## Создать новый Realm.



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

test-saml 💌	Clients > Client details	s /api/saml/	/metadata
Manage	Clients are application	ns and services that can request authentication of a user.	-
Clients	Sattings	Pales Clientecones Services Advanced	
Client scopes	Settings Rey	ys nues clientiscopes Sessions Auvanced	
Realm roles	General Settings	5	·
Users	Client ID * ③	https://	
Groups			
Sessions	Name ⑦		
Events	Description ⑦		
Configure			lh.
Realm settings	Always display in UI 💿	Off	
Authentication	Access settings		
Identity providers	, locess sectings		
User federation	Root URL ③	https://	
	Home URL ③	https://///metadata	
	Valid redirect URIs ⑦	https://	0
		• Add valid redirect URIs	70

	SAML capabilities		
test-saml 🔹	Name ID format 💿	email	•
Manage	Force name ID format	O off	
Clients	0		
Client scopes	Force POST binding	Off Off	
Realm roles	0		
Users	Force artifact binding	Off Off	
Groups	0		
Sessions	Include AuthnStatement ⑦	On On	
Events			
	Include OneTimeUse Condition ⑦	Off	
Configure		_	
Realm settings	Optimize REDIRECT signing key lookup ⑦	O off	
Authentication	Allow FCP flow		
Identity providers	Allow ECF IIOW	Off	
User federation			

test-saml 🔹	Signature and End	cryption	
Manage	Sign documents ③	On On	
Clients	Sign assertions ③	On On	
Client scopes	Signature algorithm	RSA_SHA256	•
Realm roles	0		
Users	SAML signature key	NONE	•
Groups	name 💿		
Sessions	Canonicalization	EXCLUSIVE	•
Events	method ⑦		
Configure			
Realm settings	Login settings		
Authentication		( a second	
Identity providers	Login theme (2)	keycloak	•
User federation	Consent required ③	Off Off	
	Display client on	Off Off	
	screen (?)		
	Client consent screen		
	text ①		11
	Logout settings		
	Front channel logout	On On	
	0		

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	Кназад
<ul> <li>Структура компании &gt;</li> <li>Сотрудники</li> <li>График отсутствий</li> <li>Новости</li> <li>База ананий</li> <li>Пульс компании</li> <li>Есть идея</li> </ul>	Поставщик единого входа (SSO) Mer Дутентификация SAME URL IOP SSO * https:///realms/test-sami/protocol/sami IDP Entity ID * https:///realms/test-sami Eeprudpikar *
<ul> <li>Корпоративный магазин</li> <li>Заквки</li> <li>О компании</li> <li>Управление персоналом</li> <li>Управление задачами</li> </ul>	
<ul> <li>Эффективность &gt;</li> <li>Д. Отчёты</li> <li>Рекрутинг &gt;</li> <li>Обучение</li> <li>Развитие</li> <li>Опросы</li> </ul>	Создавать новых сотрудников при первой успешной авторизации ACS URL: https:///api/sami///acs PR0iy ID: https:///api/sami//metadata Corpassure.

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

Clients	Settings Keys Roles Clientscopes Sessions Advanced
Client scopes	
Realm roles	
Users	Signing keys config
Groups	If you enable the "Client signature required" below you must configure the signing keys by generating or importing keys and the
Sessions	client will sign their saml requests and responses. The signature will be validated.
Events	Client signature Off
Castieure	required 🕐
Roalm cattings	
Authentication	
Identity providers	Encryption keys config
User federation	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).

Cliente			
Clients	Settings Keys Roles Client scopes Sessions Advanced		
Client scopes	Setup Evaluate		
Realm roles			
Users	▼ Name       ▼       Add client scope       Change type to       ▼		1-2 💌 🔇 🚿
Groups		Antinendance	Description
Sessions	Assigned client scope	Assigned type	Description
Events	https:// /metadata-dedicated	none 🗸	Dedicated scope and mappers for this client
	role_list	Optional -	SAML role list
Configure			
Realm settings			1-2 👻 < >
Authentication			
Identity providers			
User federation			

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

авщик единого входа (SSO)	
Аутентификация SAML	
LIDP SSO *	
Зведите	
P Entity ID *	
Зведите	
ртификат *	
ведите	
	//0

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.

