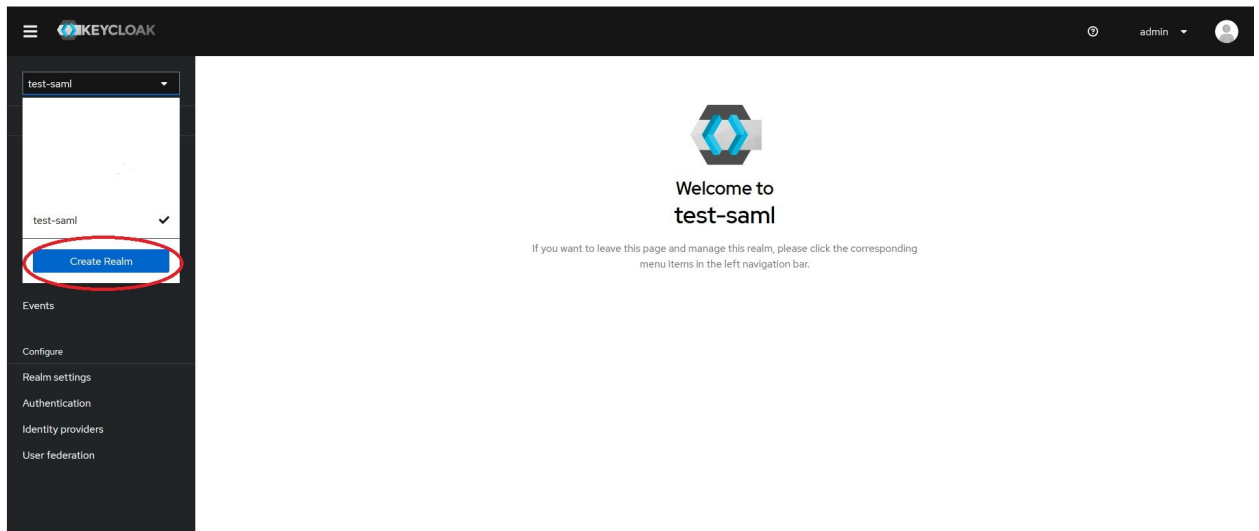
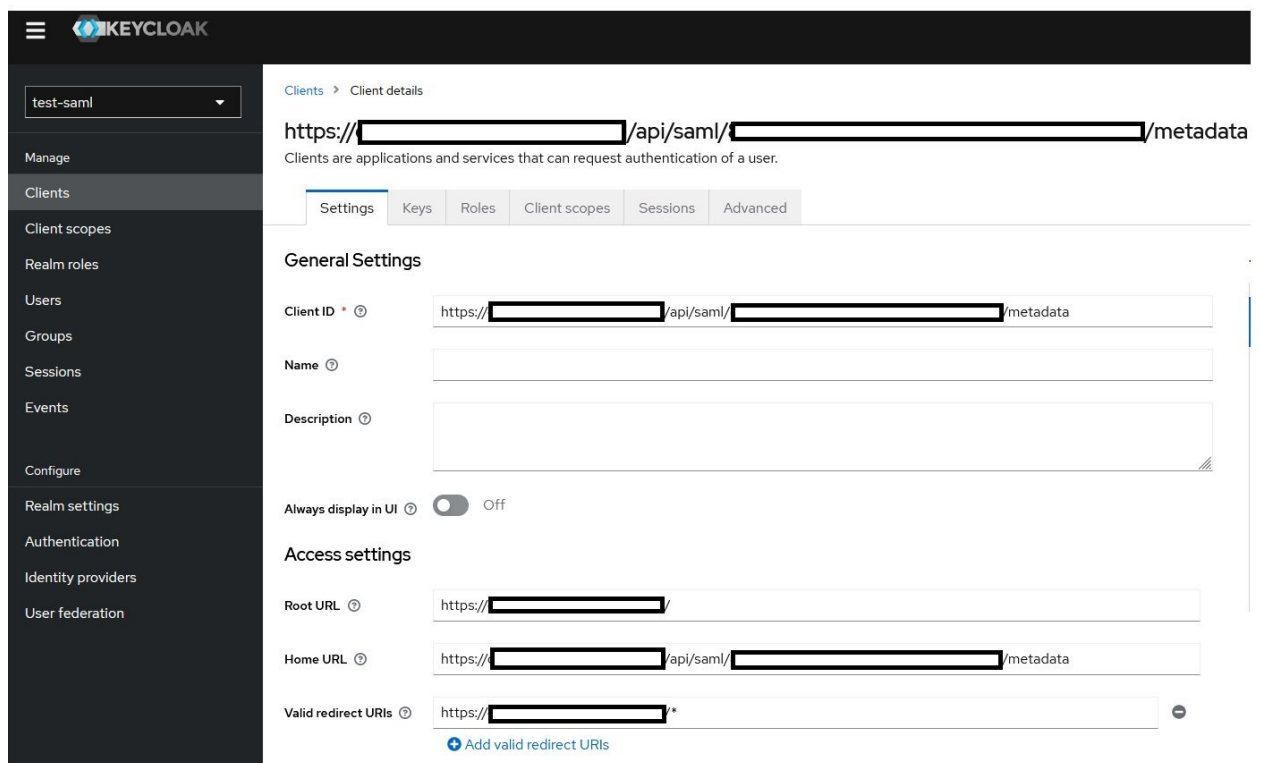
