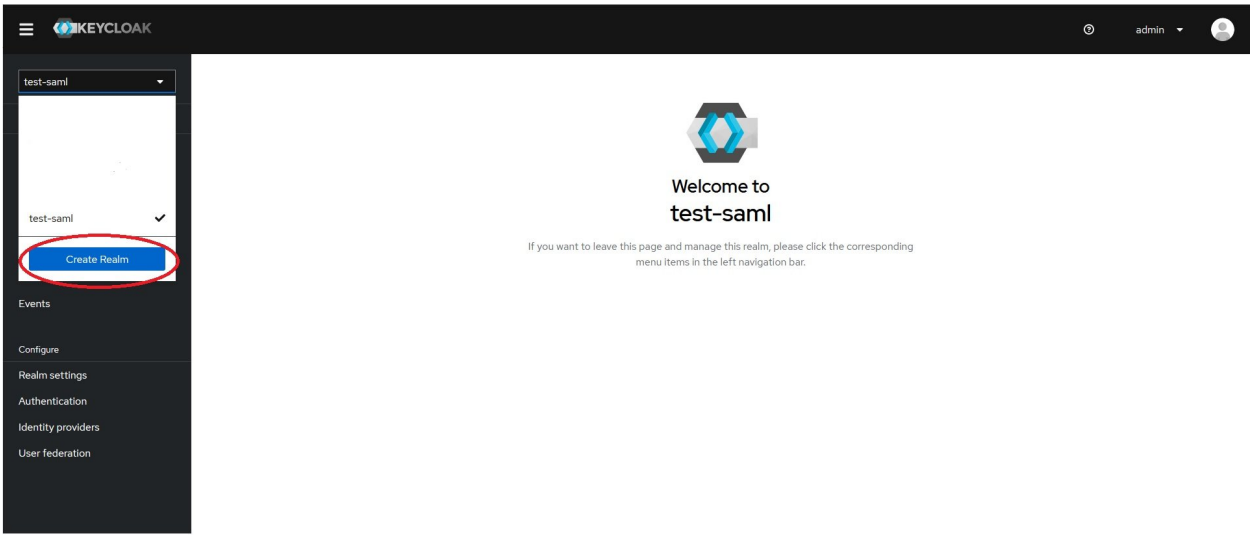
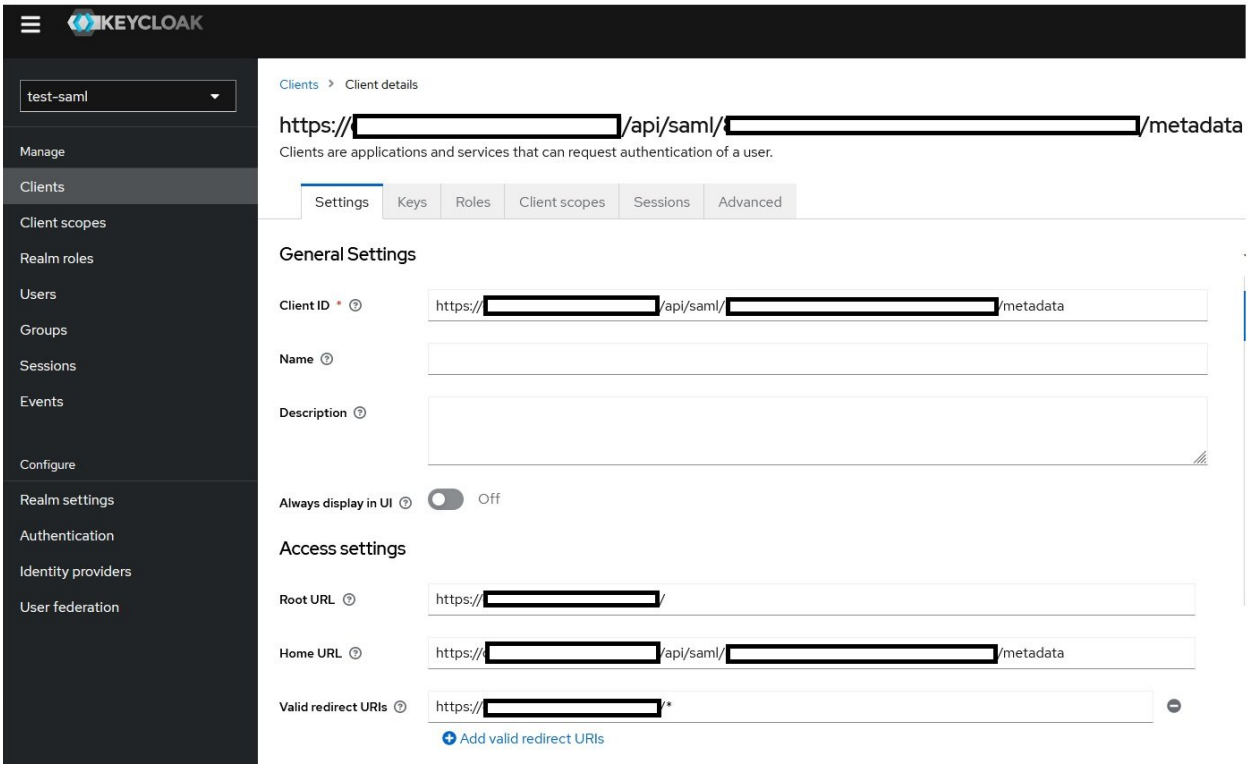
