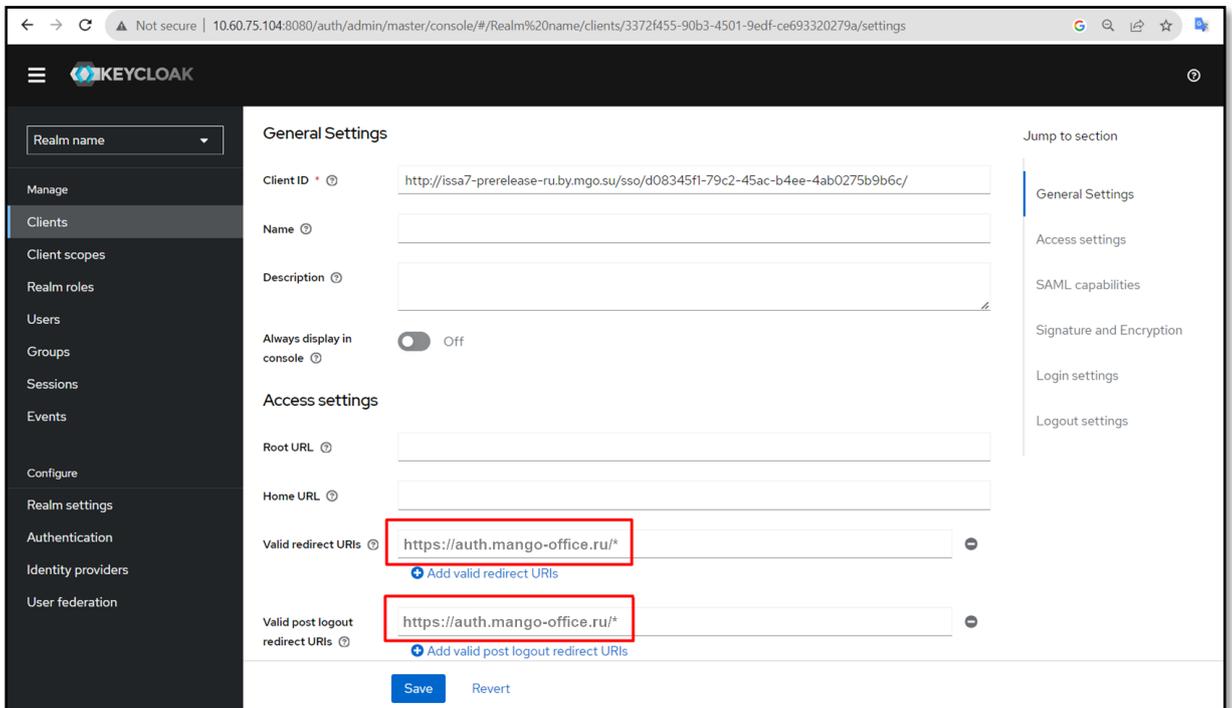


Вернитесь в Keycloak и перейдите на вкладку **Clients**. Затем импортируйте скачанный в шаге 5 файл с метаданными, нажав на кнопку «Import client».