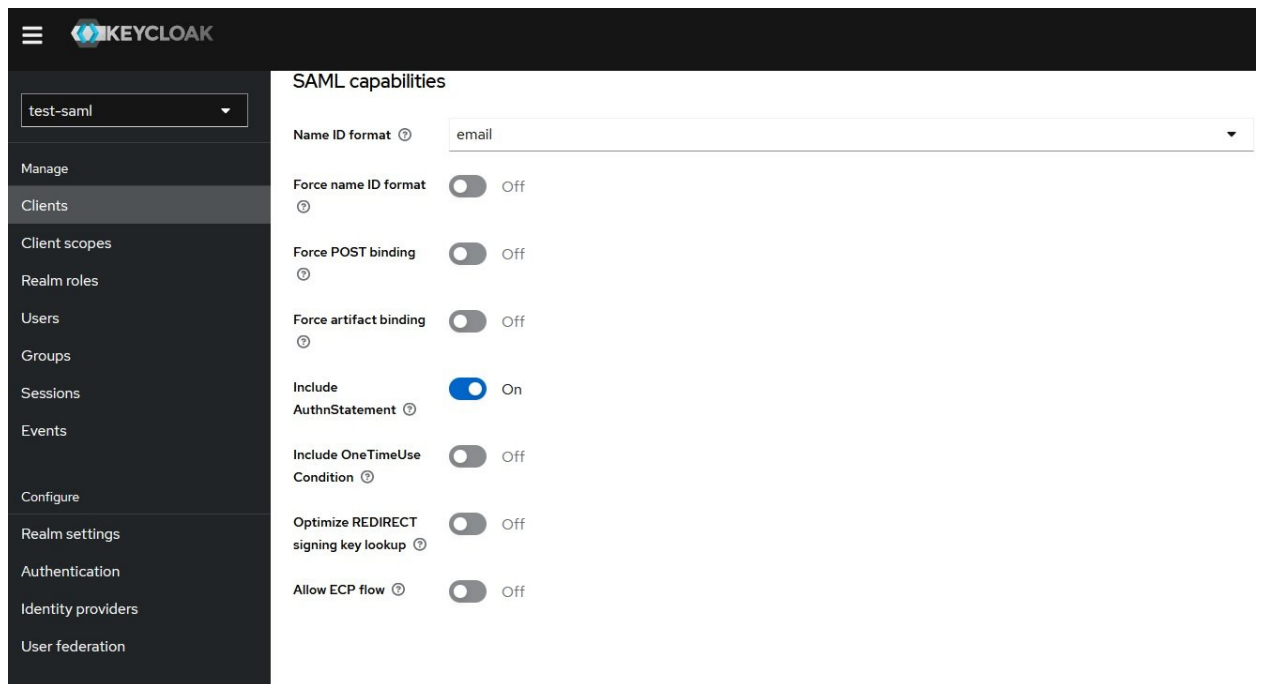