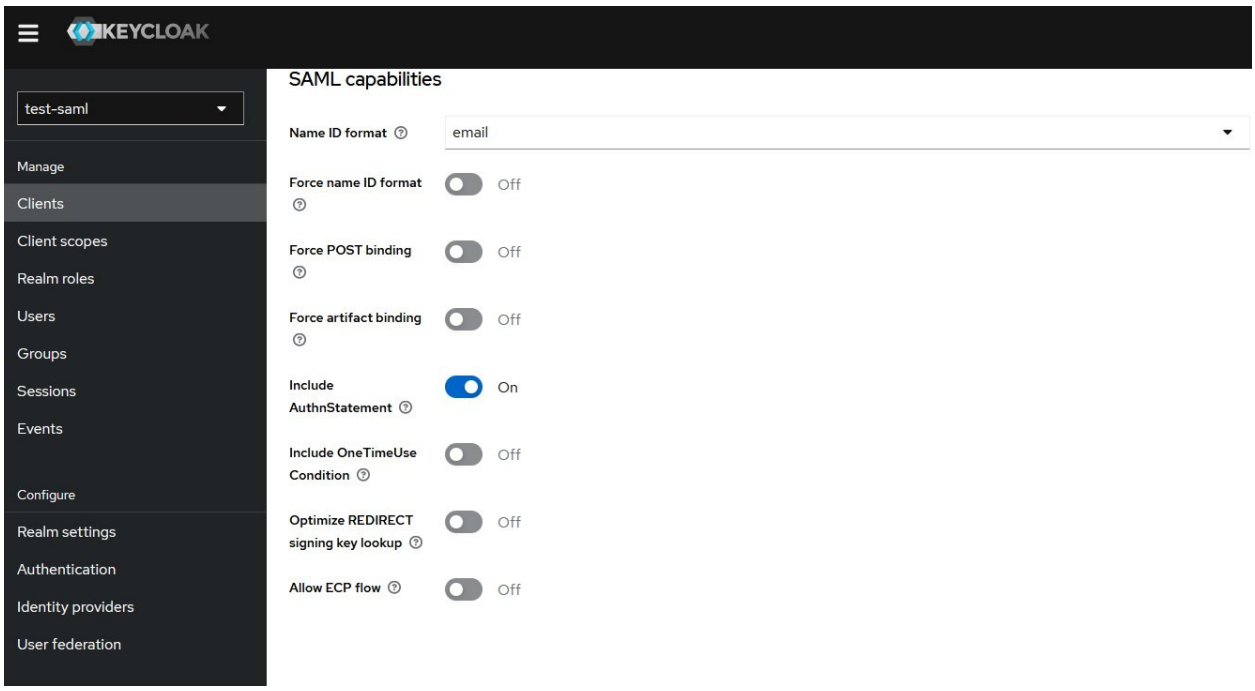