Manage	Realm settings are settir	ngs that control	the options for u	sers, applica	tions, roles, and g	roups in the current re	alm. Learn r	nore 🗹		
Clients	General Login	Email Tl	hemes Keys	Events	Localization	Security defenses	Sessions	Tokens	Client policies	User registration
Client scopes	$\smile$									
Realm roles	Realm ID *	test-saml							نل	
Users	Display pame									
Groups	-									
Sessions	HTML Display name									
Events	Frontend URL ⑦									
Configure	Require SSL ③	External reques	sts						•	
Realm settings	ACD to LoA Managing									
Authentication	⑦			No attrib button to a	utes have been def add attributes, key a	ined yet. Click the below ind value are required for a	a			
Identity providers					key pa	air.				
User federation					O Add an a	ittribute				
	User-managed access	Off								
	Endpoints ③	OpenID Endpoin AML 2.0 Identit	t Configuration I ty Provider Meta	data 🖄						

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

	Realm settings a	are setting	is that conf	rol the optic	ons for us	ers, applica	tions, roles, and ç	groups in the current re	alm. Learn r	more 🗹					
Clients	General	Login	Email	Themes	Keys	Events	Localization	Security defenses	Sessions	Tokens	Client policies	User registration			
Client scopes	Keys list	Provide	rs												
Realm roles	T Active keys	•	Q Sear	ch key			$\rightarrow$							1-4 -	< >
Users															
Groups	Algorithm			Туре		Kid				Use		Provider	Public keys		
Sessions Events	RSA-OAEP			RSA						ENC		rsa-enc-generated	Public key	Certificate	
Configure	HS256			ост						SIG		hmac-generated			
Realm settings Authentication	RS256			RSA						SIG		rsa-generated	Public key	Certificate	$\supset$
User federation	AES			ост		T				ENC		aes-generated			
														1-4 -	\$

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

Соответствие полей сотр	удника и а	атрибутов в ADFS *
Поля сотрудника *		Claim type B ADFS *
Фамилия	~	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Поля сотрудника *		Claim type в ADFS *
Имя	$\sim$	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Поля сотрудника *		Claim type в ADFS *
E-mail	~	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

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.

Add mapper 🔹		1-3 🔻 <	>
Category	Туре	Priority	
AttributeStatement Mapper	User Attribute	0	:
AttributeStatement Mapper	User Attribute	0	:
AttributeStatement Mapper	User Attribute	0	:
	Add mapper  Category AttributeStatement Mapper AttributeStatement Mapper AttributeStatement Mapper	Add mapper     Type       Category     Type       AttributeStatement Mapper     User Attribute       AttributeStatement Mapper     User Attribute       AttributeStatement Mapper     User Attribute	Add mapper     Instruction       Category     Type     Priority       AttributeStatement Mapper     User Attribute     0       AttributeStatement Mapper     User Attribute     0       AttributeStatement Mapper     User Attribute     0       AttributeStatement Mapper     User Attribute     0

1-3 ▼ 〈 >

Clients > Client details > Dedicated scopes > Mapper details

## User Attribute

Mapper type	User Attribute
lame * ③	surname
Jser Attribute 🕐	lastName
riendly Name 💿	
SAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
AML Attribute JameFormat ⑦	Basic 🔹
Aggregate attribute values ③	Off

Clients > Client details > Dedicated scopes > Mapper details

## User Attribute

Mapper type	User Attribute
Name * 🕐	givenname
User Attribute ③	firstName
Friendly Name 💿	
SAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
SAML Attribute NameFormat ③	Basic 🔹
Aggregate attribute values 💿	Off
	Save

Clients > Client details > Dedicated scopes > Mapper details

Mapper type	User Attribute
Name * 💿	emailaddress
Jser Attribute 💿	email
riendly Name 💿	
GAML Attribute Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
GAML Attribute NameFormat ③	Basic
ggregate attribute	Off