Создать новый Realm.



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





The screenshot shows the Keycloak administration interface. On the left is a dark sidebar with a menu. The top of the sidebar has a hamburger menu icon and the 'KEYCLOAK' logo. Below this is a dropdown menu showing 'test-saml'. The main menu items are: Manage, Clients (highlighted), Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'SAML capabilities'. It contains several settings: 'Name ID format' is a dropdown set to 'email'; 'Force name ID format', 'Force POST binding', 'Force artifact binding', 'Include OneTimeUse Condition', 'Optimize REDIRECT signing key lookup', and 'Allow ECP flow' are all toggle switches set to 'Off'; 'Include AuthnStatement' is a toggle switch set to 'On'.

test-saml

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

SAML capabilities

Name ID format ⓘ email

Force name ID format ⓘ Off

Force POST binding ⓘ Off

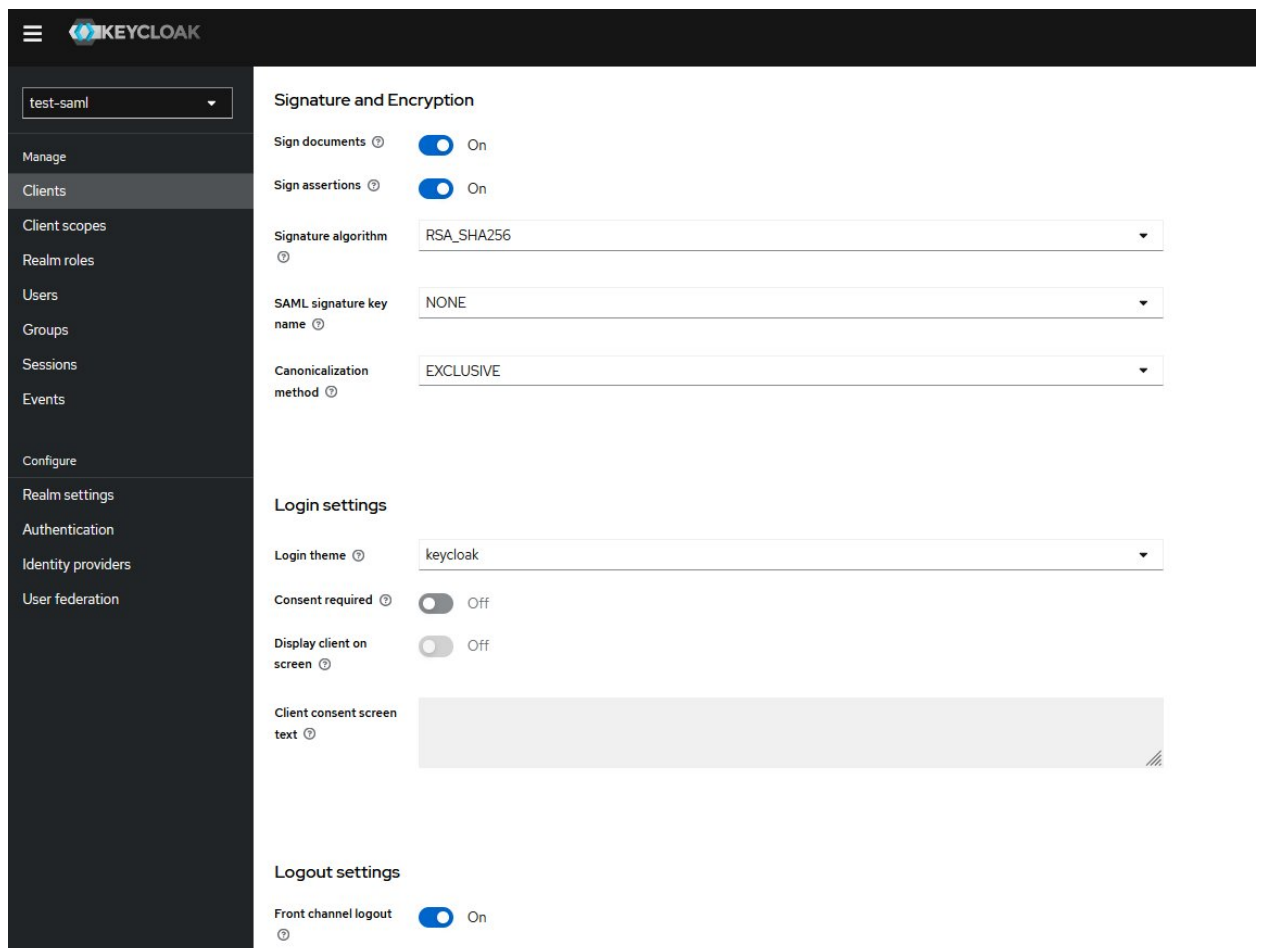
Force artifact binding ⓘ Off

Include AuthnStatement ⓘ On

Include OneTimeUse Condition ⓘ Off

Optimize REDIRECT signing key lookup ⓘ Off

Allow ECP flow ⓘ Off



The screenshot shows the 'Signature and Encryption' configuration page in Keycloak. The sidebar is identical to the previous screenshot. The main content area is titled 'Signature and Encryption'. It contains: 'Sign documents' and 'Sign assertions' are toggle switches set to 'On'; 'Signature algorithm' is a dropdown set to 'RSA_SHA256'; 'SAML signature key name' is a dropdown set to 'NONE'; 'Canonicalization method' is a dropdown set to 'EXCLUSIVE'. Below this is the 'Login settings' section: 'Login theme' is a dropdown set to 'keycloak'; 'Consent required' and 'Display client on screen' are toggle switches set to 'Off'; 'Client consent screen text' is a large text area. At the bottom is the 'Logout settings' section: 'Front channel logout' is a toggle switch set to 'On'.