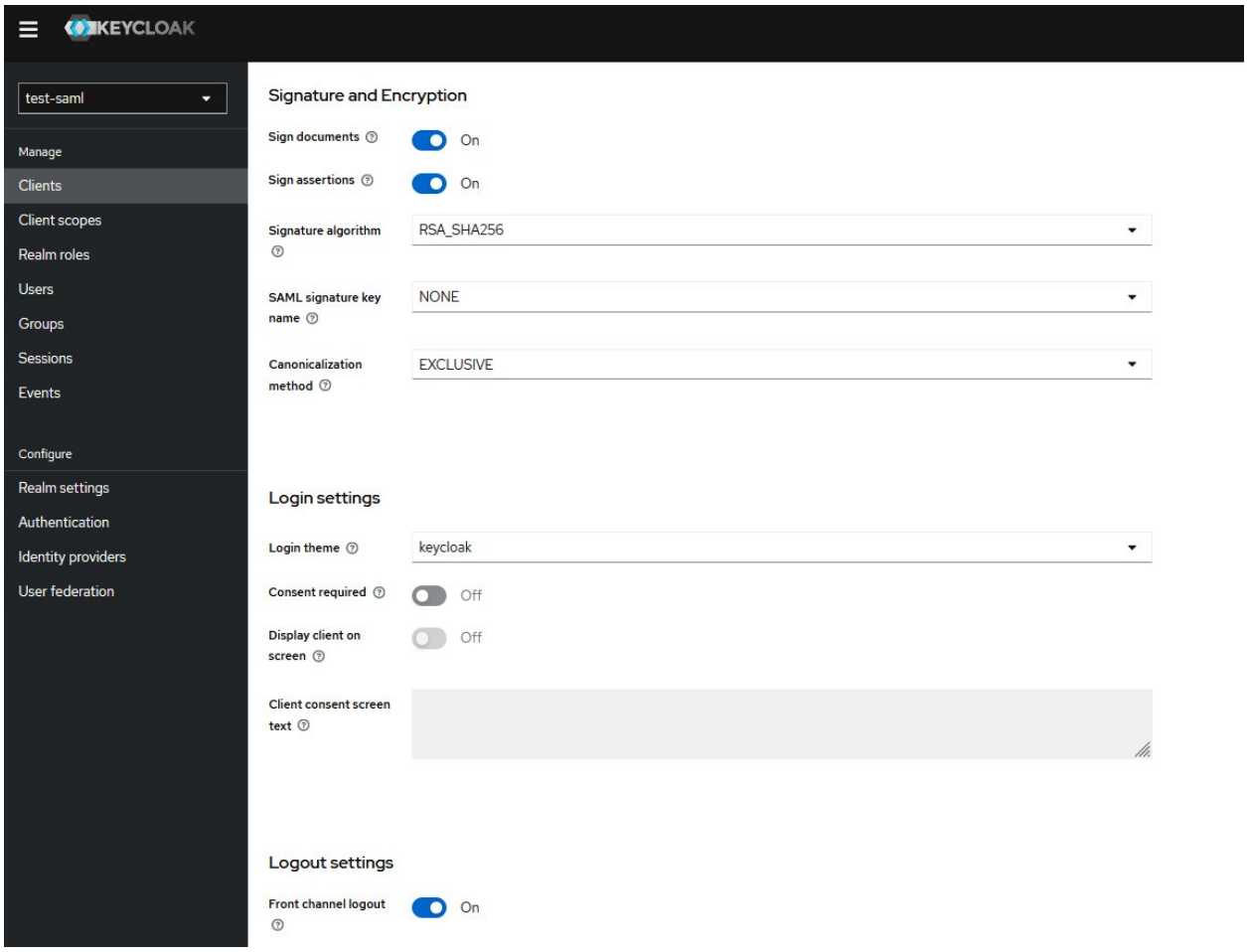
Создать новый Realm.