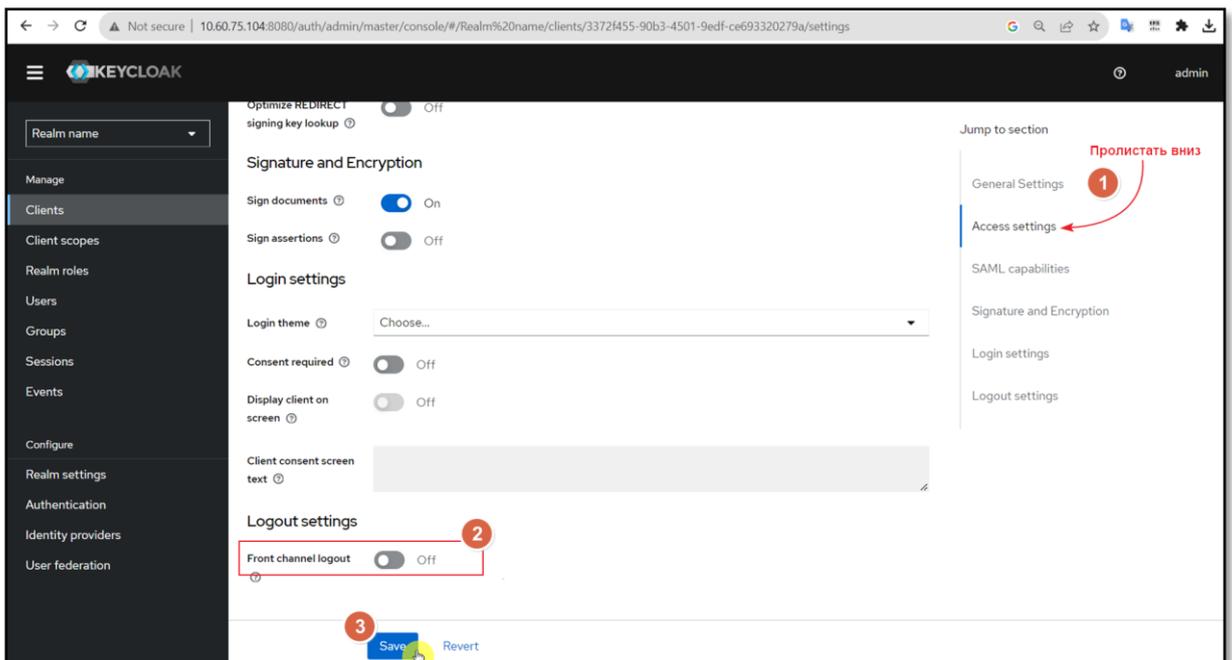




После импорта настроек, заполните параметры «Valid Redirect URIs» и «Valid Post Logout Redirect URIs» значением <https://auth.mango-office.ru/>*



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

The screenshot shows the Keycloak administration console. The left sidebar contains navigation options: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'Client details' for the client 'http://issa7-prerelease-ru.by.mgo.su/sso/d08345f1-79c2-45ac-b4ee-4ab0275b9b6c/'. The 'Client scopes' tab is selected and highlighted with a red box and a red circle with the number '1'. Below the tabs, there is a search bar and an 'Add client scope' button. A table lists assigned client scopes with columns for 'Assigned client scope', 'Assigned type', and 'Description'. A red arrow points from the 'Add client scope' button to the table, with a red circle and the number '2' next to it.

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

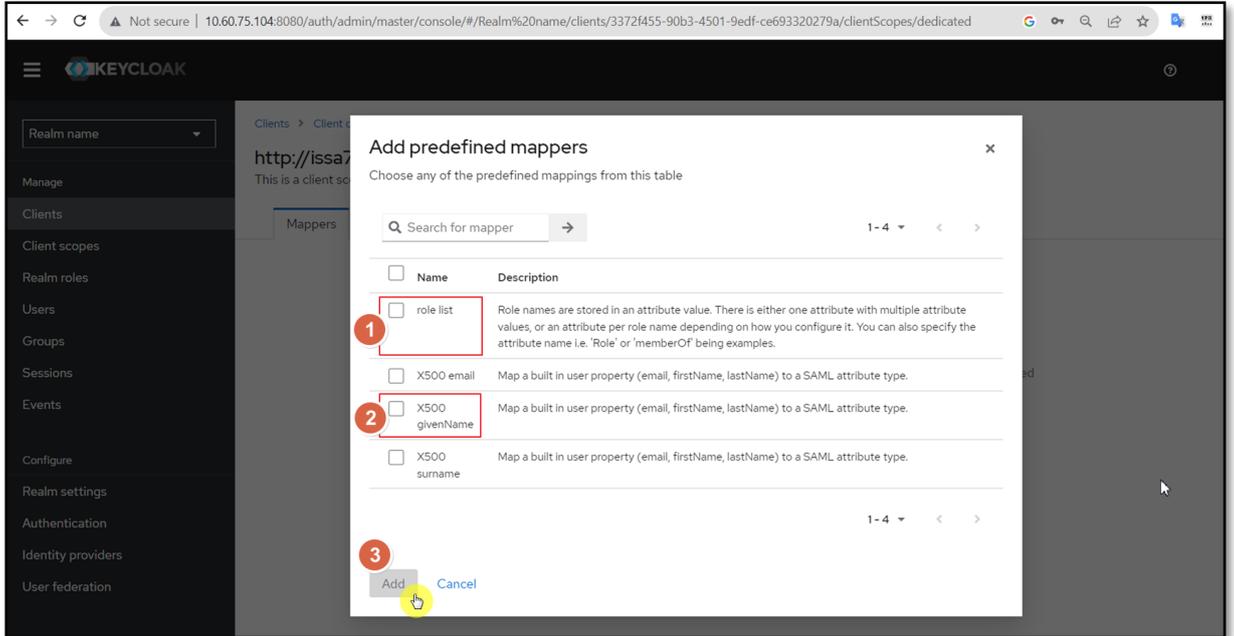
The screenshot shows the 'Dedicated scopes' configuration page in Keycloak. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Dedicated scopes' for the same client. It shows a '+ No mappers' message and a note: 'If you want to add mappers, please click the button below to add some predefined mappers or to configure a new mapper.' There are two buttons: 'Add predefined mapper' and 'Configure a new mapper'. A yellow circle with a mouse cursor is positioned over the 'Add predefined mapper' button.