test-saml

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Signature and Encryption

Sign documents ⓘ On

Sign assertions ⓘ On

Signature algorithm ⓘ RSA_SHA256

SAML signature key name ⓘ NONE

Canonicalization method ⓘ EXCLUSIVE

Login settings

Login theme ⓘ keycloak

Consent required ⓘ Off

Display client on screen ⓘ Off

Client consent screen text ⓘ

Logout settings

Front channel logout ⓘ On

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».

МояКоманда

Назад

Поставщик единого входа (SSO)

Нет Аутентификация SAML

URL IDP SSO *

https://[redacted]/realms/test-saml/protocol/saml

IDP Entity ID *

https://[redacted]/realms/test-saml

Сертификат *

☐ Создавать новых сотрудников при первой успешной авторизации

ACS URL: https://[redacted]/api/saml/[redacted]/acs

Entity ID: https://[redacted]/api/saml/[redacted]/metadata

Сохранить

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

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Settings Keys Roles Client scopes Sessions Advanced

Signing keys config

If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the client will sign their saml requests and responses. The signature will be validated.

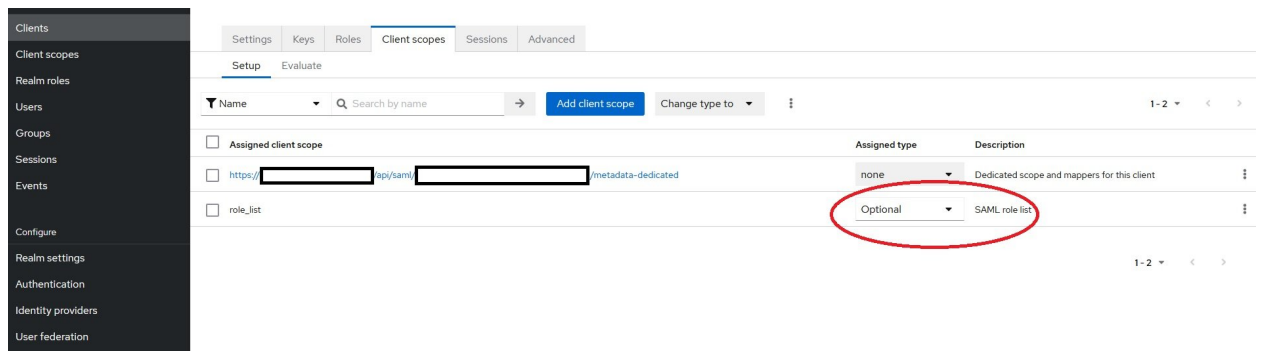
Client signature required ☐ Off

Encryption keys config

If you enable the "Encryption assertions" below, you must configure the encryption keys by generating or importing keys, and the SAML assertions will be encrypted with the client's public key using AES.

Encrypt assertions ☐ Off

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».

Поставщик единого входа (SSO)

Нет [Аутентификация SAML](#)