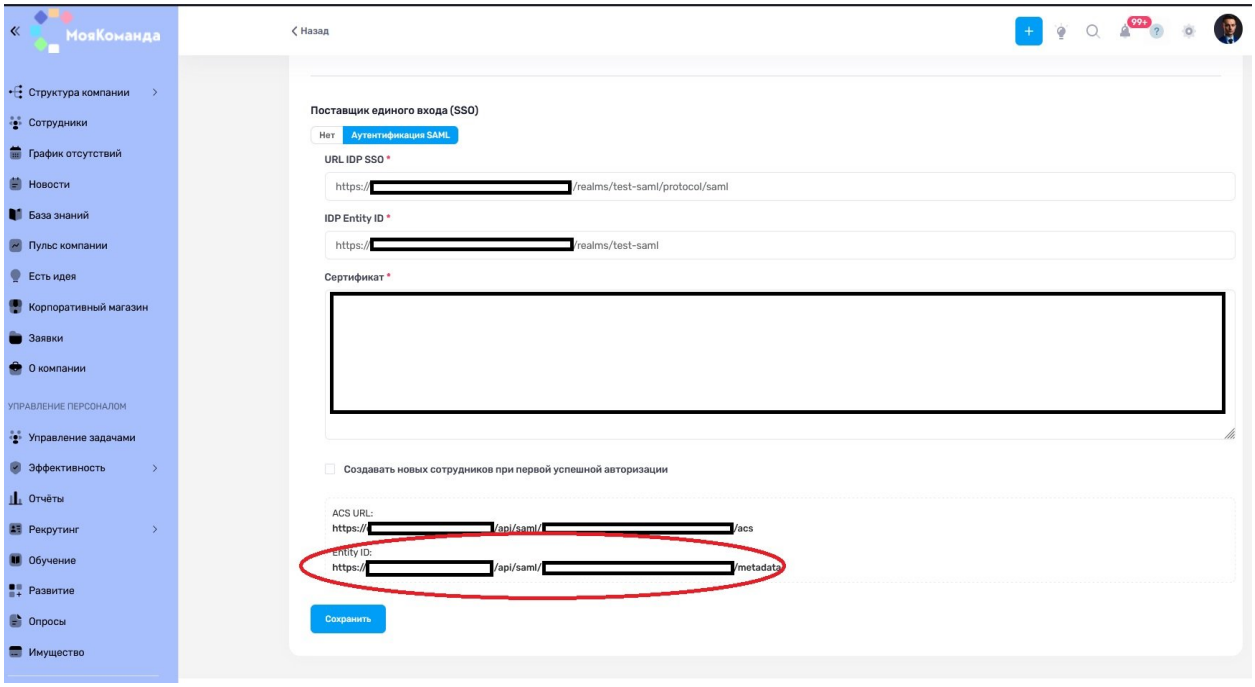
Создать новый Client. Перейдите на вкладку Clients. Заполните поля.