8 800 555 55 22

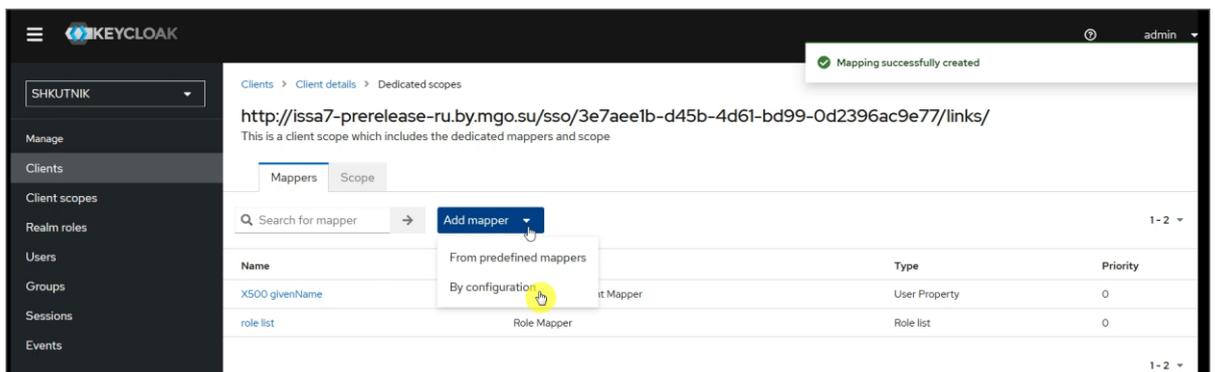
WWW.MANGO-OFFICE.RU



Добавьте мапперу атрибуты (Роль и Имя).



В разделе **Clients** на вкладке **Dedicated scopes** → **Mappers** нажмите кнопку **Add mapper** и в раскрывающемся списке выберите **By configuration**, чтобы создать новый маппер с ручной настройкой параметров.



8 800 555 55 22

WWW.MANGO-OFFICE.RU



В открывшемся окне **Configure a new mapper** выберите тип маппера **User Attribute**. Этот тип используется для передачи пользовательского атрибута Keycloak в SAML-атрибут.

The screenshot shows the 'Configure a new mapper' dialog in Keycloak. The dialog lists several mapper types. The 'User Attribute' option is highlighted with a red dashed box and a yellow circle. A success message 'Mapping successfully created' is visible in the top right corner.