URL IDP SSO *

Введите

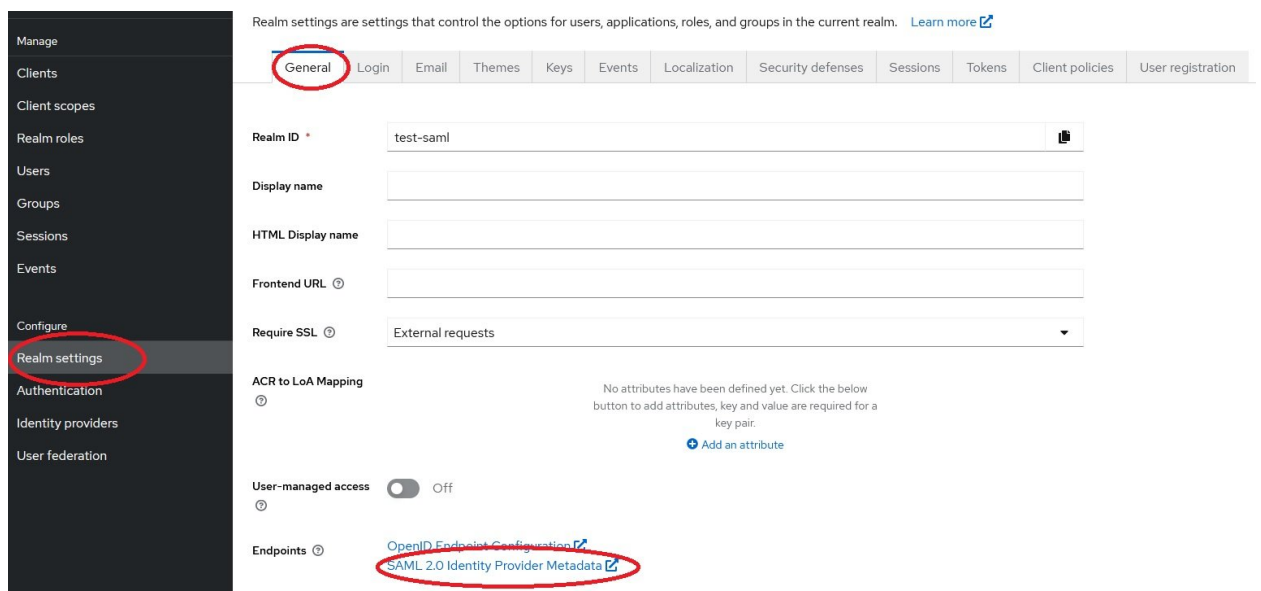
IDP Entity ID *

Введите

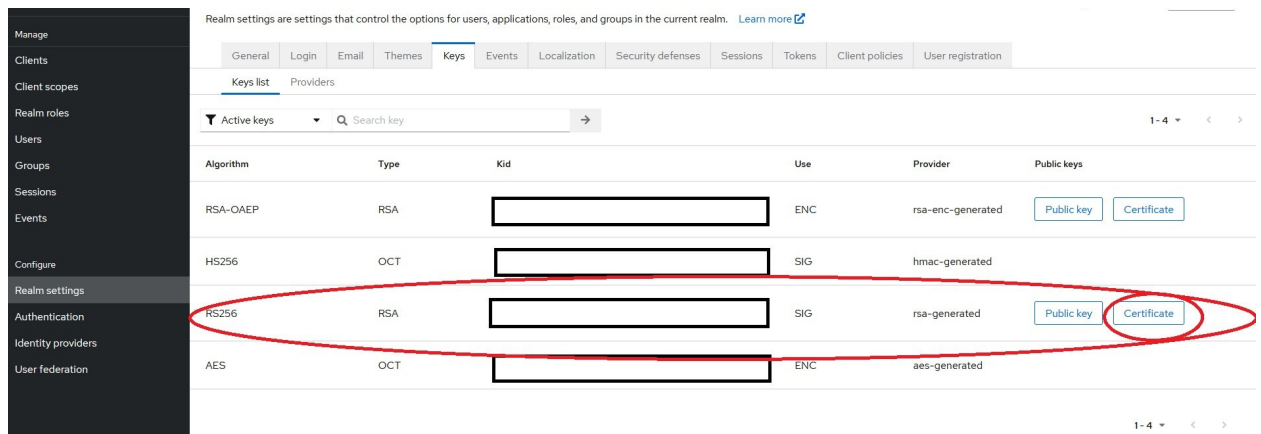
Сертификат *

Введите

Данные для полей «URL IDP SSO», «IDP Entity ID» находятся в Keycloak, Realm Settings (Раздел меню слева, секция Configure), вкладка General, 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».

☒ Создавать новых сотрудников при первой успешной авторизации

Соответствие полей сотрудника и атрибутов в ADFS *

Поля сотрудника *	Claim type в ADFS *
Фамилия	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Имя	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
E-mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

[Добавить](#)

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.

Mappers			
Name	Category	Type	Priority
surname	AttributeStatement Mapper	User Attribute	0
emailaddress	AttributeStatement Mapper	User Attribute	0
givenname	AttributeStatement Mapper	User Attribute	0

User Attribute

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

User Attribute

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

User Attribute

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