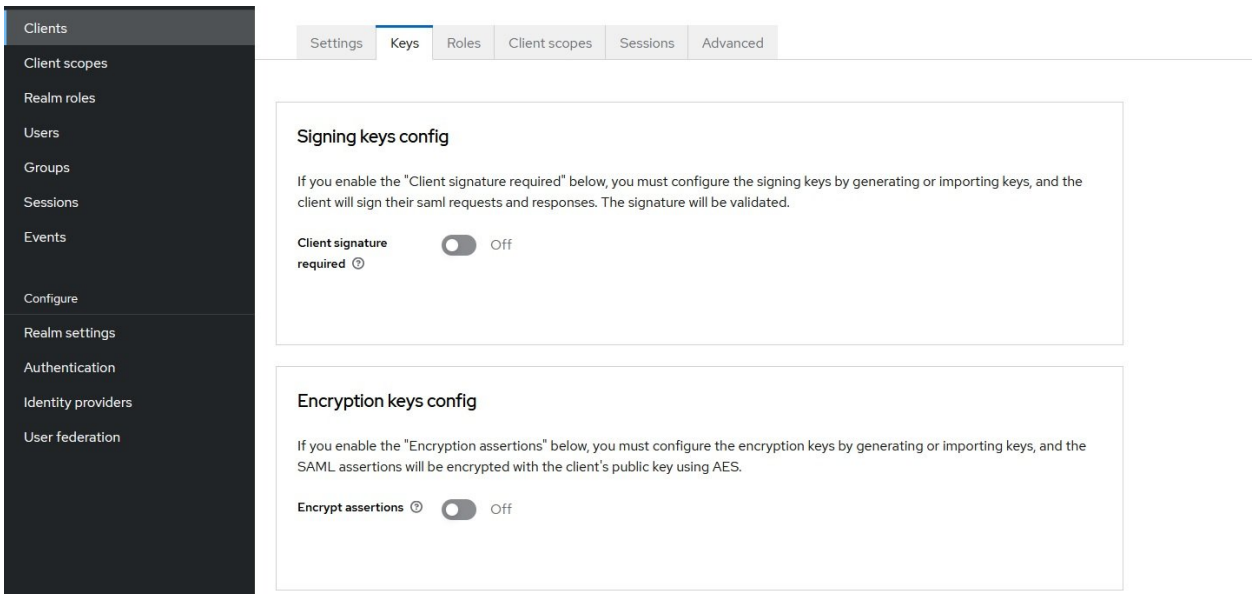




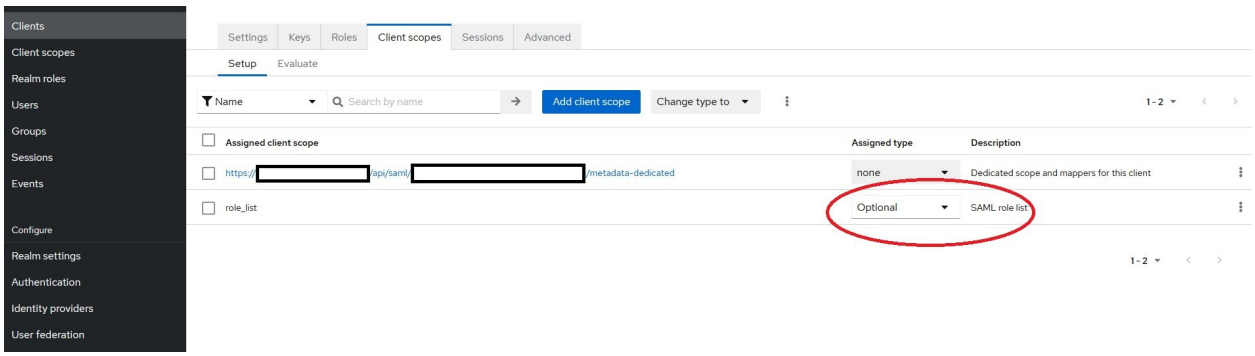
В «Моей команде» перейти в меню «Настройки» - «Аутентификация», активировать «Аутентификация SAML», скопировать значение «Entity ID» и вставить в Keycloak в поля «Client ID» и «Home URL». В поле «Root URL» указать адрес сервиса «Моя команда».



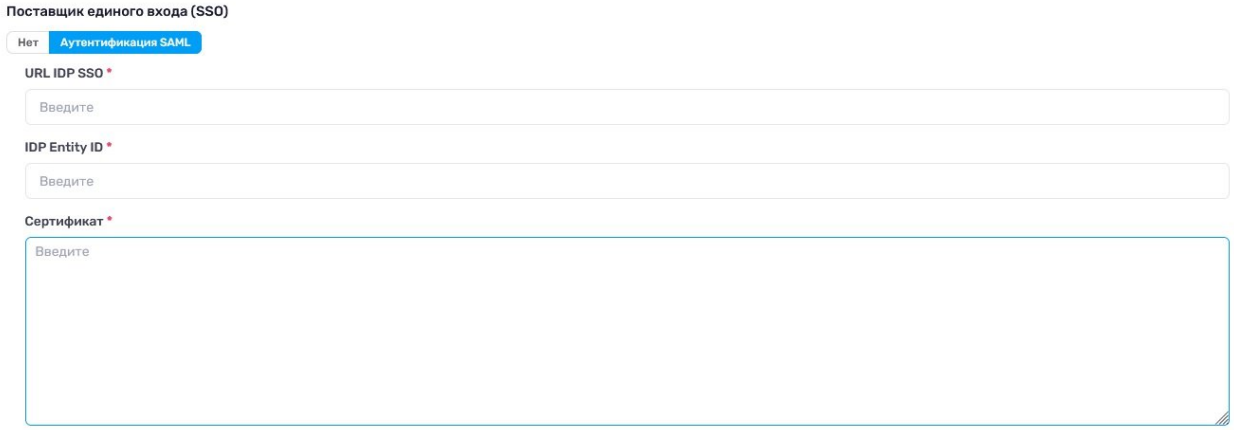
Перейти в раздел «Keys», проверить что все опции отключены.