Name	Description
Audience	Add specified audience to the audience conditions in the assertion.
Audience Resolve	Adds all client_ids of "allowed" clients to the audience conditions in the assertion. Allowed client means any SAML client for which user has at least one client role
Group list	Group names are stored in an attribute value. There is either one attribute with multiple attribute values, or an attribute per group name depending on how you configure it. You can also specify the attribute name i.e. 'member' or 'memberOf' being examples.
Hardcoded attribute	Hardcode an attribute into the SAML Assertion.
Hardcoded role	Hardcode role into SAML Assertion.
Role list	Role names are stored in an attribute value. There is either one attribute with multiple attribute values, or an attribute per role name depending on how you configure it. You can also specify the attribute name i.e. 'Role' or 'memberOf' being examples.
Role Name Mapper	Map an assigned role to a new name
User Attribute	Map a custom user attribute to a SAML attribute.
User Attribute Mapper For NameID	Map user attribute to SAML NameID value.
User Property	Map a built in user property (email, firstName, lastName) to a SAML attribute type.

Заполните параметры маппера для передачи групп пользователя в SAML-ответе:

- в поле **Name** укажите имя SAML-атрибута, которое используется в целевой системе;
- в поле **User Attribute** укажите имя пользовательского атрибута, в котором в Keycloak будут храниться значения групп;
- в поле **Friendly Name** укажите удобочитаемое имя атрибута, которое будет использоваться в SAML-утверждении;
- в поле **SAML Attribute Name** укажите имя атрибута, ожидаемое сервис-провайдером;
- в поле **SAML Attribute NameFormat** оставьте значение **Basic** или укажите формат, требуемый принимающей системой.

После заполнения параметров нажмите **Save**, чтобы сохранить маппер.

Имя атрибута должно совпадать с тем значением, которое используется при сопоставлении полей на стороне сервис-провайдера.



Clients > Client details > Dedicated scopes > Mapper details

Add mapper

If you want more fine-grain control, you can create protocol mapper on this client

Mapper type: User Attribute

Name * ⓘ:

User Attribute ⓘ:

Friendly Name ⓘ:

SAML Attribute Name ⓘ:

SAML Attribute NameFormat ⓘ: Basic

Aggregate attribute values ⓘ: Off

8 800 555 55 22

Откройте вкладку **Mappers** и убедитесь, что созданный маппер (в примере - `http://schemas.xmlsoap.org/claims/Group`) появился в списке.

Name	Category	Type	Priority
http://schemas.xmlsoap.org/claims/Group	AttributeStatement Mapper	User Attribute	0
X500 givenName	AttributeStatement Mapper	User Property	0
role list	Role Mapper	Role list	0

Mapper type: User Property

Name * ⓘ: X500 givenName

Property ⓘ: firstName

Friendly Name ⓘ: **givenName**

SAML Attribute Name ⓘ: urn:oid:2.5.4.42

SAML Attribute NameFormat ⓘ: urn:oasis:names:tc:SAML:2.0:attrname-format-uri

WWW.MANGO-OFFICE.RU



Проверьте, что его тип указан как **User Attribute**, а категория – **AttributeStatement Mapper**.

Откройте маппер **X500 givenName**. Убедитесь, что заданы следующие параметры:

- **Mapper type** – User Property;
- **Property** – firstName;
- **Friendly Name** – givenName;
- **SAML Attribute Name** – urn:oid:2.5.4.42;
- **SAML Attribute NameFormat** –
urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

Эта настройка обеспечивает передачу имени пользователя в SAML-ответе.

Перейдите в раздел **Users**, откройте карточку пользователя и выберите вкладку **Attributes**.

The screenshot shows the Mango Office web interface. On the left is a navigation menu with 'Users' selected. The main area displays the 'Users' section with a search bar and a table of users. A user card for '1@test.com' is open, showing tabs for 'Details', 'Attributes', 'Credentials', 'Role mapping', 'Groups', 'Consents', 'Identity provider links', and 'Sessions'. The 'Attributes' tab is active, showing a table of user attributes. One attribute is highlighted with a red dashed box: Key: http://schemas.xmlsoap.org/claims/Group, Value: CN=Администратор, OU=Mango, OU=SecurityGroups, DC=tcp, DC=... The 'Credentials' tab is also visible, showing a password field.

Добавьте атрибут с ключом `http://schemas.xmlsoap.org/claims/Group`. В поле значения укажите группы пользователя, например:

- CN=Администратор, OU=Mango, OU=SecurityGroups

Сохраните изменения. Добавленные атрибуты будут передаваться через настроенный маппер в SAML-ответе при аутентификации пользователя.