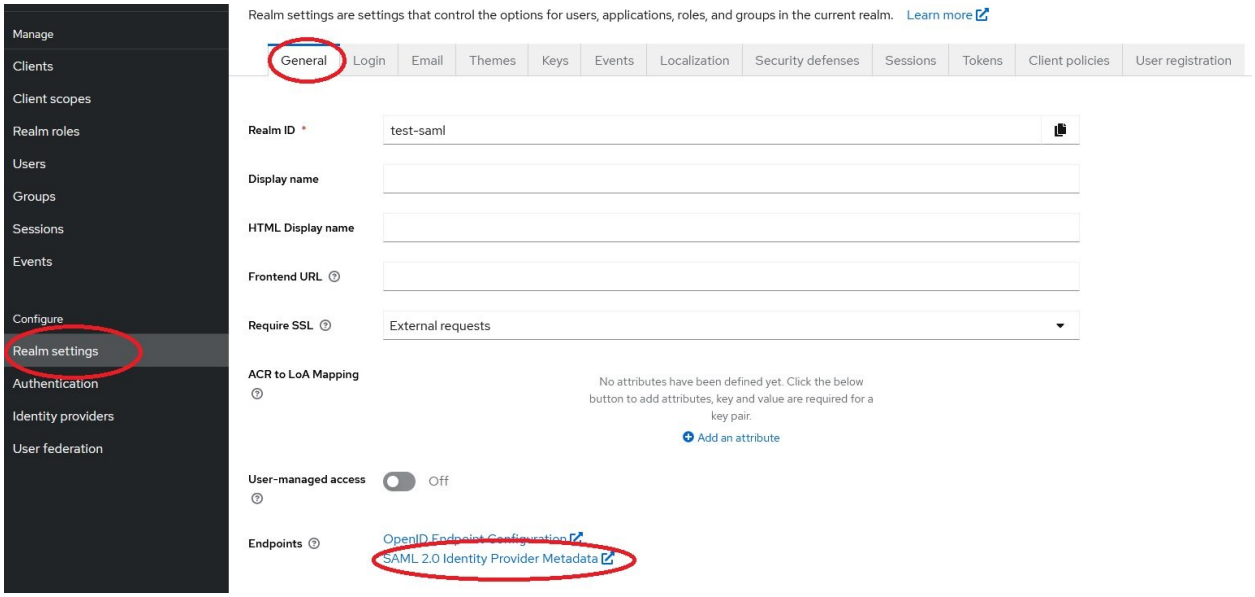
В разделе «Client scopes». Установите для role_list параметр «Assigned type» в значение Optional (по умолчанию там Default).



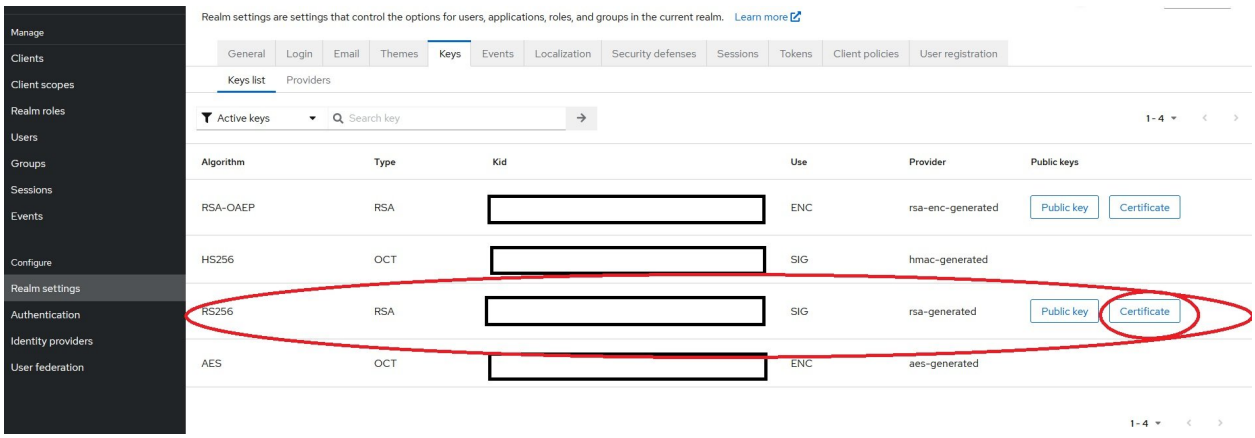
В моей команде заполнить поля «URL IDP SSO», «IDP Entity ID» и «Сертификат».



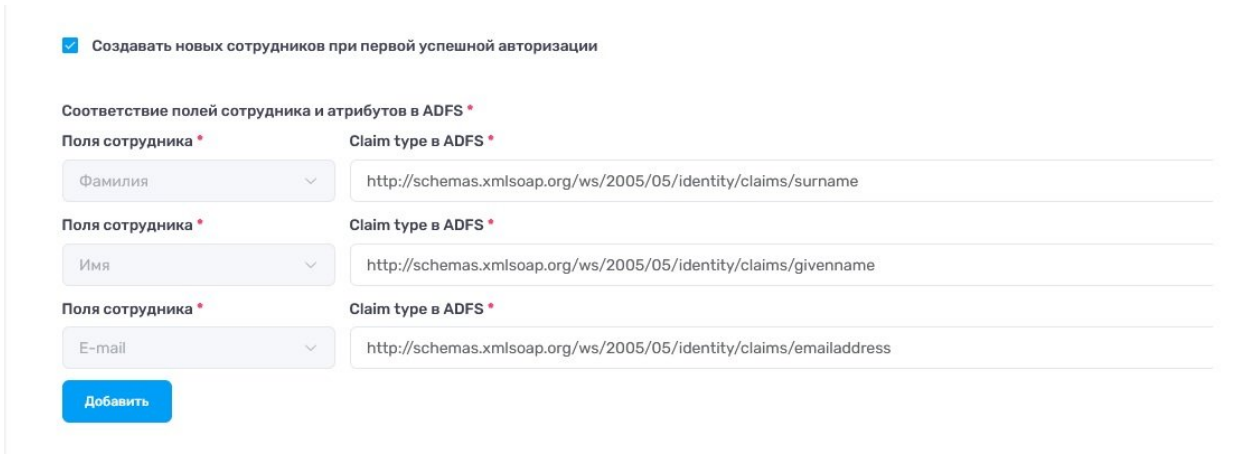
Данные для полей «URL IDP SSO», «IDP Entity ID» находятся в Keycloak, Realm Settings (Раздел меню слева, секция Configure), вкладка Genetal, ссылка SAML 2.0 Identity Provider Metadata.



Сертификат находится в Keycloak, Realm Settings (Раздел меню слева, секция Configure). Вкладка «Keys», необходим сертификат «SIG».



Включаем в «Моей команде» функцию «Создавать новых сотрудников при первой успешной авторизации».



В Keycloak переходим в «Clients»(Раздел меню слева), вкладка «Client scopes», выбираем ранее созданного клиента. Создаем «Mappers» с типом «User Attribute». Данные для поля «SAML Attribute Name» берем из «Моей команды» в соответствующих полях «Claim type в ADFS». В поле «User attribute» указать значение атрибута которое используется в вашей системе авторизационных данных синхронизированной с Keycloak.

Clients > Client details > Dedicated scopes > Mapper details

User Attribute

[redacted]

Mapper type	User Attribute
Name *	surname
User Attribute	lastName
Friendly Name	
SAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
SAML Attribute NameFormat	Basic
Aggregate attribute values	Off

Save Cancel

Clients > Client details > Dedicated scopes > Mapper details

User Attribute

[redacted]

Mapper type	User Attribute
Name *	givenname
User Attribute	firstName
Friendly Name	
SAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
SAML Attribute NameFormat	Basic
Aggregate attribute values	Off

Save Cancel

Clients > Client details > Dedicated scopes > Mapper details

User Attribute

[redacted]

Mapper type	User Attribute
Name *	emailaddress
User Attribute	email
Friendly Name	
SAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
SAML Attribute NameFormat	Basic
Aggregate attribute values	Off

Save Cancel